



CLAVISTER®

Clavister NetWall W50 Getting Started Guide

Clavister AB
Sjögatan 6J
SE-89160 Örnsköldsvik
SWEDEN

Head office/Sales: +46-(0)660-299200
Customer support: +46-(0)660-297755
www.clavister.com

Published 2019-04-03
Copyright © 2019 Clavister AB

Clavister NetWall W50

Getting Started Guide

Published 2019-04-03

Copyright © 2019 Clavister AB

Copyright Notice

This publication, including all photographs, illustrations and software, is protected under international copyright laws, with all rights reserved. Neither this manual, nor any of the material contained herein, may be reproduced without the written consent of Clavister.

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	5
1. W50 Product Overview	7
1.1. Unpacking the W50	7
1.2. Interfaces and Ports	10
1.3. Display and Keypad	12
1.4. Hardware Sensor Monitoring	14
2. Registering with Clavister	16
3. W50 Installation	21
3.1. General Installation Guidelines	21
3.2. Flat Surface Installation	23
3.3. Rack Installation	24
3.3.1. Front Bracket Installation	24
3.3.2. Side-Rail Installation	25
3.4. Management Computer Connection	29
3.5. Local Console Port Connection	32
3.6. Connecting Power	34
4. cOS Core Configuration	37
4.1. Web Interface and Wizard Setup	37
4.2. Manual Web Interface Setup	47
4.3. Manual CLI Setup	61
4.4. License Installation Methods	69
4.5. Setup Troubleshooting	71
4.6. Going Further with cOS Core	73
5. W50 Maintenance	76
5.1. Power Supply Replacement	76
5.2. Fan Module Replacement	79
6. Interface Expansion Modules	83
7. Resetting to Factory Defaults	88
8. Warranty Service	91
9. Safety Precautions	93
A. W50 Specifications	96
B. Declarations of Conformity	98
C. Windows 7 IP Setup	100
D. Windows 8/8.1/10 IP Setup	102
E. Apple Mac IP Setup	105

List of Figures

1.1. An Unpacked Clavister W50	7
1.2. Clavister W50 Connection Ports	10
1.3. W50 Interface Ports (including expansion module)	10
1.4. The W50 Display and Keypad	12
3.1. The W50 Local Console Port	32
3.2. Rear view of the Clavister W50	34
3.3. W50 Power Switch and Power Inlet Socket	35
5.1. The Installed W50 Fan Modules	79
6.1. An 8 x RJ45 Gigabit Interface Expansion Module for the W50	83
6.2. An 8 x SFP Gigabit Interface Expansion Module for the W50	84
6.3. A 2 x SFP+ 10 Gigabit Interface Expansion Module for the W50	84
6.4. An Example of an SFP 1000 Base TX Module	86
6.5. Insertion of a Gigabit SFP Module	87
7.1. Factory Reset Using the Web Interface	89

Preface

Target Audience

The target audience for this guide is the administrator who has taken delivery of a packaged Clavister W50 appliance and is setting it up for the first time. The guide takes the user from unpacking and installation of the device through to power-up, including network connections and initial cOS Core 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.

Notes to the main text

Special sections of text which the reader should pay special attention to are indicated by icons on 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 emphasized 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.

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, W50 Specifications*.

Web links

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

Trademarks

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

cOS Core is the trademark of Clavister AB.

Windows, Windows XP, Windows Vista, Windows 7, Windows 8 and *Windows 10* are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Apple, Mac and *Mac OS* are trademarks of Apple Inc. registered in the United States and/or other countries.

Chapter 1: W50 Product Overview

- Unpacking the W50, page 7
- Interfaces and Ports, page 10
- Display and Keypad, page 12
- Hardware Sensor Monitoring, page 14



Important: Only cOS Core version 11.00.00 or later is supported

The W50 hardware product can run any cOS Core version from 11.00.00 onwards. Earlier versions are not supported and a downgrade should not be attempted.

1.1. Unpacking the W50



Figure 1.1. An Unpacked Clavister W50

This section details the unpacking of a single W50 device. Open the packaging box used for shipping and carefully unpack the contents. The packaging should contain the following:

- The Clavister W50 unit.
- RJ45 console cable.

- Power cable.
- Rack mount kit consisting of:
 - i. 2 x brackets with screws suitable for a 19-inch rack.
 - ii. 2 x ball-bearing slide-rails with screws.

The W50 comes with a single power supply unit (PSU) installed in the device as standard. A second PSU for redundancy can be ordered separately from the Clavister sales office and fitted on-site into the unused PSU slot on the back of the device. This topic is discussed further in *Section 5.1, "Power Supply Replacement"*.



Note: Report any items that are missing

If any items are missing from the W50 package, please contact the reseller or distributor. All relevant documentation in PDF format can be downloaded from the Clavister website and is included in all packaged distributions of new cOS Core versions.

Support Agreements

All purchasers of Clavister hardware products should subscribe to one of the available cOS Core support agreements. These provide access to cOS Core updates and provide a hardware replacement service in the case of a hardware fault. Without one of these agreements, hardware warranty is limited to 2 years. The warranty terms are described further in *Chapter 8, Warranty Service*, along with a description of the hardware replacement procedure.

The Cold Standby Service

To ensure maximum uptime, a *Cold Standby (CSB) Service* is available from Clavister as an addition to certain cOS Core support agreements. This service allows a second, identical W50 unit to be purchased at a discount so that it can quickly substitute for the original unit in case of failure, with the ability to quickly reassign the original cOS Core license to the standby unit. When the faulty unit is returned to Clavister, a new cold standby unit is immediately sent back. More details about the CSB service can be found in the separate *Hardware Replacement Guide*.

Downloadable W50 Resources

All documentation and other resources for the W50 can be downloaded from the W50 product page which can be found by going to <https://www.clavister.com/start> and selecting the W50 link.

Contacting Clavister Product Support

Clavister customer support can be contacted by logging in as a customer and reporting an issue on the company website at <https://www.clavister.com>. Alternatively, the direct support telephone number is +46 (0)660-29 77 55 (answered 24/7). Sales enquiries should be directed to the head office number +46 (0)660-29 92 00.

End of Life Treatment

The W50 device is marked with the European *Waste Electrical and Electronic Equipment* (WEEE)

directive symbol which is shown below.



The product, and any of its parts, should not be discarded using a regular refuse disposal method. At end-of-life, the product and parts should be given to an appropriate service that deals with the removal of such specialist materials.



CAUTION: REPLACE INTERNAL BATTERIES CORRECTLY

THERE IS A RISK OF EXPLOSION IF AN INTERNAL BATTERY IS REPLACED WITH THE INCORRECT TYPE. DISPOSE OF ANY USED INTERNAL BATTERIES ACCORDING TO THE INSTRUCTIONS.

1.2. Interfaces and Ports

This section is an overview of the W50 product's external design.



Figure 1.2. Clavister W50 Connection Ports

The W50 features the following connection ports on the front panel:

- A single fixed RJ45 Gigabit Ethernet interfaces with the logical cOS Core name **G1**. This is the default interface for management access over a network. However, it can be used for other purposes.
- An RS-232 RJ45 port for console connection marked with the letter **C**. This port is used for direct access to the cOS Core *Boot Menu* and the cOS Core *Command Line Interface (CLI)*. Connection to this port is discussed in *Section 3.5, "Local Console Port Connection"*.
- 4 x PCIe Ethernet interface expansion slots on the right side of the front panel. In a new unit, these slots are covered with a removable panel. Expansion modules can be ordered separately for these slots and the following module options are available:
 - i. 8 x RJ45 Gigabit Ethernet interfaces.
 - ii. 8 x SFP Gigabit interfaces.
 - iii. 2 x SFP+ 10 Gigabit interfaces.

Module installation is discussed in *Chapter 6, Interface Expansion Modules* as well as details about logical name assignment in cOS Core.



Note: The two USB Type A ports are not currently used

The two **USB Type A** ports on the W50 front panel are for future functionality and are not currently used by cOS Core.

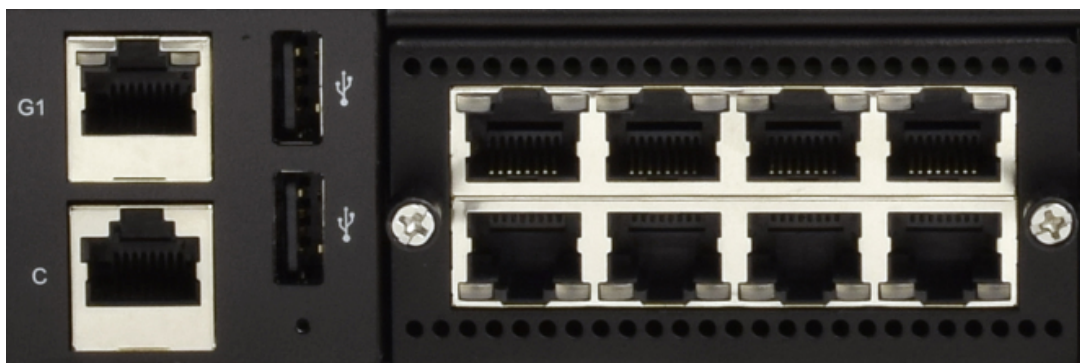


Figure 1.3. W50 Interface Ports (including expansion module)

The full connection capabilities of all W50 Ethernet interfaces are listed in *Appendix A, W50 Specifications*.

1.3. Display and Keypad

The W50 features a display and keypad on the left side of the front panel. This consists of an LCD display and 4 navigation buttons. The buttons are used to either move forwards or backwards through a sequential list of cOS Core system parameters.

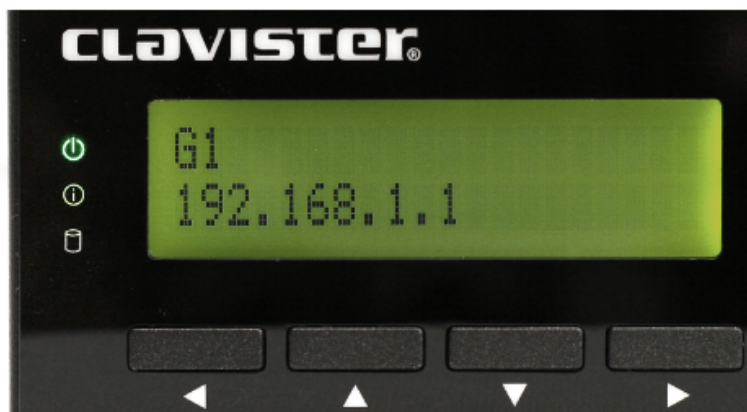


Figure 1.4. The W50 Display and Keypad

Pressing either the **Right** or **Up** button will go forward in the display sequence. Pressing either the **Left** or **Lower** button will go backwards in the sequence. When the end of the display sequence is reached, the display cycles back to the beginning.

The sequence of information that is shown in the display is as follows:

- **Hardware Model**

The model of hardware. This should always indicate W50.

- **Status**

This displays the message **Running** to indicate normal operation. If cOS Core is in 2 hour demonstration mode then this is indicated along with how much time is left before timeout. If cOS Core is in lockdown mode then this is shown.

- **Load and Connections.**

The CPU load is shown with the total number of current cOS Core state engine connections.

- **Throughput**

The data throughput of the Clavister Next Generation Firewall in bits per second and packets per second is shown. This is the total volume of all data traffic forwarded through the firewall over a one second interval.

These values are for raw data and include any overhead incurred with protocols such as IPsec. The actual throughput of, for example, unencrypted data flowing inside VPN tunnels, may be marginally less.

- **High Availability**

This shows the HA mode (master or slave) and the HA status (active or passive). If the W50 is not part of a high availability cluster, this information is skipped.

- **Time**

The date and time currently set for the hardware system clock is shown. If this is incorrect, it should be corrected through one of the cOS Core management interfaces.

- **Memory**

The current uptime (time since last restart), the total hardware RAM memory available to cOS Core and the current memory usage is shown.

- **Anti-Virus**

This shows the current signature count in the anti-virus database and the time of the last database update.

If the cOS Core anti-virus subsystem is not activated, this information is skipped.

- **IDP**

This shows the current signature count in the Intrusion Detection and Prevention (IDP) database and the time of the last database update.

If the IDP subsystem is not activated, this information is skipped.

- **Interfaces**

Multiple sets of information, one set for each physical Ethernet interface is shown. Each set consists of:

- i. The logical interface name in the cOS Core configuration.
- ii. The current link speed.
- iii. If the link is full-duplex (FD) or half-duplex (HD). This is not shown if the link speed is Gigabit since it will always be full-duplex.
- iv. The IPv4 address assigned to the interface.

- **Hardware Monitoring**

This consists of multiple sets of information, one for each sensor. The sensor information displayed shows operating temperatures and fan speeds.

Hardware monitoring must be enabled in cOS Core through one of the management interfaces for this to be shown, otherwise this information is skipped.

- **cOS Core version**

The version of cOS Core currently running in the W50.

After the cOS Core version is displayed, going forward will cycle back to the first information displayed in the sequence which is the hardware model.

1.4. Hardware Sensor Monitoring

The W50 is equipped with sensors that provide cOS Core with information about operational parameters such as CPU temperature. This information is available to the administrator through the cOS Core management interfaces.

In addition, log message alerts can be automatically generated if a sensor reaches a value outside of its normal operational range.

Configuring this feature, as well as a list of all the sensors available on each Clavister hardware model and their normal ranges, can be found in the *Hardware Monitoring* section of the separate *cOS Core Administration Guide*.

Chapter 2: Registering with Clavister

Before applying power to the W50 and starting cOS Core, it is important to understand the customer and product registration procedures. There are two types of registration:

- **Registering as a Clavister Customer**

This involves registering basic contact and company information on the Clavister website and establishing login credentials. Later, these credentials can also be used by cOS Core for automatically registering the W50 hardware unit and automatically downloading the correct license.

This is a mandatory requirement for all new customers and needs to be done only once. A description of doing this can be found below. Even if registration is not done before starting the cOS Core wizard, the wizard will provide a link to the registration page so it can be done while the wizard is running.

- **Registration of the W50 Hardware Unit**

This is mandatory for every hardware unit before a license can be downloaded. It can be done in the following ways:

- i. **Automatic registration after cOS Core starts** - This can be done by the *Setup Wizard* which starts automatically in the Web Interface when cOS Core is started for the first time. The wizard is described in *Section 4.1, "Web Interface and Wizard Setup"*.
- ii. **Manual registration of the W50 on the Clavister website** - This is described in the last half of this chapter. Manual registration may be necessary if the W50 does not have Internet access.

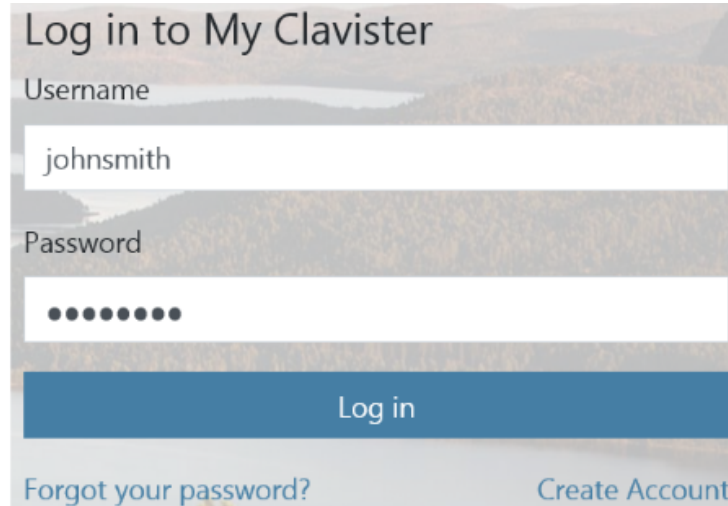
A. Registering as a Clavister Customer

The W50 registration steps for a first time user of Clavister hardware are as follows:

1. Open a web browser, go to **<https://www.clavister.com>** and select the **Login** link at the top of the page.



2. The *MyClavister* login page is presented. If you are already registered, log in and skip to step 8. If you are a new customer accessing *MyClavister* for the first time, click the **Create Account** link.



Log in to My Clavister

Username

johnsmith

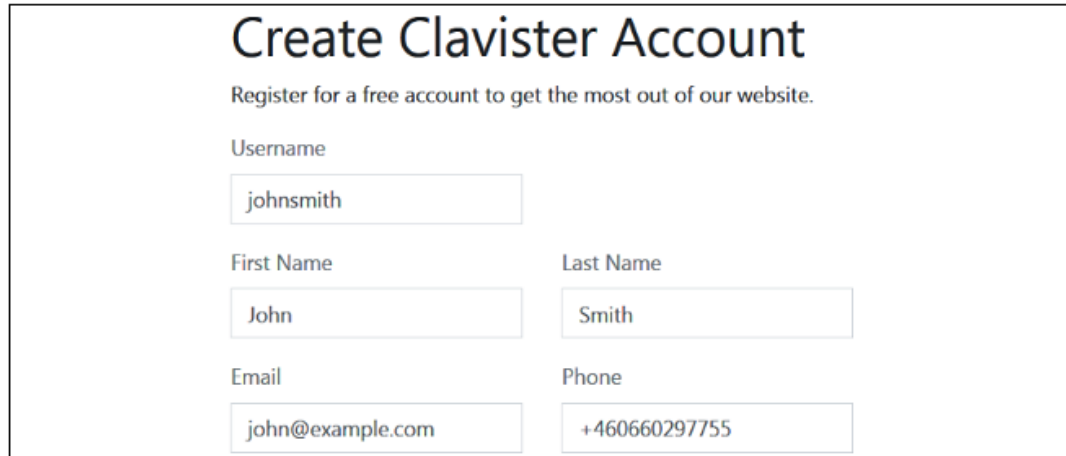
Password

●●●●●●●●

Log in

[Forgot your password?](#) [Create Account](#)

3. The registration page is now presented. The required information should be filled in. In the example below, a user called *John Smith* is registering.



Create Clavister Account

Register for a free account to get the most out of our website.

Username

johnsmith

First Name

John

Last Name

Smith

Email

john@example.com

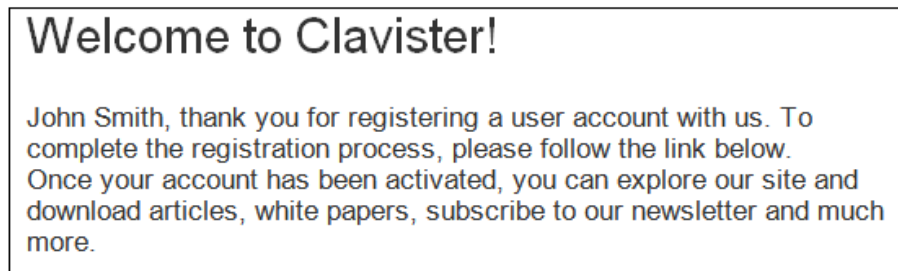
Phone

+460660297755

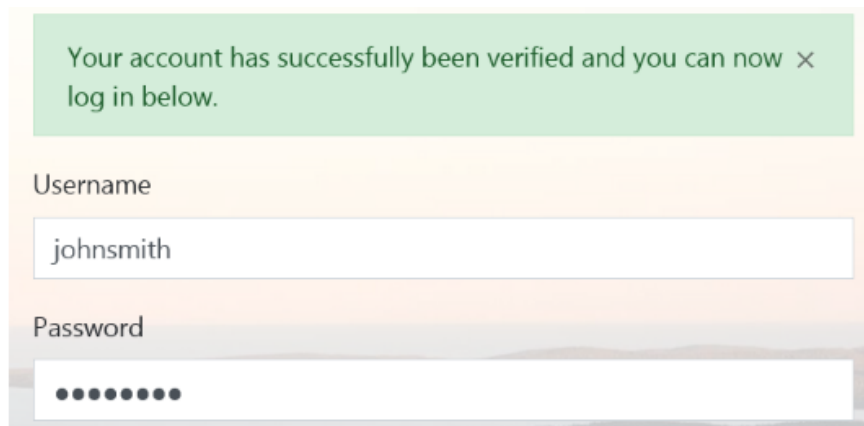
4. When the registration details are accepted, an email is sent to the email address given so that the registration can be confirmed.

