Forcepoint

NGFW Security Management Center

6.8.4

Release Notes

Contents

About this release

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

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, Web Portal Server: 6 GB RAM ■ If all SMC servers are on the same computer: 16 GB RAM ■ If you use the SMC Web Access feature: an additional 2 GB RAM per administrator session ■ Management 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 10016.
Management Client peripherals	■ A mouse or pointing device ■ SVGA (1024x768) display or higher

⚠️ **CAUTION**

To protect the privacy of your data, we recommend using dedicated hardware for all NGFW, SMC, and SMC Appliance installations. For cloud-based virtualization platforms, use an instance type that runs on dedicated hardware. For on-premises virtualization platforms, install the NGFW Engines, SMC components, or SMC Appliance on a hypervisor that does not host any other virtual machines. For third-party hardware, do not install any other software on the computer where you install the NGFW Engines or SMC components.

Operating systems

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

Linux	Microsoft Windows
■ CentOS 7 and 8 ■ Red Hat Enterprise Linux 7 and 8 ■ SUSE Linux Enterprise 12 and 15 ■ Ubuntu 16.04 LTS and 18.04 LTS	Standard and Datacenter editions of the following Windows Server versions: ■ Windows Server 2019 ■ Windows Server 2016 ■ Windows Server 2012 R2 On Windows 10, you can install the SMC in demo mode. You can also install the Management Client.

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 6.8.4 is 10922. This release contains Dynamic Update package 1310.

Use checksums to make sure that files downloaded correctly.

- smc_6.8.4_10922.zip

  ```
  SHA1SUM:
  69c0f6f86db60e674db6b664478db6482a90f3b3

  SHA256SUM:
  816204d57297523850ccdcbc1ababc8bd2f785b90492adb5e4f0e8ad2b34cb18

  SHA512SUM:
  4e40d4b82daf71f374b408e947a927ba
  8fdd8d8e54fbb2ddd787c0e70126a899
  3cfbaccbe62e57c3d4e2571fe0179f95
  e4ac06489ae97ebc0ae02771c49abc51
  ```

- smc_6.8.4_10922_linux.zip

  ```
  SHA1SUM:
  91f0d169e9c5845472dbf22ca959a8c5604e21c7

  SHA256SUM:
  f58977a94f296e6d8cd82b4209cc25bfe111c15e9caefefdec0397685bab2fa5

  SHA512SUM:
  0142527e485a393c299e70053e86ebd5
  76417688085ce30f12b2bfaaa70c6346
  d6a6e898385bb4757780f14620a9600f
  21719a287a74f8e592070d196fe2612d
  ```

- smc_6.8.4_10922_windows.zip

  ```
  SHA1SUM:
  a6b35c5c19d94d95b538d6aacd0add4243018092

  SHA256SUM:
  56044e59be145ee076c4ca2db3aac369c6f8cf96d9b94360352ee6f9aae514a6

  SHA512SUM:
  6096c7e790b2d7782e291dfd924f2c37
  c1c89e9baa84391f541665d506c753e9
  e11aa58d4dc4551f616fab0a6cdd13b2
  cf75d4af4ddd73f4d365c81060fbf1b4
  ```

Compatibility

SMC 6.8 can manage all compatible Forcepoint NGFW Engine versions up to and including version 6.8.

⚠️ **Important**

Some versions of Forcepoint NGFW have reached end-of-life status and no longer receive maintenance releases that contain security updates. Even though these Forcepoint NGFW versions might be compatible with the SMC, we recommend that you use a Long-Term Support version that is still supported. For more information about the Forcepoint NGFW lifecycle policy, see https://support.forcepoint.com/ProductSupportLifeCycle.

SMC 6.8 is compatible with the following component versions.

■ Forcepoint Next Generation Firewall (Forcepoint NGFW) 6.3 or higher

■ McAfee Next Generation Firewall (McAfee NGFW) 5.10

■ Stonesoft Firewall/VPN Express 5.5

■ McAfee ePolicy Orchestrator (McAfee ePO) 5.3 or higher

■ McAfee Enterprise Security Manager (McAfee ESM) 9.2.0 or higher (9.1.0 CEF only)

New features

This release of the product includes these new features. For more information and configuration instructions, see the *Forcepoint Next Generation Firewall Product Guide* and the *Forcepoint Next Generation Firewall Installation Guide*.

