Forcepoint

Network Security Platform

7.4.1

Security Management Center Appliance (SMC Appliance)

Release Notes

Revision A

Contents

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.

Note

The SMC Appliance does not support high-availability for the Management Server or the Log Server.

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 7.4.1 is 12025. This release contains Dynamic Update package 1991.

Use checksums to make sure that files downloaded correctly.

- 7.4.1P001.sap

```
SHA256SUM:
b303c6e046140a4a2db65320ce7cecc93f65102de5d4ba1cb42fd668eae290f0

SHA512SUM:
d8c10ea3fdd25d45daec5bed626eea8e
a906d55e936b0744ef1ba0fff2b89870
213bda0754df1d43478620e50d827359
0c5244fb628fd25ec206a2569f0ec8c5
```

- 7.4.1Q002.sap

```
SHA256SUM:
df30db99799d093beee376792d8a2776c3f5081bee9f456ce26ee9d84289fe85

SHA512SUM:
36c2f8fc96cd1e78e17061ffa10db960
8f3ec879e76ebadb7113264a55ac5a49
00279ba91b6a89980c647db11ba3b5d8
1c64f0db8ab26e2573eee10058d1e0b1
```

- 7.4.1U001.sap

```
SHA256SUM:
e5c9abffeef15f704c2b13336d5a9c7046981db42e46f906d343928f8aa1d2bc

SHA512SUM:
10c6104a5b3906bdbfaf84dbb18c6b5f
14ef6ce7e5e95f4818bf2de1f6a27dee
0121bda893010950dca22bd678dee790
fa37b446b7f967c96af26ced91c58227
```

- smca-7.4.1-12025.x86_64.iso

```
SHA256SUM:
6caa7376f25dbd3c1e93c782a5380e0867008cc925bd2b33a4a745153fec8563

SHA512SUM:
066f110cea4ceb377b8097026abac893
459a1c9147303049ad2c35ac3c771175
99e41482973ca5e40d2a6397b6b7e6f3
aded2f3c7de84417ff3367b2b2c816d8
```

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
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 7.4 can manage all compatible Security Engine versions from 7.1.0 up to and including version 7.4.

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* and the *Forcepoint Network Security Platform Installation Guide*.

Explicit proxy support for HTTP and HTTPS protocols

The Security Engine can be configured to act as an explicit proxy for HTTP and HTTPS connections. Proxy authentication is supported.

Note

The Explicit Proxy feature requires a separate license.

HTTP/3 inspection (Experimental)

The Security Engine can now inspect the complete HTTP/3 connection by decrypting the traffic between the client and server. After inspection, the engine re-encrypts the data before forwarding it to the intended recipient. This feature's support status is experimental in this release.

SAML user authentication

Both Application Access Portal (previously SSL VPN Portal) and Browser Based User Authentication features now support user authentication via SAML.

Enhancements

This release of the product includes these enhancements.

Enhancements in SMC Appliance version 7.4.0

Enhancement	Description
Application Access Portal improvements	Application Access Portal (previously SSL VPN portal) now supports TLS 1.3. Also support for WebSocket protocol has been added.
Datagram Transport Layer Security (DTLS) tunneling protocol support	The Security Engine supports DTLS tunneling protocol for Forcepoint VPN Client versions that have the DTLS support included. This feature can now be configured normally through SMC. Using DTLS can improve remote access performance compared to TLS based tunnels when network conditions are challenging.
Local ThreatSeeker URL Categorization database	You can choose to either use the locally downloaded ThreatSeeker URL Categorization database or use the Cloud-based ThreatSeeker URL Categorization database for URL filtering.  **Note** This feature is supported on engines that have at least 16 GB of memory.
Log Server per Virtual Engine	You can now assign a dedicated log server to a virtual engine. Previously, the log data from virtual engine was sent to the same log server as the Master Engine.
Support for user authentication using email format usernames	Previously user authentication did not support usernames that contain the @-character used in email addresses or in UPN Active Directory user attribute. Forcepoint Network Security Platform can now be configured to allow the use of either an email address or a UPN as the user ID in configuration and user authentication.
URL Category sync with Forcepoint portfolio	Unified the URL category taxonomy across web security features for all Forcepoint products.  **Note** When upgrading from SMC version 7.3 or earlier to version 7.4, any URL categories that are used in policies will be automatically converted to reflect the latest changes present in the URL Categories.

Enhancement	Description
User or group-based policies	You can now include users and user groups in access policy rules for a managed engine even if SMC is not able to query an external LDAP or AD server. **Note** The engine must be able to access the LDAP server for user authentication, even if the LDAP server is not accessible from SMC. When user authentication is SAML-based, it is also possible to operate the engine without LDAP server access.

Resolved and known issues

For a list of resolved and known issues in this product release, see Knowledge Base article 12234.

Security updates

For information about third-party packages and associated vulnerabilities included with SMC Appliance in this product release, see Knowledge Base article 12283 .

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) 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, 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.

11) Import the licenses for all components.
    You can generate licenses at https://stonesoftlicenses.forcepoint.com.

12) 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 7.4.1.

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 7.4 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 - 6.10.18

- 7.1.1 - 7.1.9
- 7.2.1 - 7.2.6
- 7.3.0 - 7.3.3
- 7.4.0

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. See 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*

Published 20 March 2026