Forcepoint

NGFW Security Management Center Appliance

7.1.7

Release Notes

Revision B

Contents

- About this release on page 2
- Build number and checksums on page 2
- System requirements on virtualization platforms on page 3
- Compatibility on page 4
- New features on page 4
- Enhancements on page 5
- Security updates on page 8
- Resolved and known issues on page 8
- Install the SMC Appliance on page 8
- Upgrade the SMC Appliance on page 9
- Find product documentation on page 10

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 7.1.7 is 11439. This release contains Dynamic Update package 1803.

Use checksums to make sure that files downloaded correctly.

- 7.1.7P001.sap

```
SHA256SUM:
eaa2b400e6f4cd3f317de4a08856a1c9ec3345546f5b9ec65926020d37d0f1e8

SHA512SUM:
2631f6bc40dc1f858433baf91a211b00
d3ddc9c46fae8fdfb6ca972dbfcb78bd
d1b199abcc808f5d83b34f3042ec8a33
a6661e6f296101898f5b25b2bc0a4fda
```

- 7.1.7U001.sap

```
SHA256SUM:
ad0cd8534fbe9a2686a3c9ea23b9390677528f7e2e9fd417902f34b5a554daea

SHA512SUM:
82e444ebff33aee4253e320ea1fb78a4
9256a22c3ffb6c3c654e4d2461f87abc
dd755b75b1ba63970959dcf69213eb73
84f9d022765234ca11a0904e16de8411
```

- smca-7.1.7-11439.x86_64.iso

```
SHA256SUM:
063b4957e94ca2dde95d73ed25dc5e27ca8eb743bc426a27695510b4599414b4

SHA512SUM:
fd1157bfd320b9a038d84589bc726a4b
ce14e0e5e2ec4b24f7e6b89ccc1312e3
a311841d4ce6a4bc83d1d600137dc3cc
a13854b2ba3ff686fbaaa36973ce6816
```

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 7.1 can manage all compatible Forcepoint NGFW Engine versions up to and including version 7.1.

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 7.1 is all compatible with the Secure SD-WAN Engine versions up to and including version 7.1.

SMC 7.1 is compatible with Engine 6.8 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*.

Forward traffic to specific tunnels or routers

By configuring the Forced Next Hop (FNH) option in the access rule you can now force forward traffic to a specific tunnel or router.

The advantage of using this option is that you can forward the matched traffic to a specific application that has the server behind a tunnel.

For more information, see *Configure Forced Next Hop routing* section in *Forcepoint Next Generation Firewall Product Guide*.

SMC contact via FQDN

Support for using FQDN as the contact address to enable the engine to contact the SMC management server or log server. This can be beneficial when you run the SMC management server or log server in a cloud environment where managing long term public IP address is not feasible or is difficult.

For more information, see *Define Management Server or Log Server contact addresses*, and *Define contact address* sections in *Forcepoint Next Generation Firewall Product Guide*.

Additional admin user authentication methods supported

The following admin user authentication methods are supported:

- OpenID Connect authentication by using an OpenID Connect provider.
- SAML authentication by using a SAML based identity provider.

For more information, see *Authenticate administrators using OpenID authentication method*, and *Authenticate administrators using SAML v2 authentication method* sections in *Forcepoint Next Generation Firewall Product Guide*.

Improved SMC Domain Overview

The Domain Overview is updated to improve its scalability and usability to help users to easily navigate and find the domain information that they are looking for.

For more information, see *Log on to a Domain from the Domain Overview* section in *Forcepoint Next Generation Firewall Product Guide*.

User Interface Themes

You can switch between light and dark theme for SMC.

For more information, see *Customize the Management Client layout* section in *Forcepoint Next Generation Firewall Product Guide Product Guide*.

DNS Sinkholing

You can now configure DNS sinkholing for UDP and TCP service elements. One of the scenarios where this feature can be useful is, when there is an infected machine in the internal network. It can be identified by using the DNS sinkholing.

For more information, see *Create custom service elements* section in *Forcepoint Next Generation Firewall Product Guide*.

Enhancements

This release of the product includes these enhancements.

Enhancements in SMC version 7.1.4

Enhancement	Description
Radius authentication for engine log in	It is now possible to configure engines so that local administrators are authenticated via RADIUS. Also, it is possible to control if the root admin can log in only from local console or via network using SSH. RADIUS authentications of engine supports access challenge methods.  **Note** This enhancement is only supported on engine versions 7.1.3 or later.

Enhancements in SMC version 7.1.2

Enhancement	Description
Elasticsearch version update	Updated the Elasticsearch client libraries to version 8.9.2.

