Network Security Platform

7.3.0

Security Management Center (SMC)

Release Notes

Revision A

Contents

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.

Product name change

Starting from Forcepoint Network Security Platform version 7.3 release the product name has changed from Forcepoint FlexEdge Secure SD-WAN to Forcepoint Network Security Platform. The primary changes are listed below:

Component	Old name	New name
Solution	Forcepoint FlexEdge Secure SD-WAN	Forcepoint Network Security Platform
Management	FlexEdge Secure SD-WAN Manager / SD-WAN Manager Console (SMC)	Security Management Center (SMC)
Engine	FlexEdge Secure SD-WAN Engine	Security Engine

Note

The migration of the new Web Portal UI to the Management Server, the existing Web Portal Server will be retained solely for WebSwing access. As a result, the term Web Portal Server will be replaced with Web Access Server across all relevant components.

Currently, product name change is visible in SMC and in the following documentations:

- *Forcepoint Security Management Center API User Guide*
- *Forcepoint Network Security Platform Installation Guide*
- *Forcepoint Network Security Platform Product Guide*
- *Forcepoint Network Security Platform Online Help*
- *Forcepoint Network Security Platform Quick Start Guide*

For more information on SMC UI terminology change, refer to the **About this Help** section in the *Forcepoint Network Security Platform Product Guide*.

Note

Some documentations, knowledge base articles, and other support information are still using the old product name.

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.

Lifecycle model

This release of Forcepoint Network Security Platform's Security Management Center is a Long-Term Support (LTS) version.

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

Component	Requirement
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 *minimum* 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 8, and 9 ▪ SUSE Linux Enterprise 12 and 15 ▪ Ubuntu 22.04 LTS and 24.04 LTS ▪ Amazon Linux 2 Kernel 15	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 7.3.0 is 11693. This release contains Dynamic Update package 1887.

Use checksums to make sure that files downloaded correctly.

- smc_7.3.0_11693.zip

```
SHA256SUM:
4bc088f53a8ef38985c8ce0bb056969f8ed760ef288a2211248e095b18e56360

SHA512SUM:
adff05265c7528f509b00acd217fe28b
21a90cb2f70313a6a973acabc8948410
f6bfaa191577d91cfdb31961a1fe375c
60bbe4b72f4a9002a076b99ac724f182
```

- smc_7.3.0_11693_linux.zip

  ```
  SHA256SUM:
  18d7ca090d7673d1ab62c5ef6f57156e260a9bd78c7da91ac74ee53e4f2b4db8

  SHA512SUM:
  2b8cd9b293049d6245b62c41c390bedb
  2321e4b441916ec43076d9563005480e
  f3c60e88f541ebf3703f8fab2d16defc
  519f318e4426ccb40a40f02f5ea94b64
  ```

- smc_7.3.0_11693_windows.zip

  ```
  SHA256SUM:
  2bf51c3327adf578473d060fb5bdb06568f54f6d770e849461e639dc4a029a19

  SHA512SUM:
  748942904fbe710c037d1128ea880a29
  97c9a795422ba38907f505a052b33b0e
  671cc39af8fb4cf76db12000bd4943e3
  1cbd7895bfc9143328dedb804ad7e348
  ```

Compatibility

SMC 7.3 can manage all compatible Security Engine versions from 6.10 up to and including version 7.3.

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 Security Engine Manager and VPN Broker Product Guide*.

Post-quantum Security for IPsec VPNs

Post-quantum security is now supported for site-to-site IPsec VPN tunnels by mixing preshared keys in the Internet Key Exchange Protocol Version 2 (IKEv2) as specified in RFC 8784.

SMC Web Access certificate authentication

The SMC Web Access UI can authenticate administrators utilizing client certificates.

Read-only Web Portal UI for admins (Experimental)

The previously deprecated Web Portal UI functionality re-implemented utilizing the SMC API can now be enabled via SMC API settings of the Management Server. The old Web Portal UI will no longer be available in SMC 7.3.0.

Explicit proxy with IWA proxy authentications (Experimental)

You can now configure the Explicit HTTP proxy to allow clients to send traffic to the engine before it is sent to the destination.

Enhancements

This release of the product includes these enhancements.

Enhancements in SMC version 7.3.0

Enhancement	Description
AES-GCM-256 support in IKEv2	IPsec VPNs can now be configured to use AES-GCM cipher mode also in IKE negotiations. This mode is used in three new predefined VPN profiles: CNSA-GCM-256-ECDH-384, CNSA-GCM-256-DH-3072 and CNSA-GCM-256-DH-4096.
Wi-Fi 6 (802.11ax) support	WLAN interface configuration now supports new 802.11ax wireless mode and WPA3 security that can be used with compatible appliance revisions.
CRL prefetching	Administrator configured certificate revocation lists (CRLs) can now be fetched and cached even before those are needed for certificate validation.

Resolved and known issues

For a list of resolved and known issues in this product release, see Knowledge Base article 11661 .

Security updates

For information about third-party packages and associated vulnerabilities included with SMC in this product release, see Knowledge Base article 11726 .

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 7.3 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 7.3, 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.
- 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 – 6.10.17 (LTS release versions), 6.10.100
  - 6.11.0 – 6.11.2
  - 7.0.0 – 7.0.4
  - 7.1.0 – 7.1.7 (LTS release versions)
  - 7.2.0 – 7.2.4

Deprecated features

Before upgrading, please consider these feature deprecations.

Feature	Description
Legacy IPsec VPN algorithms removed	Support for legacy and insecure IPsec VPN algorithms has been removed from Security Engine version 7.3. This includes the removal of support for DES and Blowfish ciphers, the MD5 message digest algorithm, and Diffie-Hellman groups 1 (768-bit) and 2 (1024-bit). SMC still supports configuring these algorithms for older, supported versions of the Security Engines.
Legacy Web Portal UI service removed	Support for the legacy and insecure Web Portal UI service has been removed. It has been replaced with a re-implemented service using the SMC API, offering similar basic read-only admin access.

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 Security Engine Manager and VPN Broker Product Guide*

Published 11 June 2025