



STORMSHIELD



**STORMSHIELD MANAGEMENT
CENTER**

RELEASE NOTES

Version 3

Document last updated: August 30, 2022

Reference: [sns-en-SMC-release_notes-v3.3.1](#)



Table of contents

New SMC behavior	3
SMC 3.3.1 new features and enhancements	4
Resolved vulnerabilities for SMC 3.3.1	5
SMC 3.3.1 fixes	6
Compatibility	9
Recommendations	11
Known issues	13
Explanations on usage	14
Documentation resources	15
Downloading this version	16
Previous versions of SMC v3	17
Contact	46

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.



New SMC behavior

Changes introduced in version 3.2.1

In SMC, SNS firewalls in versions lower than 3.7 can no longer be connected and managed.

If you have SNS firewalls in versions below 3.7 connected to SMC, they will no longer be able to connect to SMC 3.2.1. We recommend that you update your SNS firewalls to a version that SMC supports.



SMC 3.3.1 new features and enhancements

3DS Outscale hosting

The SMC server can now be hosted by 3DS Outscale in Bring Your Own License (BYOL) mode.

You can choose from various types of instances so that the resources of the SMC server can be optimally adapted based on the number of firewalls to manage.

[Find out more](#)

SMC CLI scripts

Delayed script execution

The execution of SMC CLI scripts can be launched or scheduled on firewalls that are offline at the time of execution. Scripts will be automatically executed the next time such firewalls connect to SMC.

[Find out more](#)

SMC firewall monitoring

Shortcut to SLS (Stormshield Log Supervisor)

If you have an SLS server to centrally manage logs collected from your SMC firewalls, you can now configure shortcuts to the SLS server in SMC. This will allow you to read logs from the entire pool, or logs filtered by a firewall of your choice.

[Find out more](#)

VPN topologies

New Diffie-Hellman groups

In encryption profiles, you can now select Diffie-Hellman groups 31 (EC25519) and 32 (EC448).

Filter and NAT rules

ACK queue

In order to support QoS on firewalls in at least version 4.3.0, the new **ACK queue** field in the **Action > QoS** menu of a filter rule makes it possible to set a specific queue for TCP ACK traffic.

[Find out more](#)

S7+ protocol added

The S7+ application protocol can now be selected in filter and translation rules.



Resolved vulnerabilities for SMC 3.3.1

Node.js vulnerability

Clandestine HTTP requests

A high severity vulnerability was fixed after the Node.js component was upgraded.

Details on this vulnerability can be found on our website

<https://advisories.stormshield.eu/2022-018/>.

Javascript library

A low severity vulnerability was fixed after the Javascript Moment.js library was upgraded.

Details on this vulnerability can be found on our website

<https://advisories.stormshield.eu/2022-022/>.



SMC 3.3.1 fixes

Object database

Network objects

Support reference 84405

Network objects with a subnet mask in /32 can no longer be used or imported in the firewall configuration. The consistency checker will raise an alarm if such objects are found on SMC.

Router objects

Support reference 84643

Router objects can now be created even when the HTTPS port object does not exist in the SMC object database.

Monitoring SMC with SNMP

Status of the SNMP service after updating SMC

Support reference 84438

When SNMP is enabled on the SMC server, it will now automatically restart after SMC is updated. The service remains enabled after SMC is restarted.

System

`service` command

Support reference 84381

SMC no longer supports the `service` command. Since version 3.0, the use of the `service --status-all` command, which listed the services on the system, would make SMC stop functioning.

Some errors caused SMC to stop

Some errors, which could occur during a configuration deployment for example, caused SMC server to stop. SMC now continues to run correctly even if these errors occur.

Configuration deployment

Use of the same peer in VPN topologies

Support references 84584 and 84647

Whenever the same peer was used twice in a VPN topology, SMC would no longer restart during a deployment. This would make the deployment fail and SMC would display an error message.



Filter rules

Use of the @ character in the comments of a rule

Support reference 84423

The local filter rules on SNS firewalls now display correctly in SMC when the @ character is used in comments.

