



NGFW Security Management Center

6.8.3

Release Notes

Contents

- [About this release](#) on page 2
- [System requirements](#) on page 2
- [Build number and checksums](#) on page 4
- [Compatibility](#) on page 4
- [New features](#) on page 5
- [Enhancements](#) on page 6
- [Resolved issues](#) on page 8
- [Installation instructions](#) on page 9
- [Upgrade instructions](#) on page 10
- [Known issues](#) on page 11
- [Find product documentation](#) on page 11

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	<ul style="list-style-type: none">■ Management Server: 6 GB■ Log Server: 50 GB

Component	Requirement
Memory	<ul style="list-style-type: none"> ■ 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 <p>The SMC server requirements are the <i>minimum</i> requirements. The Management Server and Log Server in particular benefit from having more than the minimum amount of RAM.</p> <p>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.</p>
Management Client peripherals	<ul style="list-style-type: none"> ■ 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
<ul style="list-style-type: none"> ■ 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 	<p>Standard and Datacenter editions of the following Windows Server versions:</p> <ul style="list-style-type: none"> ■ Windows Server 2019 ■ Windows Server 2016 ■ Windows Server 2012 R2 <p>On Windows 10, you can install the SMC in demo mode. You can also install the Management Client.</p>

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 6.8.3 is 10916. This release contains Dynamic Update package 1298.

Use checksums to make sure that files downloaded correctly.

■ smc_6.8.3_10916.zip

```
SHA1SUM:
0c2972a71562370069689c6c7045884364f8546f

SHA256SUM:
8d86a8beed34717ca4fdbaac8288568c161e704a4fc77effc97192389b9b19e0

SHA512SUM:
be8fd1f57045c4842c06a8bd0ccaf091
b514e12d829d6027c56cc529482ed6f1
75aef069a1ac53c105797df2cd7d829d
294a8e99b02e19d6fde747ee615dcec0
```

■ smc_6.8.3_10916_linux.zip

```
SHA1SUM:
e5ab7116be0ae27a3d470f1291b64777a2280503

SHA256SUM:
f8bb32e2dced352ca7fa00cec339f643215c9afdea495a1b10419c910f7fb13c

SHA512SUM:
e37e915546c645ac6889c61e7440284b
2bf7de2a18c46a888e80cbf8f4f30959
bbd9774ebf89531fc14cca9752603914
23330be3194338e3290c7c746e9f57ce
```

■ smc_6.8.3_10916_windows.zip

```
SHA1SUM:
0e9f9db64923be703256bcdea90d9b921bfe967a

SHA256SUM:
9393953faeb4e827594696332f1b160cdbeb927b867d9005ed61180fd4cb4362

SHA512SUM:
f3603e784942789aab88fbb61db9460c
c5d3f29d1104161225969de3e2acbc07
bf0d049f99e00ee385acccc68787c24c
7a0ec6a55189f1d7989f508fa6e24f93
```

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*.

UUID 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 (UUID). 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 UUID. Using UUID binding allows organizations to obtain SMC licenses without disclosing the internal IP addresses of the SMC components.



Note

The UUID is not stored in SMC backups or restored when you restore a backup. After the UUID 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 UUID-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	<p>Previously, monitoring views might have failed to open when there were several backup Log Servers and the primary Log Server was unreachable.</p> <p>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:</p> <pre>SESMON_LOGSERVER_SELECTION_TIMEOUT=<timeout_in_milliseconds></pre> <p>The default value is 20000.</p>

Enhancements in SMC version 6.8.3

Enhancement	Description
Resource monitoring for SMC servers and the Management Client	<p>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.</p> <p>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.</p> <div>  <p>Important</p> <p>Due to changes introduced by this enhancement, customized heap size values for servers, the Web Portal, and Management Clients are not preserved when you upgrade to SMC version 6.8.3. You must modify your configuration if you previously changed the Java heap size of the Management Client using the MAX_HEAP_SIZE parameter in the sgClient.sh or sgClient.bat file. For more information, see the upgrade instructions.</p> </div>
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	<p>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.</p> <p>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.</p>
More granular identification of Microsoft Office 365 network applications	<p>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.</p> <p>No action is required if you use the Microsoft-Office-365 Network Application element in the following types of rules:</p> <ul style="list-style-type: none"> ■ Access rules with the Allow, Discard, Refuse, or Jump action ■ NAT rules <p>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.</p> <p>For more information, see Knowledge Base article 19195.</p>

