# NGFW Security Management Center

## Release Notes

**6.3.2**
**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

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 6.3.2 build version is 10430.

This release contains Dynamic Update package 1018.

# Product binary checksums

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

- smc_6.3.2_10430.zip

```
SHA1SUM:
20ed6f8b7d5c48fd90b9d2ff0b9fd9f2c037c7dd

SHA256SUM:
65ae02eae284d2819b7df1c40ccf1a6a48f1ce9f39b56b46bb9c717e50376ac5

SHA512SUM:
58465b716671285410c17775beee7a53
8152fab0f6e3492bb0693f4b3777fe9f
c021e4dd84cdb4cc83ee9a95ea380642
fd7bf70b60bca2fc33f0aa4abc46250e
```

- smc_6.3.2_10430_linux.zip

```
SHA1SUM:
ae3e85b0e8efc2cd8999b0bfb312b207b841568c

SHA256SUM:
81cf037e78147394e4912e1c5c334df1d0447011690d17b5e405a74bdedda256

SHA512SUM:
f355bc24ebb742e26e57e3c6543a4234
2e0af38bbb9ed6c93d402f465caf8cd1
1c4f978ea27e26566bce5e070326c0c6
6957f925f0e3302799214af0723cf057
```

- smc_6.3.2_10430_windows.zip

```
SHA1SUM:
421fde4ea5d5339cd0aa2dbc9656506ae0711ffc

SHA256SUM:
188c58608f8cc11e9c3c7dc34d52d0bfb563c32beb86f8776380090bab722cf0

SHA512SUM:
5ce2975eae8c1fccc8d4ba0d15d90391
a917768165ea6d77b75061268673d557
7b64c1e215e356b1d4d0cbe47c6fcf43
ebc1fe66ef897fa8f354154aa1fd696e
```

- smc_6.3.2_10430_webstart.zip

```
SHA1SUM:
1231f79318ea5ebc08b70267d19b0f03e7858fb5

SHA256SUM:
59d802be0074745e730613fe166a193a9361a8a8e4fcfd8476425dc3c09ec372

SHA512SUM:
cfc96890ef8cf866e3f55b108e29bd44
f4925da30e2bbed02f12bba30c5396a5
d94ad5432a7a2ba1f9b0194ca99d4c03
dab93bcd56803d186d7f78e1e0ae5f93
```

# 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. |

# 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. |

| Enhancement | Description |
|---|---|
| SMC API enhancements | • You can use SMC API read-only queries on a standby Management Server in a high availability setup.<br>• You can use SMC API queries to view the history information of an element.<br>• You can use the WebSocket protocol to view active alerts for an element. |

# 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 |
|---|---|
| When you add users to the InternalDomain while you are logged on to an administrative Domain, the users might not be replicated to firewalls. However, replication works for users that you add to the InternalDomain while you are logged on to the Shared Domain. | SMC-3838 |
| If you use alert thresholds in Overviews, the Management Server might use too much memory. The following message is shown: "Out of memory." | SMC-4062 |
| When you create a new TLS Match element, input validation incorrectly prevents you from using a wildcard character (*) in the Matching Domain field. An "Invalid domain name" tooltip message is shown. Because the problem is caused by input validation, existing TLS Matches that use wildcard characters work correctly. | SMC-5219 |
| Every time the NGFW Engine is saved, an audit entry regarding antispoofing being updated for a dynamic interface is created, even if there were no changes to antispoofing. | SMC-5259 |
| When the translation value for an Alias on an NGFW Engine is modified, pending changes are shown for all the NGFW Engines. | SMC-5351 |
| If you try to delete a backup in the Management Client, this might fail with the message: "Delete Failed. Backup Failed. Management server is running." | SMC-5703 |
| NAT rule validation gives a warning about duplicate rules if a rule uses Any as the matching criteria and an earlier rule has more specific matching criteria. | SMC-6583 |
| It is not possible to forward audit data from the Management Server in the CEF and LEEF formats. | SMC-8219 |
| In Policy Snapshots, the settings for scan detection are not correctly displayed. | SMC-8374 |
| Certain dynamic routing configurations do not prevent policy installation, even when the uploaded dynamic routing configuration is blank. Only a warning is shown. Examples of such configurations are a BGP Peering and an External BGP Peer element being used in another network, or OSPF being used for a network while another OSPF area has already been defined. | SMC-8383 |
| When using the "search for unused elements" or "where used" search features, you might see the error message "Database problem. Failed to read Soft Interface from OSPF Area Reference." if an OSPFv2 Area is defined for a loopback IP Address. | SMC-8391 |

| Description | Issue number |
|---|---|
| After an NGFW Engine has been downgraded to a version earlier than 6.3, it is still possible to install a multi-layer policy where layer 2 interfaces are configured on an NGFW Engine in the Firewall/VPN role. | SMC-8782 |
| When you forward data to syslog servers in the CEF and LEEF formats, extra zeros are added to the end of the MAC Address fields and the MAC source and destination are the same. In McAfee ESM format, the MAC addresses are the same and extra characters are added. | SMC-8784 |
| In the Home view of an administrative Domain, when you select a VPN gateway that is used in a mobile VPN, the Tunnels view shows all VPN gateways that are used in mobile VPNs in all administrative Domains. | SMC-8792 |
| In large VPN configurations, VPN validation can cause the Management Server to become unresponsive. | SMC-8812 |
| When you use the Save and Refresh option in the Engine Editor, the Engine Editor prompts you to save the changes when you close the tab even if there are no unsaved changes. | SMC-8868 |
| You cannot add or edit DHCP settings for VLAN interfaces. | SMC-8935 |
| The Log Server stores received counter data in memory rather than storing to disk. This can cause memory consumption to become unusually high on the Log Server. | SMC-8995 |
| If an NGFW Engine that refers to a McAfee Logon Collector is deleted, it is not possible to edit another NGFW Engine that refers to the same McAfee Logon Collector. | SMC-9004 |
| Active alerts might significantly increase CPU usage of the Management Server if a rule in an Alert Chain is defined with a delay. If the following rule in the chain involves an external action (email, script, or SMS), alerts that reach the rule are repeatedly forwarded. | SMC-9159 |
| It is not possible to add a Group under a Tunnel Interface in the Routing pane of the Engine Editor. | SMC-9168 |
| When you create a remote upgrade task on the Administration | Tasks branch of the Configuration view, creating the task fails. | SMC-9292 |
| When you add or remove an Aggregated Link interface, the aggregate IDs for other Aggregated Link interfaces on the same NGFW Engine might change. Traffic that uses the Aggregated Link interfaces might be interrupted. | SMC-9340 |
| You cannot import an IP Address List if the list has the Category defined. | SMC-9674 |
| The pre-shared key for a route-based VPN tunnel configuration might become corrupted when the VPN configuration is edited. | SMC-9718 |

# 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 – 6.2.4 and 6.3.0. Versions earlier than 5.6.2 require an upgrade to one of these versions before upgrading to 6.3.2.

# 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*