Forcepoint

NGFW Security Management Center Appliance

6.7.5

Release Notes

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 6.7.5 is 10834. This release contains Dynamic Update package 1271.

Use checksums to make sure that files downloaded correctly.

- 6.7.5U001.sap

```
SHA1SUM:
f0215070a69dccf07dd39f5b294ffbb9b78e0a5b

SHA256SUM:
795627df0989ef430696152f42fcc7560847dfa981eec7b00290b8feacab87f0

SHA512SUM:
6a5204a02d6b7c89a469c1943bb81383
5b7f6c4e375a984d63866faf2fca4c2f
c49509a66f74972bf273b161c2b9e985
16982671ac8bc4bf12b266b2b0f98a34
```

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.

Enhancement	Description
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.

Enhancements in SMC version 6.7.5

Enhancement	Description
Option to export elements without referenced elements	It is now possible to export an element without the export including referenced elements. To export elements without referenced elements, edit the <installation folder>/data/SGConfiguration.txt file and add the following parameter: `EXPORT_PERMISSION_SETTINGS=false`

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 the "Lock Management Client Window After the User Session is Idle" option is enabled, the Management Center Locked popup is shown on top of all windows. The popup remains on top of other windows unless it is minimized.	SMC-24085
When you duplicate a system Situation element, the original system situation might no longer be included in the configuration for the NGFW Engine.	SMC-24458
After you reconnect the Management Client session, the Info and Drill-Down panes in the Home view are not updated until you select an element.	SMC-25377
The Management Server does not request automatic license updates and downloads even though the Management Server regularly queries the status of licenses from the Forcepoint license server.	SMC-28425
When a WebSocket connection to the SMC API is closed, the related session is not closed immediately.	SMC-28451
The Convert Engine to Master NGFW Engine and Virtual NGFW Engines wizard fails to apply changes on the "Define Interface for the Master NGFW Engine" page when you try to assign multiple interfaces to a Virtual Resource at the same time.	SMC-28595
When you create custom Situation elements, the elements might be shown in the Management Client by the situation ID only.	SMC-28617
The first policy refresh after upgrading the SMC might fail.	SMC-28626
For external tests, the path to the script file on the command line has a limit of 80 characters.	SMC-28639
In rare cases, normal logs might be sent as alerts.	SMC-28748
When the SMC API is used to add an IP address to an existing Virtual NGFW Engine interface, antispoofing is not configured correctly.	SMC-28781
The SMC Appliance does not allow dashes (-) in the FQDN for the NTP server or in the user name for SNMP.	SMC-28987
The Control Management Servers dialog box always tries to connect to the active Management Server, even if it is unreachable.	SMC-29139
The DHCP tab is not shown in the Info pane for NGFW Engines in the Layer 2 Firewall role.	SMC-29144
When the path to the script to execute after the task in an Export Log Task includes spaces, script execution fails.	SMC-29221
When you delete a Virtual NGFW Engine, the Master NGFW Engine might not be notified of the deletion. As a result, the policy of the Master NGFW Engine refers to a Virtual NGFW Engine that no longer exists and policy installation fails.	SMC-29306
Hardware monitoring incorrectly reports Half / Forced for an interface when the NGFW Engine does not provide data for send values for speed, duplex, and auto-negotiation. This issue occurs on interfaces where negotiation settings cannot be changed.	SMC-29310
When you create an inspection rule from a log entry, saving the policy fails and an "invalid element" error message is shown.	SMC-29317
The Routing Monitoring view can take several minutes to load. In addition, while the Routing Monitoring view is loading, routing monitoring cannot be performed using the SMC API.	SMC-29321
The details are not always refreshed when you select different NGFW Engine nodes in the Home view.	SMC-29380

Description	Issue number
Viewing or comparing snapshots might fail and the following error message might be shown: "Database problem. DB Transaction failed while processing transaction".	SMC-29529
Aliases for which no value has been defined are not visible in the Engine Editor. The Alias elements can still be edited outside of the Engine Editor.	SMC-29581
When the Log Server has been configured to forward log data in different formats to different external hosts, the Log Server might send log data in the wrong format for some hosts.	SMC-29701
When you create a new NetLink add it to an Outbound Multi-Link element that is used for NAT, the configuration that is generated for the NGFW Engine might not be correct.	SMC-29803
When User elements from different LDAP domains have the same name, user, or group, you cannot use the User elements in the same rule. One of the User elements is ignored.	SMC-30016
When you configure host name for the SSL VPN Portal, host names that end with .ye are not accepted.	SMC-30353
When there is an empty Group element in the source or destination cell of a rule, the whole rule might be ignored even if there are other elements in the same source or destination cell.	SMC-30542
When you use an FQDN as the host name of the HTTP proxy that the NGFW Engine uses to connect to anti-malware database mirrors, the following warning is incorrectly shown during policy installation: "The proxy IP Address X defined in the Anti-Malware settings in invalid". The HTTP proxy is configured correctly.	SMC-30757
If there are many policy snapshots, upgrading the Management Server might fail.	SMC-30769
When you use Group elements in the Routing view, the routing table does not show all networks and IP addresses in the groups correctly.	SMC-30800
The "Only One Logon Session for Each User" option on the Password Policy tab of the Global System Properties dialog box should invalidate an administrator's previous session and allow the administrator to start a new session. The option incorrectly prevents administrators from logging on if there is already an existing session.	SMC-30831
When you use the "IP Protocol" field as a field resolver in a Logging Profile element, the value is not correctly resolved.	SMC-30926

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 6.7.5.

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 – 6.5.17
- 6.6.0 – 6.6.5
- 6.7.0 – 6.7.4

- 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 6.7.5U001
```

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/6.7.5U001.sap
```

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

```
sudo ambr-install 6.7.5U001
```

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 6.7.5.

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, release notes, Knowledge Base articles, downloads, cases, and contact information.

You might need to log on to access the Forcepoint support website. If you do not yet have credentials, create a customer account. See https://support.forcepoint.com/CreateAccount.

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 10 September 2020