UIID license binding for SMC licenses

When you install the SMC or upgrade the SMC to version 6.8, the SMC generates a Unique Installation Identifier (UIID). As an alternative to binding licenses for SMC components to the IP addresses of the components, you can now bind the SMC licenses to a UIID. Using UIID binding allows organizations to obtain SMC licenses without disclosing the internal IP addresses of the SMC components.

> **Note**
>
> The UIID is not stored in SMC backups or restored when you restore a backup. After the UIID is generated, it will not be overwritten when you restore backups or upgrade the SMC in the future.

You can continue to use your existing licenses or optionally change the license binding method. You can use IP-address-bound licenses for some SMC components and UIID-bound licenses for other SMC components.

Management Client downloads from the Management Server

Java Web Start is no longer supported in SMC 6.8. As an alternative, you can now configure the Management Server to provide the Management Client installation files on a download web page hosted by the Management Server. Administrators download and install the Management Client from the locally hosted SMC Downloads web page.

> **Note**
>
> Management Client downloads are not supported for macOS in SMC 6.8. For administrators who use macOS, we recommend using the SMC Web Access feature.

Enhancements

This release of the product includes these enhancements.

Enhancements in SMC version 6.8.0

Enhancement	Description
Easier configuration of dynamic link selection for NGFW Engines	It is now possible to select Link Usage Profile elements for NGFW Engines in the Firewall/VPN role to define which link types are preferred, avoided, or not used for specific types of outbound Multi-Link traffic. NGFW Engine-specific exceptions to the Link Usage Profile also allow you to specify which traffic uses specific NetLinks.
Re-authentication when using browser-based user authentication	If an end user has authenticated using browser-based user authentication and the session will soon expire, the user can re-authenticate to extend the authentication time-out and avoid connections closing before the user has finished their tasks.
Custom script upload for NGFW Engines when using Custom Properties Profile elements	To upload custom scripts to the NGFW Engine, you can add the scripts to the properties of the NGFW Engine using a Custom Properties Profile element. The scripts are uploaded when the policy is installed or refreshed.
Expiration time for one-time passwords	You can now set the expiration time for one-time passwords that are generated when you save the initial configuration for an NGFW Engine. If the one-time password is not used, it automatically expires after the expiration time has elapsed. By default, one-time passwords expire after 30 days.
PPPoE support on VLAN interfaces	You can now configure point-to-point protocol over Ethernet (PPPoE) for dynamic IP addresses that are assigned to VLAN interfaces.
User domain support for integrated ICAP servers for DLP	NGFW integration with external ICAP servers for DLP now uses the WinNT schema in the X-Authenticated-Users header instead of the Local schema that was used previously. Using the WinNT schema allows matching users against a user domain in the user directory on the ICAP server.

Enhancements in SMC version 6.8.2

Enhancement	Description
Configurable timeout for session monitoring	Previously, monitoring views might have failed to open when there were several backup Log Servers and the primary Log Server was unreachable. You can now define the timeout for receiving monitoring data from NGFW Engines. To define the timeout, edit the <installation folder>/data/SGConfiguration.txt file and add the following parameter: `SESMON_LOGSERVER_SELECTION_TIMEOUT=<timeout_in_milliseconds>` The default value is 20000.

