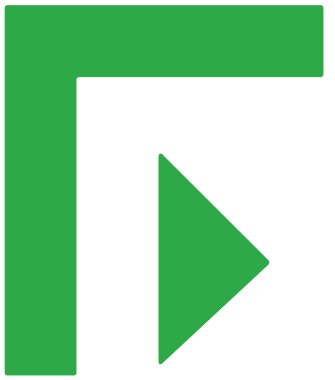

FORCEPOINT

# Stonesoft Management Center

## Release Notes

### 5.10.1

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 5.10.1 build version is 10027.

This release contains Dynamic Update package 740.

## Product binary checksums

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

- smc_ 5.10.1.10027.iso

```
SHA1SUM:
fff1d9dc30a2d2f8a274575a7c8ad46160439c03

SHA512SUM:
97c033aa7110ce7523737eaf722a6b09
d20c0ca26ffef42c8af251f0dfac0a38
a7c68105ef0d0c5a4eb22bf5384d1bf9
a991ce9848ff68cf10a8eab1f8914e81
```

- smc_ 5.10.1.10027.zip

```
SHA1SUM:
36b273471c55d04076412716b11f3ecf3f44e575

SHA512SUM:
f529deb5b4a0688de793ecac3fa1cab4
d45628c2a5d8c44fc1c0d6557415b572
554efb1195150d323688be546996bf2b
12c69dcb703a5d583c24864651cb8c44
```

- smc_ 5.10.1.10027_linux.zip

```
SHA1SUM:
acf9c868c4a4a5f939f5fc00989e4fe1c2fd3147

SHA512SUM:
068d5ad4ade9bd917cf7b89a26df5a5b
41877b5acd4d5eb190cad2e2719c27ce
93e0792d730bd41c921c6f473659e30e
161de315443930c48269e4bd2692c23e
```

- smc_ 5.10.1.10027_windows.zip

```
SHA1SUM:
90fc41aea0bcb65e748a37b7b508cdee4dcd69bb

SHA512SUM:
ff4fac51c87e38544226f942ef8d9d0e
f0afbd9147bc6abe73fd5df1cdb8cb00
b434a60a6443249ed5aab28e9e61d375
9de44390ea8b763a11f3f0c8846d0210
```

- smc_ 5.10.1.10027_webstart.zip

```
SHA1SUM:
4f20ddf01b3b6eed8a7633e43c69dfc1830dca77

SHA512SUM:
6375e5a4897ff1b9e5bc9a0e58e61a05
d3240107e1f99ab76b6483fbbe0aeb29
b16dc3e887866cef4a56a50bb504bce8
cc0fe440ba3cb3e2974caebcf293ba58
```

# Compatibility

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

## Minimum component versions

SMC 5.10.1 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.

## 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.

## 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.

## Setting SNMP location separately for each node

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

# 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 |
|---|---|
| The number of active alerts on the yellow triangle in the System Status view might differ from the total number of active alerts in the Active Alerts view. Alerts without a Severity value are counted and visible only in the Active Alerts view. | 117287 |
| When you view an Element Snapshot for a VPN element in audit logs, you can only view the VPN Properties pane, not the whole configuration. The comparison on the "Site-to-Site VPN" tab does not show any gateways either. | 117332 |
| Import of elements fails if the imported file contains an Outbound Multi-Link element with a defined category. The resulting error message contains the text: "DTD claims: Validation error, encountered element <category_ref> as a child of <outbound_multilink>: Expected <multilink_qos_class>, netlink_address> or </outbound_multilink>". | 117345 |
| The Management Client can sometimes crash when a Management Server or Log Server runs on a 32-bit Linux operating system. | 121951 |
| Printing a report with a custom PDF template might fail with the following message: "Failed to read PDF template content Details:". This occurs if the operating system of the Management Client and the Management Server are different. | 122336 |
| A loopback IP address might appear as an internal VPN endpoint instead of a loopback endpoint. | 122380 |
| When you edit the log filters on the Permissions tab of the Administrator Properties dialog box, the filter is not applied as the default filter for the administrator in the Logs view. | 123315 |
| Installing the same policy for several Virtual Security Engines on the same Master Engine can fail with this error message shown: “Engine error: Message code 1005 Session is already reserved by some other SMC.” | 123389 |
| The new Internal CA remains in "Renewal started" state even after all engines have received the new CA. Furthermore, new certificates are still generated using the old CA. According to the progress report for the “Renew Internal Certificate Authorities” task "All components have not yet received the new Internal Certificate Authority". | 123422 |
| A search or type-ahead search for a partial IP address returns too many results. All engines are included in the results. For elements with both IPv4 and IPv6 addresses, a search by an IPv6 address does not return results. | 123435 |
| VPNs and gateways are not shown in the System Status view when the routing for a Master Engine includes NetLink elements. | 123488 |
| The change of SSL VPN Portal port might not be saved in the Engine Editor when there are several VPN gateways for the firewall. | 123554 |
| Using the PUT method in the SMC API for updating an element that has a password can fail when the encrypted password attribute taken from the GET method response is reused. The password will be rejected during the PUT method processing or a wrong value will be stored in the database. | 123565 |
| SMC API enables setting the same rule ranking for several rules. This can result in unexpected rule rearrangement when the policy is edited later. | 123568 |
| After activating a dynamic update package, policy installation can fail. The following message is shown: "Validation for policy upload failed due to: Validation failed because timeout exceeded." | 123578 |

