



# **FORCEPOINT**

## **NGFW Security Management Center Appliance**

**Release Notes**

**6.2.5**

Revision A

## Contents

- [About this release](#) on page 2
- [Compatibility](#) on page 2
- [New features](#) on page 3
- [Enhancements](#) on page 4
- [Resolved issues](#) on page 6
- [Installation instructions](#) on page 7
- [Known issues](#) on page 8
- [Find product documentation](#) on page 8

## About this release

This document contains important information about this software release for the Forcepoint NGFW Security Management Center Appliance (SMC Appliance).

We strongly recommend that you read the entire document.

The SMC Appliance ships with pre-installed Forcepoint NGFW Security Management Center (SMC) software. The pre-installed SMC includes a Management Server and a Log Server.



**Note:** The SMC Appliance does not support high-availability for the Management Server or the Log Server.

The SMC Appliance software can also be installed on a virtualization platform. For more information, see the *Forcepoint Next Generation Firewall Installation Guide*.

## 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.

Enhancement	Description
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.

## 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.
New commands for SMC Appliance	The following new subcommands of the smca-system command have been added: <ul style="list-style-type: none"> <li>smca-system serial-number — Shows the hardware serial number for the SMC Appliance.</li> <li>smca-system fingerprint — Shows the fingerprint for the CA used by the Management Client.</li> </ul>

## 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
Administrators with unrestricted permissions are replicated on the SMC Appliance as local users. API Clients with unrestricted permissions are also replicated on the SMC Appliance even though API Clients do not have passwords.	SMC-10110
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
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 the SMC Appliance.

For detailed information about installing the SMC Appliance and the NGFW Engines, see the *Forcepoint Next Generation Firewall Installation Guide*. All guides are available for download at <https://support.forcepoint.com>.

## Steps

- 1) Turn on the SMC Appliance.
- 2) Select the keyboard layout for accessing the SMC Appliance on the command line.
- 3) Accept the EULA.
- 4) Enter the account name and password.  
For credential requirements, see the *Forcepoint Next Generation Firewall Installation Guide*.
- 5) Make your security selections.
- 6) Complete the network interface and network setup fields.
- 7) Enter a host name for the Management Server.
- 8) Select the time zone.
- 9) (Optional) Configure NTP settings.
- 10) After the SMC Appliance has restarted, install the Management Client.  
You can use Java Webstart or install the Management Client from a file to allow remote access to the SMC. Java Web Start is enabled by default on the Management Server that is pre-installed on the SMC Appliance.
- 11) Create the NGFW Engines elements, then install and configure the NGFW Engines.

## Upgrade the SMC Appliance

---

Upgrade the SMC Appliance from a previous version to version 6.2.5.



**CAUTION:** Before upgrading the SMC Appliance from version 6.2.0, install the 6.2.0P001 patch. For more information, see Knowledge Base article [14168](#).



**Note:** The SMC Appliance must be upgraded before the engines are upgraded to the same major version.

## Steps

- 1) Log on to the SMC Appliance.

- 2) Enter `sudo ambr-query` and press **Enter** to check for available patches.
- 3) Enter `sudo ambr-load <patch>` and press **Enter** to load the patch on the SMC Appliance. To load the patch that upgrades the SMC Appliance to version 6.2.5, enter `sudo ambr-load 6.2.5U001` and press **Enter**.



**Note:** If you downloaded the patch and transferred it to the SMC Appliance, append the load command with the `-f` option and specify the full path to the patch file. For example, `sudo ambr-load -f /var/tmp/6.2.5U001.sap`.

- 4) Enter `sudo ambr-install <patch>` and press **Enter** to install the patch on the SMC Appliance. To install the 6.2.5U001 SAP, enter `sudo ambr-install 6.2.5U001` and press **Enter**. The installation process prompts you to continue.
- 5) Enter `y`.

## Result

The installation process restarts the appliance and installs the patch. When the upgrade is finished, the appliance restarts. The appliance is now running SMC Appliance 6.2.5.

# Installing SMC Appliance patches

---

We recommend checking the availability of SMC Appliance patches regularly, and installing the patches when they become available.

The SMC Appliance patches can include improvements and enhancements to the SMC software, the operating system, or the SMC Appliance hardware.

For detailed information about installing SMC Appliance patches, see the *Forcepoint Next Generation Firewall Installation Guide*. All guides are available for download at <https://support.forcepoint.com>.

# 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*

