



Network Security Platform

7.4.0

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

Release Notes

Contents

- [About this release](#) on page 2
- [Build number and checksums](#) on page 3
- [System requirements](#) on page 3
- [Compatibility](#) on page 4
- [New features](#) on page 4
- [Enhancements](#) on page 5
- [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.



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.

Upgrade deadline

Without installing the separate certificate update patch that is described in the [12281](#) Knowledge Base Article, this update can only be installed before 21st of January 2026 due to the expiration of the current update certificate. If you cannot install this update before 21st of January 2026, install the patch that is described in the [12281](#) Knowledge Base Article before that date to update only update certificates of your current installation. Otherwise, SMC Appliance upgrades or patches cannot be successfully installed after that date.

Build number and checksums

The build number for SMC 7.4.0 is 12012. This release contains Dynamic Update package 1958.

Use checksums to make sure that files downloaded correctly.

■ 7.4.0P001.sap

SHA256SUM:
21d81f108161f2f1db795dc535ff4045034e4a36b27056a47a659dafb23c2c70

SHA512SUM:
ef5fe15ca9f018f29180829595d00eb4
d9f322fc3e19f34698ef6439d1501725
33d8ce01f55b956859addfb59a4c5a59
d6c018fb1bb877953bf27b2944f67d16

■ 7.4.0U001.sap

SHA256SUM:
42e530a78e7348fb66a4b7fc78c845e4797b4fc415104d7eb50d5543b1148488

SHA512SUM:
571faf1a6b8db03baa0af109683ab9e8
9ae445df2cecb9fa857fb3e7b6cfc8ee
ab84c1fa84b6295dc2fbe573f44df3dc
1c78a51d5f196e348ef64b0e217bcd90

■ smca-7.4.0-12012.x86_64.iso

SHA256SUM:
25b9b3c480a2259d57a96a8aef191d57f3d70b08da5174672f122eed36bbc43d

SHA512SUM:
4c371b153100c56f34079870dcf5475d
2309fdd832b21e63c8c48769106aa4b9
bb8a6adcb504a2f00d494e053fe0fc66
60c749b4ec5ec551d67f9a286990dc40

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	<p>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.</p> <div>  <p>Note</p> <p>This feature is supported on engines that have at least 16 GB of memory.</p> </div>
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	<p>Unified the URL category taxonomy across web security features for all Forcepoint products.</p> <div>  <p>Note</p> <p>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.</p> </div>
User or group-based policies	<p>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.</p> <div>  <p>Note</p> <p>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.</p> </div>

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 7.4.0.

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 - 7.1.8
 - 7.2.1 - 7.2.6
 - 7.3.0 - 7.3.1

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. 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*

