

# NETASQ Centralized Manager version 1.2

---

## Highlights

---

Centralized management of appliances  
Management of fleet tracking  
Life cycle of appliances  
Automatic update of appliances  
  
Automatic policy deployment  
Easy VPN configuration  
Appliance monitoring

Real-time alert  
  
Role-based administrator management  
Restriction of access to appliances  
Tracking of administrator activity

---

## Compatibility

---

### **NETASQ multi-function firewall**

Version 8.0.x  
Version 8.1.x  
Version 9.0.x

---

### **Hardware compatibility**

NETASQ U Series  
NETASQ NG Series  
NETASQ Virtual Appliance  
NETASQ F Series

---

---

## Version 1.2

---

Features: Major

---

## New features

---

### Graphical interface

#### General points

The NETASQ Centralized Manager web portal offers several views according to the type of data to be managed:

- Manager view
- Appliance group view
- Equipment view
- Profile view

Each view has its own menus displaying the possible actions that can be performed on the information contained.



**The accessible functions depend on the privileges granted to the administrator.**

#### The privileged administrator view

This view on the NETASQ Centralized Manager web portal is only accessible to the platform's privileged administrator. In addition to the features in manager view for all appliances managed by the platform, this view offers:

- The management of administrators of the platform with a dedicated tab that synthesizes information on the administrators created.
- The management of delegation profiles that allow managing roles implemented in the administration team

#### Manager view

This view is the home page that a manager sees when he logs on to the NETASQ Centralized Manager web portal. It synthesizes information on appliance groups managed by the connected administrator and contains 3 tabs:

- **The status tab** lists the groups of appliances by presenting a synthesis of the operational status of the appliances in each group.
- **The information tab** allows finding out the types of services (monitoring, security policy, and VPN profile) configured on the appliances for each appliance group.
- **The asset tab** sets out hardware information (serial number, software version, maintenance type) by appliance group and the validity dates of the software modules on each appliance.

Depending on the actions allowed and configured by the privileged administrator, this view provides access to the following features:

- Managing information relating to the manager
- Creating a group of equipment
- Managing configuration elements
- Tracking the operational status of appliances
- Monitoring console
- Appliance statistics

## Appliance group view

This view is the manager's main management page. It provides detailed information on a group of appliances and contains 7 tabs:

- **The Status tab** shows the appliances' activity curves. These curves are built from logs sent by the appliances and are grouped by type of event:
  - Firewall
  - IPS
  - Antivirus
  - Antispam
  - URL filtering
- **The Equipment tab** lists the appliances of the group and displays their status. It also allows finding out the types of services (monitoring, security policy, and VPN profile) configured on the appliances for each appliance group.
- **The Asset tab** sets out the list of appliances by showing their statuses and hardware information (serial number, software version, maintenance type) and the validity dates of the software modules.
- **The VPN tab** lists the VPN profiles defined at the appliance group level. For each VPN topology, it displays the appliances that participate in it as well as the type of topology (star or mesh). By clicking on the name of a VPN profile, it is possible to access the corresponding profile view.
  -  **NOTE**  
This tab may present VPN topologies including appliances from another group (as in the case of a global VPN).
- **The Monitoring tab** lists the monitoring profiles defined at the appliance group level. For each profile, it sets out the attached appliances. A monitoring profile allows defining the customized monitoring curves and configuring alert thresholds based on the value of SNMP objects. By clicking on the name of a monitoring profile, it is possible to access the corresponding profile view.
- **The Configuration tab** lists the configuration profiles defined at the appliance group level. For each profile, it sets out the attached appliances. A configuration profile is made up of a set of configurations that globally define a security policy. By clicking on the name of a configuration profile, it is possible to access the corresponding profile view.
- **The Planning tab** lists scheduling profiles defined at the appliance group level. For each profile, it sets out the attached appliances. A scheduling profile is made up of execution settings (launch date, frequency) and the set of commands to be sent to the attached appliances. By clicking on the name of a scheduling profile, it is possible to access the corresponding profile view.

