NETASQ CENTRALIZED MANAGER

V. 1.2

USER GUIDE

Date	Version	Author	Details
June 2010	V1.0	NETASQ	Creation
November 2011	V1.1	NETASQ	Update
February 2012	V1.2	NETASQ	Update

Reference: naengde_ncm-web-portal-v1.2

Products concerned

NETASQ Firewall: in version 8 and version 9
NETASQ products: NG series, U series, VA series, F series

FOREWORD

Copyright

© Copyright NETASQ 2011. All rights reserved. Under copyright law, any form of reproduction whatsoever of this user manual without NETASQ's prior written approval is prohibited. NETASQ rejects all liability arising from the use of the information contained in these works.

Liability

This manual has undergone several revisions to ensure that the information in it is as accurate as possible. The descriptions and procedures herein are correct where NETASQ firewalls are concerned. NETASQ rejects all liability directly or indirectly caused by errors or omissions in the manual as well as for inconsistencies between the product and the manual.

Notice

WEEE Directive

All NETASQ products that are subject to the WEEE directive will be marked with the mandated "crossed-out wheeled bin" symbol (as shown above) for items shipped on or after August 13, 2005. This symbol means that the product meets the requirements laid down by the WEEE directive with regards to the destruction and reuse of waste electrical and electronic equipment.

For further details, please refer to NETASQ's website at this address: http://www.netasq.com/recycling.html

License Agreement

Introduction

The information contained in this document may be changed at any time without prior notification. Despite the care taken in preparing this document, it may contain some errors. Please do not hesitate to contact NETASQ if you notice any.

NETASQ will not be held responsible for any error in this document or for any resulting consequence.

Acceptance of terms

By opening the product wrapping or by installing the administration software you will be agreeing to be bound by all the terms and restrictions of this License Agreement.

License

NETASQ hereby grants, and you accept, a non-exclusive, non-transferable license only to use the object code of the Product. You may not copy the software and any documentation associated with the Product, in whole or in part. You acknowledge that the source code of the Product, and the concepts and ideas incorporated by this Product, are valuable intellectual property of NETASQ. You agree not to copy the Product, nor attempt to decipher, reverse translate, de-compile, disassemble or create derivative works based on the Product or any part thereof, or develop any other product containing any of the concepts and ideas contained in the Product. You will be held liable for damages with interests therein in favor of NETASQ in any contravention of this agreement.

Limited warranty and limitation of liability

a - Hardware

NETASQ warrants its hardware products to be free of defects in materials and workmanship for a period of one year, in effect at the time the Purchase order is accepted. This period begins with effect from the date on which the product is activated.

b - Software

NETASQ Software products ("Software") are warranted for a period of 90 days (unless otherwise stated at purchase) from the date of the product's activation to be free from defects and to operate substantially according to the manual, as it exists at the date of delivery, under the operating system versions supported by NETASQ.

NETASQ does not warrant its software products for use with operating systems not specifically identified.

c - Default

NETASQ's entire liability and your exclusive remedy shall be, at NETASQ's option, either a return of the price paid for this License or Product resulting in termination of the agreement, or repair or replacement of the Product or media that does not meet this limited warranty.

d - Warranty

Except for the limited warranties set forth in the preceding paragraph, this product is provided "*as is*" without warranty of any kind, either expressed or implied. NETASQ does not warrant that the product will meet your requirements or that its operation will be uninterrupted or error free. NETASQ disclaims any implied warranties or merchantability or fitness for particular purpose, or non-infringement.

e - Recommendations

In no event will NETASQ be liable to you or any third party for any damages arising out of this agreement or the use of the product, including lost profit or savings, whether actual, indirect, incidental, or consequential, irrespective of whether NETASQ has been advised of the possibility of such damages. NETASQ's maximum liability for damages shall be limited to the license fees received by NETASQ under this license for the particular product(s) which caused the damages.

Any possible legal action relating to the alleged defectiveness of the software will come under the jurisdiction of NETASQ's headquarters, French law being the binding authority.

🛑 WARNING

1) Certain NETASQ products enable gathering and analyzing logs.   This log information allows the activity of internal users to be tracked and may provide nominative information. The legislation in force in the destination country may impose the application of certain measures (namely administrative declarations, for example) when individuals are subject to such monitoring. Ensure that these possible measures have been applied before any use of the product.
2) NETASQ products may provide cryptographic mechanisms which are restricted or prohibited by the legislation in force in the destination country. Despite the control made by NETASQ before exportation, ensure that the legislation in force allows you to use these cryptographic mechanisms before using NETASQ products.
3) NETASQ disclaims all liability for any use of the product deemed illegal in the destination country.

1. INTRODUCTION

NETASQ Centralized Manager is an application that allows a team of administrators to schedule tasks and to manage the security policy for several equipments from a central point. Once these policies have been created, just a simple click of the mouse will deploy them on several equipments.

NETASQ Centralized Manager therefore makes it possible to:
- Monitor equipments
- Work as a team
- Manage an equipment fleet

1.1.   Who should read this?

This manual is intended for network administrators or, at the least, for users with IP knowledge.

In order to configure your NETASQ product in the most efficient manner, you must be familiar with these protocols and their specific features:

- ICMP (*Internet Control Message Protocol*)
- IP (*Internet Protocol*)
- TCP (*Transmission Control Protocol*)
- UDP (*User Datagram Protocol*)

Knowledge of the general operation of the major TCP/IP services is also desirable:

- HTTP
- FTP
- Mail (SMTP, POP3, IMAP)
- Telnet
- DNS
- DHCP
- SNMP
- NTP

If you do not possess this knowledge, don't worry: any general book on TCP/IP can provide you with the required elements.

The better your knowledge of TCP/IP, the more efficient your filter rules and the greater your IP security.

1.2. Typographical conventions

1.2.1. Abbreviations

For the sake of clarity, the usual abbreviations have been kept. For example, **VPN** (*Virtual Private Network*).

1.2.2. Display

Names of windows, menus, sub-menus, buttons and options in the application will be represented in the following fonts:

Example
Menu `Interfaces`

1.2.3. Indications

Indications in this manual provide important information and are intended to attract your attention to important points. Among these, you will find:

NOTE /REMARKS

These messages provide a more detailed explanation on a particular point.

WARNING

These messages warn you about the risks involved in performing a certain manipulation or about how not to use your equipment.

TIP

This message gives you ingenious ideas on using the options on your product.

DEFINITION

Describes technical terms relating to NETASQ or networking. These terms will also be covered in the glossary.

1.2.4. Messages

Messages that appear in the application are indicated in double quotes.

Example
"Delete this entry?"

1.2.5. Examples

Example
This allows you to have an example of a procedure explained earlier.

1.2.6. Command lines

Command lines
```
Indicates a command line (for example, an entry in the DOS command
window).
```

1.2.7. Reminders

Reminders are indicated as follows:
🔹 Reminder.

1.2.8. Access to features

Access paths to features are indicated as follows:
↪ Access the menu `File\Firewall.`

1.3.   Vocabulary used in the manual

Equipment	Refers to the security device (firewall). The terms "equipment" and "security device" are used interchangeably.
Dialup	Interface on which the modem is connected.
NCM	Abbreviation for NETASQ Centralized Manager.
Firewall	NETASQ UTM device /product
Intrusion prevention	IPS is also used in its place.
Configuration slot	(Or policy). "Slot" or "policy" (filter, NAT, etc) are used interchangeably.
Host	Terms used as much to refer to workstations as to users.
Logs	A record of user activity for the purpose of analyzing network activity.

1.4. Getting help

To obtain help regarding your product and the different applications in it:
- Website: www.netasq.com. Your secure-access area allows you to access a wide range of documentation and other information.
- User manuals: NETASQ UNIFIED MANAGER, NETASQ REAL-TIME and NETASQ EVENT REPORTER.

1.5. Technical assistance centre

NETASQ provides several means and tools for resolving technical problems on your firewall.
- A knowledge base.
- A certified distribution network. As such, you will be able to call on your distributor.
- Documents: these can be accessed from your client or partner area. You will need a client account in order to access these documents.

For further information regarding technical assistance, please refer to the document "Standard NETASQ support".

1.6. Getting familiarized with the Web Portal

1.6.1. Logging on

Users can log onto NETASQ Centralized Manager from the web portal installed on the internal server or from outside your company network.

Services offered on the NCM web portal depend on the connected user accessing the application. User profiles can be defined by logging on as "Super Administrator" in NETASQ Centralized Manager.

1.6.2. General concept

The intuitive NETASQ Centralized Manager web portal is built around these two main objects – equipments and profiles.

