FORCEPOINT

NGFW Security Management Center

Release Notes

6.2.5

Revision A

Contents

- About this release on page 2
- System requirements on page 2
- Build version on page 3
- Compatibility on page 4
- New features on page 5
- Enhancements on page 7
- Resolved issues on page 8
- Installation instructions on page 9
- Known issues on page 10
- Find product documentation on page 10

About this release

This document contains important information about this release of Forcepoint NGFW Security Management Center (SMC); formerly known as Stonesoft® Management Center by Forcepoint (SMC).

We strongly recommend that you read the entire document.

System requirements

Make sure that you meet these basic hardware and software requirements.

Basic management system hardware requirements

You can install SMC on standard hardware.

- Intel® Core™ family processor or higher recommended, or equivalent on a non-Intel platform
- A mouse or pointing device (for Management Client only)
- SVGA (1024x768) display or higher (for Management Client only)
- Disk space for Management Server: 6 GB
- Disk space for Log Server: 50 GB
- Memory requirements:
  - 6 GB RAM for the Management Server, Log Server, or Web Portal Server (8 GB if all servers are installed on the same computer)

- 2 GB RAM for Management Client

Operating systems

SMC supports the following operating systems and versions.

Note: Only U.S. English language versions have been tested, but other locales might also work.

Supported Microsoft Windows operating systems (64-bit only):

- Windows Server 2016 Standard and Datacenter editions
- Windows Server 2012 R2
- Windows Server 2008 R1 SP2 and R2 SP1
- Windows 7 SP1
- Windows 10

Supported Linux operating systems (64-bit only):

- CentOS 6
- CentOS 7
- Red Hat Enterprise Linux 6
- Red Hat Enterprise Linux 7
- SUSE Linux Enterprise 11 SP3
- SUSE Linux Enterprise 12 SP1
- Ubuntu 14.04 LTS
- Ubuntu 16.04 LTS

Web Start client

The Web Start distribution of the Management Client requires that 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 later and additional Linux distributions. For SMC 6.2, JRE 1.8.0_77 or a later critical patch update (CPU) release is required.

Build version

SMC 6.2.5 build version is 10363.

This release contains dynamic update package 1031.

Product binary checksums

Use the checksums to make sure that the installation files downloaded correctly.

- smc_6.2.5_10363.zip

```
SHA1SUM:
65ed9d8270905b9ac1cf15b21964cb8e78ab0c92

SHA256SUM:
fcf536200602e0be662ede729a6cd335d009006a306d2385d5b76e2c70d98470

SHA512SUM:
7eacd3de13e51abf592cff903214f9b6
418126833bb17950c50e3c02c0be6654
6e3b83f2c31dc5dfd1a006ab4bd34e48
a719278f6e4414b8156718e970db9c11
```

- smc_6.2.5_10363_linux.zip

```
SHA1SUM:
4d47d07f1f982a38778a7d669074cae9bff17af3

SHA256SUM:
3fa31fcdfa872474e75db73fbc6c9ce97403f0c3294e6d7e2fd4919d10412361

SHA512SUM:
f95e850295c1a84bc43e7bd2645b2d8a
22266a6fe36db5ecbf0e4ee6a81b690c
a8b45e2982235e6b96c5f35bdfb2e7ea
a670bed640c10da1f91444ab81ecf8c8
```

- smc_6.2.5_10363_windows.zip

```
SHA1SUM:
537b9e3ba90760508ddbf000ee0c0dfac434a20d

SHA256SUM:
793e2e731ee79362fee3ba4ea78279f21aa5a76f0d6d2ce54d6722887a633fd9

SHA512SUM:
acdfced29c16d7768b5780974eac6e77
87319ca8a9eb5cca38259771cf4e636b
8f309c7e4ccc058cc71a912c1a36e426
80607f78d86aedb1ef8f3291155d474c
```

- smc_6.2.5_10363_webstart.zip

```
SHA1SUM:
e5f3f7744bcdc2c6d5a80cdd36ca86fef6cd874b

SHA256SUM:
acaae2bac77c2400c7c37f015e5083046b5ed23409661e1ec09ef6884f97cd5b

SHA512SUM:
6efbc9df6509916d9c089671061896ae
9402291366829 3185f350df53b6bb091
b7b626319e9b1347536c4dd2ad59af7c
ca12ce301cd69647dad4c798eea82f22
```

Compatibility

SMC 6.2 has the following requirements for compatibility and native support.

Note: SMC 6.2 can manage all compatible Forcepoint NGFW engine versions up to and including version 6.2.

