Forcepoint

NGFW Security Management Center Appliance

6.8.3

Release Notes

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 number and checksums

The build number for SMC 6.8.3 is 10916. This release contains Dynamic Update package 1298.

Use checksums to make sure that files downloaded correctly.

- 6.8.3U001.sap

```
SHA1SUM:
af4ab56ebec94f9f5a0114b7e0cec9894b34d6d2

SHA256SUM:
9630550c4010b833616bc5ab9e53d63540118208321a5da186fd6d5a2ca05980

SHA512SUM:
698f4dd1c3645810e833a56e6b03364c
872852f388ea93948c3e8ffaa62cbb90
e2ad8086f1b073c912b1f64a1a8101b1
100f882208d628c62067507996edd39e
```

System requirements on virtualization platforms

As an alternative to using the SMC Appliance software on the pre-installed Forcepoint appliance, you can install the SMC Appliance software on a virtualization platform.

CAUTION

To protect the privacy of your data, we recommend installing the NGFW Engines, SMC components, or SMC Appliance on a hypervisor that does not host any other virtual machines.

Component	Requirement
Hypervisor	VMware ESXi version 6.0 or higher
Memory	8 GB RAM
Virtual disk space	120 GB
Interfaces	At least one network interface

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 6.8 can manage all compatible Forcepoint NGFW Engine versions up to and including version 6.8.

Important

Some versions of Forcepoint NGFW have reached end-of-life status and no longer receive maintenance releases that contain security updates. Even though these Forcepoint NGFW versions might be 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 https://support.forcepoint.com/ProductSupportLifeCycle.

SMC 6.8 is compatible with the following component versions.

- Forcepoint Next Generation Firewall (Forcepoint NGFW) 6.3 or higher
- McAfee Next Generation Firewall (McAfee NGFW) 5.10
- Stonesoft Firewall/VPN Express 5.5
- McAfee ePolicy Orchestrator (McAfee ePO) 5.3 or higher
- 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*.

UIID license binding for SMC licenses

When you install the SMC or upgrade the SMC to version 6.8, the SMC generates a Unique Installation Identifier (UIID). As an alternative to binding licenses for SMC components to the IP addresses of the components, you can now bind the SMC licenses to a UIID. Using UIID binding allows organizations to obtain SMC licenses without disclosing the internal IP addresses of the SMC components.

Note

The UIID is not stored in SMC backups or restored when you restore a backup. After the UIID is generated, it will not be overwritten when you restore backups or upgrade the SMC in the future.

You can continue to use your existing licenses or optionally change the license binding method. You can use IP-address-bound licenses for some SMC components and UIID-bound licenses for other SMC components.

Management Client downloads from the Management Server

Java Web Start is no longer supported in SMC 6.8. As an alternative, you can now configure the Management Server to provide the Management Client installation files on a download web page hosted by the Management Server. Administrators download and install the Management Client from the locally hosted SMC Downloads web page.

Note

Management Client downloads are not supported for macOS in SMC 6.8. For administrators who use macOS, we recommend using the SMC Web Access feature.

SMC Web Access support

The SMC Web Access feature is now supported on the SMC Appliance. As an alternative to installing the Management Client locally, you can use SMC Web Access to start and run the Management Client in a web browser.

SMC Web Access is enabled by default for new installations of the SMC Appliance. If you upgrade the SMC Appliance to version 6.8.0, you must manually enable SMC Web Access. For instructions, see the upgrade instructions in these release notes.

Note

Java Web Start is no longer supported in SMC 6.8.

Enhancements

This release of the product includes these enhancements.

