



NGFW Security Management Center

6.5.17

Release Notes

Contents

- [About this release](#) on page 2
- [System requirements](#) on page 2
- [Build number and checksums](#) on page 4
- [Compatibility](#) on page 5
- [New features](#) on page 5
- [Enhancements](#) on page 6
- [Resolved issues](#) on page 8
- [Installation instructions](#) on page 9
- [Upgrade instructions](#) on page 10
- [Known issues](#) on page 11
- [Find product documentation](#) on page 11

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
Management Client peripherals	<ul style="list-style-type: none">■ A mouse or pointing device■ SVGA (1024x768) display or higher
Disk space	<ul style="list-style-type: none">■ Management Server: 6 GB■ Log Server: 50 GB

Component	Requirement
Memory	<ul style="list-style-type: none"> Management Server, Log Server, Web Portal Server: 6 GB RAM If all SMC servers are on the same computer: 16 GB RAM Management Client: 2 GB RAM <p>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.</p> <p>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.</p>

**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
<ul style="list-style-type: none"> CentOS 6 and 7 Red Hat Enterprise Linux 6 and 7 SUSE Linux Enterprise 11 SP3 and 12 SP1 Ubuntu 14.04 LTS and 16.04 LTS 	<p>Standard, Datacenter, and Essentials editions of the following Windows Server versions:</p> <ul style="list-style-type: none"> Windows Server 2016 Windows Server 2012 <p>On Windows 10, you can install the SMC in demo mode. You can also install the Management Client.</p>

We recommend that you only use operating system versions that are currently supported by the vendor.

**Note**

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.

Web Start client

The Web Start distribution of the Management Client requires that a 64-bit Java Runtime Environment (JRE) is installed on the operating system.

Web Start is certified to run only on the listed official operating systems. However, it can also run on other operating systems that have JRE installed, for example, on macOS 10.9 or higher and additional Linux distributions. JRE 1.8.0_121 or a later critical patch update (CPU) release is required.

Build number and checksums

The build number for SMC 6.5.17 is 10689. This release contains Dynamic Update package 1270.

Use checksums to make sure that files downloaded correctly.

■ smc_6.5.17_10689.zip

```
SHA1SUM:
18699619a340b4e08b65d091972f0f429881765a

SHA256SUM:
9e99ec63b8e23957d4e9f1b7b4ff1634b481a3d6b689fee402e2925a73d0567d

SHA512SUM:
17ea2c2a373e89e9ba63dfb4061a5709
535c3484a3872182c1043324a6fed103
4fd33584ec605d387762d4e39c836a1c
a4a809d1152b73c9fdb434f2de28f27b
```

■ smc_6.5.17_10689_linux.zip

```
SHA1SUM:
0f20b8b4c03f8dc41bacabc6975dfb9d31fe2363

SHA256SUM:
50ca6883da5bf143ec0aac9c02ab559a1f84563a94dc072b39cab939ff1a8a68

SHA512SUM:
6238b55e0e8e78a726da0800b25e705a
b6bfc1e28ac53406684ddd401ea15dbf
668b70dc28270f2421c403613c876ba1
f6666135364e78eadc68d18331f0abf0
```

■ smc_6.5.17_10689_windows.zip

```
SHA1SUM:
6e0adb598a531c587cccb50a982facbccd8cf0a5

SHA256SUM:
fc3aed113fd126b487ae3c497cfcf17c3fb5f2dfb6d347394df5e3fb1c72a824

SHA512SUM:
91e4993739a4742fad08829a5f15de1a
d20dc87bf5c2b08501861261b7313a17
737c2542aa81532c509df96daff4a620
76ac6a4ecd6c4790d74f54af73a84157
```

■ smc_6.5.17_10689_webstart.zip

```
SHA1SUM:
bd6525d745fcd5449ea4b6fac08623cca2d59cd0

SHA256SUM:
4e0397b13b10d3e9e83699058d4f6376a440c1990e80f072d38f8eb883e92995

SHA512SUM:
10965ad9f689257f803e16875403ce2c
e402f3031469024027d49a9bd141b1c2
0c0bd4f5fbed0b46a708195d8e08418
2e8ae89d430f8d9877c8d0d09f5d3828
```

Compatibility

SMC 6.5 can manage all compatible Forcepoint NGFW Engine versions up to and including version 6.5.



Important

Some versions of Forcepoint NGFW have reached end-of-life status. Maintenance releases that contain security updates are no longer provided for Forcepoint NGFW versions that have reached end-of-life status. Even though these Forcepoint NGFW versions are 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 6.5 is compatible with the following component versions.

- Forcepoint™ Next Generation Firewall (Forcepoint NGFW) 6.2 or higher
- Stonesoft® Next Generation Firewall by Forcepoint (Stonesoft NGFW) 6.0 and 6.1
- McAfee® Next Generation Firewall (McAfee NGFW) 5.7, 5.8, 5.9, and 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*.