Your account has successfully been created, but before you can login you must first verify your email address. An email has been sent to you with further instructions on how to complete the registration.

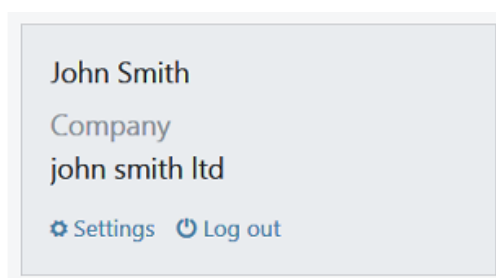
5. Below is an example of the heading in the email that would be received.



6. The confirmation link in the email leads back to the Clavister website to show that confirmation has been successful and logging in is now possible.



7. After logging in, the customer name is displayed with links for changing settings and logging out.

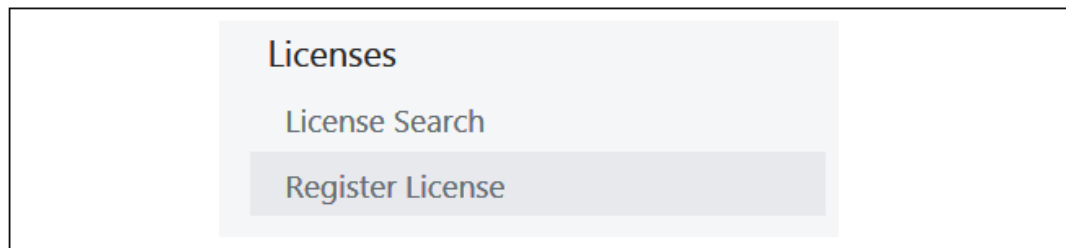


B. Registration of the W50 Hardware Unit

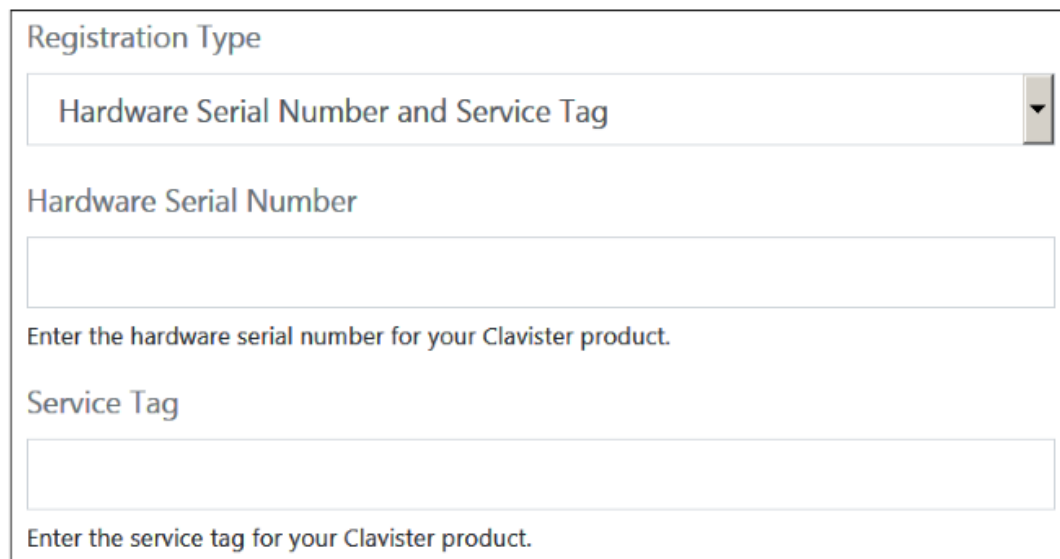
This section can be skipped if the W50 has access to the Internet. With Internet access available, registration can be performed automatically by the cOS Core *Setup Wizard* which will appear as a browser popup window in the Web Interface when cOS Core starts for the first time. The wizard is described in *Section 4.1, "Web Interface and Wizard Setup"*.

If the unit does not have Internet access then manual registration is required and this is done using the following steps:

1. Log in to the Clavister website and select the **Register License** option.



2. The registration page is displayed. Under the tab **Hardware Serial Number and Service Tag**, enter the *Hardware Serial Number* and *Service Tag* must be entered. **These two codes are found on a label which should be attached to the W50 hardware itself.** The label is usually found on the hardware's underside but may be found in another position.

A screenshot of a web registration form. At the top, there is a section titled 'Registration Type' with a dropdown menu. The dropdown menu is open, showing the selected option 'Hardware Serial Number and Service Tag'. Below this, there are two input fields. The first is labeled 'Hardware Serial Number' and has a text box below it. The second is labeled 'Service Tag' and also has a text box below it. Below each text box is a small instruction: 'Enter the hardware serial number for your Clavister product.' and 'Enter the service tag for your Clavister product.' respectively.

The image above shows an example label which illustrates the typical layout of identification labels found on Clavister hardware products.



After Successful Hardware Registration

Once the W50 hardware unit is registered, a cOS Core license for the unit becomes available for download and installation from Clavister servers. This installation can be done automatically through the cOS Core *Setup Wizard* which is described in *Section 4.1, "Web Interface and Wizard Setup"*.

If the W50 is not connected to the Internet, the license must be manually downloaded from the cOS Core website and then manually uploaded.

All license installation options are listed and discussed in *Section 4.4, "License Installation Methods"*.

Chapter 3: W50 Installation

- General Installation Guidelines, page 21
- Flat Surface Installation, page 23
- Rack Installation, page 24
- Management Computer Connection, page 29
- Local Console Port Connection, page 32
- Connecting Power, page 34

3.1. General Installation Guidelines

Follow these general guidelines when installing your Clavister W50 appliance:

- **Safety**

Take notice of the safety guidelines laid out in *Chapter 9, Safety Precautions*. These are specified in multiple languages.

- **Power**

Make sure that the power source circuits are properly grounded and then use the power cord supplied with the appliance to connect it to the power source.

- **Using Other Power Cords**

If your installation requires a different power cord than the one supplied with the appliance, be sure to use a cord displaying the mark of the safety agency that defines the regulations for power cords in your country. Such marks are an assurance that the cord is safe.

- **Power Overload**

Ensure that the appliance does not overload the power circuits, wiring and over-current protection.

To determine the possibility of overloading the supply circuits, add together the ampere ratings of all devices installed on the same circuit as the appliance and compare the total with the rating limit for the circuit. The maximum ratings for the W50 are listed in *Appendix A, W50 Specifications*.

- **Surge Protection**

A third party surge protection device should be considered and is strongly recommended as a means to prevent electrical surges reaching the appliance. This is mentioned again in *Section 3.6, "Connecting Power"*.

- **Temperature**

Do not install the appliance in an environment where the ambient temperature during operation might fall outside the specified operating range. This range is documented in *Appendix A, W50 Specifications*.

The intended operating temperature range is "room temperature". That is to say, the temperature most commonly found in a modern office and in which humans feel comfortable. This is usually considered to be between 20 and 25 degrees Celsius (68 to 77 degrees Fahrenheit). Special rooms for computer equipment may use a lower range and this is also acceptable.

- **Airflow**

Make sure that airflow around the appliance is not restricted.

- **Dust**

Do not expose the appliance to environments with elevated dust levels.



Note: The specifications appendix provides more details

*Detailed information concerning power supply range, operating temperature range and other operating details can be found at the end of this document in **Appendix A, W50 Specifications**.*

3.2. Flat Surface Installation

The W50 can be mounted on any appropriate stable, flat, level surface that can safely support the weight of the appliance and its attached cables. However, the W50 is designed to be rack mounted and installation on a flat surface is not recommended and should only be done for testing purposes.



Caution: Noise levels can be elevated from W50 fans

The W50 can emit elevated levels of fan noise and caution should be taken to protect hearing when spending extended periods of time in proximity to the appliance.

It is strongly recommended that the W50 operates within an acoustically contained area, such as a special computer room.



Important: Always leave space around the appliance

Always ensure there is adequate space around the appliance for ventilation and access to operating switches and cable connectors. No objects should be placed on top of the casing.

3.3. Rack Installation

The W50 is designed to be installed in most standard 19-inch equipment racks. The following general guidelines for racks should be followed:

- The rack or cabinet used for mounting should be adequately secured to prevent it from becoming unstable and/or falling over.
- Devices installed in the rack or cabinet should be mounted as low as possible, with the heaviest devices at the bottom and progressively lighter devices installed above.

Two Rack Mounting Kits Are Included

There are two rack mounting kits, included **both** must be installed for mounting the W50 into a rack. In the packaging for the W50 the following should be found:

- A front bracket kit.
- A side-rail kit.

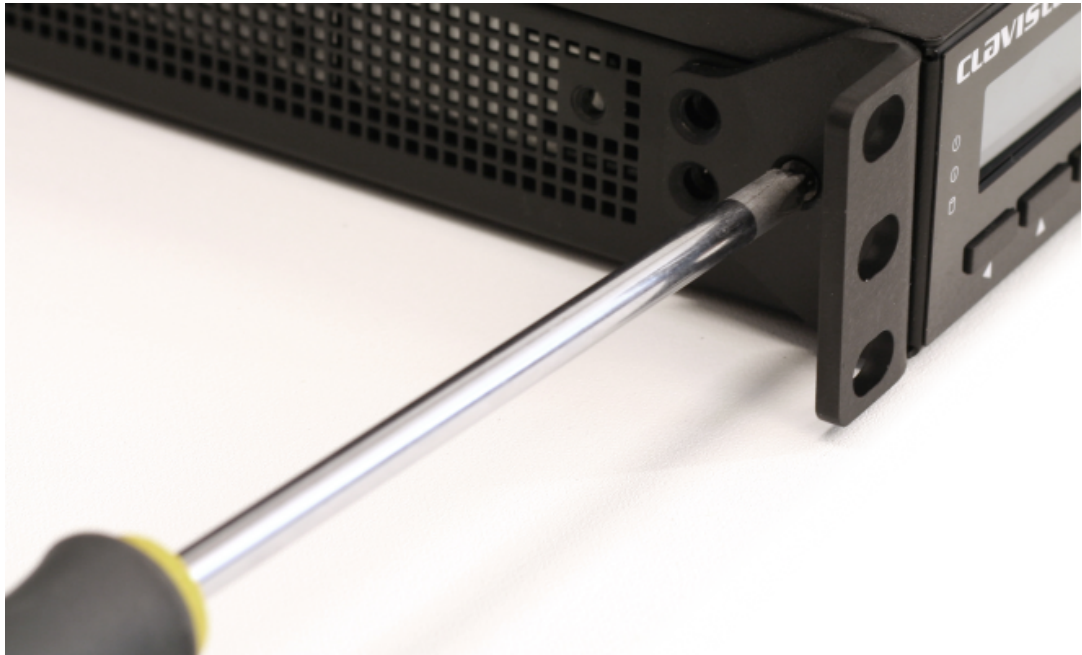
Installing these kits is described in the following two subsections. The ordering of attachment is not important but **both** should be installed before mounting the W50 in the rack.

3.3.1. Front Bracket Installation

The front bracket kit consists of two brackets, each of which has three screws for attachment to the front-sides of the W50 as shown in the image below. There are predrilled holes already in the sides of the which are used for attaching the brackets.



A bracket should be attached to each side of the W50 with a screwdriver using the screws supplied.



After attaching a bracket to either side of the unit, the next step is to install the side-rails parts on both the W50 and the rack. This is described next.

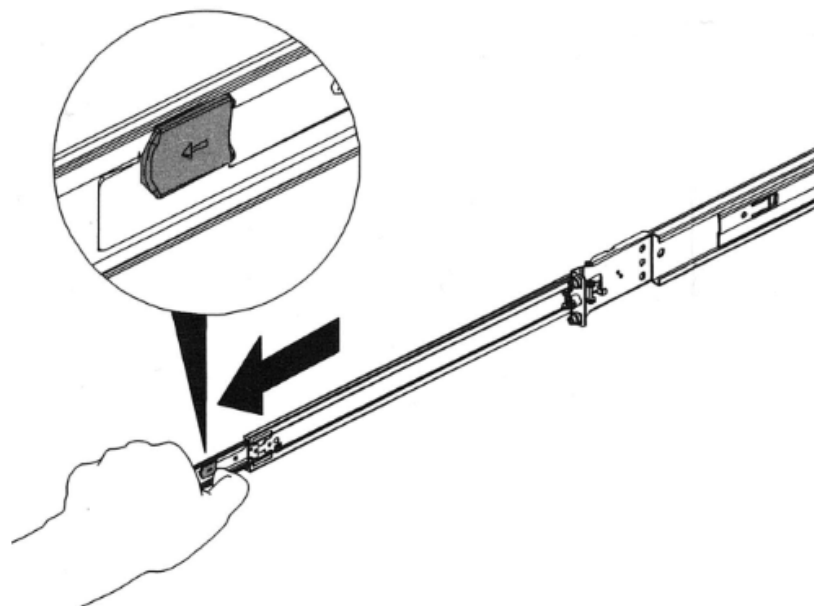
3.3.2. Side-Rail Installation

The side-rail kit consists of two ball-bearing slide-rails for either side of the W50. Each side-rail consists of two parts. One part attaches to a side of the W50 and the other part attaches to the rack. The W50 is then slid into the rack by re-engaging the two parts.

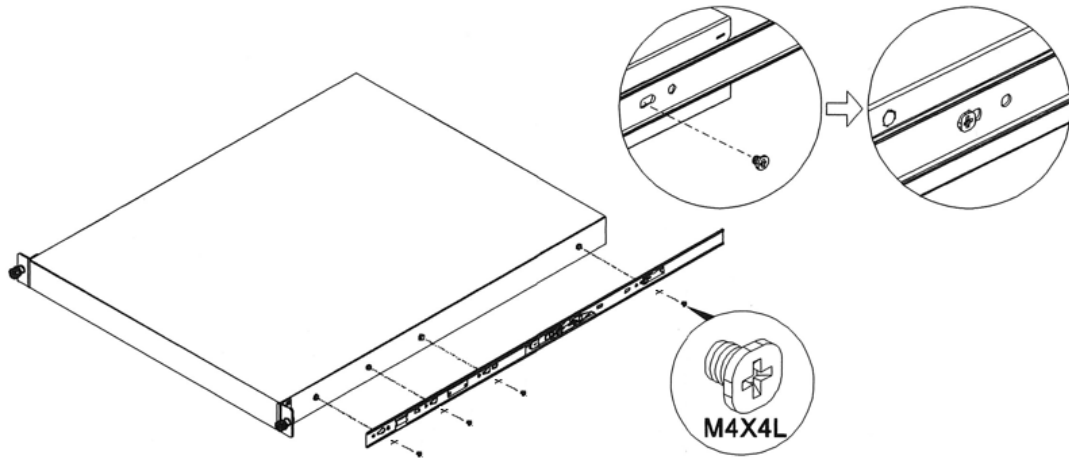
A. Installing the Rail

The steps for mounting a slide-rail on the side of the W50 and in the rack are as follows:

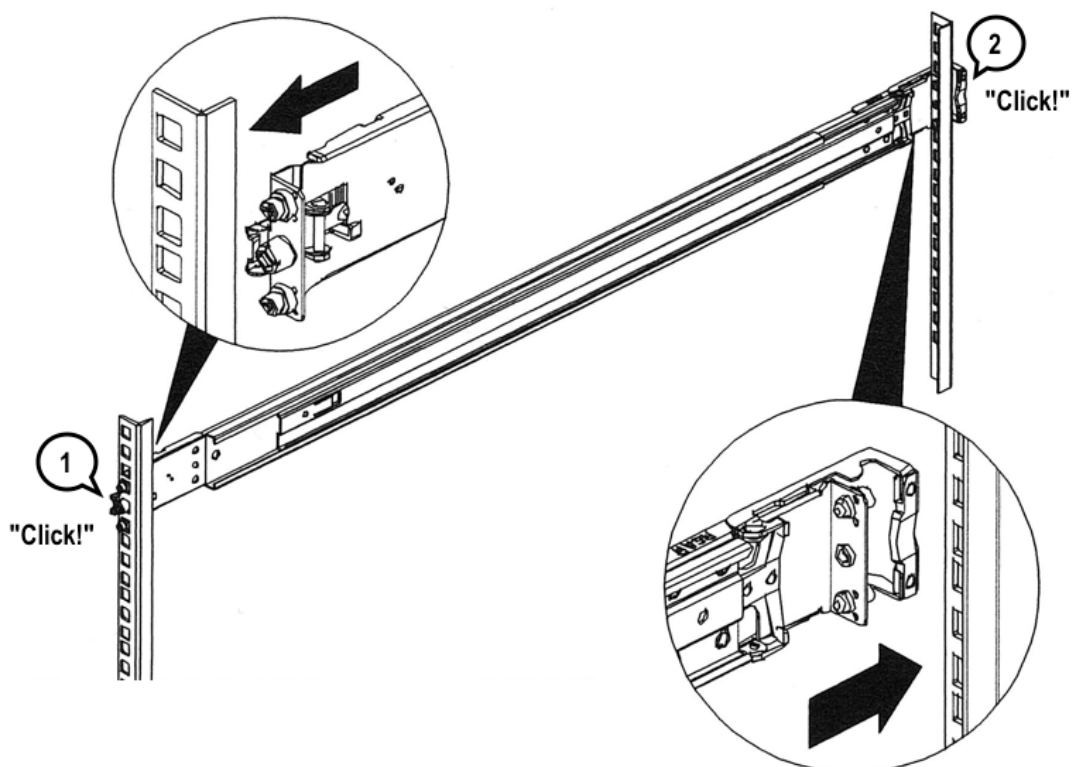
1. Release and detach the inner part of one of the rails by using the release latch.



