



NGFW Security Management Center

6.8.10

Release Notes

Contents

- [About this release](#) on page 2
- [System requirements](#) on page 2
- [Build number and checksums](#) on page 4
- [Compatibility](#) on page 4
- [New features](#) on page 5
- [Enhancements](#) on page 6
- [Resolved and known issues](#) on page 8
- [Installation instructions](#) on page 8
- [Upgrade instructions](#) on page 9
- [Find product documentation](#) on page 10

About this release

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

System requirements

To use this product, your system must meet these basic hardware and software requirements.

SMC hardware requirements

You can install the SMC on standard hardware.

Component	Requirement
CPU	Intel® Core™ family processor or higher recommended, or equivalent on a non-Intel platform
Disk space	<ul style="list-style-type: none">■ Management Server: 6 GB■ Log Server: 50 GB

Component	Requirement
Memory	<ul style="list-style-type: none"> ■ Management Server, Log Server, Web Portal Server: 6 GB RAM ■ If all SMC servers are on the same computer: 16 GB RAM ■ If you use the SMC Web Access feature: an additional 2 GB RAM per administrator session ■ Management Client: 2 GB RAM <p>The SMC server requirements are the <i>minimum</i> requirements. The Management Server and Log Server in particular benefit from having more than the minimum amount of RAM.</p> <p>On high-end appliances that have a lot of RAM, the SMC might not provision the maximum amount of RAM for use by the SMC servers. For information about how to manually modify the provisioning, see Knowledge Base article 10016.</p>
Management Client peripherals	<ul style="list-style-type: none"> ■ A mouse or pointing device ■ SVGA (1024x768) display or higher

**CAUTION**

To protect the privacy of your data, we recommend using dedicated hardware for all NGFW, SMC, and SMC Appliance installations. For cloud-based virtualization platforms, use an instance type that runs on dedicated hardware. For on-premises virtualization platforms, install the NGFW Engines, SMC components, or SMC Appliance on a hypervisor that does not host any other virtual machines. For third-party hardware, do not install any other software on the computer where you install the NGFW Engines or SMC components.

Operating systems

You can install the SMC on the following operating systems. Only 64-bit operating systems are supported.

Linux	Microsoft Windows
<ul style="list-style-type: none"> ■ CentOS 7 and 8 ■ Red Hat Enterprise Linux 7 and 8 ■ SUSE Linux Enterprise 12 and 15 ■ Ubuntu 18.04 LTS and 20.04 LTS 	<p>Standard and Datacenter editions of the following Windows Server versions:</p> <ul style="list-style-type: none"> ■ Windows Server 2019 ■ Windows Server 2016 ■ Windows Server 2012 R2 <p>On Windows 10, you can install the SMC in demo mode. You can also install the Management Client.</p>

**Note**

Ubuntu 16.04 LTS is no longer supported after 30 April 2021. If you use Ubuntu 16.04 LTS, upgrade the operating system before installing the SMC.

We recommend that you only use operating system versions that are currently supported by the vendor.

Other versions of the listed operating systems might be compatible, but have not been tested. Only U.S. English language versions of the listed operating systems have been tested, but other locales might also be compatible.

Build number and checksums

The build number for SMC 6.8.10 is 10948. This release contains Dynamic Update package 1414.

Use checksums to make sure that files downloaded correctly.

■ smc_6.8.10_10948.zip

```
SHA1SUM:
9a93cc03e544b67ae2c392d3ef09b7130f844e34

SHA256SUM:
70f87f205b4f222c9b9ff6c94e768507809b82ba866b191cca42e41233fa7456

SHA512SUM:
b564b1879bf322269824b5afec814bc5
f35d05ac0b744d5de81c2734127ac2cf
ec4b4f01fafb533c078cb89c7d060c14
d96a2a51eeee9255d06c9b7f1f1087c7
```

■ smc_6.8.10_10948_linux.zip

```
SHA1SUM:
d15b5404863acb4cb800d5fe8256a16e99919c3a

SHA256SUM:
e61c7c8e12328bd074299ad71f2709ac8ac9ef2e6ec1ed7850816030ca353b02

SHA512SUM:
0947c23494c969a181f27a677242173f
855662653026c393b049270c33e82b14
5d8efb8b6ce7f577462634ceea587206
c67ee58dab4f666947c76da9d2773b77
```

■ smc_6.8.10_10948_windows.zip

```
SHA1SUM:
5e094937983a7ce329a6060d96226ed6cbf98ee5

SHA256SUM:
981eff70cf4c7705b5056788294f162d3c48aacac23b25c3f000426eef93cf3f

SHA512SUM:
29bcfd99ca6f6f2eb751bd4457f02e74
d599c43329fedb6f39ccbf247a916197
485c205bc4773713e909301b8c7443e1
4c3e25f3bbf9f5924093a56df9846142
```

Compatibility

SMC 6.8 can manage all compatible Forcepoint NGFW Engine versions up to and including version 6.8.



