



# **FORCEPOINT**

## **NGFW Security Management Center Appliance**

### **Release Notes**

**6.5.14**

**Revision A**

## Contents

- [About this release](#) on page 2
- [Build number and checksums](#) on page 2
- [System requirements on virtualization platforms](#) on page 3
- [Compatibility](#) on page 3
- [New features](#) on page 4
- [Enhancements](#) on page 4
- [Resolved issues](#) on page 7
- [Install the SMC Appliance](#) on page 9
- [Upgrade the SMC Appliance](#) on page 10
- [Known issues](#) on page 11
- [Find product documentation](#) on page 11

## About this release

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

The SMC Appliance ships with pre-installed Forcepoint NGFW Security Management Center (SMC) software. The pre-installed SMC includes a Management Server and a Log Server. You can alternatively install the SMC Appliance software on a virtualization platform.



**Note:** The SMC Appliance does not support high-availability for the Management Server or the Log Server.

## Build number and checksums

The build number for SMC 6.5.14 is 10676. This release contains Dynamic Update package 1230.

Use checksums to make sure that files downloaded correctly.

- 6.5.14U001.sap

```
SHA1SUM:
8c059e9e960f09204858546d95785232d505d093

SHA256SUM:
35903ab06e89278ff5ce84b2cda668fb10ea1306eca353f66ad2350674838042

SHA512SUM:
bac30b52a69bcda3e7c1de3f600eccc6
dfd892c1169bb673e219bd6b8a622ef7
980b77cddb5ac9a11643a870543dc187
c97d7c5a0079928843cf024735898b88
```

# System requirements on virtualization platforms

As an alternative to using the SMC Appliance software on the pre-installed Forcepoint appliance, you can install the SMC Appliance software on a virtualization platform.



**CAUTION:** To protect the privacy of your data, we recommend installing the NGFW Engines, SMC components, or SMC Appliance on a hypervisor that does not host any other virtual machines.

Component	Requirement
Hypervisor	VMware ESXi version 6.0 or higher
Memory	8 GB RAM
Virtual disk space	120 GB
Interfaces	At least one network interface

The .iso installation file that is used to install the SMC Appliance software on a virtualization platform is available only for major versions of the SMC Appliance. To install the maintenance version, first install the .iso for the major version, then upgrade to the maintenance version.

## 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
Viewing log data on the SMC Appliance command line	A new option “log-view” for the smca-system command line tool allows you to view the contents of log files in the SMC Appliance log data directory /var/log and in any of its subdirectories.
Audit data storage	For new installations, audit data is stored on its own partition.
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.

Enhancement	Description
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 <a href="#">16193</a> .
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 <a href="#">16290</a> .

## 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"> <li><a href="https://autoupdate.ngfw.forcepoint.com/dynup.rss">https://autoupdate.ngfw.forcepoint.com/dynup.rss</a></li> <li><a href="https://autoupdate.ngfw.forcepoint.com/ngfw.rss">https://autoupdate.ngfw.forcepoint.com/ngfw.rss</a></li> </ul> <p> <b>Note:</b> 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 <a href="https://update-pool.stonesoft.com/index.rss">https://update-pool.stonesoft.com/index.rss</a> 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 <a href="#">16589</a>.</p>
Enhancements in the User Dashboard	<p>The following enhancements have been made in the User Dashboard:</p> <ul style="list-style-type: none"> <li>The user domain is now always shown for users in the User Dashboard.</li> <li>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.</li> <li>The endpoint IP address is now always shown for users in the User Dashboard.</li> </ul>
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.

## Enhancements in SMC version 6.5.11

Enhancement	Description
New default settings for VPN profiles	The default values that are selected when you create a new VPN Profile element have been changed to better meet the needs of typical users.

## Enhancements in SMC version 6.5.14

Enhancement	Description
Route monitoring in the SMC API	The SMC API now responds with an error code if a monitoring session cannot be opened when the client makes an HTTP request to retrieve routing monitoring information. For more information, see Knowledge Base article <a href="#">18186</a> .

