Forcepoint

NGFW Security Management Center Appliance

6.8.2

Release Notes

Revision B

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 6.8.2 is 10913. This release contains Dynamic Update package 1281.

Use checksums to make sure that files downloaded correctly.

- 6.8.2U001.sap

```
SHA1SUM:
d01e00437bafc7d1a6c725b13ec23d9dbff1acb0

SHA256SUM:
2b9de7ef02567f12205acfe15ac9d6df71e947021be85183f8eda89f54fbd35b

SHA512SUM:
fc2f94d4980ad2178af360d88e349b89
c74a44b41ce5e2663feeb567e2e57352
a43d1c8e074851056441855878e7e6ff
9a8dbad3f95ebf05e36a13b5b77fac96
```

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.
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 you install a policy after you change the active Management Server, the Status tree in the home view might show pending changes that have already been committed.	SMC-23679
When the "Lock Management Client Window After the User Session is Idle" option is enabled, the Management Center Locked popup is shown on top of all windows. The popup remains on top of other windows unless it is minimized.	SMC-24085
The DHCP tab is not shown in the Info pane for NGFW Engines in the Layer 2 Firewall role.	SMC-29144
When the path to the script to execute after the task in an Export Log Task includes spaces, script execution fails.	SMC-29221
When you create an inspection rule based on a log entry, custom Inspection Policy elements are not found.	SMC-29730
When you use the Where Used? tool to find a rule in the policy editor, a new tab opens when you edit the matching rule.	SMC-30119

Description	Issue number
When an Access Control List includes the "Edit Element Properties" permission, administrators are allowed to edit the Access Control List element itself.	SMC-30365
When multiple Log Servers are selected, exporting log entries from the Logs view stops after 5 minutes even though log entries from the defined time period have not been completely processed.	SMC-30468
When you change the contact address of a Log Server, you must restart the Management Client to use the new contact address.	SMC-30535
For mobile VPNs, the Export iOS VPN Configuration Profile option does not work.	SMC-30709
If automated RSA certificate management fails to create a certificate for a VPN gateway, policy installation for the NGFW Engine might fail. This issue might occur when node-initiated contact to the Management Server is enabled for an NGFW Engine that has an integrated switch with port group interfaces.	SMC-30750
When you use an FQDN as the host name of the HTTP proxy that the NGFW Engine uses to connect to anti-malware database mirrors, the following warning is incorrectly shown during policy installation: "The proxy IP Address X defined in the Anti-Malware settings in invalid". The HTTP proxy is configured correctly.	SMC-30757
If there are many policy snapshots, upgrading the Management Server might fail.	SMC-30769
When you have replaced hardware, the MSSP Report might show incorrect information for the node.	SMC-30798
When you use Group elements in the Routing view, the routing table does not show all networks and IP addresses in the groups correctly.	SMC-30800
The "Only One Logon Session for Each User" option on the Password Policy tab of the Global System Properties dialog box should invalidate an administrator's previous session and allow the administrator to start a new session. The option incorrectly prevents administrators from logging on if there is already an existing session.	SMC-30831
The Disable SSH option is not shown in the right-click menu for an NGFW Engine on which SSH has been enabled.	SMC-30875
When you use the "IP Protocol" field as a field resolver in a Logging Profile element, the value is not correctly resolved.	SMC-30926
When you are using a Management Client that was installed using the MSI installation package that is provided on the SMC Downloads page, you cannot edit IP Address List elements.	SMC-31019
If you previously created a duplicate of a template policy, then selected the original template policy as the parent template of the duplicate template policy, the insert point might be missing from the template policy. After you upgrade the SMC, the intended rules might be missing from the policy.	SMC-31078
If the Management Client window is locked after the Management Server has become unreachable, the CPU load on the computer where you use the Management Client might become high.	SMC-31230
The maximum number of backup Log Servers is one less than the value defined for the MAX_SECONDARY_LOGSERVER parameter in the LogServerConfiguration.txt file.	SMC-31335
The Tunnels pane in branch home pages in the SD-WAN dashboard might show Endpoint B as <unknown>.	SMC-31338
You cannot terminate GRE connections in the Monitoring > Connections view.	SMC-31352
When you open a sub-policy for editing, rule counters for the main policy are reset.	SMC-31410

Description	Issue number
When an interface on an NGFW Engine has several IP addresses, activating the internal DHCP server on the interface fails. The following message is shown: "There are multiple IPv4 networks behind Interface 0. You cannot configure the DHCP server for Interface X". This issue does not occur on VLAN interfaces.	SMC-31430
When there are NGFW Engines that have port group interfaces, opening the $$ Default NAT Address Alias element fails.	SMC-31434
In the Engine Editor, the value of system aliases might be shown as NONE even though the value of these aliases is resolved for the NGFW Engine.	SMC-31437
Opening the properties of an Authentication Method element fails. The following message is shown: "Failed to display."	SMC-31468
When you back up policy snapshots and select the option to delete the original policy snapshot, the Management Client might become unresponsive.	SMC-31490
When you restore a backup of a policy snapshot, you cannot compare the restored policy snapshot to the most recently saved policy.	SMC-31492
The selected options for diagnostic log data are cleared when you save changes to the NGFW Engine element. For Master NGFW Engines, the Master NGFW Engine element and individual Master NGFW Engine nodes might have conflicting diagnostics settings.	SMC-31559
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-31851

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 6.8.2.

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 – 6.5.17
  - 6.6.0 – 6.6.5
  - 6.7.0 – 6.7.5
  - 6.8.0 – 6.8.1
- 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.

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 6.8.2U001 patch file.
   - To download the 6.8.2U001 patch using the Management Client, right-click the 6.8.2U001 patch, then select **Download SMC Appliance Patch**.
   - If you manually downloaded the 6.8.2U001 patch, right-click **SMC Appliance Patches**, select **Import SMC Appliance Patches**, browse to the 6.8.2U001 patch file, then click **Import**.

5) Right-click the 6.8.2U001 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 6.8.2U001
```

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/6.8.2U001.sap
```

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

```
sudo ambr-install 6.8.2U001
```

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 6.8.2.

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*
- *Forcepoint VPN Client User Guide* for Windows or Mac
- *Forcepoint VPN Client Product Guide*

Published 04 December 2020