



# **FORCEPOINT**

## **Stonesoft Management Center**

**Release Notes**

**5.10.3**

Revision A

# 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.....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 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 5.10.3 build version is 10032.

This release contains Dynamic Update package 780.

## Product binary checksums

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

- **smc\_5.10.3.10032.iso**

```
SHA1SUM:  
1116ccf18dfbeb255dccb9fdc72b00831b901fde
```

```
SHA512SUM:  
a0f49ff898a5ae99be083bda90189e56  
2e8b5c8f15ddb808eb0d81a0139625ff  
91851939f3e3236b9eaada74beeacd3c  
95497bdf33a6ff2ad1c7af415bbead3a
```

- **smc\_5.10.3.10032.zip**

```
SHA1SUM:  
59271dae19b775ea69b9d697bee2346dd6695f39
```

```
SHA512SUM:  
a6e4c03d42c65b027d1a12782762b2ba  
d1023d746a81d3345db6085499f00d15  
5e8181e9441cd25ce455a905692f7735  
7dce6552d3c77c5880862de83d23c61e
```

- **smc\_5.10.3.10032\_linux.zip**

```
SHA1SUM:  
34ca958e065dadfc82a270d21dc2bd1a2012d73e
```

```
SHA512SUM:  
bcd8e95a13ecb9b9b0bcd913fd55eeeb  
344a1f327100d51f5560356070b0e91e  
0ec84eeac0ef6a8ba40f503231ada443  
1095f3a9720d8f3362bb0212eb8e2eb6
```

- **smc\_5.10.3.10032\_windows.zip**

```
SHA1SUM:  
e7a0a2d9ae5d4214753c7a7433b3acb7736fce72
```

```
SHA512SUM:  
8da904de6e6a1a7ed598c196cd84975e  
4950b0937fec31d8900c885309386d7e  
7e79665e1f361178d8b9ffac29646561  
686a506d390abb27e9c416435ebb963e
```

- **smc\_5.10.3.10032\_webstart.zip**

```
SHA1SUM:  
ab7df0fd15c13022ebb416ea43e6e255f4200ba8
```

```
SHA512SUM:  
093720abb0654646dd0c6aef5bbaf447  
9f6f2293c7245f23d2b0f2c81e6daccb  
15dc01d3a6774a6e40cbe460febb3173  
29ae0bde788be5f1bead141b3f3eef0c
```

## Compatibility

---

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

### Minimum component versions

SMC 5.10.3 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 <b>OPC UA Inspection</b> branch under <b>Add-Ons</b> 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	<p>The sgArchiveExport script that exports logs from archive now supports CEF, LEEF, and ESM formats in addition to CSV and XML.</p> <p>You can now schedule Export Log Tasks to run hourly using relative time ranges.</p>



# 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
Opening the properties of or trying to delete a PDF style template fails. When opening the properties, the following type of message is shown: "Failed to display".	129548
If a directly connected network has been renamed before upgrading the SMC, the network might disappear from the Anti-spoofing tree after the upgrade.	130561
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.	131051
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.	131456
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.	131859
Policy installation for a Virtual Security Engine can fail when an SSL VPN has been configured. The following type of message is shown: "Policy for Virtual Firewall <name> contains an SSL VPN configuration. SSL VPN is only supported on 64-bit engines." This happens when the Platform information for the Virtual Security Engine is not available on the General tab of the Info pane.	132509
After activating dynamic update package 774 or later, the appliance image and interfaces for the NGFW 115 appliance might not be shown correctly in the System Status view.	133092
Starting the Management Client using Java Web Start might not work with JRE version 8 update 102.	133329
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.	133411

# 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.



**Note:** SMC 5.9.5 can only be upgraded to SMC 5.10.1 or higher.

# Known issues

---

For a list of known issues in this product release, see [KB10139](#).

# 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 [KB10097](#).

- *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*