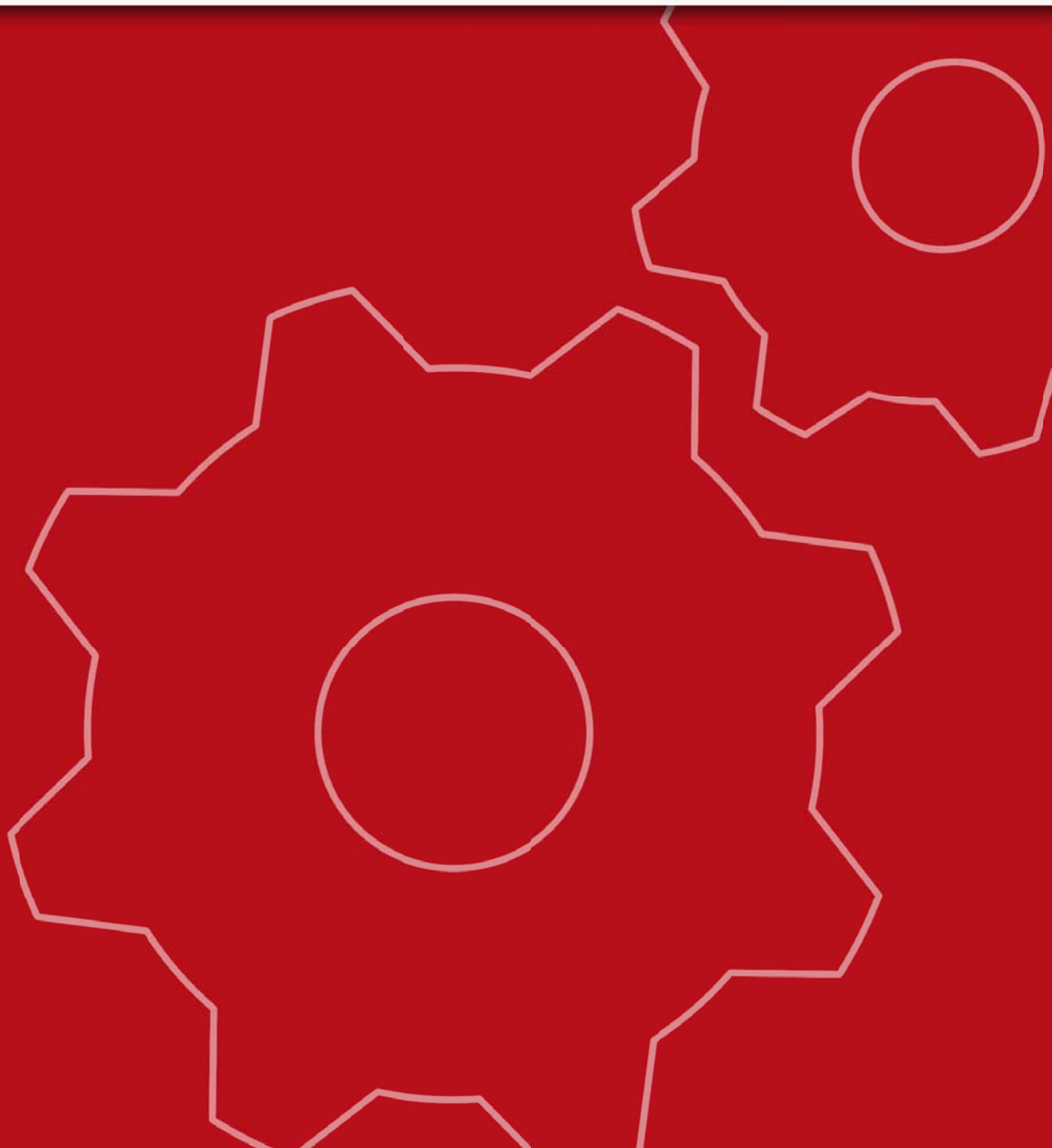




NETASQ  
**UNIFIED MANAGER**



# **NETASQ UNIFIED MANAGER**

## **V. 7.0.2**

### **USER CONFIGURATION MANUAL**

#### **(NTP)**

Reference : ENCH0803\_NTP-V7.0.2  
Created : March 2008  
Modified : March 2008

## Introduction

This protocol allows synchronizing clients' and servers' real-time clock. NTP is based on UDP, which makes it an unconnected protocol. In fact, it is an upgraded version of Time Protocol and ICMP Timestamp Message protocols and an appropriate replacement.

