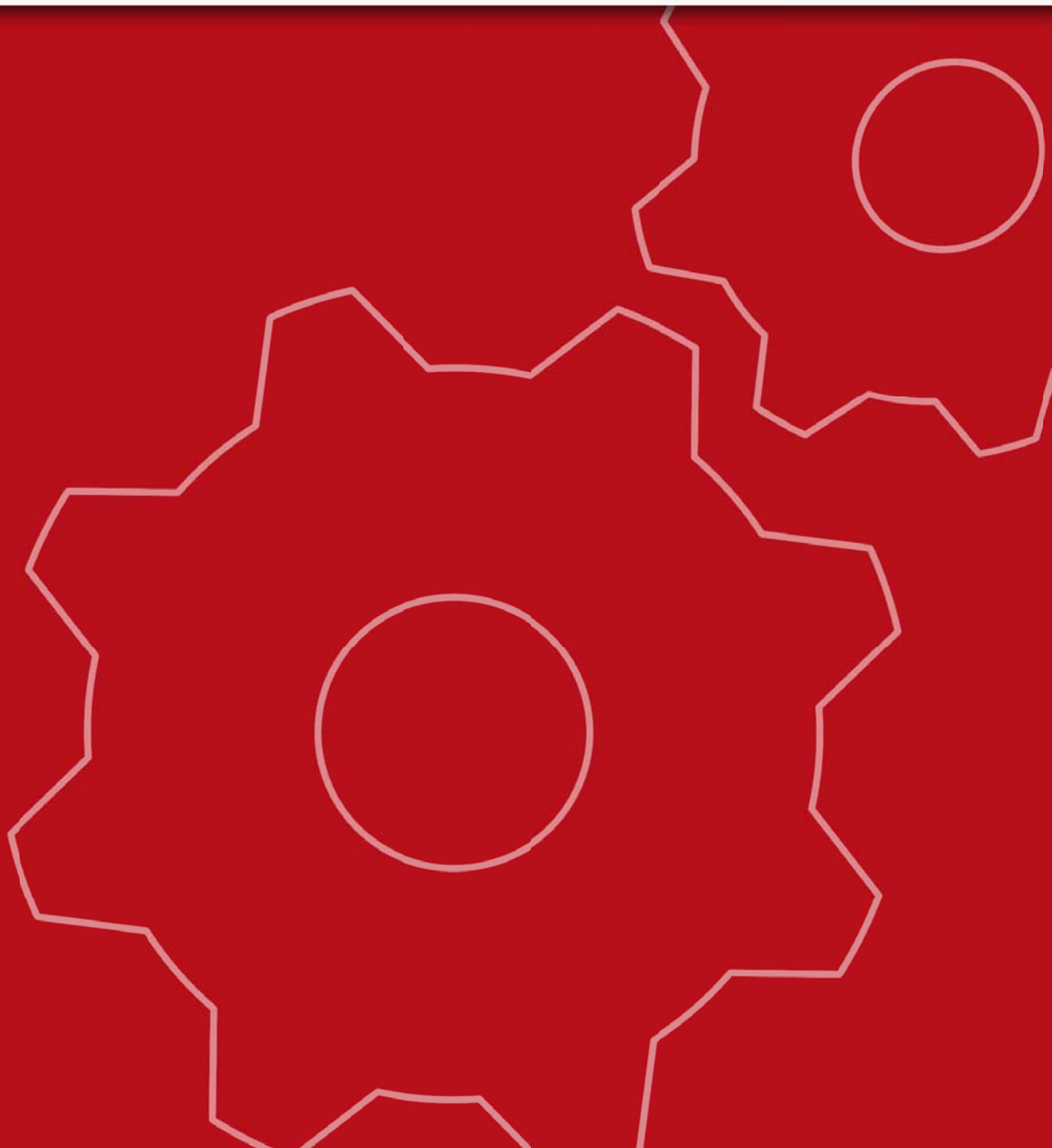




NETASQ
UNIFIED MANAGER



NETASQ UNIFIED MANAGER

V. 7.0.2

USER CONFIGURATION MANUAL

(Secure configuration)

Reference : ENCH0803_SECURE-CONFIGURATION-V7.0.2
Created: March 2008
Modified: March 2008

Introduction

Highly sensitive information is contained in the configuration of a firewall, information that exposes network activity and ways to bypass this network's protection mechanisms. Such data can be protected by using the encryption features found in the configuration files of the Firewall.

