FORCEPOINT

NGFW Security Management Center

Release Notes

6.7.2

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 6.7.2 is 10827. This release contains Dynamic Update package 1218.

Use checksums to make sure that files downloaded correctly.

- smc_6.7.2_10827.zip

```
SHA1SUM:
da32462904e3f34f496621b4990e44db7849656a

SHA256SUM:
b02ed9c67061c3f54ff6a58ecc41ba5aa4bec723831006416255fa29f44986b7

SHA512SUM:
988c1fb940e21eef578ace6c4b177dc8
bffa6d370d8ac06ecefdd4840cc16664
667ec4d164019c0a498b9f0070373d1c
06742a8aa3c67ae1bc5409eeea3b28fd
```

- smc_6.7.2_10827_linux.zip

```
SHA1SUM:
ec54ade2b993c2b6a4635028dbc63da74745d876

SHA256SUM:
1f13283d5892f9d1344d4131033289cdcd6c0325a33c96b595949537cd0f07ca

SHA512SUM:
69662c2ed810e7b21f83153e585f173f
7cfea29208ec110f8af9b00298402e75
61d7b6fb53cdaf20856553d38c045763
e24479f6ca99ac6d1119336b41d5e5ad
```

- smc_6.7.2_10827_windows.zip

```
SHA1SUM:
6d55bf68e7b2711ab480a3bb993f4352d906dc56

SHA256SUM:
3c31a7cd1459b4d63c33b08237ffa1f0e755ab39970a1a5372f2dc6defe7af77

SHA512SUM:
de5f031bbcdea7639593425d69e8e30c
56501ca2f90ac3467dbdec8201c22c69
e268fcfee4da4d9ae9bb9fdcd2c9a521
fb75909830130ac822ce2f6a8d009de9
```

- smc_6.7.2_10827_webstart.zip

```
SHA1SUM:
f58bb68cd4011ba959831f1aa60cbacc9aba94a9

SHA256SUM:
e91509528732364cf55ee35b9846bddf5401207e0daec0b30690ebef24db106f

SHA512SUM:
b18c666979fcf7a63f859bca0db81f6e
60bc9aedb3498524cfdf8a5e3f11f3af
ab39c40e29cd0d8b5d8906adfc6046b0
fa76b6f913388de14a1c82d8230bbd01
```

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
Vulnerability elements are not filtered correctly in the Management Client when you view Vulnerabilities by Tag.	SMC-23449
If you use the SSM FTP Proxy or the SSM TFTP Proxy in an Access rule, deep inspection must be enabled in the Access rule. Otherwise, the NGFW Engine discards the related connections.	SMC-23530
Policy validation might incorrectly show issues about unreachable rules when rules in a sub-policy have the same source and destination as the Jump rule that references the sub-policy.	SMC-23709
When a Task is run manually, the progress bar does not update automatically.	SMC-24296
If you make changes to VPN endpoints and renew the VPN certificate, the policy installation validation still advises you to renew the VPN certificate.	SMC-24537
Report sections cannot be managed through the SMC API.	SMC-24675
If you use the SMC Web Access feature to run the Management Client in a browser and the Management Client runs out of memory, the previous session instead of a new session opens when you try to reconnect to the SMC.	SMC-24788
It is not possible to change the tunnel type of a Route-Based VPN Tunnel from VPN to another type with no encryption.	SMC-24791
An administrator that does not have unrestricted permissions (superuser) cannot save a new startup session bookmark if the previous session bookmark includes the Logs view.	SMC-24810
Policy installation fails if you use an IP Address List and a Zone element as the source or destination in an Access rule.	SMC-25004
The Management Server might not start after you have saved an Incident Case element that contains a large amount of log data.	SMC-25042
You cannot use some special characters in URL List Application elements, even though the characters are valid according to RFC 3986.	SMC-25122
If the Node-initiated Contact to Management Server option is enabled, the NGFW Engine uses only either IPv4 or IPv6 addresses to contact Management Servers.	SMC-25143
If an administrator has permissions granted for an Administrative domain that is deleted, the administrator is no longer able to do many administrative tasks.	SMC-25178
The Log Server might stop responding after an NGFW Engine element is deleted.	SMC-25215
In rare cases, the Management Client user interface might become unresponsive after opening the Monitoring view.	SMC-25295
Custom Network Applications that have modified ports might not match traffic as expected.	SMC-25321
An administrator that has the Viewer role can see details in the Info panel for NGFW elements that they have not been granted permissions for.	SMC-25332
The Web Start Management Client does not launch after upgrading to Java version 8 update 241. After upgrading to SMC 6.5.12 or SMC 6.7.2, follow the instructions in Knowledge Base article 17991.	SMC-25422

Description	Issue number
Policy validation shows a warning if an element that has one or more IPv6 addresses but no IPv4 address is used in an IPv4 Access rule.	SMC-25478
When you use the SMC API to add a VLAN interface, the VLAN interface is added, but DHCP Servers in the VPN Client configuration are removed.	SMC-25539
If the Service Definition in an Access rule contains a Network Application element with the "Application Identifiable by TLS Match Alone" option selected and a TLS Match element, some traffic might incorrectly match the rule.	SMC-25557
Type-ahead search is slow in the Route-Based VPN Tunnels view if there are hundreds of tunnels configured.	SMC-25581
In the properties of an NGFW Engine, custom Aliases are listed twice.	SMC-25637
When you modify a URL List Application element, pending changes are shown for any NGFW Engine that includes a custom URL List Application element in its policy.	SMC-25659
When using the Search Rules pane in a policy, the title for the Authentication field is not shown.	SMC-25707

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 – 6.5.12
  - 6.6.0 – 6.6.4
  - 6.7.0 – 6.7.1

  Versions lower than 5.6.2 require an upgrade to one of these versions before upgrading to 6.7.2.
- 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*