NGFW Security Management Center

6.7.4

Release Notes

Revision B

Contents

About this release

This document contains important information about this release of Forcepoint NGFW Security Management Center (SMC). We strongly recommend that you read the entire document.

System requirements

To use this product, your system must meet these basic hardware and software requirements.

SMC hardware requirements

You can install the SMC on standard hardware.

Component	Requirement
CPU	Intel® Core™ family processor or higher recommended, or equivalent on a non-Intel platform
Disk space	■ Management Server: 6 GB ■ Log Server: 50 GB

Component	Requirement
Memory	■ Management Server, Log Server, Web Portal Server: 6 GB RAM ■ If all SMC servers are on the same computer: 16 GB RAM ■ If you use the SMC Web Access feature: an additional 2 GB RAM per administrator session ■ Management Client: 2 GB RAM The SMC server requirements are the *minimum* requirements. The Management Server and Log Server in particular benefit from having more than the minimum amount of RAM. On high-end appliances that have a lot of RAM, the SMC might not provision the maximum amount of RAM for use by the SMC servers. For information about how to manually modify the provisioning, see Knowledge Base article 10016.
Management Client peripherals	■ A mouse or pointing device ■ SVGA (1024x768) display or higher

CAUTION

To protect the privacy of your data, we recommend using dedicated hardware for all NGFW, SMC, and SMC Appliance installations. For cloud-based virtualization platforms, use an instance type that runs on dedicated hardware. For on-premises virtualization platforms, install the NGFW Engines, SMC components, or SMC Appliance on a hypervisor that does not host any other virtual machines. For third-party hardware, do not install any other software on the computer where you install the NGFW Engines or SMC components.

Operating systems

You can install the SMC on the following operating systems. Only 64-bit operating systems are supported.

Linux	Microsoft Windows
■ CentOS 6 and 7 ■ Red Hat Enterprise Linux 6 and 7 ■ SUSE Linux Enterprise 12 and 15 ■ Ubuntu 16.04 LTS and 18.04 LTS	Standard, Datacenter, and Essentials editions of the following Windows Server versions: ■ Windows Server 2019 ■ Windows Server 2016 ■ Windows Server 2012 On Windows 10, you can install the SMC in demo mode. You can also install the Management Client.

We recommend that you only use operating system versions that are currently supported by the vendor.

Other versions of the listed operating systems might be compatible, but have not been tested. Only U.S. English language versions of the listed operating systems have been tested, but other locales might also be compatible.

Web Start client

The Web Start distribution of the Management Client requires that a 64-bit Java Runtime Environment (JRE) is installed on the operating system.

Web Start is certified to run only on the listed official operating systems. However, it can also run on other operating systems that have JRE installed, for example, on macOS 10.9 or higher and additional Linux distributions. JRE 1.8.0_201 or a later critical patch update (CPU) release is required.

Note

SMC 6.7 is the last major version that will support using Java Web Start to access the Management Client.

Build number and checksums

The build number for SMC 6.7.4 is 10833. This release contains Dynamic Update package 1248.

Use checksums to make sure that files downloaded correctly.

- smc_6.7.4_10833.zip

```
SHA1SUM:
656a44207c0ced57c6dba5b8f8cd45146e7fc007

SHA256SUM:
ea2267ec6f352d7c62c65a393cb33094acf39d55f2a504f7dd8808cbc80cd2b0

SHA512SUM:
054c86c94a8cea3601c706cb99f38c84
b92236d8602e7784420cf5f3b03cef8e
a15c63ddf92c796f5ea88c0e9dadf359
1a64654761b390c3cba33a4252afa86e
```

- smc_6.7.4_10833_linux.zip

```
SHA1SUM:
da8c4d632b3c8ca5b43d7517327a136945b28b0f

SHA256SUM:
61c7be25d8b6d56c96e85acecf32a42a1055eeee201b31cac0519853dd4b7630

SHA512SUM:
2086ba76d244055bdc93306a133632eb
08558cccb41effc2b4d9fb0d91304504
daa084660e987799c63b953540dd68a2
facc7f210e81b374adc9e4cd96827d56
```

- smc_6.7.4_10833_windows.zip

```
SHA1SUM:
578409a16c8d859eb29b65109be62351cccd8b90

SHA256SUM:
8706d372f305dac56b191aadbafe9189444f202d87b47eb28b69a1218e1de85d

SHA512SUM:
6041aad9bb7bb2ed389be8aaaaebe39d
220674b115c387da75ce4472bfe15216
b2d4f23574cc95bfd14e664ae837f629
dd8131d4b3f83e3388daf590aa4a10c6
```