Equipments correspond to the devices being managed (firewalls). The first step that a manager has to carry out is the creation of an equipment within a group of equipments.

The second step corresponds to the provisioning process. When the equipment is preconfigured to be contactable by NETASQ Centralized Manager, the manager will have to activate the site through the NETASQ Centralized Manager web portal. During this step, NCM will connect to the equipment and configure it automatically with the profiles that have been attached to it and will assign a digital certificate to it.

A single equipment can be attached to several profiles (Configuration, VPN, etc…), which can be created easily thanks to NETASQ Centralized Manager's intuitive interface. As soon as the manager attaches an equipment to a profile, NCM will automatically update the profile by applying the new configuration.

1.6.3. Layout of the interface

Access to objects management is based on a hierarchical organization. For example, in order to access the management of an equipment, you will need to browse the management of the corresponding equipment group.

The diagram below sets out the hierarchical organization of the various views.

Arrows represent the top-down menus that appear when browsing through the different views.

🛈 **NOTE:**
Avoid using the Back button on your browser and use the arrows on your NETASQ Centralized Manager taskbar instead (below the logo).

The banner at the top is divided into several sections that present:

- IDs and privileges of the connected manager:

- The general status of managed equipments, represented in 5 colors:

Green -> number of active sites
Yellow -> number of uncertain sites
Red -> number of uncontactable sites
Blue -> number of sites that have never been contacted successfully
Gray -> total number of sites

- The name of the view displayed and the access path from the manager view:

In the example above, after the ID of the manager (NCMG2), the ID of the equipment group (NCMA63) and the equipment being viewed (NCM1941) are indicated.

This access path allows:
- Identifying the entity being managed
- Browsing to one of the higher entities

1.6.4. Overview of the menus

The taskbar contains three main menus:

GENERAL ▼	MANAGEMENT ▼	MONITORING ▼

Each object type (manager/group/profile/equipment) has its own menu entries. Even though the name of the menu remains the same in general, entries inside it will differ according to the type of entity managed.

Furthermore, the display of menu entries is conditioned by the delegation profile (authorized actions), associated with the connected manager.

Menus Entities	GENERAL	MANAGEMENT	MONITORING
Actions allowed at the manager level	Looking up information Modifying information	Creating managers Creating groups of equipments Creating delegations Managing the repository	Status of equipments Monitoring console Statistics of equipments Managing certificates Life cycles of equipments Activity reports
Actions allowed at the group level	Looking up information Deleting the group of equipments	Creating equipments Creating local VPNs Creating global VPNs Creating configuration profiles Creating scheduling profiles Creating monitoring profiles Managing modifications on equipments	Monitoring console Status of equipments Statistics of equipments

Actions allowed at the equipment level	Editing the equipment Editing configuration variables Editing the configuration Attached profiles Duplicating the equipment Deleting the equipment Pre-configuring the equipment (win32) Pre-configuring the equipment (Linux) Activating the equipment High availability Rebooting the equipment Renewing certificates Updating the configuration Upgrading the license Upgrading the firmware		Managing equipment notifications Events of the week Events of the month Correlation of curves Full activity reports VPN activity reports

1.6.5. Ease of use

In order to facilitate the monitoring of equipments, some screens will open in a separate browser window.

Example
Menu `Monitoring\Monitoring console`

2. ACCESSING THE WEB PORTAL

2.1. User profiles

Administrator logins are defined by the "super administrator": this represents the only user who has administration privileges over NETASQ Centralized Manager products. This user is created during the installation of the NETASQ Centralized Manager solution and possesses all privileges as well as a special "ADMIN" privilege that only he holds. This gives him the right to perform certain operations such as the management of administrators. The super administrator cannot be configured.

2.2. Data models

Security profiles are used for managing equipments that are under the responsibility of service providers, often called managers. These service providers manage the NETASQ Centralized Manager equipments according to the groups of equipments that are attached to them.

This model creates an association between rules and classic RBAC roles (Role Based Access Model) illustrated below:

Privileged manager	Manager with all management privileges over the NETASQ Centralized Manager platform installed.
Manager	Service provider's team, which can manage some or all equipment groups.
Group of equipments	Console of an equipment group in read-only mode.

2.3. Role Based Access Model

2.4. Management and Delegation profile

The table below sets out the default permissions for each account:

	Privileged manager	Manager	Group
Create//Modify/Delete manager accounts	√		
Limit a manager's perimeter to a sub-set of subscribers	√		
Create/Modify/Delete subscriber accounts	√	√	
Create/Modify/Delete equipments	√	√	
Create/Modify/Delete profiles	√	√	
Access to the monitoring console in real time	√	√	√
View security dashboards	√	√	√
View Silver Monitoring statistics	√	√	√
View Gold Monitoring log reports	√	√	√

NCM's *Role Based Access Control* (RBAC) mechanism provides modular control over access to managed services by restricting their use only to authorized users.

Features can be accessed through delegation profiles. These profiles are managed by the privileged manager and allow the easy deployment of privileges over several user accounts.

2.5. Connecting to the Web portal

Proceed as follows to connect to the NETASQ Centralized Manager web portal:

1 Open your web browser and enter the URL https://server_name/NCM/en/

ℹ **NOTE**

"server_name" may be the host name, the IP address or the domain name of the server that launches NETASQ Centralized Manager.

The operator will need to retrieve the connection address as well as an account with which the necessary privilege level is associated.

Once he has logged on, the user will be redirected to his home page.

Below is an example:

3. GETTING STARTED WITH NCM

3.1. Introduction

This section sets out the different steps to carry out in order to manage your equipments with NETASQ Centralized Manager.

First of all, the privileged administrator will need to create a delegation profile, in which he will allow a user named "manager" to manage groups of equipments and as such, individual equipments.

Once you have opened your browser, (https://server_name/NCM/en/), you will access your NCM homepage which will set out your privileges.

Example

3.2. List of steps

1. Creation of a delegation profile
2. Creation of a manager associated with a delegation profile
3. Creation of an equipment group
4. Provisioning of configuration items
5. Creation of an equipment
6. Pre-configuration of an equipment: basic configuration of an equipment according to the information entered during its creation so that NCM can access the equipment and push the final configuration.
7. Creation of a configuration profile
8. Association of the configuration profile with an equipment
9. Activation of the equipment

3.3. NETASQ Centralized Manager views

3.3.1. Introduction

For each entity managed, NETASQ Centralized Manager offers several views that allow focusing on relevant information according to the type of action to perform.

This information is represented by tabs, enabling faster identification.

3.3.2. Privileged manager view

3.3.3. Manager view

3.3.4. Equipment group view

3.3.5. Equipment view

4. MANAGING MANAGERS

4.1. Introduction

The steps described in this section are intended only for the privileged manager, who has specific entries in the menu.

The `Management` menu allows:
- Creating managers
- Creating delegations
- Creating groups of equipments
- Managing repository

The `Monitoring` menu will allow the privileged manager to:
- Manage certificates
- View the life cycles of equipments
- View the activity reports of these equipments
- View billing tickets
- Access the monitoring console

4.2. Creating a Delegation profile

Customizable privileges are presented in a hierarchical form in order to allow quick and easy configuration of all specific privileges.

Enter information about the profile: (Delegation Profile)

Name [   ]   Comment [   ]

Configure right delegations

☐ click to toggle all rights for every category/all categories

⊟ monitoring ✔
           ↳ mapview ✔
                  ↳ topology ✔
                  ↳ profile ✔
                  ↳ google map ✔
           ↳ Equipment ✔
                  ↳ RRD ✔
                  ↳ security status ✔
                  ↳ logs ✔
                  ↳ detailed report ✔
                  ↳ correlation ✔
                  ↳ asset ✔
                  ↳ activity report ✔
           ↳ profile ✔
                  ↳ correlation ✔
           ↳ group of equipments ✔
                  ↳ top 5 ✔
                  ↳ history ✔
                  ↳ correlation ✔

⊟ managed equipments ☐
           ↳ configuration variables ☐
                  ↳ edit ☐
                  ↳ edit value ☐
           ↳ general ☐
                  ↳ create ☐
                  ↳ delete ☐
                  ↳ duplicate ☐
                  ↳ edit QOS policy ☐
                  ↳ file staging management ☐
                  ↳ edit ☐
                  ↳ passwd ☐
                  ↳ provisioning ☐
                  ↳ reboot ☐
                  ↳ redundancy ☐
                  ↳ staging ☐
                  ↳ vpn function ☐

⊟ monitoring equipments ☐
           ↳ general ☐
                  ↳ create ☐
                  ↳ delete ☐
                  ↳ duplicate ☐
                  ↳ edit ☐
                  ↳ passwd ☐
                  ↳ provisioning ☐
                  ↳ staging ☐

⊞ profiles ☐

⊞ repository ☐

⊞ group of equipments ☐

⊟ VPN ☐
           ↳ general ☐
                  ↳ certificates renewal ☐
                  ↳ configurations update ☐
                  ↳ create ☐
                  ↳ delete ☐
                  ↳ edit ☐
                  ↳ passwd ☐

[Cancel]   [Validate]

Managers have no privileges as long as they are not attached to a delegation profile. A manager's ability to manage individual privileges can simply be summarized as associating the appropriate delegation profile.

