FORCEPOINT

Stonesoft Management Center

Release Notes

6.0.4

Revision B

Table of contents

About this release

This document contains important information about the current release of Stonesoft® Management Center by Forcepoint (SMC; formerly known as McAfee® Security Management Center). We strongly recommend that you read the entire document.

Note: We have rebranded the SMC, the Stonesoft Next Generation Firewall (Stonesoft NGFW) product, and the Stonesoft NGFW product documentation. However, the old product name is still used in the NGFW appliances and documents included in the NGFW appliance delivery.

System requirements

Make sure that you meet these basic hardware and software requirements.

Basic management system hardware requirements

You can install SMC on standard hardware.

- Intel® Core™ family processor or higher recommended, or equivalent on a non-Intel platform
- A mouse or pointing device (for Management Client only)
- SVGA (1024x768) display or higher (for Management Client only)
- Disk space for Management Server: 6 GB
- Disk space for Log Server: 50 GB
- Memory requirements for 32-bit Linux operating systems:
  - 2 GB RAM for the Management Server, Log Server, or Web Portal Server (3 GB if all servers are installed on the same computer)
  - 1 GB RAM for Management Client
- Memory requirements for 64-bit operating systems:
  - 6 GB RAM for the Management Server, Log Server, or Web Portal Server (8 GB if all servers are installed on the same computer)
  - 2 GB RAM for Management Client

Operating systems

SMC supports the following operating systems and versions.

Note: Only U.S. English language versions have been tested, but other locales might also work.

Supported Microsoft Windows operating systems:

- Windows Server 2012 R2 (64-bit)
- Windows Server 2008 R1 SP2 and R2 SP1 (64-bit)
- Windows 7 SP1 (64-bit)

Supported Linux operating systems:

- CentOS 6 (for 32-bit and 64-bit x86)
- CentOS 7 (for 64-bit x86)

- Red Hat Enterprise Linux 6 (for 32-bit and 64-bit x86)
- SUSE Linux Enterprise 11 SP3 (for 32-bit and 64-bit x86)
- Ubuntu 12.04 LTS (for 64-bit x86)
- Ubuntu 14.04 LTS (for 64-bit x86)

Note: 32-bit compatibility libraries lib and libz are needed on all Linux platforms.

Web Start client

In addition to the operating systems listed, SMC can be accessed through Web Start by using Mac OS 10.9 and JRE 1.8.0_77 or a later critical patch update (CPU) release.

Build version

SMC 6.0.4 build version is 10138.

This release contains Dynamic Update package 841.

Product binary checksums

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

- smc_6.0.4_10138.zip

```
SHA1SUM:
39bee1e32eb16e745477222b5de7d8fefd036ad5

SHA256:
84e2af2fafb670f34e37d88921607df9b6c2e0778263655c0dd292469b238c70

SHA512SUM:
ad0f6e77f8d58c5e366e8e284ed7f226
2f546381079d1142583f9dbe73438290
cae597226cd7d6411686680a44bf6002
b65caa28ab26a70cd00854883814b3ef
```

- smc_6.0.4_10138_linux.zip

```
SHA1SUM:
0ccea9882598ae3372cdf9bf78f701a6144d63a7

SHA256:
7a69780dc20139c0b316ba309344c73396547f7a544c4ba50f42fc87a3e23506

SHA512SUM:
9b896f5871a4bfb60077ec08b305617e
15bee1fae4d74a5e86a16fd063c45ba2
d6e0eda545c235910eaf8149c8caf49b
633f9f820d9dedfeb380405ad4584d56
```

- smc_6.0.4_10138_windows.zip

```
SHA1SUM:
46401660462a87b604fe23c33aee93814f66599b

SHA256:
aea085a0a0c67596db024be41026c98d8e4a7347ce0a297da3e007ac038d1e41

SHA512SUM:
0f212fb186a78de73b88946cf7d8c93d
6cd9dd9a1fc4f330072330478ad95efe
267a829862f5c450448ca763a92d7b01
947fb2d6f9580d9b6bac4553674b1634
```

- smc_6.0.4_10138_webstart.zip

```
SHA1SUM:
6031a9334e03d02daf557c947af5459f9da12e20

SHA256:
b3edd0165b002dd20295ae357de7ad1bab06528b3e1675b78b4caa0147de1856

SHA512SUM:
d20c0851e65e2d36aa1159d53a636887
b51e88142fc640d7af5427e06d631303
c0c5918e40efd5e8f2ab62321532a741
f2b3bb007841b9cfad0a1acdbf9d95a7
```

Compatibility

SMC 6.0 has the following requirements for minimum compatibility and native support.

