Forcepoint

NGFW Security Management Center

6.8.1

Release Notes

Revision B

Contents

About this release

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

System requirements

To use this product, your system must meet these basic hardware and software requirements.

SMC hardware requirements

You can install the SMC on standard hardware.

Component	Requirement
CPU	Intel® Core™ family processor or higher recommended, or equivalent on a non-Intel platform
Disk space	■ Management Server: 6 GB ■ Log Server: 50 GB

Component	Requirement
Memory	■ Management Server, Log Server, Web Portal Server: 6 GB RAM ■ If all SMC servers are on the same computer: 16 GB RAM ■ If you use the SMC Web Access feature: an additional 2 GB RAM per administrator session ■ Management Client: 2 GB RAM The SMC server requirements are the *minimum* requirements. The Management Server and Log Server in particular benefit from having more than the minimum amount of RAM. On high-end appliances that have a lot of RAM, the SMC might not provision the maximum amount of RAM for use by the SMC servers. For information about how to manually modify the provisioning, see Knowledge Base article 10016.
Management Client peripherals	■ A mouse or pointing device ■ SVGA (1024x768) display or higher

CAUTION

To protect the privacy of your data, we recommend using dedicated hardware for all NGFW, SMC, and SMC Appliance installations. For cloud-based virtualization platforms, use an instance type that runs on dedicated hardware. For on-premises virtualization platforms, install the NGFW Engines, SMC components, or SMC Appliance on a hypervisor that does not host any other virtual machines. For third-party hardware, do not install any other software on the computer where you install the NGFW Engines or SMC components.

Operating systems

You can install the SMC on the following operating systems. Only 64-bit operating systems are supported.

Linux	Microsoft Windows
■ CentOS 7 and 8 ■ Red Hat Enterprise Linux 7 and 8 ■ SUSE Linux Enterprise 12 and 15 ■ Ubuntu 16.04 LTS and 18.04 LTS	Standard and Datacenter editions of the following Windows Server versions: ■ Windows Server 2019 ■ Windows Server 2016 ■ Windows Server 2012 R2 On Windows 10, you can install the SMC in demo mode. You can also install the Management Client.

We recommend that you only use operating system versions that are currently supported by the vendor.

Other versions of the listed operating systems might be compatible, but have not been tested. Only U.S. English language versions of the listed operating systems have been tested, but other locales might also be compatible.

Build number and checksums

The build number for SMC 6.8.1 is 10911. This release contains Dynamic Update package 1267.

Use checksums to make sure that files downloaded correctly.

- smc_6.8.1_10911.zip

```
SHA1SUM:
a56d320443e996670733ac5a6fc88e6d62c6a53b

SHA256SUM:
64d66d3a7db7a17c5c8ef009047b34bf879bc204eee8027031b7066217f30a4c

SHA512SUM:
e0fd91bf0a6a5d14a70b66c1e627b4ed
e0b626078a0d28a2bd660dd26fb555a3
41b4b74ebc169f22fd2857a0ffe24102
80383d3713e86c72ccc9f332af024ac3
```

- smc_6.8.1_10911_linux.zip

```
SHA1SUM:
baa8900290ead15b5db558fdfe9bc38721ab07f8

SHA256SUM:
5ee2038bda9136489a888e3568d14f5793138e75542e6db15f8c0e352c6d9110

SHA512SUM:
3f6fc78480ccfaa665a46c0e74369e1c
ee950201aa624e704cc9523a430dcc6c
52b195b9f492b565d86dc503c0a127f7
ebfafb348cecac5c72b52d509fa040a2
```

- smc_6.8.1_10911_windows.zip

```
SHA1SUM:
0c212aae30097200be4cc2a35d1a18b61ff686c8

SHA256SUM:
9e403b8c2d91c5dff61aaf3ea0ee15bd4352c142f78ecac9975f10d2aef281fa

SHA512SUM:
a5da0ffe2fd4376c7f7ad45140b95851
49ebc7a64f75cde7be59c2709a459c1e
bedf223185f8f9b6d2834dbc639bb21f
9858c46a7444dc247b5eb9b68c84b784
```

Compatibility

SMC 6.8 can manage all compatible Forcepoint NGFW Engine versions up to and including version 6.8.

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 6.8 is compatible with the following component versions.

