



FORCEPOINT

NGFW Security Management Center

Release Notes

6.5.9

Revision A

Contents

- [About this release](#) on page 2
- [System requirements](#) on page 2
- [Build number and checksums](#) on page 4
- [Compatibility](#) on page 5
- [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
Management Client peripherals	<ul style="list-style-type: none">• A mouse or pointing device• SVGA (1024x768) display or higher
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 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>



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 6 and 7 Red Hat Enterprise Linux 6 and 7 SUSE Linux Enterprise 11 SP3 and 12 SP1 Ubuntu 14.04 LTS and 16.04 LTS 	<ul style="list-style-type: none"> Windows Server 2016 Standard and Datacenter editions Windows Server 2012 R2 Windows Server 2008 R1 SP2 and R2 SP1 <p>On Windows 7 SP1 and 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.



Note: 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.

Web Start client

The Web Start distribution of the Management Client requires that a 64-bit Java Runtime Environment (JRE) is installed on the operating system.

Web Start is certified to run only on the listed official operating systems. However, it can also run on other operating systems that have JRE installed, for example, on macOS 10.9 or higher and additional Linux distributions. JRE 1.8.0_121 or a later critical patch update (CPU) release is required.

Build number and checksums

The build number for SMC 6.5.9 is 10656. This release contains Dynamic Update package 1183.

Use checksums to make sure that files downloaded correctly.

- **smc_6.5.9_10656.zip**

```
SHA1SUM:
e232cdc0ba0fd0e3c673787f15f8b79e3150a36b

SHA256SUM:
40717fe9e337dd788e340dca0b121f6b7af5a9a3c646cb846a24b5128d77f322

SHA512SUM:
f07062c95eed450a8f6fb131254ee623
5b4689ac0d7e431580803afd59310a33
c64978149f2c16a9ff5232714232aeeb
fcd8e55e16d4a2c32e40320d14330f8a
```

- **smc_6.5.9_10656_linux.zip**

```
SHA1SUM:
43b6f6f197a39974ed3138fe8f3eee9b1e3d976f

SHA256SUM:
cfebc27918b2f03b5189e1b388b953a7ee6c3723485d51f35654207ee026246e

SHA512SUM:
c754190625f365b4fd7e444f4dd99a08
4c81419071f15cb98af9e76e38639628
04aef31b90e48f08dc54453ed97d2310
98268ae54430a588a69e3d180dc878c2
```

- **smc_6.5.9_10656_windows.zip**

```
SHA1SUM:
f5ddee5da22580d29f9f5bd05eadb908d8165164

SHA256SUM:
23a2c1cea61553f9c8e8b1e55637f693683714c7e958ac16d2e20ac16690073a

SHA512SUM:
0123175b6896d815a0fded51b64b2d9f
1afca46b50e8e7882a423a549a0acca3
bc8ef3f740c8011fa11cd4bb7eb9258d
4546b75133ba76a9c75286775af0d701
```

- **smc_6.5.9_10656_webstart.zip**

```
SHA1SUM:
a83ee0e9a7413780c32ab5019834c6bb7d5b377b

SHA256SUM:
c02672a82d3d183c8839b37df78e2a4f07e909030d84381ac92195fe11586e00

SHA512SUM:
a55d694d5f20001bf22943f68805d809
1de68ab9c8b7065cd035546bca216f71
499fcffa916cd3b553090b3f64d5f696
f40a95b70164214a798f974b5da613b5
```

Compatibility

SMC 6.5 can manage all compatible Forcepoint NGFW Engine versions up to and including version 6.5.



Important: Some versions of Forcepoint NGFW have reached end-of-life status. Maintenance releases that contain security updates are no longer provided for Forcepoint NGFW versions that have reached end-of-life status. Even though these Forcepoint NGFW versions are 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 6.5 is compatible with the following component versions.

- Forcepoint™ Next Generation Firewall (Forcepoint NGFW) 6.2 or higher
- Stonesoft® Next Generation Firewall by Forcepoint (Stonesoft NGFW) 6.0 and 6.1
- McAfee® Next Generation Firewall (McAfee NGFW) 5.7, 5.8, 5.9, and 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*.

SD-WAN dashboard

The SD-WAN dashboard makes the software-defined wide area network (SD-WAN) features that are already part of Forcepoint NGFW more visible. The SD-WAN dashboard allows you to monitor SD-WAN features, such as outbound Multi-Link and Multi-Link VPNs, and to view statistics and reports related to SD-WAN features.

Application routing

You can now apply different NAT rules to traffic, select which VPN traffic uses, and redirect traffic to different proxy servers depending on the network applications detected in the traffic.

