FORCEPOINT

NGFW Security Management Center

Release Notes

6.4.8

Revision A

Contents

About this release

This document contains important information about this release of Forcepoint NGFW Security Management Center (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 higher 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 6.4.8 build version is 10530.

This release contains Dynamic Update package 1126.

Product binary checksums

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

- smc_6.4.8_10530.zip

```
SHA1SUM:
48ed4128cc6cc9a5cc5c741930dc28ded86b7320

SHA256SUM:
e60467fa68417a976fee6ba9e24a44be3f4624912832b54e3f564da4d747885b

SHA512SUM:
d3562f208687c662c3b5a14d14615165
fbcdbe98556e9d49d72765e52082f6a2
7db469abbd71330d2b8cb6c748caa351
6a3b0b63fdeece072f6b377ce7032e2d
```

- smc_6.4.8_10530_linux.zip

```
SHA1SUM:
41e7d83adbf66c45b0e2b76436501286c7089764

SHA256SUM:
05f3890bfb351489f43b1e791f027190975e958bbfa996489d26d9a57a983f41

SHA512SUM:
89595f61a933208802b20995b14a822e
481e369c0eb917353f5e1192e61d48db
f3f49c128bf99f6789f1e970b6fea787
e9198b62586c61830411e57dd4e562d5
```

- smc_6.4.8_10530_windows.zip

```
SHA1SUM:
dd098f8c436f274a6a21246959202886f9a0f23c

SHA256SUM:
308a06f8a62286632df766f3b376d4fdfcdf3a1d8da10cc9228413c45d364489

SHA512SUM:
d67e1fedcbbc36ebe5806b0fff23535b
15797c5e82a32c5e3b483f1f99e1c7e8
56a6572b153a1a5b616dd60a05baaf88
d01c158e15759cbb82e88e5ebf8b7d99
```

- smc_6.4.8_10530_webstart.zip

```
SHA1SUM:
6689d20ece0ec0feaf14ff7a2b232ffd5051e426

SHA256SUM:
0cc8b350e4cfb85db49c143f5088c26cfa61cfa4063e1cd40fca2e6508aad3d9

SHA512SUM:
7bb2a753123c0a72dfe16af5dbcbbf24
4a954a6118d69ec6a4f5e37f19c80a69
8c44accc8d04a5f1f7b79e96655b0bb0
56abccd789e6fbb90d2162a36926dc0e
```

Compatibility

SMC 6.4 is compatible with the following component versions.

Important: Some versions of Forcepoint NGFW have reached end-of-life status. Maintenance releases that contain security updates are no longer provided for versions of Forcepoint NGFW that have reached end-of-life status. Even though these versions of Forcepoint NGFW are compatible with the SMC, 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 6.4 can manage all compatible Forcepoint NGFW engine versions up to and including version 6.4.

- Forcepoint™ Next Generation Firewall (Forcepoint NGFW) 6.2 or higher
- 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 or higher (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*.

User information in the Home view

In the Home view of the Management Client, you can now see statistics about users and their activity. You can configure user alert checks that contain thresholds for generating user alerts. For example, you can configure a user alert check to generate a user alert if the user consumes excessive bandwidth, accesses restricted files or web content, or if the user is involved in an attack scenario. The user information is shown on the Users home page of the Home view, and the user alerts are shown in the User Behavior Events pane.

Certificate-based authentication for administrators

Administrators can now use certificate-based authentication to log on to the Management Client. For example, administrators can use the certificate stored on a Common Access Card (CAC) to log on to the Management Client.

Improved integration of external NTP servers

You can now use external NTP servers to provide time synchronization for both the SMC Appliance and NGFW Engines. External NTP servers were previously supported only for the SMC Appliance. You can use the same NTP servers for the SMC Appliance and the NGFW Engines.

SNMP Agent enhancements

You can now use SNMP Agents when you configure SNMP for the SMC Appliance. SNMP Agents were already supported for NGFW Engines in previous versions.

You can now specify the SNMP engine ID for each NGFW Engine and for the SMC Appliance. The SNMP engine ID is a unique identifier that the SNMP Agent uses to for the NGFW Engine or the SMC Appliance.