2. Attach the inner part of the rail to one side of the W50 using the screws provided.



3. Attach the outer part of the rail to the rack by clicking into position (1 and 2 in the diagram below).

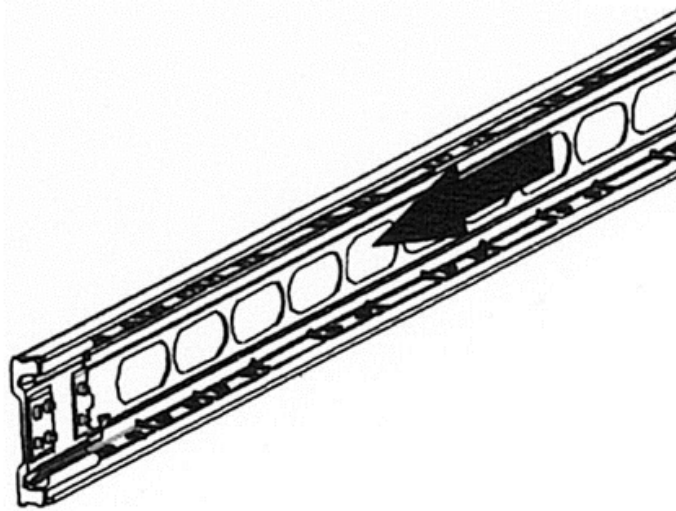


Now repeat the above steps to install the rail for the other side of the W50 unit.

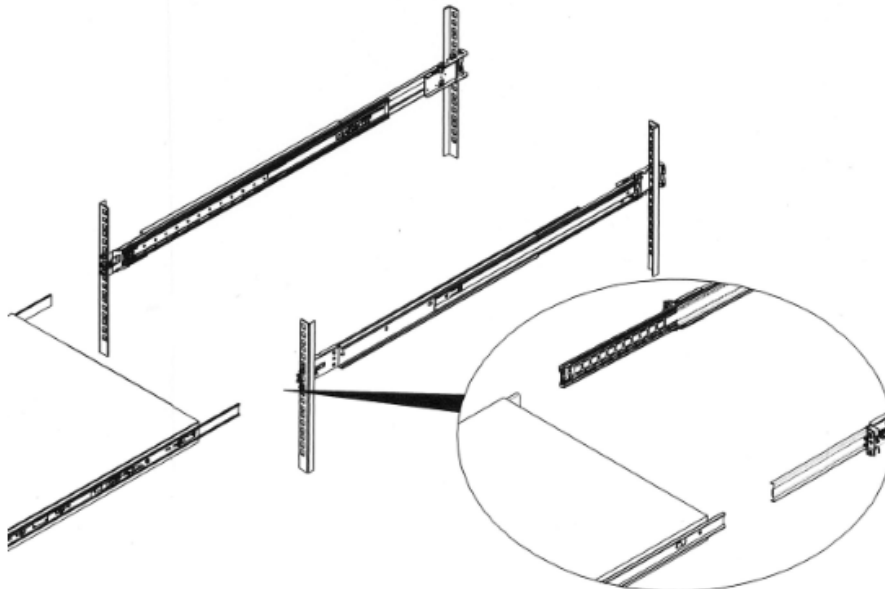
B. Mounting the W50 in the Rack

Now that the rails are installed on either side of the W50 and in the rack, the following steps describe mounting the W50 unit in the rack:

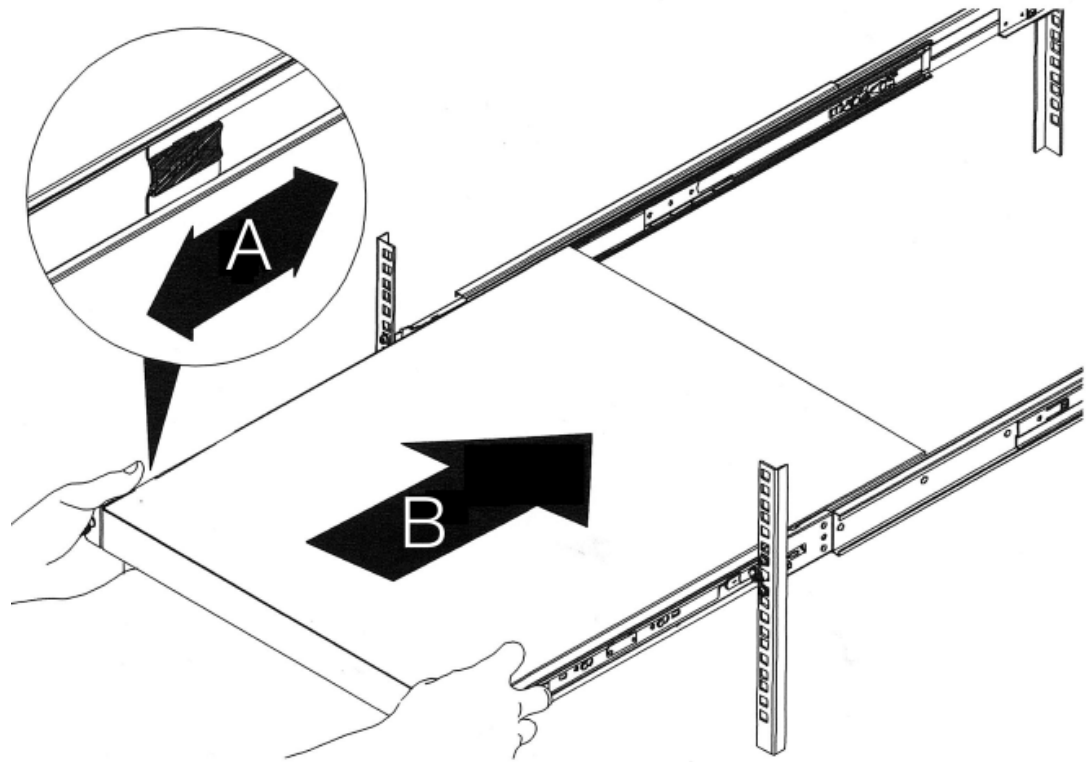
1. Slide the ball-bearing retainer on either side out so that they are locked in their most forward position.



2. With both ball-bearing retainers extended forward, line up the inner and outer rails and slide the W50 unit half way into position.



3. Slide the release tab **(A)** and push the W50 fully into the rack **(B)**.



3.4. Management Computer Connection

cOS Core Starts After Power Up

It is assumed that the W50 unit is now unpacked, positioned correctly and power is applied. If not, the earlier chapters in this manual should be referred to before continuing.

Clavister's cOS Core network security operating system is preloaded on the W50 and will automatically boot up after power is applied. After the start-up sequence is complete, an external management computer can be used to configure cOS Core. The management computer's operating system can be any kind as long it can run a standard modern web browser.

The Default Management Interface

After first time startup, cOS Core automatically makes management access available on a single predefined Ethernet interface and assigns the private IPv4 address **192.168.1.1** to it.

For the W50, the default management interface is the **G1** interface.

cOS Core Setup Methods

Initial cOS Core software configuration can be done in one of the following ways:

- **Using a web browser across a network connection**

A standard web browser running on a standalone management computer (sometimes referred to as the *management workstation*) can be used to access the cOS Core *Web Interface*. This provides an intuitive graphical interface for cOS Core management. When this 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 go directly to the Web Interface to perform setup manually.

The wizard is recommended for its simplification of initial setup and is described in detail in *Section 4.1, "Web Interface and Wizard Setup"*. The wizard assumes that configuring public Internet access is one of the tasks to be performed and has a step for this.

- **Using CLI commands across a network connection**

The setup process can be performed using CLI commands which are input into a remote management computer running console emulation software. The management computer is linked across a network to an Ethernet interface on the firewall.

Once a network link to the CLI has been established, the configuration steps using the CLI are described in *Section 4.3, "Manual CLI Setup"*.

The CLI allows step by step control of the setup process and should be used by administrators who fully understand both the CLI and the setup steps required.

- **Using CLI commands via the local console**

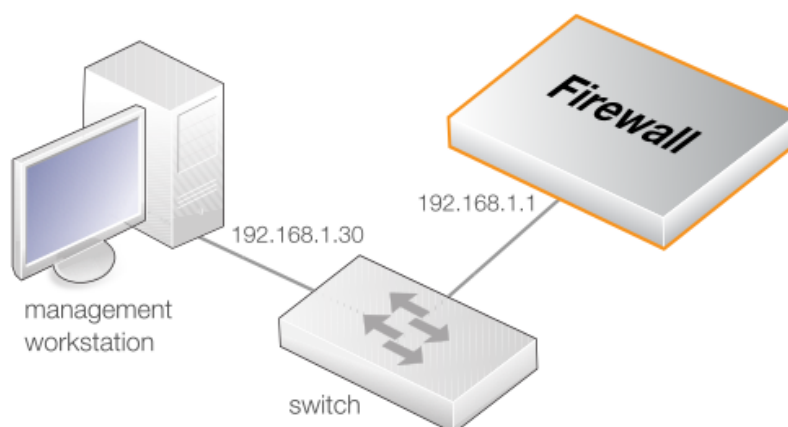
Alternatively, CLI access can be through console emulation software running on a management computer connected directly to the RJ45 local console port on the W50 hardware. Direct console connection is described in *Section 3.5, "Local Console Port Connection"*.

Network Connection Setup

For setting up access across a network using the Web Interface or the CLI via SSH, it is necessary to connect an Ethernet interface on an external management computer to the default management Ethernet interface on the W50.

The default management Ethernet interface for the W50 is **G1** and this is assigned the default IPv4 address of **192.168.1.1** by cOS Core. This interface should be connected to the same network as the management computer (or a network accessible from the management computer via one or more switches).

Typically, the connection between the management computer and the default management interface is made via a switch using standard Ethernet cables, as shown in the illustration below.



For connection to the public Internet, another W50 Ethernet interface should be connected to an ISP. In the cOS Core setup wizard this is referred to as the WAN interface. In this guide, it is assumed that the **E1-1** expansion module interface of the W50 (the first interface on the first expansion module) is used for Internet connection, although any other available interface could be used instead.

Direct Network Connection to the Firewall's Management Interface

Connection to the default management interface **G1** on the firewall from the management computer can be done directly without using switch hardware. This could be done using a crossover cable. However, all the RJ45 interfaces on the W50 support *Automatic MDI-X* and a crossover cable is not necessary with them.

Management Computer Ethernet Interface Setup

Traffic will be able to flow between the designated management computer interface and the Clavister Next Generation Firewall interface because they are on the same IP network. This means the management computer interface should be first assigned the following static IPv4 addresses:

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



Tip: Using another management interface IP address

*The IPv4 address assigned to the management computer's Ethernet interface, could be any address from the **192.168.1.0/24** network. However, the IP chosen must be different from **192.168.1.1** which is used by cOS Core's default management interface.*

The following appendices at the end of this guide describe how to set up the management computer IP with different operating systems:

- **Appendix C, Windows 7 IP Setup.**
- **Appendix D, Windows 8/8.1/10 IP Setup.**
- **Appendix E, Apple Mac IP Setup.**

3.5. Local Console Port Connection



Note: *Skip this section if using the Web Interface for set up*

Console port connection can be skipped if cOS Core setup is going to be done using the cOS Core Web Interface since neither CLI or boot menu access will be needed.

The local console port allows direct management connection to the W50, from a separate computer acting as a console terminal. Local console access can then be used for both management of cOS Core with CLI commands or to enter the *boot menu* in order to access W50 firmware loader options.

The *local console port* is the physical RJ45 RS-232 port on the left-hand side front panel of the W50 and this is marked with the letter "C".

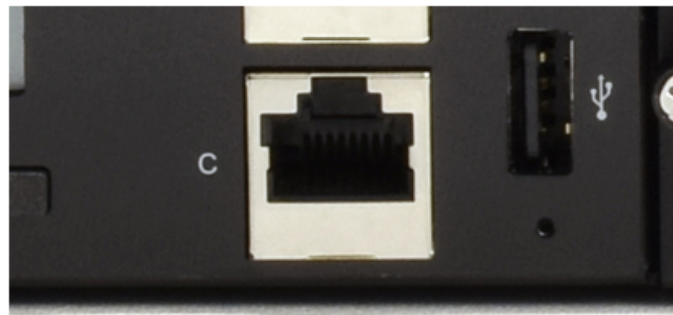


Figure 3.1. The W50 Local Console Port

Requirements for Local Console Connection

To get management access via the local console port, the following is needed:

- A computer with a serial port and the ability to emulate a console terminal (for example, using the open source *puTTY* software).
- The terminal console should have the following settings:
 - i. 9600 bps.
 - ii. No parity.
 - iii. 8 bits.
 - iv. 1 stop bit.
 - v. No flow control.
- An RS-232 cable with appropriate terminating connectors.

Connection Steps

To connect a terminal to the local console port, perform the following steps:

1. Check that the console connection settings are configured as described above.
2. Connect one of the connectors on the cable directly to the local console port on the W50.
3. Connect the other end of the cable to a console terminal or to the serial connector of a computer running console emulation software.



Note: Setting a local console password is recommended

A local console password need not be set. However, if it is not, anyone with physical access to the local console will have full administrator rights.

*Unless the hardware is placed in a secure area, it is therefore recommended to set a local console password. This is done by entering the console **boot menu** at system startup by pressing any console key before cOS Core has fully started. The boot menu and its options is discussed further in the separate **cOS Core Administration Guide**.*

Remote Console Connection Using SSH

An alternative to using the local console port for CLI access is to connect remotely over a network via a physical Ethernet interface and using a Secure Shell (SSH) client on the management computer to issue CLI commands. This is discussed further in *Section 3.4, "Management Computer Connection"*.

3.6. Connecting Power

This section describes connecting power. As soon as power is applied, the W50 will boot-up and cOS Core will start.



Important

Please review the electrical safety information in **Chapter 9, Safety Precautions**.

The image below shows the back of the W50 with both the two power supply units (PSUs) for redundancy in case of a single PSU failure.



Figure 3.2. Rear view of the Clavister W50

As standard, the W50 is delivered with only a single PSU and the second PSU slot is occupied by a dummy slot filler. A second PSU must be ordered separately. The W50 can operate with one PSU and a second can be added if required. When two PSUs are installed, the W50 runs using power from only one of the PSUs and the other delivers power only in the case of a failure by the primary unit. Installing and swapping PSUs is discussed further in *Section 5.1, "Power Supply Replacement"*.

Connecting AC Power

To connect power, follow these steps:

1. Connect the end of the power cord to the power inlet on the W50. There is a hinged silver metal cable retaining cage on the W50 PSU. This should be lifted up before inserting the power cable. Once the cable is plugged in, it should be moved back over the cable to prevent it slipping out.



Figure 3.3. W50 Power Switch and Power Inlet Socket

2. Plug the other end of the power cord into a grounded power outlet.
3. If a second PSU is used for redundancy, the dummy PSU should be removed and the actual PSU should be inserted in its place. The procedure for inserting the power cable should then be repeated for this second PSU.
4. Power is controlled by a rocker switch situated to the left of the power inlet socket. To switch on, depress the upper part of the switch so move it moves to the **On** position and then immediately release it.
5. The W50 will boot up as soon as power is applied and cOS Core will start. The progress of the boot up can be seen on a CLI console connected to the local console port.
6. After a brief period of time, cOS Core will be fully initialized and the W50 is then ready for configuration using a direct console connection or via the default management Ethernet interface.

Initial cOS Core configuration is described in *Chapter 4, cOS Core Configuration*.

Restarting the W50

In order to restart the W50 hardware, the On/Off rocker switch should be held in and then released. This will restart the W50 and reinitialize cOS Core so that it boots up.



Important: Protecting against power surges

It is recommended that the purchase and use of a separate surge protection unit from a third party is considered for the power connection to the W50 hardware. This is to ensure that the W50 is protected from damage by sudden external electrical power surges through the power cable.

Surge protection is particularly important in locations where there is a heightened risk of lightning strikes and/or power grid spikes.

Any surge protection unit should be installed exactly according to the manufacturer's instructions since correct installation of such units is vital for them to be effective.

Chapter 4: cOS Core Configuration

- Web Interface and Wizard Setup, page 37
- Manual Web Interface Setup, page 47
- Manual CLI Setup, page 61
- License Installation Methods, page 69
- Setup Troubleshooting , page 71
- Going Further with cOS Core, page 73



Note: Upgrading to the latest cOS Core version

A new W50 may not have the very latest cOS Core version pre-installed. After initial configuration, it is recommended to upgrade to the latest available version. The steps for upgrading are described in the separate cOS Core Administration Guide.

4.1. Web Interface and Wizard Setup

This section describes the setup when accessing cOS Core for the first time through a web browser. The cOS Core user interface accessed in this way is called the *Web Interface* (or *WebUI*). It assumes that a physical network connection has been set up from a management computer to the default management Ethernet interface, as described in *Section 3.4, "Management Computer Connection"*.

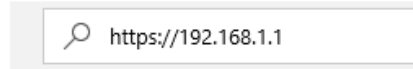


Note: Some browser screenshot images have been modified

Some of the screenshot images in this section have been modified from original screenshots to suit this document's page format. However, all relevant details in the images have been preserved.

Connect to cOS Core By Browsing to `https://192.168.1.1`

Using a standard web browser, enter the address `https://192.168.1.1` into the navigation window, as shown in the example below.



Note: HTTP access is disabled for cOS Core 11.01 and later

For cOS Core version 11.01 and later, HTTP management access is disabled in the default configuration and HTTPS must be used. Unencrypted access with HTTP can be enabled by the administrator but this is not recommended.

Troubleshooting

If there is no response from cOS Core and the reason is not clear, refer to the checklist in Section 4.5, "Setup Troubleshooting".

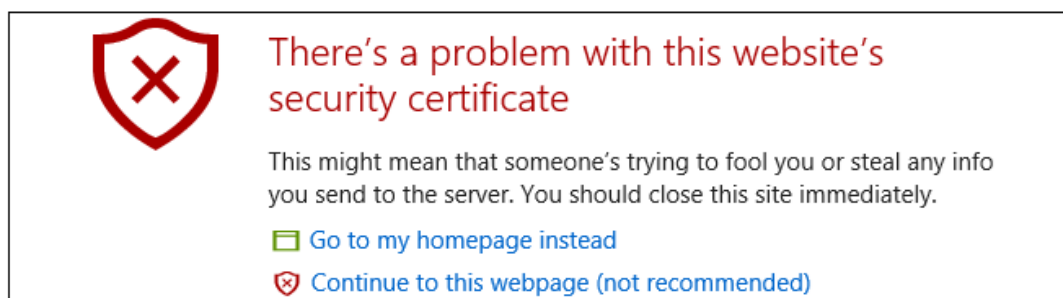


Important: Do not access cOS Core via a proxy server

Make sure the web browser doesn't have a proxy server configured for the cOS Core management IP address.

The cOS Core Self-signed Certificate

When responding to the first `https://` request in a browser session, cOS Core will send a self-signed certificate to the browser. All browsers will automatically flag this self-signed certificate as posing a potential security risk. In the latest Microsoft browser, the following error message will be displayed in the browser window.



The browser should now be told to accept the Clavister certificate by choosing the option to continue.

