FORCEPOINT

NGFW Security Management Center Appliance

Release Notes

6.3.4

Revision A

Contents

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. You can alternatively install the SMC Appliance software on a virtualization platform.

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

Build version

SMC 6.3.4 build version is 10442.

This release contains Dynamic Update package 1036.

Product binary checksums

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

- 6.3.4U001.sap

```
SHA1SUM:
dc10ff90866868f5c45c99bb56924102d546b496

SHA256SUM:
1dccc678fa73cefc3c3fa0399aaddcd1529b5b299ad903c3745c5be209e9a849

SHA512SUM:
7d470a956fe8cc42792570d11b27b8da
a91e473df257d44d213db05b8f9fd1ee
ec3844e3d2effd8697e290d3a732c7c8
cb4b4b8f2b0c27e9cf2701daf64f0135
```

System requirements on virtualization platforms

We strongly recommend using a pre-installed SMC Appliance as the hardware solution. You can alternatively install the SMC Appliance software on a virtualization platform.

The following requirements apply:

- VMware ESXi version 6.0 or higher as the hypervisor
- 120 GB virtual disk minimum
- 8 GB RAM minimum
- At least one network interface

Note: The .iso installation file that is used to install the SMC Appliance software on a virtualization platform is available only for major versions of the SMC Appliance. To install the maintenance version, first install the .iso for the major version, then upgrade to the maintenance version.

Compatibility

SMC 6.3 is compatible 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.

SMC 6.3 can manage all compatible Forcepoint NGFW engine versions up to and including version 6.3.

- Forcepoint™ Next Generation Firewall (Forcepoint NGFW) 6.2 and 6.3
- 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™) 5.0.1 and 5.1.1
- McAfee® Enterprise Security Manager (McAfee ESM) 9.2.0 and later (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*.

Support for Forcepoint Endpoint Context Agent

Support for Forcepoint Endpoint Context Agent (ECA) allows you to use endpoint information in the Forcepoint NGFW policy to control access, identify users, and log their actions. ECA is a Windows client application that provides endpoint information to the NGFW Engine. ECA is a replacement for McAfee Endpoint Intelligence Agent (McAfee EIA).

CAUTION: If McAfee Endpoint Intelligence Agent (McAfee EIA) is configured on the NGFW Engine when you upgrade to version 6.3 or later, the NGFW Engine node is returned to the initial configuration state and stops processing traffic. You must remove the McAfee Endpoint Intelligence Agent (McAfee EIA) configuration and refresh the policy before you upgrade to version 6.3 or later. For more information, see Knowledge Base article 14093.

Multi-Layer Deployment for NGFW Engines in the Firewall/VPN role

Multi-layer deployment is now supported for NGFW Engines in the Firewall/VPN role. In multi-layer deployment, NGFW Engines in the Firewall/VPN role have both layer 2 physical interfaces and layer 3 physical interfaces. The same NGFW Engine can now provide the features of the Firewall/VPN role, as well as the inspection features of the IPS and Layer 2 Firewall roles.

Route-based VPN improvements

The user interface for configuring a route-based VPN has been improved. Instead of configuring a single Route-Based VPN element, you can create individual Route-Based VPN Tunnel elements. The route-based VPN tunnels can be used in Administrative Domains other than the Shared Domain.

Improvements in Forcepoint Advanced Malware Detection

In addition to the cloud sandbox, Forcepoint Advanced Malware Detection now also supports on-premises local sandboxes. Other improvements include the following:

- The NGFW Engine can now delay file transfers until the results of the sandbox scan are received.
- The NGFW Engine now separately requests a file reputation for each file in .zip archives.
- The reporting tools in the external portal have been improved, and it is easier to access reports in the external portal from the Management Client.

NGFW on Azure and Hyper-V

You can now deploy NGFW Engines in the Microsoft Azure cloud to provide VPN connectivity, access control, and inspection for services in the Microsoft Azure cloud. The Microsoft Hyper-V virtualization platform on Windows 2012 and 2016 servers is now also supported for NGFW deployment on a virtualization platform in a private cloud. Only NGFW Engines in the Firewall/VPN role are supported in the Microsoft Azure cloud and on the Microsoft Hyper-V virtualization platform.

