STORMSHIELD

STORMSHIELD MANAGEMENT CENTER

RELEASE NOTES

Version 3

Document last update: June 17, 2021

Reference: sns-en-SMC-release_notes-v3.0

Table of contents

In the documentation, Stormshield Management Center is referred to in its short form: SMC and Stormshield Network under the short form: SN.

This document is not exhaustive and minor changes may have been included in this version.

SMC 3.0 new features

Authentication

Nested groups

Administrators that belong to an LDAP group nested in another can now connect to the SMC server.

Configuration of SN firewalls

Managing network interfaces

The network interfaces of SN firewalls can now be managed from a central point on the SMC server. On SN firewalls in at least version 3.7, SMC displays network interfaces in read-only mode. On SN firewalls from version 4.2.3 upwards, the configuration of network interfaces can be enabled in write mode in their SMC settings.

The Ethernet interfaces, bridges, VLANs and IPv4 aggregates of compatible firewalls will therefore appear on the SMC server. Their configuration can be managed without the need to connect to each firewall individually. SMC verifies the configuration of supported interfaces and reports errors through the consistency checker.

Find out more

Keeping the connection alive during deployment

When the wrong configuration is accidentally deployed, the connection between the server and firewall may be lost. On SN firewalls from version 4.2.3 upwards, the previous configuration will be restored if the connection was lost. This guarantees that the firewall will always remain reachable from the SMC server.

Find out more

Restarting after a deployment

SN firewalls may sometimes need to be restarted after a network configuration is deployed in order for changes to be applied. In such cases, SMC reports the information using the new “Reboot required” health status, and the firewalls in question can then be rebooted directly from the SMC server. This feature is supported only on firewalls in version 4.2.3.

Find out more

Detecting local modifications

After its initial deployment on a connected SN firewall, SMC now detects local modifications to the configuration of items that SMC manages. You can then decide whether to deploy the configuration currently found on the SMC server, which will overwrite local modifications. You can also restore the latest configuration deployed on the firewall in question.

Find out more

Importing firewalls from a CSV file

The command that makes it possible to import SN firewalls from a CSV file in command line has been renamed `smc-import-firewalls`. The previous command `smc-firewalls-and-packages` is no longer supported.

Find out more

Filter and NAT rules

Creating rule sets

Rule sets can now be created to group filter or translation rules that you wish to deploy on one or several firewalls. As such, a set of rules corresponding to a specific application in the configuration of various firewalls can be reused, regardless of their location in the folder tree.

Find out more

SMC 3.0 fixes

Configuration of SN firewalls

Inaccessible audit logs

Support references 79393 and 80772

On some versions of SN firewalls, access to audit logs would occasionally fail during connections to the firewall via the SMC server. This issue has been fixed.

Network configuration via USB key impossible

Support reference 79258

Due to a missing section in the connecting package, USB keys could not be used to load the network configuration on firewalls in factory configuration. The section has been added and USB keys can now be used.

Initialization of the SMC server

Ambiguous parameter

Support reference 82014

The `DNS configuration (leave blank if no DNS)` parameter requested whenever the SMC server is initialized manually, has been changed to `DNS server IPs (comma separator or leave blank if no DNS)` to remove any ambiguity.

Updates

Time zone not saved

Support reference: 80779

The set time zone is now saved after SMC is updated.

Loss of scripts

Support reference: 71885

Scripts that automatically run when a network interface on the SMC host system is enabled are now saved after updates.

Ambiguous error message

Support reference: 0081991

When there are issues restoring the server from a backup, the ambiguous error message that appears has been changed to more clearly indicate the cause of the error.

Filter and NAT rules

Importing rules

Support reference: 79314

When filter rules were imported from a CSV file, the "!" operator (NOT) would be ignored. This issue has been fixed, and fields are now imported with this operator taken into account.

Support references: 78561 and 79308

Rules containing the value "any" in a `#nat_to_target` field in the CSV file could not be imported because this value is prohibited. The value of this field is now automatically set to "none" and the import no longer fails.

Support reference: 80828

Filter and NAT rules containing domain names can now be imported.

Support reference: 80590

Rules can now be imported through a CSV file containing some IPRep categories that were previously missing.

Adaptation of protocol name

Support reference 82222

In filter rules, the "ldap" protocol has been renamed "ldap_tcp" to maintain consistency between SMC and SMC.

Error during copy and paste

Support reference: 78373

When a rule is copied and pasted to the filter or NAT rule screen, the name of the rule and its contents are now pasted correctly.