Depending on the actions allowed and configured by the privileged administrator, this view provides access to the following features:

- Managing information relating to the appliance group
- Deleting the group of equipment
- Creating an equipment
- Creating a local or global VPN

- Creating a configuration profile
- Creating a monitoring profile
- Creating a scheduling profile
- Tracking changes to the configuration of appliances
- Tracking the operational status of appliances
- Monitoring console
- Appliance statistics

## Equipment view

The appliance view groups information and actions relating to a single appliance. It offers 7 different tabs:

- **The Status tab** presents a set of information relating to the operations launched on the appliance. The following can therefore be viewed:
  - The operational status
  - The status of updates applied: configuration, certificates, software version, specific commands
  - The default curves reflecting the operational status: availability, CPU, running time, response time to commands and traffic
  - Customized curves based on SNMP counters
- **The Asset tab** presents the appliance's hardware and software information
- **The Equipment tab** lists the configuration, monitoring or scheduling profiles to which the appliance is attached. It also sets out the type of monitoring service (Silver, Gold or Mail alert) defined for the appliance.
- **The Network configuration tab** presents the appliance's network information; such as:
  - Data allowing NETASQ Centralized Manager to connect to the appliance
  - Settings indicating the time zone allowed for updates of the appliance
  - The networks defined as protected and which can be defined as traffic endpoints of the VPN tunnel
- **The Configuration files tab** lists the appliance's configuration elements. These elements are either from a configuration profile or directly attached to the appliance.
- **The Sanity Check tab** presents information on the topologies to which the appliance may be attached
- **The Information tab** lists the appliance's localization data as well as the details of the appliance's manager.

Depending on the actions allowed and configured by the privileged administrator, this view provides access to the following features:

- Editing the equipment
- Editing the configuration variables
- Editing the configuration
- Attached profiles
- Duplicating the equipment
- Deleting the equipment
- Pre-configuring the equipment
- Activating the equipment

- Configuring the equipment in high availability
- Creating a planning profile
- Rebooting the equipment
- Renewing the certificate
- Updating the configuration
- Updating the license
- Updating the firmware
- Tracking changes to the configuration
- Accessing log-based activity curves
- Accessing the full activity report
- Accessing the VPN activity report
- Accessing hardware, license and software version history

** NOTE**

Some actions also depend on the status of the appliance's life cycle.

**Profile views**

A profile view allows accessing the profile's management functions. It synthesizes information on the profile's configuration and the status of its updates. 4 types of profile can be identified, each presenting a slightly different view:

- The configuration profile view
- The VPN profile view
- The monitoring profile view
- The planning profile view

**Monitoring console**

The monitoring console offers an overview that allows tracking the operational status of appliances. There are 2 levels of presentation:

- **The global level** offers a synthetic view of all the appliance groups managed. For each group, it presents in a circular diagram the percentage of appliances in a given operational status: active, inactive or not deployed. By clicking on a pie chart, you will access the appliance group level.
- **The group level** presents the operational status of each appliance. Appliances in the group are placed on a map according to their localization. By clicking on an appliance, a detailed window will open. This window displays the appliance's hardware and software data as well as the default monitoring curves.

The group presentation level also shows appliances grouped by VPN topology. By selecting a VPN topology, attached appliances will be highlighted.

**Equipment statistics**

The NETASQ Centralized Manager solution allows viewing the system and security indicator curves for several appliances. These curves are based on the retrieval of SNMP counters and events (logs) on appliances. NETASQ Centralized Manager offers the following curves:

- CPU activity
- Running duration
- Traffic
- Number of VPN tunnels
- Response time

- Availability status
- Security indicators (Firewall, IPS, antivirus, antispam and URL filtering)

After having selected the type of curve and time slot, the administrator will select from the list of appliances that he manages the appliances whose curves he wishes to view.

