Forcepoint

NGFW Security Management Center Appliance

6.10.13

Release Notes

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 6.10.13 is 11196. This release contains Dynamic Update package 1644.

Use checksums to make sure that files downloaded correctly.

■ 6.10.13 U001.sap

```
SHA1SUM:
3da57910b98499257304b259506519a949289ea5

SHA256SUM:
9d336b6bc33049bb07a189f4bd4cd8e6e5226f441f836a29972b8de4d914ef00

SHA512SUM:
f21f2158836fa78c80f330b5d67dcb10
2a6871f874aeda8f3e608a97ae3e32b3
b60e3149ac4f2770696b4ce9660598f0
44db48abe12cff7a801ed6846fa3fe26
```

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.

> **Note**
>
> From 6.10 version onwards, running SMC Appliance on a platform other than pre-installed Forcepoint appliance or on virtualization platform, requires an SMC license that includes 'Forcepoint NGFW Security Management Center Virtual Appliance' feature pack.

Component	Requirement
Hypervisor	VMware ESXi version 6.0 or higher
Memory	16 GB RAM
Virtual disk space	130 GB
Interfaces	At least one network interface

The .iso installation file that is used to install the SMC Appliance software on a virtualization platform may not be available for all maintenance versions of the SMC Appliance. To install the latest maintenance version, first install the latest available .iso version, then upgrade to the latest maintenance version.

Compatibility

SMC 6.10 can manage all compatible Forcepoint NGFW Engine versions up to and including version 6.10.

> ⚠️ **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 6.10 is compatible with the following component versions.

- Forcepoint Next Generation Firewall (Forcepoint NGFW) 6.8 or higher
- 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*.

External CA issued certificates in internal management communication

Starting with SMC version 6.10.4, when you install a new SMC, you can now use certificates issued by an external CA instead of certificates generated by the internal CA on the Management Server for internal TLS communication between NGFW Engines and SMC components.

Snort inspection on NGFW Engines

The Snort network intrusion detection system and intrusion prevention system has been integrated into Forcepoint NGFW. You can import externally created Snort configurations into Forcepoint NGFW to use Snort rules for inspection.

You can configure Snort inspection globally for all NGFW Engines, or for individual NGFW Engines. You can use both NGFW deep inspection and Snort inspection for the same traffic, or you can use only NGFW deep inspection or only Snort inspection.

Enhancements

This release of the product includes these enhancements.

Enhancements in SMC version 6.10.0

Enhancement	Description
SMC Appliance operating system upgrade	The SMC Appliance operating system has been upgraded to a new major version.
Exact values in exported reports	You can now use exact values instead of rounded values when you export reports as tab-delimited text files. To use exact values in reports, set the value of the TXT_REPORT_RAW_VALUES parameter to true. For reports exported using the Management Client, set the parameter in the SGClientConfiguration.txt file. For reports exported on the Management Server, set the parameter in the SGConfiguration.txt file.
Improved SD-WAN monitoring	The performance of SD-WAN monitoring has been improved. New options for SD-WAN monitoring have also been introduced. ■ The performance of SD-WAN monitoring in the Home view has been improved. ■ The performance of branch connectivity monitoring has been improved. ■ Branch connectivity diagrams have been enhanced. The diagram now includes shortcuts that zoom in on specific world regions on the map. ■ The Tunnels pane of branch home pages and VPN home pages can now show the status of either individual tunnels between endpoints or an aggregate status of all tunnels between gateway pairs. Previously, the Tunnels pane only showed the status of individual tunnels between endpoints. ■ A new VPN gateways pane that summarizes the status of the Gateways in the VPN has been added to the VPN home pages. The previous VPN gateway diagram pane is still available but it is not shown by default.
OWASP encoding in SMC API responses	There is a new option in the SMC installer to enable OWASP encoding for the SMC API. When the option is enabled, the SMC API uses the OWASP encoder in responses. Using the OWASP encoder reduces the risk of cross site scripting (XSS) attacks. This option is especially useful if you use the SMC API to generate HTML pages that are shown in a browser. **Note** When you enable this option, some strings in data returned by the SMC API, such as special characters inside JSON payloads, are also encoded. We recommend enabling this option only if you use the SMC API in a web browser.
SHA-256 support for NTP servers	You can now configure NTP Server elements to use SHA-256 authentication keys.