System

Frequently encountered errors

Support reference: 81714

Errors regarding the connection to the serial port were displayed every five minutes. This issue has been fixed.

Compatibility

The following platforms are compatible with SMC 3.0.

Virtual environments

VMware ESXi	6.5 and 6.7
Microsoft Hyper-V	Windows Server 2012 R2 and 2016
KVM	Red Hat 7.6

Web browsers

In order for the firewall administration interface to operate optimally, you are advised to use the latest versions of Microsoft Edge, Google Chrome and Mozilla Firefox (ESR version - Extended Support Release). For further information on these versions, please refer to the relevant vendors for the life cycles of their products.

Active Directories

Active Directory	Windows Server 2012 R2 and 2016

Compatibility of SMC/SN firewalls

The SMC server manages SN firewalls from version 2.5.

This table lists the lowest versions of SN firewalls required in order to be compatible with the following SMC features:

Feature/Object	Version of SMC	Lowest version of SN firewall required
SNS CLI Scripts	1.1	2.5
Filter/translation rules	2.0	3.0
Policy-based VPN topologies	2.0	3.0
Router and time objects	2.1.0	3.1
Editing the firewalls output interface	2.2.0	3.3
Multiple addresses to contact SMC specified in the connecting package	2.2.1	3.3
SMC as CRL distribution point	2.2.1	3.3
Health indicators	2.5	3.6
“Responder-only” mode in star VPN topologies	2.5	3.6

AES GCM 16 encryption algorithm	2.5	3.6
Importing filter and NAT rule from the web interface	2.5	3.3
Closure of SAs (VPN Peer Inactivity)	2.6.1	3.7.2
CRLRequired parameter	2.6.1	3.8
Declaring an SCEP server associated with a certification authority / automatic renewal of SCEP certificates	2.6.1	3.9
Multiple outgoing interfaces in the connecting package	2.6.1	3.9
Securing certificates via TPM (Trusted Platform Module)	2.6.1	3.10
DSCP parameter in VPN topologies	2.6.1	3.10
Declaring an EST server associated with a certification authority/automatic renewal of EST certificates	2.7	3.10 and 4.1
Excluding private keys from automatic firewall backups	2.7	3.10 and 4.1
Route-based VPN topologies	2.8	3.3
Managing network interfaces (in read-only mode)	3.0	3.7

NOTE
To be able to monitor the status of VPN topologies containing firewalls of version 4.2 or higher, you need to use an SMC server of version 2.8.1 or higher.

Recommendations

Information about future updates

As a result of updating the SMC server to version 3.0.x, disk space on the virtual machine will be insufficient for the installation of future updates. After updating to version 3.0.x, follow the procedure described below to increase disk space of the server:

1. Back up the 3.0.x SMC server configuration.
2. Shut down the SMC server.
3. Deploy a new SMC server in the same 3.0.x version.
4. Restore the the configuration from your backup on the new virtual machine.

Information prior to an update

Minimum hardware recommendations

To ensure good performance of the SMC server, we recommend installing it on a virtual machine with at least 2 vCPUs and 4 GB of RAM.

Access to the SMC server during updates

When you update your SMC server, we recommend that you prevent other administrators from accessing SMC for the duration of the update. If you do not do so, they will not be informed of updates in progress and any configurations they are working on will not be saved.

Syslog server

If you use a remote server in Syslog format to collect SMC logs, you need to configure the remote server again after updating the SMC server, through the command `smc-syslog-ng`. This operation is no longer required from version 2.6 of SMC.

Before updating to a 2.0 version

From version 2.1.0 of the SMC server, changes have been made to the operating system so that a larger amount of data can be managed, especially by the new feature that automatically backs up the configuration of the server and of SN firewalls.

We recommend that you deploy a new *.OVA*, *.VHD* or *.qcow2* to get the best results from the following modifications:

- more efficient virtual interface,
- increased disk space to support the automatic backup feature.

We also advise you to enable the automatic backup feature only after a new machine has been deployed.

Follow the procedure below to deploy a new *.OVA*, *.VHD* or *.qcow2*:

1. Start by upgrading your machine to version 2.1.0 or upwards from an upgrade archive.
2. Back up the configuration of the server and of any logs you wish to back up.
3. Deploy a new *.OVA*, *.VHD* or *.qcow2* in version 2.1.0 or higher.

4. Through the SMC initialization wizard, restore the backed up configuration on the new machine.

To get help or more information on these procedures, please refer to the *SMC Administration guide* or contact the Technical Assistance Center.

