Forcepoint

NGFW Security Management Center Appliance

7.0.1

Release Notes

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 7.0.1 is 11318. This release contains Dynamic Update package 1534.

Use checksums to make sure that files downloaded correctly.

- smc_7.0.1U001.sap

```
SHA1SUM:
85ce88798230341967cd06d11985e03724e481e6

SHA256SUM:
12e94c3722066a69e8112f74121b1733231f0f8ed4a6bf7b8ff18d52447cfc5d

SHA512SUM:
1ae3840857071171dcc76c6aeb410159
166890df7177b4f7ff62b2e76b1c5459
68601a024bcf853b8c791e214514bb67
6f52cb0920d8c36e30082f0b815969f1
```

- smc-7.0.1-11318.x86_64.iso

```
SHA1SUM:
b492c59abd477b66dd92175fc9db9d9958f35d0a

SHA256SUM:
769803d292d07994c554669c0ab2dacdeb588a1579ce742b0894107673fa877f

SHA512SUM:
1bc067ef976fbad5e02d8215f3b41374
a4b8ab86e2d418109b91378807fb762b
508055552fc7fb98a6988ea6af9b9279
b3cdda642433636fd2bca1a18299e4a1
```

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	16 GB RAM
Virtual disk space	128 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 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 the following component versions.

- Forcepoint Next Generation Firewall (Forcepoint NGFW) 6.3 or higher
- 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*.

Application health monitoring

The Application Health Monitoring dashboard proactively detects user experience issues based on connection quality metrics. 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 FONE portal by using ZTNA connector. From 7.0 onwards, ZTNA connector is integrated with NGFW Engine by default. NGFW hosts a docker container that runs ZTNA connector, which acts as a proxy for FONE portal. 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 detection for QUIC is targeted for users who are using inspection features such as Network and URL applications 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 added for Inspection rules	Action defines the command for the Engine to carry out when a connection matches the Inspection rule. The following Action Options are available in the Inspection rules: ■ Permit ■ Terminate
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.
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: ■ 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: ■ 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 *Forcepoint Next Generation Firewall Product Guide*.
Allow multiple names in domain element	You can now set multiple names in the Domain Name network element. For more information, see *Forcepoint Next Generation Firewall Product Guide*.

Security updates

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

Resolved and known issues

For a list of resolved and known issues in this product release, see Knowledge Base article 41216 .

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/s/ article/Documentation-Featured-Article.

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 and set DNS servers.

8) Select the time zone.

9) (Optional) Configure NTP settings.

10) After the SMC Appliance has restarted, install the Management Client.
    As an alternative to installing the Management Client locally, you can use SMC Web Access to start and run the Management Client in a web browser. SMC Web Access is enabled by default for new installations of 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 7.0.1.

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: 7.0.1P001

- 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: 7.0.1U001

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*.

- 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 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; 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. For detailed information on how to upgrade SMC Appliance to a new version, see *Forcepoint Next Generation Firewall Installation Guide*.

  - 6.8.6 – 6.8.13 (LTS release versions)
  - 6.9.2 – 6.9.3
  - 6.10.4
  - 6.10.9

  For SMC Appliance versions prior to 6.8.6, see Knowledge Base article 41318 for detailed information on how to upgrade SMC Appliance to a new version.

You can upgrade the SMC Appliance using the Management Client or using the appliance maintenance and bug remediation (AMBR) patching utility on the command line of the SMC Appliance. For detailed information, see *Forcepoint Next Generation Firewall Product Guide*.

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*