# Table of contents

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

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

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

4 Resolved issues...................................................................................... 8

5 Installation instructions
   - Upgrade instructions.................................................................... 9

6 Known issues.......................................................................................... 10

7 Find product documentation
   - Product documentation............................................................ 11


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 6.0.0 build version is 10116.
This release contains Dynamic Update package 749.

Product binary checksums

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

Note: The installation files have been repackaged. The binary checksums have changed.

• smc_6.0.0.10116.iso

| SHA1SUM:         | a045dbae54bf0211ed8f3a1240c3b3801f2801 |
| SHA256:          | eb0ab8d9d9842805685292a6885328357d4e589c81cb6e0d31f351e11a9d6 |
| SHA512SUM:       | 45e20315d4c961eeaf8e844d322b5d4c46e56037f956e0c0bdcbe61b4bf7ae0b |

• smc_6.0.0.10116.zip

| SHA1SUM:         | ec916488caabf6dfb39e1215e423079850b35c6e |
| SHA256:          | f853190304588a565c773bf8102723f088c6919378027ac35349773f39d60ab |
| SHA512SUM:       | 3dc40657be81bdaa0a34589d9f8fe51 |
• smc_6.0.0.10116_linux.zip

SHA1SUM: 853abcb7ccb5d245928780263a8f872e1f03406
SHA256: 8c3adde10f26f041842892d8fb0a3205c6306c0e0d1993b867dd53b18bf3de3d
SHA512SUM: a774c226906a3bdf3435da69a79d94083ea3cb38bf264d58618d243d5d33bb0b8367b03e26443b29d72f2aaa52c97769e17751da50ac3546709c5a724a868

• smc_6.0.0.10116_windows.zip

SHA1SUM: a5fb523bfeac14319e9923169c9e3ac0b9693e
SHA256: 70ac06b80f1527eb0add0a7d00493779297/e9b8ac7d59e9857b0816af5a5b3
SHA512SUM: 531f1fd0b72cbf093a124544db9827b7aad887d516b64a8ff6a3a261c74c773d7f80e2ed3e161c6dcbe48e9b5d437f68652b1f53a6c902776e55da0d0

• smc_6.0.0.10116_webstart.zip

SHA1SUM: 12eacef9a00b03ffdaad4095e12db4bc57cf79cf
SHA256: d316a9a9a48d5826ebba8c4e3a99cc361627b12bc2b5007ea2c64f603b178
SHA512SUM: 355e7b11fa4da9864e5f42a4e3ef521ede7a3c634a9f994dd9913c2138adcfc2b1bf96af6e79eca3bb31bb81f0250f99e9907d83dbcb72c196c580b13fc

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.

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.

| Description                                                                                                                                                                                                                                                                                                                                 | Issue number |
|----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|
| Due to timing issues in contacting the Management Server after a remote upgrade, the Management Client might incorrectly show the node in the initial configuration state even though the node is online with a policy installed.                                                                                                           | 109198       |
| If you take a traffic capture and have Local Workstation selected as the Destination Path, the traffic capture does not finish properly with engines in the IPS and Layer 2 Firewall roles. The captures stops at "Deleting original Traffic Capture on IPS/Layer 2 Firewall Node..." even though the file has been saved to the correct place and deleted from the engine.                                                                                   | 111973       |
| After upgrading the SMC, an engine node can appear to be unlicensed. The proof-of-serial information from the General tab in the System Status view disappears, causing the license not to bind to the node.                                                                                                                      | 113730       |
| Generating a diagram using the Diagram Editor or selecting a Log Server element in the System Status view can result in the following error message: "Diagram Error. Auto Generation Failed. Diagram editing failed. A connection is irrational." The problem is caused by engines that have an interface with a dynamic IP address and routes to hosts defined under that interface. | 121919       |
| When using an external CA for a VPN certificate, the certificate request is created in VPN | Gateways. When you select ECDSA or DSA as the Public Key Algorithm in the Generate Certificate dialog box, you can select the Key Length from 3 default options. For ECDSA certificate requests, the Signature Algorithm is updated by the selection.                                                                 | 122337       |
| SMC API connection fails when the "Use SSL for session ID" option is selected on the SMC API tab in the Management Server Properties dialog box.                                                                                                                                                                                                 | 125010       |
| Alert escalation by email might not contain correct information about Situation elements. A notification is sent by email, but it might include additional characters, or the situation information might be missing. Log entry details might also include additional characters, or the situation information might be missing.                                                                                       | 125255       |
| By default, new BGP Peering elements are added to the Routing view under IPv4 networks even though the BGP Peering element has an IPv6 address and the interface has both IPv4 and IPv6 networks. The Routing view does not validate whether the IP address version of the element matches the IP address version of the network.                                                                 | 127236       |
| The information about the active Alert Policy in the Info view of an administrative Domain is not updated even though the policy installation for the Domain is successful.                                                                                                                                                                                                 | 127279       |
| The activation of dynamic update package 740 or newer can fail. The message includes "Element name Successful Attacks is already used. Activation failed."                                                                                                                                                                                                 | 128112       |
| The rollback timeout for Virtual Security Engines is 60 seconds even when a longer time has been set for the Master Engine in the Advanced Settings branch of the Engine Editor. If installing the policy on a Virtual Security Engine takes too long, the previous policy is restored.                                                                                                                          | 128146       |
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.

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://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, 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 KB86923.
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