TECHNICAL NOTE
STORMSHIELD NETWORK SECURITY

INITIAL CONFIGURATION FROM USB KEY

Product concerned: SNS 3.9 and higher versions, SNS 4.x

Document last updated: July 9, 2024

Reference: sns-en-initial_configuration_from_usb_key_technical_note

Table of contents

Change log

Date	Description
July 9, 2024	- SNS 4.8 release. - "*certimport*" and "*crlimport*" operations added.
April 10, 2024	- Name of "*initTPM*" operation corrected.

Getting started

This technical note explains how one or several SNS firewalls, either in their initial factory settings (new equipment) or reset to factory settings via the *reset hardware* button, can be updated and configured using a USB key.

Installation sequence

When the SNS firewall starts up on a USB key, the files found on the USB key will be imported/installed/run automatically in the following sequence:

No.	Description of the step
1	License (".licence" extension)
2	Firmware update (".maj" extension)
	Firewall restart **IMPORTANT** The USB key must be removed when the firewall restarts.
3	Configuration backup file (".na" extension)
4	SMC connecting package (".pack" extension)
5	Certificates (".p12" extension), from SNS version 3.9.0 onwards
6	Password of the *admin* account (".pwd" extension), from SNS version 3.9.0 onwards
7	Dynamic routing configuration files (".bird" and ".bird6" extensions), from SNS version 3.10.2 or from SNS version 4.1.1
8	Additional configuration files (".csv" extension), from SNS version 3.9.0 onwards

If any of the files in the list above is not on the key, the corresponding step will simply be skipped.

Preparing files

This section specifies the format and designation of files that can be imported.

You can use a single USB key for the initial configuration of several firewalls. As a result, several files of the same format can be found on the same USB key.

Licenses (*.licence*)

Each firewall has its own license file.

You can obtain the licenses of your SNS firewalls from your MyStormshield are in **Products > Product management**. For more information, see the section Downloading a product's license file in the *Managing registered products* guide.

Name

```
Firewall_Serial_Number.licence
```

EXAMPLES
SN320A000000000Z.licence
SN320B000000000Z.licence

Software updates (*.maj*)

To download SNS firewall software update files:

1. Log in to your MyStormshield area.
2. Go to **Downloads > Stormshield Network Security > Firmware**. If necessary, select a version branch as well, to narrow down the list.
3. Locate the version(s) that you wish to install. To do so:
   - Refer to the version release notes to find out what the SNS versions contain,
   - Ensure that the version is compatible with your firewall model. If several firewalls have been configured using the same USB key, you may need several software update files (different firewall architectures, different preloaded software versions, etc).
   - If a version has several patch versions, always choose the most recent so that you benefit from the latest functional patches and bug fixes,
   - Use versions that have not yet expired. For more information, refer to the Network Security & Tools product life cycle guide.
4. To choose the desired version, click on the name that matches the firewall model to download its software update file (*.maj*).

Name

EXAMPLES
fwupd-4.8.1-SNS-armv6-S.maj
fwupd-4.8.1-SNS-amd64-M.maj
fwupd-4.8.1-SNS-amd64-XL.maj

IMPORTANT
During the installation sequence, the USB key must be removed when the firewall restarts.

If the increment between the major firmware version of the firewall in factory settings and the software versions found on the key is lower than 2 (e.g., firewall in version 3.9.0 and firmware 4.0.0 on the key), only the higher software version on the key will be installed. If this is not the case, an intermediate firmware version must be provided on the key so that an automatic update can be carried out in stages (e.g., firewall in version 2.14.0 and firmware versions 3.9.0 and 4.0.0 on the key).

Configuration backups (*.na)*

You can create configuration backup files from the active firewall's web administration interface, By enabling in **Configuration > System > Maintenance > Backup.**

Name

If the configuration is the same on all firewalls:

```
default.na
```

Otherwise:

```
Firewall_Serial_Number.na
```

EXAMPLES
SN310A00000000Z.na
SN310B00000000Z.na

SMC connecting packages (*.pack)*

If the SNS firewall is going to be managed from a Stormshield Management Center server, a connecting package (*.pack* file) must be generated from the SMC server. For more information, see the section Connecting firewalls in factory configuration to the server in the *SMC administration guide.*

IMPORTANT
Ensure that the firewall's connecting package **does not include** any network configuration. Otherwise, the package will overwrite the network configuration that was restored using the *.na* file.

Name

```
Firewall_Serial_Number.pack
```

EXAMPLES
SN310A00000000Z.pack
SN310B00000000Z.pack

Certificates (*.p12*)

Certificates can be imported from SNS version 3.9.0 onwards.