Display of local filter rules

Support references 84396, 84440 and 84442

The local filter rules on SNS firewalls now display correctly in SMC when:

- they use a group of regions, a category of public IP address reputations or web services that SMC does not know.
- they use router objects,
- they use objects that SNS did not export in SMC,

Configuration of SNS firewalls

Managing network interfaces

Support reference 84529

SMC now no longer deploys the network configuration if it has not retrieved all network interfaces beforehand.

Importing SNS firewalls

Support reference 84644

The #vpn_fw_public_ip_address parameter functions again when importing SNS firewalls from a CSV file.

Consistency check on network interfaces

Support reference 84576

The consistency check no longer fails when it analyzes network interfaces with IP addresses in /32.

Authorities and certificates

Verification of the revocation list

Support reference 84603

SMC now forces SMC firewalls to retrieve the certificate revocation list (CRL) after every time the configuration is deployed. So when a VPN topology is deployed with the CRL verification option enabled, tunnels will be operational immediately. There is no longer any need to wait for the firewalls to retrieve the CRL.



Changes to the CRL

Support reference 84646

SMC now ignores the CRL file *CA.crl.pem* in the folder *ConfigFiles/Global/Certificates/<topo_name>/* of SMC firewalls, so it no longer raises any alerts when this file is modified locally.



Compatibility

To update a SMC server to version 3.3.1, intermediate updates may be required depending on its original version:

From a 2.X version	Updating to version 3.1.6
--------------------	---------------------------

Hypervisors

VMware ESXi	6.5, 6.7 and 7.0
Microsoft Hyper-V	Windows Server 2012 R2, 2016 and 2019
KVM	Red Hat 7.9

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 3.7.

This table recaps 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 SNS firewall required
SNS CLI Scripts	1.1	3.7.0
Filter/translation rules	2.0	3.7.0
Policy-based VPN topologies	2.0	3.7.0
Router and time objects	2.1.0	3.7.0



Editing the firewalls output interface	2.2.0	3.7.0
Multiple addresses to contact SMC specified in the connecting package	2.2.1	3.7.0
SMC as CRL distribution point	2.2.1	3.7.0
Health indicators	2.5	3.7.0
“Responder-only” mode in star VPN topologies	2.5	3.7.0
AES GCM 16 encryption algorithm	2.5	3.7.0
Importing filter and NAT rule from the web interface	2.5	3.7.0
Closure of SAs (VPN Peer Inactivity)	2.6.1	3.7.2
CRLRequired parameter	2.6.1	3.8.0
Declaring an SCEP server associated with a certification authority / automatic renewal of SCEP certificates	2.6.1	3.9.0
Multiple outgoing interfaces in the connecting package	2.6.1	3.9.0
Securing certificates via TPM (Trusted Platform Module)	2.6.1	3.10.1
DSCP parameter in VPN topologies	2.6.1	3.10.1
Declaring an EST server associated with a certification authority/automatic renewal of EST certificates	2.7	3.10.1 and 4.1.1
Excluding private keys from automatic firewall backups	2.7	3.10 and 4.1
Route-based VPN topologies	2.8	3.3.0
Managing network interfaces (in read-only mode)	3.0	3.7.0
Managing network interfaces (in write mode)	3.0.1	4.2.3
Managing “ <i>Diffusion Restreinte</i> (DR)” mode	3.1	4.3.3
Active Update distribution point	3.1	4.3.3
Various versions of IKE supported on the same firewall	3.1.3	3.7.0
Routing (read/write)	3.2	4.2.4
SD-WAN support	3.2	4.3.3

i NOTE

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



Recommendations

Information prior to an update of the SMC server

Size of the System disk

After successive updates of the SMC server, it may happen that free space on the System disk is not enough to allow new updates to be installed:

1. Use the following command to check the state of the system disk:

```
df -h /
```

For example:

```
[root@smc] - {~} > df -h /  
Filesystem      Size  Used Avail Use% Mounted on  
/dev/root       1.9G  1.5G  215M  88% /
```

