



Network Security Platform

7.5.1

**Security Management Center
Appliance (SMC Appliance)**

Release Notes

Contents

- [About this release](#) on page 2
- [Build number and checksums](#) on page 2
- [System requirements](#) on page 3
- [Compatibility](#) on page 4
- [New features](#) on page 4
- [Enhancements](#) on page 6
- [Resolved and known issues](#) on page 6
- [Security updates](#) on page 6
- [Install the SMC Appliance](#) on page 6
- [Upgrade the SMC Appliance](#) on page 7
- [Find product documentation](#) on page 8

About this release

This document contains important information about this software release for the Forcepoint Network Security Platform Security Management Center Appliance (SMC Appliance). We strongly recommend that you read the entire document.

The SMC Appliance ships with pre-installed Forcepoint Security Management Center 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.

Experimental Features

Some features are marked as *Experimental*. These are newly introduced features or enhancements that are still in the testing phase and may not yet be fully polished or stable. They are released to gather user feedback and identify potential issues before a broader rollout.

Build number and checksums

The build number for SMC 7.5.1 is 12645. This release contains Dynamic Update package 2069.

Use checksums to make sure that files downloaded correctly.

■ 7.5.1P001.sap

```
SHA256SUM:
ad663e0a3a2c339d6658e81fa411732bfe76bfa1d933bffff89a9dcb1d8db9ba

SHA512SUM:
4c83ff6e1c2eb3b9ef5505389db9ab6a
0b51a7bc2dcc20d3ec34c94fd146cfd8
0c7bc61b064b699800edf08f49089de9
02077ad7a3e455a83b5d88947cbcebb7
```

■ 7.5.1U001.sap

```
SHA256SUM:
58de9b2f8d34de71399c4e89733969102eded50a3cf3784340901147f8afd0ab

SHA512SUM:
85a87fcd011df468bd6d3c5d770f087a
abc103ae4371d70676881ed5e975c938
a6586dfd6ed1dbdcc18e47a4f183b54f
067ea4d76b838825846ad2d574ace4b6
```

■ smca-7.5.1-12645.x86_64.iso

```
SHA256SUM:
bc94717541aaa3d39579b664248d241c14bf536f448c590934673c92c8bae0d9

SHA512SUM:
4bb75b76cb58f8c063a2a5b72ce8e143
42b25901928bf2645dd8de605c3ba0ec
61ab74bbfae2eea41205f8c16555650c
0396ad909b06151c40f1ad10c99da47a
```

System requirements

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

Forcepoint appliance requirements

This release supports the following SKUs for the Forcepoint SMC Appliance:

- SMCAP
- SMCAPG5

Virtualization platform requirements

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.

Component	Requirement
Hypervisor	VMware ESXi version 7.0 or higher
Memory	16 GB RAM
Virtual disk space	128 GB

Component	Requirement
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 7.5 can manage all compatible Security Engine versions from 7.1.0 up to and including version 7.5.

New features

This release of the product includes these new features. For more information and configuration instructions, see the *Forcepoint Network Security Platform Product Guide*, the *Forcepoint Network Security Platform Installation Guide*, and the *Forcepoint NGFW Manager and VPN Broker Product Guide*.

Management Server High Availability (HA) support for SMC Appliance

SMC Appliance now supports Management Server High Availability (HA), allowing one Management Server to be active while the other Management Servers remain on standby. For more details, refer to the [Management Servers for HA](#) topic.

Quarantine for Malicious Files

Added the ability to quarantine and store malicious files identified by File Filtering policy rules, enabling secure forensic analysis via the Log Server.

IPv6 Support for Modem (LTE/5G) Interfaces

Modem interfaces can now be configured to acquire dynamic IPv6 address.

Multiple LTE/5G APN for Modem interfaces

Added support for configuring multiple LTE/5G Access Point Names (APNs) to enable advanced network connectivity requirements.

Local Web Content Classification for Uncategorized URLs

Added support for real-time methods for local scanning to enable content classification based on the actual web page content when a predefined URL category is not available in the local database. This reduces reliance on cloud queries and minimizes Unknown results. This feature is available in engines with URL Filtering license and 16 GB or more memory. For more details, refer to the *Enable ThreatSeeker* topic in the *Forcepoint Network Security Platform Online Help*

Security Engine HA with Policy-Based VPN in Cloud Environments

Enables multiple Engines to share an identical VPN gateway configuration, allowing for seamless failover and load balancing in cloud and disaster recovery environments using the High Availability (HA) script. For more details, refer to the [000012534](#) Knowledge Base Article

