



NGFW Security Management Center

7.0.2

Release Notes

Contents

- [About this release](#) on page 2
- [System requirements](#) on page 2
- [Build number and checksums](#) on page 3
- [Compatibility](#) on page 4
- [New features](#) on page 5
- [Enhancements](#) on page 5
- [Resolved and known issues](#) on page 7
- [Security updates](#) on page 7
- [Installation instructions](#) on page 7
- [Upgrade instructions](#) on page 7
- [Find product documentation](#) on page 8

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">■ Management Server: 6 GB■ Log Server: 50 GB

Component	Requirement
Memory	<ul style="list-style-type: none"> Management Server, Log Server, Web Portal Server: 16 GB RAM If all SMC servers are on the same computer: 32 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 33316.</p>
Management Client peripherals	<ul style="list-style-type: none"> A mouse or pointing device Display with 1280x768 resolution or higher

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"> 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>

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 7.0.2 is 11323. This release contains Dynamic Update package 1568.

Use checksums to make sure that files downloaded correctly.

- `smc_7.0.2_11323.zip`

```
SHA256SUM:  
f69f3c5538d6a45641070ef0d8398f44b573ec167829eea76f40c1d548ef8475
```

```
SHA512SUM:  
7156ab2ca37b6c17359e05ace1ce4749  
ac6c1ac17279c210a2c135e250e7f80a  
10db03868ae16b4bbbd4072db4d8bf28  
c2278e23a01461260a17b3895ccfd110
```

- `smc_7.0.2_11323_linux.zip`

```
SHA256SUM:  
c51d7db33e7f984387e1b8982f400e503a417d31e2eeb8b11d3cfaff34140f11
```

```
SHA512SUM:  
58b630ba4f9d34877ec120edf8867de1  
9dc91d881e449d945f3e8ae9be8d417d  
e1925b931e2f4083d7990fcde8fae132  
99349f823da0dd25db595056cdcd7adf
```

- `smc_7.0.2_11323_windows.zip`

```
SHA256SUM:  
67f7aed47a1ed8aa0d6ffe91c3298ed6936d965e3ab6e0af37adbfc27b43a843
```

```
SHA512SUM:  
be494d24027bf1b968ff5168881c5b49  
324df212c64add2bb47ab53a5aaf3378  
5350155470192ccae7a827d528323390  
1a2afba92ab438cdd7725e3eb0e03a87
```

Compatibility

SMC 7.0 can manage all compatible Forcepoint NGFW Engine versions up to and including version 7.0.



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 7.0 is compatible with Forcepoint Next Generation Firewall (Forcepoint NGFW) 6.5 or higher.



Note

SA-per-host switch in the IPsec VPN configuration is deprecated and will not be available from the GUI for new configurations by default in 6.11 and later versions of SMC. This option is not needed for standard VPN use cases, but can be re-enabled via a parameter in the `SGConfiguration.txt` if required for troubleshooting or testing purposes.

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*.

Application health monitoring

The Application Health Monitoring dashboard proactively detects user experience issues based on connection quality metrics. This release introduces a new dashboard and new set of widgets for Application Health Monitoring. For more information, see *Forcepoint Next Generation Firewall Product Guide*.

Integration of ZTNA connector with NGFW Engine

NGFW Engine is typically located in the perimeter of the network where internal resources are located. Therefore, if ZTNA connector is integrated with NGFW Engine, it can be used as a connection point for many services that you might want to publish through Forcepoint ONE portal by using ZTNA connector. From 7.0 onwards, ZTNA connector is integrated with NGFW Engine by default. For more information about enabling the ZTNA connector, see *Forcepoint Next Generation Firewall Product Guide*. For more information about the ZTNA connector, see *Zero Trust Network Access* section in *Forcepoint ONE Admin Guide*.

Web filtering and Network Application detection for QUIC

Web filtering and web application detection for QUIC is targeted for users who are using inspection features such as Network Applications and URL Categories but are not decrypting the traffic.

