Forcepoint

NGFW Security Management Center

6.8.8

Release Notes

Revision A

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 18.04 LTS and 20.04 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.

Note

Ubuntu 16.04 LTS is no longer supported after 30 April 2021. If you use Ubuntu 16.04 LTS, upgrade the operating system before installing the SMC.

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 6.8.8 is 10942. This release contains Dynamic Update package 1385.

Use checksums to make sure that files downloaded correctly.

- smc_6.8.8_10942.zip

```
SHA1SUM:
4ad0734c182bb02abb7b0b877d08d828d71cadca

SHA256SUM:
9fd996ee826f3babccb66ad93ba14410edcd170ec8ccd91e9c366268116bf929

SHA512SUM:
c45a1ef4c4d8876d8b613fe70b9ff729
0e6eb1480565eaa68426033a5559e8e1
c0470507950437d61a32b70cee63fe6a
1fd03a2fc0a9c928f1ae75225cd35946
```

- smc_6.8.8_10942_linux.zip

```
SHA1SUM:
e1ea3a597a2853c20716092793de54a0fbbf86c3

SHA256SUM:
dc3f195bd8e24e79ba087581d170560fa1747b6dc9b2d25966290861184faf76

SHA512SUM:
934329e4d62847ef2251a149b4d41a33
660b8a2227c3c35d6fd4aca0db0e1730
d843f24cefc47053840cbf64555b70c4
22616704bcb77d6261352e9b8b24e2bf
```

- smc_6.8.8_10942_windows.zip

```
SHA1SUM:
c92cd66d4639b587ce4104bdf8548b71c3d26bc9

SHA256SUM:
77da4c2c5f0fef50828da09160971501ba8086cccabccc75c3857e54bf73521d

SHA512SUM:
e1b3ea274b2a2d7e399e98ecde5f6093
1c582fb884e794714eff3d7a8b5cac91
8f08799214cadb9a440ad2a1e85b33ba
e66cb2b2ad2b06bf69c6efef523d2c3b
```

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 6.8.2

Enhancement	Description
Configurable timeout for session monitoring	Previously, monitoring views might have failed to open when there were several backup Log Servers and the primary Log Server was unreachable. You can now define the timeout for receiving monitoring data from NGFW Engines. To define the timeout, edit the <installation folder>/data/SGConfiguration.txt file and add the following parameter: `SESMON_LOGSERVER_SELECTION_TIMEOUT=<timeout_in_milliseconds>` The default value is 20000.

Enhancements in SMC version 6.8.3

Enhancement	Description
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.
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.
New Log Server and Management Server configuration parameters	In the LogServerConfiguration.txt file, you can now add a new configuration parameter to recover connectivity from the Log Server to TCP syslog servers. For more information, see Knowledge Base article 19219. In the SGConfiguration.txt file, you can now add a new configuration parameter to define how many tasks the Management Server can run in parallel. For more information, see Knowledge Base article 19218.
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.

Enhancements in SMC version 6.8.4

Enhancement	Description
Optimization of status monitoring in large-scale SMC environments	New parameters for the Management Server and Log Server allow you to optimize the performance of status monitoring for NGFW Engines, VPNs, and NetLinks for SD-WAN in large-scale SMC environments. For more information, see Knowledge Base article 19285.

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
Setting the same dynamic NAT IP address for separate elements in element-based NAT causes a validation warning: "Dynamic NAT definitions that do not have a Port Filter defined have the same external IP address."	SMC-30184
Viewing or comparing snapshots fails and the following error message is shown: 'DTD claims: Element <smtp_server> has no attribute "ipv6_address"'. In the past, it was possible to add an IPv6 address to an SMTP Server element, but this option is no longer supported.	SMC-32148
Inspection policy validation does not treat situation tags the same as single situations or situation types.	SMC-37022
The Log Server might spend a lot of time processing active alerts, which can affect log reception.	SMC-38299
When you drag a VLAN interface that has DHCP configured to a different physical interface, the DHCP configuration is removed from the VLAN interface.	SMC-38404
When you convert a Firewall Cluster to a Master NGFW Engine and Virtual NGFW Engines, the link status test that is originally set for "ALL with CVI" interfaces is not converted and is ignored when a policy is installed on the Master NGFW Engine.	SMC-38645
The default memory heap size for the Management Client has been increased to 1524Mb.	SMC-38675
When an NGFW Engine node has a static IP address on the control interface, the Management Server does not verify the certificate of the node. For example, if an NGFW Engine running on a virtualization platform is reverted to an older certificate, the Management Server communicates with the NGFW Engine even though it expects a newer certificate.	SMC-38692
When you use the "Additional Networks to automatically add to antispoofing" option in the dynamic routing configuration, the exceptions to automatic antispoofing are not added to the generated NGFW Engine configuration.	SMC-38833
When you configure IPv6 policy routing, the routing configuration is not correctly generated in NGFW Engine configuration.	SMC-38968
When you use Route Map elements and you edit the dynamic routing configuration, there might be a conflict between the new Route Map element and the change history of the removed Route Map element.	SMC-38999
In the Situations view, the Last update column shows -1 for custom elements.	SMC-39037
Create a new Route Map element for dynamic routing fails. The following error message is shown: "Database problem. Impossible to store element".	SMC-39302
When an administrator whose Management Client window was locked because the session was idle for too long logs on again, the administrator can very briefly perform actions in the Management Client even if the incorrect password was entered.	SMC-39404
When you create new users in the InternalDomain LDAP domain, the "Member of" list is empty even though the user was correctly added to existing groups.	SMC-39490
In rare cases, duplicating an NGFW Engine element might fail with the following error message: "Failed to construct the alias values".	SMC-39553

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.

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 – 6.5.18
- 6.6.0 – 6.6.5
- 6.7.0 – 6.7.5
- 6.8.0– 6.8.7

Versions lower than 5.6.2 require an upgrade to one of these versions before upgrading to 6.8.8.

- 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.

Note

In SMC version 6.8.3 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, follow these steps:

1) On the Management Server or the Web Portal Server, edit the `SGConfiguration.txt` or `WebPortalConfiguration.txt` file.

2) Add the following parameter:

```
XVFB_RUN_DEFAULT_PATH=<path>
```

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

Note

If you use the SMC-Python library for interacting with the SMC API, you must upgrade the SMC-Python library to version 0.7.0b27 when you upgrade to SMC 6.8.4 or higher. To upgrade the SMC-Python library, see https://github.com/Forcepoint/fp-NGFW-SMC-python.

Known issues

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

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

Published 22 September 2021