- smc_6.7.4_10833_webstart.zip

```
SHA1SUM:
78cdeccb9790c54a038d1abcee0cf8c7b6bbb32a

SHA256SUM:
90fab64ceeeb8a0b67ceba159978833632c44fe797ab811d6733c441e8b5117c

SHA512SUM:
132fdb37e7dd6ca277b838e59ebbaad9
a4758a79b2ba08e3caa9051c5b0198c0
9a6f0f3e0beda2ad1501f2b7ffc32f1e
3d919eee8325b65139a79daa8ac8861b
```

Compatibility

SMC 6.7 can manage all compatible Forcepoint NGFW Engine versions up to and including version 6.7.

Important

Some versions of Forcepoint NGFW have reached end-of-life status and no longer receive maintenance releases that contain security updates. Even though these Forcepoint NGFW versions might be compatible with the SMC, we recommend that you use a Long-Term Support version that is still supported. For more information about the Forcepoint NGFW lifecycle policy, see https://support.forcepoint.com/ProductSupportLifeCycle.

SMC 6.7 is compatible with the following component versions.

- Forcepoint Next Generation Firewall (Forcepoint NGFW) 6.3 or higher
- McAfee Next Generation Firewall (McAfee NGFW) 5.10
- Stonesoft Firewall/VPN Express 5.5
- McAfee ePolicy Orchestrator (McAfee ePO) 5.3 or higher
- McAfee Enterprise Security Manager (McAfee ESM) 9.2.0 or higher (9.1.0 CEF only)

New features

This release of the product includes these new features. For more information and configuration instructions, see the *Forcepoint Next Generation Firewall Product Guide* and the *Forcepoint Next Generation Firewall Installation Guide*.

On-premises DLP integration

You can now integrate ICAP servers with Forcepoint NGFW to provide DLP scanning in the File Filtering Policy for outbound file transfers.

There are some limitations when you use ICAP servers with Forcepoint NGFW for DLP scanning. For more information, see Knowledge Base article 17727.

Enhancements

This release of the product includes these enhancements.

Enhancements in SMC version 6.7.0

Enhancement	Description
Improvements to rule validity time configuration	New options for defining rule validity time allow you to define rule validity time more precisely. It is now also possible to define when individual rules start being enforced, and when the rules automatically expire. When you upgrade to version 6.7, existing rule validity times are automatically converted to use the new rule validity time options. However, some previous rule validity time options are no longer supported in version 6.7 and higher. If you used rule validity times in a previous version, check your policies to make sure that the rule validity time options match as intended.
More granular log management permissions in Administrator Role elements	You can now separately select permissions to export logs, archive logs, and delete logs in Administrator Role elements.
Support for forwarding log data using the Kafka plugin	You can now forward log data from the Management Server and the Log Server in JSON format as Kafka topics to an Apache Kafka cluster.
Optimization of URL categories	When you upgrade to SMC 6.7 or higher, URL categories are optimized and reorganized into five top-level URL Category Groups: ■ **Security** — Group of categories known to pose a security threat ■ **Reputation** — Group of categories that might have security implications ■ **Legal Liability** — Group of categories that contain content related to a potential age restriction or legal infringement ■ **Bandwidth** — Group of categories known to consume bandwidth resources ■ **Baseline** — Group of categories related to general web access traffic Action might be needed if you have enabled ThreatSeeker for URL categorization for an NGFW Engine in the Engine Editor and you use ThreatSeeker categories for URL filtering in Access rules. For more information, see Knowledge Base article 17133.
QinQ inspection support	Deep inspection now supports inspection of double-tagged VLAN (QinQ) traffic with layer 2 interfaces in inline or capture mode.

Enhancements in SMC version 6.7.1

Enhancement	Description
Improved default values in VPN Profiles	The default values that are selected when you create a new VPN Profile element have been changed to better meet the needs of typical users.

Enhancements in SMC version 6.7.3

Enhancement	Description
Improvements to importing elements	There is a new option for importing elements that imports only new elements and ignores all conflicts.

Resolved issues

These issues are resolved in this release of the product. For a list of issues fixed in a previous release, see the Release Notes for the specific release.

