Forcepoint

NGFW Security Management Center Appliance

6.8.5

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 6.8.5 is 10932. This release contains Dynamic Update package 1337.

Use checksums to make sure that files downloaded correctly.

- 6.8.5U001.sap

```
SHA1SUM:
7bee0528a4182deb51ca1f3a2f0f4a8bf4ca8e92

SHA256SUM:
eb9c8aaad1fd547094e3640dbbf9939e784685ad8035733169e5a8c3454462a5

SHA512SUM:
b6975cf3384316f8518b8056b0635a4d
78990cc581a1b1f532a289687b6608fa
14525d885cd5df3ec7c944ea392e3399
022a4bbfc0efd7810d9f8fba467eab63
```

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.
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.
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.

Enhancements in SMC version 6.8.4

Enhancement	Description
Optimization of status monitoring in large-scale SMC environments	New parameters for the Management Server and Log Server allow you to optimize the performance of status monitoring for NGFW Engines, VPNs, and NetLinks for SD-WAN in large-scale SMC environments. For more information, see Knowledge Base article 19285.

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
Installation of a policy on a firewall can complete successfully, but still show the error message: "WARNING Failed to create a Policy Snapshot for Firewall Policy Example policy".	SMC-31540
While another action, such as policy installation, is in progress, the following error message might be shown: "Failed to construct the alias values." The original action succeeds despite the error message.	SMC-32455
After you enable or disable the Node-Initiated Contact to Management Server option for an NGFW Engine, policy installation fails even if the nodes have already made initial contact the the Management Server and have the initial policy installed.	SMC-32603
The monitoring icon for Forcepoint Cloud might appear gray in the System Connections even though the NGFW Engine is connected to the sandbox service.	SMC-32888
When you use the Upgrade Software action at the cluster level for a Master NGFW Engine cluster, the second node in the cluster might start the upgrade sequence before the Virtual NGFW Engines are active on the first upgraded node.	SMC-32926
When URL List or Situation elements have been updated frequently, it eventually becomes impossible to make more updates to the elements. This issue might happen when the whole content of a URL List element is frequently overwritten using the SMC API.	SMC-33279
The SMC Appliance does not allow administrator names to include an underscore. When you restore a backup from a normal SMC installation on an SMC appliance, administrator accounts with underscores in their names no longer work.	SMC-33346
sgInfo might not collect all expected files from the <installation folder>/data/tmp directory.	SMC-33361
If you export a Firewall element that has a loopback IP address and several internal VPN Gateway elements configured, you cannot import the element in a different SMC.	SMC-33512
In rare cases when you have filtered the Active Alerts view, acknowledging the filtered alerts might also acknowledge other alerts.	SMC-33522
When the Management Server is an SMC Appliance, it is not possible to enable Management Client downloads in the properties of the Management Server.	SMC-33929
When adding filters in the logs or monitoring views, you might see the error message: "Index X out of bounds for length Y".	SMC-33942