2. If the disk is almost full, you need to deploy a new virtual machine using the following procedure:
 - a. **Back up** the 3.x SMC server configuration.
 - b. Shut down the SMC server.
 - c. **Deploy a new SMC server** in the same 3.x version.
 - d. Restore the the configuration from your backup on the new virtual machine.
3. Update your new SMC server to the new 3.y version.

i EXAMPLE

To update from a 3.1.4 version to a 3.1.6 version:

- a. Back up the 3.1.4 SMC server configuration.
- b. Shut down the server.
- c. Deploy a new 3.1.4 server.
- d. Restore the backed up configuration on the new 3.1.4 server.
- e. Update the new server to version 3.1.6.

To get help or more information on these procedures, refer to the *SMC Administration guide* or contact the [Technical Assistance Center](#).

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 Stormshield [Knowledge base](#) article.

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.



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.

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, Application settings** section 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

Various versions of the IKE protocol supported on the same firewall

In VPN topologies, different versions of the IKE protocol can be supported on the same firewall only if there is a single firewall in common across several topologies. If several topologies configured with various versions of IKE have several firewalls in common, the version of the topology that was created first in the topology configuration screen will be the one deployed.

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 SNS 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 SNS firewalls, first ensure that you delete them before modifying or deleting a topology in SMC.

VPN topologies deployment

VPN topologies cannot be deployed 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 SNS 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 3.3.1 version of Stormshield Management Center:

1. Log in to MyStormshield with your login and password.
2. In the panel on the left, select the **Downloads** section.
3. In the panel on the right, select the relevant product and version.
4. Download the files *build.sha256sum*, *build.sha256sum.sign* and *smc-sign.crt* as well if you wish to check the integrity of binary files.

Checking the integrity of binary files

Enter one of the following commands to check the integrity of Stormshield Management Center binary files:

- Linux operating system: `sha256sum -c build.sha256sum`
- In PowerShell on a Windows operating system:
 - Enter `cat build.sha256sum`. The command will return the hashes and associated files.
 - To compare a file's hash, copy it and enter `(Get-FileHash my-file.ext -A SHA256).Hash -eq "hash"`.

Verifying the signature of the *build.sha256sum* file

The *build.sha256sum.sign* file is the signature of the *build.sha256sum* file. Verifying it will guarantee that *build.sha256sum* has not been modified.

OpenSSL is required to verify the file's signature.

1. If you need to install OpenSSL in Microsoft Windows, use the winget tool and the PowerShell command below:

```
> winget install ShiningLight.OpenSSL
```

2. Next, run the "Win64 OpenSSL Command Prompt" program.

To verify the signature in Linux and Windows operating systems:

1. Use the certificate *smc-sign.crt*:

```
openssl x509 -in smc-sign.crt -pubkey -noout -out smc-sign.pem
openssl dgst -sha256 -verify smc-sign.pem -signature
build.sha256sum.sign build.sha256sum
```

If you want to verify whether the certificate was indeed issued by the [SMC certification authority](#), use the command:

```
openssl verify -CAfile Stormshield.Management.Center.2.pem smc-sign.crt
```




Previous versions of SMC v3

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

3.2.2			Bug fixes
3.2.1	New features		Bug fixes
3.1.6		Resolved vulnerabilities	Bug fixes
3.1.5			Bug fixes
3.1.4			Bug fixes
3.1.3	New features		Bug fixes
3.1.2			Bug fixes
3.1.0	New features	Resolved vulnerabilities	Bug fixes
3.0.1	New features	Resolved vulnerabilities	Bug fixes
3.0	New features		Bug fixes



Version 3.3.0 not published

Version 3.3.0 is not available to the public.



SMC 3.2.2 fixes

SMC Certification authority

Update of the certification authority

The certification authority (CA) which manages the certificate of the license used by SMC has been renewed until June 09, 2026.



SMC 3.2.1 new features and enhancements

Network configuration

SD-WAN - Selecting the best link

In SMC, specific criteria can be centrally managed to determine whether a WAN link meets the quality level adapted to its type of traffic (VoIP, video, etc.).