NTP provides time synchronization mechanisms with a nanosecond precision, while preserving an unambiguous date. This protocol includes the possibility of specifying information on the precision and error estimated in the local clock as well as indications on the reference clock with which it can synchronize.

## Using the NETASQ Firewall's NTP service

NTP is based on a hierarchical structure in which the firewall is only a client.

## Operation

➔ The NTP service has to be activated in order to be used, via the menu **Services\NTP**.

### Remark

The other elements in the window will be enabled or disabled depending on whether NTP has been enabled.

The NTP service configuration window comprises two sections:

- The **servers** tab: list of public or private NTP servers.
- The **keys** tab: list of authentication keys.

### Remark

A star will appear in the window's title bar when changes are made to the configuration to inform the user that data may have been changed.

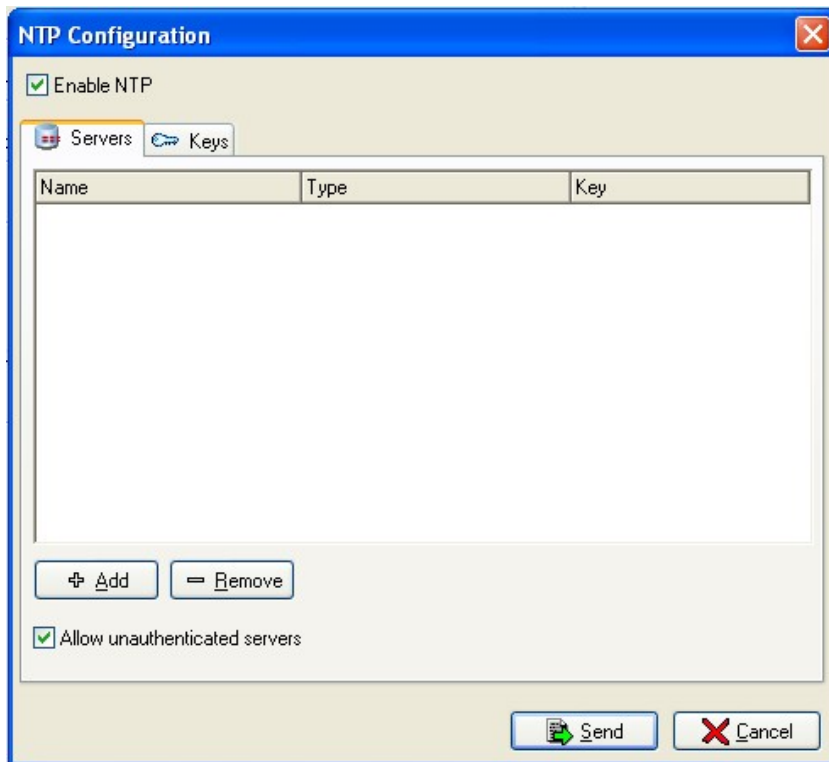
## Servers

This window allows adding, editing or deleting NTP servers and allows assigning keys to them if necessary.

It comprises 3 columns: the object name, type (host, address range or group) and the associated key where applicable (with an indication of "none" or a number between 1 and 15, or "invalid" if the associated key no longer exists).

Authentication keys can be selected in this window, or deleted by selecting “None” in the drop-down list.

A key cannot be used more than once in the table.