Appliance statistics can be accessed from the manager and appliance group views.

### **Tracking the operational status of equipment**

Tracking the operational status lists all the appliances managed by a manager. The general status of each appliance is presented, and the administrator can apply the following filters:

- The operational status
- The appliance group
- Name of the appliance

For each appliance, the administrator can also view the default curves of system indicators based on the retrieval of SNMP counters. The curves offered by default on NETASQ Centralized Manager are:

- Availability status
- CPU activity
- Running duration
- Traffic
- Response time
- Number of VPN tunnels

The operational status of appliances can be tracked in the manager and appliance group views.

### **Events on equipment**

The NETASQ Centralized Manager solution allows looking up events (logs) sent by appliances. These events are sent through the syslog protocol. There are 2 types of events:

- **Alarms** are alerts relating to appliances. These may be alerts following the unavailability of an appliance, the loss of a VPN tunnel or the expiry of a license.
- **Logs** concern events that have been generated by appliances. These events are classified by category: Firewall, IPS, antivirus, antispam, URL filtering, VPN and other logs.

For each type of event, NETASQ Centralized Manager offers a monthly and weekly view.

Once the administrator accesses the screen for tracking events, NETASQ Centralized Manager will display 3 tabs that list the associated events:

- Log summary
- Alarm summary
- Details of the day's alarms

For each list the administrator can apply filters by category and by severity. By selecting an element from the list, the administrator will access either the raw logs or the details of the alert raised by NETASQ Centralized Manager.

## Managing administrators

### General points

NETASQ Centralized Manager offers a set of features that provide very high granularity in the management of privileges assigned to appliance managers. There are 3 levels of management:

- **Management of administrators** by defining authorized actions and the appliances the administrator can access
- **Definition of administrator roles** by selecting authorized actions
- **Definition of access to equipment** by indicating the appliance groups managed by the administrator

Once a role has been defined, it can be associated with several administrators. Likewise, an equipment group can be managed by several administrators with or without the same role. This granularity in the management of privileges assigned to appliance managers meets teamwork requirements.

All functions for managing administrators, roles and access to appliances are reserved for the privileged administrator. This user also has access to a detailed report that lists all actions performed by administrators of the platform.

### Management of administrators

The management of administrators allows managing users on the NETASQ Centralized Manager platform. Each administrator is associated with a delegation profile, his role and one or several appliance groups.

Once an administrator has been created, he will use the login identifiers to benefit from the features of the NETASQ Centralized Manager platform. The actions he can perform are defined by the role assigned to him.

The functions for managing administrators allow:

- Listing the administrators of the platform
- Creating an administrator
- Modifying an administrator's information and login details
- Modifying the appliance groups managed by an administrator
- Deleting an administrator

#### NOTE

The role of an administrator can be modified in the management module for delegation profiles.

### Definition of roles

The roles of administrators are managed using delegation profiles. A delegation profile is made up of a set of authorized actions. Each of these actions appears as a checkbox in the graphical interface. These actions are grouped by the type of data that can be managed:

- Monitoring elements
- Appliances
- Management profiles (configuration, monitoring, scheduling)
- Configuration elements (security policy, data elements, software, license, external certificate authority and CLI commands)
- Appliance groups
- VPN topologies

A role necessarily contains actions relating to monitoring. This is the role with the fewest privileges.

Each group of management data type is made up of a set of checkboxes representing the actions allowed by the role. Even though there are several subtle differences between each action according to the type of data to which it is attached, categories of actions can still be defined and grouped by the type of data to be managed:

- Management profiles, configuration elements and appliance groups are associated with simple actions such as: creation, edition, deletion and duplication for some.
- Appliances, in addition to these simple actions, have specific actions such as: the management of configuration variables, access to pre-configuration commands, activation, high availability management, rebooting the appliance or even access to VPN information.
- VPN topologies, in addition to these simple actions, have specific actions such as: the renewal of certificates or updates to the configuration

Once a delegation profile (a role) has been defined, it can be associated with an administrator. Likewise, during the creation of a manager, the privileged administrator can choose it using a drop-down list that displays all delegation profiles on the platform.

