FORCEPOINT

Stonesoft Management Center

Release Notes

5.10.4

Revision A

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 started rebranding the SMC, the Stonesoft Next Generation Firewall (Stonesoft NGFW) product, and the Stonesoft NGFW product documentation. We use Stonesoft in the product name in this document. However, the old product name is still used in the Management Client, NGFW appliances, the NGFW engine software, and the product documentation set that we created for the NGFW 5.10.0 release.

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 5.10.4 build version is 10034.

This release contains Dynamic Update package 802.

Product binary checksums

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

- smc_5.10.4.10034.iso

```
SHA1SUM:
3bd7248e68f39530420cc5e772532f15c01c84a4

SHA512SUM:
05247626709b2d348b8dba49bd1f28af
b25450ff2a8cd6f9517e3e81715bf4ca
b02c4ca1afdd1f45db762d591b83d682
ee0bba5ecc026c9c99bd20af03b13d3f
```

- smc_5.10.4.10034.zip

```
SHA1SUM:
6ffd531e8afbf1e67f9515858d5b42454bf9acef

SHA512SUM:
c7c8a47a89e8cb15a30b48ccf02ac91c
1f6c3d4674278484604da57650ca00a2
a7cd26bae817b402a06bde78d9f69b0d
8fa7c045ae07f7792ef80255bd73ee71
```

- smc_5.10.4.10034_linux.zip

```
SHA1SUM:
465f9b7cc9d3736a9fa13d7dae2ef3fc786c880f

SHA512SUM:
32bdf2eb699a86ab5980764cc9ad1347
92df3db6c370aca15812e1bf49c092de
61d66dd5436f1e4a9931223756ed84ba
cc2f8c04117d916f71f6c9ddbd0deaae
```

- smc_5.10.4.10034_windows.zip

```
SHA1SUM:
9accd08af92617ca5bab4a59de3e8b7d65d85a1b

SHA512SUM:
9490a9460e6e26355f290ff8badc340b
155cedc1badfa60e41eff71a8b24c71f
355fa0991121995c2e137a60fba55ffe
f73d7a624ac0cac01d1f31da9fdcc5cb
```

- smc_5.10.4.10034_webstart.zip

```
SHA1SUM:
46ecd8702c3b825fee4ea0aa8c17246555a8a003

SHA512SUM:
c41a2a96202a10b6ce2200b034390dfe
7e48fc52e6e5957f9e5247055c49da06
a58ff9e2c6cef39189530894c6d66754
9bdab4751de944f0502856d472b5e633
```

Compatibility

SMC 5.10 has the following requirements for minimum compatibility and native support.

Minimum component versions

SMC 5.10.4 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 5.4 and 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 5.10, Stonesoft NGFW 5.10 is required.

New features

This release of the product includes these new features.

SMC Appliance

This release adds support for the Stonesoft® Management Center Appliance (SMC Appliance). It combines the hardware, operating system, and SMC software into one appliance for the Management Server and Log Server.

The SMC Appliance unifies the process for creating administrator accounts and performing maintenance tasks, such as configuration backups, patches, and rollbacks. It also provides increased functionality for NTP, SNMP, and SSH.

Single sign-on (SSO) to SSL VPN Portal

The SSL VPN Portal (reverse web proxy) can be configured to cache user credentials. The portal logs on to the back-end servers with the credentials as if they came from the web browser at the endpoint. You can group the servers that use the same credentials by SSO domain, to further reduce the need to re-enter the password.

Support for Threat Intelligence Exchange

Stonesoft NGFW can now query file reputations and receive reputation updates from the McAfee® Threat Intelligence Exchange (TIE) server. TIE makes it possible for administrators to tailor comprehensive local threat intelligence from global intelligence data sources, such as McAfee® Global Threat Intelligence™ (McAfee GTI), endpoints, gateways, and other security components. File reputation data is exchanged using the McAfee® Data Exchange Layer (DXL) broker network. File reputation updates ensure that Stonesoft NGFW engines always have the latest file reputations available for use in file filtering.

New tunnel type for the route-based VPN

A new tunnel type for the route-based VPN allows the use of tunnel mode IPsec without an additional tunneling layer. The route-based VPN configuration dialog box has been improved.

Connectivity between Stonesoft NGFW and SMC using IPv6

Engines that only use IPv6 to connect to the Internet can now be managed by SMC over the Internet using IPv6-based management connections. Connectivity between SMC components still requires IPv4 addressing and connectivity.

Network Security for Industrial Control Systems (ICS)

ICS support has been enhanced with deep inspection support for DNP3 (TCP/UDP) and Open Platform Communications Unified Architecture (OPC UA).

