FORCEPOINT

NGFW Security Management Center Appliance

Release Notes

6.6.4

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 6.6.4 is 10722. This release contains Dynamic Update package 1217.

Use checksums to make sure that files downloaded correctly.

- 6.6.4U001.sap

```
SHA1SUM:
9aa3d458e3134044d576807c75f0a50eca5cb97b

SHA256SUM:
dde77584370c8de4c3b41ddbee3d1855a3064d99b6c3372a6201a2dfb7b9b968

SHA512SUM:
1387cd943cd7140e2278daa0c2a018d9
df60f57078d8823b20b7e12b878d3a32
37ea74be94d17c3f3c01bdb8881e36ac
6bf370eeb9d964b503577f3c11c0c7bd
```

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 6.6 can manage all compatible Forcepoint NGFW Engine versions up to and including version 6.6.

⚠ **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 6.6 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*.

Dynamic link selection for SD-WAN

The VPN links that are used for Multi-Link traffic from applications and protocols, and traffic associated with QoS classes are now automatically selected based on quality metrics defined for the network applications, protocols, and QoS classes. You can now also specify how different types of ISP connections are used for specific types of traffic. For each type of ISP connection, you can specify that:

- The ISP connection is used for the specified type of traffic unless an ISP connection with significantly higher quality is available.
- The ISP connection is used for the specified type of traffic only if the quality of the other ISP connections is too low or the other ISP connections are not available.
- The ISP connection must not be used for the specified type of traffic.

Storage and browsing of log data locally on NGFW Engines

You can now save copies of the most recent log entries locally on the NGFW Engine. Alert entries are also saved locally on the NGFW Engine. You can browse the saved log and alert entries on the command line of the NGFW Engine even if the log and alert entries have already been sent to the Log Server. The length of time for which the log and alert entries are stored depends on the size of the NGFW Engine’s disk and the volume of log data. You can also set limits for how long log entries are stored, and how much disk space can be used for storage.

LLDP support

NGFW Engines can now use the Link Layer Discovery Protocol (LLDP) to send information, such as information about interfaces and MAC addresses on the NGFW Engine, to directly connected devices on the network.
The NGFW Engines can also receive information that other devices on the network send. In the Management Client, you can now monitor information that the NGFW Engine has received about devices in directly connected networks.

Support for LTE modems on NGFW Engines in the Firewall/VPN role

You can now use LTE modems for mobile broadband connections on 4G networks with NGFW Engines in the Firewall/VPN role. Support for LTE modems is only available on specific purpose-built NGFW appliance models (NGFW 50 Series).

Enhancements

This release of the product includes these enhancements.

Enhancements in SMC version 6.6.0

Enhancement	Description
Easier forwarding to a proxy	You can now configure forwarding traffic to a proxy or host directly in the Access rules rather than in the NAT rules.
Shared interfaces on Master NGFW Engines	Layer 3 physical interfaces on Master NGFW Engines in the Firewall/VPN role can now be shared interfaces. • You can now connect Virtual Firewalls to the same network without dedicating one physical interface or VLAN for each Virtual Firewall. • The Virtual Firewalls can now communicate with each other without an external switch or router. • Link aggregation is supported on Virtual Firewalls.
IPv6 support for user authentication	User authentication now supports IPv6 addresses. Communication between NGFW Engines and TACACS+ authentication servers now also supports IPv6 addresses.
Server Pool enhancements	The following enhancements have been made for the Server Pool feature: • You can now use Server Pool elements in NAT rules to apply both source and destination NAT for Server Pool load balancing. • The Server Pool feature now supports IPv6.
New URLs for dynamic updates and engine upgrades	To improve the performance of automatic dynamic updates and engine upgrades, the following new URLs are available in SMC 6.5.0 and higher: • https://autoupdate.ngfw.forcepoint.com/dynup.rss • https://autoupdate.ngfw.forcepoint.com/ngfw.rss **Note:** The SMC automatically starts using the new URLs when you upgrade to SMC 6.5.0 or higher and activate the dynamic update package that includes the new URLs. The new URLs use a content distribution network (CDN) to allow the SMC to download dynamic update packages and engine upgrade files from the geographically closest server. The legacy https://update-pool.stonesoft.com/index.rss URL remains available for backward compatibility and as a backup for the new URLs.
Configurable update services for dynamic updates and engine upgrades	New Update Service elements define sets of URLs for automatic dynamic updates and engine upgrades. In SMC 6.5.0 and higher, the SMC automatically uses Update Service elements that include both the new URLs and the legacy URL. No action is needed to start using the Update Service elements that include the new URLs. Starting from SMC 6.5.2, you can optionally change which Update Service element is used for automatic dynamic updates and engine upgrades. For more information, see Knowledge Base article 16589.

Enhancement	Description
Audit log improvements	Audit entries now include information as text about the changes made to elements when the following configurations are modified: • VLAN interfaces on Master NGFW Engines • Virtual Resources on Master NGFW Engines • IP addresses on Virtual NGFW Engines • Antispoofing on Virtual NGFW Engines • Announced Networks for dynamic routing on Virtual NGFW Engines • External BGP Peers on Virtual NGFW Engines • Matching Conditions in Route Maps on Virtual NGFW Engines • Route Entry Settings in Route Maps on Virtual NGFW Engines • IP prefix lists on Virtual NGFW Engines • Comments on Virtual NGFW Engines
Improvements in the Pending Changes feature	Improvements in the Pending Changes feature prevent an element from appearing in the Pending Changes list when an administrator clicks OK without modifying the properties of the element.
User interface rendering on macOS	The Management Client now detects the operating system in use. On macOS, for example, the appropriate window control icons and special characters in keyboard shortcuts are shown.

Enhancements in SMC version 6.6.1

Enhancement	Description
Details of User Behavior Events	In the User Dashboard, you can now view related log entries for entries in the User Behavior Events pane.
New option to show disabled tunnels in the SD-WAN dashboard	A new option for viewing disabled tunnels has been added in the SD-WAN dashboard. The new Show Disabled Tunnels option is available in the Tunnels pane on branch home pages and VPN home pages.
Possibility to define the OSPF Area ID as an IP Address	You can now define the OSPF Area ID as an IP address instead of converting it to a decimal number as previously instructed in Knowledge Base article 16319.
Endpoint Information shows the user's computer name	The Endpoint Information pane in the User Dashboard can now show the computer name from which the user is connected.
ECMP option for BGP	You can now set an equal cost multi path (ECMP) value in the BGP configuration using the Management Client.

Enhancements in SMC version 6.6.2

Enhancement	Description
EasyConnect forwarding to the Forcepoint Web Security Cloud	You can now configure EasyConnect to forward web traffic from Forcepoint NGFW to Forcepoint Web Security Cloud. For more information, see Knowledge Base article 10582. ⚠ **CAUTION:** This feature requires NGFW Engine version 6.5.6, 6.6.3, 6.7.0, or higher.

Enhancements in SMC version 6.6.3

Enhancement	Description
NGFW Engine tester	You can now use the Link Status Test on layer 2 interfaces.

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 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

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 6.6.4.

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: 6.6.1P001
- 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: 6.6.1U001

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 6.6 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
- 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 6.6.4U001
```

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/6.6.4U001.sap
```

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

```
sudo ambr-install 6.6.4U001
```

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 6.6.4.

Known issues

For a list of known issues in this product release, see Knowledge Base article 16950.

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*