NGFW Security Management Center

Release Notes

6.6.5

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 - 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 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.

Build number and checksums

The build number for SMC 6.6.5 is 10727. This release contains Dynamic Update package 1227.

Use checksums to make sure that files downloaded correctly.

- smc_6.6.5_10727.zip

```
SHA1SUM:
cc04d73d2a4179f450bcdeeebf8f00be5267d542

SHA256SUM:
b44266b544753d2f41495db21c6fa7bdec7ab0e1a64be20e08701d917fde1788

SHA512SUM:
1a1107a0e21a749b1ffcd5af63056090
d833309b76486fb8f71e578d124cf13c
23fd9663286dffe92e29d453d788c512
446fafa59bc7d15e3e134bf34badbc1f
```

- smc_6.6.5_10727_linux.zip

```
SHA1SUM:
f3fc6891f768b3d1624b6d2ee901d1bd4879214c

SHA256SUM:
e354799698c8a0a3e0d8caeb4a6226d01febcb33ec0f3f301a42a1dc4689bf40

SHA512SUM:
80bd656a76ff9edf7efa1594e9ef1541
f95a3775bcd2a0a8ec55efef79805f8a
e6cc9d81d271c2db72b4a756fa9f7f3a
e28ffb0032a6451a4f738f9782b8c5c4
```

- smc_6.6.5_10727_windows.zip

```
SHA1SUM:
95d66404e721152d3f81660f6623e0ff96d6d08b

SHA256SUM:
a74339f47b483fee6fa9d9c250f1000d5e93534e8beb6823df1e0914f66830e4

SHA512SUM:
19a2e2011ba4c26a09cff81b9c5758da
83fd7695715daa0a73f9e835cb0613cb
ef2fd97f8b2bcb4553b54a71431aaa2b
1d5160abe4c39e5c1d740623c96a5ada
```

- smc_6.6.5_10727_webstart.zip

```
SHA1SUM:
717780cf0231ec2feac758214c2d6f399970d1fd

SHA256SUM:
378d7fd06a334a70ddc676c1c352c069e92c309046fdf849a9e1c7d110564ae9

SHA512SUM:
14b9fad87d6f239cf1994e5390c47c30
502e0b84c6810f5a88ef75ed88f7ac38
f3eca7c2fcd955cdc14af6607036bba0
e1039c54169b66e3a7e729fdb98903fb
```

Compatibility

SMC 6.6 can manage all compatible Forcepoint NGFW Engine versions up to and including version 6.6.

⚠ **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 6.6 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*.

Dynamic link selection for SD-WAN

The VPN links that are used for Multi-Link traffic from applications and protocols, and traffic associated with QoS classes are now automatically selected based on quality metrics defined for the network applications, protocols, and QoS classes. You can now also specify how different types of ISP connections are used for specific types of traffic. For each type of ISP connection, you can specify that:

- The ISP connection is used for the specified type of traffic unless an ISP connection with significantly higher quality is available.
- The ISP connection is used for the specified type of traffic only if the quality of the other ISP connections is too low or the other ISP connections are not available.
- The ISP connection must not be used for the specified type of traffic.

Storage and browsing of log data locally on NGFW Engines

You can now save copies of the most recent log entries locally on the NGFW Engine. Alert entries are also saved locally on the NGFW Engine. You can browse the saved log and alert entries on the command line of the NGFW Engine even if the log and alert entries have already been sent to the Log Server. The length of time for which the log and alert entries are stored depends on the size of the NGFW Engine’s disk and the volume of log data. You can also set limits for how long log entries are stored, and how much disk space can be used for storage.

LLDP support

NGFW Engines can now use the Link Layer Discovery Protocol (LLDP) to send information, such as information about interfaces and MAC addresses on the NGFW Engine, to directly connected devices on the network. The NGFW Engines can also receive information that other devices on the network send. In the Management Client, you can now monitor information that the NGFW Engine has received about devices in directly connected networks.

SMC Web Access

You can now enable the SMC Web Access feature to start and run the Management Client in a web browser.

This feature is not available on the SMC Appliance.

Support for LTE modems on NGFW Engines in the Firewall/VPN role

You can now use LTE modems for mobile broadband connections on 4G networks with NGFW Engines in the Firewall/VPN role. Support for LTE modems is only available on specific purpose-built NGFW appliance models (NGFW 50 Series).

Enhancements

This release of the product includes these enhancements.

