FORCEPOINT

NGFW Security Management Center

Release Notes

6.3.7

Revision A

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

To use this product, your system must 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 6.3, JRE 1.8.0_121 or a later critical patch update (CPU) release is required.

Build version

SMC 6.3.7 build version is 10449.

This release contains Dynamic Update package 1084.

Product binary checksums

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

- smc_6.3.7_10449.zip

```
SHA1SUM:
6f4f95bb171f52f0b8286653443e84aee015fe87

SHA256SUM:
0baa304d787ebe7dab3570a88f824d7fe0a932347e190897c0b31a0d6d451e75

SHA512SUM:
3133adca7d7dc9c27d7cb08fbb9d5141
db1db3dad3855959a0f4f6106613add5
55a6e64171fc22009aee85d5da8c0cf8
017a61f7e43eca0db81bd78d04fd8abc
```

- smc_6.3.7_10449_linux.zip

```
SHA1SUM:
5633b10afc1f798eb4848479bb7637dba5596aa3

SHA256SUM:
5016130e6ef061dcaae723d764ce5c2f1479d62eba6a222df26d6f84e9e25042

SHA512SUM:
5af59345395b02d55d449834c9dbea25
47e34087d5112de18015dc3932b0289f
7f2afda48479c1046db3517c9ccd42ef
daffcf2b568fa459d7341ffbc7c64a84
```

- smc_6.3.7_10449_windows.zip

```
SHA1SUM:
d86e4a31999b46fd5aebbfebeda24bf5722ea5f6

SHA256SUM:
f12b5dd65e4f1644e080909900c22ba03386c4131fb9211e9f86590db891d69f

SHA512SUM:
c40bda1c1030cd608892aabc7e4553bd
08622e1d268a3cff0d37d2d065da17c5
613e7cd9a759d8a708ffb065f5d7b093
36a4e1f93c35a33cfa123e7d1b18d095
```

- smc_6.3.7_10449_webstart.zip

```
SHA1SUM:
117a5ac4ac4bf99a516abe3aa675622c8c4aa509

SHA256SUM:
1092387f8dc4eb3dd89e99fb9d2ea9f18e2f78d32674a9bf123e3053db1f50eb

SHA512SUM:
3f69e2112eb9be1931d4bd712a1c6e28
9a9d8f7066e9bafe021ea03944ae9c37
6b54f2797259b12249f8c549963a9cd8
85457fae34dce9b80f4dfd3310d00c82
```

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
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.
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.
Cloud Discovery Tool	The SMC installer now includes the optional Cloud Discovery Tool component. The Cloud Discovery Tool is a command line tool that can process log data exported from the SMC to produce a summary report about cloud application usage. The Cloud Discover Tool requires a separate license.
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.

Enhancement	Description
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.
SYN rate limits support IPv6 connections	SYN rate limits now also support IPv6 connections.
SMC API improvements	Tasks and their scheduling can be managed through the SMC API.

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.

Enhancements in SMC version 6.3.5

Enhancement	Description
Improved sorting of Network elements	When you sort Network elements by IP address, the elements are sorted first by IP address, then by netmask.
License reporting tool	There is a new tool for MSSP customers that exports all data related to licenses and NGFW Engines to a CSV file.

Enhancements in SMC version 6.3.6

Enhancement	Description
Delete VPN SA monitoring entries using WebSocket API	In addition to acknowledging alerts and deleting blacklist entries, it is now possible to delete entries from the VPN SA Monitoring view using the WebSocket API. For more information about the WebSocket API, see Knowledge Base article 15540.

Resolved issues

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

Description	Issue number
Searching for ANY in the Service cell of rules does not work as expected.	SMC-9408
In an environment where there are multiple Log Servers for high availability, a large number of NGFW Engines, and frequent policy uploads, there might be replication issues in event correlation if a Log Server temporarily becomes unavailable.	SMC-12664
Creating a policy-based VPN where all central gateways have dynamic IP addresses and use a DNS name as the Phase-1 ID might fail. The following message is shown: "Endpoint with dynamic IP addresses in the Endpoint A<-> Endpoint B tunnel cannot have the same Phase1-ID (DNS : <name>)".	SMC-13192
When you are modifying the comment for an Access rule in a policy, the Comment field might unexpectedly close, removing any changes that you have made. This issue can be caused by, for example, another administrator opening another policy for editing.	SMC-13600
When the final action in an Alert Chain is None, and there are several matching rules in the Alert Policy, processing of the Alert Policy does not stop at the first matching Alert Chain. Alerts might match several rules, and several notifications might be sent for the same alert.	SMC-13755
The progress tab for Delete Log Tasks shows the number of logs that have been deleted. The number that is shown might be higher than the actual number of logs that have been deleted.	SMC-13766
It is not possible to modify Active Directory Server elements that have Domain Controllers configured using the SMC API.	SMC-13767
When you configure a GRE tunnel in a route-based VPN, the default contact address for the interface is always used for the endpoints.	SMC-13778

Description	Issue number
When several Management Clients connect to the Management Server at the same time, all of the new connections might fail. For example, after the Management Server restarts, several administrators connecting at the same time might block access to the Management Server.	SMC-13863
When a rule matches a rule search, the rule is highlighted. After some time, the highlight disappears.	SMC-13864
Creating Virtual Firewall elements using the SMC API fails if a value is defined for the "Additional Networks to Automatically Add to Antispoofing" option in the Dynamic Routing settings.	SMC-13972
If you refresh the policy on an NGFW Engine in the Home view, the Management Client might freeze.	SMC-14022
In the Routing tree, you cannot add a host to an OSPF area. The following message is shown: "In the Dynamic Routing configuration, OSPFv2 Area <area> should only have a Host defined in Unicast Communication Mode."	SMC-14036
If you edit a policy both in the Management Client and in the SMC API, this might lead to a situation where you cannot open the policy for editing. The following message is shown: "Attribute reading failed".	SMC-14076
When you change the type of the internal certificate authority in an environment with multiple Management Servers, the recertification process might not be able to generate new certificates for the additional Management Servers.	SMC-14299
Installing a policy on multiple NGFW Engines at the same time takes longer than expected.	SMC-14396
A duplicate name warning is incorrectly shown when you open a rule name for editing, then click OK to close the dialog box.	SMC-14438
When you search for elements, "Wait..." is shown at the bottom of the search results even though the search is finished and all results are shown.	SMC-14476
You cannot use the SMC API to edit permissions for NGFW Engine elements to define the allowed policies.	SMC-14534

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.

Note: If you install the SMC on Windows 10 and Windows Defender is enabled, it might take a long time to activate a dynamic update package. For more information, see Knowledge Base article 14055.

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 the SMC.

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

- SMC 6.3 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.
- To upgrade a previous version of the SMC to 6.3, 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 – 6.2.5 and 6.3.0 – 6.3.6. Versions earlier than 5.6.2 require an upgrade to one of these versions before upgrading to 6.3.7.

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*