Support for Forcepoint User ID Service

Forcepoint User ID Service collects information about users, groups, and IP addresses from Windows Active Directory (AD) servers and AD domains. You can use the information from the Forcepoint User ID Service in the Forcepoint NGFW policy to identify users and control access.

Support for HTTPS in Sidewinder HTTP Proxy

The Sidewinder HTTP Proxy can now provide decryption, inspection, protocol validation, certificate validation, and certificate revocation checking for the HTTPS protocol.

Enhancements

This release of the product includes these enhancements.

Enhancements in SMC version 6.3.0

Enhancement	Description
New commands for SMC Appliance	The following new subcommands of the smca-system command have been added: • `smca-system serial-number` — Shows the hardware serial number for the SMC Appliance. • `smca-system fingerprint` — Shows the fingerprint for the CA used by the Management Client.
Second interface on the SMC Appliance	You can now configure a second interface on the SMC Appliance when you install the appliance.
Support for serial console connections on the SMC Appliance	You can now connect to the SMC Appliance using a serial console connection, or make outbound serial console connections from the SMC Appliance to other devices, such as Forcepoint NGFW appliances.
Rate limit per Virtual NGFW Engine for traffic from the Master NGFW Engine	You can now set a rate limit per Virtual NGFW Engine for traffic from the Master NGFW Engine to the Virtual NGFW Engine. When the limit is set, a single Virtual NGFW Engine that is under very heavy load cannot disrupt the operation of the other Virtual NGFW Engines that are hosted by the Master NGFW Engine.

Enhancement	Description
Dedicated control plane operation	You can now dedicate a specified number of CPUs to control plane operations. Even under very heavy loads, you can continue to manage NGFW Engines and refresh policies, and the status of the NGFW Engines remains green in the Home view.
Changes related to certificates	The NGFW Engine can now validate certificates and check the certificate revocation status for features that have certificate validation and certificate revocation checks enabled, such as features that use a TLS Profile in the configuration. Except for VPN certificates, most elements related to certificates are now found in the **Administration** > **Certificates** branch of the **Configuration** view. There is no longer a separate Pending Certificate Request element. Certificate requests are now created as TLS Credentials elements. The state of the TLS Credentials element indicates whether is it a signed certificate or a certificate request.
Limit for half-open TCP connections	As part of the SYN flood protection feature, you can now set a limit for the number of half-open TCP connections. When the limit is reached, SYN flood protection is enabled.
Improvements to SSM architecture	Improvements to SSM integration remove some previous limitations on inspection when Sidewinder Proxies are used. These former limitations include matching traffic based on Network Applications, file filtering, and URL filtering. New Combined Protocol elements allow you to apply a standard Protocol element and a Sidewinder Proxy Protocol element to the same traffic.
New commands for managing NGFW Engines and NGFW appliances	It is now possible to power off an NGFW Engine remotely through the Management Client. In addition, you can now also reset an NGFW appliance to factory settings through the Management Client. To increase security, you can set how many times you want the stored data on the file system of the NGFW appliance to be overwritten.
Task for validating policies	There is a new task for validating policies. The Validate Policy task allows you to validate the policy installed on NGFW Engines or Master NGFW Engines or the Alert Policy installed in an administrative Domain. You can run the Validate Policy task either manually or according to a schedule.
Updated product names	The NGFW product names have been updated. Stonesoft Management Center is now called Forcepoint NGFW Security Management Center (SMC), and Stonesoft Next Generation Firewall (Stonesoft NGFW) is now called Forcepoint Next Generation Firewall (Forcepoint NGFW). The new product names are used in the SMC installer, the SMC installation directory, in the Management Client, and in the list of services in the Windows Control Panel.
Improvements in change approval process	It is now possible to give individual administrators permission to approve changes. Previously, only administrators with unrestricted permissions (superusers) could approve changes. You can also specify whether administrators are allowed to approve their own changes.
Home page improvements in the Management Client	You can now easily customize the home page for components in the Home view. You can use drag-and-drop to re-organize the panes and select new panes from a predefined selection of panes to replace existing panes on the home page. You can now include statistics in home pages. The Management Server and the Log Server now have their own home page in the Home view.

