Forcepoint

NGFW Security Management Center

6.8.2

Release Notes

Revision B

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.

SMC hardware requirements

You can install the SMC on standard hardware.

Component	Requirement
CPU	Intel® Core™ family processor or higher recommended, or equivalent on a non-Intel platform
Disk space	■ Management Server: 6 GB ■ Log Server: 50 GB

Component	Requirement
Memory	■ Management Server, Log Server, Web Portal Server: 6 GB RAM ■ If all SMC servers are on the same computer: 16 GB RAM ■ If you use the SMC Web Access feature: an additional 2 GB RAM per administrator session ■ Management Client: 2 GB RAM The SMC server requirements are the *minimum* requirements. The Management Server and Log Server in particular benefit from having more than the minimum amount of RAM. On high-end appliances that have a lot of RAM, the SMC might not provision the maximum amount of RAM for use by the SMC servers. For information about how to manually modify the provisioning, see Knowledge Base article 10016.
Management Client peripherals	■ A mouse or pointing device ■ SVGA (1024x768) display or higher

CAUTION

To protect the privacy of your data, we recommend using dedicated hardware for all NGFW, SMC, and SMC Appliance installations. For cloud-based virtualization platforms, use an instance type that runs on dedicated hardware. For on-premises virtualization platforms, install the NGFW Engines, SMC components, or SMC Appliance on a hypervisor that does not host any other virtual machines. For third-party hardware, do not install any other software on the computer where you install the NGFW Engines or SMC components.

Operating systems

You can install the SMC on the following operating systems. Only 64-bit operating systems are supported.

Linux	Microsoft Windows
■ CentOS 7 and 8 ■ Red Hat Enterprise Linux 7 and 8 ■ SUSE Linux Enterprise 12 and 15 ■ Ubuntu 16.04 LTS and 18.04 LTS	Standard and Datacenter editions of the following Windows Server versions: ■ Windows Server 2019 ■ Windows Server 2016 ■ Windows Server 2012 R2 On Windows 10, you can install the SMC in demo mode. You can also install the Management Client.

We recommend that you only use operating system versions that are currently supported by the vendor.

Other versions of the listed operating systems might be compatible, but have not been tested. Only U.S. English language versions of the listed operating systems have been tested, but other locales might also be compatible.

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.

- smc_6.8.2_10913.zip

```
SHA1SUM:
40c20029a8ff472077b99ee377dce01c6de1dd22

SHA256SUM:
08a595270db84f9b13687951d5bcd93f046c5dd5b911b0cf80341db171beafd3

SHA512SUM:
5d172bb33a97e99f351712f515a35e14
5fad72d6bc0cc6bedebbf831280ea3e1
e66066ddcd2f18c4381ee9fb740ee20c
b8236821b42bfac9f16fec9102f36e8a
```

- smc_6.8.2_10913_linux.zip

```
SHA1SUM:
42dd28e6da09109b682ba2382722e81dbaa18e9c

SHA256SUM:
e9fe7232925186c7ef42496e902c23fe8e949552b06f305574f5ad7cd21d4836

SHA512SUM:
f32959b8741b99faa27666692f38c7ec
48edaa95996ba1cd40be0cab6e60e55a
7ac3ce1bb966b22a400bd6bf7546f80f
4c1c3f50ecb5ae2ffaf949457fe97acf
```

- smc_6.8.2_10913_windows.zip

```
SHA1SUM:
57d8582bf556e8439ece02e719827a45d8299579

SHA256SUM:
01435036fbe6f050dd098fec7fcd0829c5176caab5c3cfd83af74ef9e21bf786

SHA512SUM:
c39d53277626993a3617bc38506f40b7
5f0e9d8f68c59d5366a6e229e8a62b38
e8687f097a7a90b7736b2df431763fbd
b5cf41b905100e67ed96eee5adceec70
```

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.

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 6.8.2

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.

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 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
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

Description	Issue number
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
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

Description	Issue number
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

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 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

The SMC (Management Server, Log Server, and Web Portal Server) must be upgraded before the NGFW Engines are upgraded to the same major version.

- 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 in the Management Client before upgrading the software.
- To upgrade a lower version of the SMC to 6.8, 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.
- When you upgrade the SMC, 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.
- You can upgrade from the following SMC versions:
  - 5.6.2 – 6.4.10
  - 6.5.0 – 6.5.17
  - 6.6.0 – 6.6.5
  - 6.7.0 – 6.7.5
  - 6.8.0– 6.8.1

  Versions lower than 5.6.2 require an upgrade to one of these versions before upgrading to 6.8.2.
- Before upgrading, make sure that you have removed all elements related to McAfee Endpoint Intelligence Agent (McAfee EIA). Also remove all references in Access rules.

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