Route metrics, ECMP, and route monitoring

You can now define multiple static routes to the same destination and apply metrics to the routes. The routes with a lower metric value can be used as backup routes. When you enable the equal-cost multi-path (ECMP) feature on the routes, there is a potential increase in bandwidth as traffic is balanced between the routes. In addition, you can use probes to monitor the status of a route. If a route is unavailable, the route is removed from the routing table and traffic is automatically sent over another route.

Enhancements

This release of the product includes these enhancements.


Enhancements in SMC version 6.5.0

Enhancement	Description
Integrated User ID Service on NGFW Engines	You can now use the Integrated User ID Service on the NGFW Engines to provide transparent user identification for access control by user. The Integrated User ID Service is primarily meant for demonstration purposes and proof-of-concept testing of user identification services.
LDAP authentication for administrators	You can now authenticate administrators using simple password authentication against integrated external LDAP databases.
VPN tunnels can remain established	You can now set specific VPN tunnels to always remain established even when no traffic is sent through the VPN tunnel.
Improved sorting options in the Home view	You can now organize Active Alerts by Severity and Type, and organize User Behavior Events by Activity, User, User Alert Check Type, User Alert, and Severity.
IPv6 support for DHCP relay	You can now use DHCP relay on interfaces that have IPv6 addresses.
Node-initiated contact to Management Server for clustered NGFW Engines	Firewall Clusters and Master NGFW Engines in the Firewall/VPN role now support node-initiated contact to the Management Server. The clustered NGFW Engine opens a connection to the Management Server and maintains connectivity.
More precise controls for endpoint use	You can now define which VPN endpoints can communicate with each other, and how the endpoints are used in a Multi-Link configuration.
Dynamic routing with active-active clustering	You can now use dynamic routing in Firewall Clusters that use load-balancing mode. In load-balancing mode, all nodes in the cluster are online at the same time and traffic is balanced between the nodes, increasing performance for inspection and VPN traffic.
Support for ECA Evaluation deployment	It is now easier to deploy the Endpoint Context Agent to a limited set of users for evaluation. The ECA client and all necessary certificates can be downloaded from the ECA Evaluation web application and installed on endpoints. For details, see Knowledge Base article 16193 .
Dynamic elements specific to cloud platforms	You can use a specific naming scheme with Domain Name elements in Access rules to run a script on the NGFW Engine that resolves dynamic element names specific to a cloud platform to IP addresses. The IP addresses are resolved through API calls rather than regular network DNS queries. For more information, see Knowledge Base article 16290 .

Enhancements in SMC version 6.5.1

Enhancement	Description
TLS Profile for connecting to Forcepoint servers	The Management Server now uses a custom TLS Profile element for automatically downloading license updates, dynamic updates, and NGFW Engine upgrades from Forcepoint servers. The TLS Profile element defines the settings for cryptography, trusted certificate authorities, and the TLS version used in TLS-protected traffic.

Enhancements in SMC version 6.5.2

Enhancement	Description
New URLs for dynamic updates and engine upgrades	<p>To improve the performance of automatic dynamic updates and engine upgrades, the following new URLs are available in SMC 6.5.2 and higher:</p> <ul style="list-style-type: none"> https://autoupdate.ngfw.forcepoint.com/dynup.rss https://autoupdate.ngfw.forcepoint.com/ngfw.rss <p> Note: The SMC automatically starts using the new URLs when you upgrade to SMC 6.5.2 or higher and activate the dynamic update package that includes the new URLs.</p> <p>The new URLs use a content distribution network (CDN) to allow the SMC to download dynamic update packages and engine upgrade files from the geographically closest server. The legacy https://update-pool.stonesoft.com/index.rss URL remains available for backward compatibility and as a backup for the new URLs.</p>
Configurable update services for dynamic updates and engine upgrades	<p>New Update Service elements define sets of URLs for automatic dynamic updates and engine upgrades. In SMC 6.5.2 and higher, the SMC automatically uses Update Service elements that include both the new URLs and the legacy URL. No action is needed to start using the Update Service elements that include the new URLs.</p> <p>You can optionally change which Update Service element is used for automatic dynamic updates and engine upgrades. For more information, see Knowledge Base article 16589.</p>
Enhancements in the User Dashboard	<p>The following enhancements have been made in the User Dashboard:</p> <ul style="list-style-type: none"> The user domain is now always shown for users in the User Dashboard. To prevent information about them from cluttering the User Dashboard statistics, the System and Root users are no longer shown in the User Dashboard statistics. The endpoint IP address is now always shown for users in the User Dashboard.
Alert Policy management in the SMC API	You can now manage Alert Policies using the SMC API.
Support for custom fields in CEF log format	You can now configure custom fields when you export or forward logs to an external service in CEF or LEEF formats.

