NGFW Security Management Center Appliance

6.9.1

Release Notes

Revision B

Contents

About this release

This document contains important information about this software release for the Forcepoint NGFW Security Management Center Appliance (SMC Appliance). We strongly recommend that you read the entire document.

The SMC Appliance ships with pre-installed Forcepoint NGFW Security Management Center (SMC) software. The pre-installed SMC includes a Management Server and a Log Server. You can alternatively install the SMC Appliance software on a virtualization platform.

Note

The SMC Appliance does not support high-availability for the Management Server or the Log Server.

Build number and checksums

The build number for SMC 6.9.1 is 11013. This release contains Dynamic Update package 1321.

Use checksums to make sure that files downloaded correctly.

- 6.9.1U001.sap

```
SHA1SUM:
25d0fc5cb43354f619648267d192a6759b9caea1

SHA256SUM:
e57f56aa31f021722fc6c5546b3e3317362e6cfecd32134c877195137aa4c20a

SHA512SUM:
86c39b7ad14bd46ec6e6eec777d73906
ad2a9ab37047acbfd4ea19b673567cac
d1c2d1f77925e136032dc299b66205b5
1d662543eeb8f8482f49120bf5c271ee
```

System requirements on virtualization platforms

As an alternative to using the SMC Appliance software on the pre-installed Forcepoint appliance, you can install the SMC Appliance software on a virtualization platform.

CAUTION

To protect the privacy of your data, we recommend installing the NGFW Engines, SMC components, or SMC Appliance on a hypervisor that does not host any other virtual machines.

Component	Requirement
Hypervisor	VMware ESXi version 6.0 or higher
Memory	8 GB RAM
Virtual disk space	120 GB
Interfaces	At least one network interface

The .iso installation file that is used to install the SMC Appliance software on a virtualization platform is available only for major versions of the SMC Appliance. To install the maintenance version, first install the .iso for the major version, then upgrade to the maintenance version.

Compatibility

SMC 6.9 can manage all compatible Forcepoint NGFW Engine versions up to and including version 6.9.

Important

Some versions of Forcepoint NGFW have reached end-of-life status and no longer receive maintenance releases that contain security updates. Even though these Forcepoint NGFW versions might be compatible with the SMC, we recommend that you use a Long-Term Support version that is still supported. For more information about the Forcepoint NGFW lifecycle policy, see https://support.forcepoint.com/ProductSupportLifeCycle.

SMC 6.9 is compatible with the following component versions.

- Forcepoint Next Generation Firewall (Forcepoint NGFW) 6.3 or higher
- McAfee ePolicy Orchestrator (McAfee ePO) 5.10 or higher

  Important

  SMC 6.9 is the last version of the SMC that is compatible with McAfee ePO. Features that depend on McAfee ePO, such as McAfee® Threat Intelligence Exchange (TIE) and McAfee® Data Exchange Layer (DXL) integration, will no longer be available in the next major release of the SMC.
- McAfee Enterprise Security Manager (McAfee ESM) 11.1.x or higher

New features

This release of the product includes these new features. For more information and configuration instructions, see the *Forcepoint Next Generation Firewall Product Guide* and the *Forcepoint Next Generation Firewall Installation Guide*.

Elasticsearch integration for high performance logging and reporting

Elasticsearch is an open-source search engine that runs on an external Elasticsearch server cluster. You can now forward log data from Log Servers and Management Servers to an Elasticsearch cluster to improve the performance of browsing and searching for log entries, report generation, and other log-related features. You can browse log entries that have been forwarded to an Elasticsearch cluster using the Management Client in the same way as for other log entries.

Important

Forwarding log data to an Elasticsearch cluster is an advanced feature that requires knowledge of how to configure Elasticsearch. You must already have an Elasticsearch cluster deployed and configured in your environment.

For information about the requirements for using Elasticsearch with the SMC, see Knowledge Base article 17583.

Documentation changes

This release of the product includes the following changes to the product documentation:

- The NGFW product documentation is no longer included in the SMC installation files. To find documentation for all Forcepoint products, go to the Forcepoint support website at https://support.forcepoint.com.
- The SMC installation files now include automatically generated change log reports for the SMC API in the api_change_log.zip file in the Documentation/SMC_API folder.
- The title of the *Forcepoint NGFW SMC API Reference Guide* has been changed to *Forcepoint NGFW SMC API User Guide*.