SD-WAN dashboard

The SD-WAN dashboard makes the software-defined wide area network (SD-WAN) features that are already part of Forcepoint NGFW more visible. The SD-WAN dashboard allows you to monitor SD-WAN features, such as outbound Multi-Link and Multi-Link VPNs, and to view statistics and reports related to SD-WAN features.

Application routing

You can now apply different NAT rules to traffic, select which VPN traffic uses, and redirect traffic to different proxy servers depending on the network applications detected in the traffic.

Route metrics, ECMP, and route monitoring

You can now define multiple static routes to the same destination and apply metrics to the routes. The routes with a lower metric value can be used as backup routes. When you enable the equal-cost multi-path (ECMP) feature on the routes, there is a potential increase in bandwidth as traffic is balanced between the routes. In addition, you

can use probes to monitor the status of a route. If a route is unavailable, the route is removed from the routing table and traffic is automatically sent over another route.

Enhancements

This release of the product includes these enhancements.


Enhancements in SMC version 6.5.0

Enhancement	Description
Integrated User ID Service on NGFW Engines	You can now use the Integrated User ID Service on the NGFW Engines to provide transparent user identification for access control by user. The Integrated User ID Service is primarily meant for demonstration purposes and proof-of-concept testing of user identification services.
LDAP authentication for administrators	You can now authenticate administrators using simple password authentication against integrated external LDAP databases.
VPN tunnels can remain established	You can now set specific VPN tunnels to always remain established even when no traffic is sent through the VPN tunnel.
Improved sorting options in the Home view	You can now organize Active Alerts by Severity and Type, and organize User Behavior Events by Activity, User, User Alert Check Type, User Alert, and Severity.
IPv6 support for DHCP relay	You can now use DHCP relay on interfaces that have IPv6 addresses.
Node-initiated contact to Management Server for clustered NGFW Engines	Firewall Clusters and Master NGFW Engines in the Firewall/VPN role now support node-initiated contact to the Management Server. The clustered NGFW Engine opens a connection to the Management Server and maintains connectivity.
More precise controls for endpoint use	You can now define which VPN endpoints can communicate with each other, and how the endpoints are used in a Multi-Link configuration.
Dynamic routing with active-active clustering	You can now use dynamic routing in Firewall Clusters that use load-balancing mode. In load-balancing mode, all nodes in the cluster are online at the same time and traffic is balanced between the nodes, increasing performance for inspection and VPN traffic.
Support for ECA Evaluation deployment	It is now easier to deploy the Endpoint Context Agent to a limited set of users for evaluation. The ECA client and all necessary certificates can be downloaded from the ECA Evaluation web application and installed on endpoints. For details, see Knowledge Base article 16193 .
Dynamic elements specific to cloud platforms	You can use a specific naming scheme with Domain Name elements in Access rules to run a script on the NGFW Engine that resolves dynamic element names specific to a cloud platform to IP addresses. The IP addresses are resolved through API calls rather than regular network DNS queries. For more information, see Knowledge Base article 16290 .

Enhancements in SMC version 6.5.1

Enhancement	Description
TLS Profile for connecting to Forcepoint servers	The Management Server now uses a custom TLS Profile element for automatically downloading license updates, dynamic updates, and NGFW Engine upgrades from Forcepoint servers. The TLS Profile element defines the settings for cryptography, trusted certificate authorities, and the TLS version used in TLS-protected traffic.

Enhancements in SMC version 6.5.2

Enhancement	Description
New URLs for dynamic updates and engine upgrades	<p>To improve the performance of automatic dynamic updates and engine upgrades, the following new URLs are available in SMC 6.5.2 and higher:</p> <ul style="list-style-type: none"> ■ https://autoupdate.ngfw.forcepoint.com/dynup.rss ■ https://autoupdate.ngfw.forcepoint.com/ngfw.rss <div>  <p>Note</p> <p>The SMC automatically starts using the new URLs when you upgrade to SMC 6.5.2 or higher and activate the dynamic update package that includes the new URLs.</p> </div> <p>The new URLs use a content distribution network (CDN) to allow the SMC to download dynamic update packages and engine upgrade files from the geographically closest server. The legacy https://update-pool.stonesoft.com/index.rss URL remains available for backward compatibility and as a backup for the new URLs.</p>
Configurable update services for dynamic updates and engine upgrades	<p>New Update Service elements define sets of URLs for automatic dynamic updates and engine upgrades. In SMC 6.5.2 and higher, the SMC automatically uses Update Service elements that include both the new URLs and the legacy URL. No action is needed to start using the Update Service elements that include the new URLs.</p> <p>You can optionally change which Update Service element is used for automatic dynamic updates and engine upgrades. For more information, see Knowledge Base article 16589.</p>
Enhancements in the User Dashboard	<p>The following enhancements have been made in the User Dashboard:</p> <ul style="list-style-type: none"> ■ The user domain is now always shown for users in the User Dashboard. ■ To prevent information about them from cluttering the User Dashboard statistics, the System and Root users are no longer shown in the User Dashboard statistics. ■ The endpoint IP address is now always shown for users in the User Dashboard.
Alert Policy management in the SMC API	You can now manage Alert Policies using the SMC API.
Support for custom fields in CEF log format	You can now configure custom fields when you export or forward logs to an external service in CEF or LEEF formats.