In the screen above, it is possible to attach one or several managers to a delegation profile. To do so, simply select the manager(s) from the list on the left and click on the arrow pointing to the right.

🛈 NOTE
Several managers can be selected by using the Shift and/or Ctrl keys. Clicking on the double arrow will allow attaching all managers to the delegation profile.

🛈 NOTE
In the list of managers to attach, those already associated with a delegation profile are grayed out. They can be selected in order to change their delegation profiles.

4.3.   Managing delegation profiles

Delegation profiles are listed in a specific tab on the privileged manager home page.

4.3.1. Explanation of the icons

👥 : This icon allows attaching managers to the profile.

🔍 : You can view the profile by clicking on this magnifying glass.

📝 : By clicking on this icon, you will be able to edit the profile.

❌ : This icon allows deleting the selected delegation profile.

✖ : This grayed out icon means that the selected delegation profile cannot be deleted as it is attached to several managers.

4.3.2. Creating a manager

4.3.2.1.   Step 1

1 Go to the `Administration` menu and select the option "Create a manager".

2 Fill in the required information. The name is mandatory.

3 Assign a delegation profile to the manager by selecting it from the drop-down list. If you omit this step, the default profile will be "Restricted".

4 Click on "OK".

4.3.2.2. Step 2

You will now see your manager's home page:

1 You can create a group of equipments by clicking on the button that appears. The following screen will appear:

Fill in the fields and click on "Next".

2 A window summarizing the information entered will appear:

Click on "Confirm".

Your access privileges will be indicated in a separate window:

You will now be able to connect to NETASQ Centralized Manager in order to manage this group of equipments in restricted mode.

ℹ NOTE

When you reach your manager's home page, you will be able to view his information by going to the `General` menu.

The manager's information (name, address etc.) or identification settings can be modified. You can also delete the manager or print information by clicking on the corresponding buttons.

4.4. Managing Managers

The `Managers` tab allows obtaining an overview of managers, with their logins, their associated delegations and their IDs.

When you select one of them, you will be directed to his home page.

This window shows the equipment(s) managed by the manager as well as his information.

The management of managers is explained hereafter in, Chapter 5\Manager view.

4.5. Privileged monitoring

The first monitoring features listed below are described in chapter 10.

- Monitoring-> Status of equipments
- Monitoring-> Monitoring console
- Monitoring-> Statistics of equipments

The 'Monitoring' menu in the privileged manager also allows managing:

- **Certificates:** displays certificates that are about to expire within a period that can be selected from a drop-down list.

- **Activity reports:** allows launching the generation of a page listing all tasks completed by the managers on the platform. The period of the report can be defined using the 2 date fields.

- **Life cycles of equipments:** lists all the high-level actions (creation activation and deletion) on the equipments managed from the platform.

5. MANAGER VIEW

5.1.   Home page

The home page of a manager is divided into 3 tabs:
>   - Status
>   - Information
>   - History

5.1.1. Status

Below is a preview of a manager home page in "Status" position:

The capture above shows the groups of equipment managed as well as their statuses. You will notice that this manager handles 4 equipment groups, with a total of 19 devices, 11 of which are active.

This information is also visible in the top banner represented by the color-coded icons (*cf* chapter 1 Introduction\Getting familiarized with the Web Portal \Layout of the interface).

A summary of the data relating to the manager will also appear (name, address, role etc.).

5.1.2. Information

The manager can also view information on the services enabled on the appliances that he manages:

5.1.3. Asset

The `Asset` tab control provides a detailed list of the inventory by group of devices:

5.2. Menu de la vue gestionnaire

The menus described in this section allow the manager to execute their actions. The contents of some menus may vary according to the delegation profile associated with the manager.

The `General` menu allows:

- Looking up general information on the manager. It can also access the screens that allow modifying this information

The `Administration` menu allows:

- Creating a group of appliances
- Managing the repository (see 6 MANAGING THE REPOSITORY)

The `Supervision` menu provides access to the following functions described in the chapter 9 MONITORING :

- The status of appliances
- The monitoring console
- Appliance statistics
- Certificate management
- View of appliance life cycles

6. MANAGING THE REPOSITORY

6.1. Introduction

The repository can be accessed by logging on with a manager account with the associated privilege.

Go to the menu `Administration\Manage the repository`.

The following page will appear:

6.2. Introduction to repositories

There are six categories of repositories:
- **Configuration:**
  This repository allows importing a configuration in the form of a folder.
  This configuration can be imported from an equipment that has already been deployed or an archive can be imported from a disk location.
- **Datafiles:**
  This repository represents the data files that may be used for storing or transferring information.

- **Firmware**:
  This repository allows importing updates of product version, in the form of .maj files.
- **License**:
  This repository allows importing product licenses.

- **PKI:**

    This repository allows storing and managing digital and electronic certificates from external certificate authorities.

- **Script**:

    This repository allows creating scripts that can either be associated with an equipment's configuration or integrated into a scheduling profile.

When you click on one of the entries in the list, its sub-directories will appear.

An example is given with the "License" file:

A set of icons representing the type of information in the repositories appears to the left of the screen

You will see the following icons:

- represents the root folder (or repository):

    Main directory of the repositories on the disk.

    Its sub-directories are operators.

- represents an operator:

    It is possible to have a single operator (NETASQ) with NETASQ Centralized Manager.

    Its sub-directories are groups of equipments.

- represents a group of equipments:

    Each group was initially created in the GUI.

Its sub-directories are vendor-model pairs.

- represents a vendor and a model:

  The model ("NETASQ_VERSION9") represents the main software version number of NETASQ equipments.

  Its sub-directories are types of downloads – Configuration or Script

- represents the type of download:

  There are two types: Configuration or script

- represents a configuration download:

  These file types will be displayed as configuration.

- represents a script download:

  This file types will be displayed as script.

6.3.   Managing repositories

Management features are accessible in the "Actions" column

We will set out in detail below the possible functions of this column.

6.3.1. Adding information

Adding an operator at the root level

The following window appears when you click on this icon with a single operator (NCM-NETASQ) to be added. Selecting the operator and clicking on "Add" will add the new operator to the tree.

Adding a group of devices at the operator level

The following window appears when you click on this icon with a list of equipment groups (identified by their ID and name) to be added. Selecting a group (or several) and clicking on "Add" will add the new subscriber to the tree.

NOTE
When you reach your manager's home page, you will be able to view his information by going to the `General` menu.

Adding a configuration download to the Configuration download type level

The following window appears when you click on this icon:

It is possible to import:

- An existing file through the following steps by clicking on "Import from a file":

A new window appears and allows you to specify the file to be downloaded.

When the file has been downloaded, the import window appears with the name of the folder, the tag (the file name by default) and the comment.

Nothing will be done if you cancel.

During the import, the configuration file will be added to the tree under the configuration directory.

- An existing configuration from an available equipment by clicking on "Import from an equipment".

The import window appears with the list of appliances for which the current configuration can be retrieved.

When the file has been downloaded, the import window appears with the name of the folder, the tag (the file name by default) and the comment.

Nothing will be done if you cancel.

At the end of the import process, the configuration folder "ClassicPolicy" will be added to the tree under the configuration directory as shown in the following capture.

Adding a script to the Script download type level

The following window appears when you click on this icon with the choice of the script download type.

It is possible to import:

- An existing file through the disk by clicking on "Import from disk".

A new window appears and allows you to specify the file to be downloaded:

⚠ WARNING
The file extension should be .txt

When the file has been downloaded, the import window appears with the name of the file, the tag (the file name by default) and the comment, as well as an area with the contents of the downloaded file as shown in the following capture. The information of the script can be modified before clicking on "Ok".

Nothing will be done if you cancel.

After the import treatment, the script will be added to the tree under the configuration directory as shown in the following capture.

- Or to create a new file through the following steps.

A new window appears and allows you to specify the script information. A configuration variable is specified when you give it a name prefixed with the symbols "{$" and ending with "}" as in the example "{$variable}". We will use this variable in the configuration section of an equipment as shown in the following capture:

Nothing will be done if you cancel.