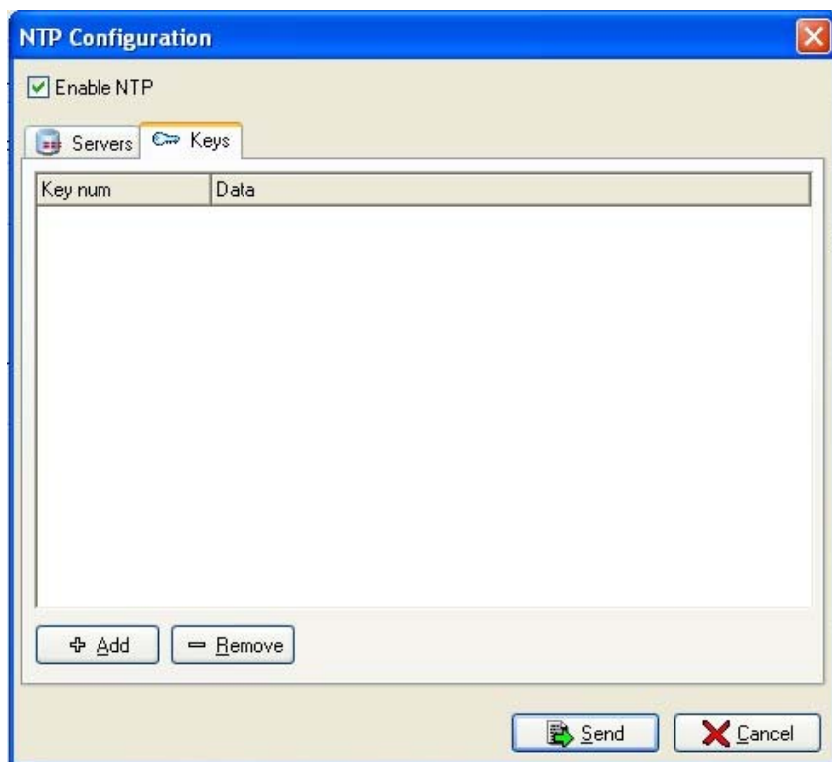
<b>Servers</b>	List of public or private NTP servers to which the Firewall can connect to synchronize.
<b>Add</b>	Accesses the objects database in order to select servers.
<b>Remove</b>	Deletes a selected server from the table.
<b>Allow unauthenticated servers</b>	This option allows you to authorize the use of servers which do not request authentication (i.e., with no associated keys).

## Keys

This tab allows you to configure keys for authentication with NTP servers. This key is visible if you connect with modification rights, otherwise it is masked.

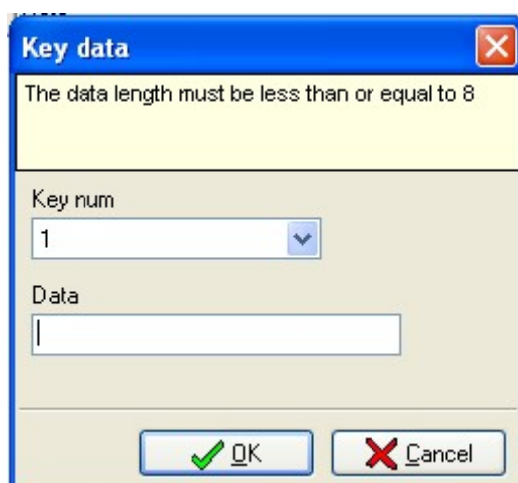
Keys are defined by a number ranging from 1 to 15. Any attempt to add a sixteenth key will cause an error message to appear.

Keys can be modified directly in the table. However, if the key key is longer than 8 characters, an error message will appear. The number of the key can also be modified. In this case, only numbers that have not yet been assigned will be suggested.



---

**Add** The following cindow appears when you click on this button:



Indicate a number for the key then indicate a value in the "Data" field.

** Remark**

The length of the data has to be 8 or less.

---

**Delete** Deletes a selected key from the table.

---

## ***Sending***

By clicking on **Send**, data will be checked and sent.

The checking stage allows determining whether the keys associated with each server actually exist. If they do not, an error message will appear and sending will be aborted.

If the option "Allow unauthenticated servers" has not been selected, an error message will appear if there are servers that do not have associated keys.

Enabled NTP configurations cannot be sent if no servers have been indicated.

If the checking procedure runs smoothly, the configuration can be sent.