

Clavister
NetWall

Clavister NetWall 100 Series Getting Started Guide

Clavister NetWall 100 Series

Getting Started Guide

Published 2021-10-26

Copyright © Clavister AB
Sjögatan 6J
SE-89160 Örnsköldsvik
SWEDEN

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

www.clavister.com

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 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. NetWall 100 Series Overview	7
1.1. Unpacking	7
1.2. Interfaces and Ports	10
1.3. Status Lights	12
1.4. Zero Touch Support	13
1.5. Hardware Sensor Monitoring	15
2. Registering with Clavister	17
3. Installation	22
3.1. General Installation Guidelines	22
3.2. Flat Surface Installation	24
3.3. Management Computer Connection	25
3.4. Local Console Port Connection	28
3.5. Connecting Power	30
4. cOS Core Configuration	32
4.1. The NetWall 100 Series Default Configuration	32
4.2. Web Interface and Wizard Setup	34
4.3. Manual Web Interface Setup	43
4.4. Manual CLI Setup	58
4.5. License Installation	67
4.6. Setup Troubleshooting	70
5. Resetting to Factory Defaults	73
6. Warranty Service	75
7. Safety Precautions	77
A. NetWall 100 Series Specifications	80

List of Figures

1.1. An Unpacked NetWall 100 Series Unit	7
1.2. NetWall 100 Series Interfaces and Ports	10
1.3. NetWall 100 Series Interface Ports	11
1.4. NetWall 100 Series Status Panel View	12
3.1. The NetWall 100 Series Local Console Port	28
3.2. NetWall 100 Series Power Inlet Connector	30
5.1. Factory Reset Using the Web Interface	74

Preface

Target Audience

The target audience for this guide is the administrator who has taken delivery of a packaged Clavister NetWall 100 Series 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, NetWall 100 Series 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: NetWall 100 Series Overview

- Unpacking, page 7
- Interfaces and Ports, page 10
- Status Lights, page 12
- Zero Touch Support, page 13
- Hardware Sensor Monitoring, page 15



Important: Only cOS Core version 14.00.00 or later is supported

The NetWall 100 Series hardware product can run any cOS Core version from 14.00.00 onwards. Earlier versions are not supported and a downgrade should not be attempted.

1.1. Unpacking



Figure 1.1. An Unpacked NetWall 100 Series Unit

This section details the unpacking of a single NetWall 100 Series device. Open the packaging box used for shipping and carefully unpack the contents. The packaging should contain the following:

- The NetWall 100 Series appliance.
- RJ45 Ethernet cable.
- Power cable.
- 12V/2A AC to DC power adapter.



Note: Report any items that are missing

If any items are missing from the NetWall 100 Series package, please contact your sales representative.

Support Agreements

All purchasers of a new NetWall hardware product must also 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 event of a hardware fault. The terms of warranty are described further in *Chapter 6, 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 NetWall 100 Series 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 *NetWall Hardware Replacement Guide* PDF publication.

Downloading NetWall 100 Series Resources

All documentation, version upgrades and other resources for the NetWall 100 Series can be downloaded from the Clavister website after logging into the relevant *MyClavister* account.

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 during business hours.

End of Life Treatment

The NetWall 100 Series appliance 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 disposal of such specialist materials.



WARNING: REPLACE ANY 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 APPROPRIATELY.

1.2. Interfaces and Ports

This section is an overview of the NetWall 100 Series product's external connectivity options.



Figure 1.2. NetWall 100 Series Interfaces and Ports



Note: The meaning of the terms "Front" and "Back"

The term "Front" will be used in this guide to refer to the side of the 100 Series that has the Ethernet ports and the term "Back" to the side that has the status lights.

The NetWall 100 Series features a number of connection ports on the front panel:

- **4 x RJ45 Gigabit Ethernet interfaces**

These have the logical cOS Core interface names **WAN1**, **LAN1**, **WAN2** and **LAN2**. These names are written above each interface on the NetWall 100 Series casing.

The **LAN1** interface is used for initial management connection. The **WAN1** is normally used for the first connection to the public Internet.

In the default cOS Core configuration, the **LAN1** interface of the NetWall 100 Series has an IPv4 DHCP server enabled on it so it will automatically hand out IP addresses belonging to the default management network to a connecting client. In addition, both the **WAN1** and **WAN2** interfaces have an IPv4 DHCP client enabled so that they can automatically be assigned an IP address if either or both are connected to an ISP (dual connection can provide redundancy).

The default cOS Core configuration contains a predefined IP rule set that allows clients on the **LAN1** interface to immediately access the Internet via either **WAN1** or **WAN2**. If both interfaces provide Internet access, **WAN1** takes precedence because its *all-nets* route has a lower metric.

The default cOS Core configuration is discussed further in *Section 4.1, "The NetWall 100 Series Default Configuration"*.

- **An RJ45 RS-232 console port**

This port is used for direct access to the cOS Core *Boot Menu* and the cOS Core *Command Line Interface* (CLI). Connecting to this port is described in *Section 3.4, "Local Console Port Connection"*.



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

*The two **USB Type A** ports on the 100 Series front panel are for future functionality and are not currently used by cOS Core.*

All the Ethernet interface ports function independently of each other and are not connected by a switch fabric. All are capable of link speed auto-negotiation and can operate using 10Base-T, 100Base-Tx, or 1000Base-T. The interface names are written by each interface.



Figure 1.3. NetWall 100 Series Interface Ports

The full connection capabilities of all the NetWall 100 Series Ethernet interfaces are listed at the end of *Appendix A, NetWall 100 Series Specifications*.

RJ45 Ethernet Interface Status LEDs

The status lights on the sides of the NetWall 100 Series RJ45 Ethernet interface sockets indicate the following states for each interface:

- **Left LED:**
 - i. **Solid Green** - The interface has power.
 - ii. **Flashing Green** - The interface is active.
- **Right LED:**
 - i. **Dark** - 10 Mbit link or no link.
 - ii. **Green** - 100 Mbit link.
 - iii. **Yellow** - 1000 Mbit link.

1.3. Status Lights

The NetWall 100 Series features a set of status lights on the opposite side to the Ethernet ports.



Figure 1.4. NetWall 100 Series Status Panel View

These LEDs indicate the overall system status, as well as the status of the Ethernet interfaces.

The two status LEDs on the left side indicate overall 100 Series status:

- **Upper Green LED** - This shows power is supplied to the unit.
- **Lower Blue LED** - cOS Core has started and is running.

The three rows of twin LEDs marked **WAN1**, **WAN2**, **LAN1** and **LAN2** mirror the status lights located on the sides of the RJ45 interface ports and indicate the following states:

- **Upper LED:**
 - i. **Solid Green** - The interface has power.
 - ii. **Flashing Green** - The interface is active.
- **Lower LED:**
 - i. **Green** - 100 Mbit link.
 - ii. **Yellow** - 1000 Mbit link.
 - iii. **Dark** - 10 Mbit link or no link.

1.4. Zero Touch Support

The NetWall 100 Series product is able to support the *Zero Touch* feature in the Clavister InControl management software product. This means that it is possible to power up a brand new NetWall 100 Series, connect it to the Internet, and the NetWall 100 Series device will automatically register itself with an InControl server. The device can then be remotely brought under centralized InControl management and configured remotely, without any local configuration needing to be done.