SNMP Agents now support IPv6 addresses.

Note: If you configured SNMP for the SMC Appliance before upgrading to version 6.4, you must configure SNMP again after upgrading to version 6.4.0 or higher.

Redirection of HTTP and HTTPS traffic to a proxy

The NGFW Engine can now transparently redirect HTTP and HTTPS traffic to a proxy. The proxy can be on-premises or a cloud-based service, such as the Forcepoint Web Security Cloud service. The traffic does not have to be redirected through a policy-based VPN.

Enhancements

This release of the product includes these enhancements.

Enhancements in SMC version 6.4.0

Enhancement	Description
Banner for sensitive data in exports	You can now configure a banner that is included in XML exports, HTML exports, and policy print-outs. The banner indicates that the exports contain sensitive or classified data.
Notification of changes to administrator permissions	If administrator permissions, roles, or access rights have changed, administrators are now notified that their permissions have changed when they log on to the Management Client.
Notification of last logon to administrators	When administrators log on to the Management Client, they are now notified of the time, date, and location of their last logon. The location is shown as an IP address.
Administrator names not saved in FIPS-compatible operating mode	When the SMC is in FIPS-compatible operating mode, the Management Client does not show recently used administrator names in the logon window. Only the recently used Management Server IP addresses are shown in the Management Client logon window.
IPv6 support for RADIUS authentication for administrators	RADIUS authentication for administrators now supports RADIUS servers with IPv6 addresses.

Enhancement	Description
Configurable action when the audit log storage or the log storage is full	You can now configure what happens if the audit log storage on the Management Server or the log storage on the Log Server is full. • For the Management Server, you can configure that the Management Server shuts down or that the Management Server overwrites audit entries, starting with the oldest audit entries. • For the Log Server, you can configure that the Log Server stops receiving log data or that the Log Server overwrites log entries, starting with the oldest log entries.
Alert when audit data or log data storage is getting full	An alert is now sent when the amount of audit log data on the Management Server or the log data on the Log Server exceeds 75% of the total storage capacity.
Improved integration of external LDAP servers and Active Directory servers	The integration of external LDAP servers and Active Directory servers with Forcepoint NGFW has been improved. • Support for the LDAPS and Start TLS protocols for securing the LDAP connection has been improved. When LDAPS or Start TLS is enabled for an LDAP Server or Active Directory Server, you can now select a TLS Profile and TLS Server Identity for the LDAP Server. • A new Authentication Method element for LDAP Authentication has been added. When LDAP Authentication is configured for a user, the user's password is checked against the user's credentials in the LDAP server that is used for user storage. LDAP Authentication can be used with the following existing features: IPsec and SSL tunnels in mobile VPNs, the SSL VPN Portal, and browser-based user authentication.
Improvements in browser-based user authentication	Browser-based user authentication now supports certificate-based authentication. Users can authenticate using a certificate file, or a certificate stored on a smart card, such as a Common Access Card (CAC).
Other authentication enhancements	The **Require Authorization** and **Timeout for Client IP Authorization** options have been removed from Authentication options for Access rules. Authorization is automatically required when you add User and Authentication Method elements to the **Authentication** cell. The **Authentication Time-Out** option in the **Add-Ons** > **User Authentication** branch of the Engine Editor replaces the **Timeout for Client IP Authorization** option.
Improvements in application detection	Because Access rules for application detection match traffic based on the payload of connections, the same connection can potentially match more than one rule based on the first SYN packet of the connection. Connection handling such as the use of VPNs, NAT, SSM Proxies, and TCP MSS enforcement is applied according to the initial match. When the final match is different from the initial match in a way that changes connection handling, the connection is dropped. In these cases, a log message that indicates a conflict between rules is generated.  **Note:** Due to changes in application detection, policies that use Network Applications, URL Categories, or URL Lists in the Access rules might work differently after upgrading to NGFW 6.4. Some traffic that was previously allowed might be discarded. After upgrading to NGFW 6.4 or higher, verify that your policies work as expected. For more information, see Knowledge Base article 15411.
New Network Application elements of the Cloud Services type	New Network Application elements of the Cloud Services type have been added to the SMC from the Forcepoint cloud access security broker (CASB) service catalog. Including the previous Network Application elements of the Web Applications and Protocols types, there are now over 7000 Network Applications available.