- Forcepoint Next Generation Firewall (Forcepoint NGFW) 6.3 or higher
- McAfee Next Generation Firewall (McAfee NGFW) 5.10
- Stonesoft Firewall/VPN Express 5.5
- McAfee ePolicy Orchestrator (McAfee ePO) 5.3 or higher
- McAfee Enterprise Security Manager (McAfee ESM) 9.2.0 or higher (9.1.0 CEF only)

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*.

UIID license binding for SMC licenses

When you install the SMC or upgrade the SMC to version 6.8, the SMC generates a Unique Installation Identifier (UIID). As an alternative to binding licenses for SMC components to the IP addresses of the components, you can now bind the SMC licenses to a UIID. Using UIID binding allows organizations to obtain SMC licenses without disclosing the internal IP addresses of the SMC components.

Note

The UIID is not stored in SMC backups or restored when you restore a backup. After the UIID is generated, it will not be overwritten when you restore backups or upgrade the SMC in the future.

You can continue to use your existing licenses or optionally change the license binding method. You can use IP-address-bound licenses for some SMC components and UIID-bound licenses for other SMC components.

Management Client downloads from the Management Server

Java Web Start is no longer supported in SMC 6.8. As an alternative, you can now configure the Management Server to provide the Management Client installation files on a download web page hosted by the Management Server. Administrators download and install the Management Client from the locally hosted SMC Downloads web page.

Note

Management Client downloads are not supported for macOS in SMC 6.8. For administrators who use macOS, we recommend using the SMC Web Access feature.

Enhancements

This release of the product includes these enhancements.

Enhancements in SMC version 6.8.0

Enhancement	Description
Easier configuration of dynamic link selection for NGFW Engines	It is now possible to select Link Usage Profile elements for NGFW Engines in the Firewall/VPN role to define which link types are preferred, avoided, or not used for specific types of outbound Multi-Link traffic. NGFW Engine-specific exceptions to the Link Usage Profile also allow you to specify which traffic uses specific NetLinks.
Re-authentication when using browser-based user authentication	If an end user has authenticated using browser-based user authentication and the session will soon expire, the user can re-authenticate to extend the authentication time-out and avoid connections closing before the user has finished their tasks.
Custom script upload for NGFW Engines when using Custom Properties Profile elements	To upload custom scripts to the NGFW Engine, you can add the scripts to the properties of the NGFW Engine using a Custom Properties Profile element. The scripts are uploaded when the policy is installed or refreshed.
Expiration time for one-time passwords	You can now set the expiration time for one-time passwords that are generated when you save the initial configuration for an NGFW Engine. If the one-time password is not used, it automatically expires after the expiration time has elapsed. By default, one-time passwords expire after 30 days.
PPPoE support on VLAN interfaces	You can now configure point-to-point protocol over Ethernet (PPPoE) for dynamic IP addresses that are assigned to VLAN interfaces.
User domain support for integrated ICAP servers for DLP	NGFW integration with external ICAP servers for DLP now uses the WinNT schema in the X-Authenticated-Users header instead of the Local schema that was used previously. Using the WinNT schema allows matching users against a user domain in the user directory on the ICAP server.

Enhancements in SMC version 6.8.1

Enhancement	Description
More granular identification of Microsoft Office 365 network applications	Starting from dynamic update package 1300, the Microsoft-Office-365 Network Application element includes dependencies that allow more granular identification of Microsoft Office 365 in traffic. No action is required if you use the Microsoft-Office-365 Network Application element in the following types of rules: ■ Access rules with the Allow, Discard, Refuse, or Jump action ■ NAT rules If you use the Microsoft-Office-365 Network Application element in an access rule with the Continue action, you must manually add the Network Application elements that are listed as dependencies. Options that are configured in a rule with the Continue action are not automatically applied to dependencies. For more information, see Knowledge Base article 19195.

Resolved issues

These issues are resolved in this release of the product. For a list of issues fixed in a previous release, see the Release Notes for the specific release.

