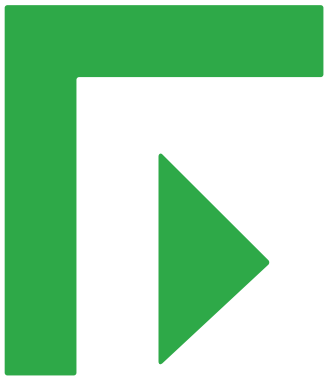

FORCEPOINT

Stonesoft Management Center

Release Notes

5.10.5

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 5.10.5 build version is 10037.

This release contains Dynamic Update package 840.

Product binary checksums

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

- smc_5.10.5.10037.zip

```
SHA1SUM:
4b8fa2054e5480d68d2f8e23bbe8af66ab1dd9d7

SHA256SUM:
303768241e77d7c0e7adc052596f0680b39d7baaf8598ca137d516dba2b8028e

SHA512SUM:
edb18d5989667f24d272ce49f4c3e708
51700abe1d9ff933cb86f215f0ad5e59
42f2ce3ad1c41da478a6dc6cf4538962
644bf16debfbe924848dc17f58faa9a9
```

- smc_5.10.5.10037_linux.zip

```
SHA1SUM:
4a661b7ef6339112b78dc9743a21214c935e3d70

SHA256SUM:
4c7b5ebb1c44d163e39c5450ab43a82ddbb4864042e3076eed5dcbc154f67ee5

SHA512SUM:
5351af67c49d9d70fc697c179c1af52c
89c384596c99fb765d31015d571ffdcb
5e39abe7c497de63f2f0e582ed667b1a
73add4624de53cf9f0dea43734d589b4
```

- smc_5.10.5.10037_windows.zip

```
SHA1SUM:
d02728b56bee828ba2488c85e6f816b1080392d7

SHA256SUM:
223333faeed209d6fae5ba1c44c7cc02a045c3fced8d20b961b0e7f4a437c936

SHA512SUM:
bd97f50e471ce9310588a4498af8e804
1c49f88dee4ca1b47ce03464167cae67
4cf6d7f90505aee89ed5d172932cf573
108c8befb2495bbe7473ba07193510a9
```

- smc_5.10.5.10037_webstart.zip

```
SHA1SUM:
936f083d0c1e0f41f779b3634ef9621ecf3d0477

SHA256SUM:
8e7c7631b1a865674340eaa88d91131173c1e9d8014a9318f2e85a72f65394f9

SHA512SUM:
1e403b620b96af92998bb3a6d4f74a0e
ec03cf7917e25b3301ef56249e2a9cc7
9b89bdbb4b3377e3437ef04af9427fd2
db1d1d4cbb23ed461a0c6b939ebb862f
```

Compatibility

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

Minimum component versions

SMC 5.10.5 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. For more information and configuration instructions, see the

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
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.	129588
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.	SMC-599
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.	SMC-893
When a report includes IP addresses without a country flag icon, printing the report or exporting the report as PDF or HTML might fail. Printing fails with "Failed to generate PDF in memory".	SMC-979
Using a Domain Controller password that is longer than 82 characters in the Active Directory Server properties prevents the Management Server from being upgraded.	SMC-1189
When you use the Upgrade to Cluster tool, and you change the NDI and CVI addresses several times, saving the Firewall Cluster element might fail.	SMC-1231
When you change the IP address of an interface from an IPv4 address to an IPv6 address or from IPv6 address to IPv4 address, the antispoofing configuration is not updated correctly. Policy installation might fail. The following error message is shown: "Syntax error in network configuration: No IPv6 connected network available on interface X near line Y".	SMC-1249
When you modify a RADIUS or TACACS+ Authentication Server, you cannot remove Authentication Methods on the Authentication Methods tab of the RADIUS Authentication Server Properties or TACACS+ Authentication Server Properties dialog box.	SMC-1483
If you use the SMC API to monitor routing, the SMC API might become unresponsive when an engine or a Log Server is unavailable.	SMC-2141
The connection from the Web Start Management Client to SMC version 5.10 or earlier fails due to certificate expiration. The client is blocked by Java Security.	SMC-2231
If you select multiple licenses in the All Licenses view and the selection includes divider rows that specify the license types, you cannot copy the license information for the selected licenses.	SMC-2421
If you use a loopback IP address as an endpoint in the Route-Based VPN, the creation of Policy Snapshots fails when you install policies. The issue also prevents you from exporting the Route-Based VPN element.	SMC-2616

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*