Safe search support

Stonesoft NGFW can be configured to enforce safe search usage for Google, Bing, Yahoo, and DuckDuckGo web searches.

Support for Intel Security Controller and VMware NSX

Intel® Security Controller is a management service that coordinates between Stonesoft NGFW and virtualization platforms. It allows the rapid deployment and provisioning of engines across a diverse virtual network. Traffic can be filtered on the perimeter of the network and within the network.

Enhancements

This release of the product includes these enhancements.

Enhancements in SMC version 5.10.0

Enhancement	Description
Logon banner	The Management Client, the Web Portal, and the web-based authentication logon page can be set to display a disclaimer or banner that the user must accept before being allowed to log on. Administrators can configure the content for the disclaimer or banner.
Password policy enhancements	A number of new settings enable more granular options for administrators for defining password policies.
Auditing enhancements	Auditing features have been improved to meet new certification requirements.
TLS-protected syslog export	There is a new TCP with TLS service that can be used in log and audit data forwarding rules. The option enables TLS-protected log and audit data forwarding from the Log Server and the Management Server to an external syslog server.
Integrated switch in Single Firewalls	The switch functionality is only supported on Single Firewall engines that run on specific Stonesoft NGFW appliances that have an integrated switch (currently Stonesoft NGFW 110 appliances only).
OPC UA enhancements	It is now possible to configure OPC UA Secure Conversation decryption in transparent mode and import the required keys in the SMC using the **OPC UA Inspection** branch under **Add-Ons** in the Engine Editor.
Reporting enhancements	There are a number of new styles, elements, and visualizations available that allow reporting and monitoring in a more granular way.
SMC performance improvements	Various performance improvements have been made, especially in the Engine Editor and the Security Engine Configuration view as well as in the handling of large policy sections.
SMC administrator authentication with TACACS+	Support for a TACACS+ based external authentication method has been added to the SMC administrator authentication options.
SSL VPN Portal address	The external URL of the SSL VPN Portal (reverse web proxy) can now contain an IP address instead of a fully qualified domain name (FQDN), which used to be the only alternative in the portal. An FQDN requires setting up DNS, even for small-scale installations. This feature enables quicker portal setup.
McAfee Advanced Threat Defense communication logging improvements	Improvements have been made to the communication protocol and logging features between McAfee® Advanced Threat Defense and Stonesoft NGFW. Stonesoft NGFW now logs the dynamic analysis results when available from McAfee Advanced Threat Defense. Stonesoft NGFW provides the file name, destination IP address, and URL details when sending the file to McAfee Advanced Threat Defense for analysis.

Enhancement	Description
File filtering improvements	Improvements have been made to file type detection and filtering. We recommend that you update your file filtering policies with the new file type categories.
Analyzers and Sensor-Analyzers no longer supported	Legacy Analyzer nodes and combined Sensor-Analyzer nodes are no longer supported. To upgrade to SMC 5.10.0 or later, you must remove these elements.

Enhancements in SMC version 5.10.1

Enhancement	Description
Setting SNMP location separately for each node	SNMP location can be set for each cluster node in the Clustering pane in the Engine Editor.

Enhancements in SMC version 5.10.2

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.

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
Retrieving routing information through the SMC API can work unreliably, especially with a large number of dynamic routes on Virtual Firewalls.	116761
Searching for IPv6 addresses does not return results when the search criteria includes letters.	126308
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.	127250
Configuring a route-based VPN tunnel in tunnel mode between a Firewall and a Virtual Firewall fails with the following error "Incorrect parameters: Unsupported Class with ID".	133858
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.	133915
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 lead to only the last change being saved.	134253
Snapshot comparison can fail with the error "Database error. Details: Failed to read import exported:data.xml." The problem can occur when a custom VPN profile is in use.	134280
Comparing Policy Snapshots can fail and give a "Database Error" message on Master Engines when you have moved networks from one interface to another interface and then deleted the original interface.	134411
Links to the License Center do not point to the new Forcepoint location: https://stonesoftlicenses.forcepoint.com/managelicense.do.	134624
A route-based VPN tunnel cannot be saved if an external gateway has only dynamic endpoints. Saving the VPN tunnel fails with the message "Failed to apply changes".	135173
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 prevents importing the exported Security Engine element into the SMC.	135184

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 **Security Engine 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 5.10.

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

- SMC 5.10 requires an updated license if upgrading from 5.9 or earlier.
  - 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 5.10, 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 5.2.0 require an upgrade to version 5.2.0–5.9.5 before upgrading to 5.10.

Known issues

For a list of known issues in this product release, see Knowledge Base article 10139.

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 Management Center Appliance Quick Start Guide*
- *Stonesoft Management Center Appliance Hardware Guide*
- *Stonesoft Next Generation Firewall Quick Start 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*