# Software Quick Start Guide

## 1 Install your stand-alone hardware in a suitable location.

The Clavister Security Gateway can run on non-Clavister stand-alone hardware.

Make sure that the hardware chosen meets the minimum hardware requirements specified at www.clavister.com.

The stand-alone hardware should be physically installed according to the manufacturer's recommendations.

## 2 Connect the hardware to the network

The stand-alone hardware needs to be connected to a network.

Make sure that one of the interfaces on the hardware is connected to a PC workstation that you will use to manage the Security Gateway from (this is the workstation which you will install Clavister FineTune on).

Note:
If you are not connecting the stand-alone hardware with the management PC to a Switch or a Hub in between then a crossover cable must be used.

## 3 Installing the Clavister FineTune management software

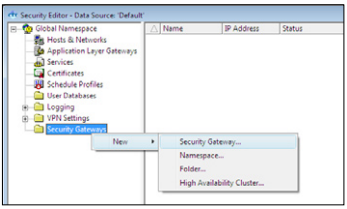
Install and start the Clavister FineTune management software.

Clavister FineTune should be installed on the Windows PC workstation that you connected to the stand-alone hardware in the previous step.

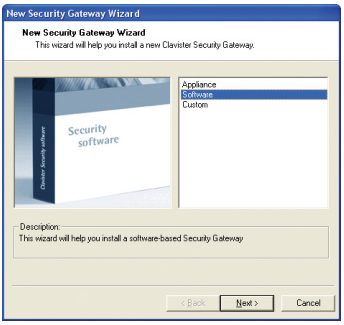
The Clavister FineTune installation package can be found on the Clavister Software CD-ROM.

## 4 Run the New Security Gateway Wizard

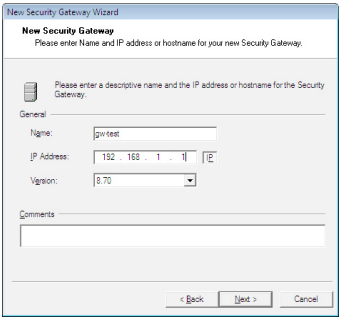
a) When the main FineTune window appears, open up the Default Data Source by pressing the **Security Editor** button. To create a new Gateway, right-click on the **Security Gateways** tree node and select the **New > Security Gateway** menu options.



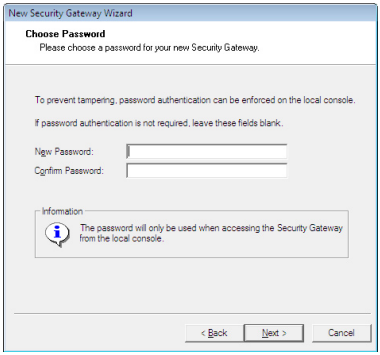

b) Now Select **Software** and click **Next**.




c) Select a name and enter an IP address which will be used for communication between the management workstation you are using now and the stand-alone hardware.

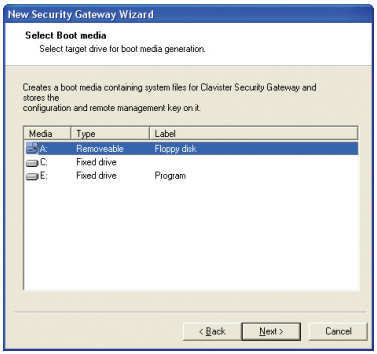


d) Enter a password *if* you want to protect access to the local Security Gateway console. Keep a record of this password.

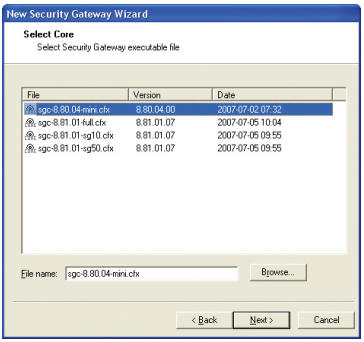



e) Select the target drive for boot media generation.

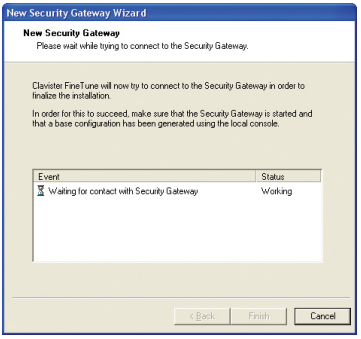
Note:
The target media must be formatted and all pre-existing data files must be erased.




f) Select the appropriate core from the list. If you are going to use a floppy-disk as the boot media you should choose the mini core option.




g) Contacting the gateway.
The Clavister FineTune management software will wait for you to insert the boot media in the stand-alone hardware and for the base setup to be finalized on the Security Gateway.