| Description | Issue number |
|---|---|
| Refresh Policy on Master Engines and Virtual Security Engines task fails to run all the operations needed. | 123581 |
| On the Connection tab in the Management Server Properties dialog box, a Management Server can be configured to use a proxy server to connect to servers for license updates, dynamic updates, engine upgrades, and certificate revocation lists (CRLs). If the proxy server cannot be reached on the first try, the Management Server can try to connect to the servers directly. | 124114 |
| When you right-click Licenses in the Administration tree and select Get POS Information From Engines, the Master Engine licenses become unbound. | 124556 |
| Policy refresh on Master Engines and Virtual Security Engines might fail with the message: "Engine error: Engine error: Message code 1006 Session information did not match to reservation." As a result of the error, one node in the Master Engine cluster performs a rollback. As the nodes run different policies, this node goes offline. | 124604 |
| Administrator logon might fail because additional database connections cannot be opened. This can occur with large-scale environments. | 124646 |
| Logging on to a Management Server can sometimes fail because of an internal error. The problem is caused by corrupted audit status. | 124784 |
| File Filtering Policy is defined on the Inspection tab of the engine policy. File Filtering Policy selection change is saved even when exiting the engine policy without saving. | 124824 |
| Announced networks disappear from BGP (Border Gateway Protocol) configuration when you upgrade the SMC. | 125100 |
| The following warning message about an unreachable sub-policy rule might be shown when installing a policy: “The IPv4 Access rule <rule tag> in Firewall Sub-Policy <policy name> is unreachable. The Jump rule <rule tag> that directs connections for matching against the Sub-Policy does not match the same network details.” | 125113 |
| When you click an icon in the Management Client toolbar, a new view opens in a new tab instead of opening in the tab that is already open. | 125153 |
| Upgrading a legacy Sensor-Analyzer engine to a Single IPS engine fails. Routing and antispoofing configuration cannot be created for the new Single IPS element. | 125188 |
| When you change the IP address of a BGP Peering element and try to save the element, the IP address reverts to the previously used IP address in the Routing pane in the Engine Editor. | 125534 |
| "Refresh Policy on Master Engines and Virtual Security Engines" task on a Master Engine or several Master Engines can fail for some Virtual Security Engines. The message is "failed to build dynamic routing configuration". The failure is not limited to specific Virtual Security Engines. | 125550 |
| The contact address of a VPN endpoint for a Location is not the same as the contact address that is defined for the corresponding CVI for the same Location. | 125606 |
| If the task "Refresh Policy on Master Engines and Virtual Security Engines" is scheduled to run repeatedly it can fail with the message "Upload failed Out Of Memory". | 125847 |
| Policy installation for a Virtual Security Engine can fail when an SSL VPN has been configured. The message shown is: "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. | 125872 |
| The type-ahead search deletes the first character of the search string if you access the Management Client using Web Start on the Mac OS. | 125880 |

| Description | Issue number |
|---|---|
| Expanding a Policy-Based VPN to see all the gateways and sites can be slow. The same can happen when using the Engine Editor if a Firewall is referenced in hundreds of VPNs. | 125881 |
| When you add a dynamic IPv4 address for a physical interface and define a password in the PPP Settings dialog box, the password is not saved. | 125959 |
| When restoring a policy snapshot, ARP entries included in the Firewall properties are not restored. | 125961 |
| Using NPS as the external authentication method for administrators does not work because the Management Server does not contact the Active Directory Server. | 126166 |
| A rule with an Expression element evaluated as NONE in the generated configuration might be evaluated differently by policy validation. | 126212 |
| Full database replication (automatic and manual) in a high-availability Management Server environment fails in Windows. | 126226 |
| Importing Network elements (Host, Networks and Address Ranges) from a CSV (comma-separated value) file or a TSV (tab-separated value) file fails. The following message is shown: "Failed to read import <file> Details: Import failed." | 126356 |
| Policy installation with a new custom Application element created might fail with the message “Invalid situation parameters". | 126390 |
| A null cipher algorithm is not included in a VPN configuration for an engine with a Russian license. | 126675 |
| Restoring or comparing policy snapshots might fail. The database message shown includes the information "Failed to read import xported_data.xml". | 126719 |
| A policy installation validation warning referring to rule tag @260036.0 is shown even if anti-malware Add-Ons are not enabled in the properties of the Firewall element or no Access rule has file filtering enabled. | 126882 |
| A custom Situation with BrightCloud Categories as the Situation Type prevents the installation of a policy. The installation fails with the message "Failed to build common configuration". | 126922 |
| If you update thousands of elements by running the sgImport.sh\|bat script this consumes too much memory. As a result, the Management Server becomes unresponsive and logon to the Management Client fails. | 127324 |

# Installation instructions

Use these high-level steps to install SMC and the Stonesoft NGFW engines.

For detailed information, see the *McAfee 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.

- *McAfee 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.
- *McAfee Next Generation Firewall Installation Guide*

Other available documents include:

- *McAfee Security Management Center Appliance Quick Start Guide*
- *McAfee Security Management Center Appliance Hardware Guide*
- *McAfee Next Generation Firewall Quick Start Guide*
- *McAfee Next Generation Firewall Hardware Guide* for your model
- *McAfee SMC API Reference Guide*
- *McAfee VPN Client User Guide* for Windows or Mac
- *McAfee VPN Client Product Guide*