To do so, for each traffic type, you can set an SLA (Service Level Agreement) commitment based on one or several thresholds out of the criteria below:

- Latency,
- Jitter,
- Packet loss,
- Unavailability.

As soon as any threshold is not being met, the firewall will select another WAN link with a suitable SLA status for the traffic in question.

This SLA commitment is set through a new SLA object that you can use in several router objects.

Router objects now also include monitoring options that are the same for all gateways specified in the object.

Regardless of the type of traffic, you can also set up a more general configuration to ensure that all communications will automatically be redirected to a backup link when an Internet connection is down.

In the new **Routers** monitoring panel, the status of all gateways and the quality of connections can be looked up in real time, therefore saving time in the event of a failure. If a router issue is detected on a firewall, a probe will warn the user.

This monitoring data can be exported in .csv format.

SD-WAN can be managed from SMC on SMC firewalls in at least version 4.3.3.

[Find out more](#)

Configuring routing from SMC

Routing can now be configured in SMC. It can be accessed in read/write mode on SNS firewalls in at least version 4.2.4, and in read-only mode on firewalls in version 3.7 and upwards. Only IPv4 is supported.

In SMC, in the new **Routing** tab of each firewall's settings, configure and deploy:

- static routes,
- return routes,
- a default route,
- dynamic routing settings.

Routing configurations already found on SNS firewalls can now also be looked up in the **Routing** tab.

This new feature therefore makes it possible to look up routing configuration and prepare changes even when firewalls are offline.



For example, in the static route configuration in SMC, dedicated routes to Virtual IPsec interfaces (VTIs) can be created in route-based VPN topologies. Below is the feature allowing you to view all types of interfaces in SMC.

There are new consistency checks that allow you to check the compatibility of the routing configuration and guarantee the validity of the deployment.

[Find out more](#)

Viewing all types of network interfaces

In SMC, some interface types could already be viewed, added and modified in the **Interfaces** tab of each firewall's settings. It is now possible to retrieve all existing types of interfaces on SMC firewalls in SMC. Wi-Fi, dialup, IPsec, Loopback, GRETUN, GRETAP and USB/Ethernet interfaces are shown in read-only mode as "Other interface" in the **Interfaces** tab.

All of these interface types can be used in the SMC routing configuration.

[Find out more](#)

Managing administrators

"root" account password

You can now set the "root" account password, which will allow you to access the SMC server in command line, when you manually initialize the server from the virtual environment. Previously, this password was set in the SMC initialization wizard, which can be accessed from your web browser.

[Find out more](#)

Customizing the querying of LDAP authentication servers

You can now change the LDAP attributes used by default in SMC to query authentication servers, by using three new environment variables.

[Find out more](#)

Filter and NAT rules

Naming copied rules

When a rule with a customized name is copied then pasted in the same context (firewall, folder or rule set), the "_copy" suffix is now added to the end of the name. This makes it possible to keep track of the relationship with the original rule and makes it easier to create rules with similar properties and names.

If the rule is pasted in a different context and a rule with the same name does not yet exist, the name will remain the same.

When a rule with a name generated by default by the system is copied and pasted, a new default name will be assigned to it.

Integrity of SMC server binary files

Checking the integrity of binaries

SMC binary files are now signed to guarantee better protection from corruption.



Refer to [Downloading this version](#) to find out the new procedure for checking binary files.



SMC 3.2.1 fixes

SMC update

Update process

Support reference 84277

During the SMC update process, errors that were not serious and did not affect the update process would appear in command line mode. The server now only shows relevant errors.

Managing administrators

Authentication via OpenLDAP

Support reference 84152

In the LDAP authentication settings of the **Administrators** menu, the **ID** field of the connection account was renamed **Administrator DN** for OpenLDAP servers. The expected ID format for this field is a DN (without the base DN), such as "cn=administrator".

Configuration of SNS firewalls

Naming firewalls

Support reference 84452

The error message and audit log generated during an attempt to create a firewall with the same name as an object found in the database have been improved to indicate that a firewall or an object with the same name already exists.