However, this feature will only work if the following prerequisites are true:

- The version of InControl being used for device management is 2.00.00 or later.
- The FQDN or IP address of the management InControl server has been set in the *MyClavister* account associated with the NetWall 100 Series device. This is done by logging in to the relevant *MyClavister* account, selecting *Settings* and then selecting the *Zero Touch* tab. Only one InControl server address can be associated with one *MyClavister* account.
- The zero touch feature has been enabled for the license associated with the NetWall 100 Series device. This in the *MyClavister* account by selecting *Licenses* and then enabling the *Zero Touch* button next to the relevant license. If the zero touch button is grayed out then the feature is not available with that device. There is an option in the previous step to always enable zero touch by default for all new licenses.
- The version of cOS Core running on the NetWall 100 Series must be 12.00.16 or later. This might require an upgrade of the factory installed cOS Core version.
- The cOS Core configuration is in its "factory default" state. Following an upgrade to a version that supports zero touch or any configuration change, this will require a manual reset to the default cOS Core configuration. In the Web Interface this is done by going to:

Status > Maintenance > Reset & Restart

And then selecting the following option:

Reset the configuration to current core default

Note that a full hardware reset to factory defaults will undo any cOS Core version upgrade and this should therefore not be done. Also note that any configuration change that is saved after a reset to the default configuration will disable the zero touch feature.

- The NetWall 100 Series can be connected to an ISP or other network that can provide Internet access and that has a DHCP server enabled which can provide a public DNS server address to the device. Note that physical connection to the Internet should be performed only after the device is running a zero touch supporting version of cOS Core with the factory default configuration.
- Access is not blocked by surrounding network equipment for TCP traffic on port 998. This traffic is required for the NetWall 100 Series to communicate with the InControl server. DNS traffic between the NetWall 100 Series and public DNS servers must also not be blocked.

Internet Connection Must Use a Specific Interface for Zero Touch

When the NetWall 100 Series is running a version of cOS Core that supports the zero touch feature, the initial connection to the Internet for InControl management must be made via the **WAN1** interface for the feature to function.

Zero Touch Can Also Simplify Hardware Replacement

In addition to simplifying the addition of a new NetWall 100 Series, the zero touch feature can also simplify hardware replacement of a NetWall 100 Series with another NetWall 100 Series. When the replacement hardware is connected to the Internet, InControl can automatically install the correct license as well as the correct cOS Core version. In addition, InControl will upload its copy of the cOS Core configuration from the old hardware.

A complete description of the zero touch feature and how it functions can be found in the separate *InControl Administration Guide* in the chapter titled *Zero Touch*.

1.5. Hardware Sensor Monitoring

The NetWall 100 Series 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 NetWall 100 Series 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 100 Series 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 a NetWall 100 Series 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 4.2, "Web Interface and Wizard Setup"*.
- ii. **Manual registration of the NetWall 100 Series on the Clavister website** - This is described in the last half of this chapter. Manual registration may be necessary if the appliance does not have Internet access.

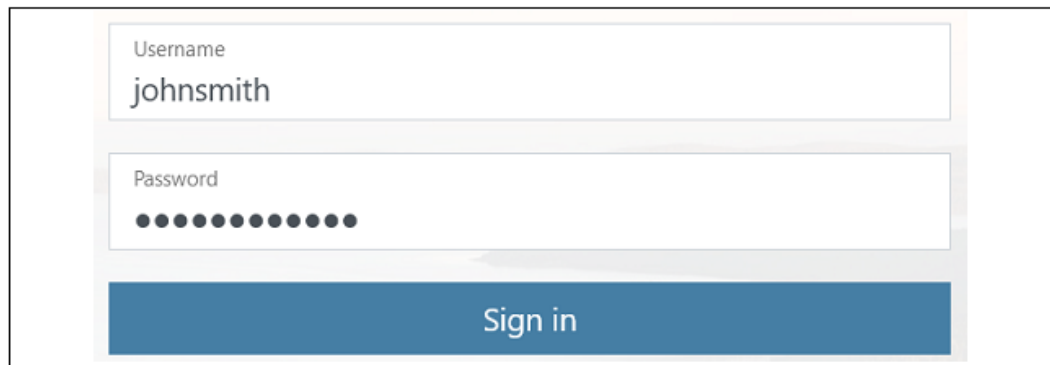
A. Registering as a Clavister Customer

The NetWall 100 Series registration steps for a first time user of Clavister hardware are as follows:

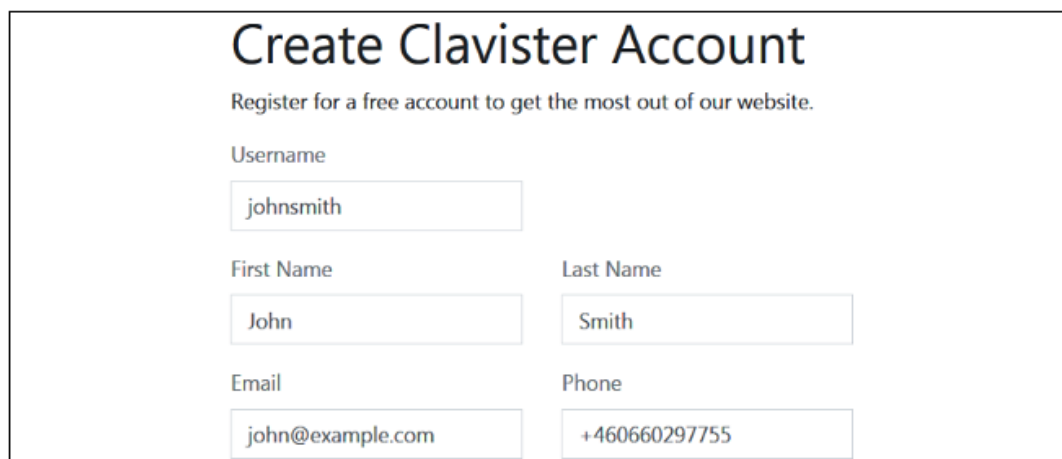
1. Open a web browser, go to **<https://www.clavister.com>** and select the **MyClavister** link.



- 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.

A login form with two input fields. The first field is labeled 'Username' and contains the text 'johnsmith'. The second field is labeled 'Password' and contains ten black dots. Below the fields is a blue button with the text 'Sign in'.

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

A registration form titled 'Create Clavister Account' with the subtitle 'Register for a free account to get the most out of our website.' The form contains five input fields: 'Username' (johnsmith), 'First Name' (John), 'Last Name' (Smith), 'Email' (john@example.com), and 'Phone' (+460660297755).

- 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.

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

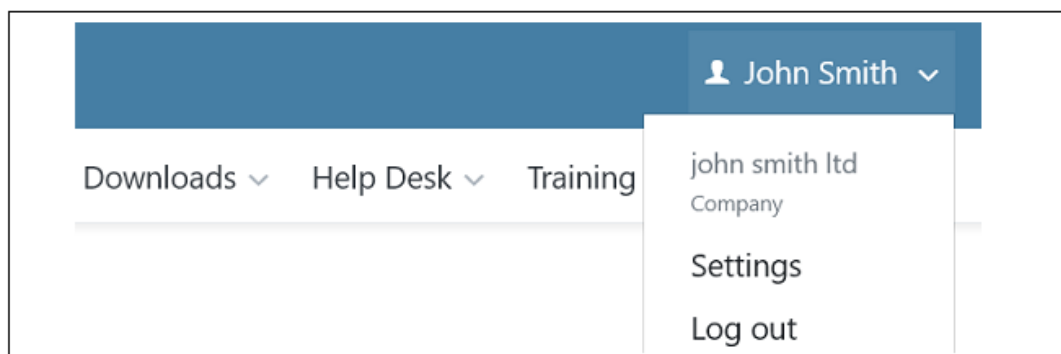
Welcome to Clavister!

John Smith, thank you for registering a user account with us. To complete the registration process, please follow the link below. Once your account has been activated, you can explore our site and download articles, white papers, subscribe to our newsletter and much more.

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.

Your account has successfully been verified and you can now  log in below.

7. After logging in, the customer name is displayed with menu options for changing settings and logging out. Note also that multi-factor authentication can be enabled for increased security in *Settings*.