Compatible component versions

SMC 6.2 works with the following component versions.

Note: Some versions of Forcepoint NGFW might have reached end-of-life status. We recommend that you use a Long-Term Support version that is still supported. For more information about the Forcepoint NGFW lifecycle policy, see Knowledge Base article 10192.

- Forcepoint™ Next Generation Firewall (Forcepoint NGFW) 6.2
- 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 Security Engine 5.5
- Stonesoft Firewall/VPN Express 5.5
- McAfee® ePolicy Orchestrator® (McAfee ePO™) 5.0.1 and 5.1.1
- McAfee® Enterprise Security Manager (McAfee ESM) 9.2.0 and later (9.1.0 CEF only)

Native support

To use all features of SMC 6.2, Forcepoint NGFW 6.2 is required.

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*.

Forcepoint Advanced Malware Detection

Forcepoint Advanced Malware Detection uses file reputation scans in a sandbox service to detect advanced threats. The Cloud Sandbox analyzes the behavior of files in a restricted operating system environment and returns a reputation score for the files. From the Logs view of the Management Client, you can access an external portal where you can view detailed reports for files that have been analyzed in the Cloud Sandbox. You can also use analysis and reporting tools in the external portal.

Note: Forcepoint Advanced Malware Detection requires a separate license for the Cloud Sandbox service. See Knowledge Base article 12514.

Pending configuration changes shown for NGFW Engines

You can now view configuration changes that you and other administrators have made before the new configurations are transferred to the engines. The pending changes are shown in the Home view and on the selected engine's home page. You can optionally also enforce an approval workflow. When an approval workflow is enforced, administrators with unrestricted permissions must approve all pending changes before the changes can be committed.

New search bar in the Management Client

There is a new search bar in the Management Client header. The search bar is the fastest way to find elements, folders, and actions. You can also access related drill-down actions, and drag and drop elements from the search results list to other views, such as the Policy Editing view or the Routing view for an engine.

Support for Sidewinder Proxies on Virtual NGFW Engines in the Firewall/VPN role

You can now use Sidewinder Proxies (HTTP, SSH, TCP, and UDP) on Virtual NGFW Engines in the Firewall/VPN role. Sidewinder Proxies on Forcepoint NGFW enforce protocol validation and restrict the allowed parameters for each protocol. Sidewinder Proxies are primarily intended for users in high assurance environments, such as government or financial institutions. In environments that limit access to external networks or access between networks with different security requirements, you can use Sidewinder Proxies for data loss protection.

DNS Relay on NGFW Engines in Firewall/VPN role

DNS relay allows NGFW Engines in the Firewall/VPN role to provide DNS services for internal networks. The firewall forwards DNS requests from clients in the internal network to remote DNS servers and temporarily stores the results of the DNS requests in the cache. The firewall can forward DNS requests to different DNS servers depending on the domain in the DNS request. The firewall can also return fixed DNS results for specific hosts or domains, and translate external IP addresses in DNS replies to IP addresses in the internal network.

Improved dynamic multicast routing support on NGFW Engines in Firewall/VPN role

You can now configure protocol-independent multicast (PIM) on NGFW Engines in the Firewall/VPN role in the Management Client. Previously, you could only configure PIM on the engine command line. You can use source-specific multicast (PIM-SSM), sparse mode (PIM-SM), or dense mode (PIM-DM).

Improved logging and diagnostics for SSL VPN Portal

Logging and diagnostics have been improved for the SSL VPN Portal. Log entries are generated when an SSL VPN Portal user starts and ends a session. If diagnostics are enabled for the SSL VPN Portal, log entries are also generated for HTTP or HTTPS transactions. SSL VPN Portal users can see the time of their last logon and the number of failed logon attempts in the status bar of the SSL VPN Portal.

Enhancements

This release of the product includes these enhancements.