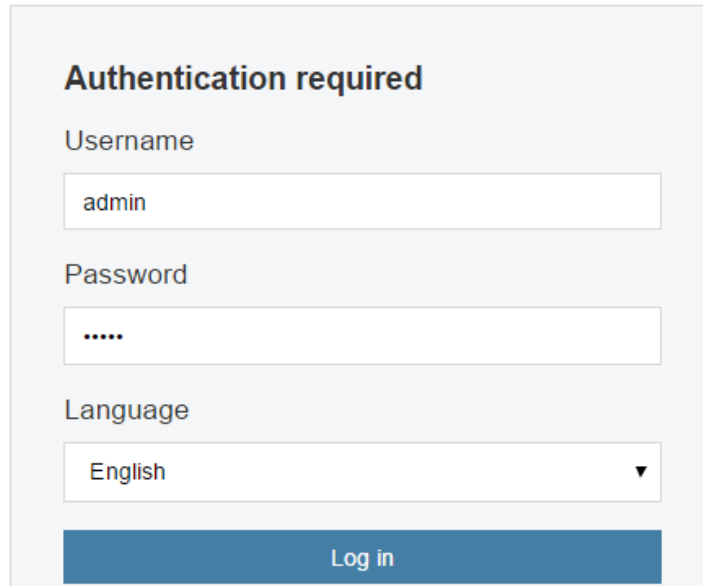


Note: Sending a CA signed certificate can be configured

It is possible to configure cOS Core to use a CA signed certificate instead of its default self-signed certificate for the management login. Doing this is described in the cOS Core Administration Guide.

The Login Dialog

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



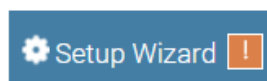
The image shows a web-based authentication dialog box. At the top, it says "Authentication required" in bold. Below this are three input fields: "Username" with the text "admin", "Password" with masked characters ".....", and "Language" with a dropdown menu showing "English". At the bottom is a blue button labeled "Log in".

The available Web Interface language options are selectable at the bottom of this dialog. This defaults to the language set for the browser if cOS Core supports that language.

Enter the administrator username as **admin** and use the default password **admin**.

Starting the Setup Wizard

After logging in for the first time, the Web Interface will appear and the cOS Core setup wizard should begin automatically as a popup window. If the wizard is blocked by the browser, it can be started manually by pressing the *Setup Wizard* button in the Web Interface toolbar (shown below).



Once the wizard is started, the first dialog displayed is the wizard welcome screen.



Canceling the Wizard

The setup wizard can be canceled at any point before the final *Activate* screen. It can run again by pressing the *Setup Wizard* button in 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 cOS Core 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 Next Generation Firewall is being used in *Transparent Mode* between two internal networks, then the configuration setup is best done with manual Web Interface steps or through the CLI instead of through the wizard and these are explained in the two sections that follow.

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 following the welcome screen are listed next.

Wizard step 1: Enter a new *admin* password and optionally change the username

The first step in setup with the wizard is to enter a new password for the *admin* user. Always doing this is recommended. The *admin* username can also be changed if this is required. The next screenshot shows this step.

The *Enforce Strong Passwords* option is only present in cOS Core versions 11.05 and later. This is a global setting that will enforce the listed strong passwords rules for **all** users in any local user database in the configuration. If required, this option can be disabled later. It is recommended to leave this option enabled, which means that the default password of *admin* must be changed to a conforming strong password before the wizard can move on to the next step.

Note that restoring cOS Core to factory defaults will restore the original *admin/admin* credential combination for management access.

☒ Enforce Strong Passwords policy

Passwords must comply with these complexity rules:

- Be at least 8 characters in length.
- Not contain significant portions of the user name.
- Contain characters from three out of these four categories:
 - Uppercase characters.
 - Lowercase characters.
 - Digits (0-9)
 - Non-alphanumeric characters (!, \$, #, %...)

Username:

Password:

Confirm

Password:

Wizard step 2: Set the date and time

Many cOS Core functions rely on an accurate date and time, so it is important that this is set correctly in the fields shown below. The default time zone location is *ClavisterHQ* which means the default location and time zone will be Stockholm. If this is not correct it should be changed to another location and timezone using the drop-down list.

DATE AND TIME SETTINGS

Set system date and time for proper function of features like logging, UTM and updates.

Current Date and Time

2018-05-16

12:48:16

Set

TIMEZONE SETTINGS

Location

ClavisterHQ

Enable daylight saving time

☒

Wizard step 3: Select transparent mode interfaces

This step allows any transparent mode interfaces to be set up. If no transparent mode interfaces are required, leave this dialog in the default **Normal Mode** and go to the next step. Transparent mode interfaces can be configured at any time later, outside of the wizard.

☐ Normal Mode
 ☒ Transparent Mode

Remember that Transparent Mode does not support High Availability and they should not be. Please select the interfaces to enable Transparent Mode on, from the list of available interfaces.

Available	Selected
G1	
G2	
G3	

+ Include

✕ Remove

Network:

☐ DHCP Passthrough
 ☐ L2 Passthrough for Non-IP Protocols

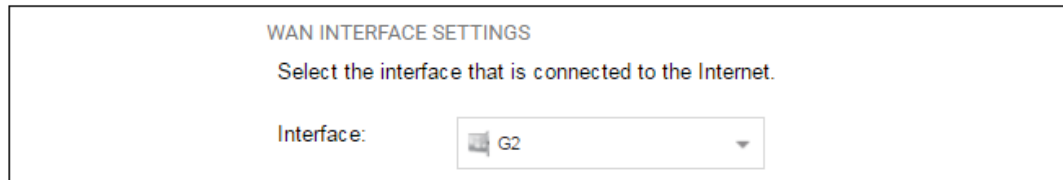


Note: This step is only available with version 11.04 or later

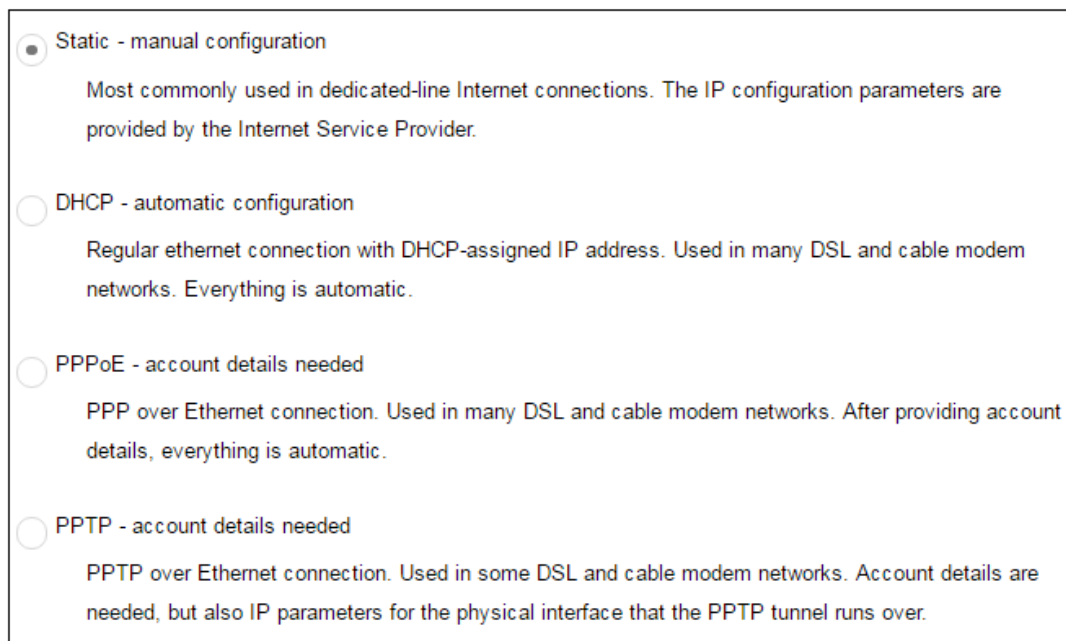
The step to optionally set up transparent mode interfaces in the startup wizard is only available with cOS Core version 11.04 or later. Also, the available interface list shown above will vary according to the platform on which cOS Core is running.

Wizard step 4: Select the WAN interface

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


Wizard step 5: 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.



☒ **Static - manual configuration**
Most commonly used in dedicated-line Internet connections. The IP configuration parameters are provided by the Internet Service Provider.

☐ **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. Account details are needed, but also IP parameters for the physical interface that the PPTP tunnel runs over.

These four different connection options are discussed next in the subsections **5A** to **5D** that follow.

- **5A. 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. The IP configuration parameters are provided by the Internet Service Provider.

IP Address:

Network:

E.g. 192.168.1.0/24

Gateway:

Primary DNS server:

Secondary DNS server:

- **5B. 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.

- **5C. PPPoE settings**

The username and password supplied by an 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.

- **5D. PPTP settings**

The username and password supplied by an 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 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 6: DHCP server settings

If the Clavister Next Generation Firewall 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 IPv4 addresses that can be handed out must be specified in the form *n.n.n.n-n.n.n.n*, where *n* is a number between 0 and 255 and *n.n.n.n* is a valid IPv4 address within a subnet local to the firewall.

For example, the private IPv4 address range might be specified as *192.168.1.50 - 192.168.1.150* with a netmask of *255.255.255.0*.

☐ Disable DHCP Server

☒ Enable DHCP Server

Interface:

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:

For the default gateway, it is recommended to specify the IPv4 address assigned to the internal network interface. The DNS server specified should be the DNS supplied by an ISP.

Wizard step 7: 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 cOS Core. By selecting the **Clavister** option, the current time will be updated over the Internet from Clavister's own timeserver.

HELPER SERVER SETTINGS

Additional servers for keeping the time accurate and for logging data.

☐ Disabled
☒ Clavister (pre-configured timesync server)
☐ Custom

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)

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 8: Activate setup

The final step for the configuration is to save and activate it 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.

Wizard step 9: License Activation

This last and optional step is to install a license which is fetched automatically from Clavister servers. Internet access must have been set up in previous wizard steps for this option to function. The only input required is the *MyClavister* username and password for the Clavister website. This also creates a lasting link between the W50 and the Clavister servers so that any future license updates can be installed automatically.

MYCLAVISTER CONNECTION

To enable automatic license checking via the MyClavister Connection, please enter username and password for your Clavister website account. After successful download of the key, click activate to save and complete the connection.

Username:

Password:

If customer registration has not been previously been done, a link is provided to open a browser window to complete registration. After registration, come back to this step.

Alternatively, this step can be skipped and license installation can be done later, in which case cOS Core will run in *demo mode* with a 2 hour time limit. After the 2 hour period, only management access will be allowed.

If a license is installed at this point, the wizard will then ask if a reconfigure or restart operation should be performed. To ensure that the W50 can make use of the full capabilities of the license, the restart option should be chosen.

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 firewall has its factory defaults restored, in which case the device will behave as though it were being started for the first time.

4.2. Manual Web Interface Setup

This section describes initial cOS Core 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 cOS Core.

Ethernet Interfaces

The physical connection of external networks to the Clavister Next Generation Firewall is through the various *Ethernet interfaces* which are provided by the hardware platform. On first-time startup, cOS Core 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 cOS Core interfaces are logically equal for cOS Core and although their physical capabilities may be different, any interface can perform any logical function.

With the W50, the **G1** interface is the default management interface. To describe manual Internet setup, it is assumed here that the **G1** interface will also be used for connection to a protected internal client network. It is also assumed that at least one Ethernet ports expansion module is fitted and the **E1-1** interface (the first interface of the first expansion module) will be used for connection to the public Internet.

Setting the Date and Time

Many cOS Core functions rely on an accurate date and time, so it is important that this is set correctly. To do this, select **System > Device > Date and Time**. The current system time is displayed and this can be changed by selecting the date and time fields then manually entering the desired figures. Pressing the **Set** button will then set the time to the entered values.

2017-06-12	14:05:10	Set	Synchronize
------------	----------	-----	-------------

Also choose the correct time zone from the **Location** drop-down list. The default location is *ClavisterHQ* which is Stockholm time.

Location:	ClavisterHQ
-----------	-------------

Alternatively, the **Synchronize** button can be pressed to get the current date and time from the configured **Network Time Protocol** (NTP) server. In the default configuration, Clavister's own NTP server is automatically configured. However, accessing this server requires Internet access.

Configuring a custom NTP server configuration is shown below.

<input type="radio"/> Disabled <input type="radio"/> Clavister (pre-configured timesync server) <input checked="" type="radio"/> Custom
Primary Time Server: <input type="text"/>



Note: Specifying a URL for the time server

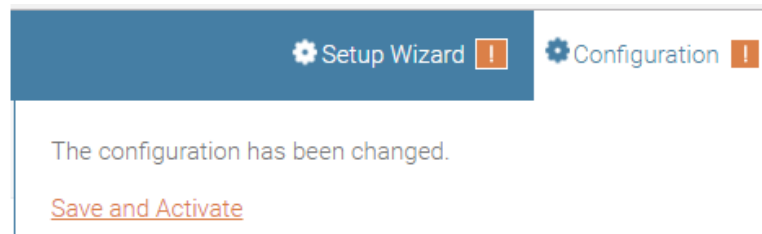
For cOS Core versions prior to 12.00.09 a time server URL must have the prefix "**dns:**".

For version 12.00.09 and later, an **FQDN Address** address must be used instead of a direct URL reference. See the relevant cOS Core Administration Guide for more explanation.

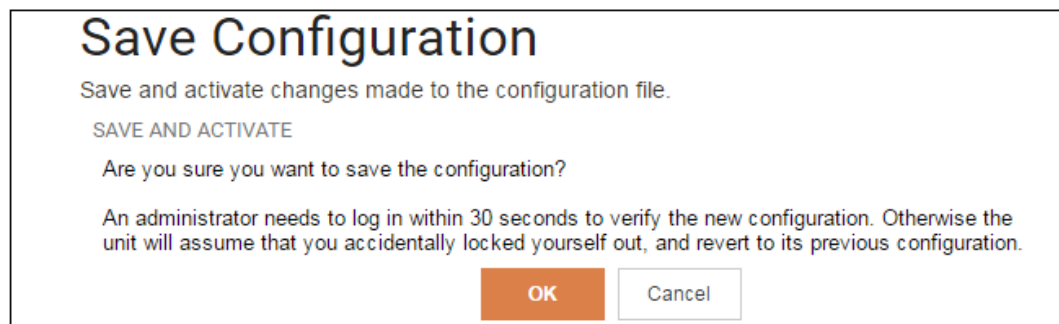
Once the values are set correctly, we can press the **OK** button to save the values while we move on to more steps in cOS Core configuration. Although changed values like this are saved by cOS Core, they do not become active until the entire saved configuration becomes the current and active configuration.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

Activating Configuration Changes

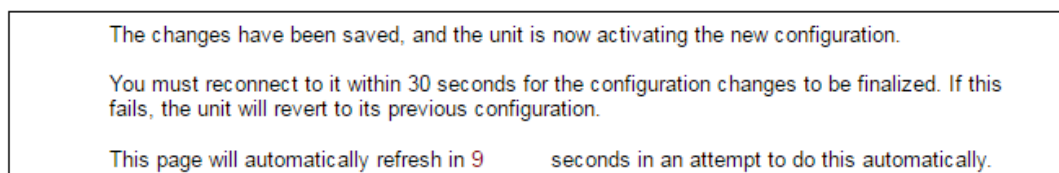
To activate any cOS Core configuration changes made so far, select the **Save and Activate** option from the **Configuration** menu (this procedure is also referred to as *deploying a configuration*).



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



After clicking **OK**, cOS Core *reconfiguration* will take place and, after a short delay, the Web Interface will try and connect again to the firewall.



If no reconnection is detected by cOS Core within 30 seconds (this length of time is a setting that can be changed) then cOS Core 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 cOS Core 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 Next Generation Firewall should rarely be lost.



Tip: How frequently to commit configuration 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.

However, it is not advisable to leave changes uncommitted 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), cOS Core 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 with the CLI. There are four options for setting up access which are listed below and then described in detail.

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 cOS Core manually.








Note: The interface DHCP option should be disabled

For static configuration of the Internet connection, the DHCP option must be disabled in the properties of the interface that will connect to the ISP.

The initial step is to set up a number of IPv4 address objects in the cOS Core *Address Book*. Let us assume that the interface used for Internet connection is to be *E1-1* and that the static IPv4 address for this interface is to be *203.0.113.35*, the ISP's gateway IPv4 address is *203.0.113.1*, and the network to which they both belong is *203.0.113.0/24*.

Now, add the gateway *IP4 Address* object using the address book name *wan_gw* and assign it the IPv4 address *203.0.113.1*. The ISP's gateway is the first router hop towards the public Internet from the Clavister Next Generation Firewall. Go to **Objects > Address Book** in the Web Interface.

The current contents of the address book will be listed and will contain a number of predefined objects automatically created by cOS Core after it scans the interfaces for the first time. The screenshot below shows the initial address book for the W50.

#	Name ▲	Address	User Auth Groups	Comments
2	 all-nets	0.0.0.0/0		All possible networks
3	 all-nets6	:::0		All possible IPv6 networks
1	 InterfaceAddresses			
4	 localhost	127.0.0.1 (127.0.0.2)		Localhost, for non-management High Availa
5	 localhost6	:::1 (:::2)		Localhost, for non-management High Availa



Note: The all-nets address

*The IPv4 address object **all-nets** is a wildcard address that should never be changed and can be used in many types of cOS Core rules to refer to any IPv4 address or network range.*

For the W50, all the Ethernet interface related address objects are gathered together in an *address book folder* called *InterfaceAddresses*. By clicking on this folder, it will be opened and the individual address objects it contains can be viewed. Predefined addresses in the folder are shown below.

# ▲	Name	Address	User Auth Groups	Comments
1	 G1_ip	192.168.1.1		IP address of interface G1
2	 E1-1_ip	127.0.1.1		IP address of interface E1-1

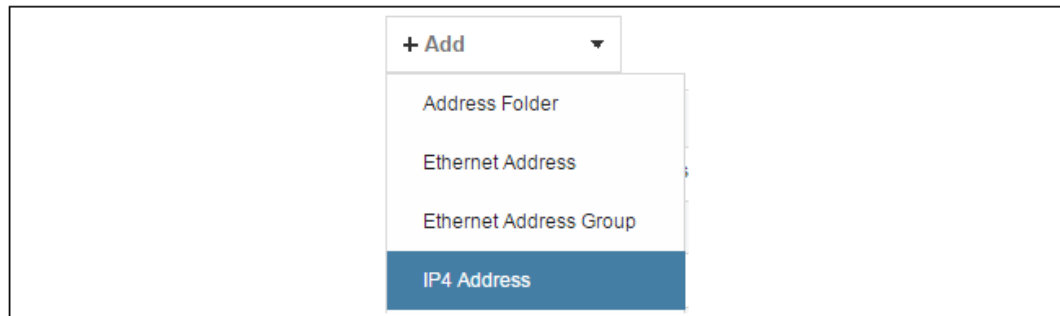
On initial startup, two IPv4 address objects are created automatically for each interface detected by cOS Core. One IPv4 address object is named by combining the physical interface name with the suffix *"_ip"* and this is used for the IPv4 address assigned to that interface. The other address object 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* object. Below, the IPv4 address 203.0.113.1 has been entered for the address object called *wan_gw*. This is the IP of the ISP's router which acts as the gateway to the public Internet.

IP4 Address

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

General
User Authentication

Name:

Address:

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

Then set up *E1-1_ip* to be 203.0.113.35. This is the IPv4 address of the *E1-1* interface which will connect to the ISP's gateway.

Lastly, set the *IP4 Address* object *E1-1_net* to be 203.0.113.0/24. Both the address objects *E1-1_ip* and *wan_gw* must belong to the same network in order for the interface to communicate with the ISP.

Together, these three IPv4 address objects will be used to configure the interface connected to the Internet which, in this example, is *E1-1*. Select **Network > Interfaces and VPN > Ethernet** to display a list of the physical interfaces and address book objects assigned to them.

