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................................................................................................................................................8

5 Installation instructions................................................................................................................................10
   Upgrade instructions..................................................................................................................................10

6 Known issues......................................................................................................................................................11

7 Find product documentation..........................................................................................................................12
   Product documentation..............................................................................................................................12
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 6.0.1 build version is 10133.

This release contains Dynamic Update package 767.

Product binary checksums

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

- smc_6.0.1.10133.iso

  SHA1SUM: 5a4d04170de28edc1c78cc0066c60c702d329dca

  SHA256: f3b04799b4bd6b973b13f5a0829128c84685853f75446ec5d8b3f22f65d7b95

  SHA512SUM: aec08bf8559b5553d69f87f18433d0e8a003fd7307f68f6817f14e0302f92e95b4d87b5f5c5647b55d7b1af4167597a6a9d8e82ae9db9a6276d57671353d08

- smc_6.0.1.10133.zip

  SHA1SUM: 9a1f68051fa3d078594d7d5ae94a3b0824843585

  SHA256: 8384f5545236d10aa3bd7a1754c8f323fa96cb0b6858a5194e2de9cc178e519a

  SHA512SUM: fe1fc3e9c85784a8249ed3715b3c8d5138b150ee61840a6d7942c50dab475c7a5c407d5d0ecf84aca1c68b107354267bd9a5756236ef2ae81c243b8c85209d
• smc_6.0.1.10133_linux.zip

SHA1SUM:
7ffe27ceb777729966e63cdebe7e5c5dc66dfad2d

SHA256:
5c549ffeffff2f97d85c3a84df178fcacf3588627f9ad5d6ec44e270ecb73e9e41

SHA512SUM:
481300f9e3d1832d0ea0a64857c84667

• smc_6.0.1.10133_windows.zip

SHA1SUM:
db0954d95ffe843a75d45479dc51c0e20265a565

SHA256:
21d840373f9efa0a57d21cdca1b9ec2a088f525b54288396b7dd43c3db02692

SHA512SUM:
55aebd91d93786414e25557418a2fbc7

• smc_6.0.1.10133_webstart.zip

SHA1SUM:
b1c32af85a422e9e7b7c36d46d7024f57380497

SHA256:
b0b4fe26bb23f1c90548448abfcc75a836d2c4473ffe51666c4ee5172fc9ca1

SHA512SUM:
d09faf33e81d470f3010eb628d4195ec

Compatibility

SMC 6.0.1 has the following requirements for minimum compatibility and native support.

Minimum component versions

SMC 6.0.1 is compatible with the following component versions.

• 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)

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.

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.