Enhancements in SMC version 7.1.1

Enhancement	Description
Local Sandbox - Advanced Malware Detection & Protection option	You can now configure an Advanced Malware Detection & Protection local sandbox to detect advanced threats by analyzing the behavior of files in a restricted operating system environment. **Note** You need a local Advanced Malware Detection & Protection server to use this local sandbox service. For more information, see the *Connect Secure SD-WAN to a sandbox service and the Define Sandbox Service elements* sections in the *Forcepoint Next Generation Firewall Product Guide*.
Easy identification of VPN site status	Support for enabled and disabled VPN site icons are added. The appropriate VPN site icon is displayed in the preview or editor view in SMC User Interface to help easily differentiate, if the VPN site is in enabled or disabled state.
Temporarily Ban for Multiple Failed Logon Attempts (Password Policy) option	You can now configure the password policy in the global system settings to temporarily ban an IP address, when logon attempts by a SMC administrator from a single IP address reaches the maximum failed logon attempts. For more information, see the *Centralized management of global system settings* section in the *Forcepoint Next Generation Firewall Product Guide*.
Updated the Elasticsearch client libraries to version 8.8.2	The Elasticsearch client libraries are updated to the version 8.8.2 to improve the indexing performance. **Note** In the Elasticsearch version 8.8.2, OpenSearch is no longer supported. For more information, see the *Requirements for using Elasticsearch with Forcepoint NGFW Security Management Center (SMC)* Knowledge Base Article.

Enhancements in SMC version 7.1.0

Enhancement	Description
BGP Monitoring Protocol (BMP) Configuration	Support for BMP configuration options from the Dynamic Routing Editor. It is used to monitor BGP sessions and send the monitored data from BGP routers to the network management entities. Also, when configured the log events includes the information for the configured options, and which in turn helps to make correlation of BMP and engine logs easy for analytics. For more information, see *Create core elements for dynamic routing*, and *Enable BGP on the Engine, Engine Cluster, or Virtual Engine* sections in *Forcepoint Next Generation Firewall Product Guide*.
Improved Application Health Monitoring	The Application Health Monitoring feature now comes with the following support: ■ Enhanced engine monitoring and better support for non-TCP traffic, that is there is now support for applications that use UDP for data transport. ■ Visibility into application health history and health status history of network applications. ■ Better ISP link status monitoring. ■ Application health status history. For more information, see *Application Health Monitoring Dashboard* section in *Forcepoint Next Generation Firewall Product Guide*.
Improved SD-WAN algorithms and link selection logic	The following updates have been done to provide for better user experience: ■ Engine logic is updated to avoid too much packet loss before the traffic is sent to the better links. ■ The QoS link value is tuned to make QoS link value selection feature to work as intended. Also, the **Default SD-WAN Link Balancing Preference** option is made available to allow you to set the preferences on how the traffic is balanced over the links for each engine. For more information, see *Create Link Usage Profile elements* section in *Forcepoint Next Generation Firewall Product Guide*.
Tunnel interface now supports multiple IP addresses	It is now possible to add multiple IP addresses (that can be of types IPv4 and IPv6) for tunnel interfaces.

Enhancement	Description
IPFIX forwarding	When you export IPFIX information, the following new IPFIX Element IDs are now supported: ■ EID 5 ipClassOfService ■ EID 58 vlanId (source VLAN) ■ EID 59 postVlanId (destination VLAN) ■ EID 60 ipVersion ■ EID 89 forwardingStatus ■ EID 90 mplsVpnRouteDistinguisher ■ EID 131 exporterIPv6Address **Note** 1) EID 90 mplsVpnRouteDistinguisher is exported, only when BMP monitoring is configured for the engine that originates the log entries. 2) The following IPFIX element IDs are only generated by engine version 7.1.0 or later: ■ EID 5 ipClassOfService ■ EID 89 forwardingStatus ■ EID 90 mplsVpnRouteDistinguisher

Security updates

For information about third-party packages and associated vulnerabilities included with SMC in this product release, see Knowledge Base article 11241 .

Resolved and known issues

For a list of resolved and known issues in this product release, see Knowledge Base article 4751.

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 from Forcepoint support or from P patch.
    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 7.1.7.

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: 7.1.1P001
- 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: 7.1.1U001

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 7.1 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*.
  - 6.10.13 - 6.10.17
  - 7.1.1 - 7.1.5

  For detailed information on how to upgrade the SMC Appliance from a version that is not listed above to a newer version, see Knowledge Base article 41318 .
- If you configured SNMP for the SMC Appliance before upgrading to version 6.4.0 or higher, you must configure SNMP again.

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. To create a customer account, navigate to the Customer Hub Home page, and then click the **Create Account** link.

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*

Published 13 October 2025