Enhancements in SMC version 6.8.3

Enhancement	Description
Resource monitoring for SMC servers and the Management Client	The **Info** pane for Management Servers, Log Servers, and Web Portal Servers now shows information about resource usage on the computers where the servers are installed. The bottom right corner of the Management Client window shows the memory usage of the Management Client. If the memory usage gets too high, the Management Server, Log Server, Web Portal Server, or the Management Client automatically restarts. When the server or the Management Client restarts, an alert and an audit entry are generated. You can optionally disable automatic restart.
Password policy enhancements	The settings for password complexity requirements in the password policy now also apply to SMC administrator accounts that are replicated as local administrator accounts on NGFW Engines, the root account on NGFW Engines, and the Management Server database password.
New Log Server and Management Server configuration parameters	In the LogServerConfiguration.txt file, you can now add a new configuration parameter to recover connectivity from the Log Server to TCP syslog servers. For more information, see Knowledge Base article 19219. In the SGConfiguration.txt file, you can now add a new configuration parameter to define how many tasks the Management Server can run in parallel. For more information, see Knowledge Base article 19218.
More granular identification of Microsoft Office 365 network applications	Starting from dynamic update package 1300, the Microsoft-Office-365 Network Application element includes dependencies that allow more granular identification of Microsoft Office 365 in traffic. No action is required if you use the Microsoft-Office-365 Network Application element in the following types of rules: ■ Access rules with the Allow, Discard, Refuse, or Jump action ■ NAT rules If you use the Microsoft-Office-365 Network Application element in an access rule with the Continue action, you must manually add the Network Application elements that are listed as dependencies. Options that are configured in a rule with the Continue action are not automatically applied to dependencies. For more information, see Knowledge Base article 19195.

Enhancements in SMC version 6.8.4

Enhancement	Description
Optimization of status monitoring in large-scale SMC environments	New parameters for the Management Server and Log Server allow you to optimize the performance of status monitoring for NGFW Engines, VPNs, and NetLinks for SD-WAN in large-scale SMC environments. For more information, see Knowledge Base article 19285.

Resolved issues

These issues are resolved in this release of the product. For a list of issues fixed in a previous release, see the Release Notes for the specific release.

Description	Issue number
If the name of an NGFW element includes only numbers, the name might not be shown correctly in all views.	SMC-28359
If the Log Server is restarted while a scheduled task is running, the task stops progressing and prevents other scheduled tasks from running. The issue does not occur if the Log Server is stopped for a while before it is started again.	SMC-28910
If the Log Server's archive directory contains a large number of files, upgrading the Log Server might be slow.	SMC-29186
The appliance diagram does not show interface status for NGFW appliances that have an integrated switch.	SMC-32495
During the renewal of the SMC's internal certificate authority, the previous CA is in the "Active" state at the same time as the new CA is in the "Ready to Use" state. If a new NGFW Engine attempts to make initial contact while the CA renewal is in progress and the Management Server has already been certified using the new CA, initial contact might fail.	SMC-32809
Validation of the authentication key for NTP Server elements enforces a maximum key length for each key type and does not allow you to enter the key in ASCII. The value of the Key field is also shown by default while the key is being entered. After the changes, the maximum lengths for the authentication key are 32 hexadecimal characters for MD5, 40 hexadecimal characters for SHA-1, and 64 hexadecimal characters for SHA-2. If ASCII characters are used, the maximum length is 20 characters for all key types.	SMC-33006
Customized heap size values for Log Server, Web Portal, and Management Clients are not preserved when you upgrade to SMC version 6.8.3. You must modify your configuration if you previously changed the Java heap size of the Management Client using the MAX_HEAP_SIZE parameter in the sgClient.sh or sgClient.bat file.	SMC-33340
If you use a scheduled task to refresh the policy on Master NGFW Engines and Virtual NGFW Engines, the policy might not be refreshed on the Virtual NGFW Engines even though the task history shows that the task is finished.	SMC-33341
When there are multiple administrative Domains, the default LDAP domain setting in the Shared Domain overrides the default LDAP domain setting in individual administrative Domains.	SMC-33381
You cannot use an Alias element as the translation value of another Alias element that is used as the source of a dynamic NAT rule.	SMC-33452
When using the SMC API, if a sequence to GET a cluster is updated to use PUT, NGFW Engine tester definitions are removed.	SMC-33661
When you select a Virtual NGFW Engine as the sender, some sections in VPN Overviews do not show any data.	SMC-33863
If the antispoofing configuration includes an element that refers to itself, the following error message is shown when you try to view the policy snapshot for the NGFW Engine: "The creation of the storable antispoofing element for the interface with a dynamic IP address failed".	SMC-33870
When you use the SMC API to replace a router that has a dynamic IP address with a Dynamic NetLink element in the routing configuration for an interface that has a dynamic IP address, routes through both the router and the NetLink appear in the Routing view.	SMC-33895

Description	Issue number
When user authentication is enabled in an Access rule, policy validation incorrectly gives a warning.	SMC-33964

Installation instructions

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

For detailed information, see the *Forcepoint Next Generation Firewall Installation Guide*. All guides are available for download at https://support.forcepoint.com/Documentation.