As these encrypted configuration files can only be decrypted with a secret key shared by the Firewall and the administrator, it is the administrator's duty to prevent its theft and the illicit use of his Firewall. Without decrypting these files, the Firewall cannot be used.

Operation


To implement this technology, NETASQ offers the possibility of using USB keys that contain exchanged secret keys. Without this key, the Firewall cannot be started. Once the configuration has been loaded into memory, the USB key can be removed in order to keep configuration files confidential, but will be necessary for the next connection.

Warning

USB keys are compatible with this feature, and only USB keys manufactured and distributed by NETASQ are supported for this feature.

This feature is only available for products that have an operational USB port.

Configuration

 Secure configuration features can be enabled via the menu **Firewall\Secure configuration** in the menu bar in NETASQ UNIFIED MANAGER graphical interface.



The options for secure configuration are as follows:

Secure Button that activates secure configuration. Once it is activated, the

configuration	Firewall's configuration files will be encrypted, therefore the USB key is essential for decrypting its configuration.
Key status	Value displayed by the Firewall indicating the current status of the key that will be used for storing the decryption secret. There are three different statuses: <ul style="list-style-type: none"> ● USB key not found: the key has not been inserted in the firewall's USB port or has not been formatted according to its file format ● USB key not initialized: the key has been detected but does not contain the decryption secret for the Firewall configuration, ● USB key initialized: the key has been detected and contains a decryption secret for the Firewall configuration.
Check key	Before displaying the Secure Configuration menu, NETASQ UNIFIED MANAGER checks the key's status. The Check key button refreshes the data on display. <p>If a USB key is inserted after the Secure configuration menu appears, click on the Check key button to refresh data on the key's status.</p>
File to restore	If the key or the secret contained in the key is defective, this backup can then be restored on the same key or on a new key.
Send	Activates secure configuration. Before closing the menu, a path must be specified for backing up the encryption key that was inserted in the USB key.
Cancel	Cancels modified parameters in secure configuration.

Encrypted configuration files

To make it easier to configure, activate and use this feature, the firewall does not offer the choice of encrypting configuration files. By default the files encrypted by the secure configuration feature are:

- Pre-shared keys VPN configuration;
- LDAP directory configuration;
- Authentication configuration;
- Keytab file in SPNEGO configuration;
- The private key of the PKI's certification authority;
- PKI configuration;
- Certificates signed by the PKI's certification authority.

Using secure configuration

The configuration encryption feature can only be used with products that have a USB port, and the administrator must have a compatible USB key. Contact your NETASQ partner to obtain a USB key.

Once the secure configuration feature has been enabled, the USB key containing the secret is necessary for starting up the appliance. After the firewall has booted, the administrator can remove the key. The configuration of the appliance is secure.


The procedure for activating secure configuration is as follows:

- 1 Select the configuration menu **Firewall\Secure Configuration**, which will open the secure configuration window.
- 2 Connect the USB key.
- 3 Click on **Test key**, which should display the key status as “USB key not initialized”.
- 4 Check the option **Secure configuration**
- 5 Click on **Send** to activate secure configuration.
- 6 The key is now initialized, Firewall configuration files are encrypted and you will be asked to specify a path for copying the backup file.

Restoring a defective key or creating a backup key

When initializing the USB key containing the secret shared with the firewall, the firewall will back up this secret. It will then be possible to perform backup operations on USB keys.

The procedure for restoring a USB key is as follows:

- 1 Select the configuration menu **Firewall\Secure Configuration**, which will open the secure configuration window.
- 2 Connect the USB key.
- 3 The key status should either be “USB key not initialized” or “USB key initialized”.
- 4 The option “Secure configuration” should already have been selected.
- 5 Select the backup file to restore by clicking on the icon .
- 6 Click on **Restore** to restore the USB key.

7 Click on **Send** to end the restoration operation.


The procedure for creating a backup USB key is as follows:

1 Select the configuration menu **Firewall\Secure Configuration**, which will open the secure configuration window.

2 Connect the new USB key.

3 Click on **Test key**, which should display the key status as “USB key not initialized”.

4 The option **Secure configuration** should already have been selected.

5 Select the backup file to restore by clicking on the icon .

6 Click on **Restore** to restore the USB key.

7 Click on **Send** to finish creating the backup USB key.