STORMSHIELD

STORMSHIELD MANAGEMENT CENTER

RELEASE NOTES

Version 3

Document last update: November 16, 2021

Reference: sns-en-SMC-release_notes-v3.1

Table of contents

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

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

SMC 3.1 new features

Managing administrators

Access to the SMC server in SSH or console mode

All administrators can now be assigned access privileges to the SMC server via the console on the hypervisor or in SSH. Previously, only the "root" user was allowed.

This change makes it possible to facilitate access to advanced management features on the SMC server and identify administrator connections and operations, as well as any elevation of privilege, in server logs.

Administrators who authenticate via LDAP or Radius authentication servers can also access SMC through the console on the hypervisor or in SSH. The super-administrator can grant them privileges through the administration interface.

Managing administrators from external authentication servers

Administrators and groups that have accounts on an LDAP authentication server can now be managed directly in the SMC server's web interface.

The *rights.csv* file is no longer used, and the commands `smc-auth-check` and `smc-ui-password` are no longer available.

Likewise, Radius user groups can be added to the interface, the same way they are added on SNS firewalls, by using a VSA

The OpenLDAP 2.5.x authentication server is now supported.

Defining a backup authentication server

To guarantee that administrators have uninterrupted access to the SMC server, you can define a backup LDAP or Radius authentication server that will take over when the main server fails.

Find out more

Offline environment

Active Update server

The SMC server can now stand in for the Active Update server that communicates with Stormshield update servers, to distribute Active Update databases to SNS firewalls, even when they are not connected to the Internet. The service will automatically download databases on a regular basis. In this way, firewalls will always be equipped with the latest databases (context-based signatures, antivirus, Vulnerability Manager, etc.).

If the SMC server and SNS firewalls run in a closed network without Internet access, you can manually download Active Update databases and distribute them to SNS firewalls via the SMC server’s Active Update server.

Find out more

Increased security

Compliance with ANSSI '*Diffusion Restreinte*' mode

The SMC server now makes it possible to implement *Diffusion Restreinte* mode on SNS firewalls. This mode complies with ANSSI recommendations with regard to sharing communications that pass through the IPSec VPN. A consistency check on the configuration of the server and firewalls will assist you in deploying this mode by automatically detecting the parameters that need to be changed.

When DR mode is enabled on the SMC server, the configuration will be deployed on SNS firewalls. The firewalls must then be manually restarted.

Find out more

Configuration of SNS firewalls

Using custom firewall properties

Custom properties can now be created in addition to the default Name, Description and Location properties on firewalls, and specific values can be assigned to each firewall.

You can therefore filter the list of firewalls or perform searches based on these properties, which can be imported or exported in CSV format, and can also be found in exports of monitoring data.

Find out more

SNS firewall monitoring

Exporting SNS firewall monitoring data

Exported monitoring data now consists only of firewall data displayed in the panel when the list is filtered.

Find out more

Status of licensing options

The status icons in the upper banner of the administration interface and the **Licensing options** column in the firewall monitoring panel now alert the user when a license option or its maintenance package has expired or is about to expire.

Environment variables make it possible to configure alert thresholds.

Find out more

Filter and NAT rules

Looking up local rules

Firewalls' local rules are now displayed in read-only mode in the filter and NAT rule panel.

SMC server configuration

Dynamic address assignment via DHCP

You can now choose whether to assign a dynamic IP address to the SMC server via DHCP. This option is available in the SMC server initialization wizard, or in the server's settings in the administration interface.

Authorities and certificates

Verification of the Certificate Revocation List (CRL)

The environment variable FWADMIN_VPN_CRL_REQUIRED is no longer supported to verify the validity of the certificates. The **Check certificate validity** checkbox is now available in the **Configuration** > **Certificates** panel.

In the certificate management panel, the administrator can now specify for each firewall:

- The local IP address to renew SCEP/EST certificates on SNS firewalls,
- The local IP address that allows the revocation list to be verified,
- The frequency with which the revocation list is verified.