## 5 Boot the stand-alone hardware

Now you should boot the stand-alone hardware using the boot-media created in the previous steps. In some cases you must modify the boot sequence in the BIOS settings on your hardware. Once the stand-alone hardware is booted it becomes a Clavister Security Gateway.

## 6 Setup Console Access

The final phase of the base setup requires actions performed through the administrative interface on the Security Gateway.

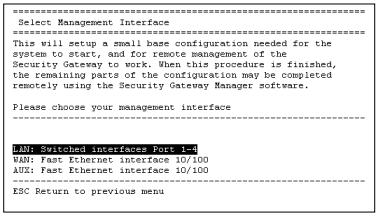
To work with the local administration interface, console access must be set up either through the use of a keyboard and monitor directly connected to the stand-alone hardware or through a RS-232 serial port.

If you plan to use a keyboard and monitor connected to the Security Gateway you can skip to the next step.

If you are going to use a separate device such as a terminal or a PC as console, a serial port and a terminal emulator such as HyperTerminal is required. The console must communicate with the console port on the Security Gateway using settings: 9600 baud, No parity, 8 bits, 1 stop bit and No Flow Control.

## 7 Start base setup

The console should now show a menu provided by the Security Gateway. The first step of the base setup is to select an interface for management access. You should pick the interface which is connected to the PC where you are running Clavister FineTune.

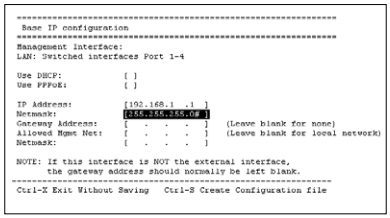



## 8 Enter IP address & Default Gateway

The console will now allow a number of options to be entered. Enter the IP address that will be used for the management interface of the Clavister Security Gateway with the appropriate netmask.

If you want to allow FineTune management access from any network, specify the Allowed Management Network as 0.0.0.0 with Netmask 0.0.0.0. However restricting access to a specific network (or IP address) is recommended and this can be done at a later time with FineTune.

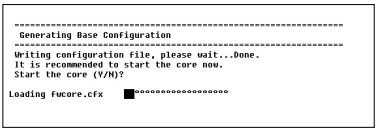
Press Ctrl-S to save the settings and continue.



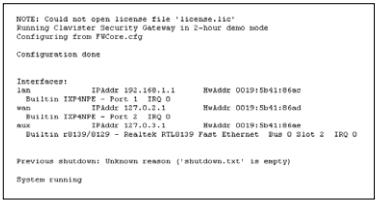
## 7 Start CorePlus™

a) The console will indicate that it is **Generating Base Configuration** and when this is complete it will say **Done**.

Now press "Y" to start the Clavister CorePlus operating system.

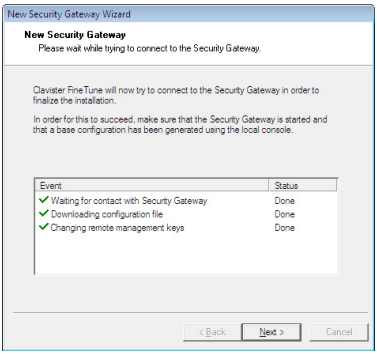



b) If everything is correctly configured, CorePlus will start and you will see a console screen similar to the one below.

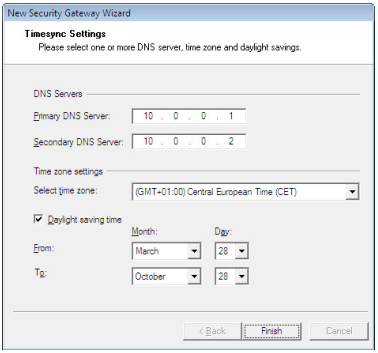



f) FineTune now contacts the Security Gateway and retrieves the base configuration as well as changing the remote management keys used for configuration communication.

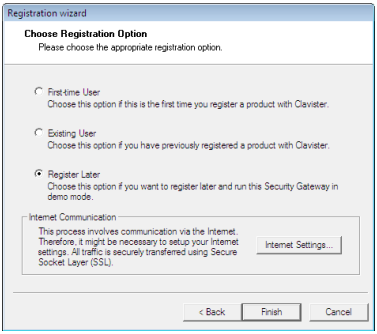
If this step fails, check your network configuration for mismatches between the Security Gateway and the management PC.




g) Enter the IP address of your DNS server. This address should be provided by your ISP.




h) If you already have internet access through another gateway or router you can register the product online by selecting one of the first two options, **First-time User** or **Existing User**. If not, choose **Register Later**.




## 9 Create security policies

Your Security Gateway is now ready for configuration using the FineTune management software and you should refer to the "FineTune Administration Guide" to find out how to create your first security policies.

Published September 2007