Forcepoint

NGFW Security Management Center

6.11.1

Release Notes

Revision A

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.

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 (1280x768) 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
- Red Hat Enterprise Linux 7 and 8 - 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 6.11.1 is 11219. This release contains Dynamic Update package 1467.

Use checksums to make sure that files downloaded correctly.

- smc_6.11.1_11219.zip

  ```
  SHA1SUM:
  e66ca6c7c34ac4c9a732e872bd34145b6f1aa641

  SHA256SUM:
  5cb5692dac009ded1c94730ce11485051b2d6db8e7522acff9def784a8ecaf73

  SHA512SUM:
  b0378e2bfe8db34da06d1389d3e638fa
  ad206042df780f03cb424ab74e7f4882
  865951789d610a389daffa08580a1348
  e5b44d5cd18b897082f705de92db8858
  ```

- smc_6.11.1_11219_linux.zip

  ```
  SHA1SUM:
  ecc3a9b8650cadba0877f9bf373cbbbca35a775c

  SHA256SUM:
  0e757990bd08582a7d09f939d5117de9bc2cdbfd5d50170c245686b9018f8bf1

  SHA512SUM:
  d26f91047c043a9ce22c9f7c8e8466a5
  08021ed4166642d4651fb3c86e65a364
  57ebff2ace56586b34242459105a8429
  bec8e9133cd11ee26fb11a060156d281
  ```

- smc_6.11.1_11219_windows.zip

  ```
  SHA1SUM:
  a74ff161c64a9c86e7729fa3934e15ed3a0723e1

  SHA256SUM:
  9a92c46a2db63de7e00430bb6a5f59ec6b8f3adcd447bef787f987a334e024f0

  SHA512SUM:
  819a9f1328952f526d3a77e1f580ca6f
  4d0cb259b856eceed4048e1fd8f28c7a
  0330e4d0213ea055a1df01d3cd48e0db
  a3083f751d6ade3b5a724402f4775578
  ```

Compatibility

SMC 6.11 can manage all compatible Forcepoint NGFW Engine versions up to and including version 6.11.

⚠ **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 6.11 is compatible with the following component versions.

- Forcepoint Next Generation Firewall (Forcepoint NGFW) 6.4 or higher
- McAfee Enterprise Security Manager (McAfee ESM) 11.1.x or higher

Note

SA-per-host switch in the IPsec VPN configuration is deprecated and will not be available from the GUI for new configurations by default in 6.11 and later versions of SMC. This option is not needed for standard VPN use cases, but can be re-enabled via a parameter in the `SGConfiguration.txt` if required for troubleshooting or testing purposes.

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*.

External CA issued certificates in internal management communication

When you install a new SMC, you can now use certificates issued by an external CA instead of certificates generated by the internal CA on the Management Server for internal TLS communication between NGFW Engines and SMC components.

Run-time selection of FIPS module

In the NGFW Configuration Wizard, you can now select which FIPS module is used when the NGFW Engine is in FIPS-compatible operating mode. You can select whether to use the FIPS 140-2 module or the updated FIPS 140-3 module.

Move Quagga to Free Range Routing (FRR)

The dynamic routing features in the NGFW Engine that previously used the Quagga dynamic routing suite now uses the Free Range Routing (FRR) dynamic routing suite. The Free Range Routing (FRR) is a general purpose routing stack applicable to a wide variety of use cases including connecting hosts, virtual machines, and containers to the network, advertising network services, LAN switching and routing, internet access routers, and Internet peering.

Support for TLS 1.3

In addition to the previously supported TLS versions, the NGFW Engine now supports TLS inspection for TLS version 1.3 without downgrading the inspected connections to TLS version 1.2.

IPv6 - IPv4 Translation Support

The NGFW Engine now has basic support for IPv6 transition mechanisms. IPv6 transition mechanisms enable limited communication between devices that have only IPv6 addresses and devices that have only IPv4 address. Supported translations modes are NAT64, 464XLAT, and SIIT EAM.

