FORCEPOINT

NGFW Security Management Center Appliance

Release Notes

6.7.1

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 6.7.1 is 10819. This release contains Dynamic Update package 1205.

Use checksums to make sure that files downloaded correctly.

- 6.7.1U001.sap

```
SHA1SUM:
f3fc8153aec1d37cc7edf8d4848ee2def1879de0

SHA256SUM:
b2e5afdc323dc28d210566a2bca7ab393bb68a4a0418a63b4f55ca96563d024c

SHA512SUM:
d8ec9a8330ca5a12f893c9dda12a6654
c75594700632aca5efb0d1f67d3c2391
84c4ba96471b1d0b2085a03b3ae2edfc
dfc6d1a25440fad2d4fd904ea0a95a8a
```

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
If the Management Server is configured to automatically download and activate dynamic update packages, the Management Server might repeatedly download a dynamic update package. Multiple SMC backups are created, and multiple alerts are generated because the Management Server attempts to activate a dynamic update package that has already been activated.	SMC-22879
When you click "View Statistics" in the Configuration pane of a Master NGFW Engine home page, the IPS Details overview opens.	SMC-23369
A blacklist entry generated by a Correlation Situation is not generated correctly if the Address option on the Blacklist Scope tab is set to Attacker.	SMC-23680
When there is a VPN validation warning or error for a VPN that includes mobile VPNs, policy snapshot comparison fails. The following message is shown: 'Element <vpn_gw_gw_issue> has no attribute "culprit_gateway_ref_key".'	SMC-23751
Even though ECA provides endpoint client information to the NGFW Engine, Access rules that use endpoint information as the source or destination do not match.	SMC-24007
When users are stored in a user group in an external LDAP domain, retrieving users using the SMC API is slow.	SMC-24011
When you select an entry in the Routing monitoring view, the view stops working. The following message is shown: "Database problem. DB Transaction failed while processing transaction".	SMC-24014
When VPN endpoints have a dynamic contact address or an FQDN as the contact address, VPN validation fails.	SMC-24026
Importing externally signed certificates using the SMC API fails.	SMC-24027
When an External VPN Gateway element has two endpoints with dynamic IP addresses, saving the element fails. The following message is shown: "An error occurred when saving Endpoint X (Dynamic) in external Gateway. IP address IPv4 dynamic is already defined in endpoint Y (Dynamic)."	SMC-24032
When you create a new NGFW Engine in the Firewall/VPN role, VPN endpoints and the automatic site are not automatically configured if you configure the default route using the routing tools.	SMC-24119
After you select the High Priority QoS Class for a NetLink in an Outbound Multi-Link element, you cannot remove the High Priority QoS Class.	SMC-24224
When there are a large number of log entries that match a filter in an overview, opening the Logs view from the overview might take a long time, or cause the Management Client to become unresponsive.	SMC-24280

Description	Issue number
Opening the properties of an internal certificate fails. The following message is shown: "Invalid parameter: DB Key missing."	SMC-24307
When you use the search bar to search for Host elements, not all Host elements are found.	SMC-24313
When you use User Response elements in a Layer 2 Interface Policy, responses are not sent to users.	SMC-24399
When you edit the regular expression in an existing custom Situation element, the changes are not saved.	SMC-24413
In the Home view, the status cards for Virtual NGFW Engines might incorrectly show CPU load statistics.	SMC-24470
When you create a report, it is not possible to configure the report to be sent to multiple email addresses on the Task tab of the Report Operation Properties dialog box.	SMC-24482
When you select an IP address for a BGP Peering element on the Routing branch of the Engine Editor, this list of IP addresses might be too long to show all options.	SMC-24539
When you create a new Active Directory Server element, the default attribute for Userid is cn, which is not a unique attribute within AD domains.	SMC-24544
When you remove a user that has group membership from the internal LDAP domain, user database replication might stop working.	SMC-24620
When you use the SMC API, it is not possible to set all of the same options for third party monitoring that are available in the Management Client.	SMC-24692

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 6.7.1.

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 – 6.5.11
  - 6.6.0 – 6.6.3
  - 6.7.0

- 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 6.7.1U001
```

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/6.7.1U001.sap
```

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

```
sudo ambr-install 6.7.1U001
```

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 6.7.1.

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*