The value of the previous variable FWADMIN_VPN_CRL_REQUIRED will not be kept when the SMC server is updated, and the **Outgoing interface** field in the certificate renewal panel has been removed.

Local IP address for the renewal of certificates obtained via SCEP or EST

For SNS firewalls that have certificates obtained via SCEP or EST, you can now specify the local IP address that will be used to renew certificates for each firewall. Previously, the renewal address was indicated in the certification authority settings, and was therefore the same for all certificates issued by the same authority.

Find out more

VPN topologies

Configuring PRF in encryption profiles

You can now choose an algorithm that must be negotiated as a PRF (Pseudo-Random Function) in the **IKE** tab in the encryption profiles used in VPN topologies. This option is supported from version 4.2.3 of SNS firewalls onwards and is only compatible with IKEv2 topologies.

Find out more

New encryption profiles

The three encryption profiles offered by default on the SMC server – "Strong encryption", "Mobile encryption" and "Good encryption" – have been renamed "Strong encryption legacy", "Mobile encryption legacy" and "Good encryption legacy". If you have modified them, they will revert to their default configuration.

The "Good encryption legacy" profile now uses AES instead of Blowfish and Diffie-Hellman group 2 replaces Diffie-Hellman group 14 in phase 2.

Three new profiles – "Strong encryption", "Mobile" and "Good encryption" – replace the previous profiles.

All six profiles are in read-only mode.

Object database

Importing router objects

SNS firewalls in version 4.3.0 make it possible to export router objects and the associated gateways. The SMC server now supports importing/exporting router objects in the same format as SNS firewalls.

The use of the CSV format (before SMC 3.1) is no longer supported for router objects. The gateway configuration associated with a router object is not compatible with SMC in versions lower than 3.1.

Hosting Amazon Web Services

The SMC server can now be hosted by Amazon Web Services (AWS) in BYOL (Bring Your Own License) mode.

You can choose between several types of instances to adapt the SMC server's resources as closely as possible to the number of firewalls to manage.

Find out more

SMC 3.1 fixes

Authorities and certificates

Subject length in certificates

Support reference 184536CW

Previously, the SMC server would truncate text entered in the Subject (DN) field in certificates when it exceeded 140 characters, causing the deployment of VPN topologies to fail. The SMC server now accepts certificates with subjects that exceed 140 characters.

Updating certificates in command line

Support reference 167610PW

Certificates installed on a firewall can now be updated using the command `smc-install-certificate`.

Filter and NAT rules

Filtering by user name

Support reference 167465PW

Traffic that filters user names containing apostrophes can now be declared in filter rules.

Warning regarding the analysis of encrypted traffic

Support reference 167465PW

The consistency check no longer raises a warning when a traffic decryption rule is placed before a rule that analyzes the same decrypted traffic.

Updating an SMC server in a version lower than 2.7.0

Support reference 185398CW

SMC servers in versions lower than 2.7.0 could not be updated to a 3.0.0 version if a block filter rule that performed destination NAT with a "network-any" value was defined in the policy. SMC servers containing such a rule can now be updated to a 3.1.0 version.

Object database

Searching for object groups

Support reference 167465PW

In the window to create or edit object groups, the **Search** field now extends to the IP addresses of objects.

Forced deployment of objects

Support reference 167698PW

When updating the SMC server to version 3.x, objects with forced deployment set on SNS firewalls now keep this parameter when they are migrated.

VPN topologies

IKE fragmentation

Support reference 167619PW

Previously, IKE fragmentation could not be enabled from the SMC server on SNS firewalls in version 3.7.x. It can now be enabled on firewalls in version 3.7.22, and fragment size can be configured.

SNS firewall monitoring

Display error in the firewall monitoring window

Support references 186959CW and 186343CW

In some error cases on SNS firewalls, the monitoring window in the administration console would no longer display. This issue has been fixed.

