



# **NGFW Security Management Center**

**6.9.1**

**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 7
- [Installation instructions](#) on page 7
- [Upgrade instructions](#) on page 8
- [Find product documentation](#) on page 9

# 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.

For detailed information about changes introduced in the SMC API since the previous version, see the automatically generated change log reports in the `api_change_log.zip` file in the `Documentation/SMC_API` folder of the SMC installation files.

# 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"><li>■ Management Server: 6 GB</li><li>■ Log Server: 50 GB</li></ul>

Component	Requirement
Memory	<ul style="list-style-type: none"> <li>■ Management Server, Log Server, Web Portal Server: 6 GB RAM</li> <li>■ If all SMC servers are on the same computer: 16 GB RAM</li> <li>■ If you use the SMC Web Access feature: an additional 2 GB RAM per administrator session</li> <li>■ Management Client: 2 GB RAM</li> </ul> <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 <a href="#">10016</a>.</p>
Management Client peripherals	<ul style="list-style-type: none"> <li>■ A mouse or pointing device</li> <li>■ SVGA (1024x768) display or higher</li> </ul>

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

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 6.9.1 is 11013. This release contains Dynamic Update package 1321.

Use checksums to make sure that files downloaded correctly.

## ■ smc\_6.9.1\_11013.zip

```
SHA1SUM:
8925d17baf05b3e63a2f4999529956d088bf6457

SHA256SUM:
7230583c0afa21d844d68573205408718c5cd8e065d6f864d1494befa63262d6

SHA512SUM:
fab85ab6a314930de058927103fa36b0
2af2c5c073ce2a57f232537678ae42d9
70213c078700ada19d2c78fb24dd206f
cd9ffa702f60a2611b48a27bf62edd5d
```

## ■ smc\_6.9.1\_11013\_linux.zip

```
SHA1SUM:
34d0cf0fba9f9967b89555b277af4f0a46cc031c

SHA256SUM:
2440d7c0f79efb6fb435b7b3d3c65c2bd66c49bb9f03ccad77c8857281925ea7

SHA512SUM:
b4128971c2212db99a6410457912a67c
12021923d712850a6d3cd20e899b360e
73baf9884d243b642e2f773c9a47776a
ad8dc4fb9326ae0d1f6786a2c78f63a1
```

## ■ smc\_6.9.1\_11013\_windows.zip

```
SHA1SUM:
894bfa3d6101bb85adf494356f80c61e56345836

SHA256SUM:
a98d0f5300a90f1b1b135065be7827cf234c1ae46f5072a2c84cc157c09b6996

SHA512SUM:
f0bb6b367b1386f40a914338c1d5393e
a9c55e36a9d0dca9fbf679d786341359
e05ee0863e49422ed983937e3a30fa1c
c5e615aaea8413e73528add4072ab17a
```

# Compatibility

SMC 6.9 can manage all compatible Forcepoint NGFW Engine versions up to and including version 6.9.



### 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 6.9 is compatible with the following component versions.

- Forcepoint Next Generation Firewall (Forcepoint NGFW) 6.3 or higher
- McAfee ePolicy Orchestrator (McAfee ePO) 5.10 or higher



#### Important

SMC 6.9 is the last version of the SMC that is compatible with McAfee ePO. Features that depend on McAfee ePO, such as McAfee® Threat Intelligence Exchange (TIE) and McAfee® Data Exchange Layer (DXL) integration, will no longer be available in the next major release of the SMC.

- McAfee Enterprise Security Manager (McAfee ESM) 11.1.x or higher

## 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*.

### Elasticsearch integration for high performance logging and reporting

Elasticsearch is an open-source search engine that runs on an external Elasticsearch server cluster. You can now forward log data from Log Servers and Management Servers to an Elasticsearch cluster to improve the performance of browsing and searching for log entries, report generation, and other log-related features. You can browse log entries that have been forwarded to an Elasticsearch cluster using the Management Client in the same way as for other log entries.