Enhancements in SMC version 6.8.0

Enhancement	Description
Easier configuration of dynamic link selection for NGFW Engines	It is now possible to select Link Usage Profile elements for NGFW Engines in the Firewall/VPN role to define which link types are preferred, avoided, or not used for specific types of outbound Multi-Link traffic. NGFW Engine-specific exceptions to the Link Usage Profile also allow you to specify which traffic uses specific NetLinks.
Re-authentication when using browser-based user authentication	If an end user has authenticated using browser-based user authentication and the session will soon expire, the user can re-authenticate to extend the authentication time-out and avoid connections closing before the user has finished their tasks.
Custom script upload for NGFW Engines when using Custom Properties Profile elements	To upload custom scripts to the NGFW Engine, you can add the scripts to the properties of the NGFW Engine using a Custom Properties Profile element. The scripts are uploaded when the policy is installed or refreshed.
Expiration time for one-time passwords	You can now set the expiration time for one-time passwords that are generated when you save the initial configuration for an NGFW Engine. If the one-time password is not used, it automatically expires after the expiration time has elapsed. By default, one-time passwords expire after 30 days.
PPPoE support on VLAN interfaces	You can now configure point-to-point protocol over Ethernet (PPPoE) for dynamic IP addresses that are assigned to VLAN interfaces.
User domain support for integrated ICAP servers for DLP	NGFW integration with external ICAP servers for DLP now uses the WinNT schema in the X-Authenticated-Users header instead of the Local schema that was used previously. Using the WinNT schema allows matching users against a user domain in the user directory on the ICAP server.

Enhancements in SMC version 6.8.1

Enhancement	Description
Tool to remove old backups	The smca-backup-remove command has been added to remove old SMC Appliance backup files.

Enhancements in SMC version 6.8.2

Enhancement	Description
Configurable timeout for session monitoring	Previously, monitoring views might have failed to open when there were several backup Log Servers and the primary Log Server was unreachable. You can now define the timeout for receiving monitoring data from NGFW Engines. To define the timeout, edit the <installation folder>/data/SGConfiguration.txt file and add the following parameter: `SESMON_LOGSERVER_SELECTION_TIMEOUT=<timeout_in_milliseconds>` The default value is 20000.

Enhancements in SMC version 6.8.3

Enhancement	Description
Resource monitoring for SMC servers and the Management Client	The **Info** pane for Management Servers, Log Servers, and Web Portal Servers now shows information about resource usage on the computers where the servers are installed. The bottom right corner of the Management Client window shows the memory usage of the Management Client. If the memory usage gets too high, the Management Server, Log Server, Web Portal Server, or the Management Client automatically restarts. When the server or the Management Client restarts, an alert and an audit entry are generated. You can optionally disable automatic restart. **Important** Due to changes introduced by this enhancement, customized heap size values for servers, the Web Portal, and Management Clients are not preserved when you upgrade to SMC version 6.8.3. You must modify your configuration if you previously changed the Java heap size of the Management Client using the MAX_HEAP_SIZE parameter in the sgClient.sh or sgClient.bat file. For more information, see the upgrade instructions.
Password policy enhancements	The settings for password complexity requirements in the password policy now also apply to SMC administrator accounts that are replicated as local administrator accounts on NGFW Engines, the root account on NGFW Engines, and the Management Server database password.
New Log Server and Management Server configuration parameters	In the LogServerConfiguration.txt file, you can now add a new configuration parameter to recover connectivity from the Log Server to TCP syslog servers. For more information, see Knowledge Base article 19219. In the SGConfiguration.txt file, you can now add a new configuration parameter to define how many tasks the Management Server can run in parallel. For more information, see Knowledge Base article 19218.

Enhancement	Description
More granular identification of Microsoft Office 365 network applications	Starting from dynamic update package 1300, the Microsoft-Office-365 Network Application element includes dependencies that allow more granular identification of Microsoft Office 365 in traffic. No action is required if you use the Microsoft-Office-365 Network Application element in the following types of rules: ■ Access rules with the Allow, Discard, Refuse, or Jump action ■ NAT rules If you use the Microsoft-Office-365 Network Application element in an access rule with the Continue action, you must manually add the Network Application elements that are listed as dependencies. Options that are configured in a rule with the Continue action are not automatically applied to dependencies. For more information, see Knowledge Base article 19195.

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 a Management Client session is closed due to the logon options in the password policy, the status of the administrator who was using the Management Client is still shown as connected.	SMC-28448
When the Log Server fails to start due to the disk being too full, the reason for the failure is not indicated to the administrator.	SMC-29175
When you export the Administrator Activity Summary report as a PDF, the report might show * in place of some characters.	SMC-30481
When you generate system reports for multiple SMC servers, sections that are normally combined might be printed on separate pages.	SMC-30537
In large SMC environments, the Management Server might not be able to process the status of all Log Servers. The status icons for the Log Servers appear gray.	SMC-30754
Scheduled backup tasks might fail to run at the scheduled time.	SMC-31362
If the names of custom Situation elements include the less than (<), greater than (>), or pipe (|) characters, snapshot comparison fails.	SMC-31444
When you export an NGFW Engine element as XML, route metrics are not included in the export.	SMC-31548
When you change the Interface for DHCP Relay setting for the VPN Client, the change does not appear in the policy snapshot.	SMC-31605
When you configure diagnostics settings for individual NGFW Engine nodes, the settings are not always saved.	SMC-31637
The rules in the default Firewall Template policy do not allow destination NAT using the public IP address of NGFW Engines deployed in the Azure cloud.	SMC-31711

