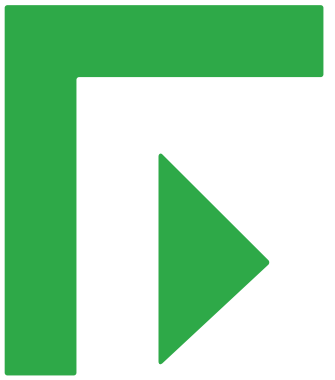

FORCEPOINT

Stonesoft Management Center

Release Notes

5.10.2

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 5.10.2 build version is 10028.

This release contains Dynamic Update package 763.

Product binary checksums

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

- smc_ 5.10.2.10028.iso

```
SHA1SUM:
7de94379eb7916d78bd93cd5ca74a35c79b092e7

SHA512SUM:
0d3a0c9f45450d8fb6ca2ce1a06d2f69
20c7c0bb9784d143604bf977f9b2ebbf
29b7d6c3c87040439270def7e9e09206
5dc443387c46d3b897fbdf83e50b1a15
```

- smc_ 5.10.2.10028.zip

```
SHA1SUM:
4fa5d71bdd85e85e21f18191068444663070aa38

SHA512SUM:
d0428b83796b22e10040f626c7c9dfdf
0aa08c044cedf3935ca53ea0f628420f
26f87c5168fac6b67dabd247de41d359
b58afbc788600bf7e7e360b87028159d
```

- smc_ 5.10.2.10028_linux.zip

```
SHA1SUM:
7f1a07ae7635a4d605bdc997c405b2b194c881d5

SHA512SUM:
8da8c5f407b54f5119e0932a8eb66b7e
57d8ec5261f448c843b3e71927da70ae
6a66393c80223b1a9fc635bb3ba31b62
31be0347fc93cc8fcc47bcc4e74d1cdc
```

- smc_ 5.10.2.10028_windows.zip

```
SHA1SUM:
bd79d9c230c217a78351d79c60ddab211799bd54

SHA512SUM:
334ec817064ce30fc4a5b4c84bb7e4e4
a687d1105e71d8efd6a9e04c97ff1f91
c4b702979a233cee8c75571b91a7d310
0786e7f0016e3e85c2402dc547304466
```

- smc_ 5.10.2.10028_webstart.zip

```
SHA1SUM:
618f0916ad57ea2f66c5330697e373f25f36a724

SHA512SUM:
1cad339ebcb3d0d77ea6dddc28922a1d
e8ca0a236ebb93694d1548c803622c9e
c11cc5669f9907a24f0c79868ce083e3
c9005409637f03273c3dcaca3fed3deb
```

Compatibility

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

Minimum component versions

SMC 5.10.2 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
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
When you run the Management Client in OS X, you cannot use arrow keys to select items from the results of a type-ahead search.	123047
Using an invalid character, such as white space or line tabulation, in an element name can cause policy installation to fail. The error message refers to the invalid character that is used in the element name, but it can be difficult to find the element where it is used. The error message during policy installation and element export has been enhanced to specify the element.	123481
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
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
VPN monitoring might not be visible in an environment with administrative Domains. This issue can happen when a VPN gateway references a Location element in a different Domain.	127855
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
A route-based VPN tunnel cannot be saved if a gateway has only dynamic endpoints. Saving the VPN tunnel fails with the message "Failed to apply changes".	128427
When the policy is automatically refreshed after activating a dynamic update, several policy installation tasks start for the Master Engine. Only one policy installation task succeeds. The rest of the tasks fail with the message "Policy is already being installed on <name>".	128534
When you use the Any Network element in a VPN Site or select the "Allow SA to Any Network" option in a VPN Profile, the VPN Client configuration also includes the IPv6 network ::/0. As a result, VPN Clients try to tunnel IPv6 traffic to the gateway. IPv6 addresses for VPN Clients are only supported in NGFW version 6.0 or later.	128955
The severity value for custom Correlation Situations is not set correctly. The severity is shown as 4294967295 instead of being on a range from 0 to 10. In the Active Alerts view, opening details of an Alert based on a custom Correlation Situation might fail with the following message: "Value is out of range in literal Literal Constant".	129372

Description	Issue number
The Refresh Policy on Master Engines and Virtual Security Engines Task might fail to install the policy. The Contact Node Timeout specified for the Master Engine is ignored if another Task is running at the same time for the same Master Engine.	129672
When rules have the same Source and Destination, but different Services, policy validation might incorrectly mark the rules lower in the policy as unreachable. The following warning is shown: "The IPv4 Access rule @X is unreachable. The rule @Y matches also same network details."	130403

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.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 **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://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 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 KB85589.

Find product documentation

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 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*