FORCEPOINT

NGFW Security Management Center

Release Notes

6.5.0

Revision B

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
Management Client peripherals	• A mouse or pointing device • SVGA (1024x768) display or higher
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 • 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.

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 6 • CentOS 7 • Red Hat Enterprise Linux 6 • Red Hat Enterprise Linux 7 • SUSE Linux Enterprise 11 SP3 • SUSE Linux Enterprise 12 SP1 • Ubuntu 14.04 LTS • Ubuntu 16.04 LTS	• Windows Server 2016 Standard and Datacenter editions • Windows Server 2012 R2 • Windows Server 2008 R1 SP2 and R2 SP1 • Windows 7 SP1 • Windows 10

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 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. For SMC 6.3 or higher, JRE 1.8.0_121 or a later critical patch update (CPU) release is required.

Build number and checksums

The build number for SMC 6.5.0 is 10627. This release contains Dynamic Update package 1104.

Use the checksums to make sure that the files downloaded correctly.

- smc_6.5.0_10627.zip

```
SHA1SUM:
7130f2b5a31dbf497603fe5c9c598603ca3cac9f

SHA256SUM:
9db66ae59a40055d551e62ddce893ad0ce6987fc86ffa6324375c438706480a8

SHA512SUM:
b458686114e1b472322dbd0cc8cf6f74
57299d4d721a55d02816471425a60b39
181a5821fa88cd96b8346af472a304cb
0e818b6ad366e46b93f123b8ff696bdd
```

- smc_6.5.0_10627_linux.zip

```
SHA1SUM:
02ca6a85aacc054edb7c277a735402fbc7ec10c0

SHA256SUM:
fe5a676d2b38b9315e748c6591fd07c24d0ed6392878b660d805d7e57753197c

SHA512SUM:
5c83299856a381a5752a64edf423ff5c
b58789d0f8396242537e0a65f454b70e
da996253921a588c31e70b04702659ba
fa9f947f3214e600fbc5e00264e9ca7e
```

- smc_6.5.0_10627_windows.zip

```
SHA1SUM:
c8938347930c88b2792c71e3e15c7ac7f11bd360

SHA256SUM:
92052c88d1650e986eae7a8f51f8037a3a60f9f0981b5478b993d54951874924

SHA512SUM:
bfc656cd6e4151059a1f696b0ee8a1b5
ca2a2465ded44c465a34e2b6e889631c
281baec48ce7e3fed83a3ed4dca25e4e
2a9ceb2acca91fcde17e2751db2b6b09
```

- smc_6.5.0_10627_webstart.zip

```
SHA1SUM:
14e63ebb53e19818b49e5bae6d39d53e0778e1d9

SHA256SUM:
b1ac93270bb7546ff8f7a402a7a5f8c7303ae0e6d13f19512a5441ba096d4713

SHA512SUM:
835a2bbbd5ab8badd6061fa92adfdc7f
8d69dbc1c8512eea7ebd48ecf05bac49
46ce5ca749292bf0b353e99d877c39d0
deada9710d03a0e962fd7c616c05e7df
```

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™) 5.0.1 and 5.1.1
- 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.

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 a Top Rate type of Report Section summary contains two Report Items, the PDF output might be unreadable because the Top Limit is applied on the Y-axis. The X-axis labels might become unreadable because of this layout problem. If the same information is presented in a table, there might be readability issues as well.	SMC-1193
An expression element that includes both IPv4 and IPv6 addresses might not work as expected.	SMC-3877
It is not possible to drag and drop a filter from the Logs view in one tab to the Logs view in another tab.	SMC-3968
When the Allow Pre-Shared Key Authentication with IKEv1 option is selected on the IPSec Client tab in a VPN Profile, policy installation fails if a mobile VPN that uses the profile has an SSL VPN tunnel enabled for the endpoint.	SMC-4917
When the same subnet is reachable through several routes, policy validation does not show a warning about the routing configuration.	SMC-10358
If you use an export banner to add customized text to the beginning of the XML file for element exports, and the end of the export banner contains special characters, the importing of the elements might fail.	SMC-11765
When you enable file filtering only in the Access rules of a sub-policy, file filtering is not enabled in the main policy.	SMC-12533
The certificate that the NGFW Engine uses to connect to McAfee Logon Collector (MLC) is not updated automatically even though the certificates in the SMC and MLC are updated.	SMC-12540
When editing a policy in an environment that has multiple administrative Domains, you might get an error if you use type-ahead search to add an element.	SMC-13140
When you validate a policy, the validation incorrectly marks rules as unreachable if the rule is in a sub-policy and has the Continue action.	SMC-13144
When a new VPN tunnel is successfully added to the configuration, the tunnel might not be shown in the Tunnels pane in the Home view until the Management Server is restarted.	SMC-13490
External SMC authentication using a Windows Network Policy Server (NPS) does not work if the Active Directory server and the NPS server are separate servers, and the Management Server must connect to the NPS using a different IP address.	SMC-13566
If you export an iOS VPN configuration profile, the exported configuration does not include the contact address of the VPN endpoint.	SMC-14304
An incorrect filter expression is created if the criteria includes a Group element.	SMC-15988
When selecting a mix of different NGFW Engine element types in the Home view, pending changes for all managed elements are shown.	SMC-16242

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 10 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.
- Upgrading is supported from SMC versions 5.6.2 – 6.3.8 and 6.4.0 – 6.4.5. Versions lower than 5.6.2 require an upgrade to one of these versions before upgrading to 6.5.0.
- 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, Knowledge Base articles, downloads, cases, and contact information.

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*
- *Stonesoft VPN Client User Guide* for Windows or Mac
- *Stonesoft VPN Client Product Guide*