Enhancements in SMC version 6.3.2

Enhancement	Description
Java cryptography extension included for Webstart clients	The Java jurisdiction policy files that are required for Webstart Management Clients to connect to Management Servers that use 256-bit encryption are now included. Java version 1.8.0_151 is required on the computer where you use the Webstart Management Client. For more information, see Knowledge Base article 10136.
SMC API enhancements	• You can use SMC API read-only queries on a standby Management Server in a high availability setup. • You can use SMC API queries to view the history information of an element. • You can use the WebSocket protocol to view active alerts for an element.

Enhancements in SMC version 6.3.4

Enhancement	Description
TLS decryption is more visible in the Logs view	TLS traffic that is decrypted is shown in the TLS Decrypted and TLS Detected log fields in the Logs 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
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
Log entries related to traffic are not stored on the Log Server and are not visible in the Logs view when you use FW-105 appliances. Log entries related to the operation of the system are correctly stored.	SMC-8700
Administrators without the Refresh Policies and Upload Policies permissions cannot save changes in the Engine Editor. A blank dialog box is shown when you try to save a change.	SMC-9644
The Log Server might incorrectly treat some transient log entries as alerts. As a result, the Active Alerts view might be full of log entries that are not alerts.	SMC-10230
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

Description	Issue number
When you add a VLAN Interface to a Physical Interface with a dynamic IP address that is enabled as a VPN endpoint, saving the changes fails. The following message is shown: "Failed to close changed element section".	SMC-10421
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
If there are several Network elements that have the same IP address but different netmasks, the wrong Network element might be added to the routing configuration when you add a route using the SMC API.	SMC-10604
When you configure log forwarding from the Log Server or audit log forwarding from the Management Server to the syslog server in the Management Client, you can select a TLS profile to enable TLS protection. You can also configure that the identity of the TLS server is checked. If the TLS server uses a certificate from an intermediate Certificate Authority (CA), log forwarding fails if only the root CA is selected as a trusted CA in the TLS profile.	SMC-10764
When you select several Log Servers for the Export Log Task, the Storage directories to export from option does not show the correct Log Server directories.	SMC-10806
With the SMC API, it is not possible to run report tasks that use a filter.	SMC-10862
It is not possible to change the name of an Alias element without editing the translation value.	SMC-10904
Policy snapshots might become corrupted if an inspection rule includes a custom Correlation Situation. This occurs when a Context for a custom Correlation Situation includes a custom Event Binding.	SMC-10963
If diagnostics mode has been enabled for Virtual NGFW Engines, the SMC API does not correctly inform which diagnostic options have been enabled.	SMC-10970
When installing a policy, and the message "Warning: X issue(s) have been detected" is shown, the report of the number of issues might differ from the actual number of issues, as duplicate issues are not correctly taken into account.	SMC-10971
When activating a dynamic update package, you might see the following warning message: "Invalid Filter Expression Authentication Server. Value is out of range in literal Literal Constant". You can ignore the warning.	SMC-11040
When you browse to Configuration > Administration > Alert Configurations > Alert Senders > Domains, the Alert Policy shown in the Info pane is not updated when the Alert Policy is installed on an administrative Domain.	SMC-11095
Rule counter values that are provided through the SMC API might not be correct.	SMC-11178

Common Vulnerabilities and Exposures (CVEs)

Audit

- Imports fixes for CVE-2015-5186. (SMC-11104)

bash

- Imports fixes for CVE-2016-0634. (SMC-11604)

Intel Page Table Vulnerability (also known as Meltdown)

- Imports fixes for CVE-2017-5754. (SMC-10776)

