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 6.0.2 build version is 10136.

This release contains Dynamic Update package 791.

Product binary checksums

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

- smc_6.0.2.10136.zip
  
  SHA1SUM: 79785edab5d2a191a3065510756f72883952455
  SHA256SUM: b00dd5c6316fbc1a79fa8ab97f5318728f92bd5438e6fae5a5a9669c19189cb
  SHA512SUM: f01e89dbd28af40a555b58daffb424d44
  fbeef43f09a5489039a46a6962ab2d2e
  9ee593f8717aca6c5de894504772ae3d
  64c6669efabff22daffd897ae99ecbf5

- smc_6.0.2.10136_linux.zip
  
  SHA1SUM: 38ba293d3e09894c11456ba8bc4faf693b34ba37
  SHA256SUM: 65936bf685b22313040e4f5db21f87ce87f08567d010ad0456a9878e4a47e09
  SHA512SUM: 3f96f249ca1071abe73951248a59f43
  ee67d5e67ef21e5fe2d0ed4e767bb3
  0fca30bbe65231fd6977b0347a10870a
  695d93fd24e37af7d0f8a8d99a73febb
Compatibility

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

Minimum component versions

SMC 6.0 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.

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>
</tbody>
</table>
| 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

<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>Restoring a firewall Policy Snapshot might fail with the following type of message: &quot;Database problem. Error while storing object meta-data for Storable Id[X,X,X].&quot; Importing the same policy fails with the following type of message: &quot;Element appears invalid: Firewall Policy &lt;name&gt; is invalid. IPv4 Access must have unique defined rank values.&quot; This can occur if the policy has many rules that were created from log entries.</td>
<td>113902</td>
</tr>
<tr>
<td>On the Mobile VPN tab of the Policy-Based VPN view, selecting the &quot;Selected Gateways below&quot; option prevents access to the Tunnels tab.</td>
<td>128278</td>
</tr>
<tr>
<td>When the Service Definition in an Access rule contains a Situation for category-based URL filtering, an HTTP Service, and no TLS Match, saving the Service definition can fail and the following type of message is shown: &quot;Error while storing object meta-data for Storable Id[#,#,#]&quot; The same message can be shown in the Edit Source or Edit Destination dialog boxes if a User element has previously been added and you try to add another element.</td>
<td>129175</td>
</tr>
<tr>
<td>Opening the properties of or trying to delete a PDF style template fails. When opening the properties, the following type of message is shown: &quot;Failed to display&quot;.</td>
<td>129548</td>
</tr>
<tr>
<td>The Management Server does not enforce a license for virtual appliances only. Even if the Management Server can see that the node count has been exceeded, installing the policy on a platform other than a virtual appliance still succeeds.</td>
<td>131267</td>
</tr>
<tr>
<td>The use of unsupported characters in element names can prevent policy installation or cause corrupted snapshots. Element validation prevents the use of characters such as &quot;white space&quot; or &quot;unit separator&quot;.</td>
<td>131330</td>
</tr>
<tr>
<td>Log forwarding might not resolve the name of the Situation. Instead, the situation ID is shown.</td>
<td>131547</td>
</tr>
<tr>
<td>Removing a firewall interface that has browser-based user authentication enabled causes a policy installation validation error.</td>
<td>131851</td>
</tr>
<tr>
<td>The information about the active Alert Policy in the Info pane of an administrative Domain is updated too soon after starting to install a new policy.</td>
<td>131859</td>
</tr>
<tr>
<td>When the Management Server is installed on a different computer than the Log Server, notification scripts in the &lt;installation folder&gt;/data/notification directory are not correctly formatted.</td>
<td>131942</td>
</tr>
<tr>
<td>Policy installation for a Virtual Security Engine can fail when an SSL VPN has been configured. The following type of message is shown: &quot;Policy for Virtual Firewall &lt;name&gt; contains an SSL VPN configuration. SSL VPN is only supported on 64-bit engines.&quot; This happens when the Platform information for the Virtual Security Engine is not available on the General tab of the Info pane.</td>
<td>132509</td>
</tr>
<tr>
<td>When installing 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>132842</td>
</tr>
<tr>
<td>After activating dynamic update package 774 or later, images for some appliances might not be shown correctly in the System Status view or the Home view. Policy installation might also fail if the appliance has wireless interfaces.</td>
<td>133092</td>
</tr>
</tbody>
</table>
### Description

<table>
<thead>
<tr>
<th>Description</th>
<th>Issue number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Negated network expressions are interpreted incorrectly in the Inspection Policy. As result, rules intended for IPv4 addresses might also match IPv6 addresses.</td>
<td>133192</td>
</tr>
<tr>
<td>Starting the Management Client using Java Web Start might not work with JRE version 8 update 102.</td>
<td>133329</td>
</tr>
<tr>
<td>If a Virtual Resource is added to a Master Engine using the SMC API, and no concurrent connection limit is set, refreshing the policy for the Virtual Security Engine associated with the Virtual Resource might fail.</td>
<td>133411</td>
</tr>
<tr>
<td>An empty Group element used in an expression prevents the policy installation, but the validation error does not provide a reason for the failure.</td>
<td>133888</td>
</tr>
<tr>
<td>When the number of VPN tunnels for a firewall is counted in X0000, policy generation can take up to an hour because the topology is retrieved several times during the policy generation.</td>
<td>133915</td>
</tr>
</tbody>
</table>
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.
Known issues

For a list of known issues in this product release, see 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 10097.

- *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*