Enhancements

This release of the product includes these enhancements.

Enhancements in SMC version 6.9.0

Enhancement	Description
Configuration of bidirectional forwarding detection using the Management Client	Forcepoint NGFW Engine previously supported the configuration of bidirectional forwarding detection (BFD) using command line tools on the NGFW Engine. You can now configure BFD using the Management Client. When you use the BGP protocol for dynamic routing, you can optionally use BFD to detect neighbor failures. The NGFW Engine sends packets at the specified interval and waits for a reply. If the NGFW Engine does not receive a reply within the specified length of time, the neighbor is considered to have failed.
Improved performance for policy installation	The performance of policy installation has been improved. Policy installation is now faster and requires less memory.
New Management Client look-and-feel	The look-and-feel of the Management Client has been updated to reflect the new Forcepoint brand identity.
Option to generate one report per sender	When you generate reports, you can now generate one report for each NGFW Engine that is detected as a sender of log data. A new option in the Engine Editor allows you to define the default email addresses to which generated reports are sent when the NGFW Engine is the sender of log data for the report.
Password policy enhancements	The settings for password complexity requirements in the password policy now also apply to SMC administrator accounts that are replicated as local administrator accounts on NGFW Engines, the root account on NGFW Engines, and the Management Server database password.
Resource monitoring for SMC servers and the Management Client	The **Info** pane for Management Servers, Log Servers, and Web Portal Servers now shows information about resource usage on the computers where the servers are installed. The bottom right corner of the Management Client window shows the memory usage of the Management Client. If the memory usage gets too high, the Management Server, Log Server, Web Portal Server, or the Management Client automatically restarts. When the server or the Management Client restarts, an alert and an audit entry are generated. You can optionally disable automatic restart.
SMC HA Administration for Log Servers	In a high availability (HA) environment with multiple Log Servers, information about the Log Servers now also appears in the SMC HA Administration dialog box (formerly Control Management Servers dialog box). Previously, this dialog box only allowed you to control how the Management Servers function in an HA environment.

Resolved and known issues

For a list of resolved and known issues in this product release, see Knowledge Base article 19276.

Install the SMC Appliance

Use these high-level steps to install the SMC Appliance.

For detailed information about installing the SMC Appliance and the NGFW Engines, see the *Forcepoint Next Generation Firewall Installation Guide*. All guides are available for download at https://support.forcepoint.com/Documentation.

Steps

1) Turn on the SMC Appliance.

2) Select the keyboard layout for accessing the SMC Appliance on the command line.

3) Accept the EULA.

4) Enter the account name and password.
   For credential requirements, see the *Forcepoint Next Generation Firewall Installation Guide*.

5) Make your security selections.

6) Complete the network interface and network setup fields.

7) Enter a host name for the Management Server.

8) Select the time zone.

9) (Optional) Configure NTP settings.

10) After the SMC Appliance has restarted, install the Management Client.
    As an alternative to installing the Management Client locally, you can use SMC Web Access to start and run the Management Client in a web browser. SMC Web Access is enabled by default for new installations of the SMC Appliance.

11) Import the licenses for all components.
    You can generate licenses at https://stonesoftlicenses.forcepoint.com.

12) Create the NGFW Engine elements, then install and configure the NGFW Engines.

Upgrade the SMC Appliance

Use an upgrade patch to upgrade the SMC Appliance from a previous version to version 6.9.1.

There are two kinds of SMC Appliance patches:

- Hotfix patches include improvements and enhancements for the current SMC Appliance version.
  Hotfix patch files use the letter P as a separator between the version number and the patch number. Example: 6.9.1P001
- Upgrade patches upgrade the SMC Appliance to a new version.
  Upgrade patch files use the letter U as a separator between the version number and the patch number. Example: 6.9.1U001

We recommend checking the availability of SMC Appliance patches regularly, and installing the patches when they become available. For detailed information about installing SMC Appliance patches, see the *Forcepoint Next Generation Firewall Installation Guide*.