Certificates must be in PKCS#12 format (encrypted file that contains the firewall's certificate and its private key). These files must be exported from the workstation that manages the organization's PKI.

If your firewall is equipped with a TPM, and you wish to protect the private key contained in the PKCS#12 file, refer to the section ***p12import* operation**.

Name

The names of PKCS#12 files for a specific firewall consist of the firewall's serial number followed by an optional suffix, and the extension "p12".

```
FirewallSerialNumber.p12
FirewallSerialNumber_text.p12
```

EXAMPLES
SN310A000000000Z.p12
SN310A000000000Z_cert1.p12
SN310A000000000Z_cert2.p12
SN310B000000000Z.p12

admin account password (*.pwd*)

The *admin* account password can be deployed from SNS version 3.9.0 onwards.

File

- Text file containing a single unencrypted string in UTF-8 format.

Password policy

- The length of the password has to be between 8 and 128 characters,
- The password must comply with rules on allowed/prohibited characters on the SNS firewall, otherwise, the *admin* account will not be able to connect to the firewall. For more information, refer to the **Allowed or prohibited names** section in the *SNS user manual*.
- The password must comply with the password policy that was restored using the configuration backup file, otherwise the password will not be applied.

Name

For a password that differs from one SNS firewall to another:

```
Firewall_Serial_Number.pwd
```

For the same password across all SNS firewalls (not recommended):

```
default.pwd
```

EXAMPLES
SN310A000000000Z.pwd
SN310B000000000Z.pwd

Dynamic routing configuration (*.bird* and *.bird6*)

Dynamic routing configuration files can be imported from SNS version 3.10.2 or 4.1.1 upwards.

Every firewall that uses a dynamic routing configuration has:

- A ".bird" file for IPv4 networks and routes,
- A ".bird6" file for IPv6 networks and routes.

These files can be retrieved via SSH on an active firewall in the folder */usr/Firewall/ConfigFiles/Bird/*.

The Bird configuration can also be displayed in the SNS firewall's administration interface in **Configuration** > **Network** > **Routing**, *Dynamic routing* tab.

Name

```
Firewall_Serial_Number.bird
Firewall_Serial_Number.bird6
```

EXAMPLES
SN310A00000000Z.bird
SN310A00000000Z.bird6

IMPORTANT
To ensure that the dynamic routing configuration is used, in addition to Bird files, you have to enable the Bird and Bird6 modules on the firewall, by using an additional "*.csv*" configuration file, which will make it possible to run a *setconf* operation. For more information, see Additional configuration files.

Additional configuration files (*.csv*)

As of SNS version 3.9.0, additional configuration operations may be performed through one or several CSV files. These files make it possible to build a firewall cluster or change a value in a firewall configuration file.

Files with *.csv* extensions have to be in UTF-8 format. **All** *.csv* files found on the USB key will be run during the installation sequence.

General structure of additional .csv configuration files

- Each line must contain an operation,
- Each line corresponding to an operation is defined according to the following nomenclature:
  ```
  "serial | any" ,"operation", ["parameter 1", etc.]
  ```
  - serial: indicates that the operation must be applied to the firewall associated with the serial number entered,
  - any: indicates that the operation must be applied regardless of the firewall involved,
  - All fields must be separated by commas,
  - Operations and parameters are explained below.
- Lines of comments beginning with the "#" character can be inserted.

setconf operation

The *setconf* operation can be used to:

- Change the value of a field found in a particular section of a configuration file,
- As of version SNS 3.10.1: add a full line to a section of a configuration file.

When a comma is needed in any of the parameters in the command, the value of the parameter must be enclosed in quotation marks.

Setting the value of a field

Format

```
"serial | any", setconf, "file", "section", "field", "value"
```

EXAMPLES
any, setconf, network, ethernet0, Protected, 0
any, setconf, object, Host, gateway, "192.168.0.254, resolve=static"
any, setconf, Bird/global, bird, state, 1

Adding a full line (as of SNS version 3.10.1)

Format

```
"serial | any", setconf, "file", "section", "line"
```

EXAMPLE
any, setconf, route, StaticRoutes, "MyNetworkObject,my-if->MyGW"

delconf operation

The *delconf* operation deletes a field found in a particular section of a configuration file. If the field is not specified, the whole section will be deleted from the configuration file.

