FORCEPOINT

NGFW Security Management Center

Release Notes

6.7.1

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	• 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 6.7.1 is 10819. This release contains Dynamic Update package 1205.

Use checksums to make sure that files downloaded correctly.

- smc_6.7.1_10819.zip

```
SHA1SUM:
3c73b530cdf9d9b18f3d9deb6ab36ef064d52f64

SHA256SUM:
3a4e42f3c06667cfc208fa214d6ac1bdbf3ff57f44288b504f6837b577fa1421

SHA512SUM:
960e5135fc9a75665ba2428cea7af68c
d4e5e5f117a6644a2d3577ccac3df941
413ab38ab0123d46d965028fa25989e2
037d4c167ad3e7b18dd0e469028cc369
```

- smc_6.7.1_10819_linux.zip

```
SHA1SUM:
fe305b04cf1565979f6b21cffe103bb13a4b03c1

SHA256SUM:
e8458149141729409315974 39c75c8c9bb2269a888ad89b9a9d1bccfa65f5f0a

SHA512SUM:
be9abbe74cf39248a66b72ae00e295a7
d4432f4e806f68814fde2b64cea550a6
d646ca0ad3578b19b31cb397eeeab46c
89f25d7fbd15d9a9c22a02ab50e70cc9
```

- smc_6.7.1_10819_windows.zip

```
SHA1SUM:
e48b12ae261fcdf80cee503eef197d439bb5a437

SHA256SUM:
c989cc48f23f3e9d06e50466016ad3d3aff866b6db540b9f14ad7dd2df8304f3

SHA512SUM:
a9c5147515e19166710d2038b35d953c
492c0a461c44f16afe1be886ece8b42b
0ea4143809ff7746a567bf0e498405f5
abd2b87636b71e095e72d05a38a4649c
```

- smc_6.7.1_10819_webstart.zip

```
SHA1SUM:
1f7b8492f1c94ee9e629714c03f7f9408b569202

SHA256SUM:
07d234c9a376a7fa5ac0129c37ae95ccc4e980b9ca0b528c000320cf00da563f

SHA512SUM:
19c55f0f66b562c382d6b95976e45064
67899b3fc6845f24daf64beabfcbf313
f9f5ccd6c3625701584ea19746dab205
b1112fbcc2278eb53df1a1fde21df572
```

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.

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
If the Management Server is configured to automatically download and activate dynamic update packages, the Management Server might repeatedly download a dynamic update package. Multiple SMC backups are created, and multiple alerts are generated because the Management Server attempts to activate a dynamic update package that has already been activated.	SMC-22879
When you click "View Statistics" in the Configuration pane of a Master NGFW Engine home page, the IPS Details overview opens.	SMC-23369
A blacklist entry generated by a Correlation Situation is not generated correctly if the Address option on the Blacklist Scope tab is set to Attacker.	SMC-23680
When there is a VPN validation warning or error for a VPN that includes mobile VPNs, policy snapshot comparison fails. The following message is shown: 'Element <vpn_gw_gw_issue> has no attribute "culprit_gateway_ref_key".'	SMC-23751
Even though ECA provides endpoint client information to the NGFW Engine, Access rules that use endpoint information as the source or destination do not match.	SMC-24007
When users are stored in a user group in an external LDAP domain, retrieving users using the SMC API is slow.	SMC-24011
When you select an entry in the Routing monitoring view, the view stops working. The following message is shown: "Database problem. DB Transaction failed while processing transaction".	SMC-24014
When VPN endpoints have a dynamic contact address or an FQDN as the contact address, VPN validation fails.	SMC-24026
Importing externally signed certificates using the SMC API fails.	SMC-24027
When an External VPN Gateway element has two endpoints with dynamic IP addresses, saving the element fails. The following message is shown: "An error occurred when saving Endpoint X (Dynamic) in external Gateway. IP address IPv4 dynamic is already defined in endpoint Y (Dynamic)."	SMC-24032
When you create a new NGFW Engine in the Firewall/VPN role, VPN endpoints and the automatic site are not automatically configured if you configure the default route using the routing tools.	SMC-24119
After you select the High Priority QoS Class for a NetLink in an Outbound Multi-Link element, you cannot remove the High Priority QoS Class.	SMC-24224
When there are a large number of log entries that match a filter in an overview, opening the Logs view from the overview might take a long time, or cause the Management Client to become unresponsive.	SMC-24280
Opening the properties of an internal certificate fails. The following message is shown: "Invalid parameter: DB Key missing."	SMC-24307
When you use the search bar to search for Host elements, not all Host elements are found.	SMC-24313
When you use User Response elements in a Layer 2 Interface Policy, responses are not sent to users.	SMC-24399
When you edit the regular expression in an existing custom Situation element, the changes are not saved.	SMC-24413

Description	Issue number
In the Home view, the status cards for Virtual NGFW Engines might incorrectly show CPU load statistics.	SMC-24470
When you create a report, it is not possible to configure the report to be sent to multiple email addresses on the Task tab of the Report Operation Properties dialog box.	SMC-24482
When you select an IP address for a BGP Peering element on the Routing branch of the Engine Editor, this list of IP addresses might be too long to show all options.	SMC-24539
When you create a new Active Directory Server element, the default attribute for Userid is cn, which is not a unique attribute within AD domains.	SMC-24544
When you remove a user that has group membership from the internal LDAP domain, user database replication might stop working.	SMC-24620
When you use the SMC API, it is not possible to set all of the same options for third party monitoring that are available in the Management Client.	SMC-24692

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 – 6.5.11
  - 6.6.0 – 6.6.3
  - 6.7.0

  Versions lower than 5.6.2 require an upgrade to one of these versions before upgrading to 6.7.1.
- 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*