Release Notes

Revision A

McAfee Security Management Center 5.10.0

McAfee Next Generation Firewall

Contents

About this release

This document contains important information about the current release of McAfee® Security Management Center (SMC). We strongly recommend that you read the entire document.

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.

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)

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_45.

Build version

SMC 5.10.0 build version is 10024.

This release contains Dynamic Update package 707.

Product binary checksums

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

- smc_ 5.10.0.10024.iso

  ```
  SHA1SUM:
  37ab6aa1f70d6fbc7c745ce16a1a3333c5500e63

  SHA512SUM:
  9895cc7a643d49f5cc549eb5d8d7fdf8
  3c882a7de6ee88c1105d5a7508889732
  13284919deb3f202f3d014ddf0c5f09e
  4c90d6c22b7f8492e63e0d0d376191c7
  ```

- smc_ 5.10.0.10024.zip

  ```
  SHA1SUM:
  2b98b12f981de9c68458f9d61dd0a18488ac9b5d

  SHA512SUM:
  758376bf945105f9f78d068a3bbcecf4
  ad7117ee48a6d09fd174bda7cc5939a4
  aae1bf016b3a2160faf77c84625df545
  cd2c2d55ed48df6a2ca0808a253a5a0a
  ```

- smc_ 5.10.0.10024_linux.zip

  ```
  SHA1SUM:
  e28564606a37268cfd03a0371abe3929270441aa

  SHA512SUM:
  107713ca8f415e6722dad1d0466abb1a
  96219f864eb696f2b351d476473dfdf5
  0d774acd3a1c5e59698e292536b81f7e
  9fe5059d979d6e38049c0ba22265db2a
  ```

- smc_ 5.10.0.10024_windows.zip

  ```
  SHA1SUM:
  53543c52ca014c43b0ccf3ee72fdb21ac4ceae94

  SHA512SUM:
  60d30c6b7f3e76785952caacd56f2c06
  56dbf8a4283d4fa1334c4a7d0aa6f2da
  dbec8d473e1352b0706b27c363416dd8
  e6348d71c911b207de19385d479d75fb
  ```

- smc_ 5.10.0.10024_webstart.zip

  ```
  SHA1SUM:
  e91eabbbcc6b75a7e95847f7db4ce0d285abef77

  SHA512SUM:
  23655090a656d8d380faa4cb97e25cec
  b69b56a618c8a987bdf4016c7dc55d11
  90475b0bc4bb2dcd06147bdaf8d7a60d
  fd85ec3431aac29db9243bc676a285cd
  ```

Compatibility

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

Minimum component versions

SMC 5.10.0 is compatible with the following McAfee and Stonesoft 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, McAfee NGFW 5.10 is required.

New features

This release of the product includes these new features.

SMC Appliance

This release adds support for the McAfee® Security 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

McAfee 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 McAfee 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 McAfee 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

McAfee 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 McAfee 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 SMC 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 security 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 McAfee NGFW appliances that have an integrated switch (currently McAfee 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.

Advanced Threat Defense communication logging improvements

Improvements have been made to the communication protocol and logging features between McAfee® Advanced Threat Defense and McAfee NGFW. McAfee NGFW now logs the dynamic analysis results when available from Advanced Threat Defense. McAfee NGFW provides the file name, destination IP address, and URL details when sending the file to 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.

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.

- In an SMC high availability setup, the Management Server might fail to start if a server is unavailable for an extended time period. This happens when the queue for sending policies with Correlation Situations to the Log Server becomes full. (1048623)
- The BGP configuration does not support configuring route-maps for redistribution, but route-maps configured for redistribution can be added to the engine configuration. (1072593)
- A change to the User DB replication setting in the engine options is lost when saved later in the Engine Editor. (1084066)
- The Engine Editor allows you to modify the VPN Automatic Site, but saving the changes reverts to the default Automatic Site. Deselect the "Add and update IP addresses based on routing" option before manually changing the VPN Automatic Site. (1088000)
- Overviews that include items "by interface," such as "Allowed traffic by interface," can show Tunnel Interface 8191, even when no Tunnel Interface has been configured. (1090222)
- Removing a Master Engine might fail with the error message "Database problem" shown. (1095469)

- After upgrading SMC 5.7 or earlier to 5.9, deleting IP addresses or interfaces in Engine Editor might fail. The following database error message is shown when you save the changes: "Failed to save Firewall <name> The element is invalid for the operation being performed." (1096038)
- After upgrading the SMC, logging on to the Management Client might fail without an error if the administrator has a startup session bookmark to a view that does not exist in the new SMC version. (1102836)
- The automatic task **Delete Old Snapshots** might fail to run and an alert is generated. This can occur after an upgrade to SMC 5.9.2 or later. (1103407)
- When the search criteria include a single parenthesis, the search or type-ahead search fails with the error "Internal Error Search failed. Incorrect parameters." When the search criteria include a wildcard, the search or type-ahead search has no results. (1105018)
- Policy installation on firewalls that have a dynamic IP address set for the Control Interface might fail with the error message "Upload Failure: Element is locked (Policy Upload)" shown. The failure is more likely to happen with a large policy and many managed engines. (1105603)
- After an upgrade in an environment with multiple Management Servers, a management database replication error might be shown soon after a successful manual database synchronization. Even though replication works, the error might be shown again shortly. (1106711)
- VPN Client configuration might not include VPN endpoint contact address. (1107136)

Installation instructions

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

For detailed information, see the *McAfee Next Generation Firewall Installation Guide*. All guides are available for download at https://support.mcafee.com.

The sgadmin user is reserved for McAfee use on Linux, so it must not exist before SMC is installed for the first time.

Task

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.

> McAfee 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 McAfee 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 5.2.0–5.9.3 before upgrading to 5.10.

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.

Task

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 McAfee product has a comprehensive set of documentation.

- *McAfee Next Generation Firewall Product Guide*
- McAfee Next Generation Firewall online Help

> By default, the online Help is used from the McAfee 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*