Format

```
"serial | any", delconf, "file", "section", "field"
```

```
"serial | any", delconf, "file", "section"
```

EXAMPLES
SN310A000000000Z, delconf, wiki, Global, Schedule
any, delconf, dns, client

setglobal operation

The *setglobal* operation changes the value of a field found in a particular section of a global configuration file (~/System/global.custom file).

Do note that the firewall must be manually restarted in order to apply any changes made to the configuration using the *setglobal* command.

Whenever this command is used, a warning will be recorded in the relevant log files.

Format

```
"serial | any", setglobal, "section", "field", "value"
```

EXAMPLE
SN310A000000000Z, setglobal, ASQ, BridgeLimit, 9

sethostname operation

This feature is available from SNS version 3.10.2 upwards or 4.1.1 upwards.

The *sethostname* operation changes the value of the following fields in the global configuration file (~/System/global file):

- SystemName: corresponds to the name of the firewall. When high availability (HA) is used, this field corresponds to the system name of the HA cluster.
- SystemNodeName: corresponds to the local name of the system node, so that it can be differentiated from the other nodes in the HA cluster.

Format

```
"serial | any", sethostname, "systemname"
```

```
"serial | any", sethostname, "systemname", "systemnodename"
```

EXAMPLE
any, sethostname, test_hostname, testnodename

createHA operation

This operation makes it possible to initialize a firewall cluster. To do so, the firewall to which the operation applies must have the HA license with the master option.

The network mask used for the HA link must accept at least three IP addresses (in CIDR notation: network mask strictly below 30).

Format

```
"serial | any", createHA, "IP_HA_master", "mask", "interface_name",
"password"
"serial | any", createHA, "IP_HA_master", "mask", "interface_name",
"password", "IP_HA_master_backup", "mask_backup", "interface_name_backup"
```

Parameter	Description
IP_HA_master	IP address assigned to the interface "interface_name" (dedicated to the main HA link).
mask	Network mask of the interface "interface_name".
interface_name	Name given to the interface dedicated to the main HA link.
password	Pre-shared key to secure the connection between members of the cluster.
IP_HA_master_backup	IP address assigned to the interface "interface_name_backup" (interface dedicated to the backup HA link).

Parameter	Description
mask_backup	Network mask of the interface "interface_name_backup".
interface_name_backup	Name given to the interface dedicated to the backup HA link.

EXAMPLES

```
SN310A00000000Z, createHA, 192.168.192.5, 255.255.255.248, HA,
PasswordValue
SN310A00000000Z, createHA, 192.168.192.5, 255.255.255.248, HA,
PasswordValue, 192.168.192.11, 255.255.255.248, HA2
```

joinHA operation

This operation allows a firewall to join a cluster, which must already be initialized. The network interfaces dedicated to HA must be physically connected (active and passive firewalls)

In an RMA hardware return, the exchanged firewall must be removed from the cluster beforehand using the following CLI / serverd commands:

```
ha cluster remove serial="remote"
ha cluster activate
```

For more information on the syntax of these commands, refer to the SNS v3 CLI/Serverd Commands Reference Guide or SNS v4 CLI/Serverd Commands Reference Guide.

The *joinHA* operation uses a third temporary IP address for the connection to the main firewall in the cluster.

Format

```
"serial | any", joinHA, "IP_HA_1", "IP_HA_2", "IP_HA_join", "mask",
interface_name", "password"
"serial | any", joinHA, "IP_HA_1", "IP_HA_2", "IP_HA_join", "mask",
interface_name", "password", "IP_HA_join_backup", "mask_backup",
"interface_name_backup"
```

Parameter	Description
IP_HA_1	First remote IP address tested to reach the cluster.
IP_HA_2	Second remote IP address tested to reach the cluster if IP_HA_1 does not respond, or IP address assigned to the interface "interface_name" (interface dedicated to HA) if the main firewall could be reached via IP_HA_1.
IP_HA_join	IP address that the firewall temporarily uses to reach the cluster.
mask	Network mask of the interface "interface_name".
interface_name	Name given to the interface dedicated to the main HA link.
password	Pre-shared key to secure the connection between members of the cluster.
IP_HA_join_backup	IP address assigned to the interface "interface_name_backup" (interface dedicated to the backup HA link).
mask_backup	Network mask of the interface "interface_name_backup".
interface_name_backup	Name given to the interface dedicated to the backup HA link.