Description	Issue number
When you convert an NGFW Engine that has an SNMP Agent configured to a Master NGFW Engine and Virtual NGFW Engines, the SNMP Agent is also configured for the Virtual NGFW Engines.	SMC-31736
If the connection between the NGFW Engine and the Log Server is unstable, session monitoring views might fail to open even when the NGFW Engine sends log data to the primary Log Server.	SMC-31898
When the SMC is installed in Linux, SMC server services might stop working due to a lack of threads even though the services are running.	SMC-31952
The Show Related Logs action does not work for rules in the Layer 2 Interface Policy.	SMC-31967
When VPN endpoints are are enabled only for the SSL VPN Portal, the NGFW Engine might incorrectly try to use them to contact a VPN Broker gateway.	SMC-31980
When you start and stop Log Servers in an environment with a large number of Log Servers, NGFW Engines connect to different Log Servers. As a result, a Log Server might stop responding when a large number of NGFW Engines tries to connect to it because the Log Server has too many open files.	SMC-31983
The traffic capture tool might fail for some NGFW Engines. A long error message is shown.	SMC-32116
In an environment with multiple Management Servers, if you upgrade a standby Management Server before the active Management Server, the standby Management Server does not start after the upgrade.	SMC-32287
After you have moved Virtual NGFW Engines from one Master NGFW Engine to another, the Management Server might try to install the policy for the Virtual NGFW Engines on the old Master NGFW Engine.	SMC-32313
Management Server licenses that include the high availability feature cannot use UIID license binding.	SMC-32316
Filtering log entries in the Web Portal might fail. An error message is shown.	SMC-32317
Some actions related to log data, such as aborting the generation of a report or refreshing the statistics while they are loading, might cause the Log Server to show a false positive "Found inconsistent file" alert.	SMC-32595
Certificate-based authentication for administrators might fail. The following error message is shown: "Authentication failed. Internal error."	SMC-32893
In the Query panel of the Logs view, the options on the Storage tab do not include the "Default" option. The "Primary Archive" option refers to active log data.	SMC-33047
When you use two-factor authentication with the SSL VPN Portal, the timeout is too short and authentication might fail even if the user enters the correct credentials.	SMC-33130
In new installations of the SMC, the InternalDomain LDAP domain is not set as the default LDAP domain.	SMC-33270

Install the SMC Appliance

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/Documentation.

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.
    As an alternative to installing the Management Client locally, you can use SMC Web Access to start and run the Management Client in a web browser. SMC Web Access is enabled by default for new installations of the SMC Appliance.

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

12) Create the NGFW Engine elements, then install and configure the NGFW Engines.

Upgrade the SMC Appliance

Use an upgrade patch to upgrade the SMC Appliance from a previous version to version 6.8.3.

There are two kinds of SMC Appliance patches:

- Hotfix patches include improvements and enhancements for the current SMC Appliance version.
  Hotfix patch files use the letter P as a separator between the version number and the patch number. Example: 6.8.1P001

- Upgrade patches upgrade the SMC Appliance to a new version.
  Upgrade patch files use the letter U as a separator between the version number and the patch number.
  Example: 6.8.1U001

We recommend checking the availability of SMC Appliance patches regularly, and installing the patches when they become available. For detailed information about installing SMC Appliance patches, see the *Forcepoint Next Generation Firewall Installation Guide*.

- SMC 6.8 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.
- The SMC Appliance must be upgraded before the NGFW Engines are upgraded to the same major version.
- You can upgrade from the following SMC versions:
  - 6.4.7 – 6.4.10
  - 6.5.1 – 6.5.18
  - 6.6.0 – 6.6.5
  - 6.7.0 – 6.7.5
  - 6.8.0 – 6.8.2
- If you configured SNMP for the SMC Appliance before upgrading to version 6.4.0 or higher, you must configure SNMP again.