Resolved vulnerabilities for SMC 3.1

Server protection

Protection of the server memory

A low severity vulnerability was fixed after the PostgreSQL component was upgraded.

Details on this vulnerability can be found on our website https://advisories.stormshield.eu.

Protection against buffer overflow attacks

A medium severity vulnerability was fixed after the OpenSSL component was upgraded.

Details on this vulnerability can be found on our website https://advisories.stormshield.eu.

Compatibility

The following platforms are compatible with SMC 3.1.

Hypervisors

VMware ESXi	6.5, 6.7 and 7.0
Microsoft Hyper-V	Windows Server 2012 R2, 2016 and 2019
KVM	Red Hat 7.6

Authentication servers

Active Directory	Windows Server 2016 and 2019
OpenLDAP	2.5
Radius	Windows Server 2016 and 2019

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.

Public Cloud

Amazon Web Services

Compatibility of SMC/SNS 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
Managing "Diffusion Restreinte (DR)" mode	3.1	4.3
Active Update distribution point	3.1	4.3

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

After the SMC server is updated from a version lower than 3.0.x, disk space on the virtual machine will be insufficient for the installation of future updates. After updating to version 3.1, follow the procedure described below to increase disk space on the server:

1. Back up the 3.1 SMC server configuration.
2. Shut down the SMC server.
3. Deploy a new SMC server in the same 3.1 version.
4. Restore the the configuration from your backup on the new virtual machine.

To get help or more information on these procedures, 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.

Information prior to an update

Address range of SMC micro-services

If the address range that your SNS firewalls use conflicts with the address range that micro-services on the SMC server use, you can change the address of the SMC server's "docker0" interface (172.17.0.1/16). To do so, follow the steps in the StormshieldKnowledge base article.

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.

Warning before connecting SNS firewalls to the SMC server

Take note of the following information if you wish to associate the SMC server with a pool of SNS 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 items are not displayed by default in the SNS web configuration interface. To display them, go to the firewall **Preferences**, section **Application settings** and enable the option **Display global policies (Filter, NAT, IPsec VPN and Objects).**

By attaching an SNS 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 the All object in VPN topologies

Within a policy-based VPN topology, when two different peers use the *All* object to define traffic endpoints, then the connection between SMC and the SN firewall may fail, unless you have configured policy-based routing rules to support this use case. In star topologies, the same problem occurs if the *All* object is used to define the center of the star and one of the satellites.

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 SNS 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 3.1 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**.

Previous versions of SMC v3

In this section, you will find the features and fixes from previous versions of SMC v3.

3.0.1	New features	Resolved vulnerabilities	Bug fixes
3.0	New features		Bug fixes

SMC 3.0.1 new feature

VPN topologies

Traffic endpoints

In VPN topologies, it is now possible to set the traffic endpoints to the *All* value in order to allow all traffic through the tunnels.

Resolved vulnerability in SMC 3.0.1

Server protection

Protection against denial of service (DoS) attacks

A moderate severity vulnerability was fixed after the NodeJS component was upgraded.

Details on this vulnerability can be found on our website https://advisories.stormshield.eu.

SMC 3.0.1 fixes

Filter and NAT rules

Filtering by domain name

Support reference 82060

Domain names used as criteria in filter rules can now be entered in any format, not only as URLs.

Exporting to CSV files

Support reference 82236

The value of the **Inspection** field in a filter rule is now correctly exported when it is either *firewall*, *IDS* or *IPS*.

Configuration deployment

Deployment status

If the SN firewall automatically restores a configuration after it is deployed from SMC, this deployment will no longer be considered successful and its number will no longer be incremented.

Configuration on a cluster

Deploying a configuration that includes a network configuration on a cluster no longer causes the cluster to restart.

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

In the filter and NAT rule window, copying and pasting text contained in the search field now pastes only the text without duplicating the highlighted rule.

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.

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.