



Network Security Platform

7.4.1

Security Management Center (SMC)

Release Notes

Contents

- [About this release](#) on page 2
- [Lifecycle model](#) on page 2
- [System requirements](#) on page 3
- [Build number and checksums](#) on page 4
- [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
- [Installation instructions](#) on page 6
- [Upgrade instructions](#) on page 7
- [Find product documentation](#) on page 8

About this release

This document contains important information about this release of Forcepoint Security Management Center. We strongly recommend that you read the entire document.

For detailed information about changes introduced in the SMC API since the previous version, see the automatically generated change log reports in the `api_change_log.zip` file in the `Documentation/SMC_API` folder of the SMC installation files.

Lifecycle model

This release of Forcepoint Network Security Platform Security Management Center is a Feature Stream (FS) version.

Support for Feature Stream versions is discontinued when a new major version of Forcepoint Network Security Platform is available.

We recommend using the most recent Long-Term Support (LTS) maintenance versions if you do not need any features from a Feature Stream version.

For more information about the Forcepoint Network Security Platform lifecycle policy, see <https://support.forcepoint.com/ProductSupportLifeCycle>.

System requirements

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

SMC hardware requirements

You can install the SMC on standard hardware.

Component	Requirement
CPU	Intel® Core™ family processor or higher recommended, or equivalent on a non-Intel platform
Disk space	- Management Server: 6 GB - Log Server: 50 GB
Memory	- Management Server, Log Server: 16 GB RAM - If all SMC servers are on the same computer: 32 GB RAM - If you use the SMC Web Access feature: an additional 2 GB RAM per concurrent administrator session - SMC Client: 2 GB RAM The SMC server requirements are the <i>minimum</i> requirements. The Management Server and Log Server in particular benefit from having more than the minimum amount of RAM. On high-end appliances that have a lot of RAM, the SMC might not provision the maximum amount of RAM for use by the SMC servers. For information about how to manually modify the provisioning, see Knowledge Base article 33316.
SMC Client peripherals	- A mouse or pointing device - Display with 1280x768 resolution or higher

Operating systems

You can install the SMC on the following operating systems. Only 64-bit operating systems are supported.

Linux	Microsoft Windows
- Red Hat Enterprise Linux 9, and 10 - SUSE Linux Enterprise 15 - Ubuntu 22.04 LTS and 24.04 LTS - Amazon Linux 2023	Standard and Datacenter editions of the following Windows Server versions: - Windows Server 2025 - Windows Server 2022 You can also install the SMC stand-alone demo and SMC Client on Windows 11.

We recommend that you only use operating system versions that are currently supported by the vendor.

Other versions of the listed operating systems might be compatible, but have not been tested. Only U.S. English language versions of the listed operating systems have been tested, but other locales might also be compatible.

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.

- `smc_7.4.1_12025.zip`

```
SHA256SUM:  
1c6ffe5dafb4069d75102fccf8ad9c449d7d1d2f91c41e0d9f04c0d90c75a013
```

```
SHA512SUM:  
2d89ade01849fdf7692580d138b2178f  
71cadb34ee09fdc3c07475038122d81d  
0ca8cf9c935b9768522be2e3c52723b1  
d8f1ed7fbf1ba3aeea9738e706bde690
```

- `smc_7.4.1_12025_linux.zip`

```
SHA256SUM:  
0c1df9e6bc47ca34ced4ee9123b6fcd6996c4f57cefb1602e2edbee5250ed31a
```

```
SHA512SUM:  
31bb7cefdb5de571b79735ba495ef070  
9dfda5beee537102c28e9ee9130a081a  
d45dcfabcb9bf22bd6c3362a3229c8735  
454f34df8af17a9e75d4935e6175157f
```

- `smc_7.4.1_12025_windows.zip`

```
SHA256SUM:  
fb81237d5ad3aab804dc46eea13a3ae053293daccf900378faad2dff6b0f4101
```

```
SHA512SUM:  
13aaecca3976e46894a31746189ec81  
163656b83a741418c8897310877627f0  
e236f22084419e32ac985c766bc1a476  
b9905233393e3fe21b3d6529540de3aa
```

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*, the *Forcepoint Network Security Platform Installation Guide*, and the *Forcepoint NGFW Manager and VPN Broker Product 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 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.

Enhancement	Description
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.
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 in this product release, see Knowledge Base article [12235](#).

Installation instructions

Use these high-level steps to install the SMC and the Security Engines.

For detailed information, see the *Forcepoint Network Security Platform Installation Guide*. All guides are available at help.forcepoint.com.

Steps

- 1) Install the Management Server, the Log Servers.
- 2) Import the licenses for all components.
You can generate licenses at <https://stonesoftlicenses.forcepoint.com>.

- 3) Configure the Engine elements in the SMC Client from the **Engine Configuration** navigation menu.
- 4) To generate initial configurations, right-click each Security Engine, then select **Configuration > Save Initial Configuration**.
Make a note of the one-time password.
- 5) Make the initial connection from the Security Engines to the Management Server, then enter the one-time password.
- 6) Create and upload a policy on the Security Engines in the SMC Client.

Upgrade instructions

Take the following into consideration before upgrading the SMC.



Note

The SMC (Management Server, Log Server, and Web Access Server) must be upgraded before the Engines are upgraded to the same major version.

- 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 in the SMC Client before upgrading the software.
- To upgrade a lower version of the SMC to 7.4, we strongly recommend that you stop all SMC servers and create a backup before continuing with the upgrade. After creating the backup, run the appropriate setup file, depending on the operating system. The installation program detects the old version and does the upgrade automatically.
- To upgrade a non LTS version of SMC to 7.4, we strongly recommend that you first upgrade to the next LTS version of SMC before you upgrade to the latest version of SMC.
- When you upgrade the SMC, the dynamic update package that is included with the SMC installer is imported and activated. However, if a newer version of the dynamic update package has previously been imported or downloaded before the upgrade, the newest version is activated instead.
- 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 Security Engine versions being managed.
 - 6.10.0 – 6.10.18 (LTS release versions)
 - 7.1.0 – 7.1.9 (LTS release versions)
 - 7.2.0 – 7.2.6
 - 7.3.0 – 7.3.3 (LTS release versions)
 - 7.4.0

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 Hardware Guide* for your model
- *Forcepoint Network Security Platform 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*