- SMC 6.9 requires an updated license.
  - 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.
- The SMC Appliance must be upgraded before the NGFW Engines are upgraded to the same major version.
- You can upgrade from the following SMC versions:
  - 6.4.7 – 6.4.10
  - 6.5.1 – 6.5.18
  - 6.6.0 – 6.6.5
  - 6.7.0 – 6.7.5
  - 6.8.0 – 6.8.4
  - 6.9.0
- If you configured SNMP for the SMC Appliance before upgrading to version 6.4.0 or higher, you must configure SNMP again.

You can upgrade the SMC Appliance using the Management Client or using the appliance maintenance and bug remediation (AMBR) patching utility on the command line of the SMC Appliance.

Note

In SMC version 6.9.0 and higher, the default path to the installation of xvfb-run for SMC Web Access is set to /usr/bin, and you cannot change the path using the Management Client.

If you use SMC Web Access on a Management Server or Web Portal Server installed on a Linux platform and need to change the path to the installation of xvfb-run, edit SGConfiguration.txt or WebPortalConfiguration.txt and add the following parameter:

```
XVFB_RUN_DEFAULT_PATH=<path>
```

Replace `<path>` with the path to the installation of xvfb-run.

Upgrade the SMC Appliance in the Management Client

You can use the Management Client to upgrade the SMC Appliance. In some certified environments, you must use the Management Client to install SMC Appliance patches.

Steps

For more details about the product and how to configure features, click **Help** or press **F1**.

1) Start the Management Client.

2) Select **Configuration**, then browse to **Administration**.

3) Browse to **SMC Appliance Patches**.

4) Download or import the 6.9.1U001 patch file.
   - To download the 6.9.1U001 patch using the Management Client, right-click the 6.9.1U001 patch, then select **Download SMC Appliance Patch**.
   - If you manually downloaded the 6.9.1U001 patch, right-click **SMC Appliance Patches**, select **Import SMC Appliance Patches**, browse to the 6.9.1U001 patch file, then click **Import**.

5) Right-click the 6.9.1U001 patch file, then select **Activate**.

6) (Optional) To allow administrators to start and run the Management Client in a web browser, enable the SMC Web Access feature after the upgrade is complete.

   a) Log on to the SMC Appliance.

   b) To enable the SMC Web Access feature, enter the following command:

   ```
   sudo /usr/local/forcepoint/smc/bin/sgActivateWebswing.sh
   ```

   c) When prompted, enter your SMC user credentials.

   When the configuration is complete, administrators can start and run the Management Client in a web browser.

Upgrade the SMC Appliance on the command line

You can use the AMBR patching utility to patch or upgrade the SMC Appliance on the command line.

Steps

1) Log on to the SMC Appliance.

2) To check for available upgrade patches, enter the following command:

```
sudo ambr-query -u
```

3) To load the patch on the SMC Appliance, enter the following command:

```
sudo ambr-load 6.9.1U001
```

If you downloaded the patch and transferred it to the SMC Appliance, append the load command with the `-f` option and specify the full path to the patch file. Example:

```
sudo ambr-load –f /var/tmp/6.9.1U001.sap
```

4) To install the patch on the SMC Appliance, enter the following command:

```
sudo ambr-install 6.9.1U001
```

The installation process prompts you to continue.

5) Enter `Y`.

The installation process restarts the appliance and installs the patch. When the upgrade is finished, the appliance restarts. The appliance is now running SMC Appliance 6.9.1.

6) (Optional) To allow administrators to start and run the Management Client in a web browser, enable the SMC Web Access feature after the upgrade is complete.

a) Log on to the SMC Appliance.

b) To enable the SMC Web Access feature, enter the following command:

```
sudo /usr/local/forcepoint/smc/bin/sgActivateWebswing.sh
```

c) When prompted, enter your SMC user credentials.

When the configuration is complete, administrators can start and run the Management Client in a web browser.

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, release notes, Knowledge Base articles, downloads, cases, and contact information.

You might need to log on to access the Forcepoint support website. If you do not yet have credentials, create a customer account. See https://support.forcepoint.com/CreateAccount.

Product documentation

Every Forcepoint product has a comprehensive set of documentation.

- *Forcepoint Next Generation Firewall Product Guide*
- Forcepoint 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.

- *Forcepoint Next Generation Firewall Installation Guide*

Other available documents include:

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

Published 09 April 2021