### **Access to equipment**

Access to appliances can be managed in an administrator's management screen. This access can be configured appliance group by appliance group. By granting access to an appliance group, the administrator authorizes access to all appliances in this group. Access to one or several appliance groups can be configured by selecting from the list of appliance groups the groups that an administrator can access.

## **Managing equipment**

### **Life cycle of equipment**

The NETASQ Centralized Manager solution allows managing NETASQ appliances in order to ensure their maintenance, the follow-up of their configuration and their monitoring. In order to facilitate the tracking and management of appliances, NETASQ Centralized Manager manages the statuses of appliances according to their life cycles.

The general life cycle of a NETASQ appliance in NETASQ Centralized Manager can be described in the steps below:

- **Step 1: Creation of the equipment:** By entering the information that would allow NETASQ Centralized Manager to connect to the appliance, it will be created via the web portal and inserted into the database. During this step, the level of monitoring is assigned to the appliance: Silver, Gold or Mail alert.
- **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 appliance. At the end of this step, the appliance 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 appliance is physically linked to a network, NETASQ Centralized Manager can update it with the final configuration.
- **Step 4: Management and monitoring of the equipment:** Once the appliance 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.

The actions that can be launched on an appliance depend on its status. Therefore, according to the status of an appliance, certain actions are grayed out in the NETASQ Centralized Manager menu.

### **Automatic update**

NETASQ Centralized Manager offers a set of features for managing the configuration of appliances: configuration elements, configuration profile and VPN profile. Modifying one element would cause the automatic modification of appliances attached to these elements.

This automatic update feature can be configured on each appliance. A time slot for updating the firewall can be defined (updating will be prohibited any time outside this time slot). If a configuration element is modified during this time slot, NETASQ Centralized Manager will apply the modification at the beginning of the next time slot allowed for updates.

### **Maintenance operations**

NETASQ Centralized Manager offers various features to facilitate maintenance operations. As such, an administrator will be able to:

- Reboot an appliance
- Update an appliance’s license
- Update an appliance’s software version
- Update an appliance’s configuration
- Renew an appliance’s certificate
- Execute CLI commands through the script
- View changes to an appliance’s configuration

Using various types of profiles (configuration, VPN and scheduling) allows an administrator to launch these operations automatically on a fleet of appliances. Modifications to the configuration can be viewed from the appliance group, thereby providing an overview of all the appliances in a group.

### **Management of configuration backups**

NETASQ Centralized Manager regularly performs configuration backups on all appliances. Using backup information, an administrator will be able to make a comparison with the last update performed with NETASQ Centralized Manager.

This comparison will allow managing local changes to configurations. The management graphical interface for configuration backups also allows selecting the configuration backup versions to compare.

## Configuring equipment

### Operation

The configuration of appliances is made easy by the use of configuration profiles that allow defining a common security policy for several appliances. A profile is made up of a set of configuration elements. NETASQ Centralized Manager allows managing all the configuration elements offered by the NETASQ multi-function firewall.

A configuration profile can only be attached to appliances of the same group. This allows defining one security policy per domain. The use of common configuration elements for several different profiles allows defining a global security policy. Furthermore, the implementation of a global policy is made easy by the use of global configuration elements offered by NETASQ UTM firewalls.

### Specific configuration

NETASQ Centralized Manager also offers the possibility of uploading a common security policy for a given appliance. To do so, the administrator has 2 features:

- **Direct attachment** of configuration elements to the appliance. This is referred to as a specific configuration.

#### NOTE

If 2 configuration elements of the same type are attached to an appliance through a configuration profile and through a specific configuration, the element directly attached to the appliance will pre-empt.