You can upgrade the SMC Appliance using the Management Client or using the appliance maintenance and bug remediation (AMBR) patching utility on the command line of the SMC Appliance.

Note

In SMC version 6.8.3 and higher, the default path to the installation of xvfb-run for SMC Web Access is set to /usr/bin, and you cannot change the path using the Management Client.

If you use SMC Web Access on a Management Server or Web Portal Server installed on a Linux platform and need to change the path to the installation of xvfb-run, follow these steps:

1) On the Management Server or the Web Portal Server, edit the `SGConfiguration.txt` or `WebPortalConfiguration.txt` file.

2) Add the following parameter:

```
XVFB_RUN_DEFAULT_PATH=<path>
```

Replace `<path>` with the path to the installation of xvfb-run.

Important

Due to changes introduced by the resource monitoring enhancement for SMC servers and the Management Client, customized heap size values for servers, the Web Portal, and Management Clients are not preserved when you upgrade to SMC version 6.8.3. You must modify your configuration if you previously changed the Java heap size of the Management Client using the MAX_HEAP_SIZE parameter in the sgClient.sh or sgClient.bat file.

To preserve the custom heap value for the Management Client, follow these steps on each computer the Management Client is installed:

1) Browse to the `<user home>/.stonegate` folder.

2) Edit the `client_starter.xml` file.

3) Change the value of the MAX_MEMORY_IN_MB parameter to the value that you previously defined for the MAX_HEAP_SIZE parameter .

Upgrade the SMC Appliance in the Management Client

You can use the Management Client to upgrade the SMC Appliance. In some certified environments, you must use the Management Client to install SMC Appliance patches.

Steps

For more details about the product and how to configure features, click **Help** or press **F1**.

1) Start the Management Client.

2) Select **Configuration**, then browse to **Administration**.

3) Browse to **SMC Appliance Patches**.

4) Download or import the 6.8.3U001 patch file.
   - To download the 6.8.3U001 patch using the Management Client, right-click the 6.8.3U001 patch, then select **Download SMC Appliance Patch**.
   - If you manually downloaded the 6.8.3U001 patch, right-click **SMC Appliance Patches**, select **Import SMC Appliance Patches**, browse to the 6.8.3U001 patch file, then click **Import**.

5) Right-click the 6.8.3U001 patch file, then select **Activate**.

6) (Optional) To allow administrators to start and run the Management Client in a web browser, enable the SMC Web Access feature after the upgrade is complete.

   a) Log on to the SMC Appliance.

   b) To enable the SMC Web Access feature, enter the following command:

   ```
   sudo /usr/local/forcepoint/smc/bin/sgActivateWebswing.sh
   ```

   c) When prompted, enter your SMC user credentials.

   When the configuration is complete, administrators can start and run the Management Client in a web browser.

Upgrade the SMC Appliance on the command line

You can use the AMBR patching utility to patch or upgrade the SMC Appliance on the command line.

Steps

1) Log on to the SMC Appliance.

2) To check for available upgrade patches, enter the following command:

```
sudo ambr-query -u
```

3) To load the patch on the SMC Appliance, enter the following command:

```
sudo ambr-load 6.8.3U001
```

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. Example:

```
sudo ambr-load –f /var/tmp/6.8.3U001.sap
```

4) To install the patch on the SMC Appliance, enter the following command:

```
sudo ambr-install 6.8.3U001
```

The installation process prompts you to continue.

5) Enter `Y`.
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 6.8.3.

6) (Optional) To allow administrators to start and run the Management Client in a web browser, enable the SMC Web Access feature after the upgrade is complete.
   a) Log on to the SMC Appliance.
   b) To enable the SMC Web Access feature, enter the following command:

```
sudo /usr/local/forcepoint/smc/bin/sgActivateWebswing.sh
```

   c) When prompted, enter your SMC user credentials.

When the configuration is complete, administrators can start and run the Management Client in a web browser.

Known issues

For a list of known issues in this product release, see Knowledge Base article 18381.

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, release notes, Knowledge Base articles, downloads, cases, and contact information.

You might need to log on to access the Forcepoint support website. If you do not yet have credentials, create a customer account. See https://support.forcepoint.com/CreateAccount.

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 User Guide* (Formerly *Forcepoint NGFW SMC API Reference Guide*)
- *Forcepoint VPN Client User Guide* for Windows or Mac
- *Forcepoint VPN Client Product Guide*

Published 08 December 2020