FORCEPOINT

# NGFW Security Management Center

## Release Notes

**6.5.14**

**Revision A**

Contents



# About this release

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

# System requirements

To use this product, your system must meet these basic hardware and software requirements.

## SMC hardware requirements

You can install the SMC on standard hardware.

| Component | Requirement |
|---|---|
| CPU | Intel® Core™ family processor or higher recommended, or equivalent on a non-Intel platform |
| Management Client peripherals | • A mouse or pointing device<br>• SVGA (1024x768) display or higher |
| Disk space | • Management Server: 6 GB<br>• Log Server: 50 GB |

| Component | Requirement |
|---|---|
| Memory | • Management Server, Log Server, Web Portal Server: 6 GB RAM<br>• If all SMC servers are on the same computer: 16 GB RAM<br>• Management Client: 2 GB RAM<br>The SMC server requirements are the *minimum* requirements. The Management Server and Log Server in particular benefit from having more than the minimum amount of RAM.<br>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. |

**CAUTION:** To protect the privacy of your data, we recommend using dedicated hardware for all NGFW, SMC, and SMC Appliance installations. For cloud-based virtualization platforms, use an instance type that runs on dedicated hardware. For on-premises virtualization platforms, install the NGFW Engines, SMC components, or SMC Appliance on a hypervisor that does not host any other virtual machines. For third-party hardware, do not install any other software on the computer where you install the NGFW Engines or SMC components.

# Operating systems

You can install the SMC on the following operating systems. Only 64-bit operating systems are supported.

| Linux | Microsoft Windows |
|---|---|
| • CentOS 6 and 7<br>• Red Hat Enterprise Linux 6 and 7<br>• SUSE Linux Enterprise 11 SP3 and 12 SP1<br>• Ubuntu 14.04 LTS and 16.04 LTS | Standard, Datacenter, and Essentials editions of the following Windows Server versions:<br>• Windows Server 2016<br>• Windows Server 2012<br>On Windows 10, you can install the SMC in demo mode. You can also install the Management Client. |

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 6.5.14 is 10676. This release contains Dynamic Update package 1230.

Use checksums to make sure that files downloaded correctly.

- smc_6.5.14_10676.zip

```
SHA1SUM:
959165dbe6fc73c972dc59ce6cc0d671a63bb8cf

SHA256SUM:
edd8f3d36a585aa6bde88203cb636ee201a718a55b0c213c88f7d9089bbbf9cb

SHA512SUM:
2d1bbb28037d08070a8f4aa86084ee8e
92bfc9d1daad6526ee31f380c1fa856f
f68817d2750ef4c3f7df4d61decba76b
a60e05c0362e29876d848112b514e8d5
```

- smc_6.5.14_10676_linux.zip

```
SHA1SUM:
808548a7d40dc6f0f8f5f9bc7e0d79e23ccd084b

SHA256SUM:
06a0fd75f4e9cd445426b3c9fec9f04230e15ba86f5aa18c49a352c1c58dafbb

SHA512SUM:
b7af41fe8154d4c50e347bc6e54de73d
9ee9de935988119437a63e69cb47bec4
b9dc6487484672b7bf5731d44bd4bf00
f9cc8e15db6fbb4714b7551872af33ca
```

- smc_6.5.14_10676_windows.zip

```
SHA1SUM:
f84c040e8606e3f7500c86b8794251ea9eb89ae7

SHA256SUM:
62abc1046ae10b6220d81531b1f3d45bdc2a5f15f50da4245e3b21f59e8a3922

SHA512SUM:
c9a7d365401313846a0969e4656b6a26
08d682e2b2a120685749643b3618a587
109f1c805feb1a48f75863f0a3c5f1e6
98018284c5eb1fd3a9cbcbc1f52c0905
```

- smc_6.5.14_10676_webstart.zip

```
SHA1SUM:
75c596fba8760404f99f43e4bcea86f2f0262445

SHA256SUM:
610c792f71d85c60353fc0c2fba545ca53fb525bf7c04f7098047315261bb446

SHA512SUM:
6ab4440432cd6c1f3285af4850ae6718
8ea1912fcc712acde71aaef4bac095fa
d5149f4b7ccf66a6ab981fcea8009a5f
e6a1da4b05d02d09b8cd00bc12a49be8
```

# 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 | To improve the performance of automatic dynamic updates and engine upgrades, the following new URLs are available in SMC 6.5.2 and higher:<br>• https://autoupdate.ngfw.forcepoint.com/dynup.rss<br>• https://autoupdate.ngfw.forcepoint.com/ngfw.rss<br>  **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.<br>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. |
| Configurable update services for dynamic updates and engine upgrades | 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.<br>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. |
| Enhancements in the User Dashboard | The following enhancements have been made in the User Dashboard:<br>• The user domain is now always shown for users in the User Dashboard.<br>• 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.<br>• 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. |

## 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 18186. |

# 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 |

| Description | Issue number |
|---|---|
| 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 |
| 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 |

| Description | Issue number |
|---|---|
| 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 |
| 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 |

# 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.
- You can upgrade from the following SMC versions:
  - 5.6.2 – 6.4.10
  - 6.5.0 – 6.5.13

  Versions lower than 5.6.2 require an upgrade to one of these versions before upgrading to 6.5.14.
- 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*

Published 09 April 2020