Enhancements in SMC version 6.2.0

Enhancement	Description
NetLink-specific DNS IP addresses	You can now define NetLink-specific DNS IP addresses for static NetLinks. Dynamic NetLinks can automatically learn DNS IP addresses.
Improved configuration of User Responses	User Responses are now easier to configure. The new message response allows you to quickly create simple messages without using HTML markup. You can also use variables in User Responses to provide connection-specific information to the end users.
Improvements to Home view and Management Client look-and-feel	Several small enhancements have been made to the Home view in the Management Client. The look-and-feel of the Management Client has also been improved. For example, in the Home view, the layout of the panes changes dynamically, and you can now access relevant drill-down actions when you place the cursor over status cards for NGFW Engines and VPN elements.
Improvements in the Logs view	You can now save your column selections and layout in the Logs view.
Improvements in log forwarding performance	Log forwarding performance has been improved on the Log Server.
Improvements in Overviews	The maximum tracking period is now one month instead of one day in Overviews.
Automatic licensing on first-time installations	When you install the SMC for the first time, it now sends the proof-of-license codes to the Forcepoint License Center, and it generates and installs new licenses automatically by default.
More settings for Automatic Rules	You can now enable or disable Automatic Rules for authentication, DNS relay, and DHCP relay for Firewalls, Virtual Firewalls, and Master NGFW Engines. You can define whether the following types of traffic are allowed: • Traffic from the engine to the ports that are used for user authentication • Traffic from clients in the internal network to the DNS ports on listening interfaces for DNS relay • Connections from the engine to domain-specific DNS servers • Connections from interfaces on which DHCP relay is active to remote DHCP servers

Enhancements in SMC version 6.2.1

Enhancement	Description
Custom timeout for status surveillance alerts	When the Management Server is unable to contact an engine, it sends an alert after a timeout is reached. By default, the length of the timeout is 15 minutes. You can now change the length of the timeout. To change the timeout, add the following parameter to the <installation directory>/data/SGConfiguration.txt file on the Management Server: STATE_SURVEILLANCE_FREQUENCY=<time in milliseconds>
Status surveillance for Log servers	You can now enable status surveillance for Log Servers. An alert is sent when status information is not received.
Log Server high availability for monitoring routing	If the main Log Server becomes unavailable, the backup Log Server can now provide monitoring data for the Routing Monitoring view.

Enhancements in SMC version 6.2.2

Enhancement	Description
SMC API provides more appliance information	The SMC API can now provide information about the models of the NGFW appliances that are managed by the SMC.

Enhancements in SMC version 6.2.4

Enhancement	Description
Reusable task schedules	You can now drag and drop the task schedule from one Task element to another Task element to apply the same schedule to multiple tasks.

Resolved issues

These issues are resolved in this release of the product. For a list of issues fixed in earlier releases, see the Release Notes for the specific release.

Description	Issue number
In an environment with multiple Management Servers and administrative Domains, the name of the Alert Policy that is installed on the Shared Domain is not shown correctly if the Alert Policy was installed while a different Management Server was the active Management Server.	SMC-4623
You cannot edit the dynamic routing configuration for a Virtual Firewall using the SMC API.	SMC-8102
When you add a rule to a Route Map element by using the Copy Rule option on an existing rule, you cannot save the Route Map.	SMC-9672
It is possible to use the SMC API to delete a Virtual NGFW Engine element, even if it referenced in a filter.	SMC-9946
When you change the name of a Network element in the routing or antispoofing configuration using the SMC API, audit entries related to the change are corrupted.	SMC-10204

Description	Issue number
Scan detection options in Access rules that have the Discard or Refuse action are not applied. If you have enabled scan detection in the Engine Editor, you cannot disable scan detection in Access rules that have the Discard or Refuse action.	SMC-10256
The load balancing filter configuration might not be supported by the NGFW Engine in rare cases where the IP addresses of a site for a hub VPN and a site for an external VPN gateway overlap.	SMC-10325
The Save option is not available in the Engine Editor when you delete an Announced Network from the BGP settings for dynamic routing.	SMC-10475

Installation instructions

Use these high-level steps to install 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.

Note: The sgadmin user is reserved for SMC use on Linux, so it must not exist before SMC is installed for the first time.

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 with the Management Client using the **Configuration** view.

4) To generate initial configurations for the engines, right-click each Firewall, IPS, or Layer 2 Firewall element, then select **Configuration** > **Save Initial Configuration**.
   Make a note of the one-time password.

5) Make the initial connection from the engines to the Management Server, then enter the one-time password.

6) Create and upload a policy on the engines using the Management Client.

Upgrade instructions

Take the following into consideration before upgrading to SMC 6.2.

Note: SMC (Management Server, Log Server, and Web Portal Server) must be upgraded before the engines are upgraded to the same major version.

- SMC 6.2 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.
- To upgrade an earlier version of the SMC to 6.2, 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 dynamic update package has previously been imported or downloaded before the upgrade, the newer dynamic update package is activated instead.
- Upgrading is supported from SMC versions 5.6.2–6.2.4. Versions earlier than 5.6.2 require an upgrade to one of these versions before upgrading to 6.2.5.

Known issues

For a list of known issues in this product release, see Knowledge Base article 12495.

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*

- *Stonesoft VPN Client User Guide* for Windows or Mac
- *Stonesoft VPN Client Product Guide*