After the import treatment, the script will be added to the tree under the configuration directory as shown in the following capture.

6.3.2. Deleting repository information

🗑 Entities that are not used by a profile or an equipment can be deleted (we shall cover these scenarios on the following sections).

Before any entities are deleted, a confirmation message will appear according to the type
of entity:

- group of equipments

- configuration or script download type

6.3.3. Downloading a file

- Files can be downloaded by clicking on this icon.

You will then see your browser's classic download window for the selected configuration or
script file as shown in the example below a the "CA" file:

6.3.4. Finding out where a directory or a file is used

- ⊞ To recognize entities that are used, their icons have a star at the bottom right as shown in the following capture:

- 🔎 By clicking on this icon, a window will appear displaying the list of entities that use these files. When you move your mouse over it, a tooltip will appear with the list of equipments or profiles that reference this file.

6.3.5. Modifying information about elements

Tags and comments of directories and configuration or script files can be modified by double-clicking on them and pressing Enter to confirm or by clicking elsewhere on the screen.

The result appears directly in the tree after the message "Request in progress" appears:

The modification of this information from a root configuration download folder (represented by the icon 🔒) will be applied to all its sub-folders and files.

6.4. Gestion des Filtres

Filters can be specified:

- For displaying only part of the tree structure, the "Manage repositories" field
- For displaying only a tag
- For displaying only a comment
- For repositories over a certain period.

By clicking on the button [Search] the following window will appear. By clicking on "Save", the filters will be applied on the repository tree structure.

To disable any filter, simply clear the fields and save.

6.5. Other types of files

The repository also allows managing:
- Firmware files
- License files
- Certificate files

All the actions in the section 6.3 Managing repositories are available for these elements.

7. MANAGING GROUPS OF EQUIPMENTS

The profile-based approach allows defining a global security policy for a group of equipments by using a set of predefined models.

The available profiles are managed from the administration page of the equipment groups.

The main advantage of this approach is being able to deploy several equipments by configuring only one profile.

Upgradability is ensured by NETASQ's level of abstraction:
   • Same operating mode (creation of equipments, creation of profiles, attachment of equipments to profiles).
   • Generic profiles to provide security services regardless of equipment model.

7.1.   General view

Here is an example of a group home page before any equipments are attached to it:

7.1.1. Tabs in the equipment group view

You would have noticed the following tabs in the capture above:

- **Status**
- **Equipments**
- **Asset**
- **VPN**
- **Monitoring**
- **Configuration**
- **Planning**

The rest of this section will be spent explaining the various tabs. In the captures shown, it is presumed that equipments have already been created in the group.

7.1.1.1. "Status" tab

The "Status" tab provides an overview of the equipment group's activities.

- The left column presents statistics of the various features used by the equipments in the form of a bar graph.
- The right column shows a history of the various features used by the group of equipments in the form of a line graph.
  You can select a given activity period by "day", "week", "month" or "year".

7.1.1.2. "Equipments" tab

The "Equipments" tab is made up of two parts:

- The first table shows the status of the hardware and monitoring services implemented. Here, we learn that there are 27 equipments in this group, 8 of which use "Silver Monitoring", and 3 use "Gold Monitoring".
  We can also see that 17 of them use "Configuration profiles" and 13 use "Scheduling", 9 use "VPN" and 2 use "Redundancy" (high availability).

- The second table shows details of the 27 equipments identified and the services used. You have the option of displaying only information that matters to you by going to the drop-down list at the top of each column:
  You can, for example, choose to only display running services by selecting "ON" instead of "ALL".

🛈 NOTE
All information contained in the columns is displayed as "ALL" by default.

The capture below represents the columns dedicated to services ("Mail Alerting", "Silver Monitoring" etc.).

The first two columns will allow you to filter hardware by:

- Status:

- Managed equipments:

You can also filter values in the column reserved for equipments (displayed by name) as such, by typing letters or keywords in the relevant field:

7.1.1.3. "Inventory" tab

This tab is also divided into two parts:

- A "Hardware" tab

This tab sets out details of equipments contained in the group with hardware information such as the name, product model, firmware version, license type and expiry date of the certificate (icon).

In the same way as for the "Equipments" tab, filtering is possible by "Name" and by "Model" in the corresponding fields; as well as by status and managed equipments (expand the lists in which "all" is displayed).

By clicking on (help), you will see the legend of icons used in the table:

You will see as such information relating to features deployed on one of the equipments.

7.1.1.4. "VPN" tab

This tab lists the VPN topologies defined for the group of equipments.

More information on VPN profiles (topologies) will be given in chapter 7.3 Managing VPN topologies

7.1.1.5. "Monitoring" tab

This tab lists the monitoring profiles defined for the group of equipments. A monitoring profile allows defining customized graphs that will be visible when you view the equipments attached to this profile.

When you select a monitoring profile, a screen with two tabs appears:

- "Information"

You will access detailed information about the monitoring profile as well as the list of equipments attached to it and the data that allows building customized graphs.

By clicking on one of the equipments on the list, you will return to its home page.

- "Status of update"

This tab allows you to view the latest equipment updates.

7.1.1.6. "Configuration" tab

This tab lists the configuration profiles defined for the group of equipments.

More information on configuration profiles is given in chapter 7.2 Managing configuration profiles

7.1.1.7. "Planning" tab

This tab lists the scheduling profiles defined for the group of equipments. A scheduling profile allows defining the periodic execution of commands on equipments attached to this profile.

When you select a scheduling profile, a screen containing three tabs will appear:

- "Information"

You will access detailed information about the scheduling profile as well as the list of equipments attached to it.

By clicking on one of the equipments on the list, you will return to its home page.

- "Planning"

This tab displays information concerning the scheduling of the profile: list of tasks (command script) that will be performed and frequency of execution.

- "Execution status"

This tab displays information concerning the execution of scheduled tasks. After a task is executed, it is possible to view the execution report for each equipment by clicking on the icon ✅.

This report lists all commands as well as the equipment's responses.

```
Task/NSQ/NETASQ/TEST/SYSPROP                                    ⊠

nop Exemple de script

100 code=00a00100 msg="Ok"
Netasq>
nop une variable DNS=127.0.0.1
nop une variable DNS=127.0.0.1

100 code=00a00100 msg="Ok"
Netasq>
system property

101 code=00a01000 msg="Begin"
Type="Firewall"
Model="F200-B"
Version="8.0.5"
ASQVersion="4.0.4"
SerialNumber="F200XB008380600401"
```

7.2. Managing configuration profiles

The configuration profile allows defining an equipment configuration that can be shared by all equipments in the group. A profile is made up of configuration elements that are stored in the file repository. An element can be shared by several profiles, thereby making it possible to deploy this configuration element on all managed equipments.

7.2.1. Creating a configuration profile

Configuration profiles can be created from the equipment group view.

1 Go to the menu `Administration\Create a configuration profile`.

The following page will appear:

```
┌─ Configure the Profile files ─────────────────────────────┐
│  [Cancel] [Save]                                           │
│                                                            │
│  Configuration profile Name [_____]    Profile comment [_____] │
│                                                            │
│  No file attached                                          │
│                                                            │
│  Add Configuration files  [ + ]                            │
│                                                            │
│  Add Data files  [ + ]                                     │
│                                                            │
│  [Cancel] [Save]                                           │
└────────────────────────────────────────────────────────────┘
```

2 Enter the required information. The name of the profile is mandatory.

3 Attach the configuration elements to the profile by clicking on the corresponding icon ➕.

A new window will open, providing a view of the section of the repository corresponding to the selected icon.

4 Select the configuration elements by clicking on "OK".

As shown in the example below, it is possible to select either a single element, represented by the icon 📄, or a set of elements (icon 📂) or a full configuration archive (icon 📋).

> ### 🅘 NOTE
> You can select multiple elements by using the 'Shift' and 'Ctrl' keys.

5 Click on OK to confirm the selection.

Another window will appear.

Before validating the configuration profile, you can delete configuration elements. To do so, select the checkbox next to the element(s) to be deleted, then click on the icon 🗑.

6 Click on "Save" to confirm the creation of the configuration profile.

The main page of the configuration profile will then appear.

7.2.2. Configuration profile view
In the equipment group view, it is possible to administer configuration profiles by clicking on the Configuration tab.

When you select a configuration profile, a screen containing three tabs will appear:

- "Information"

This screen offers a general description of the profile and lists the attached equipments.

