



FORCEPOINT

NGFW Security Management Center

Release Notes

6.2.1

Revision A

Contents

- [About this release](#) on page 2
- [System requirements](#) on page 2
- [Build version](#) on page 3
- [Compatibility](#) on page 5
- [New features](#) on page 5
- [Enhancements](#) on page 7
- [Resolved issues](#) on page 8
- [Installation instructions](#) on page 10
- [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); 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

In addition to the operating systems listed, SMC can be accessed through Web Start by using Mac OS 10.9 or later and JRE 1.8.0_77 or a later critical patch update (CPU) release.

Build version

SMC 6.2.1 build version is 10354.

This release contains Dynamic Update package 918.

Product binary checksums

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

- **smc_6.2.1_10354.zip**

```
SHA1SUM:
298353aa081cfbf7225958d228c8679e0c18d0c3

SHA256SUM:
5d31483bc199c7baae60076c8d39a97ab9538cc208d826957a1635413de1366b

SHA512SUM:
baa343ae93f81bf57dc2d737f9de3bd7
ccaa019b5adb862fe4555d800c807990
ac6ea016a2e663a471798734847727a5
41721496ff74ab5ac6f05a629429b248
```

- **smc_6.2.1_10354_linux.zip**

```
SHA1SUM:
0ea9a960de716192e6d23713cb85ae7b274f2521

SHA256SUM:
a30411e41ba1b72f1ac14dd3beacd227f5d30bbe192b635d603f07433d04325b

SHA512SUM:
cfe0a9a22a55bbf72f77c53f54bfd993
bcd8593f902ceb99280c0c59eedc2598
3e8b466fa869d211a3bd868d55a1a449
8d950c707dac318082b3afb5bd79656b
```

- **smc_6.2.1_10354_windows.zip**

```
SHA1SUM:
837d3de69af16948a8d1e86902af48664d297fa1

SHA256SUM:
6e193c06ff1d6aefbd6e8c890272727b10e146e644be18fe0e1347cce0dcc482

SHA512SUM:
9257915d2156ad5a568feb98c4658dc3
c92e811815c4cf05948b2bafc12c8282
0dba793fff3b9cf7a344edb55490075d
7b2a6de677987d8f0d08819f0490a984
```

- **smc_6.2.1_10354_webstart.zip**

```
SHA1SUM:
f28078e9e3776e6873e90aa9f4fed1bdb84f1a23

SHA256SUM:
fc36e0e5556d682f8c30728f7449178b2a279680cab6f7959fd3ed5dc0ccb035

SHA512SUM:
0cab85f8277fda66191867d19dbddead
5d22db9ee61d14a4780688ce2df4b705
c0c90038c81f55b65f0bef7bd81e0e34
9ff5787e6cc58f281f770cf5a831fdd1
```

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: <ul style="list-style-type: none"> 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.

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
The Management Server does not send alerts generated by the Management Server itself to any other Log Servers if the Log Server selected in the Management Server Properties dialog box is not available.	SMC-803
When an Exception rule in the Inspection policy that blacklists traffic uses Attacker or Victim as the address of an endpoint, the scope of the blacklist entry might be too wide. Some Situations, especially Correlation Situations, might not include Attacker or Victim information. When this information is missing, the blacklist entry uses Any as the address of the endpoint.	SMC-1260
When you select an engine element in the Home view, a list of active alerts is shown. If you click an alert, the alert might not open, and you might see the following type of message: "Cannot open the Active Alerts view".	SMC-2403
When there are a large number of element status cards in the Home view of the Management Client, the element status cards might load slowly.	SMC-3050
When you save the initial configuration for an engine, there is the option to select the security policy to be installed automatically once the engine makes initial contact with the Management Server. If you select this option, and do not soon make initial contact, the Management Server might run out of memory.	SMC-3209
SYN Rate Limits configured in the Advanced Settings for IPS elements are enabled only for incoming traffic on the first interface of an Inline Interface pair.	SMC-3956
When you copy information from the Hex pane in the Logs view, only the hexadecimal numbers are copied. The resolved values are not copied.	SMC-3999

