

NGFW Security Management Center

6.10.18

Release Notes

Revision A

Contents

- About this release on page 2
- System requirements on page 2
- Build number and checksums on page 3
- Compatibility on page 4
- New features on page 5
- Enhancements on page 5
- Resolved and known issues 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 NGFW Security Management Center (SMC). 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.

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: 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 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 33316.
Management Client peripherals	■ A mouse or pointing device ■ SVGA (1024x768) display 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 7, 8, and 9 ■ SUSE Linux Enterprise 12 and 15 ■ Ubuntu 18.04 LTS and 20.04 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 6.10.18 is 11207. This release contains Dynamic Update package 1885.

Use checksums to make sure that files downloaded correctly.

- smc_6.10.18_11207.zip

```
SHA256SUM:
aaf60e07474cd806fbd8734701a72da41dabd461ae619d7d47214123a0dca713

SHA512SUM:
f4f17cf3bd5702f878e56e041df66157
4479eccae91e0185769e586a9173a601
d4faa704841e244cd962a23b02630fc1
c62f474d2bf180314a0f90d2c026c58f
```

- smc_6.10.18_11207_linux.zip

```
SHA256SUM:
9e2bdacbc6625c5e5f4a9122cf3dae70e0005ce6cd37de3cc0a6012bafb572c9

SHA512SUM:
2e2fc653ab9ddb37d731d75c3f93c244
1ea78134cc1705cfe62ad14c4bce052a
47850cea703e655f9bed8f2a3473b1e6
4499718c23d95b0860c18a2f28ef0a5e
```

- smc_6.10.18_11207_windows.zip

```
SHA256SUM:
07e9bcfeb1e5fd386a2c225a33e6d730a56a693278c5b1c8ab8f66a797a97d17

SHA512SUM:
3bacb7619126052e3352d0e81c4b7f2e
6a6c37ae8ea95c88b83d5429f3758a7c
783515091b3412f7bd640aa69fe80ee3
cd5f63d58a12fa22256a3e6f701da564
```

Compatibility

SMC 6.10 can manage all compatible Forcepoint NGFW Engine versions up to and including version 6.10.

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 6.10 is compatible with the following component versions.

- Forcepoint Next Generation Firewall (Forcepoint NGFW) 6.3 or higher
- McAfee Enterprise Security Manager (McAfee ESM) 11.1.x or higher

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*.

Snort inspection on NGFW Engines

The Snort network intrusion detection system and intrusion prevention system has been integrated into Forcepoint NGFW. You can import externally created Snort configurations into Forcepoint NGFW to use Snort rules for inspection.

You can configure Snort inspection globally for all NGFW Engines, or for individual NGFW Engines. You can use both NGFW deep inspection and Snort inspection for the same traffic, or you can use only NGFW deep inspection or only Snort inspection.

Enhancements

This release of the product includes these enhancements.

Enhancements in SMC version 6.10.8

Enhancement	Description
Visualization and filter elements edition support in SMC API	Filter elements can now be edited using SMC API. For more information, see Knowledge Base article 41241
Self check and automatic repair of SMC HA	To secure the data replication between Management servers, a functionality has been introduced to detect the failure and to enable an automatic full replication. For more information, see Knowledge Base article 40988 .
A new option is introduced in Export Elements tool	Export elements tool in Management Client has a new option, **Include references**. By default this option is selected; however, when unselected export is done without referenced elements.
A new Logon option has been introduced in **Global System Properties** dialog box	A new Logon option, **Administrator User Name is Case Insensitive** has been introduced in **Global System Properties** dialog box. When this option is enabled, SMC considers administrator user account names of type “Linked to LDAP” as lowercase, regardless of how they are stored in the LDAP server.
New option to force engine upgrade through SMC API	Remote upgrade through SMC API might be blocked with a warning, thereby preventing an upgrade. In such scenarios, a `force_upgrade` option is added for SMC API to perform an upgrade. For example, upgrade from NGFW version 6.3.3 to 6.8.8 using API.

Enhancements in SMC version 6.10.7

Enhancement	Description
Policy install without policy snapshot	With new Management Client, you can select options to not create policy snapshot during policy install. This is done by adding `POLICY_SNAPSHOT_CONFIGURATION=true` in the `SGClientConfiguration.txt`. The location of the file depends on the installation type of Management Client. For locally installed Management Client and standalone Management Client: ■ Edit the `<user_home>/.stonegate/SGClientConfiguration.txt` file on the client computer. ■ Edit the `<smc_installation_folder>/data/SGClientConfiguration.txt` file on the Management Server.

