FORCEPOINT

NGFW Security Management Center

Release Notes

6.7.0

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	- Windows Server 2016 Standard and Datacenter editions - Windows Server 2012 R2 - Windows Server 2008 R2 SP1 On Windows 7 SP1 and 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 6.7.0 is 10815. This release contains Dynamic Update package 1196.

Use checksums to make sure that files downloaded correctly.

- smc_6.7.0_10815.zip

  ```
  SHA1SUM:
  b4d5f4bd2f4e3897997f9465ecf8fe0f59b655e6

  SHA256SUM:
  a701185a9f56befe5ec99e145a9745f2e4aa512f47953e81db083d35310f2057

  SHA512SUM:
  49f40999f0bb62333df7f0bb80aa827c
  5104fbc230bdd3b76ed7c9c9a648c791
  2381ec458955e549c7325c3aa34b1c2b
  41c4268d22fb3f055be63a89d2ab3e27
  ```

- smc_6.7.0_10815_linux.zip

  ```
  SHA1SUM:
  969f8364b03c0420c66c3493dd69a2681f46f4e7

  SHA256SUM:
  046599e307a1f0f904e06d2565051175211b3d723841bab8f893eaf8d7532de4

  SHA512SUM:
  6632a0ce0b70c1644ece54b8c3509605
  75a57fc7244994fa34811a965d4eb061
  11faff4c3942dbf2aa9f0823c3be1800
  d375874d02626c4d79ce9b6a6e05f560
  ```

- smc_6.7.0_10815_windows.zip

  ```
  SHA1SUM:
  eb8afd98253be462b2c6972ac0de7435d3851166

  SHA256SUM:
  67eb118a210f0019d9fb8e12b63200ec7f1cd220c60f83c2fe6a555c6f45adc9

  SHA512SUM:
  e1ba28d526ba58f0e7be0e800937fbb1
  c21fbde72943b256c7ffaf672d80a81f
  baae6454004ee226d856dc2e296f5b5c
  2492b74a21a60cbe14d2f09b478fbad0
  ```

- smc_6.7.0_10815_webstart.zip

  ```
  SHA1SUM:
  23a834283efb2b6fc7ae11e4b1409eb53e1dbd07

  SHA256SUM:
  7cbf09b80917e3b42dbbb10be65f83a7a8a713f7f184fe310b2adf3884f09307

  SHA512SUM:
  a7e511db7b87a9960abab41957b5647b
  5af03adb380ef7c832d4c3f83350cecb
  6b82b4182f7a90d8cc60ece5aa7a3715
  38af2162f0bad446a179c941dfa61e97
  ```

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.
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.

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 you make a change in the SMC API settings in the properties of a Management Server, generated SMC API logs are removed. The SMC API logs are generated when the Generate Server Logs option is enabled in the SMC API settings.	SMC-19039

Description	Issue number
If a node in an NGFW Engine cluster is not online, the Neighbors and Connections monitoring views for the node do not contain any data.	SMC-20336
When you use the same Outbound Multi-Link element in different NAT rules that apply both static and dynamic address translation, only the first NAT rule matches traffic.	SMC-22643

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 – 6.2.5
  - 6.3.0 – 6.3.8
  - 6.4.0 – 6.4.10
  - 6.5.0 – 6.5.10
  - 6.6.0 – 6.6.3

  Versions lower than 5.6.2 require an upgrade to one of these versions before upgrading to 6.7.0.
- 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, 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*