FORCEPOINT

NGFW Security Management Center Appliance

Release Notes

6.7.2

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

Use checksums to make sure that files downloaded correctly.

- 6.7.2U001.sap

```
SHA1SUM:
2b5eb2641381050f2225aab85c239c14075490eb

SHA256SUM:
d4efe5101720f6248a94f50fe8a7b170c115ebbc190d59fee211fbc116018f62

SHA512SUM:
1ea5f2a3096e1c7c4ac5c6534be6f0eb
22eaa503365664124fc5c008d7090073
f4e0e9de517f97609bb1542f17ca85eb
65ac850b75a0e9ac1883ab8d3a7266bd
```

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.

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

Description	Issue number
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
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

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 6.7.2.

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*.

CAUTION: Before upgrading the SMC Appliance from version 6.2.0, install the 6.2.0P001 patch. For more information, see Knowledge Base article 14168.

- 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 – 6.5.12
  - 6.6.0 – 6.6.4

- 6.7.0 – 6.7.1

- 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 6.7.2U001
```

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/6.7.2U001.sap
```

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

```
sudo ambr-install 6.7.2U001
```

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 6.7.2.

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*