Enhancements in SMC version 6.6.0

Enhancement	Description
Easier forwarding to a proxy	You can now configure forwarding traffic to a proxy or host directly in the Access rules rather than in the NAT rules.
Shared interfaces on Master NGFW Engines	Layer 3 physical interfaces on Master NGFW Engines in the Firewall/VPN role can now be shared interfaces. • You can now connect Virtual Firewalls to the same network without dedicating one physical interface or VLAN for each Virtual Firewall. • The Virtual Firewalls can now communicate with each other without an external switch or router. • Link aggregation is supported on Virtual Firewalls.
IPv6 support for user authentication	User authentication now supports IPv6 addresses. Communication between NGFW Engines and TACACS+ authentication servers now also supports IPv6 addresses.
Server Pool enhancements	The following enhancements have been made for the Server Pool feature: • You can now use Server Pool elements in NAT rules to apply both source and destination NAT for Server Pool load balancing. • The Server Pool feature now supports IPv6.

Enhancement	Description
New URLs for dynamic updates and engine upgrades	To improve the performance of automatic dynamic updates and engine upgrades, the following new URLs are available in SMC 6.5.0 and higher: - https://autoupdate.ngfw.forcepoint.com/dynup.rss - https://autoupdate.ngfw.forcepoint.com/ngfw.rss **Note:** The SMC automatically starts using the new URLs when you upgrade to SMC 6.5.0 or higher and activate the dynamic update package that includes the new URLs. The new URLs use a content distribution network (CDN) to allow the SMC to download dynamic update packages and engine upgrade files from the geographically closest server. The legacy https://update-pool.stonesoft.com/index.rss URL remains available for backward compatibility and as a backup for the new URLs.
Configurable update services for dynamic updates and engine upgrades	New Update Service elements define sets of URLs for automatic dynamic updates and engine upgrades. In SMC 6.5.0 and higher, the SMC automatically uses Update Service elements that include both the new URLs and the legacy URL. No action is needed to start using the Update Service elements that include the new URLs. Starting from SMC 6.5.2, you can optionally change which Update Service element is used for automatic dynamic updates and engine upgrades. For more information, see Knowledge Base article 16589.
Audit log improvements	Audit entries now include information as text about the changes made to elements when the following configurations are modified: - VLAN interfaces on Master NGFW Engines - Virtual Resources on Master NGFW Engines - IP addresses on Virtual NGFW Engines - Antispoofing on Virtual NGFW Engines - Announced Networks for dynamic routing on Virtual NGFW Engines - External BGP Peers on Virtual NGFW Engines - Matching Conditions in Route Maps on Virtual NGFW Engines - Route Entry Settings in Route Maps on Virtual NGFW Engines - IP prefix lists on Virtual NGFW Engines - Comments on Virtual NGFW Engines
Improvements in the Pending Changes feature	Improvements in the Pending Changes feature prevent an element from appearing in the Pending Changes list when an administrator clicks OK without modifying the properties of the element.
User interface rendering on macOS	The Management Client now detects the operating system in use. On macOS, for example, the appropriate window control icons and special characters in keyboard shortcuts are shown.

Enhancements in SMC version 6.6.1

Enhancement	Description
Details of User Behavior Events	In the User Dashboard, you can now view related log entries for entries in the User Behavior Events pane.
New option to show disabled tunnels in the SD-WAN dashboard	A new option for viewing disabled tunnels has been added in the SD-WAN dashboard. The new Show Disabled Tunnels option is available in the Tunnels pane on branch home pages and VPN home pages.
Possibility to define the OSPF Area ID as an IP Address	You can now define the OSPF Area ID as an IP address instead of converting it to a decimal number as previously instructed in Knowledge Base article 16319.
Endpoint Information shows the user's computer name	The Endpoint Information pane in the User Dashboard can now show the computer name from which the user is connected.
ECMP option for BGP	You can now set an equal cost multi path (ECMP) value in the BGP configuration using the Management Client.

Enhancements in SMC version 6.6.2

Enhancement	Description
EasyConnect forwarding to the Forcepoint Web Security Cloud	You can now configure EasyConnect to forward web traffic from Forcepoint NGFW to Forcepoint Web Security Cloud. For more information, see Knowledge Base article 10582. ⚠ **CAUTION:** This feature requires NGFW Engine version 6.5.6, 6.6.3, 6.7.0, or higher.

Enhancements in SMC version 6.6.3

Enhancement	Description
NGFW Engine tester	You can now use the Link Status Test on layer 2 interfaces.

Enhancements in SMC version 6.6.5

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 the SMC and the NGFW Engine are deployed in the same network in the Azure cloud, the routing configuration is not generated correctly.	SMC-24162
The throughput limit defined in Virtual Resource elements is not included in the configuration.	SMC-25913

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 6.6 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 6.6, 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.
- 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 – 6.2.5
  - 6.3.0 – 6.3.8
  - 6.4.0 – 6.4.10
  - 6.5.0 – 6.5.11
  - 6.6.0 – 6.6.4

  Versions lower than 5.6.2 require an upgrade to one of these versions before upgrading to 6.6.5.
- 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 16950.

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, Knowledge Base articles, downloads, cases, and contact information.

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*