



FORCEPOINT

NGFW Security Management Center

Release Notes

6.5.8

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 10
- [Upgrade instructions](#) on page 11
- [Known issues](#) on page 12
- [Find product documentation](#) on page 12

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 6.5.8 is 10648. This release contains Dynamic Update package 1175.

Use checksums to make sure that files downloaded correctly.

- **smc_6.5.8_10648.zip**

```
SHA1SUM:
f06e8e126bd3a2e31e3a16c10f490e1885f21619

SHA256SUM:
b67582f7c2f37d928c36c70bf292ee4c08aaf82fc07ac723b795236d1d47e93f

SHA512SUM:
b4187898a22447a1f32460bfba694c8b
ca2753ccae219bc4b3f6e8d175759245
86e12bc4ea16a30760446a2cb8b107bc
a78509e245036a2608b6f8d02b16abd7
```

- **smc_6.5.8_10648_linux.zip**

```
SHA1SUM:
2603a24d93e6f611b21a1e8695baa829b187d3fe

SHA256SUM:
e666c77bd7f3b10c8e1a23febb8749a599f3bc15e2d7358c8316ff017b9841f0

SHA512SUM:
b0d7807116de83bc8b2e1158160fc371
9e93de80590d387ed0178a44d69e0903
2b9b3cb7e11c7371e1788fd10e86e228
2c4473a8e60ada020d94c9c384bb5de9
```

- **smc_6.5.8_10648_windows.zip**

```
SHA1SUM:
ebb9c4321137b41a5a0507993b14c536701515b5

SHA256SUM:
08c5a3771c75f043ba96512a944fd355b515609ed7e7d348872cea2283fd0a30

SHA512SUM:
a8f45623b04a34494f419fa6c6b3876c
a7b24280ebf1b4f0c2884ebf62932bc9
44c47510e7a3cf39114d588cfafd194f
b4bf31f9f3af9610cd5d9afc012d6fb3
```

- **smc_6.5.8_10648_webstart.zip**

```
SHA1SUM:
c764a20e891585adca311d2c65f076da66cda837

SHA256SUM:
fe636b05f8e55cf21b857d5ba3d4f1ed7441d0cf1a681dc3a38f09b0975a6c95

SHA512SUM:
6996c4d1205f3ad11f8a010515aafd10
519232b269a179eb6980b6f916fa627e
99d140fc9eb7721dd98976d1575f085a
9f7776aed3a183b5dc3ef383c9a8da5a
```

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
Rules in a policy are different colors to indicate the different template levels that the rule is inherited from. The rule template that the rule is inherited from is not shown in text format.	SMC-1279
VPN validation incorrectly gives warnings about disabled tunnels.	SMC-2405
The certificate request for browser-based user authentication does not include the Subject Alternative Name attribute. The Google Chrome web browser does not accept server certificates that do not have this attribute.	SMC-9163
Expression element translation values are not updated until the element is revalidated. If an element within an Expression element is updated, the change is not reflected in the Network Details view in the policy editor. The Expression element is revalidated when the policy is installed or if the Expression element is edited.	SMC-17851
When searching for rules in a large policy that produces many matches, not all the matching rules are shown. You must click Next to show all the matching rules.	SMC-18333
When you create an additional VPN gateway for a firewall, the list of endpoints shown in the Engine Editor does not match under the different gateways.	SMC-18400
When dragging and dropping elements between rules, or adjusting column widths, the performance of the Policy Editor decreases.	SMC-19672
If AES-GCM-256 and AES-GCM-128 are the only cipher algorithms set in the VPN profile for mobile VPN, the client configuration is not generated. When installing the policy, you see the following message: "The Configuration for FORCEPOINT IPsec VPN Client has not been generated for the Gateway: <name>. The FORCEPOINT IPsec VPN Client does not support one or more settings in the VPN Profile".	SMC-20463
When editing a large VPN, it is useful to select Tools > Filter by Gateway. However, when you select Tools > No Filtering, the filter is not removed correctly.	SMC-20798