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>.

**Note**

Apache Log4j2 <=2.14.1 JNDI features used in configuration, log messages, and parameters do not protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. From log4j 2.15.0, this behavior has been disabled by default. In previous releases (>2.10) this behavior can be mitigated by setting system property `log4j2.formatMsgNoLookups` to true or it can be mitigated in prior releases (<2.10) by removing the `JndiLookup` class from the classpath (example: `zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class`). Hence, integrate the official 2.16 version of the Log4J library that is not vulnerable to CVE 2021-44228.

SMC 6.8 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*.

UUID license binding for SMC licenses

When you install the SMC or upgrade the SMC to version 6.8, the SMC generates a Unique Installation Identifier (UUID). As an alternative to binding licenses for SMC components to the IP addresses of the components, you can now bind the SMC licenses to a UUID. Using UUID binding allows organizations to obtain SMC licenses without disclosing the internal IP addresses of the SMC components.

**Note**

The UUID is not stored in SMC backups or restored when you restore a backup. After the UUID is generated, it will not be overwritten when you restore backups or upgrade the SMC in the future.

You can continue to use your existing licenses or optionally change the license binding method. You can use IP-address-bound licenses for some SMC components and UUID-bound licenses for other SMC components.

Management Client downloads from the Management Server

Java Web Start is no longer supported in SMC 6.8. As an alternative, you can now configure the Management Server to provide the Management Client installation files on a download web page hosted by the Management Server. Administrators download and install the Management Client from the locally hosted SMC Downloads web page.

**Note**

Management Client downloads are not supported for macOS in SMC 6.8. For administrators who use macOS, we recommend using the SMC Web Access feature.

Enhancements

This release of the product includes these enhancements.

Enhancements in SMC version 6.8.0

Enhancement	Description
Easier configuration of dynamic link selection for NGFW Engines	It is now possible to select Link Usage Profile elements for NGFW Engines in the Firewall/VPN role to define which link types are preferred, avoided, or not used for specific types of outbound Multi-Link traffic. NGFW Engine-specific exceptions to the Link Usage Profile also allow you to specify which traffic uses specific NetLinks.
Re-authentication when using browser-based user authentication	If an end user has authenticated using browser-based user authentication and the session will soon expire, the user can re-authenticate to extend the authentication time-out and avoid connections closing before the user has finished their tasks.
Custom script upload for NGFW Engines when using Custom Properties Profile elements	To upload custom scripts to the NGFW Engine, you can add the scripts to the properties of the NGFW Engine using a Custom Properties Profile element. The scripts are uploaded when the policy is installed or refreshed.
Expiration time for one-time passwords	You can now set the expiration time for one-time passwords that are generated when you save the initial configuration for an NGFW Engine. If the one-time password is not used, it automatically expires after the expiration time has elapsed. By default, one-time passwords expire after 30 days.
PPPoE support on VLAN interfaces	You can now configure point-to-point protocol over Ethernet (PPPoE) for dynamic IP addresses that are assigned to VLAN interfaces.
User domain support for integrated ICAP servers for DLP	NGFW integration with external ICAP servers for DLP now uses the WinNT schema in the X-Authenticated-Users header instead of the Local schema that was used previously. Using the WinNT schema allows matching users against a user domain in the user directory on the ICAP server.

Enhancements in SMC version 6.8.2

Enhancement	Description
Configurable timeout for session monitoring	<p>Previously, monitoring views might have failed to open when there were several backup Log Servers and the primary Log Server was unreachable.</p> <p>You can now define the timeout for receiving monitoring data from NGFW Engines. To define the timeout, edit the <installation folder>/data/SGConfiguration.txt file and add the following parameter:</p> <pre>SESMON_LOGSERVER_SELECTION_TIMEOUT=<timeout_in_milliseconds></pre> <p>The default value is 20000.</p>