You can perform the following actions from this screen:

- "Attach/Detach equipments"
- "Delete the profile"

- "Configuration files"

This screen lists the profile's configuration elements

- "Status of updates"

Information	Configuration files	Status of updates	

this page is automatically refreshed every **30 s**.
last update: **14/12/2011 11:19:29**

ID - EQUIPMENT'S NAME	LAST UPDATE	EQUIPMENT UPDATE RESULT
NCM146 - TestDCO	12/09/2011 21:20:58	Command timeout on the device
NCM148 - U450_Lille		No information

This screen shows the status of configuration updates on equipments attached to the profile.

7.2.3. Managing a configuration profile

Configuration profiles can be administered from the equipment group view by clicking on the "Configuration" tab.

From the list of configuration profiles, you can click on a profile in order to administer it. You will then be at the level of the profile management view.

The "Administration" menu offers several actions:
- Deleting the profile
- Attaching/Detaching sites: this link allows attaching or detaching equipments to or from the profile.
- Modifying a configuration profile: you can add or delete configuration files to or from the profile
- Duplicating this configuration profile: the list of configuration files will be added to a new profile

These actions – attaching/detaching equipments and deleting profiles – are also available in the "Information" tab in the configuration profile view.

7.2.4. Attaching/detaching an equipment to or from a profile

By selecting this action from the menu or the button, the following page will appear with the equipments that can be attached to or detached from the profile:

To attach /detach, select the equipment and move it using the relevant arrows. Click on "Confirm" to validate your actions.

In our example, we have attached the equipments "NETASQ_1 NCM110" and "fwdemo NCM 141" to our profile. After you have confirmed the action, you will be redirected to a summary page with a button that allows you to return to the main page of the profile management.

7.2.5. Edit a profile

The modification of a profile consists of modifying the configuration elements that make up the profile.

In the view of the configuration profile to be modified, go to the menu `Management\Edit a profile`.

See paragraph 7.2.1 Creating a configuration profile to see what actions you need to carry out in order to modify the configuration profile.

7.2.6. Duplicating this profile

In the view of the configuration profile to be modified, go to the menu `Management\Duplicate this profile`.

See paragraph 7.2.1 Creating a configuration profile to see what actions you need to carry out in order to duplicate the configuration profile.

7.2.7. Deleting the profile

When this action is selected from the menu or the button, a confirmation message will appear:

If you confirm, the profile will then be deleted from the base. This action cannot be undone.

7.3. Managing VPN topologies

The VPN topology feature makes it possible to create and manage a VPN architecture involving several equipments. By associating equipments to a VPN topology, NETASQ Centralized Manager will automatically calculate and push configurations on equipments involved in this VPN architecture.

7.3.1. Introduction

There are 2 types of VPN topologies in NETASQ Centralized Manager:

- Local VPN: allows defining a VPN architecture involving only equipments of the group in which the architecture is being defined
- Global VPN: allows defining a VPN architecture involving equipments from several groups

The operating principle of the creation wizard is the same for both topologies. The difference arises when equipments are being selected, as the global topology will prompt the user to look for equipments in other groups.

NOTE
A manager can only create a global VPN topology with equipments he is able to access.

A VPN topology can be created in the equipment group view.

1 Go to the menu `Management\Create local VPN`.

The following page will appear:

2 Enter the name of the VPN topology.

3 Move the equipments that are supposed to be in the VPN topology and select the type of topology - "star" or "mesh".

ℹ NOTE

In the case of a star VPN topology, the center of the topology must also be selected (the focal point).

4 Select the certificate authority to be used for this topology..

ℹ NOTE

NETASQ Centralized Manager proposes the certificate authority embedded in the solution by default.
Other certificate authorities can be defined by adding the necessary certificates to the repository.

5 Advanced mode allows selecting the traffic endpoints for VPN tunnels.

By default, NETASQ Centralized Manager includes all endpoints that have been defined as protected at the level of equipments participating in the topology

```
NCM110 - NETASQ_1
  ☐  192.168.10.0 / 255.255.255.0
  ☑  192.168.0.0 / 255.255.255.0
NCM111 - NETASQ_2
  ☑  192.168.1.0 / 255.255.255.0
```

Traffic endpoints for each equipment can be managed in the screen for modifying equipments.

6 Click on "Next".

Another screen will appear, making it possible to monitor information about the VPN topology before confirming its creation.

7 Click on "Confirm".
The main page of the VPN profile will then be displayed.

7.3.2. VPN topology view

In the equipment group view, VPN profiles can be administered by clicking on the "VPN" tab.

You can go to a VPN profile by clicking on its name or by expanding the node in order to view equipments involved in a topology. It is possible to browse to the management of an equipment by clicking on its ID.

ℹ GENERAL NOTE

The large icon ⭐ represents a star VPN topology. The small icon ⭐ represents the equipment used as the focal point.

When you select a VPN profile, a screen containing two tabs will appear:

- "Information"

You will access detailed information about the VPN topology as well as the list of equipments attached to it.

By clicking on one of the equipments on the list, you will return directly to its home page without going through the main page.

- "Status of updates"

This tab allows you to see the latest updates of the equipments.

7.3.3. Managing a VPN topology

VPN topologies can be administered from the equipment group view by clicking on the "VPN" tab.

From the list of VPN topologies, you can click on a topology in order to administer it. You will then be at the level of the VPN management view.

The "General" menu offers several actions:

- Edit VPN information
- Delete VPN
- Renew certificates
- Update configurations

These actions – modifying and deleting topologies – are also available in the "Information" tab in the VPN topology view.

7.3.4. Edit VPN information
The modification of a topology consists of modifying VPN data, the list of equipments and the traffic endpoints of the tunnels.

In the view of the VPN topology to be modified, go to the menu, `General\Edit VPN information` (or click on "Edit information" in the "Information" tab in the VPN topology view).

7.3.5. Deleting the VPN

When this action is selected from the menu `General\Delete the VPN` (or the button in the "Information" tab, a confirmation window will appear:

If you confirm, the profile will then be deleted from the base. This action cannot be undone.

7.3.6. Renew certificates

When this action is selected in the menu `General\Renew certificates,` a window asks you if you really want to do this action.

By validating this action, certificates of configurations involved in the VPN topology will be updated.

7.3.7. Update configurations

When this action is selected in the menu `General\Update configurations,` a window asks you if you really want to do this action.

By validating this action, NETASQ Centralized Manager will impose the update of equipments involved in the VPN topology.

7.4. Managing Monitoring profiles

The monitoring profile will allow setting up customizable graphs that can be read when viewing appliances attached to the selected profile.

Creating a monitoring profile

Monitoring profiles are created from the appliance group view.

1 Go to the menu `Administration\Create a monitoring profile`. The following page will appear:

2 Enter the required information. The name of the profile is mandatory.

3 Add SNMP polling elements to the profile by clicking on the corresponding icon.

The Name, OID, Type, Min., Max., Comment, Threshold and Frequency fields appear for the relevant information to be entered.

4 Enter the required information in the corresponding fields.

ℹ️ NOTE

The Threshold and Frequency fields allow defining real-time alerts. As soon as the value of the retrieved SNMP counter exceeds the threshold value, NETASQ Centralized Manager sends an e-mail alert. It is possible to treat the occurrence period of the value using the Frequency field.

The sending of e-mails is enabled only for appliances that have a Gold monitoring level.

5 Next, define the data relating to the graph, if you wish to generate one: click on the icon [+] "Add graph rendering". New fields will appear as such:

NOTE

Several curves can be defined on the same graph. To do so, you will need to provide additional data, as each data type is associated with a particular counter on the profile.

The X-axis label corresponds to the label identifying the data (a data series). It appears under the X-axis.

6 Click on "Finish" to confirm the creation of the monitoring profile.

A page will appear asking you to attach appliances to a security profile:

7.5. Managing scheduling profiles

The scheduling profile will allow scheduling the execution of CLI command scripts on appliances attached to the profile.

Creating a scheduling profile

Scheduling profiles are created in the appliance group view.

Go to the menu `Administration\Create a schedule:`

The following page will appear:

You will see a tab named "Scheduling", which you can enable or disable by selecting or unselecting the relevant checkbox, and schedule the task when you wish:

You can schedule the task according to the following frequencies:

Scheduled:

Daily

- Now
- Once
- Daily
- Weekly
- Monthly

and select the time when it will begin.

The "Advanced" button allows displaying additional options:

Advanced
Start date: 17/02/2012
End date:

Cancel   Save

The dates on which the task begins and ends can be defined in the corresponding fields. Next, click on "Save".

The following window will provide a summary of the information you have entered.

2 Go back to the "Task List" tab and enter a name for this schedule and click on the button ➕ to add a task.

3 Expand the task tree structure (click on the "+" next to "Task") in order to reach the following page. Next, select the desired file and click on OK.