Traffic Flow Confidentiality

Added support for Precedence Hiding via Differentiated Services Code Point (DSCP) copy restriction and Traffic Flow Confidentiality (TFC) Padding to strengthen data privacy and obfuscate traffic patterns in VPN profiles. For more details, refer to the *Create VPN Profile elements* topic, in the *Forcepoint Network Security Platform Online Help*

In-band user authentication tracking for HTTP connections

Enables granular user tracking for multi-user hosts and NAT environments by utilizing encrypted HTTP cookies to bind authentication and connection confirmation for specific browser sessions. For more details, refer to the *Browser Session Options* section in the *Define Action options in Access rules* topic, in the *Forcepoint Network Security Platform Online Help*.

Confirm Action in User Response

Added support for a **Confirm** user response action that prompts users before continuing to a target domain and caches their confirmation in an encrypted HTTP cookie to bypass subsequent prompts.

Tagged and Untagged VLANs on the same Physical Interface

Engines now support configuring a native VLAN on physical interfaces, allowing both tagged and untagged traffic to be processed on Layer 3 Physical Interfaces.

Enhancements

This release of the product includes these enhancements.

Enhancements in SMC Appliance version 7.5.1

Enhancement	Description
IKEv2/IPSec Dead Peer Detection (DPD) Enhancement	Added support for configurable DPD Interval (1–28800 seconds) and DPD Timeout (1–300 seconds) values in Gateway Settings to improve IKEv2/IPSec connection monitoring.

Resolved and known issues

For a list of resolved and known issues in this product release, see Knowledge Base article [12642](#).

Security updates

For information about third-party packages and associated vulnerabilities included with SMC Appliance in this product release, see Knowledge Base article [12930](#).

Install the SMC Appliance

Use these high-level steps to install the SMC Appliance.

For detailed information about installing the SMC Appliance and the Security Engines, see the *Forcepoint Network Security Platform Installation Guide*. All guides are available for download at help.forcepoint.com.

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 Network Security Platform Installation Guide*.

- 5) Select a role of the management server from the following options:
 - Select the **Standard Appliance** option, and click **Next**, and then continue from **Step 6**.
 - Select the **Additional Management Appliance** option, and click **Next** and then do the following:
 - a) Enter the following details:
 - i) **Active Management IP / FQDN**
 - ii) **Username on Active Management**
 - iii) **Password on Active Management**
 - b) Click the **OK** button, and then continue from **Step 6**.
- 6) Make your security selections.
- 7) Complete the network interface and network setup fields.
- 8) Enter a host name for the Management Server and set DNS servers.
- 9) Select the time zone.
- 10) (Optional) Configure NTP settings.
- 11) After the SMC Appliance has restarted, you can use the SMC Web Access with a web browser to access the management UI of the SMC Appliance.

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.
- 12) Import the licenses for all components.

You can generate licenses at <https://stonesoftlicenses.forcepoint.com>.
- 13) Create the Security Engine elements, then install and configure the Security Engines.

Upgrade the SMC Appliance

Use an upgrade patch to upgrade the SMC Appliance from a previous version to version 7.5.1.

There are two kinds of SMC Appliance patches:

- 1) **Hotfix patches** include bug fixes and other improvements for the current SMC Appliance version. In addition, P patches also include binaries for the standalone client. Once the patch is activated, these binaries become available through the SMC Downloads.

Hotfix patch files use the letter **P** as a separator between the version number and the patch number.

Example: 7.3.1P001

- 2) **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: 7.3.1U001

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 Network Security Platform Installation Guide*.

- SMC 7.5 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 SMC Client before upgrading the software.
- The SMC Appliance must be upgraded before the Security 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 Engine versions being managed. For detailed information on how to upgrade SMC Appliance to a new version, see *Forcepoint Network Security Platform Installation Guide*.
 - 6.10.13 - 6.10.19
 - 7.1.1 - 7.1.10
 - 7.2.1 - 7.2.6
 - 7.3.0 - 7.3.4
 - 7.4.0 - 7.4.1

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](#).

You can upgrade the SMC Appliance using the SMC 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 Network Security Platform 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 Network Security Platform Product Guide*
- *Forcepoint Network Security Platform 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 Network Security Platform Installation Guide*

Other available documents include:

- *Forcepoint Network Security Platform Hardware Guide* for your model
- *Forcepoint Security Management Center Console Appliance Hardware Guide*
- *Forcepoint Network Security Platform Quick Start Guide*
- *Forcepoint Security Management Center Console Appliance Quick Start Guide*
- *Forcepoint Security Management Center 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*