## 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
If you use the SSM FTP Proxy or the SSM TFTP Proxy in an Access rule, deep inspection must be enabled in the Access rule. Otherwise, the NGFW Engine discards the related connections.	SMC-23530
If policies are installed on multiple Virtual NGFW Engines at the same time as blacklists are modified and time is being synchronized, the policy installations fail. The following message is shown: "X is currently locked, another command is performed on it".	SMC-23689
When there are multiple Management Servers, latency in communication between the servers can cause the replication status to be Postponed.	SMC-24388
If a VPN gateway has two VPN endpoints for an IPsec VPN tunnel, only one of the endpoints must be of the type IPsec VPN. However, if you only have one IPsec VPN endpoint, policy installation fails, and the following message is shown: "The Route-Based VPN tunnel that references the Firewall X is invalid. All Endpoints must be IPsec".	SMC-24477
When data is collected from multiple Log Servers, some sections in Overviews might be empty.	SMC-24628
When there are hundreds of NGFW Engine elements, the Pending Changes pane might load slowly. The Management Client might become unresponsive for several minutes.	SMC-25026
Log-related Tasks might not handle corrupted log data correctly. Corrupted log data can cause the Tasks to fail.	SMC-25043

Description	Issue number
If a node in an NGFW Engine cluster is in standby mode or is offline, the status of a failed NetLink is reported as Mixed (orange) instead of Error (red).	SMC-25141
A Route-based VPN tunnel might not be included in the configuration for an NGFW Engine if the Default IP Address for Outgoing Traffic option is set as the Loopback Interface.	SMC-25203
Type-ahead search is slow in the Route-Based VPN Tunnels view if there are hundreds of tunnels configured.	SMC-25581
When you modify a URL List Application element, pending changes are shown for any NGFW Engine that includes a custom URL List Application element in its policy.	SMC-25659
When using the Search Rules pane in a policy, the title for the Authentication field is not shown.	SMC-25707
The sender comment is not included in alert notifications sent by email.	SMC-25779
Administrators are not replicated to new NGFW Engines if the replication is configured before the NGFW Engine makes initial contact with the Management Server.	SMC-25819
In an NGFW Engine cluster, an interface that does not have any Node Dedicated IP Addresses (NDIs) borrows an IP address from another interface and uses the same netmask. As a result, the dynamic routing configuration considers there to be two interfaces that have the same network.	SMC-26002
When you select an NGFW Engine node in the Home view, the appliance diagram might not show the correct details.	SMC-26125
Elements that are referenced in a Layer 2 Interface policy can be deleted.	SMC-26145
Web Portal users cannot see all options in the Action, Logging, and Authentication cells in Access rules.	SMC-26248
You cannot use the Log URL Categories logging option in rules that terminate connections.	SMC-26269
If the Log Server is unavailable when you install a policy on an NGFW Engine, Correlation Situations that are processed on the Log Server cannot be replicated to the Log Server. If the Log Server is unavailable for an extended time, Correlation Situations consume a large amount of space in the Management Server database.	SMC-26272
When you copy and paste multiple policy validation results, only one of the results is pasted.	SMC-26285
The Password Age and Expiration settings in the Global System Properties dialog box also apply to administrator accounts that have the Always Active option selected. These administrators are not notified when the password is about to expire.	SMC-26313
When there are a large number of NGFW Engines, the Log Server might use a large amount of memory for storing Correlation Situations that are processed on the Log Server.	SMC-26322
When the Management Server has been shut down, the replication of active alert notifications from Log Servers might not recover after the Management Server becomes available.	SMC-26362
In the properties of a VPN Site element, there are entries in the list on the VPN References tab where the VPN name is not shown.	SMC-26427
When you set the Situation to ANY in an exception rule in an Inspection Policy, the correlation configuration is not generated for Correlation Situations that are processed on the Log Server.	SMC-26574
You cannot filter or aggregate log entries based on MAC addresses.	SMC-26586
The Management Client unnecessarily keeps the history of policy upload tasks in memory, which can cause the Management Client to use too much memory.	SMC-26594



