



Network Security Platform

7.5.1

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 7
- [Resolved and known issues](#) on page 7
- [Security updates](#) on page 7
- [Installation instructions](#) on page 7
- [Upgrade instructions](#) on page 8
- [Find product documentation](#) on page 9

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 with Service Pack 6 - Ubuntu 24.04 LTS and 26.04 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 7.5.1 is 12645. This release contains Dynamic Update package 2069.

Use checksums to make sure that files downloaded correctly.

- `smc_7.5.1_12645.zip`

```
SHA256SUM:  
6a1ca452b050aee058a9e32a1961721be4ba1756285054fe6cd9a6f640d9b671
```

```
SHA512SUM:  
8858f3ccb2d8a7d0b8aa3c6b7fc9180e  
e526cd8578ec313d18eb5f53ad90a7b0  
22c944d7a645d5c67999e7f8ccdfa307  
06500b67a4f58178abd764c74477b8c9
```

- `smc_7.5.1_12645_linux.zip`

```
SHA256SUM:  
8043b977bbd538a2ab02bfe8c354f1a5e5fdeab7a5510e0c24f0030e83b3dd7a
```

```
SHA512SUM:  
5080a665c89463053cffd4f424e6090a  
dcc68540bc3a57b492a159d813323d1c  
a0115b20042761c5acc9bdb91d62eb3a  
7e4cb9ae2e1c4a90b6c30a093917cda5
```

- `smc_7.5.1_12645_windows.zip`

```
SHA256SUM:  
2a0e217a20e70f3b3469b0103c198bd7c96d15fc057ca607c8fe27501c3395e4
```

```
SHA512SUM:  
770adad58e9bc485fe727a986809defc  
de04d4d4355f14e855df8d2daee1fd29  
f2c9d3f6767a09fb48ef01c1f24b8943  
36364fc9db1d647fdd3423e87c82e43e
```

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*.

Infrastructure-as-Code Automation for SMC using Terraform

Added support for automating Security Management Center (SMC) configurations and operations using the [Forcepoint NGFW SMC Terraform Provider](#).

Zero Touch Provisioning (ZTP) with Local Installation Server

Added capability to host the installation server locally on-premises to support secure Zero Touch Provisioning (ZTP) configurations for customer environments. For more details, refer to the [000012674](#) Knowledge Base Article.



Important

This feature is available only for appliances that are shipped with or upgraded to a version that includes this feature for Security Engine side as well. At SMC 7.5.0 release time this is supported only if Security Engine appliance is first upgraded to 7.5.0 or newer version.

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 version 7.5.0

Enhancement	Description
Elasticsearch and OpenSearch Improvements	Optimized storage efficiency for SMC logs to reduce disk space requirements in Elasticsearch and OpenSearch clusters.
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 in this product release, see Knowledge Base article [12643](#).

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 7.5 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 in the SMC Client before upgrading the software.
- To upgrade a lower version of the SMC to 7.5, 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 7.5, 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.
 - 6.10.12 – 6.10.19 (LTS release versions)
 - 7.1.0 – 7.1.11 (LTS release versions)
 - 7.3.0 – 7.3.4 (LTS release versions)
 - 7.4.0 – 7.4.1
 - 7.5.0

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*