Description	Issue number
Upgrading a large number of NGFW Engines in a short time might slow down the operation of the SMC and prevent administrators from logging on.	SMC-21010
An MSSP report might show the date 01/01/1970 for an expired license.	SMC-21039
If an Access rule includes two Users or two User Groups that have the same SamAccountName but are located in different LDAP sources, only one name is shown in the rule. For more information, see Knowledge Base article 17250 .	SMC-21072
If QoS Class elements are used for link selection for outbound traffic, when the policy is installed, the NAT entry identification changes unnecessarily. The NGFW Engine considers this to be a network configuration change, even if the configuration has not changed.	SMC-21294
When you search an external LDAP server, you might see the message: "Failed to refresh Folder Search. Could not search an entry from base dn". This might happen if there is a large number of users and groups on the external LDAP server.	SMC-21307
When you browse users on an external LDAP server (not an Active Directory server), not all users are shown, and only the default user groups are shown.	SMC-21355
The "Overwrite Oldest" setting in the "Log Storage Full" options for the Log Server might not work as intended because the function is triggered too late.	SMC-21380
In the Active Alerts view, the Details option might not be available after you change the way the view is sorted or aggregated.	SMC-21398
When you remotely upgrade an NGFW Engine cluster, the upgrade does not proceed after "Waiting for all the nodes to come back online..." is shown on the progress tab even though the upgrade is successful to all nodes.	SMC-21405
If more than 10,000 elements are selected in one view, the Management Client might become unresponsive.	SMC-21508
If a loopback interface is used as the interface for DHCP relay in the VPN Client settings for a VPN gateway, the automatic rules do not allow these relayed DHCP packets.	SMC-21683
You cannot create an SSID interface that uses a custom MAC address.	SMC-21705
The Where Used? option might not find a user or group used in a configuration if the Base DN configured on an Active Directory server uses one case (lower case, for example), but the SMC element that represents that Active Directory server is configured to use the same Base DN, but uses a different case (upper case, for example).	SMC-21717
The system alias \$\$ Local Cluster(NDI addresses only) does not include loopback NDI addresses.	SMC-21766
When you configure protocol-independent multicast (PIM) on a tunnel interface, the CVI address on the tunnel interface must be saved before you continue configuring PIM in the Routing view.	SMC-21799
The performance of the Routing view is decreased when there is a large number of tunnel interfaces.	SMC-21800
It is possible to use an SMC API Client name and authentication key to log on to the Management Client.	SMC-21817
If you right-click a VPN Site, then select New Site, the new VPN Site might replace the existing VPN Site.	SMC-21854
Policy installation fails on a Master NGFW Engine in the Firewall/VPN role that hosts a Virtual Firewall that has only a Layer 2 interface configured.	SMC-21865
It is not possible to delete a blacklist entry for a Virtual NGFW Engine.	SMC-21887

Description	Issue number
An audit entry is not created when there is a failed SMC API logon attempt and the password policy locks the account.	SMC-21928
It is not possible to set the Location option for Active Directory Server and LDAP Server elements.	SMC-21965
When you add an NGFW element to a Location element that has already been saved, the change is not saved unless you also modify the comment or name of the Location element.	SMC-21986
When you search for rules, only the rule ID for sub-policy rules is shown. If there are several levels of sub-policies, it can be difficult to see the location of the rule.	SMC-22002
When you search in rules, the search can match against a sub-policy rule, even if the jump rule to that sub-policy rule does not match.	SMC-22004
When you set the pre-shared key for an SSID interface, the key is not saved.	SMC-22040
Automatic license updates or dynamic update downloads might fail.	SMC-22093
Upgrading the Management Server might take up to an hour if there are several larger policies.	SMC-22104
In rare circumstances, when you refresh the policy on a Virtual NGFW Engine while an earlier policy refresh is still in progress for other Virtual NGFW Engines on the same Master NGFW Engine, the policy refresh might fail.	SMC-22110
When you create a backup to a local workstation, instead of storing to the user-specified path, the backup is always stored in the default folder.	SMC-22123
When you create a new VPN site from the Engine editor, the VPN Site Properties dialog box might not open or the list of available elements might be empty.	SMC-22136
The snapshot comparison view can take a long time to open.	SMC-22158
When using the SMC API, a rule can be created by specifying a rule insert point. It is not possible to query an existing rule insert point.	SMC-22166

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 10 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, and 6.5.0 – 6.5.6. Versions lower than 5.6.2 require an upgrade to one of these versions before upgrading to 6.5.8.
- 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*