Enhancements in SMC version 6.10.3

Enhancement	Description
Rule hit counters for sub-policies	You can run a rule counter analysis for a sub-policy regardless of which main policy refers to it or which NGFW Engine the policy is installed on.

Enhancements in SMC version 6.10.0

Enhancement	Description
Exact values in exported reports	You can now use exact values instead of rounded values when you export reports as tab-delimited text files. To use exact values in reports, set the value of the TXT_REPORT_RAW_VALUES parameter to true. For reports exported using the Management Client, set the parameter in the SGClientConfiguration.txt file. For reports exported on the Management Server, set the parameter in the SGConfiguration.txt file.
Improved SD-WAN monitoring	The performance of SD-WAN monitoring has been improved. New options for SD-WAN monitoring have also been introduced. ■ The performance of SD-WAN monitoring in the Home view has been improved. ■ The performance of branch connectivity monitoring has been improved. ■ Branch connectivity diagrams have been enhanced. The diagram now includes shortcuts that zoom in on specific world regions on the map. ■ The Tunnels pane of branch home pages and VPN home pages can now show the status of either individual tunnels between endpoints or an aggregate status of all tunnels between gateway pairs. Previously, the Tunnels pane only showed the status of individual tunnels between endpoints. ■ A new VPN gateways pane that summarizes the status of the Gateways in the VPN has been added to the VPN home pages. The previous VPN gateway diagram pane is still available but it is not shown by default.

Enhancement	Description
OWASP encoding in SMC API responses	There is a new option in the SMC installer to enable OWASP encoding for the SMC API. When the option is enabled, the SMC API uses the OWASP encoder in responses. Using the OWASP encoder reduces the risk of cross site scripting (XSS) attacks. This option is especially useful if you use the SMC API to generate HTML pages that are shown in a browser.  **Note** When you enable this option, some strings in data returned by the SMC API, such as special characters inside JSON payloads, are also encoded. We recommend enabling this option only if you use the SMC API in a web browser.
SHA-256 support for NTP servers	You can now configure NTP Server elements to use SHA-256 authentication keys.
Warning about timeout when importing elements	On the progress tab for importing elements, a warning message is now shown when the default timeout for resolving conflicts between elements in the import file and existing elements is about to be reached. By default, the timeout is 15 minutes. You can optionally change the timeout using the CONFLICT_RESOLVING_OPERATION_TIMEOUT_MINUTES=<number of minutes> parameter in the SGConfiguration.txt in the SGHOME/data directory on the Management Server.

Resolved and known issues

For a list of resolved and known issues in this product release, see Knowledge Base article 38461.

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/s/article/Documentation-Featured-Article.

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 6.10 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 6.10, 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:
  - 6.3.0 - 6.4.10
  - 6.5.0 - 6.5.18
  - 6.6.0 - 6.6.5
  - 6.7.0 - 6.7.5
  - 6.8.0 – 6.8.15 (LTS release version)
  - 6.9.0 – 6.9.3
  - 6.10.0 – 6.10.17 (LTS release version)

  Versions lower than 6.3.0 require an upgrade to one of these versions before upgrading to 6.10.18.
- 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.

Upgrade notes

- SMC version 6.9 was the last version of the SMC that was compatible with McAfee ePO. Features that depend on McAfee ePO, such as McAfee Threat Intelligence Exchange (TIE) local file reputation sandbox and McAfee® Data Exchange Layer (DXL) local file reputation, are no longer available in SMC 6.10 and higher.
- In SMC version 6.9.0 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, edit SGConfiguration.txt or WebPortalConfiguration.txt and add the following parameter:

  ```
  XVFB_RUN_DEFAULT_PATH=<path>
  ```

  Replace `<path>` with the path to the installation of xvfb-run.
- SMC version 6.10.2 and higher no longer supports TLS 1.0 and TLS 1.1 by default. To use TLS 1.0 and TLS 1.1 for communication with external services, you must manually enable support for these TLS versions. For more information, see Knowledge Base article 38624.

  Note

  For security reasons, we recommend that you upgrade your external services to use TLS versions higher than 1.1 as soon as possible. Enabling support for TLS 1.0 and TLS 1.1 is intended as a temporary workaround until all external components are upgraded so that the existing environment is not disrupted.

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 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 User Guide*
- *Forcepoint VPN Client User Guide* for Windows or Mac
- *Forcepoint VPN Client Product Guide*
- *Forcepoint NGFW Manager and VPN Broker Product Guide*

© 2025 Forcepoint
Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint.
All other trademarks used in this document are the property of their respective owners.
Published 12 June 2025