Description	Issue number
In Windows, maximizing the Management Client window moves it to the main display.	SMC-34008
When you use TCP to forward log data to an external syslog server, forwarding does not start again when the syslog server becomes available if the connection to the syslog server has been lost for a longer time.	SMC-34153
In an environment with multiple Management Servers, incremental replication might leave some lock files, causing later replication to fail. As a result, it is necessary to perform a full database replication between the active Management Server and additional Management Servers.	SMC-34175
If you install the Management Client using an MSI installer from the SMC Downloads page on the Management Server, you cannot edit IP Address List elements. <br/> <br/> Workaround: See the resolution in KB 18929 to address the issue.	SMC-34379
The Third Party Diagram status card might appear empty when you select an SMC server in the Home view.	SMC-34412
Administrator status shows one administrator online for each administrative Domain that an administrator has logged on to, even if all of the logons are from the same Management Client.	SMC-34458
When there are multiple Log Servers that are configured as backup Log Servers for each other, modifications in the Log Server Properties are not recorded as pending changes for NGFW Engine elements that use the Log Server as a backup Log Server.	SMC-34459
When there are multiple Management Servers, pending changes are not always cleared on standby Management Servers when a policy is installed.	SMC-34467
The Management Client does not prevent you from deleting Network elements that are selected as source networks in the Add-Ons > Endpoint Integration branch in the Engine Editor.	SMC-34571
When a Master NGFW Engine has been created by converting a Firewall element to Master NGFW Engines and Virtual Firewall elements, policy installation might fail for the Virtual Firewalls. The following error message is shown: "To enable NTP for the NGFW Engine, you must configure one or more NTP Server elements."	SMC-34576
If you run the allPermissions.sh script without the correct options, the script might change the owner of operating system folders that it should not change.	SMC-34602
If SMC 6.8.4 is installed in a custom path in Windows, locally installed Management Clients do not start. Management Clients that are installed using Management Client downloads from the Management Server and SMC Web Access are not affected.	SMC-34603
If Not Forced is selected for the Force Communication Mode option for an OSPF v2 Area, policy installation fails.	SMC-34627
SMC Appliance backups do not include full NTP settings.	SMC-34767
In rare cases, opening the Engine Editor in edit mode fails.	SMC-34772
When you use the SMC API to modify routing or anti-spoofing settings for an interface, the "Allow route monitoring probe from firewall" option in the automatic rules might be deselected.	SMC-34823
If you have used the DNO_OOM_RESTART option to prevent SMC servers from automatically restarting if the memory usage gets too high, other default settings for resource monitoring might still cause the server to be shut down if memory usage is too high.	SMC-34837
You cannot use the SPI value as a filter in the Logs view.	SMC-34890
When administrator account replication to NGFW Engines is enabled and the password policy is enforced, editing administrator properties requires you to enter the password for administrator account replication again.	SMC-34949

Description	Issue number
To use Network Application elements in NAT rules, inspection must be enabled in the Access rules.	SMC-35047
To be able to save a Proxy Server element, you must specify a non-default port for the Protocol-Specific Listening Ports option.	SMC-35146
When you use UIID-bound licenses in an environment with multiple Management Servers, the license binding for additional Management Servers is lost when the active Management Server is restarted. You must perform a full database replication to restore the licenses for the additional Management Servers.	SMC-35176
When you upgrade the Management Server to SMC 6.8.4, memory allocation might change.	SMC-35369
When different scheduled tasks are running at the same time, a task might be considered complete even if it has not finished running for all targets.	SMC-35596
When you use SMC Web Access, you cannot copy the authentication key when you create a new SMC API Client element.	SMC-35621
During an SMC upgrade, some migration steps might be very slow and the upgrade might seem like it is not progressing.	SMC-35647
In large environments, the Management Server might stop working because there are too many open files. For example, policy installation might not start.	SMC-35802
When there is an Elasticsearch Cluster, adding a new Log Server creates an unusable element.	SMC-35870
You cannot create new custom Sandbox Service elements.	SMC-36003
In an environment with multiple Management Servers, incremental replication might fail even after a successful full replication if additional Management Servers have been disconnected for a long time.	SMC-36007
It is not possible to configure RADIUS or TACACS authentication methods for the Management Server using the SMC API.	SMC-36077
If the VPN profile for a mobile VPN uses only the AES-GCM-256 cipher, the configuration that is generated for the VPN Client is incorrect.	SMC-36300
You cannot use the SMC API to update an NGFW Engine element that has policy routing entries with ANY as the destination.	SMC-36447

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 6.8.5.

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 – 6.8.4
-
- 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.

> **Note**
>
> If you use the SMC-Python library for interacting with the SMC API, you must upgrade the SMC-Python library to version 0.7.0b27 when you upgrade to SMC 6.8.4. To upgrade the SMC-Python library, see https://github.com/Forcepoint/fp-NGFW-SMC-python.

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 6.8.5U001 patch file.

   - To download the 6.8.5U001 patch using the Management Client, right-click the 6.8.5U001 patch, then select **Download SMC Appliance Patch**.
   - If you manually downloaded the 6.8.5U001 patch, right-click **SMC Appliance Patches**, select **Import SMC Appliance Patches**, browse to the 6.8.5U001 patch file, then click **Import**.

5) Right-click the 6.8.5U001 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 6.8.5U001
   ```

   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/6.8.5U001.sap
   ```

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

   ```
   sudo ambr-install 6.8.5U001
   ```

   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 6.8.5.

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 20 April 2021