Enhancements in SMC version 6.8.3

Enhancement	Description
Resource monitoring for SMC servers and the Management Client	<p>The Info pane for Management Servers, Log Servers, and Web Portal Servers now shows information about resource usage on the computers where the servers are installed. The bottom right corner of the Management Client window shows the memory usage of the Management Client.</p> <p>If the memory usage gets too high, the Management Server, Log Server, Web Portal Server, or the Management Client automatically restarts. When the server or the Management Client restarts, an alert and an audit entry are generated. You can optionally disable automatic restart.</p>
Password policy enhancements	The settings for password complexity requirements in the password policy now also apply to SMC administrator accounts that are replicated as local administrator accounts on NGFW Engines, the root account on NGFW Engines, and the Management Server database password.
New Log Server and Management Server configuration parameters	<p>In the LogServerConfiguration.txt file, you can now add a new configuration parameter to recover connectivity from the Log Server to TCP syslog servers. For more information, see Knowledge Base article 19219.</p> <p>In the SGConfiguration.txt file, you can now add a new configuration parameter to define how many tasks the Management Server can run in parallel. For more information, see Knowledge Base article 19218.</p>
More granular identification of Microsoft Office 365 network applications	<p>Starting from dynamic update package 1300, the Microsoft-Office-365 Network Application element includes dependencies that allow more granular identification of Microsoft Office 365 in traffic.</p> <p>No action is required if you use the Microsoft-Office-365 Network Application element in the following types of rules:</p> <ul style="list-style-type: none"> ■ Access rules with the Allow, Discard, Refuse, or Jump action ■ NAT rules <p>If you use the Microsoft-Office-365 Network Application element in an access rule with the Continue action, you must manually add the Network Application elements that are listed as dependencies. Options that are configured in a rule with the Continue action are not automatically applied to dependencies.</p> <p>For more information, see Knowledge Base article 19195.</p>

Enhancements in SMC version 6.8.4

Enhancement	Description
Optimization of status monitoring in large-scale SMC environments	New parameters for the Management Server and Log Server allow you to optimize the performance of status monitoring for NGFW Engines, VPNs, and NetLinks for SD-WAN in large-scale SMC environments. For more information, see Knowledge Base article 19285 .

Resolved and known issues

For a list of resolved and known issues in this product release, see Knowledge Base article [18381](#).

Log4j - CVE 2021-44228

The 2.16 version of the log4J library is now included in the Security Management Center (SMC) package.

Installation instructions

Use these high-level steps to install the SMC and the Forcepoint NGFW Engines.

For detailed information, see the *Forcepoint Next Generation Firewall Installation Guide*. All guides are available for download at <https://support.forcepoint.com/Documentation>.

Steps

- 1) Install the Management Server, the Log Servers, and optionally the Web Portal Servers.
- 2) Import the licenses for all components.
You can generate licenses at <https://stonesoftlicenses.forcepoint.com>.
- 3) Configure the Firewall, IPS, or Layer 2 Firewall elements in the Management Client from the **Configuration** view.
- 4) To generate initial configurations, right-click each NGFW Engine, then select **Configuration > Save Initial Configuration**.
Make a note of the one-time password.
- 5) Make the initial connection from the NGFW Engines to the Management Server, then enter the one-time password.
- 6) Create and upload a policy on the NGFW Engines in the Management Client.

Upgrade instructions

Take the following into consideration before upgrading the SMC.



Note

The SMC (Management Server, Log Server, and Web Portal Server) must be upgraded before the NGFW Engines are upgraded to the same major version.

- SMC 6.8 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 in the Management Client before upgrading the software.
- To upgrade a lower version of the SMC to 6.8, we strongly recommend that you stop all SMC servers and create a backup before continuing with the upgrade. After creating the backup, run the appropriate setup file, depending on the operating system. The installation program detects the old version and does the upgrade automatically.
- When you upgrade the SMC, the dynamic update package that is included with the SMC installer is imported and activated. However, if a newer version of the dynamic update package has previously been imported or downloaded before the upgrade, the newest version is activated instead.
- You can upgrade from the following SMC versions:
 - 5.6.2 – 6.4.10
 - 6.5.0 – 6.5.18
 - 6.6.0 – 6.6.5
 - 6.7.0 – 6.7.5
 - 6.8.0– 6.8.9

Versions lower than 5.6.2 require an upgrade to one of these versions before upgrading to 6.8.10.

- Before upgrading, make sure that you have removed all elements related to McAfee Endpoint Intelligence Agent (McAfee EIA). Also remove all references in Access rules.



Note

In SMC version 6.8.3 and higher, the default path to the installation of xvfb-run for SMC Web Access is set to /usr/bin, and you cannot change the path using the Management Client.

If you use SMC Web Access on a Management Server or Web Portal Server installed on a Linux platform and need to change the path to the installation of xvfb-run, follow these steps:

- 1) On the Management Server or the Web Portal Server, edit the `SGConfiguration.txt` or `WebPortalConfiguration.txt` file.
- 2) Add the following parameter:

```
XVFB_RUN_DEFAULT_PATH=<path>
```

Replace `<path>` with the path to the installation of xvfb-run.

**Note**

If you use the SMC-Python library for interacting with the SMC API, you must upgrade the SMC-Python library to version 0.7.0b27 when you upgrade to SMC 6.8.4 or higher. To upgrade the SMC-Python library, see <https://github.com/Forcepoint/fp-NGFW-SMC-python>.

Find product documentation

In the Forcepoint Customer Hub, 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 in the Forcepoint Customer Hub 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 Customer Hub. 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*

