NGFW Security
Management Center

Release Notes

6.5.5
Revision A
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.

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

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirement</th>
</tr>
</thead>
</table>
| Memory    | • 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  

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. 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.

<table>
<thead>
<tr>
<th>Linux</th>
<th>Microsoft Windows</th>
</tr>
</thead>
</table>
| • 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 | • Windows Server 2016 Standard and Datacenter editions  
• Windows Server 2012 R2  
• Windows Server 2008 R1 SP2 and R2 SP1  

On Windows 7 SP1 and 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 6.5.5 is 10642. This release contains Dynamic Update package 1153. Use the checksums to make sure that the files downloaded correctly.

- **smc_6.5.5_10642.zip**
  SHA1SUM: 7a3fb1ae92b6c235b37730592d625a2f146a6532
  SHA256SUM: e683340ba6ac9c8032bfaf3e67bacca0d6bd69c827aa1d683e290c8880d5705
  SHA512SUM: 1cc3b47929ec43ab16ab041ac7dfb1a5
  4da7660cc8cc96b0f2931df6f5b47e172
  b384e78f278205ca6ef1f332c72841ca
  15eb8eefa749c144b124db861d4e52

- **smc_6.5.5_10642_linux.zip**
  SHA1SUM: ae9eb0a2700bef7156e7390c83994491aca9e35b
  SHA256SUM: e16055b252df2ca36e04046e274903b82e28a5e631a2e3de0bdff8c01f832c4
  SHA512SUM: 405b5626dd05e69b59feaddf6ded5af1
  6a2badc67f573b56fb2816362390fcbf
  2782f5aa4eb781f55ab45b2f19f69a8
  3551b54c3efb72307e2e8651fc51c973

- **smc_6.5.5_10642_windows.zip**
  SHA1SUM: 86683d9c521f87c6c71bce66baea44b154ed8b9
  SHA256SUM: 79ef3161a5372e6f485579718633f54094175167711dd90e58a54eb39b4e
  SHA512SUM: 60566f66626fe8720f5d75b8a2036594
  7061d162542a331d68484690e9af8d5b
  f827d4bdc03d360e7948810178f8f86
  23943d9454832bdf2c0b315370b49

- **smc_6.5.5_10642_webstart.zip**
  SHA1SUM: 0d3d3165ebcede5b5d316a54b8dec4e36b4d428c9e
  SHA256SUM: 164f5f14627088b506508ff88734aa52ce658ffe0cd7be0698b32dd3bb582e0
  SHA512SUM: 1452b807e695dbd293a261a202cb036
  c5d701f80ee371aface41d4e53d5a6c
  848ef87df079d4110d17612b0ace1
  4e2148db4640d6013da536c571a6031d
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

<table>
<thead>
<tr>
<th>Enhancement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrated User ID Service on NGFW Engines</td>
<td>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.</td>
</tr>
<tr>
<td>LDAP authentication for administrators</td>
<td>You can now authenticate administrators using simple password authentication against integrated external LDAP databases.</td>
</tr>
<tr>
<td>VPN tunnels can remain established</td>
<td>You can now set specific VPN tunnels to always remain established even when no traffic is sent through the VPN tunnel.</td>
</tr>
<tr>
<td>Improved sorting options in the Home view</td>
<td>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.</td>
</tr>
<tr>
<td>IPv6 support for DHCP relay</td>
<td>You can now use DHCP relay on interfaces that have IPv6 addresses.</td>
</tr>
<tr>
<td>Node-initiated contact to Management Server for clustered NGFW Engines</td>
<td>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.</td>
</tr>
<tr>
<td>More precise controls for endpoint use</td>
<td>You can now define which VPN endpoints can communicate with each other, and how the endpoints are used in a Multi-Link configuration.</td>
</tr>
<tr>
<td>Dynamic routing with active-active clustering</td>
<td>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.</td>
</tr>
<tr>
<td>Support for ECA Evaluation deployment</td>
<td>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.</td>
</tr>
<tr>
<td>Dynamic elements specific to cloud platforms</td>
<td>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.</td>
</tr>
</tbody>
</table>
## Enhancements in SMC version 6.5.1

<table>
<thead>
<tr>
<th>Enhancement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLS Profile for connecting to Forcepoint servers</td>
<td>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.</td>
</tr>
</tbody>
</table>

## Enhancements in SMC version 6.5.2

<table>
<thead>
<tr>
<th>Enhancement</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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:  
  - https://autoupdate.ngfw.forcepoint.com/dynup.rss  
  - https://autoupdate.ngfw.forcepoint.com/ngfw.rss  
  
  **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.  

  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.  

  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:  
  - 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

<table>
<thead>
<tr>
<th>Enhancement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configurable wait time between inspected packets</td>
<td>To optimize latency and CPU utilization, you can now customize how long the inspection process waits for additional packets.</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Description</th>
<th>Issue number</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you right-click a Master NGFW Engine, then select Current Policy &gt; Refresh, the policy refresh might not start.</td>
<td>SMC-20723</td>
</tr>
<tr>
<td>Even though policy installation on a Master NGFW Engine succeeds, policy installation might be shown as failed. The following message is shown: &quot;Transaction is not started&quot;. This error prevents the &quot;Refresh Policy on Master Engines and Virtual Security Engines&quot; task from continuing, and the policy is not refreshed on the Virtual NGFW Engines. You must separately refresh the policy on the Virtual NGFW Engines.</td>
<td>SMC-20884</td>
</tr>
<tr>
<td>When you use the default External Zone element as the destination in an Access rule, the SMC generates an incorrect configuration.</td>
<td>SMC-20927</td>
</tr>
</tbody>
</table>

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 – 6.4.9, and 6.5.0 – 6.5.4. Versions lower than 5.6.2 require an upgrade to one of these versions before upgrading to 6.5.5.
- 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**