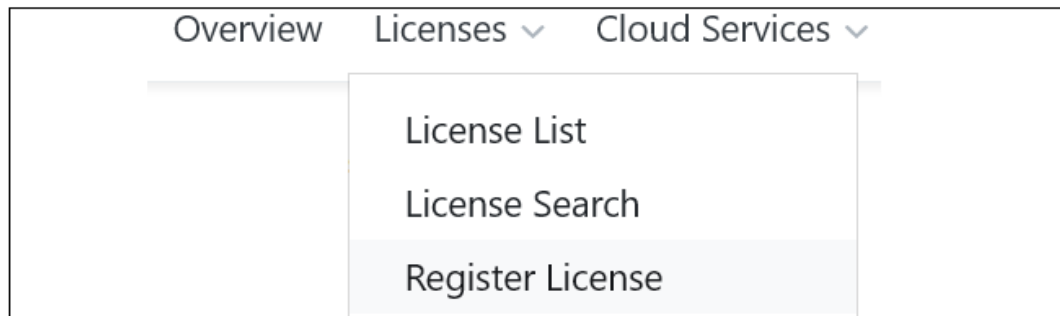


B. Registration of the NetWall 100 Series

This section can be skipped if the NetWall 100 Series unit 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 4.2, "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:

8. Now, log into the *MyClavister* website and select the **Register License** menu option.



9. Select the **NetWall** option.



10. The registration fields will be displayed. After selecting the product type, enter the *Hardware Serial Number* and *Service Tag*. **These two codes are found on a label which should be attached to the NetWall 100 Series hardware itself.** The label is usually found on the hardware unit's underside but may be found in another position.

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



After Successful Hardware Registration

Once the NetWall 100 Series 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 4.2, "Web Interface and Wizard Setup"*.

If the NetWall 100 Series 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 4.5, "License Installation"*.

Chapter 3: Installation

- General Installation Guidelines, page 22
- Flat Surface Installation, page 24
- Management Computer Connection, page 25
- Local Console Port Connection, page 28
- Connecting Power, page 30

3.1. General Installation Guidelines

Follow these general guidelines when installing the NetWall 100 Series appliance:

- **Safety**

Take notice of the safety guidelines laid out in *Chapter 7, 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 100 Series are listed in *Appendix A, NetWall 100 Series 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 3.5, "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, NetWall 100 Series 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, NetWall 100 Series Specifications**.*

3.2. Flat Surface Installation

The NetWall 100 Series 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 100 Series can also be wall mounted by sliding the two brackets on the underside of the unit onto suitably located mounting screws.



Important: Always leave space around the appliance

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

The NetWall 100 Series is not designed to be rack mounted.

3.3. Management Computer Connection

cOS Core Starts After Power Up

It is assumed that the NetWall 100 Series 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 software is preloaded on the NetWall 100 Series 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 for configuration using the cOS Core WebUI.

The Default Management Ethernet Interface

After first-time startup, cOS Core automatically makes management access available on a single predefined Ethernet interface and assigns to it the private IPv4 address **192.168.1.1** and network **192.168.1.0/24**. In addition, this interface has a DHCP server enabled. This means that any DHCP client that connects can be automatically assigned a private IPv4 address so it can communicate with the firewall.

For the NetWall 100 Series, the default management interface is **LAN1**.

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 4.2, "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 manual configuration steps using the CLI are described in *Section 4.4, "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 is possible using console emulation software running on an external computer connected directly to the RJ45 local console port on the 100 Series hardware.

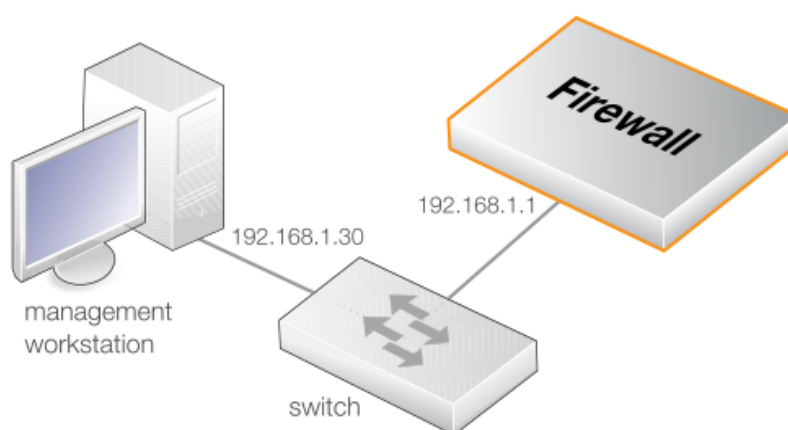
Direct console connection is described in *Section 3.4, "Local Console Port Connection"*.

In the default NetWall 100 Series configuration, login credentials are enabled for the local console. These are a username of **admin** and a password of **admin**. These credentials come from the predefined *admin* user, which is also used for SSH and Web Interface access.

Connection to an External Management Computer

For system management using the Web Interface or the CLI via SSH, the firewall's **LAN1** Ethernet interface must be connected, across a network or directly, to an Ethernet interface on an external management computer.

This connection could be made via a local switch using standard Ethernet cables, as shown in the illustration below.



Alternatively, direct local Ethernet connection to the **LAN1** interface could be done without a switch by using a crossover cable. However, all the RJ45 interfaces on the NetWall 100 Series support *Automatic MDI-X* so a crossover cable is not necessary.

Connection to an ISP for Internet Access

For access to the public Internet, another 100 Series Ethernet interface should be selected for connection to an ISP. In this guide, it will be assumed that the interface **WAN1** will be used for connection to the Internet, although another available interface could be used instead. In the cOS Core setup wizard, this interface used is always generically referred to as the WAN interface. cOS Core setup for Internet access is discussed further in *Chapter 4, cOS Core Configuration*.

Note that in the default cOS Core configuration for the NetWall 100 Series, this interface already has a DHCP client enabled so it can automatically receive an IP addresses from an ISP.



Tip: Connect the Internet before the management computer

*If the **WAN1** interface is connected to an ISP before the management computer is connected to the **LAN1** interface, DNS addresses for resolving URLs will be received from the ISP and then relayed in the DHCP lease sent to a connecting management computer.*

If the management computer is connected first, it may get its IP assigned by the firewall with a DHCP lease that will not contain DNS addresses and the lease lifetime will be 24

*hours. Renewing the lease, for example with a management computer restart, may be necessary to get DNS addresses after they are received on the **WAN1** interface. Alternatively, DNS addresses could be entered into the management computer manually.*

Management Computer Ethernet Interface Setup

The only requirement for the Ethernet interface used for connection on the management computer is that DHCP is enabled. cOS Core automatically enables a DHCP server on the firewall's **LAN1** interface and this will allocate the relevant IP address to the management computer using DHCP.

If the management computer is configured manually, the following settings should be used:

- **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.*

3.4. Local Console Port Connection



Tip: 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 NetWall 100 Series unit from an external computer acting as a console terminal. This 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 firmware loader options. The boot menu is described further in the separate *cOS Core Administration Guide*.

The *local console port* is the physical RJ45 RS-232 port on the far right-hand side of the NetWall 100 Series's front panel.

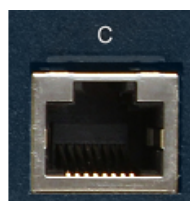


Figure 3.1. The NetWall 100 Series Local Console Port

Requirements for NetWall 100 Series Local Console Connection

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

- An external 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. 115,200 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 100 Series.

3. Connect the other end of the cable to a console terminal or to the serial connector of a computer running console emulation software.

