FORCEPOINT

NGFW Security Management Center

Release Notes

6.2.2

Revision B

Contents

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 6.2.2 build version is 10356.

This release contains dynamic update package 951.

Product binary checksums

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

- smc_6.2.2_10356.zip

```
SHA1SUM:
9ff966785828751a2773fc0d5d68057d192da757

SHA256SUM:
90759563345bac3f7a21c6d196e87d5ed6cc750a59d24a68cf570cbaba1bba66

SHA512SUM:
281866833a2bed060603394e3dca7712
00912d13d62b5fed3899513038239491
cc85fbe1c5c447c9ad8ef9c27b67a684
a469dd04986f8da7fedbeb1c3abfb329
```

- smc_6.2.2_10356_linux.zip

```
SHA1SUM:
19455af7e2c2c7d3b6ef1c571a70ba6dc1ca2904

SHA256SUM:
c8bfbb9c861f4a87498a59568cc1fb5020688b827b32b101c9adec1c7a9099ce

SHA512SUM:
bce87891c2dd45306ea85dfac2311973
bd715c0f48476ee308e9b85999328653
476b0238306b53cb3d25d3e4ab07e8b7
968416a508334fc2fe19633624791377
```

- smc_6.2.2_10356_windows.zip

```
SHA1SUM:
1a65dfd6977b47870320ecb1f02e6e10cae07b4d

SHA256SUM:
8e08a321151f2671033feca656a12cbc69dbf122de409db535e4a7c80c204577

SHA512SUM:
f10456e4cc5d88ad8e4a4b45e54f04ad
240a43777cef7cb6d8f7e72bb76397f9
1667dec4479e7e5b3e9212c740c3d952
1747d6bee99c4fd3e92705b3843df6ea
```

- smc_6.2.2_10356_webstart.zip

```
SHA1SUM:
c28cb0ddeed8b35c47562afd4d32fde214b1f06d

SHA256SUM:
6c1fa09bf75cffd08d69493556aa6ea2985f8cdf82a146766c6292961a16a5fc

SHA512SUM:
0e1798dd8f217bafbb69f3c574ef4858
6a52ebaa36bfb1cbf2ee453bc726148a
2762597b3de6136575d83af6888a89e6
ab092d689f5a45127e79b6d514744cac
```

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.

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 the Engine Editor, you cannot add more than one contact address exception for each IP address on an interface. When you add a second row in the Exceptions dialog box, it is not possible to enter the IP address.	SMC-3681
If you edit the contents of the NAT cell in an IPv4 NAT or IPv6 NAT rule in a Firewall Policy, the changes are not saved.	SMC-5135
When nodes in a cluster have been disabled, status surveillance might incorrectly generate alerts.	SMC-5531
Uploading an Alert Policy might fail if Active Alerts are received from the Log Server at the same time. This issue is especially likely to occur in environments with multiple Log Servers after the Management Server or Log Server service has been restarted.	SMC-5734
If the policy includes Correlation Situations for deep inspection, policy validation might fail in SMC 6.2.	SMC-5767
Installing an Alert Policy for a administrative Domain fails. The following error message is shown: "Transaction failed. Operation was cancelled. Details: Attribute reading failed".	SMC-5774

Description	Issue number
When you add a default contact address or a contact address exception to an interface in the Engine Editor, the following type of validation error is shown when you save the changes: "The contact address of the <interface> is not valid because <name> is already located in <name>". The same problem can occur when saving other changes in the Engine Editor if a default contact address and a location are defined for the engine.	SMC-5806
Progress information for tasks related to policies, such as the Refresh Policy, Upload Policy, or Validate Policy Tasks, might fail to open in a separate tab. These tasks do not appear in the Task History after they are run.	SMC-5838
When configuring VRRP settings for an interface, the changes are not saved.	SMC-5886
After upgrading to SMC version 6.2.1, the Management Server might not start if there are pending changes related to a deleted element.	SMC-5891
Due to the large number of notifications that the Management Client receives, the Management Client can become slow in environments that a very large number of engines and administrators.	SMC-6000
The backup Log Server does not provide monitoring data for the Routing Monitoring view for Virtual NGFW Engines.	SMC-6116
When Scan Detection Mode is set to On for an engine, scan detection triggers alerts even though an Access rule disables scan detection.	SMC-6147
When an Administrator Role does not include the Manage Alerts permission, administrator accounts that use the Administrator Role cannot run tasks. For example, the Refresh Policy Task is not available for administrators who do not have the Manage Alerts permission.	SMC-6148
In large configurations where a custom Alias has values defined for all firewalls, policy installation might be slow because creating policy snapshots takes a long time.	SMC-6286
When Web Portal Users try to view a policy in the Web Portal, the following error message is shown: "Unexpected internal error". Administrators can use the Web Portal normally.	SMC-6338
When the Service in an Access rule is NAT-T (Destination) or NAT-T (Source), the Management Server generates an incorrect configuration for the firewall.	SMC-6363
When you specify the Limit in a QoS Policy as a percentage, the Management Server might generate an incorrect configuration for the firewall.	SMC-6386
On Linux, SMC installation does not work correctly if the /tmp filesystem has the noexec flag set. Installation finishes with the following message: "The installation of Stonesoft Management Center is complete, but some errors occurred during the installation."	SMC-6442
When you add a VPN Gateway to the Central Gateways list, and select the Gateway for Mobile VPN access, creating a new Mobile VPN might fail. The following message is shown: "No gateways are included in the VPN".	SMC-6480
When there are a large number of forwarded logs, the Log Server might stop receiving logs. The status of engine elements is shown as red.	SMC-6558

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 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 5.6.2–6.1.3 and 6.2.0–6.2.1. Versions earlier than 5.6.2 require an upgrade to one of these versions before upgrading to 6.2.2.

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*