EXAMPLES

```
SN310B000000000Z, joinHA, 192.168.192.4, 192.168.192.5, 192.168.192.6,
255.255.255.248, HA, PasswordValue
SN310B000000000Z, joinHA, 192.168.192.4, 192.168.192.5, 192.168.192.6,
255.255.255.248, HA, PasswordValue, 192.168.192.12, 255.255.255.248, HA2
```

IMPORTANT

The USB key must be removed when the firewall joining the cluster restarts, during the configuration synchronization phase.

initTPM operation

This feature is available from SNS version 3.10.1 upwards or 4.0.1 upwards.

This operation initializes TPM chips by passing the password as an argument, and if the firewall is part of a cluster (high availability enabled), to derive the key from the TPM password so that both firewalls will obtain the exact same key.

The TPM password must comply with the password policy set in the configuration (file ~/ConfigFiles/serverd section PasswordPolicy).

This operation must be performed before attempting to protect any private keys with TPM.

Format

```
"serial | any", initTPM, "tpmpassword"
```

EXAMPLE

SN310A17B0023A7, initTPM, TpmPasswordValue

p12import operation

This operation is available from SNS version 3.10.1 or 4.0.1 upwards.

It allows PKCS#12 files to be imported in .p12 format. If a file is not protected by a password, the "p12password" field has to remain empty. The "ondisk" parameter makes it possible to protect the private key contained in a PKCS#12 file by storing it on the TPM.

The TPM must be initialized before it can be used to protect a private key.

Format

```
"serial | any", p12import, none|ondisk, "p12file", "p12password"
```

EXAMPLES

```
SN310A000000000Z, p12import, none, file1.p12, file1PwdValue
SN310A000000000Z, p12import, none, file2.p12
SN310A000000000Z, p12import, ondisk, file3.p12, file3PwdValue
SN310A000000000Z, p12import, ondisk, file4.p12
```

crlimport operation

This operation is available from SNS version 4.8.0 upwards.

This operation makes it possible to import a certificate revocation list (CRL) on the firewall.

The file containing the CRL has to be in these formats:

- PEM (ASCII format - Base64 encoding),
  - or -
- DER (binary).

Format

```
"serial | any", crlimport, "filename", "pem | der"
```

EXAMPLES

```
any, crlimport, mycrl.pem, pem
SN310A00000000Z, crlimport, mycrl.der, der
```

certimport operation

This operation is available from SNS version 4.8.0 upwards.

This operation makes it possible to import a certificate or certification authority (CA) on the firewall.

The file of the certificate or certification authority has to be in these formats:

- PEM (ASCII format - Base64 encoding),
  - or -
- DER (binary).

Format

```
"serial | any", certimport, "filename", "pem | der"
```

EXAMPLES

```
any, certimport, myca.pem, pem
SN310A00000000Z, certimport, mycert.der, der
```

Preparing the USB key

If you are using a USB key for a firewall's initial configuration, Stormshield strongly recommends encrypted USB keys such as Kingston Data Traveler, which are protected with a built-in PIN.

Formatting the USB key

The USB key must contain a single partition formatted to FAT32.

Copying the necessary files

Depending on the operations performed, copy the following files to the root folder of the USB key:

- Licenses (.licence),
- Software update(s) (.maj),
- Configuration backup(s) (.na),
- SMC connecting package(s) (.pack),
- PKCS#12 certificate(s) (.p12),
- Files containing the password to the *admin* account (.pwd),
- Files containing the dynamic routing configuration (.bird or .bird6),
- Additional configuration files (.csv).

Setting the initial configuration

No action is required from the operator during the initial configuration of a firewall via a USB key, except to:

- Unlock the USB key if it has been encrypted,
- Enter certificate passwords whenever certificates are imported via USB key during the configuration,
- Remove the USB key and insert it again whenever necessary.

The set the initial configuration:

1. Check that the firewall is powered off.
2. If the firewall has been assigned to a cluster, ensure that all of its HA-dedicated network interfaces are connected to the master firewall.
3. Insert the key into the firewall's USB port.
4. Power up the firewall.
   The firewall will automatically run and install the prepared files in the sequence mentioned in Installation sequence.
   It will restart only after each software update.
5. If part of the configuration involved *setglobal* commands included in a CSV file, manually restart the firewall to apply changes.
6. Once all the steps in the configuration have been completed, the firewall will be operational.
   - You can log in directly to the firewall's administration interface (*https://firewall_IP_address/admin*) or via Stormshield Management Center if the firewall is connected to an SMC server.
   - Operations that were performed during the initial configuration of the firewall, except license imports and firmware updates, will be logged in a log file created in the root folder of the USB key named *<firewall_serial_number_staging>.log*.

Further reading

Additional information and responses to questions you may have are available in the Stormshield knowledge base (authentication required).

documentation@stormshield.eu