The Default Local Console Login Credentials

The console user credentials for logging in are specified by the predefined *admin* user and are the same as the credentials for initial network access via the management Ethernet interface:

- **Username:** *admin*
- **Password:** *admin*

It is recommended to change the password for this user during initial cOS Core configuration.

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 3.3, "Management Computer Connection"*.

3.5. Connecting Power

This section describes connecting power. As soon as power is applied, the NetWall 100 Series will boot-up and cOS Core will start.



Important: Review the safety information

*Before connecting power, please review the electrical safety information found in **Chapter 7, Safety Precautions**.*

Connecting AC Power

To connect power, follow these steps:

1. Connect the end of the power adapter's power cord to the power inlet on the NetWall 100 Series. The 100 Series has a threaded connector which must be screwed firmly in place to prevent the power cable accidentally detaching.



Figure 3.2. NetWall 100 Series Power Inlet Connector

2. Plug the power adapter into a suitable AC power outlet. There is no On/Off switch so the unit will boot up as soon as power is applied.
3. The NetWall 100 Series 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.
4. After a brief period of time, cOS Core will be fully initialized and the NetWall 100 Series is then ready for configuration using a direct console connection or via a network connection to the default management Ethernet interface.

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



Important: Protecting against power surges

It is recommended to consider the purchase and use of a separate surge protection unit from a third party for the power connection to the NetWall 100 Series hardware. This is to ensure that the appliance 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

- The NetWall 100 Series Default Configuration, page 32
- Web Interface and Wizard Setup, page 34
- Manual Web Interface Setup, page 43
- Manual CLI Setup, page 58
- License Installation, page 67
- Setup Troubleshooting , page 70



Tip: Upgrade to the latest cOS Core version

*A new NetWall 100 Series unit may not have the very latest cOS Core version pre-installed. After the initial configuration described in this section, 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. The NetWall 100 Series Default Configuration

This section describes the predefined entries in the default cOS Core configuration that are unique to the NetWall 100 Series.

Ethernet Interface DHCP settings

The NetWall 100 Series appliance comes with a default cOS Core configuration with the following settings on the Ethernet interfaces:

- The *LAN1* interface has a DHCP server enabled. This means connecting clients will be automatically allocated an IP address by cOS Core, providing the client has DHCP enabled on its connecting interface. Clients will also be allocated DNS server addresses if cOS Core itself has received them from an ISP.
- The *WAN1* and *WAN2* interfaces both have a DHCP client enabled. This means they can be automatically assigned an IP address if either is connected to an ISP. DNS server addresses can also be received by cOS Core.

Zone Groupings

The Ethernet interfaces are also grouped together into a *Zone* in the cOS Core configuration in the following way:

- The interfaces *LAN1* and *LAN2* belong to a predefined *Zone* object called *LANZone*.
- The interfaces *WAN1* and *WAN2* belong to a predefined *Zone* object called *WANZone*.

The Predefined IP Rule Set

The default configuration also contains IP rule set entries that allow traffic to flow from the *LAN1* interface and its network to the *WANZone* interfaces. This means that web surfing clients on *LAN1* will have predefined access to the Internet through *WAN1*, or alternatively *WAN2* if *WAN1* is not available.

The Predefined *all-nets* Routes

There is a predefined *all-nets* route for both the *WAN1* and *WAN2* interfaces. The *WAN1* route has a lower value for its *Metric* property which means it will have precedence over *WAN2* for Internet traffic if both are connected to an ISP. However, should *WAN1* become unavailable, cOS Core will automatically route traffic through *WAN2*, providing redundancy.

Changing the Default Configuration

Note that there are no restrictions on how cOS Core is configured in the NetWall 100 Series product or how the Ethernet interfaces are used. The administrator is free to change or delete any of the default configuration components.

4.2. 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 3.3, "Management Computer Connection"*.

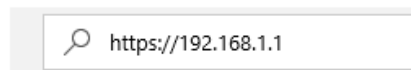


Note: Some screenshots have been rearranged

Some of the screenshot images in this section have been rearranged to fit this document's page size. 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

HTTP management access is disabled in the default cOS Core configuration and HTTPS must be used. Unencrypted HTTP access 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 4.6, "Setup Troubleshooting"*.

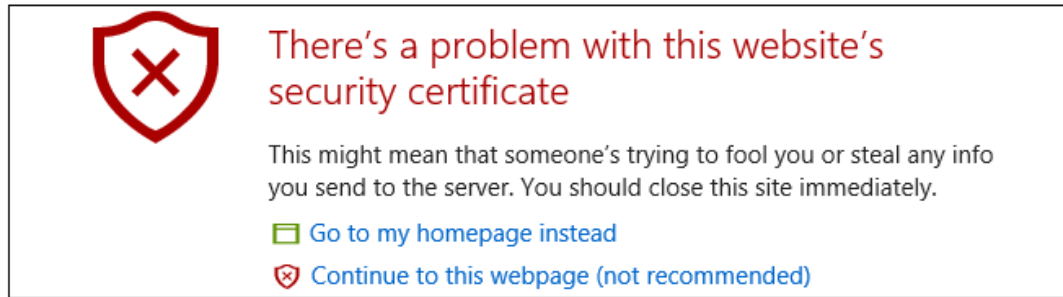


Important: Do not access cOS Core via a proxy server

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.

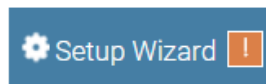
The available Web Interface language options are selectable at the bottom of this dialog. This defaults to the language set for the browser if cOS Core supports that language.

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.

DHCP on the LAN1, WAN1 and WAN2 Interfaces is Already Enabled

It should be noted that the following will already be configured:

- The **LAN1** interface has a DHCP server enabled so a management computer or clients on the connected network will get IPs automatically assigned to them.
- The **WAN1** and **WAN2** interfaces have a DHCP client enabled and will automatically be assigned an IP address when connected to an ISP.

Note that **WAN1** or **WAN2** connection should ideally be done before **LAN1** so the DNS addresses received from an ISP can propagate to clients on the **LAN1** network.

- A small predefined IP rule set automatically allows web surfing by clients on the **LAN1** interface via the **WAN1** or **WAN2** interfaces. This rule set is discussed further in *Section 4.1, "The NetWall 100 Series Default Configuration"*. interface.

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. The *admin* username can also be changed if required, as shown in the screenshot below.

The *Enforce Strong Passwords* option is present in cOS Core versions from 11.05 onwards. 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. However, it is recommended to leave this option enabled, which means that the default *admin* password 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

TIMEZONE SETTINGS

Location

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
Please select the interfaces to enable Transparent Mode on, from the list of available interfaces.

Available	Selected
<div>LAN1</div> <div>LAN2</div> <div>WAN1</div> <div>WAN2</div>	

+ Include x 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 which interface that will be used to connect to an ISP for Internet access.

WAN INTERFACE SETTINGS

Select the interface that is connected to the Internet.

Interface: WAN1

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 100 Series 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 100 Series 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.

4.3. 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 serve 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 Ethernet interfaces are logically equal for cOS Core and, although their physical capabilities may be different, any interface can perform any logical function.

