NGFW Security Management Center

Release Notes

6.3.0

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 6.3, JRE 1.8.0_121 or a later critical patch update (CPU) release is required.

Build version

SMC 6.3.0 build version is 10417.

This release contains Dynamic Update package 988.

Product binary checksums

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

- smc_6.3.0_10417.zip

```
SHA1SUM:
6d33fa2998179f5383948140b3bbce884c30e95b

SHA256:
28d3bf712d53516b8694988c8ac356db4b2d939bebe26a9802b50d8a43c83658

SHA512:
c216da900538d662ccee2c217c87749d
0b42549e09b635d141439400e877715e
63c54bf7896cde2a62fb4fb003cb60b7
94cd62b0252c20cb488d775d52e20940
```

- smc_6.3.0_10417_linux.zip

```
SHA1SUM:
7eab52a75c3edbe62600ce2f642d4b287562115b

SHA256:
8151a64fe1c499c4b3f3a3201f2c61371de8ad4c1f5fd14218d9de975c758d4b

SHA512:
88502ebaf7781bc9a738b9bfeda85294
75fa9bf9a51ddacf07aee0469d780b3d
6e310afa4a0f6e193b534d8891530d09
a175c6e407606e85aa6586c9149e954d
```

- smc_6.3.0_10417_windows.zip

```
SHA1SUM:
b95ed3e550744b7a5dadbe81f033551cbef0e320

SHA256:
207df62ddd71ec44088c21be35a6f24796bbe577fa29e1e296f44930d3c3ebfc

SHA512:
43784e862d9250657692d60f3f763f23
c1e6d6dd42cd2887e1a6e9df04fd60e6
0e47823ec1298a235562d8986019e11b
813a4c2848d9e2f27d31dbedb8b8a281
```

- smc_6.3.0_10417_webstart.zip

```
SHA1SUM:
394f4fa4158da4503bdefbeb074081ed616940de

SHA256:
a378d8fec9b818100b1a64543bc067c85ac64b1c810f3ea22cd2574d3b5b3d99

SHA512:
47d94fbb97f82231d431d2c3f5c1e955
4288bfc2852fdaf3f65268eedca6f207
a645d2f613fc8e772e0c8f95ec18d0a2
d9b34a8635081a75cbdaddc90ca79d1a
```

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.

Enhancement	Description
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.
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.

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
If you drag and drop the dynamic IP address of a physical interface to another interface, then change the IP address to a static IP address on the original interface without saving the configuration, the interface configuration becomes unusable. If the IP address on the original endpoint was used as a VPN endpoint, you can no longer open the VPN Endpoints view in the Engine Editor or any VPN where a gateway with the VPN endpoint in question is used.	SMC-1873

Description	Issue number
An administrator that has the Administrative Rights option Manage Alerts in the Administrator Role is not able to install an Alert Policy for a domain.	SMC-2005
The SSH key fingerprints for the Sidewinder SSH Proxy are shown in a different format than SSH clients typically display them, which can make it difficult to verify the fingerprint.	SMC-3782
Only one hyphen can be used in the FQDN contact address for a dynamic interface.	SMC-4846
If a policy is installed on multiple NGFW Engines, even if one of the NGFW Engines reports a failure, the policy installation is reported to have completed successfully.	SMC-4908
The "$$ Local Cluster" alias does not cover dynamic IP addresses for Single Firewalls.	SMC-4980
System elements can show in the search results when you search for unused elements. System elements cannot be deleted.	SMC-5044
Even though you can configure status monitoring and log reception for other types of servers, such as Active Directory Servers, you can only add Host and Router elements to the Monitoring tab in the Log Server Properties dialog box.	SMC-5053
It is not possible to use the Enforce TCP MSS option in the action options for an IPv6 Access rule.	SMC-5189
In the initial configuration file for the engine, special characters, such as @, are saved as encoded values. The engine does not interpret the encoding. As a result, PPP settings might not work correctly when you use a saved initial configuration file when you make initial contact with the Management Server.	SMC-5930
When setting the Distinguished Name of a Phase-1 ID for a VPN endpoint, you cannot use special characters, such as @.	SMC-6120
The maximum length for the name in a Domain Name element is 63 characters.	SMC-6452
The Default NAT option for element-based NAT includes all default routes. When there is a default route through both a NetLink and a router, the routing configuration is not generated correctly. Policy installation fails and the following message is shown: "The addresses specified for the Multi-Link Balancing CVI-X, CVI-Y are not included in its netlinks."	SMC-6539
When anti-malware is configured to use an HTTP proxy, the Access rule that allows retrieving anti-malware database updates is not automatically generated.	SMC-7275
If an Access rule references a a Zone element and a Group that includes an IP Address list element, the matching does not work correctly.	SMC-7440
Syslog data is not forwarded if the target host has only an IPv6 address defined.	SMC-7469
When you add an IP address to an interface, antispoofing entries that have been manually added are removed from the interface.	SMC-8382

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 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 an earlier 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 – 6.2.3. Versions earlier than 5.6.2 require an upgrade to one of these versions before upgrading to 6.3.0.

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*