Description	Issue number
After you have configured PIM multicast routing for an NGFW Engine, you cannot delete the NGFW Engine element.	SMC-26702
When you add several routes to the routing view at the same time, only one of the routes might be updated in the antispoofing view.	SMC-26723
It is possible to use the add route action in the SMC API even though the NGFW Engine element is locked for editing the in the Management Client	SMC-26797
In environments with Master NGFW Engines, connection monitoring using the SMC API might fail.	SMC-26888
When monitoring views for multiple NGW Engines are open at the same time, the Management Client user interface might stop responding.	SMC-27182

## Install the SMC Appliance

Use these high-level steps to install the SMC Appliance.

For detailed information about installing the SMC Appliance and the NGFW Engines, see the *Forcepoint Next Generation Firewall Installation Guide*. All guides are available for download at <https://support.forcepoint.com/Documentation>.

### Steps

- 1) Turn on the SMC Appliance.
- 2) Select the keyboard layout for accessing the SMC Appliance on the command line.
- 3) Accept the EULA.
- 4) Enter the account name and password.  
For credential requirements, see the *Forcepoint Next Generation Firewall Installation Guide*.
- 5) Make your security selections.
- 6) Complete the network interface and network setup fields.
- 7) Enter a host name for the Management Server.
- 8) Select the time zone.
- 9) (Optional) Configure NTP settings.
- 10) After the SMC Appliance has restarted, install the Management Client.  
You can use Java Web Start or install the Management Client from a file to allow remote access to the SMC. Java Web Start is enabled by default on the Management Server that is pre-installed on the SMC Appliance.

- 11) Import the licenses for all components.  
You can generate licenses at <https://stonesoftlicenses.forcepoint.com>.
- 12) Create the NGFW Engine elements, then install and configure the NGFW Engines.

## Upgrade the SMC Appliance

Use an upgrade patch to upgrade the SMC Appliance from a previous version to version 6.5.14.

There are two kinds of SMC Appliance patches:

- Hotfix patches include improvements and enhancements for the current SMC Appliance version. Hotfix patch files use the letter P as a separator between the version number and the patch number. Example: 6.5.1P001
- Upgrade patches upgrade the SMC Appliance to a new version. Upgrade patch files use the letter U as a separator between the version number and the patch number. Example: 6.5.1U001

We recommend checking the availability of SMC Appliance patches regularly, and installing the patches when they become available. For detailed information about installing SMC Appliance patches, see the *Forcepoint Next Generation Firewall Installation Guide*.



**CAUTION:** Before upgrading the SMC Appliance from version 6.2.0, install the 6.2.0P001 patch. For more information, see Knowledge Base article [14168](#).

- 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 using the Management Client before upgrading the software.
- The SMC Appliance must be upgraded before the NGFW Engines are upgraded to the same major version.
- You can upgrade from the following SMC versions:
  - 6.4.7 – 6.4.10
  - 6.5.1 – 6.5.13

Versions lower than 6.2.0 require an upgrade to one of these versions before upgrading to 6.5.14.

- If you configured SNMP for the SMC Appliance before upgrading to version 6.4.0 or higher, you must configure SNMP again.

### Steps

- 1) Log on to the SMC Appliance.
- 2) To check for available upgrade patches, enter the following command:

```
sudo ambr-query -u
```

- 3) To load the patch on the SMC Appliance, enter the following command:

```
sudo ambr-load 6.5.14U001
```

If you downloaded the patch and transferred it to the SMC Appliance, append the load command with the `-f` option and specify the full path to the patch file. Example:

```
sudo ambr-load -f /var/tmp/6.5.14U001.sap
```

- 4) To install the patch on the SMC Appliance, enter the following command:

```
sudo ambr-install 6.5.14U001
```

The installation process prompts you to continue.

- 5) Enter `y`.

## Result

The installation process restarts the appliance and installs the patch. When the upgrade is finished, the appliance restarts. The appliance is now running SMC Appliance 6.5.14.

# 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*