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 settings can be changed including the default gateway.

IP address:	E1-1_ip
Network:	E1-1_net
Default Gateway:	wan_gw

Press **OK** to save the changes. Although changes are remembered by cOS Core, the changed configuration is not yet activated and won't be activated until cOS Core is told explicitly to use 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 cOS Core 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 cOS Core configuration objects to exist before it can flow through the Clavister Next Generation Firewall:

- An *IP Policy* object in the 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 cOS Core routing table which specifies on which interface cOS Core can find the traffic's destination IP address.

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

An IP policy therefore needs to be defined that will allow traffic from clients to the Internet. In this case, that web browsing is to be allowed from the protected private network *G1_net* connected to the interface *G1* to be able to access the public Internet.

To do this, first go to **Policies > Firewalling > Main IP Rules**. The *main* IP rule set will now be displayed.

To add a new IP policy, press the **Add** button and select **IP Policy** from the menu.

<div>+ Add</div> <div>IP Policy</div>

The properties for the new object will appear. In this example, the policy will be called *lan_to_wan*. The *Service* is set to *http-all* which is suitable for most web browsing (it allows both HTTP and HTTPS connections).

Name:	lan_to_wan	
Action:	<div>ALLOW</div>	
	Interface	Network
Source:	G1	G1_net
Destination:	E1-1	all-nets
Service:	dns-all	

The destination network is specified as the predefined *IP4 Address* object *all-nets*. This is used since it cannot be known in advance to which IP address web browsing will be directed and *all-nets* allows browsing to any IP address. IP rule sets are processed in a top down fashion, with the search ending at first matching entry. An *all-nets* entry like this should be placed towards the end of the rule set since other rules with narrower destination addresses should trigger first.

In addition to entering the above for the policy, the *Source Translation* should be set to NAT and the *Address Action* left as *Outgoing Interface IP*. Note that the default source translation value for an IP policy is *Auto* and this would also provide NAT translation between a private and public IP address but NAT is specified explicitly in this section for clarity.

SOURCE TRANSLATION	
Address Translation:	NAT
Address Action:	Outgoing Interface IP

By using *NAT*, cOS Core 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 cOS Core will automatically forward the traffic back to the originating local host. Only the outgoing interface therefore needs to have a public IPv4 address and the internal network topology is hidden.

For web browsing, public 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 a similar IP rule set entry that allows this is needed. This could be done with a single IP policy that uses a custom service which combines the *HTTP* and *DNS* protocols but the recommended method is to create an entirely new IP set entry that 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 IP policy called *lan_to_wan_dns* being created to allow DNS.

The screenshot shows the configuration for an IP policy named 'lan_to_wan_dns'. The 'Action' is set to 'ALLOW'. The 'Source' is configured with 'Interface' as 'G1' and 'Network' as 'G1_net'. The 'Destination' is configured with 'Interface' as 'E1-1' and 'Network' as 'all-nets'. The 'Service' is set to 'dns-all'.

As was done for HTTP, NAT should also be enabled with this IP policy so all DNS queries are sent out by cOS Core with the outgoing interface's IP address as the source IP.

For the Internet connection to work, a *route* also needs to be defined so that cOS Core knows on which interface the web browsing traffic should leave the Clavister Next Generation Firewall. This route will define the interface where the network *all-nets* (in other words, any network) will be found. If the default *main* routing table is opened by going to **Network > Routing > Routing Tables > main**, the route needed should appear as shown below.

Type	Interface	Network	Gateway	LocalIP	Metric	Monitor this route	Comments
Route IPv4	E1-1	all-nets	wan_gw		100	No	

This required *all-nets* route is, in fact, added automatically after specifying the *Default Gateway* for a particular Ethernet interface and this was done earlier when setting up the required *IPv4 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 cOS Core. This DNS server or servers (a maximum of three can be configured) will be used when cOS Core itself needs to resolve URLs which is the case when a URL is specified in a configuration object instead of an IP address. It is also important for certificate handling

Assume an IPv4 address object called *wan_dns1* has already been defined in the address book and this is the address for the first DNS server. By choosing **System > Device > DNS**, the DNS server dialog will open and this object from the address book can be assigned as the first server.

The screenshot shows the 'DNS' configuration page. It has two tabs: 'General' (selected) and 'Advanced'. Under 'General', the 'Primary Server' is set to '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. This option is enabled by first selecting **Network > Interfaces and VPN > Ethernet** to display a list of all the interfaces.

Click the *E1-1* interface in the list to display its properties and select the option to enable the interface as a DHCP client.

The screenshot shows a configuration window for the **E1-1** interface. At the top, the **Name** is set to **E1-1**. Below this, the **IPv4** section contains several fields: **IP address** (set to **E1-1_ip**), **Network** (set to **E1-1_net**), **Default Gateway** (set to **wan_gw**), and **Receive Multicast Traffic** (set to **Auto**). At the bottom, there is a checkbox labeled **Enable DHCP Client**, which is checked.

Usually, a DHCP *Host Name* does not need to be specified but can sometimes be used by an ISP to uniquely identify this Clavister Next Generation Firewall 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 cOS Core automatically sets the relevant address objects in the address book with this information.

For cOS Core to know on which interface to find the public Internet, a *route* has to be added to the *main* cOS Core 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 cOS Core 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 set entry defined that allows it. As was done in the previous option (A) above, we must therefore define a rule set entry that will allow traffic from the source network *G1_net* and source interface *G1* to flow to the destination network *all-nets* and the destination interface *E1-1*.

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 *E1-1* and the PPPoE tunnel object created is called *wan_pppoe*. Go to **Network > Interfaces and VPN > PPPoE** and select **Add > PPPoE Tunnel**. These values can now be entered into the PPPoE Tunnel properties dialog.

Name:	wan_pppoe
Physical Interface:	E1-1
Remote Network:	all-nets
Schedule:	(None)
Username:	my_pppoe_username
Password:
Confirm Password:

An 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 cOS Core 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 **Network > Routing > Routing Tables > main** we can see this route.

Type	Interface	Network	Gateway	LocalIP	Metric	Monitor this route	Broadca
Route IPv4	wan_pppoe	all-nets			90	No	No

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 set entry defined that allows it. As was done in option **A** above, we must define a rule set entry that will allow traffic from the source network *G1_net* and source interface *G1* to flow to the destination network *all-nets* and the destination interface. Here, the destination interface is the PPPoE tunnel that has been 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 remote endpoint *203.0.113.1* which has been defined as the *IP4 Address* object *pptp_endpoint*. Go to **Network > Interfaces and VPN > PPTP/L2TP Clients** and select **Add > PPTP/L2TP Client**. The values can now be entered into the properties dialog and the *PPTP* option should be selected.




Name:	wan_pptp
Tunnel Protocol:	PPTP
Remote Endpoint:	pptp_endpoint
Remote Network:	all-nets

An 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 cOS Core 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 cOS Core 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 **Network > Routing > Routing Tables > main** we can see this route.

Type	Interface ▾	Network	Gateway	LocalIP	Metric	Monitor this route	Broadcast
 Route IPv4	 wan_pptp	 all-nets			90	No	No

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 set entry defined that allows it. As was done in option **A** above, we must define a rule set entry that will allow traffic from a designated source network and source interface (in this example, the network *G1_net* and interface *G1*) to flow to the destination network *all-nets* and the destination interface which is the PPTP tunnel that has been defined.

DHCP Server Setup

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

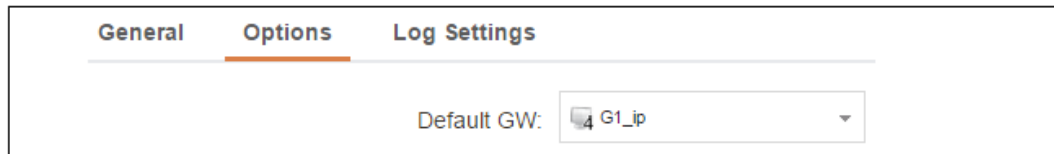
First, create an *IP4 Address* object which defines the address range to be handed out. Here, it is assumed that this has the name *dhcp_range*. It is also assumed that another *IP4 Address* object *dhcp_netmask* has been created which specifies the netmask.

We now create a DHCP server object called *my_dhcp_server* which will only be available on the *G1* interface. To do this, go to **Network > Network Services > DHCP Servers** and select **Add > DHCP Server**. The server properties can now be specified.

Name:	<input type="text" value="my_dhcp_server"/>
Interface Filter:	 G1 ▾
Relay Filter:	<input type="text" value="0.0.0.0/0"/> ▾
IP Address Pool:	 dhcp_range ▾
Netmask:	 dhcp_netmask ▾

An example IP pool range might be *192.168.1.10 - 192.168.1.20* with a netmask of *255.255.0.0*.

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 IPv4 address of the interface on which the DHCP server is configured, in this case, *G1_ip*. To set the default gateway, select the **Options** tab.



General Options Log Settings

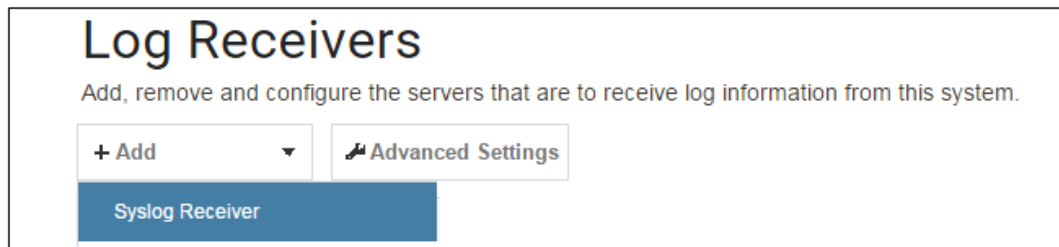
Default GW: G1_ip

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 IPv4 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 cOS Core. *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 IPv4 address of the server. We then configure the sending of log messages to a Syslog server from cOS Core by selecting **System > Device > Log and Event Receivers** and then choosing **Add > Syslog Receiver**.



Log Receivers

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

+ Add Advanced Settings

Syslog Receiver

The Syslog server properties dialog will now appear. We give the server a name, for example *my_syslog*, and specify its IPv4 address as the *syslog_ip* object.



Name: my_syslog

Routing Table: main

IP Address: syslog_ip



Tip: Address book object naming

The cOS Core 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 another example of setting up IP rule set entries, it can be useful to allow outgoing ICMP *ping* messages to pass through the firewall. To allow hosts on the internal network *G1_net* to send ping messages to any hosts on the Internet, select **Policies > Firewalling > Main IP Rules > Add** and enter the values shown below for an IP policy called *allow_ping_outbound*. This uses the predefined service called *ping_outbound*.

Name:	allow_ping_outbound	
Action:	<input checked="" type="checkbox"/> ALLOW <input type="checkbox"/>	
	Interface	Network
Source:	G1	G1_net
Destination:	E1-1	all-nets
Service:	ping-outbound	

As with previous policy definitions, NAT should also be enabled if the protected local hosts have private IPv4 addresses. The ICMP messages will then be sent out from the Clavister Next Generation Firewall with the IP address of the interface connected to the ISP as the source interface. Responding hosts will send back ICMP responses to this single IP and cOS Core will then forward the response to the correct private IPv4 address.

Adding a Drop All Policy

The top-down nature of IP rule set scanning has been mentioned earlier. If **no** matching entry is found for a new connection then the *default rule* is triggered. This rule is hidden and cannot be changed. Its action is to drop all such traffic and always generate a log message for each dropped connection.






In order to gain control over the logging of dropped traffic, it is recommended to create a drop all policy as the last entry in the *main* IP rule set. This policy will have the source and destination network set to *all-nets* and the source and destination interface set to *any*. The service should be set to *all_services* in order to capture all types of traffic.

Name:	drop_all	
Action:	<input type="checkbox"/> <input checked="" type="checkbox"/> DENY	
Deny Behavior:	<input type="checkbox"/> <input checked="" type="checkbox"/> DROP	
	Interface	Network
Source:	any	all-nets
Destination:	any	all-nets
Service:	all_services	

Logging is enabled by default for an IP rule set entry which means that a log message will be sent to all configured log servers whenever the entry triggers. Only log events that have a specified severity or above will be sent. The administrator can choose the minimum severity for log messages in each IP rule set entry, as shown below.

Logging: ON <input type="checkbox"/>	Warning <input type="text"/>
---	------------------------------

If this IP policy were the only one defined, the *main* IP rule set listing would be as shown below.

# ▲	Name	Log	Src If	Src Net	Dest If	Dest Net	Service	Application
1	■ Drop_All	✓	 any	 all-nets	 any	 all-net..	 all_services	

A Valid License Must Be Installed

Lastly, a valid license should be installed to remove the cOS Core 2 hour demo mode limitation. Without a license installed, cOS Core will have full functionality during the 2 hour period following startup, but after that, only management access will be possible. Installing a license is described in *Section 4.4, "License Installation Methods"*.

4.3. Manual CLI Setup

This chapter describes the cOS Core setup steps using CLI commands instead of the Web Interface and the setup wizard.

The CLI is accessible using either of the following two methods:

- Using an SSH (Secure Shell) client, across a network connection to the IPv4 address *192.168.1.1* on the default management Ethernet interface. The physical network connection setup to the computer running the client is described in *Section 3.4, "Management Computer Connection"* and is the same as that used in *Section 4.1, "Web Interface and Wizard Setup"*.

If there is a problem with the management computer connection, a help checklist can be found in *Section 4.5, "Setup Troubleshooting"*.

- Using a terminal or computer running a console emulator connected directly to the local console port on the W50.

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 cOS Core to respond. The response will be a normal CLI prompt if connecting directly through the local 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 cOS Core, 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 (also referred to as the *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 cOS Core gives a list of possible options in a command.

Now set the username and password for the administrator. Both are case sensitive. In the example below, the username is set to the value *new_name* and the password is set to the value *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 context which is the top level of object categories.

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

Setting the Date and Time

Many cOS Core functions, such as event logging and certificate handling, rely on an accurate date and time. It is therefore important that this is set correctly using the *time* command. A typical usage of this command might be:

```
Device:/> time -set 2017-06-24 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 Next Generation Firewall is via the various *Ethernet interfaces* which are provided by the hardware platform. On first-time startup, cOS Core determines which interfaces are available and allocates their names. One interface is chosen as the initial default management interface and this can only be changed after initial startup.

All cOS Core interfaces are logically equal for cOS Core and although their physical capabilities may be different, any interface can perform any logical function. With the W50, the **G1** interface is the default management interface. The other interfaces can be used as required. For this section, it is assumed that the *G1* interface will also be used for a network of protected internal clients. It is also assumed that at least one Ethernet ports expansion module is fitted and the **E1-1** interface (the first interface of the first expansion module) will be used for connection to the public Internet.

Setting Up Internet Access

Next, we shall look at how to set up public Internet access with the CLI. There are four options for setting up access which are listed below and then described in detail.

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 IPv4 address objects. It is assumed here that the interface used for Internet connection is *E1-1*, the ISP gateway IPv4 address is *203.0.113.1*, the IPv4 address for the connecting interface will be *203.0.113.35* and the network to which they both belong is *203.0.113.0/24*.

First, add the gateway IPv4 address object if it does not already exist:

```
Device:/> add Address IP4Address wan_gw Address=203.0.113.1
```

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=203.0.113.1
```

Now, set the gateway on the *E1-1* interface which is connected to the ISP:

```
Device:/> set Interface Ethernet E1-1 DefaultGateway=wan_gw
```

Next, set the IP address of the *E1-1_ip* address object which is the IP assigned to the interface:

```
Device:/> set IP4Address InterfaceAddresses/E1-1_ip Address=203.0.113.35
```



Note: Qualifying the names of IP objects in folders

On initial startup of the W50, cOS Core automatically creates and fills the **InterfaceAddresses** folder in the cOS Core address book with Ethernet interface related IPv4 address objects.

Note that when an IP address object which is located in a folder is specified in the CLI, the object name must be qualified with the name of its parent folder. For example, to reference the address **E1-1_ip**, it must be qualified with the folder name **InterfaceAddresses** so it becomes **InterfaceAddresses/E1-1_ip**.

If an object is not contained in a folder and is at the top level of the address book then no qualifying parent folder name is needed.

Now, set the IP object *E1-1_net* which will be the IPv4 network of the connecting interface:

```
Device:/> set IP4Address InterfaceAddresses/E1-1_net Address=203.0.113.0/24
```

Before continuing, it is recommended to verify the properties of the *E1-1* interface using the following command:

```
Device:/> show Interface Ethernet E1-1
```

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

Property	Value
Name:	E1-1
IP:	InterfaceAddresses/E1-1_ip
Network:	InterfaceAddresses/E1-1_net
DefaultGateway:	wan_gw
Broadcast:	203.0.113.255
PrivateIP:	<empty>
NOCHB:	<empty>
MTU:	1500
Metric:	100
DHCPEnabled:	No
EthernetDevice:	0:E1-1 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 cOS Core 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 Policy* which explicitly allows traffic to flow. Let us assume we want to allow web browsing from the protected network *G1_net* which is connected to the interface *G1*.

The following command will add an IP policy called *lan_to_wan* to allow HTTP and HTTPS traffic through to the public Internet:

```
Device:/> add IPPolicy Name=lan_to_wan
          SourceInterface=G1
          SourceNetwork=InterfaceAddresses/G1_net
          DestinationInterface=E1-1
          DestinationNetwork=all-nets
          Service=http-all
          Action=Allow
```

IP policies have a default value of *Auto* for the type of source translation. This means that if the source is a private IPv4 address and the destination is a public address, NAT will be performed automatically using the IP address of the outgoing interface as the new source address. Therefore the above IP policy will work both for connection to another private IP address or to public addresses on the Internet.

Instead of relying on the *Auto* option, this section will specify NAT translation explicitly for clarity. The above IP policy with explicit NAT translation becomes the following:

```
Device:/main> add IPPolicy Name=lan_to_wan
          SourceInterface=G1
          SourceNetwork=InterfaceAddresses/G1_net
          DestinationInterface=E1-1
          DestinationNetwork=all-nets
          Service=http-all
          Action=Allow
          SourceAddressTranslation=NAT
          NATSourceAddressAction=OutgoingInterfaceIP
```

Specifying *NATSourceAddressAction=OutgoingInterfaceIP* is not necessary as this is the default value but it is included here for clarity.

The service used in the above is *http-all* which will allow HTTP web browsing 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 IP policy 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 policy just for DNS traffic:

```
Device:/main> add IPPolicy Name=lan_to_wan_dns
          SourceInterface=G1
          SourceNetwork=InterfaceAddresses/G1_net
          DestinationInterface=E1-1
          DestinationNetwork=all-nets
          Service=dns-all
          Action=Allow
          SourceAddressTranslation=NAT
          NATSourceAddressAction=OutgoingInterfaceIP
```

It is recommended that at least one DNS server is also defined in cOS Core. This DNS server or servers (a maximum of three can be configured) will be used when cOS Core itself needs to resolve URLs which will be 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

Alternatively, all required IP addresses can 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 *E1-1*, then the command is:

```
Device:/> set Interface Ethernet E1-1 DHCPEnabled=Yes
```

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

For cOS Core to know on which interface to find the public Internet, a *route* has to be added to the *main* cOS Core 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 cOS Core 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 set entry defined that allows it. As was done in the previous option (A) above, we must therefore manually define an IP policy that will allow traffic from a designated source network and source interface (in this example, the network *G1_net* and interface *G1*) to flow to the destination network *all-nets* and the destination interface *E1-1*.