Enhancements in SMC version 6.5.3

Enhancement	Description
Configurable wait time between inspected packets	To optimize latency and CPU utilization, you can now customize how long the inspection process waits for additional packets.

Enhancements in SMC version 6.5.6

Enhancement	Description
Export all elements except those in the Trash	When using the SMC API or the sgExport command on the command line, there is now the option to exclude elements that are in the Trash when exporting all elements.

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
The automatic rule for Endpoint Context Agent (ECA) does not allow the necessary traffic when the Source Networks field is left blank. The default value, Internal Zone, is not used correctly.	SMC-9117
Deleting custom Endpoint Application elements is slow.	SMC-12900
When you import a Policy-Based VPN element, the import does not include the pre-shared key.	SMC-15181
If the Management Server does not have access to Forcepoint servers, the following alert is sent constantly regardless of the specified update check interval: "Management Server: Update server not available".	SMC-16638
When a VPN endpoint has Phase-1 ID exceptions configured, the VPN Client configuration always uses the default Phase-1 ID even if the VPN Client is included in a VPN for which an exception is defined.	SMC-19775
When there are three Management Servers, excluding one standby Management Server from database replication also causes a database mismatch for the other standby Management Server.	SMC-21040
You cannot sort the Routing monitoring view by the Network column.	SMC-22028
When you use the Management Client on a computer with multiple displays, popup menus might open on a different display than the main Management Client window.	SMC-22283
When using Azure automatic scaling, the Management Server creates new NGFW Engine instances automatically. Policy installation might start before initial contact has been successfully made.	SMC-22284
When you use a DNS name as a contact address, the DNS name can include only one dash (-) character.	SMC-22286
When you convert a Firewall Cluster to a Master NGFW Engine cluster, DHCP Relay settings on the VPN > VPN Client branch of the Engine Editor change.	SMC-22339

Description	Issue number
When a VPN is open in preview mode, changing to edit mode might fail. The following message is shown: "Failed to construct proxy identities".	SMC-22364
Administrators are not notified of changes to the permissions of the administrator role that is assigned to them when they log on to the Management Client.	SMC-22422
When there are several Active Directory Servers, browsing the user tree might fail.	SMC-22428
If the first node of a cluster is not available, adding or deleting blacklist entries from the Management Server fails.	SMC-22434
When you change the MTU setting for a port group interface, the routing configuration for the interface is reset to the default value.	SMC-22456
If a node for a Master NGFW Engine is disabled, it is not possible to preview the Quagga configuration on a hosted Virtual NGFW Engine.	SMC-22517
Running the Capture Traffic tool on an NGFW Master Engine fails if the first node of the cluster is in the offline state.	SMC-22543
When a new license is installed and license binding changes, the Licenses view does not show the changes until the Management Server service is restarted.	SMC-22560
After you have viewed the details of an alert in the Active Alerts view, the information might not be updated when you view the details of the next alert.	SMC-22590
Adding or editing a valid expression might fail when using the SMC API.	SMC-22598
When you export a report that includes top rate sections as a PDF, some information might not be visible in the PDF. The information is visible if you export the same report in table format.	SMC-22620
When you copy an Access rule that includes the Use VPN action from a policy in one administrative Domain to a policy in another administrative Domain, it is no longer possible to edit the policy to which you copied the rule.	SMC-22696
When there are a large number of Log Servers, viewing logs might fail after you add a new Log Server.	SMC-22705
When a Log Server forwards both active alerts and blacklist entries to the Management Server, the forwarded active alerts and blacklist entries might conflict. Either the active alerts or blacklist entries might be ignored. As a result, alert notifications might not be sent even though an alert is generated and is visible in the Logs view.	SMC-22715
When an SMC API client session times out, the Management Server might return error 404 instead of error 401.	SMC-22738

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 6.5 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 6.5, 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.
- 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.
- Upgrading is supported from SMC versions 5.6.2 – 6.4.10, 6.5.0 – 6.5.6, and 6.5.8. Versions lower than 5.6.2 require an upgrade to one of these versions before upgrading to 6.5.9.
- Due to changes in application detection, policies that use Network Applications in the Access rules might work differently after upgrading to NGFW 6.4 or higher. Some traffic that was previously allowed might be discarded. In NGFW 6.5, there are changes related to how port information is used for matching applications.

Verify that your policies still work as expected. For more information, see Knowledge Base article [15411](#).

- The legacy Stonesoft User Agent is no longer supported. If you have used the Stonesoft User Agent, make sure that the feature has been completely removed from the SMC and that the element for the Stonesoft User Agent has been removed from the Trash before you upgrade to version 6.5. We recommend that you use the Forcepoint User ID Service instead.

Known issues

For a list of known issues in this product release, see Knowledge Base article [16274](#).

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

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*