Selection

- Task
  - NCM
    - NCMA3
      - NETASQ
        - VERSION_8
        - VERSION_9
          - qualif_post
          - qualif_pre
  - NETASQ

File selected: OK
File type: Task   Cancel

The following window will appear, displaying the imported file:

Click on "Save".

The following window sets out the information regarding your schedule, namely, a summary presented in three tabs:

4 To attach or detach appliances, click on the button on the bottom left, and drag and drop the appliances to attach from one column to the other as shown in the following screen:

Once the desired operations have been performed, click on "Confirm".

The button "Profile management" will redirect you to the summary of your scheduling data seen above.

To delete the scheduling profile created, click on the button at the bottom right of the "Delete profile" screen.

8. NCM – MANAGING AN EQUIPMENT

8.1. Life cycle of an equipment

The NETASQ Centralized Manager solution allows managing NETASQ multifunction firewall in order to maintain them and follow up on their configuration and monitoring. To facilitate the follow-up and management of equipments, NETASQ Centralized Manager manages the statuses of equipments according to their life cycles.

The general life cycle of a NETASQ equipment in NETASQ Centralized Manager can be broken down into the steps below:

- **Step 1: Creation of the equipment**
- By entering the information that would allow NETASQ Centralized Manager to connect to the equipment, it will be created via the web portal and inserted into the database.
  During this step, the level of monitoring is assigned to the equipment. NETASQ Centralized Manager offers 3 levels of tracking:
    - Silver allows tracking the operational status of the equipment and obtaining monitoring graphs
    - Gold allows tracking the equipment's logs
    - Mail alert allows the administrator to receive e-mails in the event major incidents arise on the equipment

- **Step 2: Pre-configuration of the equipment**
  The operator in charge of this operation retrieves connection information from the NETASQ Centralized Manager web portal and pre-configures the equipment.
  At the end of this step, the equipment will be ready for deployment on the site so that NETASQ Centralized Manager can update it with the final configuration.

- **Step 3: Activation of the equipment**
  This step is also called "provisioning". The administrator performs this step by using an entry in the menu of the NETASQ Centralized Manager web portal. As the equipment is physically linked to a network, NETASQ Centralized Manager can update it with the final configuration.
  As proper practice, it would be useful to check that the equipment can be contacted before proceeding with its provisioning (simply ping its external address).

- **Step 4: Management and monitoring of the equipment**
  Once the equipment has been activated, it is ready for other tasks such as monitoring, configuration changes and insertion into a VPN topology. All these operations can be conducted through the NETASQ Centralized Manager web portal.

8.2.   Actions and life cycle

Once an equipment has been successfully inserted into the database, an administrator may perform many administrative or monitoring operations directly from the equipment's home page.

The screen capture below provides a preview of this home page. The various management actions allowed on this equipment are grouped into specific menus. These sections correspond to phases in the life cycle of the managed equipment.

i **GENERAL NOTE**

The contents of these menus vary according to the role of the user connected to the web portal.

Some of these operations can be performed at any moment or regardless of the equipment's status, whereas others may require:

- The provisioning of the equipment (display of the equipment's logs, asset management)
- That the equipment be online (current configuration)

The table below describes the actions that can be performed on an equipment depending on its status.

Menu Item/Action	Status of the equipment	Comments
GENERAL		
Edit the equipment	Created	
Attached profiles	Created	
Duplicate the equipment	Created	
Delete the equipment	Created	
Activate the equipment	Pre-configured and connected to the internet	You are advised to check the ISP's connectivity before launching the activation.
Reboot the equipment	Activated and connected	
Renew certificates	Activated and connected	
Update the configuration	Activated and connected	Imposes an immediate update
MONITORING		
Current configuration	Activated and connected	
Events of the week / month	Activated and connected	Requires the "Gold Monitoring" level.
Activity reports	Activated	Requires the "Gold Monitoring" level.
Asset Management		
Firmware inventory	Activated	
License management	Activated	
Hardware history	Activated	

The various entries in these menus are described in this section.

8.3.   Creating an equipment

Equipments can be created in the equipment group view.

1 Go to the menu `Management\Create a NETASQ managed equipment.`

The following page will appear:

2 Fill in the necessary fields in order to create the equipment.

The equipment creation page is divided into several functional sections:

- Selection of the equipment model.
- Administrative information: name (mandatory field), address and person in charge of the equipment.
- Assignment of the equipment to a pilot site: used for classifying the equipment as a demonstration or test site.
- Information that NETASQ Centralized Manager requires in order to connect to the equipment: all fields, except the serial number, are mandatory.
- Time slot for updating the equipment: outside this time slot, the equipment cannot be updated.
- Specification of the level of monitoring.

GENERAL NOTE
The time slot makes it possible to avoid coinciding with updates of the equipments, which may in some cases disrupt production traffic.

If the update follows an explicit command (for example `update the equipment` or `update the VPN`), the web portal will display an error screen. However, for updates following a modification of the configuration (configuration element, configuration profile or VPN topology), NETASQ Centralized Manager will attempt to update again periodically until the time slot coincides with an authorized time.

3 To configure the equipment's VPN traffic endpoints, click on "Advanced configuration".

Information regarding the management of traffic endpoints are set out in the chapter 8.3.1 Defining traffic endpoints .

4 Complete the creation step by clicking on "Finish".

The following screen will appear, allowing you to check information about the equipment before confirming its creation.

The administrator can then perform one of the following actions:
- Go back to the previous screen in order to change certain settings
- Go to the equipment's home page

8.3.1. Defining traffic endpoints

This information will be used in VPN topologies to define traffic endpoints. By default for each equipment in a VPN topology, NETASQ Centralized Manager retrieves all the traffic endpoints defined at the equipment level.

🛈 NOTE /REMARK

It is possible to define traffic endpoints that are not directly connected to the equipment. This allows managing Hub & Spoke configurations.

1 To manage an equipment's traffic endpoints, go to the equipment's management page. There are 2 ways to access it:

- During the creation of the equipment
- After having launched the menu `General / Edit the equipment,` click on "Modify information" from the viewing page.
-

2 Click on "Advanced configuration". The next part will be set out in the screen that creates/modifies equipment information.:

TRAFFIC EXTREMITY ACCESSIBLE VIA VPN:

IP address / Mask / Comment

192.168.20.0 / 255.255.255.0 /
172.16.20.0 / 255.255.255.0 /

[Add a sub-network accessible via VPN]

[Remove sub-network(s) accessible via VPN]

* This field can only include characters from the list: a..z, A..Z, 0..9, space, ', -, à, â, ç, è, é, ê, ë, ô, ï, ù, û, ü

[Cancel]   [Finish]

3 Click on "Add a sub-network accessible via VPN". The following screen will appear:

Enter information about the sub-network accessible via VPN:

IP address: [   ]   Mask: [   ]

Comment [   ]

[Cancel]   [Validate]

4 Enter the fields for the traffic endpoint and click on "Validate". The screen that creates/modifies equipment information appears with the new traffic endpoint.

5 The administrator can then add another traffic endpoint, delete selected endpoints or end the creation/modification of the equipment.

8.4. General view

The following is an example of an equipment's home page:

8.4.1. Tabs in the equipment view

You would have noticed the following tabs in the capture above:

- **Status**
- **Inventory**
- **Equipments**
- **Network configuration**
- **Configuration files**
- **Monitoring**
- **Information**

The rest of this section will be spent explaining the various tabs. In the captures shown, it is presumed that equipments have already been created in the group.

8.4.1.1. "Status" tab

The "Status" tab was covered in section 8.4 ; it is the equipment's "home page". It shows the operating status and the status of updates.

It also presents a set of graphs that take into account the equipment's operating status over time. NETASQ Centralized Manager offers 5 default graphs:
- Availability presents the equipment's accessibility status over time
- Traffic displays the throughput of the equipment's external interface over time
- Uptime presents for each time bracket the uptime of the equipment
- CPU presents the equipment's CPU consumption
- RTT/TTL shows both the response time of the ping command as well as the number of bounces.

The display of these graphs can be disabled.

Ad administrator can display customized graphs by attaching the equipment to a monitoring profile. Graphs defined at this profile's level can then be enabled or disabled according to the administrator's needs.

8.4.1.2. "Asset" tab

Status	**Asset**	Equipment	Network configuration	Configuration files	Sanity Check	Information

HARDWARE INVENTORY	
Model	
CPU	
Memory	
Serial Number	
Certificate expiration date	

FIRMWARE INVENTORY	
Firmware	
License	

LICENSE	
IPS Version	
IPS expiration date	
Antivirus Version	
Antivirus expiration date	
Antispam Version	
Antispam expiration date	
URL Version	
URL expiration date	

This page displays details of the equipment, both hardware (model, serial number…) and software (firmware version, license...).
It also presents information on the expiry dates of features deployed on the equipment.