Enhancement	Description
Warning about timeout when importing elements	On the progress tab for importing elements, a warning message is now shown when the default timeout for resolving conflicts between elements in the import file and existing elements is about to be reached. By default, the timeout is 15 minutes. You can optionally change the timeout using the CONFLICT_RESOLVING_OPERATION_TIMEOUT_MINUTES=<number of minutes> parameter in the SGConfiguration.txt in the SGHOME/data directory on the Management Server.

Enhancements in SMC version 6.10.3

Enhancement	Description
Rule hit counters for sub-policies	You can run a rule counter analysis for a sub-policy regardless of which main policy refers to it or which NGFW Engine the policy is installed on.

Enhancements in SMC version 6.10.7

Enhancement	Description
Policy install without policy snapshot	With new Management Client, you can select options to not create policy snapshot during policy install. This is done by adding `POLICY_SNAPSHOT_CONFIGURATION=true` in the `SGClientConfiguration.txt`. The location of the file depends on the installation type of Management Client. For locally installed Management Client and standalone Management Client: ■ Edit the `<user_home>/.stonegate/SGClientConfiguration.txt` file on the client computer. ■ Edit the `<smc_installation_folder>/data/SGClientConfiguration.txt` file on the Management Server.

Enhancements in SMC version 6.10.8

Enhancement	Description
Visualization and filter elements edition support in SMC API	Filter elements can now be edited using SMC API. For more information, see Knowledge Base article 41241
A new option is introduced in Export Elements tool	Export elements tool in Management Client has a new option, **Include references**. By default this option is selected; however, when unselected export is done without referenced elements.
A new Logon option has been introduced in **Global System Properties** dialog box	A new Logon option, **Administrator User Name is Case Insensitive** has been introduced in **Global System Properties** dialog box. When this option is enabled, SMC considers administrator user account names of type "Linked to LDAP" as lowercase, regardless of how they are stored in the LDAP server.

Enhancement	Description
New option to force engine upgrade through SMC API	Remote upgrade through SMC API might be blocked with a warning, thereby preventing an upgrade. In such scenarios, a `force_upgrade` option is added for SMC API to perform an upgrade. For example, upgrade from NGFW version 6.3.3 to 6.8.8 using API.

Security enhancements

For a list of security enhancements in this product release, see Knowledge Base article 38434.

Resolved and known issues

For a list of resolved and known issues in this product release, see Knowledge Base article 38461.

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/s/article/Documentation-Featured-Article.

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 and set DNS servers.

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 6.10.13.

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: 6.10.1P001

- 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: 6.10.1U001

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 6.10 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.

    - From 6.10 version onwards, running SMC Appliance on a platform other than pre-installed Forcepoint appliance or on virtualization platform, requires an SMC license that includes 'Forcepoint NGFW Security Management Center Virtual Appliance' feature pack.

- 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. For detailed information on how to upgrade SMC Appliance to a new version, see *Forcepoint Next Generation Firewall Installation Guide*.

    - 6.8.6 – 6.8.15

    - 6.9.2 – 6.9.3

    - 6.10.4

    - 6.10.9

    - 6.10.10 – 6.10.12

    For SMC Appliance versions prior to 6.8.6, see Knowledge Base article 41318 for detailed information on how to upgrade SMC Appliance to a new version.

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. For detailed information, see *Forcepoint Next Generation Firewall Product Guide*.

Upgrade notes

- SMC version 6.9 was the last version of the SMC that was compatible with McAfee ePO. Features that depend on McAfee ePO, such as McAfee Threat Intelligence Exchange (TIE) local file reputation sandbox and McAfee® Data Exchange Layer (DXL) local file reputation, are no longer available in SMC 6.10 and higher.

- SMC version 6.10.2 and higher no longer supports TLS 1.0 and TLS 1.1 by default. To use TLS 1.0 and TLS 1.1 for communication with external services, you must manually enable support for these TLS versions. For more information, see Knowledge Base article 38624.

> **Note**
>
> For security reasons, we recommend that you upgrade your external services to use TLS versions higher than 1.1 as soon as possible. Enabling support for TLS 1.0 and TLS 1.1 is intended as a temporary workaround until all external components are upgraded so that the existing environment is not disrupted.

Find product documentation

In the Forcepoint Customer Hub, 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 in the Forcepoint Customer Hub 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 Customer Hub. 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*
- *Forcepoint VPN Client User Guide* for Windows or Mac
- *Forcepoint VPN Client Product Guide*

- *Forcepoint NGFW Manager and VPN Broker Product Guide*