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
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>The SMC allows you to install a policy that uses an Any String filter in a Correlation Situation. The engine does not accept this configuration.</td>
<td>121136</td>
</tr>
<tr>
<td>It is not possible to acknowledge alerts from the Management Server on an administrative Domain other than the Shared Domain.</td>
<td>121160</td>
</tr>
<tr>
<td>When you run the Management Client in OS X, you cannot use arrow keys to select items from the results of a type-ahead search.</td>
<td>123047</td>
</tr>
<tr>
<td>Using an invalid character, such as white space or line tabulation, in an element name can cause policy installation to fail. The error message refers to the invalid character that is used in the element name, but it can be difficult to find the element where it is used.</td>
<td>123481</td>
</tr>
<tr>
<td>Using the sgRestoreArchive command to restore an archived log file to the active log storage fails. The following message is shown: &quot;Move archive files from &lt;archive folder&gt; to current storage location. Failed.&quot;</td>
<td>124871</td>
</tr>
<tr>
<td>Report generation might fail with the following error: &quot;File format no longer supported&quot;. This issue can occur when there are empty log files from dates and times specified in the report time range.</td>
<td>127565</td>
</tr>
<tr>
<td>VPN monitoring might not be visible in an environment with administrative Domains. This issue can happen when a VPN gateway references a Location element in a different Domain.</td>
<td>127855</td>
</tr>
<tr>
<td>A route-based VPN tunnel cannot be saved if a gateway has only dynamic endpoints. Saving the VPN tunnel fails with the message &quot;Failed to apply changes&quot;.</td>
<td>128427</td>
</tr>
<tr>
<td>The Management Client displays MOD-GE-8 interfaces in the incorrect order in the appliance status monitoring image.</td>
<td>128504</td>
</tr>
<tr>
<td>When the policy is automatically refreshed after activating a dynamic update, several policy installation tasks start for the Master Engine. Only one policy installation task succeeds. The rest of the tasks fail with the message &quot;Policy is already being installed on &lt;name&gt;&quot;.</td>
<td>128534</td>
</tr>
<tr>
<td>When OSPF is configured using the Management Client, policy installation might fail during the check phase if an OSPF area is defined under a Tunnel Interface.</td>
<td>128652</td>
</tr>
<tr>
<td>Tasks running at the same time can prevent each other from progressing when both Tasks need to access the same files.</td>
<td>128885</td>
</tr>
<tr>
<td>When you use the Any Network element in a VPN Site or select the &quot;Allow SA to Any Network&quot; option in a VPN Profile, the VPN Client configuration also includes the IPv6 network ::/0. As a result, VPN Clients try to tunnel IPv6 traffic to the gateway. IPv6 addresses for VPN Clients are only supported in NGFW version 6.0 or later.</td>
<td>128955</td>
</tr>
<tr>
<td>The severity value for custom Correlation Situations is not set correctly. The severity is shown as 4294967295 instead of being on a range from 0 to 10. In the Active Alerts view, opening details of an Alert based on a custom Correlation Situation might fail with the following message: &quot;Value is out of range in literal Literal Constant&quot;.</td>
<td>129372</td>
</tr>
<tr>
<td>In an environment with multiple Management Servers, duplicate certificates for SMC servers might appear in the list of Internal Certificates.</td>
<td>129586</td>
</tr>
<tr>
<td>Description</td>
<td>Issue number</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>In rare cases, automatic license binding might disappear after you install a policy. As a result, the next policy installation fails. The appliance proof-of-serial is no longer shown in the Home view, and the license changes to Unassigned.</td>
<td>129588</td>
</tr>
<tr>
<td>When Multi-Link routes are configured and there are several possible routes to the Management Server, routes other than the route through the primary control interface might be saved as the default gateway in the engine.cfg file.</td>
<td>129590</td>
</tr>
<tr>
<td>The Refresh Policy on Master Engines and Virtual Security Engines Task might fail to install the policy. The Contact Node Timeout specified for the Master Engine is ignored if another Task is running at the same time for the same Master Engine.</td>
<td>129672</td>
</tr>
<tr>
<td>When rules have the same Source and Destination, but different Services, policy validation might incorrectly mark the rules lower in the policy as unreachable. The following warning is shown: &quot;The IPv4 Access rule @X is unreachable. The rule @Y matches also same network details.&quot;</td>
<td>130403</td>
</tr>
<tr>
<td>When you have created a new custom Application element, policy installation might fail with the message &quot;Invalid situation parameters&quot;.</td>
<td>130408</td>
</tr>
<tr>
<td>In rare cases, restoring a Policy Snapshot can fail with an error message that includes the following text: &quot;Failed to read import System Snapshot&quot;.</td>
<td>130515</td>
</tr>
<tr>
<td>If a directly connected network has been renamed before upgrading the SMC, the network might disappear from the Anti-spoofing tree after the upgrade.</td>
<td>130561</td>
</tr>
<tr>
<td>For Single Firewalls, you can only add IPv6 addresses as exceptions for contact addresses. For Firewall Clusters, you can only add IPv4 addresses as exceptions for contact addresses.</td>
<td>131051</td>
</tr>
<tr>
<td>Deleting a VPN Gateway or Firewall element might fail if the VPN Gateway and its VPN certificate were previously created in another administrative Domain. The VPN certificate remains in original Domain when Firewall is moved to a different Domain.</td>
<td>131054</td>
</tr>
<tr>
<td>Virtual Security Engines inherit the value of the Contact Node Timeout setting from the Master Engine that hosts them. When the value is changed on the Master Engine, it is applied to the Virtual Security Engines when you install or refresh the policy. Saving changes on Virtual Security Engines after changing settings for the Master Engine resets the timeout to the default value of 60 seconds.</td>
<td>131456</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.mcafee.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://ngfwlicenses.mcafee.com/managelicense.do.
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 6.0.1.

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

- SMC 6.0.1 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://ngfwlicenses.mcafee.com/managelicense.do. Activate the new license using the Management Client before upgrading the software.
- To upgrade an earlier version of the SMC to 6.0.1, 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 6.0.1.
Known issues

For a list of known issues in this product release, see KB86923.
Find product documentation

On the ServicePortal, you can find information about a released product, including product documentation, technical articles, and more.

1. Go to the ServicePortal at https://support.mcafee.com and click the Knowledge Center tab.
2. In the Knowledge Base pane under Content Source, click Product Documentation.
3. Select a product and version, then click Search to display a list of documents.

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 KB84639.

- Stonesoft Next Generation Firewall Installation Guide

Other available documents include:

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

The following documents included in appliance deliveries still use the old product name and brand:

- McAfee Security Management Center Appliance Quick Start Guide
- McAfee Next Generation Firewall Quick Start Guide