Enhancement	Description
Duplicate IPv6 address detection for Layer 3 Physical Interfaces	An option for detecting duplicate IPv6 addresses has been added to the Layer 3 Physical Interface properties for NGFW Engines.
Layer 2 Physical Interfaces on Virtual Firewalls and Master Engines that host Virtual Firewalls	You can now configure Layer 2 Physical Interfaces on Virtual Firewalls and Master Engines that host Virtual Firewalls.
Easier deployment of NGFW Engines in Microsoft Azure	You can now deploy NGFW Engines from the Microsoft Azure cloud environment without first creating the NGFW Engine element in the Management Client. You deploy the NGFW Engines from the cloud environment, and you can monitor the NGFW Engines in the Management Client.
Auto-scaling in Microsoft Azure	Support for auto-scaling for NGFW Engines that are deployed in Azure has been added. When the scaling feature is used, additional NGFW Engine instances are automatically created and removed, depending on traffic load. You can monitor the NGFW Engine instances in the Management Client.
Cloud Sandbox analysis information in the external portal	You can now view analysis information in the external portal for the cloud sandbox. You must define a user name for the cloud service in the Management Client to be able to view the analysis information in the external portal.
Auto-discovery for ECA clients	The NGFW Engine can now advertise its contact address to ECA clients. If the contact address of the NGFW Engine changes, or a new NGFW Engine is added to the network, the ECA clients are still able to connect to the NGFW Engine.
Monitoring of Forcepoint User ID Service	You can now enable monitoring for the Forcepoint User ID Service. You can also configure that the Forcepoint User ID Service sends log data to the SMC.
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.
Changes in SMC API	For information about changes in the SMC since version 6.3, see Knowledge Base article 15335.
Improved online Help	The look and feel of the online Help has been updated. The search feature has been improved, and now includes type-ahead search. The new, responsive design brings greater browser support, also for mobile and tablet devices.
Change in init system for managing SMC services on Linux platforms	When you install SMC server services on Linux platforms, the installation now uses systemd instead of SysV for init system and service management. Linux distributions that run systemd can now manage SMC services. There are no changes for Linux distributions that run SysV. Because systemd maintains compatibility with other init systems, the service command continues to work in all environments. The following commands are equivalent: • # service sgMgtServer [stop|start|status] • # systemctl [stop|start|status] sgMgtServer.service

Enhancements in SMC version 6.4.1

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.
User dashboard improvements	Several enhancements have been made to the usability and functionality of the user dashboard feature: • The Management Client and the SMC API include several minor enhancements for user alert checks in environments with multiple administrative Domains. • User Alert Checks now offer a granular set of filter options for each type of check. • You can now compare snapshots of User Alert Check elements. • When you install the SMC in demo mode, the simulation now includes the user dashboard feature.

Enhancements in SMC version 6.4.2

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.

Enhancements in SMC version 6.4.5

Enhancement	Description
Export option added to monitoring views	You can now export monitoring data from the monitoring views in CSV or XML format. Data from the columns that are visible is exported.

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
When you Ctrl-click a tab, the tab does not open in a new view.	SMC-13020
When you upgrade Master NGFW Engines, hosted Virtual NGFW Engines are also upgraded. When you upgrade a large number of Master NGFW Engines within a short time, Management Server operation can slow down.	SMC-16820
At the beginning of the policy installation process, VPN validation might prevent policy installation from progressing. Policy installation takes much longer than usual.	SMC-17280
Deleting a Policy element from the trash might take a long time.	SMC-17435

