Forcepoint

NGFW Security Management Center

6.7.5

Release Notes

Revision A

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 6.7.5 is 10834. This release contains Dynamic Update package 1271.

Use checksums to make sure that files downloaded correctly.

- smc_6.7.5_10834.zip

```
SHA1SUM:
5cef7f887f1e7fcea9ddf6f75bc4b32f10faf000

SHA256SUM:
7e234e1704f4ea9b906d03dae917e67d7be8c0d1b97e8ff656fb87fd960b0791

SHA512SUM:
b661cab08d36793dc2b4ac938067225e
8b762a52f5fcd653c101ccb3b80aa823
ed940ae2a8fa117b71b0fe09e32b9b75
98bc4e155fe22583f9dc2284f7ff1f97
```

- smc_6.7.5_10834_linux.zip

```
SHA1SUM:
55a6703ae3559c6b517ae1a1e05f06c0a730cdd8

SHA256SUM:
70d01f6bc48b583ae8eec4f880a1c21579cbac28c4de7ccccd242b01e119b9a3

SHA512SUM:
5118691935da98c83e182c08656d21e6
dcba28f443ff878e14eead0944fecf82
d60f7bfe50ce79915f966b4fa02e91fb
ec1f5662c2be21d98e3adfcf2962d968
```

- smc_6.7.5_10834_windows.zip

```
SHA1SUM:
9cd138fda4ae423fc6a6fbb28eadcd8a33857a1d

SHA256SUM:
8e101167057bb53499c0f0299a0584c51af9c96ac8775c9def3ee8f061cef7af

SHA512SUM:
ce89a850bf037e18e46b8b00898c070c
6ba511aed9045bf82edaefd88b5f4742
005723604da2b6f0a503888da52942d1
96f0b1e57f07a283e6ec0e8cc4a800b5
```

- smc_6.7.5_10834_webstart.zip

```
SHA1SUM:
9e40f790d796fd343a66207a34e4228592716ba5

SHA256SUM:
cd06ae979d7154f390ac834c3ad5ecbabf1d6454f1c0db168209f8a2709d67c6

SHA512SUM:
cd6175cef00c2171add24aad4a7088bf
84651508e9f3cfe9455f2ce41bbebafe
f0c095a108b2d1d7d4cf2ddf0c25963c
47c2b1b8ca24ff05e3bf9d32a54a6f5e
```

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.

Enhancements in SMC version 6.7.5

Enhancement	Description
Option to export elements without referenced elements	It is now possible to export an element without the export including referenced elements. To export elements without referenced elements, edit the <installation folder>/data/SGConfiguration.txt file and add the following parameter: `EXPORT_PERMISSION_SETTINGS=false`

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 the "Lock Management Client Window After the User Session is Idle" option is enabled, the Management Center Locked popup is shown on top of all windows. The popup remains on top of other windows unless it is minimized.	SMC-24085
When you duplicate a system Situation element, the original system situation might no longer be included in the configuration for the NGFW Engine.	SMC-24458
After you reconnect the Management Client session, the Info and Drill-Down panes in the Home view are not updated until you select an element.	SMC-25377
The Management Server does not request automatic license updates and downloads even though the Management Server regularly queries the status of licenses from the Forcepoint license server.	SMC-28425
When a WebSocket connection to the SMC API is closed, the related session is not closed immediately.	SMC-28451
The Convert Engine to Master NGFW Engine and Virtual NGFW Engines wizard fails to apply changes on the "Define Interface for the Master NGFW Engine" page when you try to assign multiple interfaces to a Virtual Resource at the same time.	SMC-28595
When you create custom Situation elements, the elements might be shown in the Management Client by the situation ID only.	SMC-28617
The first policy refresh after upgrading the SMC might fail.	SMC-28626
For external tests, the path to the script file on the command line has a limit of 80 characters.	SMC-28639
In rare cases, normal logs might be sent as alerts.	SMC-28748
When the SMC API is used to add an IP address to an existing Virtual NGFW Engine interface, antispoofing is not configured correctly.	SMC-28781

Description	Issue number
The Control Management Servers dialog box always tries to connect to the active Management Server, even if it is unreachable.	SMC-29139
The DHCP tab is not shown in the Info pane for NGFW Engines in the Layer 2 Firewall role.	SMC-29144
When the path to the script to execute after the task in an Export Log Task includes spaces, script execution fails.	SMC-29221
When you delete a Virtual NGFW Engine, the Master NGFW Engine might not be notified of the deletion. As a result, the policy of the Master NGFW Engine refers to a Virtual NGFW Engine that no longer exists and policy installation fails.	SMC-29306
Hardware monitoring incorrectly reports Half / Forced for an interface when the NGFW Engine does not provide data for send values for speed, duplex, and auto-negotiation. This issue occurs on interfaces where negotiation settings cannot be changed.	SMC-29310
When you create an inspection rule from a log entry, saving the policy fails and an "invalid element" error message is shown.	SMC-29317
The Routing Monitoring view can take several minutes to load. In addition, while the Routing Monitoring view is loading, routing monitoring cannot be performed using the SMC API.	SMC-29321
The details are not always refreshed when you select different NGFW Engine nodes in the Home view.	SMC-29380
Viewing or comparing snapshots might fail and the following error message might be shown: "Database problem. DB Transaction failed while processing transaction".	SMC-29529
Aliases for which no value has been defined are not visible in the Engine Editor. The Alias elements can still be edited outside of the Engine Editor.	SMC-29581
When the Log Server has been configured to forward log data in different formats to different external hosts, the Log Server might send log data in the wrong format for some hosts.	SMC-29701
When you create a new NetLink add it to an Outbound Multi-Link element that is used for NAT, the configuration that is generated for the NGFW Engine might not be correct.	SMC-29803
When User elements from different LDAP domains have the same name, user, or group, you cannot use the User elements in the same rule. One of the User elements is ignored.	SMC-30016
When you configure host name for the SSL VPN Portal, host names that end with .ye are not accepted.	SMC-30353
When there is an empty Group element in the source or destination cell of a rule, the whole rule might be ignored even if there are other elements in the same source or destination cell.	SMC-30542
When you use an FQDN as the host name of the HTTP proxy that the NGFW Engine uses to connect to anti-malware database mirrors, the following warning is incorrectly shown during policy installation: "The proxy IP Address X defined in the Anti-Malware settings in invalid". The HTTP proxy is configured correctly.	SMC-30757
If there are many policy snapshots, upgrading the Management Server might fail.	SMC-30769
When you use Group elements in the Routing view, the routing table does not show all networks and IP addresses in the groups correctly.	SMC-30800
The "Only One Logon Session for Each User" option on the Password Policy tab of the Global System Properties dialog box should invalidate an administrator's previous session and allow the administrator to start a new session. The option incorrectly prevents administrators from logging on if there is already an existing session.	SMC-30831

Description	Issue number
When you use the "IP Protocol" field as a field resolver in a Logging Profile element, the value is not correctly resolved.	SMC-30926

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 – 6.5.17
  - 6.6.0 – 6.6.5
  - 6.7.0 – 6.7.4

  Versions lower than 5.6.2 require an upgrade to one of these versions before upgrading to 6.7.5.
- 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*

© 2020 Forcepoint
Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint.
All other trademarks used in this document are the property of their respective owners.
Published 10 September 2020