Description	Issue number
When Virtual NGFW Engines are used as external VPN gateways in a policy-based VPN, moving the Policy-Based VPN element to another administrative Domain also moves the Master NGFW Engine that hosts the Virtual NGFW Engines.	SMC-19761
When you preview a report, you can only view the details for one statistical item in each report section.	SMC-25938
When you select an NGFW Engine node in the Home view, the appliance diagram might not show the correct details.	SMC-26125
Policy installation fails if more than three NetLink-specific DNS IP addresses are defined.	SMC-26218
When there are a large number of NGFW Engines, the Log Server might use a large amount of memory for storing Correlation Situations that are processed on the Log Server.	SMC-26322
In the Web Portal, the Action, Authentication, and Logging cells in policy snapshots do not show all of the configured options.	SMC-26467
When you set the Situation to ANY in an exception rule in an Inspection Policy, the correlation configuration is not generated for Correlation Situations that are processed on the Log Server.	SMC-26574
You cannot filter or aggregate log entries based on MAC addresses.	SMC-26586
The Management Client unnecessarily keeps the history of policy upload tasks in memory, which can cause the Management Client to use too much memory.	SMC-26594
After you have configured PIM multicast routing for an NGFW Engine, you cannot delete the NGFW Engine element.	SMC-26702
When you add several routes to the routing view at the same time, only one of the routes might be updated in the antispoofing view.	SMC-26723
It is possible to use the add route action in the SMC API even though the NGFW Engine element is locked for editing the in the Management Client.	SMC-26797
In environments with Master NGFW Engines, connection monitoring using the SMC API might fail.	SMC-26888
The "Advertise Firewall's Contact Address to ECA Clients" option does not work when NGFW Engines are added to an existing ECA configuration. If a roaming user with the ECA Client moves to a newly added NGFW network, it does not accept the received configuration.	SMC-26908
Searching for duplicate elements using the SMC API does not work with the filter_context query parameter.	SMC-27091

Description	Issue number
In very rare cases, when you are editing an NGFW Engine element that has a large number of VPN Sites, if you save and install the policy while the view is refreshing, the VPN Sites are removed, which causes the policy installation to fail.	SMC-27108
When monitoring views for multiple NGW Engines are open at the same time, the Management Client user interface might stop responding.	SMC-27182
When a NAT rule that forwards traffic to a proxy uses an application tag instead of a network application as the service, the NAT rule is ignored.	SMC-27216
The SMC API does not correctly handle Group elements that are used in VPN Sites.	SMC-27300
When there is a backup Management Server and Log Server, the status of the backup Log Server is shown as "Not Monitored" when you set the backup Management Server to active.	SMC-27603
When you change the value of the "Decompress Archives and Rematch Content" action option for a rule with the Allow action in a File Filtering Policy, you cannot commit the change. The following message is shown: "Select at least one file scanning method".	SMC-27606
When you forward log data to a Kafka service, "KAFKA_TOPIC" is shown instead of the actual value of the configured Kafka topic if you use TLS encryption.	SMC-27616
SMC Web Access might stop working even though the number of concurrent sessions is under the limit. The following message is shown: "There are too many active connections right now, please try again later". For more information about the limit for the number of concurrent sessions, see Knowledge Base article 17248.	SMC-27653
If you install the first policy for a new NGFW Engine as part of a policy installation on multiple NGFW Engines, the policy installation might fail if the NGFW Engines are running different software versions.	SMC-27682
The Management Client incorrectly allows you to define VPN options in a rule with the Continue action. The generated firewall configuration includes a rule with the Allow action.	SMC-27686
SMC versions 6.5.14 and 6.7.3 do not include QoS exceptions for VPN tunnels in the generated firewall configuration. When you edit the VPN mode, QoS exceptions are not saved.	SMC-27705
If a member of an LDAP group does not belong to the BaseDN, a full LDAP group search might fail and not show any other users or groups.	SMC-27716
If log files are stored on several Log Servers, a log export might not export all filtered log entries.	SMC-27829
When a Logging Profile element contains ignore fields, saving the Logging Profile element fails.	SMC-27863
When you run a policy refresh task for Master NGFW Engines and Virtual NGFW Engines that have different policies, the progress tab might show that the task has stopped working even though the task finished successfully.	SMC-27944
When you change the value of the VPN Type option to only "SSL VPN Tunnel" for a VPN endpoint that is used in a mobile VPN, policy installation fails.	SMC-28001
The Home view might show that there are pending changes for a Virtual NGFW Engine after you refresh the policy on Master NGFW Engines and Virtual NGFW Engines.	SMC-28099
After a few policy installations on a Master NGFW Engine, sending commands to the NGFW Engine or opening monitoring views might fail. The following message is shown: "Element is locked (Policy refresh)".	SMC-28122
The -nodiskcheck option for the sgBackupMgtSrv command line script does not work as intended.	SMC-28169

Description	Issue number
When a Log Server has been unavailable, the Management Server might not send correlation policies to the Log Server after it becomes available again.	SMC-28223

Installation instructions

Use these high-level steps to install the SMC and the Forcepoint NGFW Engines.