C. PPPoE setup

For PPPoE connection, create the PPPoE tunnel interface on the interface connected to the ISP. The interface *E1-1* 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=E1-1
           Username=pppoe_username
           Password=pppoe_password
           Network=all-nets
```

The 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 cOS Core 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 set entry defined that

allows it. As was done in option **A** above, we must define an IP policy that will allow traffic from a designated source network and source interface (in this example, the network *G1_net* and interface *G1*) to flow to the destination network *all-nets* and the destination interface which is the PPPoE tunnel that has been 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_pttp* with the remote endpoint *203.0.113.1*:

```
Device:/> add Interface L2TPClient wan_pttp
           Network=all-nets
           username=pttp_username
           Password=pttp_password
           RemoteEndpoint=203.0.113.1
           TunnelProtocol=PPTP
```

Your ISP will supply the correct values for *pttp_username*, *pttp_password* and the remote endpoint.

Your ISP will supply the correct values for *pttp_username*, *pttp_password* and the remote endpoint. An interface is not specified when defining the tunnel because this is determined by cOS Core 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 cOS Core 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 set entry defined that allows it. As was done in option **A** above, we must define an IP policy that will allow traffic from a designated source network and source interface (in this example, the network *G1_net* and interface *G1*) to flow to the destination network *all-nets* and the destination interface which is the PPTP tunnel that has been defined.

Activating and Committing Changes

After any changes are made to a cOS Core 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 cOS Core 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 Next Generation Firewall is to act as a DHCP server then this can be set up in the following way:

First define an IPv4 address object which has the address range that can be handed out. Here, we will use the IPv4 range *192.168.1.10 - 192.168.1.20* as an example and this will be made available on the *G1* interface which is connected to the protected internal network *G1_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 *my_dhcp_server*.

```
Device:/> add DHCPserver my_dhcp_server
          IPAddressPool=dhcp_range
          Interface=G1
          Netmask=255.255.255.0
          DefaultGateway=InterfaceAddresses/G1_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, *G1_ip*.

NTP Server Setup

Network Time Protocol (NTP) servers can optionally be configured to maintain the accuracy of the system date and time. Suppose that synchronization is to be setup with the two NTP servers at hostname *pool.ntp.org* and IPv4 address *203.0.113.5*.

First, an *FQDNAddress* object needs to set up for the hostname:

```
Device:/> add Address FQDNAddress ts1_fqdn Address=pool.ntp.org
```

Next, set the servers to use for date and time synchronization:

```
Device:/> set DateTime TimeSyncEnable=Yes
          TimeSyncServer1=ts1_fqdn
          TimeSyncServer2=203.0.113.5
```

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 *192.0.2.10* then the command to create a log receiver object called *my_syslog* which enables logging is:

```
Device:/> add LogReceiverSyslog my_syslog IPAddress=192.0.2.10
```

Allowing ICMP Ping Requests

As a further example of setting up IP policies, it can be useful to allow ICMP *ping* messages to flow through the firewall. As discussed earlier, cOS Core will drop any traffic unless an IP rule set

entry explicitly allows it. Suppose that we wish to allow the pinging of external hosts by hosts located on the internal *G1_net* network. The command to define an IP policy called *allow_ping_outbound* to allow this would be the following:

```
Device:/> add IPPolicy Name=allow_ping_outbound
          SourceInterface=G1
          SourceNetwork=InterfaceAddresses/G1_net
          DestinationInterface=E1-1
          DestinationNetwork=all-nets
          Service=ping-outbound
          Action=Allow
          SourceAddressTranslation=NAT
          NATSourceAddressAction=OutgoingInterfaceIP
```

The IP policy above assumes NAT will be used and this is necessary if the protected local hosts have private IPv4 addresses. The ICMP requests will be sent out from the Clavister Next Generation Firewall with the IP address of the interface connected to the ISP as the source interface. Responding hosts will send back ICMP responses to this single IP and cOS Core will then forward the response to the correct private IP address.

Adding a Drop All Policy

Scanning of IP rule sets is done in a top-down fashion. If **no** matching rule set entry 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 policy as the last entry in the *main* IP rule set. This policy will have the source and destination network set to *all-nets* and the source and destination interface set to *any*. The service should be set to *all_services* in order to capture all types of traffic.

The following IP policy will drop all remaining traffic as well as turning off logging for that traffic:

```
Device:/main> add IPPolicy Name=drop_all
          SourceInterface=any
          SourceNetwork=any
          DestinationInterface=any
          DestinationNetwork=all-nets
          Service=all_services
          Action=Deny
          LogEnabled=No
```

A Valid License Must Be Installed

Lastly, a valid license should be installed to remove the cOS Core 2 hour demo mode limitation. Without a license installed, cOS Core will have full functionality during the 2 hour period following startup, but after that, only management access will be possible. Installing a license is described in *Section 4.4, "License Installation Methods"*.

4.4. License Installation Methods

Without a valid license installed, cOS Core will run in *demo mode* (demonstration mode) which means that it will cease to function after two hours of operation. Restarting cOS Core will re-enable cOS Core for another two hours. To remove this 2 hour restriction, a valid license must be installed.

Licenses are files which are made available for download from the Clavister servers but before they become available, the user must have registered themselves with Clavister and doing this is described in *Chapter 2, Registering with Clavister*.

Installation Methods

The following methods can be used for installing the first cOS Core license in the W50 unit:

- **Automatically through the Setup Wizard**

As described in *Section 4.1, "Web Interface and Wizard Setup"*, when the wizard is used for initially configuring Clavister hardware, the administrator can choose to install a license as one of the wizard steps.

- **Automatically through the Web Interface**

Go to **Status > Maintenance > License** and enter the customer's login credentials for the Clavister website, then press **Activate**. The license is fetched automatically across the public Internet and installed.

- **Automatically through the CLI**

In the CLI, enter the command:

```
Device:/> license -activate -request -username=myname -password=mypass
```

The customer username and password login are included in the command and the license is fetched automatically across the Internet. The login credentials are the same ones that are used for Clavister website login. The *reconf* or *shutdown* command should be used to complete installation.

- **Manually through the Web Interface or SCP**

This method is the only choice when the W50 hardware does not have a connection to the public Internet. The procedure consists of the following steps:

- In a web browser, go to the Clavister website at <https://www.clavister.com>, select **Log in** and then log in to the site. This will require registration on the site if this has not been done already.
- Go to **Licenses > Register License**.
- Select the option **Register by Service Tag and Hardware Serial Number**.
- Enter the *Serial Number* and *Service Tag* codes. For Clavister hardware products, these codes are found on a label on the unit.
- Download a license from the license list to the computer's local disk.
- The license file is uploaded to the firewall through the cOS Core Web Interface by going to **Status > Maintenance > License** and pressing the **Upload** button to select the license file. Following upload, cOS Core will install the file.

Alternatively, the license file can be uploaded using SCP. cOS Core automatically recognizes an uploaded license file but it is then necessary to manually perform a reconfigure or reboot operation to complete installation.



Important: Restart is recommended after license installation

After installing a license, a restart of cOS Core is recommended. This will ensure that cOS Core memory is correctly configured for the license parameters.

When installing a license through the Web Interface or when using the startup wizard, the options to restart or reconfigure are presented to the administrator. With the CLI and SCP, these options are not presented and restart must be initiated by the administrator.

*For restarting via the Web Interface, go to **Status > Maintenance > Reset & Restart**. With the CLI, use the command:*

```
Device:/> shutdown -reboot
```

Installing Licenses Updates

Installing license updates can be done using one of the following methods:

- Automatically, by creating a permanent link between the W50 and the associated *MyClavister* account on the Clavister website. Doing this is one of the last options in the setup wizard. Alternatively, the link can be established later by going to the **Status > Maintenance > MyClavister** in the Web Interface and entering the login credentials for the Clavister website.

The link can also be created in the CLI with the following command:

```
Device:/> license -myclavister -username=myuser -password=mypass
```

Once the link is established, cOS Core will alert the administrator in the Web Interface when a license update is available. The update process is then initiated by pressing the **Update** button in the license page.

- Manually, by logging into and downloading from the Clavister website and then uploading manually to cOS Core.
- Automatically through the separate InControl software product which is used for managing cOS Core configurations. This method can also be used to install the first license.

Licenses and license installation are described further in the separate *cOS Core Administrators Guide*.

4.5. Setup Troubleshooting

This appendix deals with connection problems that might occur when connecting a management computer to a Clavister Next Generation Firewall.

If the management interface does not respond after the Clavister Next Generation Firewall has powered up and cOS Core has started, there are a number of simple steps to troubleshoot basic connection problems:

1. Check that the correct interface is being used.

The most obvious problem is that the wrong Clavister Next Generation Firewall interface has been used for the initial connection. Only the first interface found by cOS Core is activated for the initial connection after cOS Core starts for the first time.

2. Check that interface characteristics match.

If a Clavister Next Generation Firewall'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 do not, 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 management computer IP is configured correctly.

The second most obvious problem is if the IP address of the management computer 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. Using the *ifstat* CLI command.

To investigate a connection problem further, connect the a console to the local console port on the Clavister Next Generation Firewall. Once cOS Core has started, it should respond with the a standard CLI prompt when the enter key is pressed. Now enter the following command once for each interface:

```
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 Next Generation Firewall 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.

6. Using the *arpsnoop* CLI command.

A diagnostic test to try is using the console command:

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

This will display console messages that show all the *ARP* packets being received on the different interfaces and confirm that the correct cables are connected to the correct interfaces. To look at the ARP activity only a particular interface, follow the command with the interface name:

```
Device:/> arpsnoop <interface>
```

To switch snooping off, use the command:

```
Device:/> arpsnoop none
```

4.6. Going Further with cOS Core

After initial setup is complete, the administrator is ready to go further with configuring cOS Core to suit the requirements of a particular networking scenario. All W50 resources can be downloaded from the W50 product page which can be found at <https://www.clavister.com/start>.

The primary reference documentation consists of:

- The cOS Core Administration Guide
- The cOS Core CLI Reference Guide
- The cOS Core Log Reference Guide

The cOS Core Administrators Guide

This guide is a comprehensive description of all cOS Core features and includes a detailed table of contents with a comprehensive index to quickly locate particular topics.

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.

Basic cOS Core Objects and Rules

As a minimum, the new administrator should become familiar with the cOS Core *Address Book* for defining IP address objects and with the cOS Core *IP rule set* for defining *IP Rule* objects which allow or block different traffic and which can also be used to set up NAT address translation.

IP rules identify the targeted traffic using combinations of the source/destination interface/network combined with protocol type. By default, no IP rules are defined so all traffic is dropped. At least one IP rule needs to be defined before traffic can traverse the Clavister Next Generation Firewall.

An alternative to *IP Rule* objects is to use *IP Policy* objects. These have essentially the same function but simplify the setting up of address translation and the use of important functions such as application control, virus scanning and web content filtering.

In addition to rules, *Route* objects need to be defined in a *Routing Table* so that traffic can be sent on the correct interface to reach its final destination. Traffic will need both a relevant rule and route to exist in order for it to traverse the firewall.

ALGs

Once the address book and IP rules are understood, the various ALGs will probably be relevant for managing higher level protocols such as HTTP. For example, for management of web browsing, the HTTP ALG provides a number of important features such as content filtering. Using *IP Policy* objects can remove the need to use ALGs as separate objects.

VPN Setup

A common requirement is to quickly setup VPN networks based on Clavister Next Generation Firewalls. The *cOS Core Administration 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 troubleshooting and advice on how best to deal with the networking complications that can arise with certificates.

Log Messages

By default, certain events will generate log messages and at least one log server should be configured in cOS Core to capture these messages. However, a cOS Core feature called *memlog* will capture recent log messages in local cOS Core memory. The administrator should review what events are important to them and at what severity. The *cOS Core Log Reference Guide* provides a complete listing of the log messages that cOS Core is capable of generating.

The CLI Reference Guide

The *CLI Reference Guide* provides a complete listing of the available CLI commands with their options. A CLI overview is also provided as part of the *cOS Core Administration Guide*.

cOS Core Education Courses

For details about classroom and online cOS Core education as well as cOS Core certification, visit the Clavister company website at <https://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://www.clavister.com/rss>. It is recommended to subscribe to this feed so that you receive notifications when new releases of cOS Core 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/>.

Chapter 5: W50 Maintenance

- Power Supply Replacement, page 76
- Fan Module Replacement, page 79

Replacing W50 Modules

The W50 device allows the on-site replacement of both the fan and the power supply modules. Performing these replacements is discussed in the following sections.

5.1. Power Supply Replacement

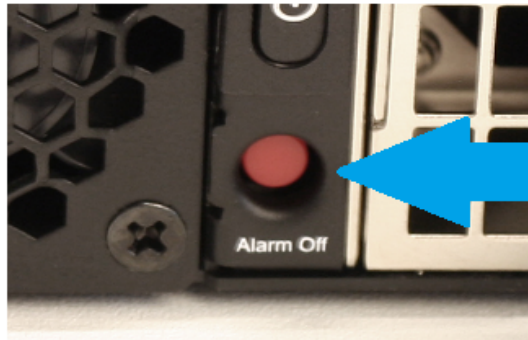
The W50 can be fitted with dual hot-swappable *Power Supply Units* (PSUs), both of which are capable of supplying power to the W50. The W50 can operate correctly with only one PSU but that configuration provides no redundancy.

As standard, the W50 is delivered with only a single PSU fitted and the second PSU slot is occupied by a dummy slot filler. The second PSU should be ordered as a separate spare part. A second PSU is fitted into the second PSU slot after taking out the dummy slot filler. Each PSU module is secured by a lock which is internal to the PSU and the lock is opened with a black locking switch on the PSU. There is also a silver metal hinged retaining cage on each PSU which is used for preventing the power cable from slipping out.

With two PSUs installed, only one of the PSUs is active and supplying power. If the active PSU fails then the other PSU will become active with no disruption to traffic throughput. The failed PSU can then be replaced with a new PSU and this can be done while the W50 is powered up.

Symptoms of PSU Failure

If two PSUs are fitted to provide redundancy and there is a single PSU failure, an audible alarm will be heard coming from the appliance. This alarm can be switched off by pressing the red button located to the left of the PSUs and marked **Alarm Off**. This button is indicated on the image shown below.



In normal operation there is a green LED light that is illuminated on the back of each PSU. This LED will **not** be illuminated if its PSU has failed. The LED position is indicated on the image shown below.



Monitoring PSU Status with cOS Core Hardware Monitoring

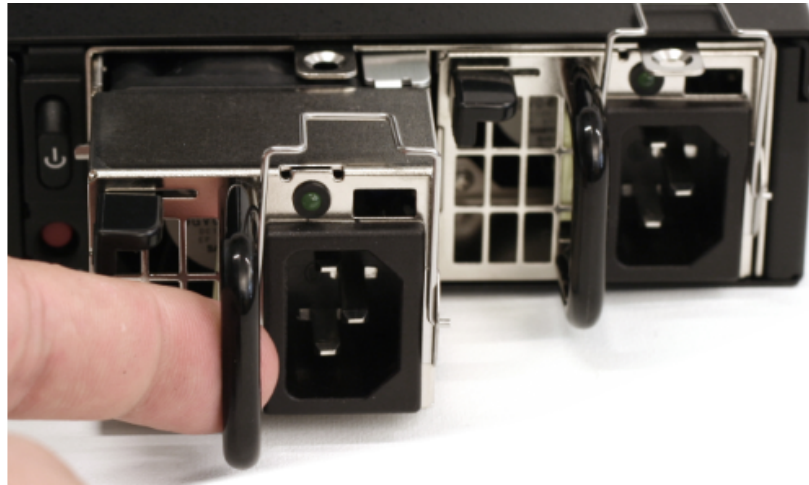
The current PSU status and therefore failure can be detected by using the *cOS Core Hardware Monitoring* feature and this is fully described in the separate *cOS Core Administration Guide*. This feature can confirm for the administrator that a PSU has failed and which PSU it is.

Steps for Swapping a PSU

To swap a PSU, use the following steps:

1. If the metal retaining cage is covering the PSU's power supply cord connector, push this upwards and fully back.
2. Remove the power supply cord from the PSU.

3. Push the PSU's locking lever to one side and pull the PSU out.



4. Insert the new PSU, making sure that it is locked securely in place.
5. Reinsert the power cord into the new PSU and apply power. The green status LED on the PSU should illuminate and cOS Core hardware monitoring should also indicate the presence and positive status of the new PSU.
6. Move the PSU's hinged metal retaining cage back so that it covers the cable connector to prevent it slipping out.



Note: Having a spare PSU available on-site

Having a spare PSU on-site and available will mean no delay if a replacement is required. These can be ordered from your Clavister sales representative.

5.2. Fan Module Replacement

Installed Fan Modules

The W50 has a series of 4 separate fan modules which are located at the back of the device. Each module contains two rotating fans giving a total of 8 fans for cooling the internal electronics. The power supply units (PSUs) contain their own separate fans for cooling and are not discussed in this section.



Figure 5.1. The Installed W50 Fan Modules

The Recommended Replacement Interval

The fan modules in the W50 are liable to wear from mechanical movement. Any fan failure can lead to much more serious internal failures from the overheating of electronic components. Although W50 fan modules are built for prolonged use, it is nonetheless a recommended precaution that modules be replaced every two years.

Detecting Fan Failure

Any of the 4 fan unit modules can be hot-swapped on-site if they require scheduled replacement or an internal failure is detected. Fan failure can be detected by using the cOS Core *Hardware Monitoring* feature and this is fully described in the separate *cOS Core Administration Guide*. This feature can tell the administrator if one or both fans inside a module have failed.



Important: Dusty environments reduce fan module lifetimes

The W50 fan modules are designed to operate in environments with reasonable air quality. Elevated dust levels in the surrounding air can substantially reduce the operating lifetimes of these fan modules.

Fan Replacement Steps

To replace a fan module, use the following steps:

1. Unscrew the individual fan module's retaining screw. This is located at one corner of each module.



2. Firmly grip the fan module and pull it out from the W50 chassis.



3. Insert the new module and secure its corner retaining screw.



4. The new module should start up immediately if power is available.



Tip: Having spare fan modules available on-site

Having spare fan modules on-site and available will mean no delay if a replacement is required. Modules can be ordered from your Clavister sales representative.

Chapter 6: Interface Expansion Modules

The W50 product has four expansion slots, each of which can accept a Clavister *interface expansion module*. There are three different module types available and these are purchased separately to the W50 unit. Each of the three module types has different capabilities and can be one of the following:

- 8 x RJ45 Gigabit Ethernet interfaces.
- 8 x SFP Gigabit interfaces.
- 2 x SFP+ 10 Gigabit interfaces.

These optional modules are shown below:



Figure 6.1. An 8 x RJ45 Gigabit Interface Expansion Module for the W50

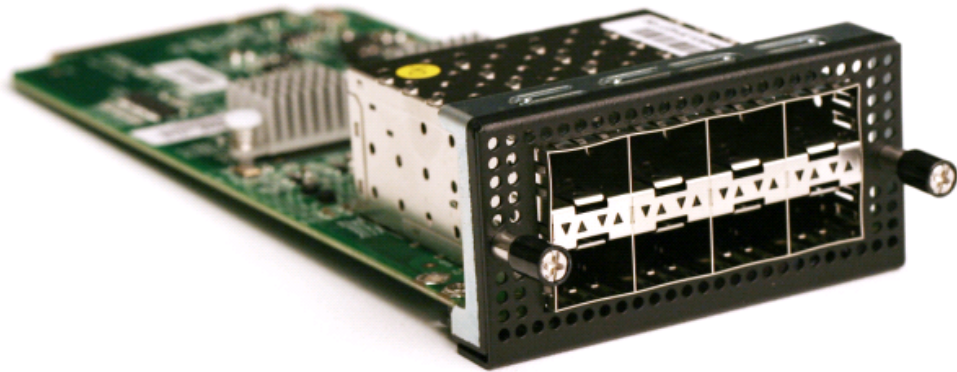


Figure 6.2. An 8 x SFP Gigabit Interface Expansion Module for the W50

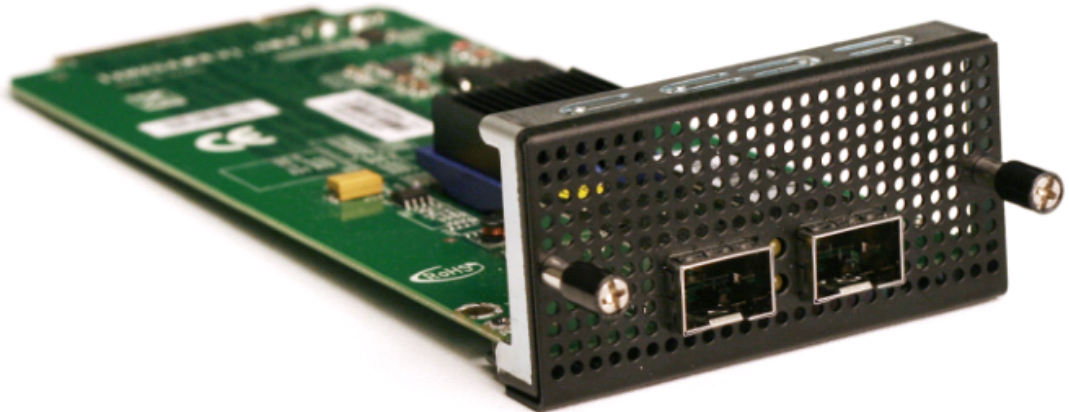


Figure 6.3. A 2 x SFP+ 10 Gigabit Interface Expansion Module for the W50

The full connection capabilities of all these Ethernet interfaces are listed in *Appendix A, W50 Specifications*.

Adding an Expansion Module

A W50 expansion module is added using a *cold swap* procedure. The steps are as follows:

1. Shutdown cOS Core and power down the W50. For safety, disconnecting the power cable is advised.
2. Take off the plate covering the empty expansion slot. This is done by first undoing the two retaining screws on either side of the plate. These screws may need loosening with a suitable screwdriver before undoing completely by hand. The screws are on springs and will spring out when they are no longer held by the thread in the chassis.
3. Attach an earthed *anti-static wrist strap* to the wrist of the hand that will handle the module. Doing this is strongly advised since expansion modules are not closed units.
4. With the hand that is correctly earthed, remove the expansion module from its anti-static bag. Try not to touch any of the exposed electronics when doing this.

5. Gently insert the expansion module by sliding it into the expansion slot, as shown below. The module should engage with rails on either side. Do not force it as it may not be properly aligned or may be the wrong way up.



6. Secure the module by hand tightening the two screws on either side. These screws are on springs and will first need to be pushed in to make contact with the thread in the chassis. After hand tightening, finish by applying minimal extra tightening with a suitable screwdriver to ensure the screws are secure.
7. Now, power up the hardware to restart cOS Core. As explained in detail below, the additional Ethernet interfaces will be automatically detected by cOS Core and added to the configuration with a logical name derived from the chassis slot number and interface position in the module.

The inserted module may be removed or swapped with a different expansion module by following the same procedure.

Ethernet Interface and Address Object Naming in cOS Core

After startup, cOS Core will detect the presence of the extra interfaces and add them to the configuration. No action from the administrator is needed for this to happen. The interfaces will be named according to the slot they are in (some hardware products have more than one slot) and their position on the expansion module.

The assigned interface name will always have the following form: **En-m**. The name always begins with the letter **E**. The number **n** is the slot number and the number **m** is the position on the expansion module. For example, the second interface of an expansion module in the first slot will have the name **E1-2**.

For the W50, the slot numbers go from left to right when looking at the front of the device. In other words, slot number **1** is on the furthest left hand side, next to the single fixed **G1** Ethernet port.

cOS Core will also automatically add an IP and network address object into the configuration's address book using the normal convention for interfaces. For example, the interface **E1-2** will get an IPv4 address object called **E1-2_ip** and an IPv4 network object called **E1-2_net**.

Removing Interfaces

An expansion module can also be removed after powering off the W50. When cOS Core is started again, the configuration will be unchanged. However, no data will be received or sent on an interface that does not physically exist.

If another expansion module is then fitted later and it contains an interface port that has the same position as the removed one (in other words, it's logical cOS Core name is the same) traffic can flow through the new interface since the configuration references will now have a corresponding physical interface.

Installing SFP/SFP+ Modules

Two of the W50 expansion module options provide connectivity for *Small Form Pluggable* (SFP) and *Small Form Pluggable Plus* (SFP+) modules. The W50 expansion modules do not come as standard with any SFP or SFP+ modules but they can be ordered from your Clavister reseller. Shown below is a typical SFP unit.



Figure 6.4. An Example of an SFP 1000 Base TX Module

Installation of the different types of SFP/SFP+ modules is performed in a similar way. For example, with the module shown above, insertion into the sockets is done with the label facing upwards. The module slides into position by gently pressing it inwards.

The image below shows insertion of an SFP module into the expansion module option that provides connectivity for 8 Gigabit SFP modules.



Figure 6.5. Insertion of a Gigabit SFP Module



Warning: Insert SFP/SFP+ modules in the correct sockets

*An SFP module must **not** be inserted in an SFP+ socket. Similarly, SFP+ modules must **not** be inserted in an SFP socket.*

Chapter 7: Resetting to Factory Defaults

In some circumstances, it may be necessary to reset the W50 hardware to the state it was in when it left the factory and was delivered to a customer. This process is known as a *reset to factory defaults* or simply a *factory reset*.



Caution: cOS Core upgrades and current configuration are lost

Resetting to factory defaults means that the default cOS Core configuration will be restored as well as the original version of cOS Core that the product left the factory with. Any cOS Core upgrades that have been installed will be lost.

This means:

- *Any cOS Core upgrades that have been performed since the product left the factory will be lost. An upgrade to a newer cOS Core version must be repeated.*
 - *The current cOS Core configuration will be lost but can be restored if a backup is available.*
-

With the W50, a reset can be done in one of the following ways:

- **Using the Web Interface**

A factory reset is possible through a web browser over a network connection using the cOS Core Web Interface (WebUI). The steps to do this are the following:

1. Open a web browser and enter the IP address of the management interface. The cOS Core web interface login dialog should be displayed. Connecting with a browser is described further in *Section 3.4, "Management Computer Connection"*.
2. Log in to cOS Core as an administrator
3. Go to: **Status > Maintenance > Reset & Restart**
4. Select the option: **Reset the entire unit to factory defaults.**
5. Press the **Reset** button.

Note that this will reset all the IP addresses on Ethernet interfaces to their defaults which might mean that the network connection will be lost.

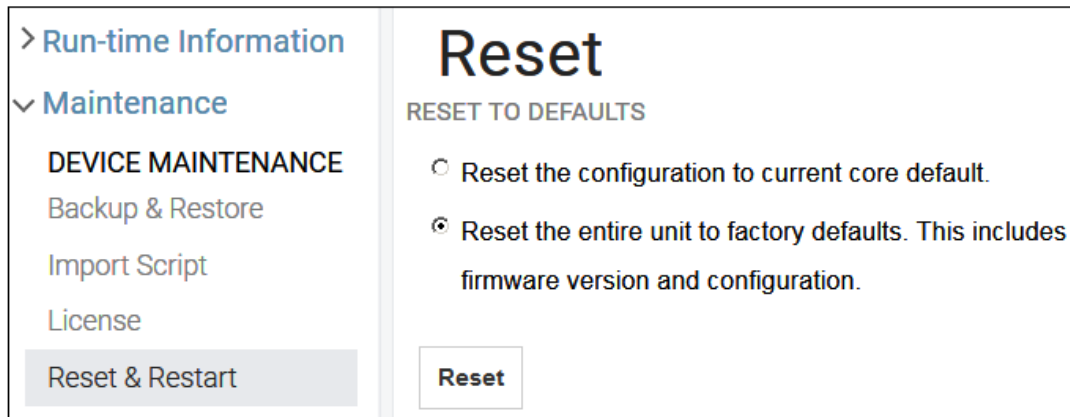


Figure 7.1. Factory Reset Using the Web Interface

- **Using the CLI**

The cOS Core CLI can be used by connecting to one of the W50's Ethernet interfaces using an SSH client over a network. A reset is performed by entering the `reset -unit` command twice in succession:

```
Device:/> reset -unit
Device:/> reset -unit
```

Entering the command twice is a safeguard against accidental use. Note that, like using the Web Interface method above, this will reset all the IP addresses on Ethernet interfaces to their defaults which may mean that the SSH connection will be lost.

- **Using the Boot Menu**

The boot menu can be accessed through the local CLI console by pressing any console key while cOS Core is starting up. The resetting of Ethernet interface IP addresses will not affect the local console connection. A factory reset using the boot menu is performed with the following steps:

1. Make sure a separate management computer running as a console is attached to the local console port of the W50.
2. Power up the W50 unit. This may require a restart if the hardware is already powered up.
3. As the console output appears, press any console key before cOS Core has fully started.
4. The *boot menu* will now be displayed on the console.
5. Choose the menu item **Reset Options**.
6. Various reset options are now displayed on the console. For a full reset, select the menu option **Reset to Factory Defaults**.

A complete description of the boot menu and all its options can be found in the separate *cOS Core Administrators Guide*.

- **Performing a Reset Manually**

The W50 can be reset manually with the following steps:

1. The progress of the reset can be followed using a local console connection. If that is required, open a console display window connected to the W50 local console port.
2. Power off the W50.
3. Push in the recessed reset button on the W50 with a suitable pointed tip tool and keep it pushed in. A suitable paper-clip could be used to do this.
4. Power up the W50 while still holding the reset button in.
5. Continue holding the button in for at least 30 seconds longer after the power is applied.
6. If a console was connected in step **1**, the console output will indicate that the hardware has been reset to its factory defaults.
7. Release the button and the W50 can now be configured as though it had been newly delivered and had not been previously configured.



Important: The local console password will be reset to none

*If a local console password was set this will also be reset to the factory default of no password. If required, the local console password should be set later by choosing the boot menu option **Enable Console Password**.*

Chapter 8: Warranty Service

Limitation of Warranty

Clavister warrants to the customer of the W50 Appliance that the Hardware components will be free from defects in material and workmanship under normal use for a period of two (2) years from the Start Date (as defined below). The warranty will only apply to failure of the product if Clavister is informed of the failure not later than two (2) years from the Start Date or thirty (30) days after that the failure was or ought to have been noticed by the customer.

The warranty will not apply to products from which serial numbers have been removed or to defects resulting from unauthorized modification, operation or storage outside the environmental specifications for the product, in-transit damage, improper maintenance, defects resulting from use of third-party software, accessories, media, supplies, consumables or such items not designed for use with the product, or any other misuse. Any replacement Hardware will be warranted for the remainder of the original warranty period or thirty days, whichever is longer.

Note that the term "Start Date" means the earlier of the product registration date **OR** ninety (90) days following the day of shipment by Clavister.

Obtaining Warranty Service with an RMA

Warranty service can be obtained within the warranty period with the following steps:

1. Obtain a **Return Material Authorization (RMA) Number** from Clavister. This number **must** be obtained before the product is sent back.

An RMA number can be obtained online by logging in to the Clavister website (<http://www.clavister.com/login>) and selecting the **Help Desk** option.



Note: The cold standby service uses a different procedure

*If the defective unit is subject to a Clavister **Cold Standby (CSB)** agreement then the procedure to follow is described in the relevant section of the separate **Clavister Hardware Replacement Guide**.*

This guide also describes the cOS Core configuration steps for swapping any Clavister firewall with a replacement unit.

2. The defective unit should be packaged securely in the original packaging or other suitable

shipping packaging to ensure that it will not be damaged in transit.

3. The RMA number must be clearly marked on the outside of the package.
4. The package is then shipped to Clavister with all the costs of mailing/shipping/insurance paid by the customer. The address for shipping is:

Clavister AB
Sjögatan 6J
891 60 Örnsköldsvik
SWEDEN

If the product has not yet been registered with Clavister through its website, some proof of purchase (such as a copy of the dated purchase invoice) must be provided with the shipped product.



Important: An RMA Number must be obtained before shipping!

Any package returned to Clavister without an RMA number will be rejected and shipped back at the customer's expense. Clavister reserves the right in such a case to levy a reasonable handling charge in addition to mailing and/or shipping costs.

Data on the Hardware

Note that Clavister is not responsible for any of the software, firmware, information, or memory data contained in, stored on, or integrated with any product returned to Clavister pursuant to a warranty claim.

Contacting Clavister

Should there be a problem with the online form then Clavister support can be contacted by going to: <https://www.clavister.com/support/>.

Customer Remedies

Clavister's entire liability according to this warranty shall be, at Clavister's option, either return of the price paid, or repair or replacement of the Hardware that does not meet Clavister's limited warranty and which is returned to Clavister with a copy of your receipt.

Limitations of Liability

Refer to the legal statement at the beginning of the guide for a statement of liability limitations.

Chapter 9: Safety Precautions

Safety Precautions

Clavister W50 devices are *Safety Class I* products and have protective ground terminals. There must be an uninterrupted safety earth ground from the main power source to the product's input wiring terminals, power cord, or supplied power cord set. Whenever it is likely that the protection has been impaired, disconnect the power cord until the ground has been restored.

For LAN cable grounding:

- If your LAN covers an area served by more than one power distribution system, be sure their safety grounds are securely interconnected.
- LAN cables may occasionally be subject to hazardous transient voltage (such as lightning or disturbances in the electrical utilities power grid). Handle exposed metal components of the network with caution.

There are no user-serviceable parts inside these products. Only service-trained personnel can perform any adjustment, maintenance or repair.

Säkerhetsföreskrifter

Dessa produkter är säkerhetsklassade enligt klass I och har anslutningar för skyddsjord. En obruten skyddsjord måste finnas från strömkällan till produktens nätkabelanslutning eller nätkabel. Om det finns skäl att tro att skyddsjorden har blivit skadad, måste produkten stängas av och nätkabeln avlägnas till dess att skyddsjorden har återställts.

För LAN-kablage gäller dessutom att:

- om LAN:et täcker ett område som betjänas av mer än ett strömförsörjningssystem måste deras respektive skyddsjord vara ihopkopplade.
- LAN kablage kan vara föremål för farliga spänningstransienter (såsom blixtnedslag eller störningar i elnätet). Hantera metallkomponenter i förbindelse med nätverket med försiktighet.

Det finns inga delar i produkten som kan lagas av användaren. All service samt alla justeringar, underhåll eller reparationer får endast utföras av behörig personal.

Informations concernant la sécurité

Cet appareil est un produit de classe I et possède une borne de mise à la terre. La source d'alimentation principale doit être munie d'une prise de terre de sécurité installée aux bornes du câblage d'entrée, sur le cordon d'alimentation ou le cordon de raccordement fourni avec le produit. Lorsque cette protection semble avoir été endommagée, débrancher le cordon d'alimentation jusqu'à ce que la mise à la terre ait été réparée.

Mise à la terre du câble de réseau local:

- si votre réseau local s'étend sur une zone desservie par plus d'un système de distribution de puissance, assurez-vous que les prises de terre de sécurité soient convenablement interconnectées.
- Les câbles de réseaux locaux peuvent occasionnellement être soumis à des surtensions transitoires dangereuses (telles que la foudre ou des perturbations dans le réseau d'alimentation public). Manipulez les composants métalliques du réseau avec précautions.

Aucune pièce contenue à l'intérieur de ce produit ne peut être réparée par l'utilisateur. Tout dépannage, réglage, entretien ou réparation devra être confié exclusivement à un personnel qualifié.

Hinweise zur Sicherheit

Dies ist ein Gerät der Sicherheitsklasse I und verfügt über einen schützenden Erdungsterminal. Der Betrieb des Geräts erfordert eine ununterbrochene Sicherheitserdung von der Hauptstromquelle zu den Geräteingabeterminals, den Netzkabeln oder dem mit Strom belieferten Netzkabelsatz voraus. Sobald Grund zur Annahme besteht, dass der Schutz beeinträchtigt worden ist, das Netzkabel aus der Wandsteckdose herausziehen, bis die Erdung wiederhergestellt ist.

Für LAN-Kabelerdung:

- Wenn Ihr LAN ein Gebiet umfasst, das von mehr als einem Stromverteilungssystem beliefert wird, müssen Sie sich vergewissern, dass die Sicherheitserdungen fest untereinander verbunden sind.
- LAN-Kabel können gelegentlich gefährlichen Übergangsspannungen ausgesetzt werden (beispielsweise durch Blitz oder Störungen in dem Starkstromnetz des Elektrizitätswerks). Bei der Handhabung exponierter Metallbestandteile des Netzwerkes Vorsicht walten lassen.

Dieses Gerät enthält innen keine durch den Benutzer zu wartenden Teile. Wartungs-, Anpassungs-, Instandhaltungs- oder Reparaturarbeiten dürfen nur von geschultem Bedieningspersonal durchgeführt werden.

Considerazioni sulla sicurezza

Questo prodotto è omologato nella classe di sicurezza I ed ha un terminale protettivo di collegamento a terra. Dev'essere installato un collegamento a terra di sicurezza, non interrompibile che vada dalla fonte d'alimentazione principale ai terminali d'entrata, al cavo d'alimentazione oppure al set cavo d'alimentazione fornito con il prodotto. Ogniqualvolta vi sia probabilità di danneggiamento della protezione, disinserite il cavo d'alimentazione fino a quando il collegamento a terra non sia stato ripristinato.

Per la messa a terra dei cavi LAN:

- se la vostra LAN copre un'area servita da più di un sistema di distribuzione elettrica, accertatevi che i collegamenti a terra di sicurezza siano ben collegati fra loro;
- i cavi LAN possono occasionalmente andare soggetti a pericolose tensioni transitorie (ad esempio, provocate da lampi o disturbi nella griglia d'alimentazione della società elettrica); siate cauti nel toccare parti esposte in metallo della rete.

Nessun componente di questo prodotto può essere riparato dall'utente. Qualsiasi lavoro di riparazione, messa a punto, manutenzione o assistenza va effettuato esclusivamente da personale specializzato.

Consideraciones sobre seguridad

Este aparato se enmarca dentro de la clase I de seguridad y se encuentra protegido por una borna de puesta a tierra. Es preciso que exista una puesta a tierra continua desde la toma de alimentación eléctrica hasta las bornas de los cables de entrada del aparato, el cable de alimentación hasta haberse subsanado el problema.

Puesta a tierra del cable de la red local (LAN):

- Si la LAN abarca un área cuyo suministro eléctrico proviene de más de una red de distribución de electricidad, cerciorarse de que las puestas a tierra estén conectadas entre sí de modo seguro.
- Es posible que los cables de la LAN se vean sometidos de vez en cuando a voltajes momentáneos que entrañen peligro (rayos o alteraciones en la red de energía eléctrica). Manejar con precaución los componentes de metal de la LAN que estén al descubierto.

Este aparato no contiene pieza alguna susceptible de reparación por parte del usuario. Todas las reparaciones, ajustes o servicio de mantenimiento debe realizarlos solamente el técnico.

Appendix A: W50 Specifications



Dimensions, Weight and MTBF

Height x Width x Depth (mm)	44 x 438 x 580
Hardware Weight	10.5 kg (no expansion modules, single PSU)
Packaged Weight	18.6 kg (no expansion modules, single PSU)
Second PSU Weight	0.6 kg
8 x RJ45 Module Weight	0.25 kg
8 x SFP Module Weight	0.2 kg
2 x SFP+ Module Weight	0.16 kg
Hardware Form Factor	1U
19-inch Rack Mountable	Yes, using rack mount kit
MTBF	106,299 hours

Regulatory and Safety Standards

Safety	CE, UL
EMC	FCC class A, CE class A

Environmental

Operating Humidity	5% to 90% (non-condensing)
Storage Humidity	5% to 95% (non-condensing)
Operating Temperature	0 to 45° C
Storage Temperature	-20 to 70° C
Random vibration IEC 60068-2-64 (operating)	0.5 G2/Hz (5-500 Hz)

Power Specifications

Redundant Hot-Swappable Power Supply (AC)	100-240 VAC, 50-60 Hz, 3.5-1.7 A
Typical Power Consumption	230 W
Typical Current @ 230V	1 A
BTU	785 BTU
PSU Rated Power	400 W for each PSU

Ethernet Interface Support

Gigabit RJ45 interfaces	Automatic MDI-X 1000BASE-T (copper RJ45 100m) 100BASE-TX (copper RJ45 100m) 10BASE-T (copper RJ45 100m)
SFP interfaces (if expansion module installed)	1000BASE-SX (multi-mode 550m) 1000BASE-LX (single-mode 10,40,80km)

	1000BASE-T (copper RJ45 100m)
SFP+ interfaces (if expansion module installed)	10GBASE-SR (multi-mode 300m) 10GBASE-LR (single-mode 10km) 10GBASE-ER (single-mode 40km) 10GBASE-ZR (single-mode 80km) 10GBASE-CR (direct attach)

For more information about Clavister products, go to: <http://www.clavister.com>.

Appendix B: Declarations of Conformity

CLAVISTER



DECLARATION OF CONFORMITY

We, the manufacturer,
Clavister AB
Sjögatan 6J
SE-891 60 ÖRNSKÖLDSVIK
SWEDEN

Declares that the product

Product Description: Network Security Appliance
Model Designation: **Clavister Wolf W50 Series**

Is in compliance with the essential requirements and other relevant provisions of the following directives:

Electromagnetic Compatibility Directive	(2004/108/EC)
RoHS Directive	(2011/65/EU)

The product is compatible with the following norms / standards:

EN 55022	(2010 + AC: 2011, Class A)
EN 61000-3-2	(2006 + A1:2009 + A2:2009, Class A)
EN 61000-3-3	(2008)
EN 55024	(2010)
IEC 61000-4-2	(2008)
IEC 61000-4-3	(2006 + A1:2007 + A2:2010)
IEC 61000-4-4	(2004 + A1:2010)
IEC 61000-4-5	(2005)
IEC 61000-4-6	(2008)
IEC 61000-4-8	(2009)
IEC 61000-4-11	(2004)
AS/NZS CISPR 22	(2009 + A1:2010, Class A)

Manufacturer/Authorised representative

Jim Carlsson, CEO
Örnsköldsvik, 2015-09-15

Report ID: EC412288

CLA APP-W50-CEDOC-A002

CLAVISTER



DECLARATION OF CONFORMITY

We, the manufacturer,
Clavister AB
Sjögatan 6J
SE-891 60 ÖRNSKÖLDSVIK
SWEDEN

Declares that the product

Product Description: Network Security Appliance
Model Designation: **Clavister Wolf W50 Series**

Is in compliance with the essential requirements and other relevant provisions of the following:

FCC CFR Title 47 Part 15 Subpart B: 2010

Federal Communication Commission
Code of Federal Regulations
Telecommunications, Radio frequency devices,
unintentional radiators

Canadian Standards Association
Standard ICES-003

Spectrum Management and
Telecommunications Policy Interference-
Causing Equipment Standard, Digital Apparatus

The product is compatible with the following norms / standards:

FCC CFR Title 47 Part 15 Subpart B Class A: 2010
CSA ICES-003 Class A
ANSI C63.4-2009

Manufacturer/Authorised representative

A handwritten signature in blue ink, appearing to read 'Jim Carlsson'.

Jim Carlsson, CEO
Örnsköldsvik, 2015-09-14

Certificate ID: FV412288

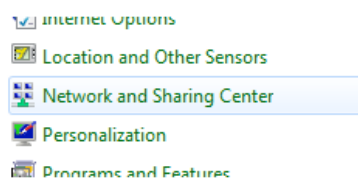
CLA-APP-W50-FCCDOC-A601

Appendix C: Windows 7 IP Setup

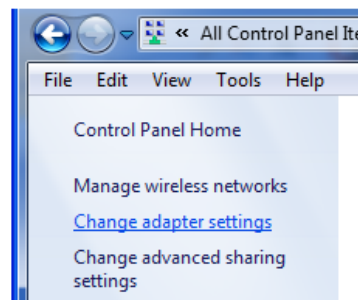
If a PC running Microsoft Windows 7™ is being used as the cOS Core management computer, the computer's Ethernet interface connected to the Clavister Next Generation Firewall must be configured with an IPv4 address which belongs to the network *192.168.1.0/24* and is different from the firewall's address of *192.168.1.1*.

The IPv4 address *192.168.1.30* will be used for this purpose and the steps to set this up with Windows 7 are as follows:

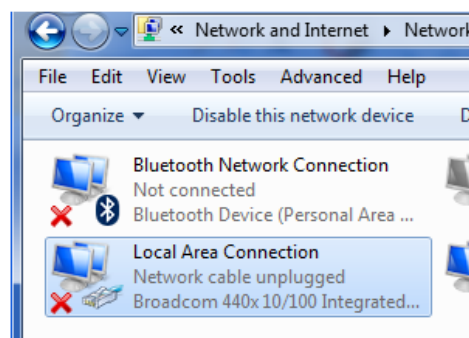
1. Press the Windows **Start** button.
2. Select the **Control Panel** from the start menu.
3. Select **Network & Sharing Center** from the control panel.



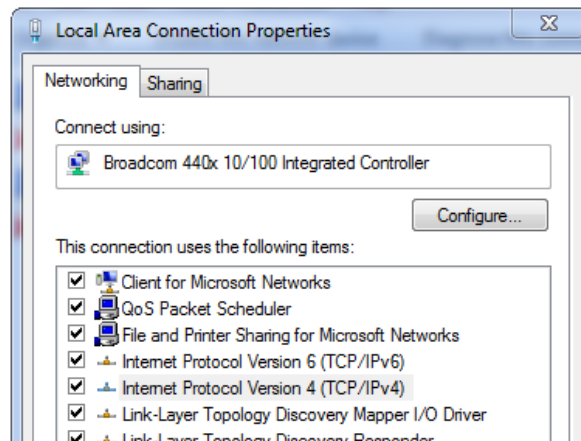
4. Select the **Change adapter settings** option.



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

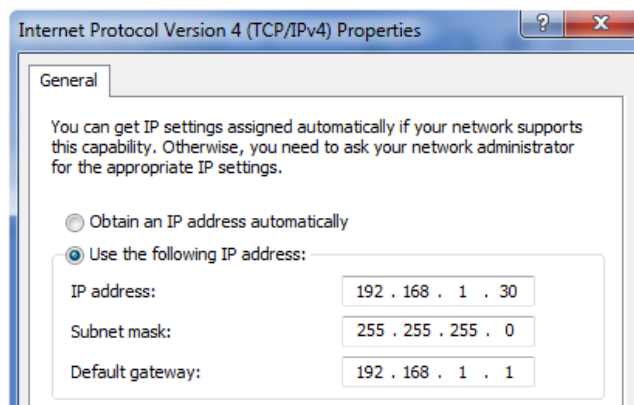


6. The properties for the selected interface will appear.



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



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

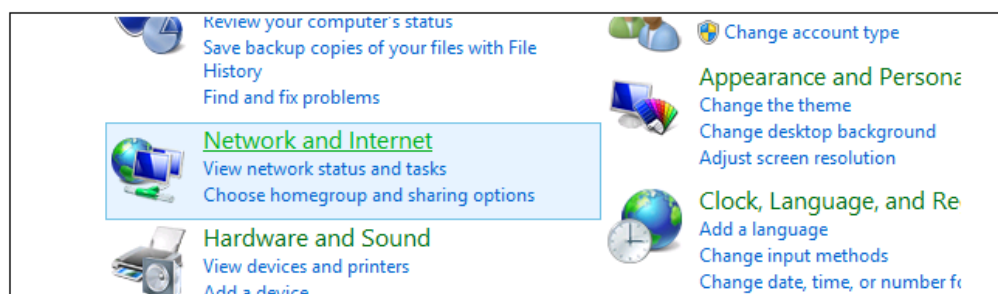
8. Click **OK** to close this dialog and close all the other dialogs opened since step (1).

Appendix D: Windows 8/8.1/10 IP Setup

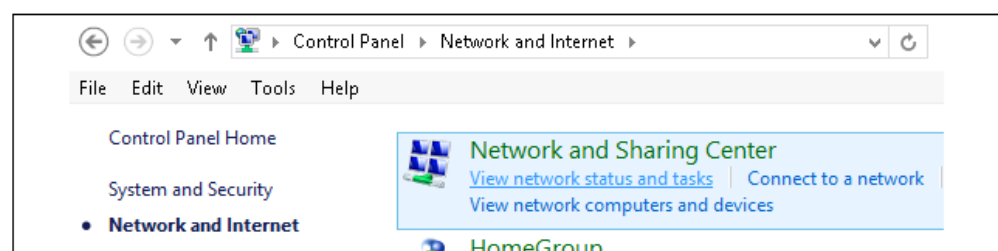
If a computer running Windows is being used as the cOS Core management computer and a DHCP server is not enabled on the cOS Core management interface, the management computer's Ethernet interface connected to the Clavister Next Generation Firewall should be configured with an IPv4 address which belongs to the network 192.168.1.0/24. That address must be different from the firewall's default management interface address of 192.168.1.1.

It is assumed that the IPv4 address 192.168.1.30 will be used for this purpose and the steps to set this up with Windows versions 8, 8.1 or 10 are as follows:

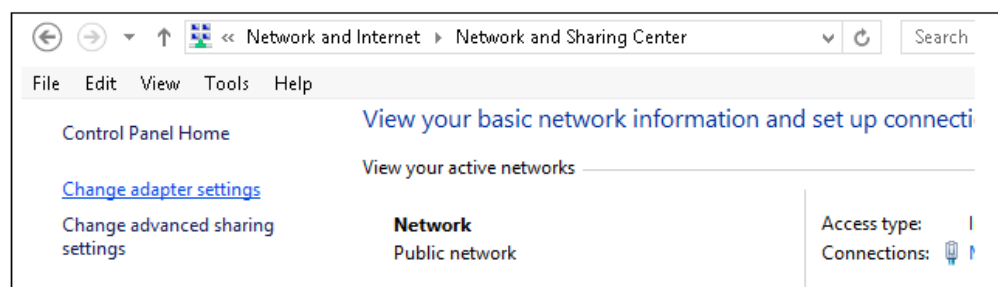
1. Open the Windows **Control Panel** (the *Category* view is assumed here).
2. Select **Network & Internet** from the control panel.



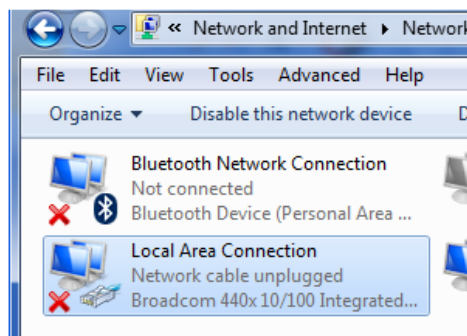
3. Then, select the **Network & Sharing Center** option.



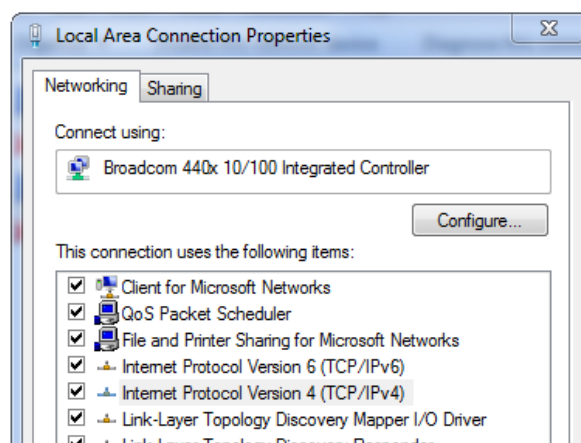
4. Now, select the **Change adapter settings** option.



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

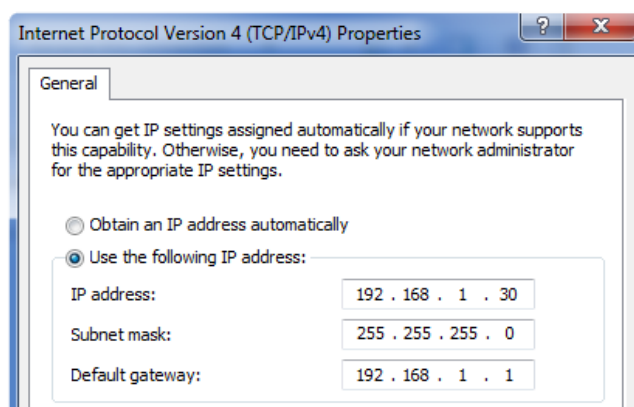


6. The properties for the selected interface will appear.



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



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)**.

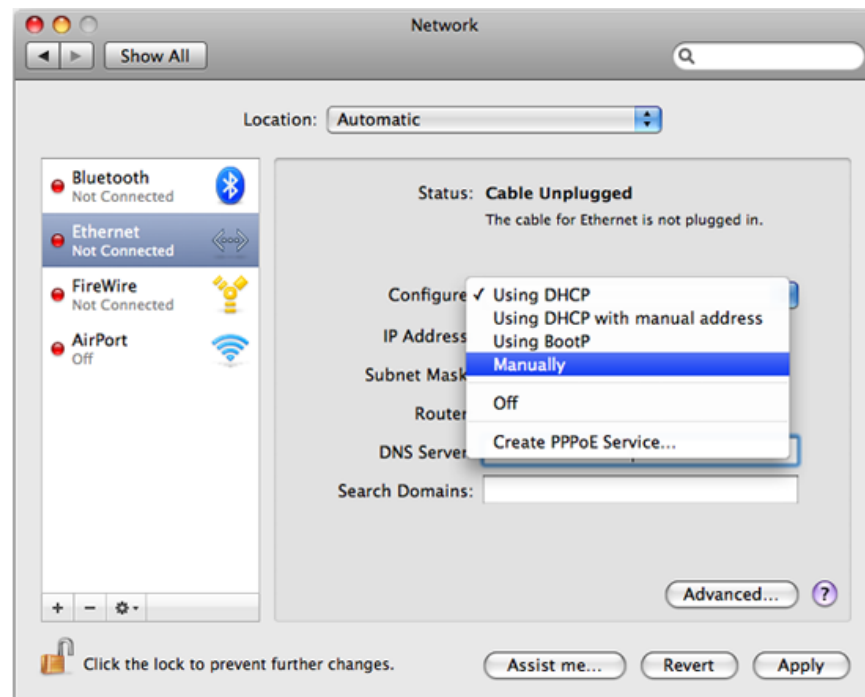
Appendix E: Apple Mac IP Setup

An Apple Mac can be used as the management computer for initial setup of a Clavister Next Generation Firewall. 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**.

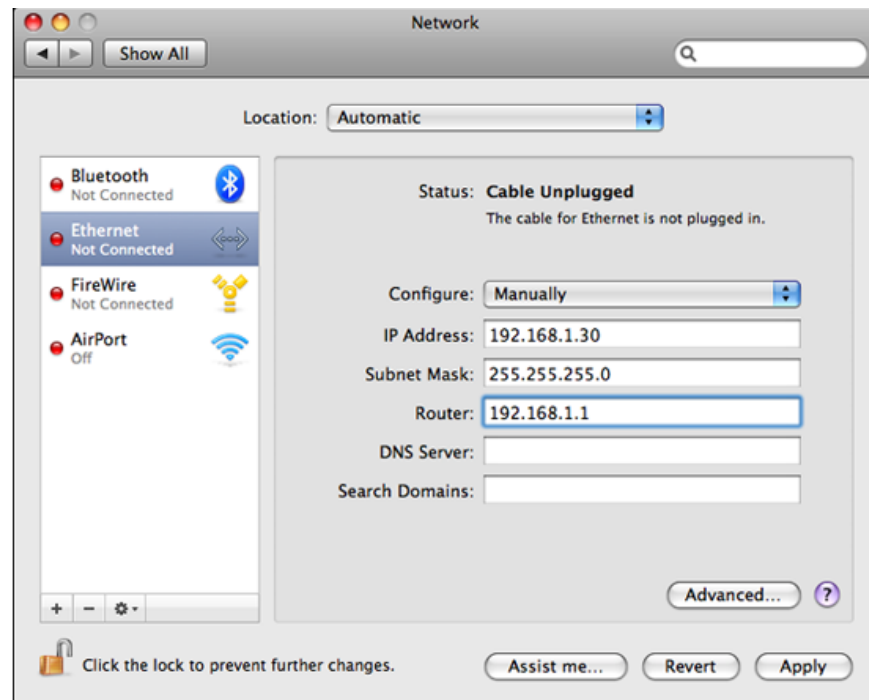


3. Select **Ethernet** from the left sidebar menu.
4. Select **Manually** in the **Configure** pull down menu.



5. Now set the following values:

- **IP Address:** 192.168.1.30
- **Subnet Mask:** 255.255.255.0
- **Router:** 192.168.1.1



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



CLAVISTER®

CONNECT • PROTECT

Clavister AB
Sjögatan 6J
SE-89160 Örnsköldsvik
SWEDEN

Head office/Sales: +46-(0)660-299200
Customer support: +46-(0)660-297755

www.clavister.com