Upcoming events notification

The upcoming events feature informs users about events that are going to happen soon, such as expiration of licenses and certificates, and failures of scheduled tasks, that require administrator action.

Support TLS server certificate verification before decryption decision

The NGFW Engine now fetches TLS server certificate for verification from destination TLS server with separate probe connection so that it can make a more accurate decision about whether to decrypt TLS connection before the original client to server connection is established.

Status history reporting

The status history provides historical data for monitoring and reporting on NGFW Engines, Netlinks, and SD-WAN branch or tunnel statuses over time. New status history views help to visualize past changes in the system status and the traffic, connection volumes, and ISP link quality over time. Status monitoring enhancements improve the existing monitoring of SD-WAN branches and VPN tunnels as well as NGFW Engine and Netlink performance history.

Local alternative policies

A local alternative policy can now be defined that can be uploaded but not activated on the NGFW Engine during policy installation. If connectivity between the NGFW Engine and the Management Server is lost, any policy can be selected whether it is a normal policy or one of the local alternative policies.

Deep inspection throughput improved

NGFW detaches deep inspection when it is not needed to improve throughput performance and appliance capacity. This can improve performance for example with encrypted traffic that is not decrypted (e.g. QUIC, SSH, TLS), application identification when further inspection is not needed, and with big file or UDP data steams where NGFW deep inspection is not providing added value.

Enhancements

This release of the product includes these enhancements.

Enhancements in SMC version 6.11

Enhancement	Description
Performance improvements for large environments	Several performance improvements for policy upload, move to domain, and background validation operations are done for large environments with multiple firewalls.
Better feature coverage via common properties dialog	There is now better coverage of the features and options, as well as possibility to override existing values using this dialog.
Option to disable sending active alerts	It is now possible to disable forwarding active alerts from Log Server to the Management Server (and standby servers in the SMC high availability setup). To disable sending active alerts on the SMC Log Server add the following line to the `<installation folder>/data/LogServerConfiguration.txt file`: `IGNORE_ACTIVE_ALERT_SENDING=true`
Explicit log out message	To meet SRG-APP-000297-NDM-000281, SRG-APP-000297AU-000570, and APSC-DV-000100 requirements, the SMC user interface should present explicit log out confirmation dialog to confirm the session closure before the user interface closes fully.
SMC backup with scheduled task with custom path	It is now possible to use the UI, SMC_API, and CLI to: ▪ define a custom path for saving the backup (path for CLI or `server_target_path` for SMC API) ▪ define a custom script to be executed at the end of a backup task (script for CLI or `script_to_execute` for SMC API) The custom script must be present in the `SG_HOME/data/script` path. If error is detected during the execution of the script, an error file will be populated with the root cause of the failure, otherwise the script result file will be populated with the status OK in the location where the script is run.
Elasticsearch Kibana reporting	SMC version 6.11 adds new fields to the Elasticsearch (ES) cluster integration which offers better support to 3rd party log visualization tools like Kibana with the NGFW log data. Kibana provides log data visualization in the web browser and can combine data from multiple sources. This release also supports the Elastic Common Schema (ECS) for log data. For more information, see https://www.elastic.co/kibana, https://www.elastic.co/guide/en/ecs/current, and https://www.opensearch.org.

Note

The SMC integrated incident management feature will be discontinued along with the release of the next major version. SMC version 6.11.0 will be the last version that can be used with the existing incident records remaining on the SMC server before upgrade.

Enhancements in SMC version 6.11.1

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. For Web Access: - Edit the `<smc_installation_folder>/data/SGClientConfiguration.txt` file on the Management Server.
TLS credentials support several intermediate certificates	You can import CA bundle as TLS credentials intermediate certificate.

Resolved and known issues

For a list of resolved and known issues in this product release, see Knowledge Base article 39146.

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.

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 6.11 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 6.11, 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 – 6.8.12
  - 6.9.0 – 6.9.3
  - 6.10.0 – 6.10.7
  - 6.11.0
- 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

- All documentation for SMC for 6.11 and later versions will have the terms black list and white list deprecated.

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

Published 19 May 2022