QUIC protocol is always inspected and by default matched for web traffic rules. In this release, decryption of QUIC traffic is not supported but discarding the QUIC traffic causes most of the standard web clients fall back to earlier versions of HTTP, for which decryption by TLS inspection is supported. For more information about this feature, see *Forcepoint Next Generation Firewall Product Guide*.

Enhancements


This release of the product includes these enhancements.

Enhancements in SMC version 7.0

Enhancement	Description
Action options are now configurable in the Inspection Situation Tree	Action options can now be configured for situations directly in the inspection policy's Inspection tab where the global inspection situation tree with Permit and Terminate actions are configured.
Blacklist and Whitelist terminologies are not used in customer views	The old terminologies "Blacklist" and "Whitelist" are replaced with "Block List" and "Allow List" respectively.

Enhancement	Description
Inspection categories have been renamed	Inspection categories have been renamed to provide clear and concise naming convention, and unify the category names for better user experience.
Usability improvements	The SMC user interface has been enhanced to provide better user experience. The following are some of the enhancements done in this release: <ul style="list-style-type: none"> Improved the appearance of SMC user interface. SMC populates both internal and external interfaces while creating a new single firewall.
Enhancement of Backup Task Properties dialog box	The Backup Task Properties dialog box has been enhanced to add the following: <ul style="list-style-type: none"> A custom destination path where the files generated by backup tasks are stored. The log server triggers Script to Execute After the Task script after completing a task. For more information, see <i>Forcepoint Next Generation Firewall Product Guide</i> .
Allow multiple names in domain element	You can now set multiple names in the Domain Name network element. For more information, see <i>Forcepoint Next Generation Firewall Product Guide</i> .
4096 bit RSA key support for Browser Based User Authentication (BBA)	Browser Based User Authentication (BBA) HTTPS settings now support generating 4096 bit RSA key certificate request for the BBA server component.
Policy changes are installed faster for remote NGFW Engines	With policy refresh only files with configuration changes are uploaded to the NGFW Engine. Rules alone are now stored on their own configuration file reducing amount of data to be uploaded to NGFW Engine with just a policy change. As result policy refresh for remote engines behind slow throughput Internet connection is faster.

Enhancements in SMC version 7.0.1

Enhancement	Description
Block files with SHA256	Forcepoint NGFW allows you to block files based on SHA256 hash using the file SHA256 Hash situation contexts in the inspection policy. For more information, see Knowledge Base article 18551 .
Advanced Malware Detection & Protection Sandbox Type	The engine uses the Advanced Malware Detection & Protection cloud service for sandbox analysis and file reputation scan. <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 10px; margin-top: 10px;">  <p>Note</p> <p>This is a licensed service which requires a subscription to use.</p> </div>

Resolved and known issues

For a list of resolved and known issues in this product release, see Knowledge Base article [41216](#) .

Security updates

For information about third-party packages and associated vulnerabilities included with SMC in this product release, see Knowledge Base article [41238](#) .

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/s/article/Documentation-Featured-Article>.

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 7.0 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 7.0, 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; however, only the latest maintenance release and LTS versions are tested. Hence, It is recommended to upgrade to the latest LTS release of SMC, regardless of NGFW Engine versions being managed.
 - 6.3.0 – 6.5.18
 - 6.6.0 – 6.6.5
 - 6.7.0 – 6.7.5
 - 6.8.0 – 6.8.14 (LTS release versions)
 - 6.9.0 – 6.9.3
 - 6.10.0 – 6.10.10 (LTS release versions)
 - 6.11.0 – 6.11.2
 - 7.0.0 - 7.0.1

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 User Guide*
- *Forcepoint VPN Client User Guide* for Windows or Mac
- *Forcepoint VPN Client Product Guide*
- *Forcepoint NGFW Manager and VPN Broker Product Guide*