Configuration deployment

Synchronizing nodes of a cluster

Support reference 84333

When the automatic synchronization of an HA cluster was disabled through the environment variable `FWADMIN_HASYNC_ON_DESYNCHRO`, deploying the configuration on a cluster would automatically desynchronize nodes. This issue has been fixed.

VPN topologies

Deploying an IKEv2 topology

Support reference 84230

When an IKEv2 VPN topology is deployed from SMC, changing a peer's settings directly on an SNS firewall no longer causes any server errors.



Failed tunnel negotiation

Support reference 84490

The negotiation of a tunnel fails whenever a peer's certificate contains the firewall's contact IP address in the certificate's *Subject Alternative Name* field. This is because the firewall will use this address as the peer's **Local ID**.

To prevent this from happening, the use of the certificate's *Subject* field as the peer's **Local ID** can be forced by setting the `FWADMIN_CERT_SUBJECT_AS_PEER_LOCALID` variable to "True". This variable is set to "False" by default.

Reading logs

Audit logs

Support reference 84279

Logs regarding anonymous users were generated in audit logs. As such information is not relevant, these logs are no longer generated.



Resolved vulnerabilities for SMC 3.1.6

Server protection

Protection against denial of service attacks

A moderate severity vulnerability was fixed after the OpenSSL and NodeJS components were upgraded.

Details on this vulnerability can be found on our website
<https://advisories.stormshield.eu/2022-011/>.



SMC 3.1.6 fixes

Authorities and certificates

Access to the Certificate Revocation List

SNS firewalls no longer return an error when a certificate is deployed with the value “any” as the Local IP address for CRL verification. Support reference 84433



SMC 3.1.5 fixes

SMC update

Updating from 2.8.x to 3.1.4 version

Support reference 84331

Because of an issue during migration of the authentication configuration on the SMC server, it is not possible to update from a 2.8.x version to the 3.1.4 version. Version 3.1.5 fixes this issue. You can now update from SMC 2.8.x to SMC 3.1.5.

SNS firewall monitoring

Status of licensing options

Support reference 84121

When at least one of the license options Breach Fighter, Extended Web Control, Kaspersky, Stormshield Vulnerability Manager and Industrial Security Pack had expired for a firewall, SMC displayed the **Critical** status, even if the option was no longer used.

The warning for the imminent expiry of license options is now disabled by default.

The [Administration guide](#) will help you enabling the feature.

Configuration of SNS firewalls

Managing network interfaces

Support reference 84270

SMC could not display the network interfaces of an SNS firewall which used an interface of the type aggregate. This issue has been fixed and SMC now automatically displays all the types of managed interfaces.



SMC 3.1.4 fixes

SMC update

Updating from 2.8.x to 3.1.3 version

Support references [189860CW](#) and [189875CW](#)

Because of an issue during migration of the authentication configuration on the SMC server, it is not possible to update from a 2.8.x version to the 3.1.3 version. Version 3.1.4 fixes this issue. You can now update from SMC 2.8.x to SMC 3.1.4.



SMC 3.1.3 new features

Managing administrators

Managing connections to external authentication servers

Connections to LDAP, OpenLDAP and Radius authentication servers can now be configured directly in the web interface of the SMC server.

As a result, administrator accounts are more easily and securely managed.

The *auth-server.ini* file, which previously made it possible to configure these connections in command line, no longer exists. If you have configured connections to external servers via this file in the past, the parameters will automatically be migrated in the SMC database and you will find them in the web interface.

[Find out more](#)

VPN topologies

Various versions of the IKE protocol supported on the same firewall

From version 3.7 of SNS firewalls onwards, the same firewall can be used in several topologies configured with various versions of IKE.

If a firewall in a version lower than 3.7 is used in several topologies with various versions of IKE, the consistency checker will report an error that will then prevent the deployment.

Different versions of IKE can be supported on the same firewall only if there is a single firewall in common across several topologies. If several topologies configured with various versions of IKE have several firewalls in common, the version of the topology that was created first in the topology configuration screen will be the one deployed.