- **Attachment of scripts** in order to launch the execution of the CLI command to refine the configuration. There are 2 types of attachments:
  - Pre-script: commands will be executed before the application of the configuration profile and the specific configuration.
  - Post-script: commands will be executed after the application of the configuration profile and the specific configuration.

### Multi-form configuration

NETASQ Centralized Manager configuration elements support the use of variables in the configuration of an element. These variables are defined by the use of the keyword `{$variable}`. The value that the variable has to take is defined in each appliance. As such, when updating the configuration of an appliance, NETASQ Centralized Manager will substitute the keywords `{$variable}` with the corresponding value.

Each appliance will therefore have specific values while using a global profile.

## VPN Profile

### Configuration wizard

NETASQ Centralized Manager facilitates the configuration of complicated VPN topologies. The configuration wizard simplifies the creation or modification of a VPN topology, which consists of:

- Selecting the appliances participating in the topology
- Choosing the type of topology – star or mesh
- Defining the appliance at the center of the star (for star topologies)

- Choosing the certificate authority that manages the certificates implemented by the topology
- Refine the traffic endpoints of each appliance

** NOTE:**

By default the wizard selects all the networks defined as protected, but offers the possibility of excluding some.

Once the administrator has confirmed the creation or modification of a VPN topology, NETASQ Centralized Manager will calculate the VPN configurations of each appliance and will automatically launch their update.

### Complex architecture

The implementation of a complex VPN architecture is possible by combining several VPN topologies that share common appliances. It is possible, for example, to deploy a mesh topology in which each appliance is the center of a star topology and allows each protected satellite network to access protected networks on another satellite.

### Internal and external PKI

NETASQ Centralized Manager embeds a certificate authority. This authority is automatically implemented by default to guarantee the security of VPN topologies. An appliance participating in a VPN topology authenticates by using the certificate created and automatically pushed by the NETASQ Centralized Manager certificate authority.

The internal PKI's management features allow:

- Listing the expiry dates of certificates of appliances
- Renewing the certificate of an appliance
- Renewing the certificates of appliances in a VPN topology

NETASQ Centralized Manager also offers the possibility of authenticating appliances of a VPN topology by using certificates from an external certificate authority. Once the certificates have been imported, NETASQ Centralized Manager can associate them automatically to the appliances.

Several external certificate authorities can be managed. The authority is chosen using the radio button in the wizard for creating a VPN topology. NETASQ Centralized Manager therefore supports different VPN topologies that use different certificate authorities.

## Monitoring profile

Monitoring profiles allow defining additional monitoring parameters besides those provided by default by NETASQ Centralized Manager. The default monitoring parameters offer the following features:

- Checking the availability of appliances by sending pings
- Display of an appliance availability curve
- Regular retrieval of SNMP counters in order to build the following curves:
  - CPU activity
  - Running time
  - Traffic
  - Response time to pings
  - Number of VPN tunnels

The creation of an additional monitoring profile consists of defining the SNMP object identifier (OID) and the type of curve to associate. By associating the profile with an appliance, the additional curves will automatically be available in the appliance view.

The use of monitoring profiles also allows defining a threshold value. In the event the threshold is exceeded for a given SNMP counter, an alert will be generated. For appliances configured in “Gold” monitoring, this alert will be relayed to the appliance’s manager.

**i NOTE**

A monitoring profile can only be used for defining alert thresholds.

## Scheduling profile

### Principles

A scheduling profile allows scheduling the execution of CLI commands on a fleet of appliances. CLI commands offer the same management and maintenance functions as the appliance management graphical interface. As such, an administrator will be able to use scheduling profiles to schedule maintenance operations on his appliances.