8.4.1.3. "Equipment" tab

This screen offers visibility over associated profiles as well as the type of service associated with the equipment.

Status	Asset	**Equipment**	Network configuration	Configuration files	Sanity Check	Information

ASSOCIATED PROFILES
Monitoring Profile : **0**
Configuration Profile : **NCMPR47**
Planning Profile : **0**

LOG MANAGEMENT:	
Silver Monitoring: **yes**	SNMP community: **COMMUNITY**
Gold Monitoring: **yes**	
Mail alert: **yes**	Email: ⬛⬛⬛⬛@netasq.com

8.4.1.4. "Network configuration" tab

This screen provides connection information that has been defined so that NETASQ Centralized Manager can manage the equipment.

Status	Asset	Equipment	Network configuration	Configuration files	Sanity Check	Information

INTERFACE	
User name: admin	User password: *****
External Interface IP address: 123.123.123.123	Mask: 255.255.255.240
Administration Interface name : ethernet0	External gateway: 123.123.123.122
Hostname: NCM148	Serial Number

PLANNING A TIME SLOT FOR THE CONFIGURATION UPDATE	
Begin time: 00:00	End time: 23:59

Traffic extremity accessible via VPN:		
IP address:	Mask:	Comment
192.168.1.0	255.255.255.0	LAN
172.31.1.0	255.255.255.0	DMZ1

8.4.1.5. "Configuration files" tab

This screen lists all the files (configuration, license and software version) associated with the equipment.

Status	Asset	Equipment	Network configuration	Configuration files	Sanity Check	Information

Configuration files	Tag	Comment	D
NCM_1 ➡ /ASQ/00.def	NCM_1		1
NCM_1 ➡ /ASQ/01	NCM_1		1
NCM_1 ➡ /ASQ/01.def	NCM_1		1
NCM_1 ➡ /ASQ/02	NCM_1		1
NCM_1 ➡ /ASQ/02.def	NCM_1		1
NCM_1 ➡ /ASQ/03	NCM_1		1
NCM_1 ➡ /ASQ/03.def	NCM_1		1
NCM_1 ➡ /ASQ/slotinfo	NCM_1		1
NCM_1 ➡ /AntiSPAM/antispam	NCM_1		1
NCM_1 ➡ /AntiVIRUS/00	NCM_1		1
NCM_1 ➡ /AntiVIRUS/01	NCM_1		1

These files are either directly attached to the equipment (applies to software version and the 2 configuration files, network and route) or attached through a configuration profile (grayed out files).

8.4.1.6. "Sanity check" tab

This tab indicates whether VPN features have been enabled during the last activation.

Status	Asset	Equipment	Network configuration	Configuration files	Sanity Check	Information

STATUS:

Are VPN functions enabled ? **yes**

Last provisioning date: **No provisioning yet**

8.4.1.7. "Information" tab

This screen shows the equipment's data (name, address, etc.), its manager and its IDs.

Status	Asset	Equipment	Network configuration	Configuration files	Sanity Check	Information

EQUIPMENT:

Name: **U450_Lille**

External reference: **NCM148**

Address: **rue du buisson**

ZIP Code: **59000**   City: **Lille**

Country: **France**

Remarks:

PILOT EQUIPMENT / BILLING DATE:

Pilot equipment: **no**   Billing Date: **12/09/2011**

ADMINISTRATOR:

Name: **rup TOTO**

Address:

ZIP Code: City:

Country:

Email: **dcouturier@netasq.com**

Phone: **1234567**   Fax:

MANAGEMENT INFORMATION:

Login

Password *****

Equipment identifier: **NCM148**

Group identifier: **NCMA6**

Control key (V2.1): **23-87-7633/2**

8.5. GENERAL Menu

The General menu in the equipment view is presented as follows:

Some entries are grayed out according to status or the configuration of the equipment. In the capture above, the entries "Update the license" and "Update the firmware" are grayed out as there are no files (license and firmware) associated with them.

8.5.1. Editing the equipment

By selecting the menu `General\Edit the equipment information`, the page for managing the equipment appears. The "Information" tab presents a summary of all the equipment's settings (except for attached profiles). The "Status" tab indicates the date and time of the last activation as well as information about the equipment's involvement in a VPN topology.

To modify certain settings, the administrator has to click on "Modify information". He will then be able to modify data except for the following:

- The type of device linked to this hardware equipment cannot be changed.
- Some parameters are enabled only once during the activation. Changing their values would require a new activation. These parameters concern mainly the ISP's connectivity such as the external IP address and the default gateway (router).

The administrator will see the same screens as those during the creation of the equipment (minus the choice of the model).

i NOTE /REMARK

Some modifications may cause incompatibility issues with the various profiles attached to this device. The user will then be asked to detach these conflicting profiles from the site or cancel his changes.

8.5.2. Editing configuration variables

Configuration variables allow making scripts and configuration elements generic. A variable can be associated with a command value or a configuration parameter.

To do so, insert a code where the value of the command or the configuration parameter should be.

The example below is based on a particular object from the object database, which consists of defining a server. This object is used in the filter rules of each equipment in order to allow access to this server. This server has the same function on all sites but its IP address is different. We will therefore use a variable whose value will depend on the value of the variable defined for each equipment.

```
myServer={$IPAddress_MyServer}
```

When updating the equipment, NETASQ Centralized Manager will substitute {$IPAddress_MyServer} with the data that has been defined at the equipment level via the management of configuration variables.

1 To manage configuration variables, go to the menu `General\Edit Configuration variables`, the following screen will appear:

2 Click on [+]. A new line will appear in the list of variables

3 Enter the name and the value of the variable.

⚠ **WARNING**

Several variables with the same name cannot be created. Special characters are prohibited. Only alphanumeric characters and "_" are allowed.

ℹ **NOTE**

The name of the variable has to be the same as the one used in the configuration element or the command script.

4 Validate the creation of variables by clicking on "Save variables". The administrator will then be redirected to the equipment's home page

⚠ **WARNING**

After saving them, the configuration variables will be switched to the database of the configuration generation engine "SecEngine". Switching over from one database to another may last a while. As such, the script results may appear to be unresolved.

From the variable management page, the administrator will also be able to:

- Delete some or all configuration variables
- Export configuration variables to an XML file that can be stored in the storage area of the user's computer
- Import configuration variables from an XML file saved beforehand in the storage area of the user's computer

8.5.3. Editing the configuration files

Editing the configuration allows the administrator to configure or overload the configuration of an equipment. In the case of an overload, the equipment must first be attached to a configuration profile).

By selec ting this action in the menu `General\Edit configuration files` (or the button in the "Information" tab, the following screen appears:

In the above capture, the configuration elements generated from the profile attached to the equipment are grayed out. The 2 elements that have been specifically associated with the equipment appear in black.

> ### 🛈 NOTE
> Even though the equipment has configuration elements attached by its configuration profile, you will notice that the checkboxes of directories and files are not selected. Indeed, when managing from an equipment, configuration elements cannot be changed.

For a similar configuration element, it will be the element specified at the equipment level that will be deployed instead of the one at the profile level.

The operating mode is the same for the configuration profile (see 7.2.1 Creating a configuration profile)

It is possible to attach and detach configuration files, scripts, licenses, software versions, certificates of an external PKI or imported data from an equipment. These data are available in the repository either at the general level or at the level of the equipment group that the equipment belongs to.

8.5.4. Duplicating the equipment

NCM provides a convenient way to duplicate the equipment. Even though this procedure retains most of the parameters that have already been defined for the original perimeter, many parameters are still private, such as the attachment of profiles.

1 By selecting this action from the menu `General\Duplicate the equipment`, the following screen will appear:

2 Fill in all the fields needed for duplicating the equipment

3 Click on "Validate" to finish creating the duplicated equipment

8.5.5. Deleting the equipment

The very last phase of an equipment's life cycle is of course its destruction. This operation consists of:

- Detaching the device from all the profiles to which he was attached.
- Keeping a record for billing
- Deleting from the database all information relating to this equipment
  A window asks you to confirm deleting the equipment.

8.5.6. Pre-configuring the equipment

The pre-configuration of an equipment consists of preparing the equipment so that it can be contacted by NETASQ Centralized Manager when it is activated. To do so, you will need to send a certain number of commands to the equipment which is in factory configuration. This is generally referred to as "staging".