Update of the SMC certification authority

In SMC previous versions, the certification authority of the component checking the signature of the license file expired on July 4, 2022. In version 3.1.2, the certification authority has been updated in order to extend the validity period. You must update SMC to be able to continue using your current license after July 4, 2022.



SMC 3.1.3 fixes

Configuration deployment

Deployment on firewalls with TPMs

Support reference 167766PW

Configurations can now be deployed from SMC to an SNS firewall in version 4.2.4 and above, using a TPM. Previously, the progress of the deployment remained stuck at 57% because the use of a TPM was not compatible with the feature that backs up the configuration on the SNS firewall when connection issues occur with SMC. This feature was introduced in version 4.2.4 of SNS.

As this backup feature is enabled by default, you can disable it if you use a TPM, using the environment variable `FWADMIN_FW_DEPLOYMENT_DISABLE_ROLLBACK`. To find out more about this feature, refer to [Deploying a configuration on firewalls](#).

Configuration of SNS firewalls

Detection of changes in the local configuration on firewalls with TPMs

Support reference 168275PW

The feature enabling the SMC server to detect changes performed in the local configuration on an SNS firewall using a TPM is now working correctly.



SMC 3.1.2 fixes

Updating the SMC server

Access to the web administration interface after an update to version 3.1.0

After an update to version 3.1.0, users would no longer be able to access the web interface whenever the **Outgoing interface** field was specified in certification authorities to manage certificate renewals.

This field is now managed individually in version 3.3.1 by firewall, instead of by certification authority.

Users can now access the interface again.

Managing administrators

Logins containing the "." character

Support references 188742CW and 168382PW

Users can now log in again to the SMC server if their logins contain the "." character, regardless of the origin of the administrator account (local, LDAP or Radius).

Connection with an LDAPS account

Support references 168375PW, 168393PW, 188642CW and 188403CW

After an update to version 3.1.2, users can now connect to the SMC server again with an LDAPS account.

Active Updates

Manually updating Active Update databases

Support reference 168411PW

All Active Update databases can now be manually updated again from the file generated by the database download script.



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](#)



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>.



SMC 3.1 fixes

Authorities and certificates

Subject length in certificates

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. **Support reference 184536CW**

Updating certificates in command line

Certificates installed on a firewall can now be updated using the command `smc-install-certificate`. **Support reference 167610PW**

Filter and NAT rules

Filtering by user name

Traffic that filters user names containing apostrophes can now be declared in filter rules. **Support reference 167465PW**

Warning regarding the analysis of encrypted traffic

The consistency check no longer raises a warning when a traffic decryption rule is placed before a rule that analyzes the same decrypted traffic. **Support reference 167465PW**

Updating an SMC server in a version lower than 2.7.0

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. **Support reference 185398CW**

Object database

Searching for object groups

In the window to create or edit object groups, the **Search** field now extends to the IP addresses of objects. **Support reference 167465PW**



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.



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

Domain names used as criteria in filter rules can now be entered in any format, not only as URLs. Support reference 82060

Exporting to CSV files

The value of the **Inspection** field in a filter rule is now correctly exported when it is either *firewall*, *IDS* or *IPS*. Support reference 82236

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

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 reference: 79314**

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 references: 78561 and 79308**

Filter and NAT rules containing domain names can now be imported. **Support reference: 80828**

Rules can now be imported through a CSV file containing some IPRep categories that were previously missing. **Support reference: 80590**

Adaptation of protocol name

In filter rules, the "ldap" protocol has been renamed "ldap_tcp" to maintain consistency between SMC and SMC. **Support reference 82222**

Error during copy and paste

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. **Support reference: 78373**

System

Frequently encountered errors

Errors regarding the connection to the serial port were displayed every five minutes. This issue has been fixed. **Support reference: 81714**



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.



STORMSHIELD

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

Copyright © Stormshield 2022. All rights reserved. All other company and product names contained in this document are trademarks or registered trademarks of their respective companies.