Enhancements in SMC version 6.5.3

Enhancement	Description
Configurable wait time between inspected packets	To optimize latency and CPU utilization, you can now customize how long the inspection process waits for additional packets.

Enhancements in SMC version 6.5.6

Enhancement	Description
Export all elements except those in the Trash	When using the SMC API or the sgExport command on the command line, there is now the option to exclude elements that are in the Trash when exporting all elements.

Enhancements in SMC version 6.5.11

Enhancement	Description
New default settings for VPN profiles	The default values that are selected when you create a new VPN Profile element have been changed to better meet the needs of typical users.

Enhancements in SMC version 6.5.14

Enhancement	Description
Route monitoring in the SMC API	The SMC API now responds with an error code if a monitoring session cannot be opened when the client makes an HTTP request to retrieve routing monitoring information. For more information, see Knowledge Base article 18186 .

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
When Virtual NGFW Engines are used as external VPN gateways in a policy-based VPN, moving the Policy-Based VPN element to another administrative Domain also moves the Master NGFW Engine that hosts the Virtual NGFW Engines.	SMC-19761
In very rare cases, when you are editing an NGFW Engine element that has a large number of VPN Sites, if you save and install the policy while the view is refreshing, the VPN Sites are removed, which causes the policy installation to fail.	SMC-27108
When a NAT rule that forwards traffic to a proxy uses an application tag instead of a network application as the service, the NAT rule is ignored.	SMC-27216

Description	Issue number
When you use TLS to secure the connection to the external host, forwarding audit data from the Management Server fails.	SMC-27468
If a member of an LDAP group does not belong to the BaseDN, a full LDAP group search might fail and not show any other users or groups.	SMC-27716
When the policy includes element-based NAT, viewing policy snapshots might fail. The following message is shown: "DB Transaction failed while processing transaction".	SMC-27787
When you change the value of the VPN Type option to only "SSL VPN Tunnel" for a VPN endpoint that is used in a mobile VPN, policy installation fails.	SMC-28001
The -nodiskcheck option for the sgBackupMgtSrv command line script does not work as intended.	SMC-28169
The Management Server does not request automatic license updates and downloads even though the Management Server regularly queries the status of licenses from the Forcepoint license server.	SMC-28425
When a WebSocket connection to the SMC API is closed, the related session is not closed immediately.	SMC-28451
For external tests, the path to the script file on the command line has a limit of 80 characters.	SMC-28639
In rare cases, normal logs might be sent as alerts.	SMC-28748
The Control Management Servers dialog box always tries to connect to the active Management Server, even if it is unreachable.	SMC-29139
The details are not always refreshed when you select different NGFW Engine nodes in the Home view.	SMC-29380
Notifying a Master NGFW Engine of deleted Virtual NGFW Engines might fail. As a result, policy installation for the Master NGFW Engine fails and the following message is shown: "Master engine's virtual engine nic mapping is not valid".	SMC-29477
Policy installation for a Master NGFW Engine node might fail due to license checks.	SMC-29515
When the names of nodes include commas, the MSSP Report table is formatted incorrectly.	SMC-29638
If there are many policy snapshots, upgrading the Management Server might fail.	SMC-30769

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 6.5 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 Management Client before upgrading the software.
- To upgrade a lower version of the SMC to 6.5, 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.
- 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 – 6.5.16

Versions lower than 5.6.2 require an upgrade to one of these versions before upgrading to 6.5.17.

- Due to changes in application detection, policies that use Network Applications in the Access rules might work differently after upgrading to NGFW 6.4 or higher. Some traffic that was previously allowed might be discarded. In NGFW 6.5, there are changes related to how port information is used for matching applications.

Verify that your policies still work as expected. For more information, see Knowledge Base article [15411](#).

- The legacy Stonesoft User Agent is no longer supported. If you have used the Stonesoft User Agent, make sure that the feature has been completely removed from the SMC and that the element for the Stonesoft User Agent has been removed from the Trash before you upgrade to version 6.5. We recommend that you use the Forcepoint User ID Service instead.

Known issues

For a list of known issues in this product release, see Knowledge Base article [16274](#).

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*