Description	Issue number
If you import a new license or close the License Properties dialog box by clicking OK, the Management Server tries to contact Forcepoint servers even when the "Enable Sending Proof-of-License Codes to FORCEPOINT Servers" option is not selected in the Global System Properties dialog box. The following message might be shown: "Update server not available - can't get url: https://update.stonesoft.com/index.rss. Server could not save appliance initial configuration. Appliance Initial Configuration upload failed: appliance Proof-of-Serial is missing." It is also not possible to add the Proof-of-Serial code for a Single Firewall element after you have saved the element for the first time.	SMC-4058
When you select an NGFW Engine element in the Home view, a list of active alerts is shown. When you click an alert, the alert might not open. The following message might be shown: "Cannot open the Active Alerts view".	SMC-4107
Importing MIBs fails.	SMC-4185
The sgRestoreMgtBackup command does not list the available backup files in a logical order. The files are not ordered alphabetically or chronologically.	SMC-4218
When you use the Create Multiple Single Firewalls wizard to create several Single Firewall elements, the Proof-of-Serial (POS) codes are not saved. The wizard fails to finish, and the following message is shown: "Failed to upload the initial configuration to the Installation Server. Management Server could not save appliance initial configuration. Appliance Initial Configuration upload failed: appliance Proof-of-Serial is missing." It is also not possible to add the Proof-of-Serial code for a Single Firewall element after you have saved the element for the first time.	SMC-4254
When you delete an Incident Case element, the files attached to it are not deleted. The files are still stored in the <installation directory>/data/incidents/<ic_id> directory on the Management Server.	SMC-4293
When you select View Logs for a VPN in the Home view, the Logs view fails to open.	SMC-4333
When you create a manual blacklist entry based on an alert entry in the Active Alerts view, the source and destination IP address might be reversed in the blacklist entry.	SMC-4350
When there is a default route through both a NetLink and a Tunnel Interface, the routing configuration generated for the engine is incorrect. Outbound traffic might try to use the wrong interface.	SMC-4632
When you use the NGFW Initial Configuration Wizard, the status of the node changes, even if you cancel using the wizard. In the Management Client, the status information is not shown and the configuration status in the properties of the node is "Configured".	SMC-4633
When installing a policy, the Management Server increments the policy identifier by one when uploading the new policy. When uploading policies for Single Firewalls and Firewall Clusters at the same time, the Management Server might use same policy identifier for two or more elements. The policy installation fails if the engine receives a policy identifier that is lower than the identifier for the current policy.	SMC-4860
When you select a third-party element or an SMC server element in the Home view, the diagram might take a long time to appear. When there is a large number of monitored third-party and server elements, drawing diagrams might use too much memory.	SMC-4905
When you use administrative Domains, it is not possible to create new elements using the + in the Home view for a specific Domain.	SMC-4943
When log forwarding is enabled, the Log Server might stop working correctly if any of the target hosts that receive logs are unavailable.	SMC-4978

Description	Issue number
If you remove an IP address from an interface and add the same IP address to another interface without saving the intermediate changes, the IP address is configured on both interfaces.	SMC-5007
After you recertify a Log Server, the Log Server might fail to connect to the Management Server.	SMC-5023
If an Overview Template element does not include information about the date when it was created and the administrator who created it, you cannot delete the Overview Template.	SMC-5041
It is not possible to save changes to SMC API Client elements unless you change the authentication key.	SMC-5073
In an environment with multiple Management Servers and Log Servers, memory consumption on servers that monitor other SMC servers can increase when one of the SMC servers is unavailable for a long time.	SMC-5076
When there is an Alias element in the Trash, you cannot save changes in the Engine Editor.	SMC-5093
Saving a policy fails if you edit the time range on a rule then move the rule up or down in the policy.	SMC-5156
When you add a contact address to a Tunnel Interface or change the IP address of a Tunnel Interface, routing for the Tunnel Interface might become invalid.	SMC-5231
When the Log Server selected for a Management Server is unavailable, the replication status for the Management Server changes to red. Even if you select a different Log Server for the Management Server, the replication status does not recover.	SMC-5242
After upgrading the SMC, manually added elements under tunnel interfaces in the Antispoofing tree might disappear.	SMC-5311
The Approve All option for Pending Changes might fail, especially after an element has been deleted.	SMC-5325
When you use the SMC API to edit a dynamic routing Route Map, if you modify any field other than Matching Condition, the existing value in the Matching Condition field is removed.	SMC-5424
On NGFW Engine versions lower than 6.1, policy installation might fail when the policy includes IP Address List elements. IP Address Lists were introduced in NGFW version 6.1 and are not supported on lower engine versions.	SMC-5498
When the Management Server service is not running, new active alerts are spooled on the Log Server. After the Management Server service starts, the waiting alerts might not be forwarded to the Management Server.	SMC-5823

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.
- Upgrading is supported from SMC versions 5.6.2 – 6.1.3 and 6.2.0. Versions earlier than 5.6.2 require an upgrade to one of these versions before upgrading to 6.2.1.

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*