Note: SMC 6.0 can manage all compatible Stonesoft NGFW engine versions up to and including version 6.0.

Minimum component versions

SMC 6.0 is compatible with the following component versions.

- Stonesoft Next Generation Firewall (Stonesoft NGFW) 6.0.
- McAfee® Next Generation Firewall (McAfee NGFW) 5.7, 5.8, 5.9, and 5.10
- Stonesoft Security Engine 5.5
- McAfee® ePolicy Orchestrator® (McAfee ePO™) 5.0.1 and 5.1.1
- McAfee® Endpoint Intelligence Agent (McAfee EIA) 2.5
- McAfee® Enterprise Security Manager (McAfee ESM) 9.2.0 and later (9.1.0 CEF only)

For more information about the Stonesoft Next Generation Firewall lifecycle policy, see Knowledge Base article 10192.

Native support

To use all features of SMC 6.0, Stonesoft NGFW 6.0 is required.

New features

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

Rebranding

Stonesoft Next Generation Firewall (Stonesoft NGFW) and Stonesoft Management Center (SMC) are now part of Forcepoint. The look and feel of the Management Client, Web Portal, SSL VPN Portal, and the NGFW Authentication Portal have been updated to reflect the Forcepoint brand. The default template for PDF reports has also been updated.

New look and feel

The look and feel of the Management Client has been simplified and updated to reflect the Forcepoint brand. The most important changes include the following:

- The previous **System Status** view is now the **Home** view. The **Home** view shows you the status of the most important system components at a glance and allows you to browse the elements by type.
- All task-specific configuration views have been merged into a single **Configuration** view. Instead of opening in separate tabs, different parts of the **Configuration** view are grouped into branches.
- All menus have been grouped under the Menu button in the toolbar. The layout of the toolbar has also been updated.
- The updated **Save or Upload Initial Configuration** dialog helps you to select the most suitable way to save the initial configuration for engines.
- The **Info** pane has been moved to the right side of the window. The contents of the **Info** pane have been reorganized to make information easier to find.
- The new **Drill-downs** pane allows you to easily access element-specific views and tools.
- Icons, colors, and fonts have been updated.

Dynamic Routing for OSPFv2 in the Management Client

You can now configure OSPFv2 (Open Shortest Path First v2) dynamic routing using the Management Client.

Improved vulnerability reporting

To provide more useful information in the Management Client and in reports about situations that are related to vulnerabilities, the following information is now available in the properties of Vulnerability elements:

- Type and impact categories
- Printable name and description
- Hyperlinks to the referenced security advisories

Enhancements

This release of the product includes these enhancements.

Enhancements in SMC version 6.0.0

Enhancement	Description
Support for IPv6 in the Stonesoft VPN Client	You can now connect with the Stonesoft VPN Client client for Windows over an IPv6 network. Traffic inside the VPN tunnel still uses IPv4. IPv6 tunneling is already supported in site-to-site VPNs.
Improved logging for the SSL VPN Portal	The SSL VPN Portal can now create log entries the first time that an SSL VPN Portal Service is accessed in each user session, both when permission is granted and when permission is denied. Logs about related connections now include the rule tag from the matching rule in the Firewall Policy. Logs about unsuccessful authentication attempts now include the attempted user ID.
Obsolete features removed from the Management Client	The following features are obsolete and have been removed from the Management Client: • Legacy SSL VPN • Snort rule import • User limits for the Web Portal • Support for Stonesoft NGFW engine versions lower than 5.5
SSL VPN tunnel for firewalls that have a Firewall license	A mobile VPN to a firewall that has a Firewall license was earlier possible with IPsec only. With SMC 6.0, it is also possible to connect with the SSL protocol. This improves connectivity in certain network environments. When you upgrade the SMC, SSL VPN tunnel usage is enabled for firewalls that have a Firewall license. The VPN Clients and the firewalls that have a Firewall license do not need to be upgraded.  **Note:** This change does not affect the use of the SSL VPN Portal. You can only configure the SSL VPN Portal if you have a Security Engine license for the firewall, not if you have a Firewall license.