> **Note**
>
> The sgadmin user is reserved for SMC use on Linux, so it must not exist before the SMC is installed for the first time.

> **Note**
>
> If you install the SMC on Windows and Windows Defender is enabled, it might take a long time to activate a dynamic update package. For more information, see Knowledge Base article 14055.

Steps

1) Install the Management Server, the Log Servers, and optionally the Web Portal Servers.

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

3) Configure the Firewall, IPS, or Layer 2 Firewall elements in the Management Client from the **Configuration** view.

4) To generate initial configurations, right-click each NGFW Engine, then select **Configuration** > **Save Initial Configuration**.
   Make a note of the one-time password.

5) Make the initial connection from the NGFW Engines to the Management Server, then enter the one-time password.

6) Create and upload a policy on the NGFW Engines in the Management Client.

Upgrade instructions

Take the following into consideration before upgrading the SMC.

> **Note**
>
> The SMC (Management Server, Log Server, and Web Portal Server) must be upgraded before the NGFW Engines are upgraded to the same major version.

- SMC 6.8 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 Management Client before upgrading the software.
- To upgrade a lower version of the SMC to 6.8, 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:
  - 5.6.2 – 6.4.10
  - 6.5.0 – 6.5.18
  - 6.6.0 – 6.6.5
  - 6.7.0 – 6.7.5
  - 6.8.0– 6.8.3

  Versions lower than 5.6.2 require an upgrade to one of these versions before upgrading to 6.8.4.
- Before upgrading, make sure that you have removed all elements related to McAfee Endpoint Intelligence Agent (McAfee EIA). Also remove all references in Access rules.

> **Note**
>
> In SMC version 6.8.3 and higher, the default path to the installation of xvfb-run for SMC Web Access is set to /usr/bin, and you cannot change the path using the Management Client.

If you use SMC Web Access on a Management Server or Web Portal Server installed on a Linux platform and need to change the path to the installation of xvfb-run, follow these steps:

1) On the Management Server or the Web Portal Server, edit the `SGConfiguration.txt` or `WebPortalConfiguration.txt` file.

2) Add the following parameter:

```
XVFB_RUN_DEFAULT_PATH=<path>
```

Replace `<path>` with the path to the installation of xvfb-run.

> **Note**
>
> If you use the SMC-Python library for interacting with the SMC API, you must upgrade the SMC-Python library to version 0.7.0b27 when you upgrade to SMC 6.8.4. To upgrade the SMC-Python library, see https://github.com/Forcepoint/fp-NGFW-SMC-python.

Known issues

For a list of known issues in this product release, see Knowledge Base article 18381.

Find product documentation

On the Forcepoint support website, 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 on the Forcepoint support website 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 support website. If you do not yet have credentials, create a customer account. See https://support.forcepoint.com/CreateAccount.

Product documentation

Every Forcepoint product has a comprehensive set of documentation.

- *Forcepoint Next Generation Firewall Product Guide*
- Forcepoint Next Generation Firewall 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 Next Generation Firewall Installation Guide*

Other available documents include:
- *Forcepoint Next Generation Firewall Hardware Guide* for your model
- *Forcepoint NGFW Security Management Center Appliance Hardware Guide*
- *Forcepoint Next Generation Firewall Quick Start Guide*
- *Forcepoint NGFW Security Management Center Appliance Quick Start Guide*
- *Forcepoint NGFW SMC API Reference Guide*
- *Forcepoint VPN Client User Guide* for Windows or Mac
- *Forcepoint VPN Client Product Guide*