To ease this deployment phase, NETASQ Centralized Manager offers a means that consists of provisioning the set of commands that will allow the preparing operator to pre-configure the equipment.

By selecting this action from the menu `General\Duplicate the equipment`, the administrator will be asked to save a file in his computer's storage area. This file is an archive that contains a command file and an executable that allows sending commands over the equipment, which must be directly connected to the operator's computer.

There are 2 types of pre-configuration that depend on the operating system of the operator's computer - Win32 or Linux.

8.5.7. Activating the equipment

This is step 3 in the life cycle of an equipment. At the end of this step, the equipment will be in the monitoring and maintenance phase. This step requires the equipment to be physically linked to the network, allowing NETASQ Centralized Manager to update it with the final configuration.

The equipment can be activated in the menu `General\Duplicate the equipment.`

8.5.8. High availability

NETASQ Centralized Manager offers several means of managing equipments configured in high availability.

To create a set of equipments in high availability, you must first create the first equipment by following the standard procedure.

Next, you will need to follow this procedure:

1 Go to the menu `General\ High availability`.

The following page will appear:

PRIMARY EQUIPMENT INFO:		
Serial Number		

SECONDARY EQUIPMENT INFO:		
* Name:		
Serial Number		

HA CONFIGURATION:		
HA Interface:		
HA Secundary Interface:		
HA Address:		

Cancel   Validate

* This field can only include characters from the list: a..z, A..Z, 0..9, space, ', -, à, â, ç, è, é, ê, ë, ô, ï, ù, û, ü

2 Fill in all the necessary fields for the creation of the second equipment.

3 Click on "Validate" to show the screen summarizing the high availability information.

The administrator can then click on "Manage the equipment" to browse to the home page of the equipment that has just been created.

8.5.9. Other actions

The general menu of the equipment view allows launching various maintenance actions on the equipment:

- Rebooting the equipment
- Renewing certificates
- Updating the configuration
- Updating the license
- Updating the firmware

8.6. Supervision Menu

The general menu of the equipment view is presented as follows:

8.6.1. Managing equipment modifications

By selecting this option (via the previous capture), the following screen will appear:

[1] To conduct a comparison, you need to select 2 revisions from the from.

[2] Next, click on "Compare".

[3] Next, select the file you wish to look up.

4 You will reach a screen that compares the last two revisions:

8.6.2. Events of the week or the month

NCM gathers security and operating events from the managed equipments when the "Silver Monitoring" or "Gold Monitoring" service is enabled.

8.6.3. Correlation of the curve

NCM offers a log correlation feature, allowing various problems to be analyzed, such as application errors due to network disconnections, traffic congestion or other issues. The "Silver Monitoring" and "Gold Monitoring" services have to be enabled on the administered equipment in order to allow the correlation.

The correlation page is illustrated with graphs for different event categories. Information is specific to the equipment and concerns:

- Availability
- CPU load
- Network traffic
- RTT and TTL
- Operating duration

The user can choose the time range for events correlation

8.6.4. Full activity report

This menu provides information on the equipment's activity.

They are classified in sections:

- General information about the system
- Network interface configuration
- Traffic statistics
- cpu
- uptime
- IKE SA
- RTT/TTL
- Antivirus
- Antispam
- URL
- Firewall
- QoS
- Availability

8.6.5. Asset management

NCM directly maintains information on assets from managed equipments. NCM can retrieve information such as the hardware type, the hardware version, license expiry dates and similar information.

8.7. Commands for updating a HA cluster

The aim of this section is to briefly describe the actions that NETASQ Centralized Manager has to perform in order to activate or configure the update of a high availability cluster.

1 NCM connects to the active equipment in the cluster and restores the saves configuration.

2 Once the restoration is complete, NCM will reboot the active equipment.

3 NCM will then attempt to reconnect to the cluster: in general, this will be on the second firewall, which has become the active firewall as the other is rebooting.

4 When NCM succeeds in connecting to the cluster, it will then periodically check the status of the firewall that has just been updated and wait until it is available.

5 As soon as this firewall is available, NCM will swap the equipments: the active firewall becomes passive and vice-versa, the passive firewall becomes active.

6 After the cluster us swapped, NCM will disconnect and reconnect to the cluster, but this time it has to go back to the first firewall: the one that has been updated.

7 It will then execute a post-configuration script if there is one.

NETASQ Centralized Manager will then launch the synchronization of the configuration on the passive equipment of the cluster and reboot it.

Once these steps are carried out, all the equipments in the cluster will have the same updated configuration.

9. MONITORING

9.1. Introduction

Monitoring screens can be accessed either in the manager view or from the equipment group view.

The only difference is in the number of equipments that can be monitored:
- for a manager: all equipments that belong to groups managed by the manager
- for a group of equipments: all equipments in the group

A new window will open.

9.2 MONITORING Menu

9.3 Monitoring console

9.3.1 Topological view

Go to the menu `Monitoring\Monitoring console.`

9.3.2 Geographical view

The screen shows the existing VPNs in the left column and where the equipment is located on the map.

You can zoom in or out of the view using the sliding rule.

9.3.3 Equipment view

This is a typical page that appears when you click on the equipment:

9.4   Status of equipments

To see the general status of your equipments, go to the menu **Monitoring** > **Monitor equipments of a group**, accessible in global view.

9.5   Statistics of equipments

In the global view, you can also look up your equipments' summary reports (menu **Monitoring** > **Equipments statistics**):

When this option is selected, the following window will appear:

1 First, selected the desired report type:

2 Next, select the "start" date for the report to be generated:

3 Then select the desired time slots:

4 Select an "end" date from the calendar.

5 Click on OK.

The following screen will display the list of all the visible reports, grouped by group name, equipment name and ID:

Enter dates and report type to generate:

| Report Type | CPU | From: | 23/10/11 | 00 H | : | 00 | To: | 16/12/11 | 11 H | : | 08 | OK |

☐ Click to collapse all

Group's name	Equipment's name	ID		
NETASQ	NETASQ_Benelux	NCM112	NETASQ Generic	⊞ Click to show more
NETASQ	NETASQ_Dach	NCM206	NETASQ Virtual appliance	⊞ Click to show more
NETASQ	NETASQ_HQ maste...	NCM110	NETASQ Generic	⊞ Click to show more
NETASQ	NETASQ_HQ2	NCM111	NETASQ Generic	⊞ Click to show more
NETASQ	NETASQ_India	NCM208	NETASQ Virtual appliance	⊟
NETASQ	NETASQ_Italia	NCM181	NETASQ Virtual appliance	⊞ Click to show more
NETASQ	NETASQ_MEast	NCM209	NETASQ Virtual appliance	⊟
NETASQ	NETASQ_Spain	NCM205	NETASQ Virtual appliance	⊟
NETASQ	NETASQ_UK	NCM207	NETASQ Virtual appliance	⊟

6 To display a report, click on the ID that represents it in the third column.

You will arrive at the screen:

| GENERAL ▼ | SUPERVISION ▼ | ASSET MANAGEMENT ▼ | 11:14:43 | ? |

| Status | Asset | Equipment | Network configuration | Configuration files | Sanity Check | Information |

last update: 16/12/2011 11:14:40

PING STATUS	SELECTED EQUIPMENT		MODEL:
🌐	NETASQ_Benelux (NCM112)	🔧 V50-A	

STATUS OF UPDATES

STATUS	UPDATE	LAST UPDATE	INFORMATION
❌	Configuration update	12/12/2011 18:42:20	Local command failed
✔	Certificate renewal	12/12/2011 18:42:19	
⚙	Licence update		
⚙	Firmware update		
❌	Script execution	17/10/2011 18:24:02	SYSTEM LICENCE 200 code=00102e00 msg="Licence have expired" Netasq>

○ day ⦿ week ○ month ○ year ○ custom   Start: 12/11/2011 10:40:30   End: 12/12/2011 10:40:30 ▷
☑ Availability   ☑ Traffic   ☐ Uptime   ☐ CPU   ☐ RTT/TTL

Availability from 09/12/2011 11:14:39 to 16/12/2011 11:14:39

| Sat 10/12 | Sun 11/12 | Mon 12/12 | Tue 13/12 | Wed 14/12 | Thu 15/12 |

■ Up ■ Unreliable ■ Unavailable

Up: 99.8 % Unreliable: 0.2 % Unavailable: 0.0 % Unknown: 0.0 %

Traffic from 09/12/2011 11:14:39 to 16/12/2011 11:14:39

Bytes per second
5 M
0

| Sat 10/12 | Sun 11/12 | Mon 12/12 | Tue 13/12 | Wed 14/12 | Thu 15/12 |

■ Incoming ■ Outgoing

documentation@netasq.com