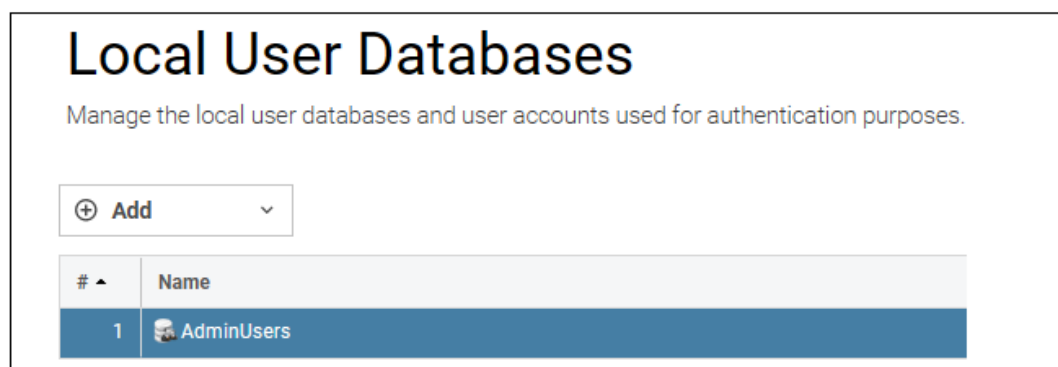
The NetWall 100 Series uses the **LAN1** interface as its default management interface. To describe manual Internet setup, it is assumed here that the **LAN2** interface will be used for connection to a protected internal client network and the **WAN2** interface will be used for connection to the public Internet.

As mentioned earlier, the **LAN1** and **WAN1** interfaces could be used to connect automatically to clients and the Internet because they already have DHCP enabled in the default configuration and there are predefined entries in the IP rule set that allow clients to browse the Internet. The default configuration is discussed further in *Section 4.1, "The NetWall 100 Series Default Configuration"*. However, the purpose of this section is to show how manual setup can be done.

The **WAN2** interface also has a DHCP client enabled on it in the default configuration so it is assumed that this client will be disabled for manual setup.

Changing the *admin* Password

It is **strongly** recommended to change the password of the *admin* user as the first task in manual cOS Core setup. This is done by first selecting the **System** option from the Web Interface toolbar and then **Local User Databases** from the navigation pane to display the local user database list, as shown below.



Next, select *AdminUsers* and then the **Users** tab to display the contents of this predefined database

General		Users	
<div> <div>⊕ Add</div> <div>▼</div> </div>			
Name ▲	Groups	Static Client IP Address	Networks Bel
admin	administrators, auditors		
audit	auditors		

Select the default user *Admin* to open a dialog to change its password.

Name:	<input type="text" value="admin"/>
Password:	<input type="password" value="••••••••"/>
Confirm Password:	<input type="password" value="••••••••"/>

By default, using a strong *admin* password will be enforced meaning that the new password must comply with a set of strong password conventions. Activating configuration changes will not be possible while the password is weak. The only way around this is to first turn off the strong password policy in the configuration, but this is not recommended.

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.

<input type="text" value="2017-06-12"/>	<input type="text" value="14:05:10"/>	<input type="button" value="Set"/>	<input type="button" value="Synchronize"/>
---	---------------------------------------	------------------------------------	--

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

Location:	<input type="text" value="ClavisterHQ"/>
-----------	--

Alternatively, the **Synchronize** button can be pressed to get the current date and time from external **Network Time Protocol** (NTP) servers. Clavister's own NTP server is also an option. Using NTP servers will require Internet access.

An example of configuring a custom NTP server configuration is shown below.

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

Primary Time Server:



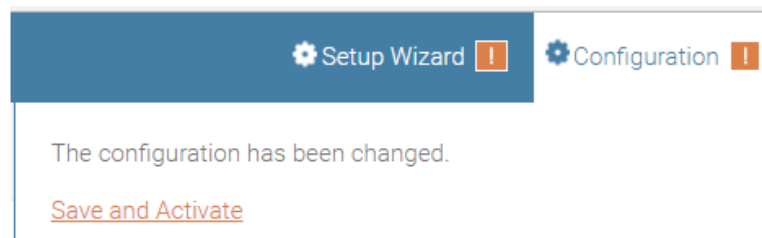
Note: Use an FQDN address for a time server

An **FQDN Address** object must be used when specifying a time server address. See the relevant cOS Core Administration Guide section for more explanation.

Once the values are set correctly, press the **OK** button to save the values temporarily. Configuration changes will not become active until the new configuration becomes the current and active configuration. Doing this is discussed 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.

Save Configuration

Save and activate changes made to the configuration file.

SAVE AND ACTIVATE

Are you sure you want to save the configuration?

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

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

The changes have been saved, and the unit is now activating the new configuration.

You must reconnect to it within 30 seconds for the configuration changes to be finalized. If this fails, the unit will revert to its previous configuration.

This page will automatically refresh in 9 seconds in an attempt to do this automatically.

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 a new configuration does not accidentally lock out the administrator. After reconfiguration and reconnection, a success message will be displayed.

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 firewall should rarely be lost.



Tip: How frequently to commit configuration changes

It is up to the administrator how many changes to make before activating a new configuration. Activating changes in small batches can be the best approach 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 the pending changes 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 pending changes are lost.

Setting Up Internet Access

Setting up public Internet access manually using the Web Interface will now be described. There are four options which are listed below.

A. Static - manual configuration.

B. DHCP - automatic configuration.

C. PPPoE setup

D. PPTP setup

The steps to configure these Internet connection alternatives with the Web Interface are discussed next.

Note that on the NetWall 100 Series, a DHCP client is enabled in the default configuration on the **WAN1** and **WAN2** interfaces so that usually method **B** is used. The other methods are included here in case they are needed.

A. Static - manual configuration

Manual configuration means that there will be a direct connection to the ISP and all relevant IP addresses for the connecting interface are fixed values that will be 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 Ethernet interface that will connect to the ISP. In this case, **WAN2**.*

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 WAN2 and that the static public 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 NetWall 100 Series.

#	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.*

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.

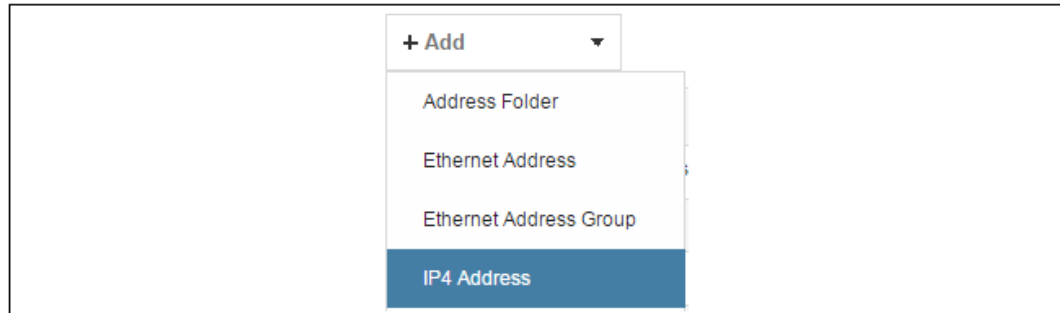
On initial startup, two IPv4 address objects are created automatically for each Ethernet interface detected by cOS Core. One IPv4 address object is named by combining the physical interface name with the suffix "_ip" and this is used for the IPv4 address assigned to that interface. The other address 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 *WAN2_ip* to be *203.0.113.35*. This is the IPv4 address of the *WAN2* interface which will connect to the ISP's gateway.

Lastly, set the *IP4 Address* object *WAN2_net* to be *203.0.113.0/24*. Both the address objects 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 Ethernet interface connected to the Internet which, in this example, is Select **Network > Interfaces and VPN > Ethernet** to display a list of the physical interfaces and address book objects assigned to them.

# ▲	Name	IPv4 Address	IPv4 Network	IPv4 Gateway	IPv6 Address	IPv6
1	WAN1	ip_WAN1	WAN1net			
2	WAN2	ip_WAN2	WAN2net			
3	LAN1	ip_LAN1	LAN1net			
4	LAN2	ip_LAN2	LAN2net			

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:	WAN2_ip
Network:	WAN2_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 exist that will allow traffic from clients to the Internet.

Note that with the NetWall 100 Series, the main IP rule set will already contain a number of predefined entries in the default configuration that will allow clients on the **LAN1** interface to access the Internet via the **WAN1** or WAN2 interfaces. This is discussed in more detail in *Section 4.1, "The NetWall 100 Series Default Configuration"*.