Description	Issue number
In an environment with multiple Management Servers, the active Management server might be shown as isolated from database replication due to "file system failure" after the connection to another Management Server has failed. After the connection has been restored, replication does not recover automatically.	SMC-23634
The Convert Engine to Master NGFW Engine and Virtual NGFW Engines wizard fails to apply changes on the "Define Interface for the Master NGFW Engine" page when you try to assign multiple interfaces to a Virtual Resource at the same time.	SMC-28595
When you create custom Situation elements, the elements might be shown in the Management Client by the situation ID only.	SMC-28617
The first policy refresh after upgrading the SMC might fail.	SMC-28626
When you use SMC Web Access, manually saving a report as a PDF fails.	SMC-28631
For external tests, the path to the script file on the command line has a limit of 80 characters.	SMC-28639
In rare cases, normal logs might be sent as alerts.	SMC-28748
When the SMC API is used to add an IP address to an existing Virtual NGFW Engine interface, antispoofing is not configured correctly.	SMC-28781
It is not possible to remove an IPv4 DHCP server from an NGFW Engine interface.	SMC-28792
When you upload a policy on multiple NGFW Engines, the progress tab shows only the "operation finished" status.	SMC-29135

Description	Issue number
When you delete a Virtual NGFW Engine, the Master NGFW Engine might not be notified of the deletion. As a result, the policy of the Master NGFW Engine refers to a Virtual NGFW Engine that no longer exists and policy installation fails.	SMC-29306
Hardware monitoring incorrectly reports Half / Forced for an interface when the NGFW Engine does not provide data for send values for speed, duplex, and auto-negotiation. This issue occurs on interfaces where negotiation settings cannot be changed.	SMC-29310
When you create an inspection rule from a log entry, saving the policy fails and an "invalid element" error message is shown.	SMC-29317
The details are not always refreshed when you select different NGFW Engine nodes in the Home view.	SMC-29380
With a Master NGFW Engine, monitoring of routes does not work reliably during policy installation.	SMC-29497
Viewing or comparing snapshots might fail and the following error message might be shown: "Database problem. DB Transaction failed while processing transaction".	SMC-29529
Aliases for which no value has been defined are not visible in the Engine Editor. The Alias elements can still be edited outside of the Engine Editor.	SMC-29581
Expression elements might be incorrectly shown as having related sub-elements. This issue makes it difficult to edit the expressions.	SMC-29629
When the Log Server has been configured to forward log data in different formats to different external hosts, the Log Server might send log data in the wrong format for some hosts.	SMC-29701
When you configure host name for the SSL VPN Portal, host names that end with .ye are not accepted.	SMC-30353
When there is an empty Group element in the source or destination cell of a rule, the whole rule might be ignored even if there are other elements in the same source or destination cell.	SMC-30542

Installation instructions

Use these high-level steps to install the SMC and the Forcepoint NGFW Engines.

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

Note

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

Note

If you install the SMC on Windows and Windows Defender is enabled, it might take a long time to activate a dynamic update package. For more information, see Knowledge Base article 14055.

Steps

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://stonesoftlicenses.forcepoint.com.

3) Configure the Firewall, IPS, or Layer 2 Firewall elements in the Management Client from the **Configuration** view.

4) To generate initial configurations, right-click each NGFW Engine, then select **Configuration** > **Save Initial Configuration**.
   Make a note of the one-time password.

5) Make the initial connection from the NGFW Engines to the Management Server, then enter the one-time password.

6) Create and upload a policy on the NGFW Engines in the Management Client.

Upgrade instructions

Take the following into consideration before upgrading the SMC.

Note

The SMC (Management Server, Log Server, and Web Portal Server) must be upgraded before the NGFW Engines are upgraded to the same major version.

- SMC 6.8 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 in the Management Client before upgrading the software.
- To upgrade a lower version of the SMC to 6.8, we strongly recommend that you stop all SMC servers 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.
- When you upgrade the SMC, the dynamic update package that is included with the SMC installer is imported and activated. However, if a newer version of the dynamic update package has previously been imported or downloaded before the upgrade, the newest version is activated instead.
- You can upgrade from the following SMC versions:
  - 5.6.2 – 6.4.10
  - 6.5.0 – 6.5.16
  - 6.6.0 – 6.6.5
  - 6.7.0 – 6.7.4
  - 6.8.0

  Versions lower than 5.6.2 require an upgrade to one of these versions before upgrading to 6.8.1.
- Before upgrading, make sure that you have removed all elements related to McAfee Endpoint Intelligence Agent (McAfee EIA). Also remove all references in Access rules.

Known issues

For a list of known issues in this product release, see Knowledge Base article 18381.

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 Reference Guide*
- *Forcepoint VPN Client User Guide* for Windows or Mac
- *Forcepoint VPN Client Product Guide*

Published 04 December 2020