Enhancements in SMC version 6.0.1

Enhancement	Description
Log export improvements	The sgArchiveExport script that exports logs from archive now supports CEF, LEEF, and ESM formats in addition to CSV and XML. You can now schedule Export Log Tasks to run hourly using relative time ranges.

Enhancements in SMC version 6.0.2

Enhancement	Description
Improved BGP configuration	You can now preview or edit the Route Map in the BGP Peering element properties.

Resolved issues

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

Description	Issue number
Using a Domain Controller password that is longer than 82 characters in the Active Directory Server properties prevents the Management Server from being upgraded.	SMC-1189
When you use the Upgrade to Cluster tool, and you change the NDI and CVI addresses several times, saving the Firewall Cluster element might fail.	SMC-1231
When you change the IP address of an interface from an IPv4 address to an IPv6 address or from IPv6 address to IPv4 address, the antispoofing configuration is not updated correctly. Policy installation might fail. The following error message is shown: "Syntax error in network configuration: No IPv6 connected network available on interface X near line Y".	SMC-1249
When you modify a RADIUS or TACACS+ Authentication Server, you cannot remove Authentication Methods on the Authentication Methods tab of the RADIUS Authentication Server Properties or TACACS+ Authentication Server Properties dialog box.	SMC-1483
Third-party log reception stops when there are 10000 messages in the queue to process. Log reception does not automatically resume.	SMC-1593
If you use the SMC API to monitor routing, the SMC API might become unresponsive when an engine or a Log Server is unavailable.	SMC-2141
The connection from the Web Start Management Client to SMC version 6.0 might fail when you update your Java Runtime Environment (JRE) to version 8 update 111 or later. When you connect, the following message might be shown: "Application Blocked by Java Security." The Web Start Management Client opens, but some parts of the Management Client might not work correctly. For example, the Home view might be shown without the System Status tree.	SMC-2168
Non-Latin text in the Management Client is unreadable. For example, Cyrillic text and Japanese text are not displayed correctly.	SMC-2235
If you select multiple licenses in the All Licenses view and the selection includes divider rows that specify the license types, you cannot copy the license information for the selected licenses.	SMC-2421
In a high availability SMC environment, the active Management Server might become unresponsive or fail to start if standby Management Servers have been configured, but those additional Management Servers are no longer available.	SMC-3102

Installation instructions

Use these high-level steps to install SMC and the Stonesoft NGFW engines.

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

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

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 with the Management Client using the **Configuration** view.
4. To generate initial configurations for the engines, right-click each Firewall, IPS, or Layer 2 Firewall element, then select **Configuration** > **Save Initial Configuration**.

   Make a note of the one-time password.
5. Make the initial connection from the engines to the Management Server, then enter the one-time password.
6. Create and upload a policy on the engines using the Management Client.

Upgrade instructions

Take the following into consideration before upgrading to SMC 6.0.

Note: SMC (Management Server, Log Server, and Web Portal Server) must be upgraded before the engines are upgraded to the same major version.

- SMC 6.0 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 using the Management Client before upgrading the software.
- To upgrade an earlier version of the SMC to 6.0, we strongly recommend that you stop all Stonesoft NGFW services 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.
- Versions earlier than 5.6.2 require an upgrade to version 5.6.2–5.10 before upgrading to 6.0.

Note: You can upgrade only to an SMC version that is released after the current SMC maintenance version was released.

You can upgrade SMC 6.0.4 to the following:

- A later SMC 6.0 maintenance version
- SMC 6.1.2 or a later SMC 6.1 maintenance version

Known issues

For a list of known issues in this product release, see Knowledge Base article 10233.

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.

- *Stonesoft Next Generation Firewall Product Guide*
- Stonesoft 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.

- *Stonesoft Next Generation Firewall Installation Guide*

Other available documents include:

- *Stonesoft Next Generation Firewall Hardware Guide* for your model
- *Stonesoft Management Center Appliance Hardware Guide*
- *Stonesoft Next Generation Firewall Quick Start Guide*
- *Stonesoft SMC API Reference Guide*
- *Stonesoft VPN Client User Guide* for Windows or Mac
- *Stonesoft VPN Client Product Guide*

The following document included in appliance deliveries still uses the old product name and brand:

- *McAfee Security Management Center Appliance Quick Start Guide*