# Table of contents

1 **About this release** ................................................................................................................................. 3  
   System requirements ................................................................................................................................. 3  
   Build version............................................................................................................................................. 4  
   Compatibility............................................................................................................................................. 5  

2 **New features** ........................................................................................................................................ 6  

3 **Enhancements** ....................................................................................................................................... 7  

4 **Resolved issues** ...................................................................................................................................... 9  

5 **Installation instructions** ......................................................................................................................... 11  
   Upgrade instructions................................................................................................................................... 11  

6 **Known issues** ........................................................................................................................................ 12  

7 **Find product documentation** .................................................................................................................. 13  
   Product documentation............................................................................................................................... 13
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_74.

Build version

SMC 6.0.3 build version is 10137.
This release contains Dynamic Update package 812.

Product binary checksums

Use the checksums to make sure that the installation files downloaded correctly.
• smc_6.0.3_10137.zip

<table>
<thead>
<tr>
<th>SHA1SUM</th>
<th>SHA256SUM</th>
<th>SHA512SUM</th>
</tr>
</thead>
<tbody>
<tr>
<td>406115d0cefd0f400753023b6f2b04e5ce3bc92</td>
<td>4603bd3e2f3cbe0e7f7ca9c118b3d0c56d7d656ef948347f354398ad823abac2</td>
<td>9fc5334b89ee6e242e12c1f795ae99119f6d2b18f855f04e1b4149930c963a8f50946ae001a44475736b6557 debilitating</td>
</tr>
<tr>
<td>12e969704bbf45b52ded92b3c66ce9ffec3b20e38</td>
<td>da3ffb783db9d89ee6e242e12c1f795ae99119f6d2b18f855f04e1b4149930c963a8f50946ae001a44475736b6557 debilitating</td>
<td>9edf30205695da983e40fb1ec1c74cf543cd5b60fe2276c6e19491f3547cb56752af79d734f609c101a62987ba753ae6b6e2</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Enhancement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support for IPv6 in the Stonesoft VPN Client</td>
<td>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.</td>
</tr>
<tr>
<td>Improved logging for the SSL VPN Portal</td>
<td>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.</td>
</tr>
<tr>
<td>Obsolete features removed from the Management Client</td>
<td>The following features are obsolete and have been removed from the Management Client:</td>
</tr>
<tr>
<td></td>
<td>• Legacy SSL VPN</td>
</tr>
<tr>
<td></td>
<td>• Snort rule import</td>
</tr>
<tr>
<td></td>
<td>• User limits for the Web Portal</td>
</tr>
<tr>
<td></td>
<td>• Support for Stonesoft NGFW engine versions lower than 5.5</td>
</tr>
<tr>
<td>SSL VPN tunnel for firewalls that have a Firewall license</td>
<td>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.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Enhancement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log export improvements</td>
<td>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.</td>
</tr>
</tbody>
</table>
## Enhancements in SMC version 6.0.2

<table>
<thead>
<tr>
<th>Enhancement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Improved BGP configuration</td>
<td>You can now preview or edit the Route Map in the BGP Peering element properties.</td>
</tr>
</tbody>
</table>
## 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.

<table>
<thead>
<tr>
<th>Description</th>
<th>Issue number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retrieving routing information through the SMC API can work unreliably, especially with a large number of dynamic routes on Virtual Firewalls.</td>
<td>116761</td>
</tr>
<tr>
<td>Searching for IPv6 addresses does not return results when the search criteria includes letters.</td>
<td>126308</td>
</tr>
<tr>
<td>Changing the interface ID and creating a new interface with the same ID can result in an incorrect automatic routing configuration if all the interface configuration changes are not saved at the same time.</td>
<td>127250</td>
</tr>
<tr>
<td>Editing or previewing the route-based VPN is not possible after you have disabled endpoints that are referenced in the route-based VPN.</td>
<td>131049</td>
</tr>
<tr>
<td>Removing an IP Prefix List element from a Route Map can result in a database error when you save the Route Map. Editing the Route Map rule several times can cause only the last change to be saved.</td>
<td>134253</td>
</tr>
<tr>
<td>When a custom VPN Profile is used, snapshot comparison can fail with the error &quot;Database error. Details: Failed to read import exported: data.xml.&quot;</td>
<td>134280</td>
</tr>
<tr>
<td>When you move networks from one interface to another on Master Engines and then delete the original interface, comparing Policy Snapshots can fail and give a &quot;Database Error&quot; message.</td>
<td>134411</td>
</tr>
<tr>
<td>When there are hundreds of elements, selecting elements in the Home view can result in the Management Client running out of memory. A diagram is drawn for each element, which consumes memory.</td>
<td>134543</td>
</tr>
<tr>
<td>Links to the License Center do not point to the new Forcepoint location: <a href="https://stonesoftlicenses.forcepoint.com/managelicense.do">https://stonesoftlicenses.forcepoint.com/managelicense.do</a>.</td>
<td>134624</td>
</tr>
<tr>
<td>You cannot edit a Single Firewall element after it has been converted to a Firewall Cluster element if the Single Firewall had browser-based user authentication enabled when you gave the Upgrade to Cluster command.</td>
<td>134950</td>
</tr>
<tr>
<td>A Security Engine element exported in XML format might contain an invalid antispoofing parameter if the IP address of an interface has been changed from dynamic to static. This configuration prevents importing the exported Security Engine element into the SMC.</td>
<td>135184</td>
</tr>
<tr>
<td>You cannot view or restore a Policy Snapshot if it contains a Policy-Based VPN that forwards traffic between gateways.</td>
<td>135352</td>
</tr>
<tr>
<td>If the same matching criteria, for example a Host and a Zone, are used in several Access rules, deleting one of the rules or removing the matching criteria from one of the rules also removes it from other rules that have the same matching criteria defined. As the result, policy installation might fail with the error &quot;Element does not exist or is not accessible by the user. Failed to build specific configuration for &lt;element name&gt;.&quot;</td>
<td>135471</td>
</tr>
<tr>
<td>When you install a policy, a NAT rule can be ignored if an Alias element within an Alias element has been used as the translation value. The following type of message is shown: &quot;The IPv4 NAT rule @X.X is ignored: in the source translation, the definition for the translated address is empty&quot;.</td>
<td>SMC-559</td>
</tr>
<tr>
<td>After you have activated a dynamic update package, status cards for some appliances might not be shown correctly in the System Status view. Policy installation might also fail if the appliance has a wireless interface.</td>
<td>SMC-599</td>
</tr>
<tr>
<td>Description</td>
<td>Issue number</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Routing and antispooﬁng conﬁgurations are not updated when you add a new IPv4 address to an interface, save the changes to the interface, then update the netmask in the IPv4 address, and save the changes again. A Network element with the old netmask and another Network element with the new netmask are shown in the Routing and Antispooﬁng views.</td>
<td>SMC-893</td>
</tr>
<tr>
<td>You cannot disable or delete API Client elements.</td>
<td>SMC-1029</td>
</tr>
</tbody>
</table>
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 cannot upgrade SMC 6.0.3 to SMC 6.1.0.
For a list of known issues in this product release, see Knowledge Base article 10233.
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