NGFW Security Management Center Appliance

Release Notes

6.7.3

Revision A

Contents

About this release

This document contains important information about this software release for the Forcepoint NGFW Security Management Center Appliance (SMC Appliance). We strongly recommend that you read the entire document.

The SMC Appliance ships with pre-installed Forcepoint NGFW Security Management Center (SMC) software. The pre-installed SMC includes a Management Server and a Log Server. You can alternatively install the SMC Appliance software on a virtualization platform.

Note: The SMC Appliance does not support high-availability for the Management Server or the Log Server.

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.

- 6.7.3U001.sap

```
SHA1SUM:
58998b62bc8a89154a232e64c51c9dcf557d4adc

SHA256SUM:
a87262087770084b9724098c80b00f65ca81a2a30ea55eec1c4902d17ee32b14

SHA512SUM:
0ae5d7e4507394becba2528cb2dc3224
032d574448a65ff7e0f0a7d8f87eac82
c02c72f4575c662ce33431cb7e83219f
92b3c627e89e9221def1f4eed8779338
```

System requirements on virtualization platforms

As an alternative to using the SMC Appliance software on the pre-installed Forcepoint appliance, you can install the SMC Appliance software on a virtualization platform.

CAUTION: To protect the privacy of your data, we recommend installing the NGFW Engines, SMC components, or SMC Appliance on a hypervisor that does not host any other virtual machines.

Component	Requirement
Hypervisor	VMware ESXi version 6.0 or higher
Memory	8 GB RAM
Virtual disk space	120 GB
Interfaces	At least one network interface

The .iso installation file that is used to install the SMC Appliance software on a virtualization platform is available only for major versions of the SMC Appliance. To install the maintenance version, first install the .iso for the major version, then upgrade to the maintenance version.

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

Description	Issue number
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
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

Description	Issue number
It is not possible to set log compression options for VLAN interfaces.	SMC-26528

Install the SMC Appliance

Use these high-level steps to install the SMC Appliance.

For detailed information about installing the SMC Appliance and the NGFW Engines, see the *Forcepoint Next Generation Firewall Installation Guide*. All guides are available for download at https://support.forcepoint.com/Documentation.

Steps

1) Turn on the SMC Appliance.

2) Select the keyboard layout for accessing the SMC Appliance on the command line.

3) Accept the EULA.

4) Enter the account name and password.

   For credential requirements, see the *Forcepoint Next Generation Firewall Installation Guide*.

5) Make your security selections.

6) Complete the network interface and network setup fields.

7) Enter a host name for the Management Server.

8) Select the time zone.

9) (Optional) Configure NTP settings.

10) After the SMC Appliance has restarted, install the Management Client.

    You can use Java Web Start or install the Management Client from a file to allow remote access to the SMC. Java Web Start is enabled by default on the Management Server that is pre-installed on the SMC Appliance.

11) Import the licenses for all components.

    You can generate licenses at https://stonesoftlicenses.forcepoint.com.

12) Create the NGFW Engine elements, then install and configure the NGFW Engines.

Upgrade the SMC Appliance

Use an upgrade patch to upgrade the SMC Appliance from a previous version to version 6.7.3.

There are two kinds of SMC Appliance patches:

- Hotfix patches include improvements and enhancements for the current SMC Appliance version.
  Hotfix patch files use the letter P as a separator between the version number and the patch number. Example: 6.7.1P001
- Upgrade patches upgrade the SMC Appliance to a new version.
  Upgrade patch files use the letter U as a separator between the version number and the patch number. Example: 6.7.1U001

We recommend checking the availability of SMC Appliance patches regularly, and installing the patches when they become available. For detailed information about installing SMC Appliance patches, see the *Forcepoint Next Generation Firewall Installation Guide*.

- 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 using the Management Client before upgrading the software.
- The SMC Appliance must be upgraded before the NGFW Engines are upgraded to the same major version.
- You can upgrade from the following SMC versions:
  - 6.4.7 – 6.4.10
  - 6.5.1 – 6.5.13
  - 6.6.0 – 6.6.5
  - 6.7.0 – 6.7.2
- If you configured SNMP for the SMC Appliance before upgrading to version 6.4.0 or higher, you must configure SNMP again.

Steps

1) Log on to the SMC Appliance.

2) To check for available upgrade patches, enter the following command:

```
sudo ambr-query -u
```

3) To load the patch on the SMC Appliance, enter the following command:

```
sudo ambr-load 6.7.3U001
```

If you downloaded the patch and transferred it to the SMC Appliance, append the load command with the `-f` option and specify the full path to the patch file. Example:

```
sudo ambr-load -f /var/tmp/6.7.3U001.sap
```

4) To install the patch on the SMC Appliance, enter the following command:

```
sudo ambr-install 6.7.3U001
```

The installation process prompts you to continue.

5) Enter Y.

Result

The installation process restarts the appliance and installs the patch. When the upgrade is finished, the appliance restarts. The appliance is now running SMC Appliance 6.7.3.

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