Description	Issue number
Every time that you modify an element, the validation index for the element in the database increases. When you have made a large number of changes to the same element, the maximum value of the validation index is reached, and the following message is shown: "Cannot increase the sequence value".	SMC-17501
You cannot add Route Map elements using the SMC API.	SMC-17544
When the Blacklist Scope options in an Exception rule match any IP address for Endpoint 2, you might not be able to remove the blacklist entry from the Blacklist Monitoring view. The ID of the blacklist entry in the Blacklist Monitoring view is different from the ID of the blacklist entry on the NGFW Engine.	SMC-17610
The value of the down ratio parameter for the Link Status test is not shown in the Management Client. The default value of the down ratio parameter for aggregated link interfaces in load balancing mode is 30. The default value of the down ratio parameter for other types of interfaces is different.	SMC-17696
When you change the interface ID of an interface that has a dynamic IP address, an invalid routing configuration is generated.	SMC-17706
The first time that you right-click an internal VPN gateway in the VPN editing view and select Properties, the Engine Editor does not open.	SMC-17867
You cannot add rules to QoS Policies using the SMC API.	SMC-17924
In a high availability (HA) SMC environment, the backup Management Server might generate status surveillance alerts.	SMC-18076
When an NGFW Engine in the Firewall/VPN role has layer 2 physical interfaces with VLAN retagging configured, policy installation might fail. The following message is shown: "inline VLAN pair x.xx -> y.yy that has vlan re-tagging configured. This can only be used in with interfaces in 'normal' failure mode configuration".	SMC-18081
After you use the rule search, rule counter analysis might fail when the period for the analysis is a long time range.	SMC-18226
Once an hour, the Log Server creates and opens new files to store received logs. At the end of the hour, the files are closed and removed from memory. An ongoing log deletion task can prevent files from being closed. When many files remain open, memory consumption can increase until the Log Server becomes unresponsive.	SMC-18344
It is not possible to set the cluster parameters Heartbeat Message Period and Heartbeat Failover Time using the SMC API.	SMC-18355
If you install more than 7 policies at the same time using the SMC API, the SMC API might return a 404 HTTP response even though the policy installations are proceeding.	SMC-18380
It is not possible to remove a route from the Routing view if the Any Network element is under a tunnel interface.	SMC-18399
When you use the Ctrl-C and Ctrl-V keyboard shortcuts to copy and paste a VLAN from one physical interface to another, the pasted VLAN has the wrong VLAN ID.	SMC-18436
If a Single Firewall or a Virtual NGFW Engine in the Firewall/VPN role uses its own IP address as an IP address in a NAT entry, and the Automatic Proxy ARP option is enabled in the NAT entry, the proxy ARP entry might be generated for the firewall's IP address, causing connectivity through the interface to fail.	SMC-18493
If you open an Overview that uses the "Access Overview" template, data is not shown if the sender is a Virtual NGFW Engine.	SMC-18520

Description	Issue number
It is not possible to sort matching criteria alphabetically in the Rule Service Definition of a policy.	SMC-18596
When you use TLS Match elements, policy snapshots might be corrupted. When you compare policy snapshots, the following message is shown: "Cannot import parameter valuation entry".	SMC-18637
In an environment that has separate Management Servers and Log Servers, the monitoring and logging for a newly-created NGFW Engine might not work, even if it possible to otherwise manage the NGFW Engine.	SMC-18691

Installation instructions

Use these high-level steps to install the 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/Documentation.

Note: The sgadmin user is reserved for SMC use on Linux, so it must not exist before the 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 in the Management Client from the **Configuration** view.

4) To generate initial configurations, right-click each NGFW Engine, then select **Configuration** > **Save Initial Configuration**.
   Make a note of the one-time password.

5) Make the initial connection from the NGFW Engines to the Management Server, then enter the one-time password.

6) Create and upload a policy on the NGFW Engines in 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 6.4 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 lower version of the SMC to 6.4, 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 – 6.3.8 and 6.4.0 – 6.4.7. Versions lower than 5.6.2 require an upgrade to one of these versions before upgrading to 6.4.8.
- Due to changes in application detection, policies that use Network Applications in the Access rules might work differently after upgrading a previous NGFW version to NGFW 6.4 or higher. Some traffic that was previously allowed might be discarded. After upgrading to NGFW 6.4 or higher, verify that your policies work as expected. For more information, see Knowledge Base article 15411.

Known issues

For a list of known issues in this product release, see Knowledge Base article 15418.

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*