The creation of a scheduling profile consists of:

- Choosing the CLI commands to execute, referred to as “actions”. These commands are set out in the form of scripts. A script may contain one or several CLI commands. The administrator may choose to embed one or several scripts into his scheduling profile
- Defining time settings for scheduling. The administrator can configure:
  - The time and/or the day CLI commands will begin executing
  - Execution frequency by selecting one of the following values: Now, Only once, every day, every week, every month.
  - The date on which scheduling ends
- Selecting the appliances to associate with the scheduling profile

Once the profile has been created, NETASQ Centralized Manager will launch the execution of CLI commands on all appliances attached to the profile.

In order to facilitate the use of identical commands on different appliances, NETASQ Centralized Manager supports the use of variables in scripts. These variables are defined by the use of the keyword *{ $\$$ variable}*. The value that the variable has to take is defined in each appliance. As such, when executing the CLI command on an appliance, NETASQ Centralized Manager will substitute the keywords *{ $\$$ variable}* with the corresponding value.

### Tracking operations

The scheduling profile view on the NETASQ Centralized Manager web portal lists the profiles that have been created. By clicking on a profile, the administrator can look up the profile’s settings and access execution reports.

For each appliance associated with the profile, NETASQ Centralized Manager displays a status indicating whether the CLI commands could be executed as well as an execution status corresponding to the results of various actions. Furthermore, the administrator can access the CLI command execution report on an appliance. This report presents all the CLI commands executed as well as the appliance’s return code.

## Monitoring

### Levels of monitoring

NETASQ Centralized Manager offers 3 types of appliance monitoring:

- **"Silver"** offers tracking of the operational status of appliances
- **"Gold"** allows collecting appliance logs in order to compile activity graphs
- **"Mail alert"** takes charge of raising real-time alerts on major incidents that arise on appliances.

The monitoring level is defined on appliances. It is therefore possible to define different monitoring levels on various appliances.

### Silver Monitoring

The "Silver" monitoring level offers a set of features to track the operational status of appliances:

- A display of the operational status of appliances measured by regular pings
- A display of the default monitoring curve that makes it possible to track appliance capacities
- The configuration of the monitoring profile

Using pings, NETASQ Centralized Manager determined the operational status of appliances. There are 3 statuses:

- **Available:** represented by a green icon, this status ensures that the appliance has responded to the last ping
- **Uncertain:** represented by an orange icon, this status indicates that the appliance did not respond within a certain time limit, which can be configured in console mode.
- **Uncontactable:** represented by a red icon, this status indicates that an appliance in an uncertain status still has not responded within a certain time limit, which can also be configured in console mode.

### Gold Monitoring

The "Gold" monitoring level relies on the receipt and treatment of logs sent by appliances. Based on these events, NETASQ Centralized Manager classifies them and suggests activity curves by event type. There are 6 types of events:

- Firewall
- IPS
- Antivirus
- Antispam
- URL filtering
- Other types of events

NETASQ Centralized Manager also provides events curves relating to major events that may arise on an appliance (loss of connection, expiry of license, loss of VPN tunnel, etc). This is an "Alarm" event.

The NETASQ Centralized Manager web portal also displays, for each event type, 4 top 5 lists – 2 daily and 2 monthly, on:

- Appliances that generate the most events, by type of event
- The most frequent messages by type of event

Lastly, collected logs can be looked up from the NETASQ Centralized Manager web portal. This is facilitated by the use of filters that allow restricting the display to a single type of event.

### **Mail alert**

The Mail alert monitoring level ensures real-time tracking of major events on appliances. These are “Alarm” events that group:

- Loss of connection with an appliance
- Retrieval of connection with an appliance
- Modification of a dynamic IP address
- Loss of a VPN tunnel
- Expiry of a license
- ...

When the alarm appears, NETASQ Centralized Manager sends an e-mail to certain recipients, which are configured through the web portal. They are:

- The person in charge of the NETASQ Centralized Manager platform
- The administrator(s) attached to the group that the appliance belongs to
- The contact person configured for the appliance group
- The e-mail address defined during the creation of the appliance