This section will discuss how IP rule set entries could be manually created to allow Internet access for clients on LAN2 via interface WAN2.

To add an IP policy, go to **Policies > Firewalling > Main IP Rules**. The *main* IP rule set will now be displayed. 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 web browsing (it allows HTTP and HTTPS connections).

Name:	<input type="text" value="lan_to_wan"/>		
Action:	<input type="button" value="ALLOW"/>		
	Interface	Network	Geolocation
Source:	<input type="text" value="LAN2"/>	<input type="text" value="LAN2_net"/>	<input type="text" value="(Anywhere)"/>
Destination:	<input type="text" value="WAN2"/>	<input type="text" value="all-nets"/>	<input type="text" value="(Anywhere)"/>
Service:	<input type="text" value="http-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 the 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:	<input type="text" value="NAT"/>
Address Action:	<input type="text" value="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 URIs 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. However, the recommended method is to create an entirely new IP set entry that specifies the service as *dns-all*. This provides more clarity when the configuration is examined for problems. The screenshot below shows a new IP policy called *lan_to_wan_dns* being created to allow DNS.

Name:

Action: ALLOW

	Interface	Network	Geolocation
Source:	LAN2	LAN2_net	(Anywhere)
Destination:	WAN2	all-nets	(Anywhere)

Service: 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 web browsing traffic should leave the firewall. This route defines 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	WAN2	all-nets	wan_gw		100	No	

This *all-nets* route is added automatically when the *Default Gateway* for an Ethernet interface is specified, as was done earlier when setting up the required *IP4 Address* objects.



Note: Disabling automatic route generation

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

As part of the setup, it is also recommended that at least one DNS server is also defined in cOS Core. A DNS server or servers (a maximum of three can be configured) will be used when cOS Core itself needs to resolve URIs, such as with FQDN address objects. It can also be 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.

DNS

Configure the DNS (Domain Name System) client settings.

General
Advanced

Primary Server: wan_dns1

B. DHCP - automatic configuration

All the required IP addresses for Internet connection can, alternatively, be automatically retrieved from an ISP's DHCP server by enabling the **DHCP Client** option for the interface connected to the ISP.

Note that on the NetWall 100 Series, a DHCP client is enabled in the default cOS Core configuration on the *WAN1* and *WAN2* interfaces. Enabling DHCP is described here in case it needs to be manually enabled.

A DHCP client is enabled by first selecting **Network > Interfaces and VPN > Ethernet** to display a list of all the interfaces.

Click the *LAN2* interface in the list to display its properties and select the option to enable the interface as a DHCP client.



IP address: WAN2_ip

Network: WAN2_net

Default Gateway: wan_gw

Receive Multicast Traffic: Auto

Enable DHCP Client: ☒

Usually, a DHCP *Host Name* does not need to be specified but can sometimes be needed by an ISP to uniquely identify the firewall as a particular DHCP client for 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 and source interface to flow to the destination network *all-nets* and the destination interface.

C. PPPoE setup

For PPPoE connection, we must create a PPPoE tunnel interface associated with an Ethernet interface. Assume that the Ethernet interface is *WAN2* 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:	WAN2
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 an IP rule set entry that will allow traffic from the source network and source interface 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




Your ISP will supply the correct values for *pptp_username*, *pptp_password* and the remote endpoint. An Ethernet 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 an Ethernet interface by the

entries 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. 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 *LAN2_net* and interface *LAN2*) to flow to the destination network *all-nets* and the destination interface, which is the PPTP tunnel.

DHCP Server Setup

If a NetWall 100 Series interface is to have a DHCP server enabled on it, 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.

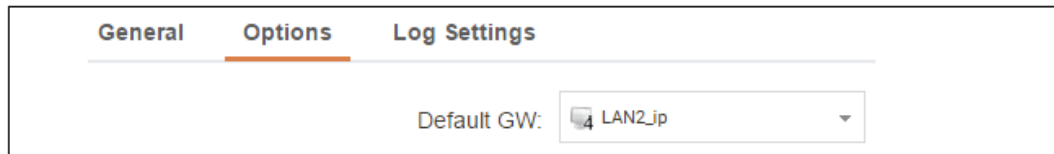
We now create a DHCP server object called *my_dhcp_server* which will only be available on the *LAN2* interface. Note that the NetWall 100 already has a DHCP server predefined on the *LAN1* interface in the default configuration but *LAN2* does not. To do this, go to **Network > Network Services > DHCP Servers** and select **Add > DHCP Server**. The server properties can now be specified.

Name:	my_dhcp_server
Interface Filter:	 LAN2 ▾
Relay Filter:	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, *LAN2_ip*.

To set the default gateway, select the **Options** tab.



General Options Log Settings

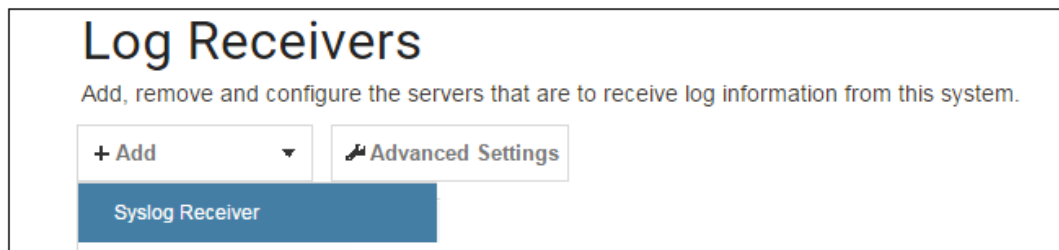
Default GW: LAN2_ip

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*.

External Syslog Server Setup

By default, only cOS Core's internal *memlog* feature will capture generated log messages. To send logs to an external Syslog server, a log receiver object must be configured.

To send logs to Syslog server, first create an *IP4 Address* object called, for example, *syslog_ip* which is set to the IPv4 address of the server. Next, select **System > Device > Log and Event Receivers** and choose **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 appear. Specify a name, for example *my_syslog*, and specify the 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 to send ping messages to any hosts on the Internet, select **Policies > Firewalling > Main IP Rules > Add** and enter the values shown below for the 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		Geolocation		
Source:	LAN2	LAN2_net		(Anywhere)		
Destination:	WAN2	all-nets		(Anywhere)		
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 firewall with the IP address of the interface connected to the ISP as the source. Responding hosts will send back ICMP responses to this address and cOS Core will then forward the traffic to the correct private IPv4 address.

Adding a "Drop All" Policy is Recommended

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

In order to gain more control over dropped traffic and its logging, it is recommended to create an explicit "drop all" IP policy as the **last** entry in the *main* IP rule set. This policy has both the source and destination network set to *all-nets* and both the source and destination interface set to *any*. The service would be set to *all_services* in order to trigger on all traffic types, as shown in the example below.

Name:	drop_all					
Action:	<input type="checkbox"/> <input checked="" type="checkbox"/> DENY					
Deny Behavior:	<input type="checkbox"/> <input checked="" type="checkbox"/> DROP					
	Interface	Network		Geolocation		
Source:	any	all-nets		(Anywhere)		
Destination:	any	all-nets		(Anywhere)		
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:	<input checked="" type="checkbox"/> ON <input type="checkbox"/>	Warning
----------	---	---------

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 4.5, "License Installation"*.

4.4. 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 the Local Console**

An external computer running a console emulator can be physically connected directly to the local console port on the NetWall 100 Series.

- **Using a Network Connection**

An SSH client on an external computer can be used to connect across a network 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 3.3, "Management Computer Connection"* and is the same as that used in *Section 4.2, "Web Interface and Wizard Setup"*.