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
When a Management Client session is closed due to the logon options in the password policy, the status of the administrator who was using the Management Client is still shown as connected.	SMC-28448
When the Log Server fails to start due to the disk being too full, the reason for the failure is not indicated to the administrator.	SMC-29175
When you export the Administrator Activity Summary report as a PDF, the report might show * in place of some characters.	SMC-30481
When you generate system reports for multiple SMC servers, sections that are normally combined might be printed on separate pages.	SMC-30537
In large SMC environments, the Management Server might not be able to process the status of all Log Servers. The status icons for the Log Servers appear gray.	SMC-30754
Scheduled backup tasks might fail to run at the scheduled time.	SMC-31362
If the names of custom Situation elements include the less than (<), greater than (>), or pipe () characters, snapshot comparison fails.	SMC-31444
When you export an NGFW Engine element as XML, route metrics are not included in the export.	SMC-31548
When you change the Interface for DHCP Relay setting for the VPN Client, the change does not appear in the policy snapshot.	SMC-31605
When you configure diagnostics settings for individual NGFW Engine nodes, the settings are not always saved.	SMC-31637
The rules in the default Firewall Template policy do not allow destination NAT using the public IP address of NGFW Engines deployed in the Azure cloud.	SMC-31711
When you convert an NGFW Engine that has an SNMP Agent configured to a Master NGFW Engine and Virtual NGFW Engines, the SNMP Agent is also configured for the Virtual NGFW Engines.	SMC-31736
If the connection between the NGFW Engine and the Log Server is unstable, session monitoring views might fail to open even when the NGFW Engine sends log data to the primary Log Server.	SMC-31898
When the SMC is installed in Linux, SMC server services might stop working due to a lack of threads even though the services are running.	SMC-31952
The Show Related Logs action does not work for rules in the Layer 2 Interface Policy.	SMC-31967
When VPN endpoints are enabled only for the SSL VPN Portal, the NGFW Engine might incorrectly try to use them to contact a VPN Broker gateway.	SMC-31980
When you start and stop Log Servers in an environment with a large number of Log Servers, NGFW Engines connect to different Log Servers. As a result, a Log Server might stop responding when a large number of NGFW Engines tries to connect to it because the Log Server has too many open files.	SMC-31983
The traffic capture tool might fail for some NGFW Engines. A long error message is shown.	SMC-32116

Description	Issue number
In an environment with multiple Management Servers, if you upgrade a standby Management Server before the active Management Server, the standby Management Server does not start after the upgrade.	SMC-32287
After you have moved Virtual NGFW Engines from one Master NGFW Engine to another, the Management Server might try to install the policy for the Virtual NGFW Engines on the old Master NGFW Engine.	SMC-32313
Management Server licenses that include the high availability feature cannot use UUID license binding.	SMC-32316
Filtering log entries in the Web Portal might fail. An error message is shown.	SMC-32317
Some actions related to log data, such as aborting the generation of a report or refreshing the statistics while they are loading, might cause the Log Server to show a false positive "Found inconsistent file" alert.	SMC-32595
Certificate-based authentication for administrators might fail. The following error message is shown: "Authentication failed. Internal error."	SMC-32893
In the Query panel of the Logs view, the options on the Storage tab do not include the "Default" option. The "Primary Archive" option refers to active log data.	SMC-33047
When you use two-factor authentication with the SSL VPN Portal, the timeout is too short and authentication might fail even if the user enters the correct credentials.	SMC-33130
In new installations of the SMC, the InternalDomain LDAP domain is not set as the default LDAP domain.	SMC-33270

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 – 6.5.18
 - 6.6.0 – 6.6.5
 - 6.7.0 – 6.7.5
 - 6.8.0 – 6.8.2

Versions lower than 5.6.2 require an upgrade to one of these versions before upgrading to 6.8.3.

- 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.



Important

Due to changes introduced by the resource monitoring enhancement for SMC servers and the Management Client, customized heap size values for servers, the Web Portal, and Management Clients are not preserved when you upgrade to SMC version 6.8.3. You must modify your configuration if you previously changed the Java heap size of the Management Client using the `MAX_HEAP_SIZE` parameter in the `sgClient.sh` or `sgClient.bat` file.

To preserve the custom heap value for the Management Client, follow these steps on each computer the Management Client is installed:

- 1) Browse to the `<user home>/stonegate` folder.
- 2) Edit the `client_starter.xml` file.
- 3) Change the value of the `MAX_MEMORY_IN_MB` parameter to the value that you previously defined for the `MAX_HEAP_SIZE` parameter.

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*