For detailed information, see the *Forcepoint Next Generation Firewall Installation Guide*. All guides are available for download at https://support.forcepoint.com/Documentation.

Note

The sgadmin user is reserved for SMC use on Linux, so it must not exist before the SMC is installed for the first time.

Note

If you install the SMC on Windows and Windows Defender is enabled, it might take a long time to activate a dynamic update package. For more information, see Knowledge Base article 14055.

Steps

1) Install the Management Server, the Log Servers, and optionally the Web Portal Servers.

2) Import the licenses for all components.
   You can generate licenses at https://stonesoftlicenses.forcepoint.com.

3) Configure the Firewall, IPS, or Layer 2 Firewall elements in the Management Client from the **Configuration** view.

4) To generate initial configurations, right-click each NGFW Engine, then select **Configuration** > **Save Initial Configuration**.
   Make a note of the one-time password.

5) Make the initial connection from the NGFW Engines to the Management Server, then enter the one-time password.

6) Create and upload a policy on the NGFW Engines in the Management Client.

Upgrade instructions

Take the following into consideration before upgrading the SMC.

Note

The SMC (Management Server, Log Server, and Web Portal Server) must be upgraded before the NGFW Engines are upgraded to the same major version.

- SMC 6.7 requires an updated license.
  - If the automatic license update function is in use, the license is updated automatically.
  - If the automatic license update function is not in use, request a license upgrade on our website at https://stonesoftlicenses.forcepoint.com. Activate the new license in the Management Client before upgrading the software.
- To upgrade a lower version of the SMC to 6.7, we strongly recommend that you stop all SMC servers and create a backup before continuing with the upgrade. After creating the backup, run the appropriate setup file, depending on the operating system. The installation program detects the old version and does the upgrade automatically.
- When you upgrade the SMC, the dynamic update package that is included with the SMC installer is imported and activated. However, if a newer version of the dynamic update package has previously been imported or downloaded before the upgrade, the newest version is activated instead.
- You can upgrade from the following SMC versions:
  - 5.6.2 – 6.4.10
  - 6.5.0 – 6.5.15
  - 6.6.0 – 6.6.5
  - 6.7.0 – 6.7.3

  Versions lower than 5.6.2 require an upgrade to one of these versions before upgrading to 6.7.4.
- Before upgrading, make sure that you have removed all elements related to McAfee Endpoint Intelligence Agent (McAfee EIA). Also remove all references in Access rules.
- SMC API version 6.6.0 is the last version that provides backward compatibility for version 5.10. Starting from version 6.6.1, you must update scripts that use the version-specific URI for version 5.10 to use the version-specific URI for version 6.5.

Known issues

For a list of known issues in this product release, see Knowledge Base article 17718.

Find product documentation

On the Forcepoint support website, you can find information about a released product, including product documentation, technical articles, and more.

You can get additional information and support for your product on the Forcepoint support website at https://support.forcepoint.com. There, you can access product documentation, release notes, Knowledge Base articles, downloads, cases, and contact information.

You might need to log on to access the Forcepoint support website. If you do not yet have credentials, create a customer account. See https://support.forcepoint.com/CreateAccount.

Product documentation

Every Forcepoint product has a comprehensive set of documentation.

- *Forcepoint Next Generation Firewall Product Guide*
- Forcepoint Next Generation Firewall online Help

Note

By default, the online Help is used from the Forcepoint help server. If you want to use the online Help from a local machine (for example, an intranet server or your own computer), see Knowledge Base article 10097.

- *Forcepoint Next Generation Firewall Installation Guide*

Other available documents include:

- *Forcepoint Next Generation Firewall Hardware Guide* for your model
- *Forcepoint NGFW Security Management Center Appliance Hardware Guide*
- *Forcepoint Next Generation Firewall Quick Start Guide*
- *Forcepoint NGFW Security Management Center Appliance Quick Start Guide*
- *Forcepoint NGFW SMC API Reference Guide*
- *Forcepoint VPN Client User Guide* for Windows or Mac
- *Forcepoint VPN Client Product Guide*

Published 26 May 2020