If there is a problem with the management computer connection, a help checklist can be found in *Section 4.6, "Setup Troubleshooting"*.

Note that the setup steps listed in this section are grouped so that they closely follow the order of the options 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 *admin* Account Password

It is **strongly** recommended to change the password of the *admin* user as the first task in manual cOS Core setup. To do this, 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: Tab completion makes CLI usage easier

The tab key can be pressed at any time so that cOS Core either completes a command portion or provides a list of possible command options.

Now set a new password for the administrator which is difficult to guess. For example:

```
Device:/AdminUsers> set User admin Password=Mynew*pass99
```

The next step is to return the CLI to the default CLI context:

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

By default, using a strong *admin* account password will be enforced meaning that the new password must comply with a set of strong password conventions. Activating configuration changes will not be possible while the password does not comply. The only way around this is to first turn off the strong password policy in the configuration but this is not recommended.

Setting the Date and Time

Many cOS Core functions, such as event logging and certificate handling, rely on an accurate system time. It can be set manually using the *time* command. A typical example might be:

```
Device:/> time -set 2021-03-24 14:43:00
```

Note that the date is entered in *yyyy-mm-dd* format and the time is stated in 24 hour *hh:mm:ss* format. Automatically setting the time with a time server is discussed at the end of this section.

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 100 Series, the **LAN1** interface is the default management interface. To illustrate manual Internet setup, it is assumed here that the **LAN2** interface will also be used for connection to a protected internal client network and the **WAN2** interface will be used for connection to the public Internet.

As mentioned earlier, the **LAN1** and **WAN1** interfaces could be used to connect automatically to clients and the Internet because they already have DHCP enabled and there are predefined entries in the IP rule set that allow clients to browse the Internet. The default configuration is discussed further in *Section 4.1, "The NetWall 100 Series Default Configuration"*. However, the purpose of this section is to show how manual setup can be done.

Setting Up Internet Access

Setting up public Internet access manually using the CLI will now be described. There are four options which are listed below.

A. Static - manual configuration.

B. DHCP - automatic configuration.

C. PPPoE setup.

D. PPTP setup.

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

Note that on the NetWall 100 Series, a DHCP client is enabled by default on the **WAN1** interface so that usually method **B** is used. The other methods are included here in case they are needed.

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 WAN2, 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 WAN2 interface which is connected to the ISP: Next, set the IP address of the WAN2_ip address object which is the IP assigned to the interface:

```
Device:/> set Address IP4Address InterfaceAddresses/WAN2_ip  
Address=203.0.113.35
```



Note: Qualifying the names of IP objects in folders

On initial startup of the 100 Series, 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 **WAN2_ip**, it must be qualified with the folder name **InterfaceAddresses** so it becomes **InterfaceAddresses/WAN2_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 WAN2_net which will be the IPv4 network of the connecting interface:

```
Device:/> set Address IP4Address InterfaceAddresses/WAN2_net  
Address=203.0.113.0/24
```

In the default configuration of the NetWall 100 Series, a DHCP client is automatically enabled on the WAN2 interface, so this must be disabled for a manual setup:

```
Device:/> set Interface Ethernet WAN2 DHCPEnabled=No
```

Before continuing, it is recommended to verify the properties of the WAN2 interface using the following command:

```
Device:/> show Interface Ethernet WAN2
```

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

Property	Value
-----	-----
Name:	WAN2
IP:	InterfaceAddresses/WAN2_ip

```

        Network:      InterfaceAddresses/WAN2_net
    DefaultGateway:   wan_gw
        Broadcast:    203.0.113.255
        PrivateIP:    <empty>
            NOCHB:    <empty>
            MTU:      1500
            Metric:   100
        DHCPEnabled:  No
        EthernetDevice: 0:WAN2 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 existence of an *IP Policy* which explicitly allows traffic to flow. Let us assume we want to allow web browsing from the protected network *LAN2_net* which is connected to the interface *LAN2*.

Note that with the NetWall 100 Series, the main IP rule set will already contain a number of predefined entries that will allow clients on the **LAN1** interface to access the Internet via the **WAN1** or **WAN2** interfaces. This is discussed in detail in *Section 4.1, "The NetWall 100 Series Default Configuration"*.

This section will discuss how IP rule set entries could be manually created to allow Internet access for clients on *LAN2* via interface *WAN2*.

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=LAN2
           SourceNetwork=InterfaceAddresses/LAN2_net
           DestinationInterface=WAN2
           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 translation 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, NAT translation can be specified explicitly. For this, the previous IP policy definition with explicit NAT translation becomes the following:

```

Device:/> add IPPolicy Name=lan_to_wan
           SourceInterface=LAN2
           SourceNetwork=InterfaceAddresses/LAN2_net
           DestinationInterface=WAN2
           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 web browsing from the protected network but this does not include the DNS protocol to resolve URIs 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:/> add IPPolicy Name=lan_to_wan
           SourceInterface=LAN2
           SourceNetwork=InterfaceAddresses/LAN2_net
           DestinationInterface=WAN2
           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 URIs, which will be the case when an FQDN 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.

Note that the 100 Series, DHCP is already enabled on the **WAN1** interface by default. If DHCP needs to be enabled on any other interface then this can be done as shown in the example below.

If the interface on which DHCP is to be enabled is *WAN2* then the command to do this is:

```
Device:/> set Interface Ethernet WAN2 DHCPEnabled=Yes
```

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

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 until an IP rule set entry is defined that allows the flow. 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 *LAN2_net* and interface *LAN2*) to flow to the destination network *all-nets* and the destination interface *WAN2*.

C. PPPoE setup

For PPPoE connection, define a PPPoE tunnel interface on the interface connected to the ISP. The interface *WAN2* 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=WAN2
                Username=pppoe_username
                Password=pppoe_password
                Network=all-nets
```

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

The PPPoE tunnel interface can now be treated exactly like a physical interface by the policies defined in 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 the source network and source interface (in this example, the network *LAN2_net* and interface *LAN2*) to flow to the destination network *all-nets* and the destination interface, which is the PPPoE tunnel.

D. PPTP setup

For PPTP connection, first define the PPTP tunnel interface. The following command will create a PPTP tunnel object called *wan_pptp* with the remote endpoint *203.0.113.1*:

```
Device:/> add Interface L2TPClient wan_pptp
                Network=all-nets
                username=pptp_username
                Password=pptp_password
                RemoteEndpoint=203.0.113.1
                TunnelProtocol=PPTP
```

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

The PPTP client tunnel interface can now be treated exactly like an Ethernet 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 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 the source network and source interface (in this example, the network *LAN2_net* and interface

LAN2) to flow to the destination network *all-nets* and destination interface, which is the PPTP tunnel.

Activating and Committing Changes

After any changes are made to a cOS Core configuration, they will form a new configuration but will not yet be activated. To activate new configuration changes, the following command must be entered:

```
Device:/> activate
```

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

```
Device:/> commit
```

The reason for having a two command sequence is to prevent the new configuration accidentally locking out the administrator. If a lock-out occurs then the *commit* command cannot be received and cOS Core will automatically revert back to the original configuration after the 30 second time period (this time period is a setting that can be changed).

If the *admin* account password has not been changed earlier to a strong password and strong passwords are enabled (by default, they are) then activating configuration changes will not be allowed by cOS Core. The solution to this is either to change the *admin* account password to a strong one or turn off strong passwords with the following command:

```
Device:/> set Settings MiscSettings EnforceStrongPasswords=No
```

Note that if activation fails because of a weak password, the old *admin* password must be reset anyway, even if the new value is the same as the old.

DHCP Server Setup

Any interface on the NetWall 100 Series can be set up with a DHCP server so connecting clients can be automatically allocated an IP address from a predefined range.

By default on the NetWall 100 Series, the interface *LAN1* already has a DHCP server enabled on it which hands out addresses from the predefined address object *LAN_DHCPPool* (192.168.1.100-192.168.1.250). This means that clients connecting to the *LAN1* interface will automatically receive an IPv4 address from the pool. If a DHCP server were to be enabled manually, this can be done as shown in the example below where a DHCP server is enabled on the **LAN2** interface.

First, define an IPv4 address object which has the address range that can be handed out. In this example, we will use the IPv4 range 192.168.1.10 - 192.168.1.20 and this will be made available on the *LAN2* interface which is connected to the protected network *LAN2_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=LAN2
          Netmask=255.255.255.0
          DefaultGateway=InterfaceAddresses/LAN2_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, *LAN2_ip*.

NTP Server Setup

Network Time Protocol (NTP) servers can be configured to maintain the accuracy of the system date and time. By default, no time server is configured. Clavister provides its own time server which can be used with the following command:

```
Device:/> set DateTime TimeSynchronization=Clavister
```

Alternatively, a custom time server can be configured. 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 TimeSynchronization=Custom
           TimeSyncServer1=ts1_fqdn
           TimeSyncServer2=203.0.113.5
```

External Syslog Server Setup

By default, only cOS Core's internal *memlog* feature will capture generated log messages. To send logs to an external Syslog server, a log receiver object must be configured. For example, the following command will send logs to a Syslog server at the IP address *192.0.2.10*:

```
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 protected network. The command to define an IP policy called *allow_ping_outbound* to allow this traffic would be the following:

```
Device:/> add IPPolicy Name=allow_ping_outbound
           SourceInterface=LAN2
           SourceNetwork=InterfaceAddresses/LAN2_net
           DestinationInterface=WAN2
           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 to the Internet with the IP address of the firewall interface connected to the ISP. Responding hosts will send back ICMP responses to this single IP and cOS Core will then forward the traffic to the correct private IP address.

Adding a "Drop All" Policy is Recommended

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

In order to gain more control over dropped traffic and its logging, it is recommended to create an explicit "drop all" IP policy as the **last** entry in the *main* IP rule set. This policy has both the source and destination network set to *all-nets* and both the source and destination interface set to *any*. The service would be set to *all_services* in order to trigger on all traffic types.

The following command defines an explicit "drop all" policy with logging disabled:

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

A Valid License Should 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 4.5, "License Installation"*.

4.5. License Installation

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*.

The NetWall 100 Series Uses a SECaaS License

When cOS Core runs on the NetWall 100 Series hardware it requires a subscription based *Security as a Service* (SECaaS) license. The SECaaS license is managed in the same way as an older non-SECaaS license but requires the following to be configured in cOS Core:

- Internet Access.
- A public DNS server.

SECaaS licenses require periodic access to Clavister license servers to check validity and for automatic updates. If cOS Core cannot reach the license servers within a certain period of time then throughput is reduced to a maximum limit of 1 Mbps.

Installation Methods

The following methods can be used for installing the first cOS Core license in the 100 Series unit:

- **Automatically through the Setup Wizard**

As described in *Section 4.2, "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 100 Series hardware does not have a connection to the public Internet. The procedure consists of the following steps:

- i. 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.

- ii. Go to **Licenses > Register License**.
- iii. Select the option **Register by Service Tag and Hardware Serial Number**.
- iv. Enter the *Serial Number* and *Service Tag* codes. For Clavister hardware products, these codes are found on a label on the unit.
- v. Download a license from the license list to the computer's local disk.
- vi. 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 to 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 100 Series 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*.

4.6. 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
```

7. Check the management access rules for a network connection.

If connecting to the default management interface using the Web Interface or an SSH client, check that the management access rules are correctly configured to allow access through the interface and from the desired source IP range. These rules can be displayed with the CLI command:

```
Device:/> show RemoteManagement
```

Chapter 5: Resetting to Factory Defaults

In some circumstances, it may be necessary to reset the NetWall 100 Series appliance to the state it was in when it left the factory and before it 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.

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 NetWall 100 Series, 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 3.3, "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.

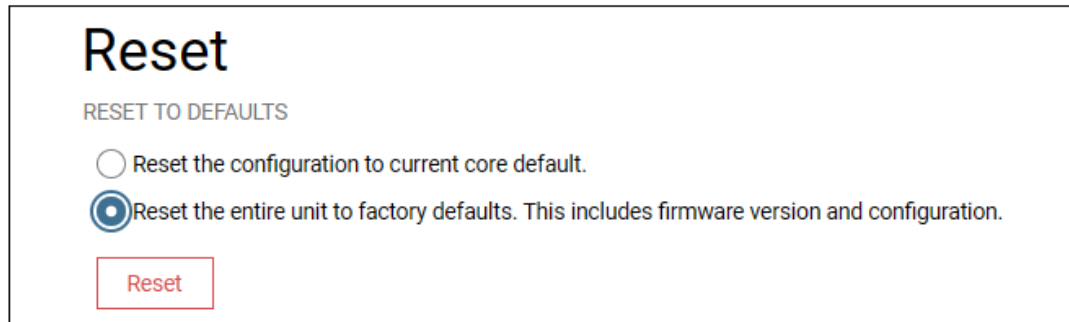


Figure 5.1. Factory Reset Using the Web Interface

- **Using the CLI**

The cOS Core CLI can be used by connecting to one of the NetWall 100 Series'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 repeatedly pressing the **Esc** key while cOS Core is starting up. The resetting of Ethernet interface IP addresses will not affect the local console connection. The complete procedure 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 NetWall 100 Series.
2. Power up the NetWall 100 Series unit. This may require a restart if the hardware is already powered up.
3. As console output appears, repeatedly press the **Esc** key before cOS Core has fully started.
4. The *boot menu* will now be displayed on the console.
5. Choose the **Reset system to factory default** option.



Caution: The local console credentials will be reset

The local console login credentials will be reset to the default values of username **admin** and password **admin**.

Chapter 6: Warranty Service

Limitation of Warranty

Clavister warrants to the customer of the 100 Series 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 **NetWall Hardware Replacement Guide** which is part of the cOS Core documentation set for each release.*

This guide also describes the 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.

Note that the procedures for swapping any NetWall hardware model with an identical or different model type are described in the separate *NetWall Hardware Replacement Guide*.

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 7: Safety Precautions

Safety Precautions

Clavister NetWall 100 Series 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: NetWall 100 Series Specifications



Dimensions and Weight

Height x Width x Depth (mm)	34 x 180 x 131
Hardware Unit Weight	0.63 kg
Packaged Weight	2.6 kg
Hardware Form Factor	Desktop / Wall mounted

Regulatory and Safety Standards

Safety	CE, UL
EMC	FCC, CE, VCCI

Environmental

Operating and Storage Humidity	0% to 95% (non-condensing)
Operating Temperature	5 to 35° C
Vibration/shock	10 ~ 500 Hz, 2G 10min/1 cycle, period for 60min, each along X, Y, Z

Power Specifications

Power Supply (AC)	100-240 VAC, 50-60 Hz, 0.6 A
Typical Power Consumption	12 W
PSU Rated Power	24 W

Ethernet Interface Support

Gigabit RJ45 interfaces	Automatic MDI-X 1000BASE-T (copper RJ45 100m) 100BASE-TX (copper RJ45 100m) 10BASE-T (copper RJ45 100m)
-------------------------	--

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



#NoBackDoors and Third-party Access Restriction

Clavister hereby certifies that Clavister products do not contain any “back-doors”, meaning that there are no mechanisms deliberately incorporated that would allow a company or an organization to access or control a Clavister product without prior acceptance from the administrator of the product in question.

John Vestberg, CEO, Clavister

www.clavister.com/SecurityBySweden

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