Feel free to look up the SNS knowledge base as well in your MyStormshield area. The knowledge base explains how to manually increase disk size and modify the virtual interface.

Warning before connecting SN firewalls to the SMC server

Take note of the following information if you wish to associate the SMC server with a pool of SN firewalls already used in production, and which contain global configuration items.

Whenever SMC deploys a configuration on a firewall, all global configuration items found on this firewall will be deleted and replaced with configuration items defined in the SMC configuration, if any.

This includes:

- global objects defined on the firewall
- global filter rules defined on the firewall
- global VPN tunnels defined on the firewall

These elements are not displayed by default in the SNS web configuration interface. To display them, go to the firewall **Preferences**, **Application settings** section and enable the option **Display global policies (Filter, NAT, IPsec VPN and Objects)**.

By attaching an SN firewall to SMC, you therefore accept that these global items, which could have been set up on this firewall, will be overwritten as soon as SMC deploys the configuration.

However, local objects, rules and VPN tunnels (which you handle by default in the firewalls' web administration interface) will never be modified or deleted when SMC deploys a configuration.

We therefore recommend that you recreate these global items in the form of local items on the firewall or rewrite rules in SMC before attaching the firewall to SMC, in order to avoid losing configuration items and disrupting production.

In most cases, in which the firewall to be connected does not have any global configuration items, no particular precautions need to be taken in attaching the firewall to SMC, and doing so will leave no impact on production.

In any case, we advise you to back up your firewall's configuration before connecting it to SMC.

Known issues

The up-to-date list of the known issues related to this version of SMC is available on the Stormshield Knowledge base. To connect to the Knowledge base, use your MyStormshield customer area identifiers.

Explanations on usage

Using VTI objects generated by route-based VPN topologies

When a route-based VPN topology is modified or deleted in SMC, Host VTI objects that this topology automatically generates to represent remote peers will also be modified or deleted. If you are using such objects in the local configuration of your SN firewalls, first ensure that you delete them before modifying or deleting a topology in SMC.

VPN topologies deployment

It is not possible to deploy a VPN topology from the SMC server if the name of a firewall is too long. The names of VPN topologies on firewalls cannot contain more than 127 characters.

Configuring routing on SMC

Several of the interfaces used for contacting the SMC server can be configured, but only one default gateway can be declared on a single interface. Routing must be configured manually for the other interfaces. An article in the Stormshield Knowledge base sets out the procedure to follow.

Using global network objects in a local configuration

On SN firewalls, global objects may be used in local configurations. However, when SMC deploys a configuration on a firewall, existing global objects on the firewall will be deleted and replaced with objects defined in the SMC configuration. To keep the local configuration running, you need to impose the deployment of necessary global objects on affected firewalls.

For more information, refer to the section Warning before connecting SN firewalls to the SMC server.

Migrating a V model virtual firewall to an EVA model

V-50, V-100 and V-200 virtual firewalls can no longer be upgraded to EVA models using the variable %FW_UPD_SUFFIX% in an SNS CLI script run from the SMC server.

To work around this issue, replace the variable %FW_SIZE% with the value "XL-VM" in the upgrade script.

Documentation resources

The following technical documentation resources are available on the Stormshield Technical Documentation website or on Stormshield Institute website. We suggest that you rely on these resources for a better application of all features in this version.

Guides

- Stormshield Management Center Installation guide
- Stormshield Management Center Administration guide
- Stormshield Network Configuration and Administration Manual

Videos

- CLI Commands and Scripts, available on Institute.

Downloading this version

Going to your MyStormshield personal area

You need to go to your MyStormshield personal area in order to download the 3.0 version of Stormshield Management Center:

1. Log in to MyStormshield with your personal identifiers.
2. In the left panel, select **Downloads**.
3. In the right panel, select the relevant product and version.

Checking the integrity of the binary files

To check the integrity of Stormshield Management Center binary files:

1. Enter one of the following commands and replace `filename` by the name of the file you want to check:
   - Linux operating system: `sha256sum filename`
   - Windows operating system: `CertUtil -hashfile filename SHA256`
2. Compare with hashes provided on MyStormshield personal area, section **Downloads**.

Contact

To contact our Stormshield Technical Assistance Center (TAC):

- https://mystormshield.eu/
  All requests to technical support must be submitted through the incident manager in the private-access area https://mystormshield.eu, under **Technical support** > **Manage cases**.
- +33 (0) 9 69 329 129
  In order for us to provide high-quality service, you are advised to use this communication method only to follow up on incidents that have been created earlier on https://mystormshield.eu.

All images in this document are for representational purposes only, actual products may differ.