#### Important

Forwarding log data to an Elasticsearch cluster is an advanced feature that requires knowledge of how to configure Elasticsearch. You must already have an Elasticsearch cluster deployed and configured in your environment.

For information about the requirements for using Elasticsearch with the SMC, see Knowledge Base article [17583](#).

## Documentation changes

This release of the product includes the following changes to the product documentation:

- The NGFW product documentation is no longer included in the SMC installation files. To find documentation for all Forcepoint products, go to the Forcepoint support website at <https://support.forcepoint.com>.
- The SMC installation files now include automatically generated change log reports for the SMC API in the `api_change_log.zip` file in the `Documentation/SMC_API` folder.
- The title of the *Forcepoint NGFW SMC API Reference Guide* has been changed to *Forcepoint NGFW SMC API User Guide*.

# Enhancements

This release of the product includes these enhancements.

## Enhancements in SMC version 6.9.0

Enhancement	Description
Configuration of bidirectional forwarding detection using the Management Client	<p>Forcepoint NGFW Engine previously supported the configuration of bidirectional forwarding detection (BFD) using command line tools on the NGFW Engine. You can now configure BFD using the Management Client.</p> <p>When you use the BGP protocol for dynamic routing, you can optionally use BFD to detect neighbor failures. The NGFW Engine sends packets at the specified interval and waits for a reply. If the NGFW Engine does not receive a reply within the specified length of time, the neighbor is considered to have failed.</p>
Improved performance for policy installation	The performance of policy installation has been improved. Policy installation is now faster and requires less memory.
New Management Client look-and-feel	The look-and-feel of the Management Client has been updated to reflect the new Forcepoint brand identity.
Option to generate one report per sender	When you generate reports, you can now generate one report for each NGFW Engine that is detected as a sender of log data. A new option in the Engine Editor allows you to define the default email addresses to which generated reports are sent when the NGFW Engine is the sender of log data for the report.
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.
Resource monitoring for SMC servers and the Management Client	<p>The <b>Info</b> 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>
SMC HA Administration for Log Servers	In a high availability (HA) environment with multiple Log Servers, information about the Log Servers now also appears in the SMC HA Administration dialog box (formerly Control Management Servers dialog box). Previously, this dialog box only allowed you to control how the Management Servers function in an HA environment.

## Enhancements in SMC version 6.9.1

Enhancement	Description
Permanent link for sandbox analysis reports for Forcepoint Advanced Malware Detection	<p>Previously, dynamic links to sandbox analysis reports for Forcepoint Advanced Malware Detection in log entries required you to authenticate in the external portal to view the reports. Due to changes in the licensing model for Forcepoint Advanced Malware Detection, the SMC now shows permanent links to sandbox analysis reports that do not require separate authentication in log entries. These new permanent links make it easier to view and share individual reports.</p> <p>To start using the new permanent links, you must upgrade your licenses for Forcepoint Advanced Malware Detection. For more information, see Knowledge Base article <a href="#">19409</a>.</p>

## Resolved and known issues

For a list of resolved and known issues in this product release, see Knowledge Base article [19276](#).

## 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>.



### Note

The sgadmin user is reserved for SMC use on Linux, so it must not exist before the SMC is installed for the first time.



### Note

If you install the SMC on Windows and Windows Defender is enabled, it might take a long time to activate a dynamic update package. For more information, see Knowledge Base article [14055](#).

## 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 6.9 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 6.9, 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 – 6.8.4
  - 6.9.0

Versions lower than 5.6.2 require an upgrade to one of these versions before upgrading to 6.9.1.

- 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 6.9.0 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, edit SGConfiguration.txt or WebPortalConfiguration.txt and add the following parameter:

```
XVFB_RUN_DEFAULT_PATH=<path>
```

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

## 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 User Guide* (Formerly *Forcepoint NGFW SMC API Reference Guide*)
- *Forcepoint VPN Client User Guide* for Windows or Mac
- *Forcepoint VPN Client Product Guide*