Linux kernel

- Imports fixes for CVE-2017-9150, CVE-2017-9077, CVE-2017-9076, CVE-2017-9075, CVE-2017-9074, CVE-2017-9059, CVE-2017-7495, CVE-2017-9211, CVE-2017-9074, CVE-2017-1000380, CVE-2017-1000364, CVE-2017-1000370, CVE-2017-1000371, CVE-2017-1000379, CVE-2017-1000253, CVE-2017-1000112, CVE-2017-1000111, and CVE-2017-14991. (SMC-11590, SMC-11621, and SMC-11632)

ncurses

- Imports fixes for CVE-2017-10685 and CVE-2017-10684. (SMC-11593)

OpenSSL

- Imports fixes for CVE-2017-3737, CVE-2017-3736, CVE-2017-3735, CVE-2016-8610, and CVE-2017-10684. (SMC-11079, SMC-11078, SMC-11077, and SMC-11596)

Samba

- Imports fixes for CVE-2017-7494. (SMC-11594)

tcpdump

- Imports fixes for CVE-2017-13027, CVE-2017-13028, CVE-2017-13025, CVE-2017-13026, CVE-2017-13035, CVE-2017-13030, CVE-2017-13023, CVE-2017-13037, CVE-2017-13032, CVE-2017-13034, CVE-2017-13029, CVE-2017-13033, CVE-2017-13036, CVE-2017-13024, CVE-2017-13031, CVE-2017-13038, CVE-2017-13725, CVE-2017-13690, CVE-2017-13689, CVE-2017-13688, CVE-2017-13687, CVE-2017-13055, CVE-2017-11108, CVE-2017-12989, CVE-2017-12896, CVE-2017-12990, CVE-2017-12985, CVE-2017-12986, CVE-2017-12900, CVE-2017-12894, CVE-2017-12987, CVE-2017-12902, CVE-2017-12898, CVE-2017-12893, CVE-2017-12901, CVE-2017-12897, CVE-2017-12895, CVE-2017-12988, CVE-2017-12899, CVE-2017-13006, CVE-2017-13000, CVE-2017-12995, CVE-2017-12996, CVE-2017-12992, CVE-2017-13002, CVE-2017-13004, CVE-2017-13001, CVE-2017-12999, CVE-2017-13003, CVE-2017-12998, CVE-2017-12993, CVE-2017-12994, CVE-2017-12991, CVE-2017-12997, CVE-2017-13005, CVE-2017-13022, CVE-2017-13016, CVE-2017-13015, CVE-2017-13020, CVE-2017-13012, CVE-2017-13019, CVE-2017-13007, CVE-2017-13008, CVE-2017-13010, CVE-2017-13011, CVE-2017-13009, CVE-2017-13021, CVE-2017-13014, CVE-2017-13013, CVE-2017-13018, CVE-2017-13017, CVE-2017-13053, CVE-2017-13049, CVE-2017-13054, CVE-2017-13045,

CVE-2017-13046, CVE-2017-13043, CVE-2017-13048, CVE-2017-13050, CVE-2017-13041, CVE-2017-13052, CVE-2017-13039, CVE-2017-13040, CVE-2017-13042, CVE-2017-13044, CVE-2017-13051, and CVE-2017-13047. (SMC-11605, SMC-11616, SMC-11613, SMC-11622, SMC-11623, SMC-11624, and SMC-11625)

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) Import the licenses for all components.
    You can generate licenses at https://stonesoftlicenses.forcepoint.com.

12) 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 6.3.4.

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.

SMC 6.3 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.

Steps

1) Log on to the SMC Appliance.

2) Enter `sudo ambr-query`, then press **Enter** to check for available patches.

3) Enter `sudo ambr-load <patch>`, then press **Enter** to load the patch on the SMC Appliance.
To load the patch that upgrades the SMC Appliance to version 6.3.4, enter `sudo ambr-load 6.3.4U001`, then 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/6.3.4U001.sap`.

4) Enter `sudo ambr-install <patch>`, then press **Enter** to install the patch on the SMC Appliance.
To install the 6.3.4U001 SAP, enter `sudo ambr-install 6.3.4U001`, then 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 6.3.4.

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 14117.

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*