FORCEPOINT

NGFW Security Management Center

Release Notes

6.7.3

Revision A

Contents

- About this release on page 2
- System requirements on page 2
- Build number and checksums on page 4
- Compatibility on page 5
- New features on page 5
- Enhancements on page 6
- Resolved issues on page 7
- Installation instructions on page 9
- Upgrade instructions on page 9
- Known issues on page 10
- Find product documentation on page 10

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 6.7.3 is 10831. This release contains Dynamic Update package 1227.

Use checksums to make sure that files downloaded correctly.

- smc_6.7.3_10831.zip

```
SHA1SUM:
718d164b34a95429205458fd52649da77f8039b9

SHA256SUM:
cf06d5f0fa925612af1f0c19d76cdfa774091f77f7bf7090b57a2a4cdcfe4eac

SHA512SUM:
4cae6be15ee96f34257e4bc3b540d8af
0d971f30e9a765ffab6f4fad50ad6cc6
db95ad605b8712054eba7e580ff973fe
9a9a6b525851cccc35ee2c38262a8a16
```

- smc_6.7.3_10831_linux.zip

```
SHA1SUM:
426ce4e25cb89dbff9877fff38ef8db598f25b90

SHA256SUM:
ecc9e68220b8565e275688b86c0797d8d90ede0e37d09903812e9bb128114d4b

SHA512SUM:
568a2b94e2a01d006c8dbda782439603
a894fde634743be143c29f9a7bcc0488
af92394a27c5f977fa98b892376e3222
7cbbf43ecc74ac1c906ec002c976c5c7
```

- smc_6.7.3_10831_windows.zip

```
SHA1SUM:
44d21b0c629d0f68f0e1311f6df711ab65cd26f7

SHA256SUM:
a4e324e6d2c46f606950556b9cbaac39d81df93e3d24b0bc0a81ef31d2a0009a

SHA512SUM:
d36769e83ba505b2430938a4eb358e49
d14f917d8e096455f1afc76526a37719
11ec069740ac79ab2e0d0bceed630be5
8628e04c3263e0d97304357adefe970c
```

- smc_6.7.3_10831_webstart.zip

```
SHA1SUM:
2801e2ee317f6e9bfd5227c2f680e5ac0a159360

SHA256SUM:
58357195393a6ff6bf14cc06224a5b79984795db7d864c15a34cdee7378718b2

SHA512SUM:
719cafa0a66931c7641400089cc4f22a
060a2ec24d0e86e1e8144ff5f52956fd
179421f61135fc70bed09f28a6ccb066
d712e916077cbb4b0597f101fcd0cc52
```

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
If policies are installed on multiple Virtual NGFW Engines at the same time as blacklists are modified and time is being synchronized, the policy installations fail. The following message is shown: "X is currently locked, another command is performed on it".	SMC-23689
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
When there are multiple Management Servers, latency in communication between the servers can cause the replication status to be Postponed.	SMC-24388
If a VPN gateway has two VPN endpoints for an IPsec VPN tunnel, only one of the endpoints must be of the type IPSec VPN. However, if you only have one IPsec VPN endpoint, policy installation fails, and the following message is shown: "The Route-Based VPN tunnel that references the Firewall X is invalid. All Endpoints must be IPsec".	SMC-24477
When there are hundreds of NGFW Engine elements, the Pending Changes pane might load slowly. The Management Client might become unresponsive for several minutes.	SMC-25026
Log-related Tasks might not handle corrupted log data correctly. Corrupted log data can cause the Tasks to fail.	SMC-25043
If a node in an NGFW Engine cluster is in standby mode or is offline, the status of a failed NetLink is reported as Mixed (orange) instead of Error (red).	SMC-25141
A Route-based VPN tunnel might not be included in the configuration for an NGFW Engine if the Default IP Address for Outgoing Traffic option is set as the Loopback Interface.	SMC-25203
When the Security Management Center (SMC) is uninstalled on a Microsoft Windows system, not all the related registry entries are removed.	SMC-25459
After you add or edit a rule in a large policy, the editing view scrolls down.	SMC-25561
External authentication of administrators fails if the Network Policy Server (NPS) for Active Directory is defined using a fully qualified domain name (FQDN).	SMC-25789
Administrators are not replicated to new NGFW Engines if the replication is configured before the NGFW Engine makes initial contact with the Management Server.	SMC-25819
If you have a custom script in the Alert Chain of an Alert Policy, the output of the script changes after upgrading the Security Management Center (SMC).	SMC-25851
The throughput limit defined in Virtual Resource elements is not included in the configuration.	SMC-25913

Description	Issue number
Policy installation fails when including a Link Usage Profile that has more than one link usage exception.	SMC-25918
It is possible to delete a Rule Validity Time element. If the element is used in a policy, deleting the element can cause errors in the policy.	SMC-25922
When you configure a Route-Based VPN Tunnel of the GRE tunnel type with no encryption, the remote IP address is not saved.	SMC-25943
The Log Server might keep counter data that it has previously received in memory. Keeping this data in memory can cause the Log Server to run out of memory.	SMC-25945
In an NGFW Engine cluster, an interface that does not have any Node Dedicated IP Addresses (NDIs) borrows an IP address from another interface and uses the same netmask. As a result, the dynamic routing configuration considers there to be two interfaces that have the same network.	SMC-26002
Elements that are referenced in a Layer 2 Interface policy can be deleted.	SMC-26145
Log forwarding fails when the filter for the log forwarding rule is too big.	SMC-26180
Web Portal users cannot see all options in the Action, Logging, and Authentication cells in Access rules.	SMC-26248
You cannot use the Log URL Categories logging option in rules that terminate connections.	SMC-26269
If the Log Server is unavailable when you install a policy on an NGFW Engine, Correlation Situations that are processed on the Log Server cannot be replicated to the Log Server. If the Log Server is unavailable for an extended time, Correlation Situations consume a large amount of space in the Management Server database.	SMC-26272
When you copy and paste multiple policy validation results, only one of the results is pasted.	SMC-26285
When you select several Master NGFW Engines and try to refresh the current policy, the Management Client might become unresponsive.	SMC-26293
The Password Age and Expiration settings in the Global System Properties dialog box also apply to administrator accounts that have the Always Active option selected. These administrators are not notified when the password is about to expire.	SMC-26313
When the Management Server has been shut down, the replication of active alert notifications from Log Servers might not recover after the Management Server becomes available.	SMC-26362
When you enable or disable an administrator account, the action might fail. The following message is shown: "Database Error Impossible to enable or disable Administrators".	SMC-26422
If you have selected No Client Authentication as the value of the Log Server TLS Certificate Used for Forwarding Logs option in the log forwarding settings for the Log Server, you cannot change the value of the setting to Use Internal Certificate.	SMC-26424
In the properties of a VPN Site element, there are entries in the list on the VPN References tab where the VPN name is not shown.	SMC-26427
It is not possible to set log compression options for VLAN interfaces.	SMC-26528

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 – 6.5.13
  - 6.6.0 – 6.6.5
  - 6.7.0 – 6.7.2

  Versions lower than 5.6.2 require an upgrade to one of these versions before upgrading to 6.7.3.
- 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*

Published 17 March 2020