FORCEPOINT

NGFW Security Management Center Appliance

Release Notes

6.5.1

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 6.5.1 is 10631. This release contains Dynamic Update package 1118.

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

- smca-6.5.1_10631.x86_64.iso

```
SHA1SUM:
6e48f5155b5ba569b6d954efb62b5f89f2ff96f4

SHA256SUM:
083ef8b1eb04dc028112a127500d78d5bf068f7059e4d7851409a309f6b29dab

SHA512SUM:
9802fa9efcca8a5b0ac98ccd4df823af
4643b1bc24e34e4f815b5d601ee81861
a6c03f4393f9dc06aa90ab4bc7301bbf
ad58176fa67f7f76d42dd6a3fe4ed17e
```

- 6.5.1P001.sap

```
SHA1SUM:
6fad13df445609cb4052cd89a36a5242f95bdb19

SHA256SUM:
b0effbd66de351720ab51989b7b70e58225464a7254f1d21831982c9fb8c5b21

SHA512SUM:
e133ae8edda587792e69f0c883c87c4f
f24c147baf5b96e42bf6978e5ae56c06
79db9e110eb443b61e19ac14c207314c
f761e28869a03a7a56b74da9dddb47e8
```

- 6.5.1U002.sap

```
SHA1SUM:
9642a1cab7cc6023384435a040238dcc8a30d851

SHA256SUM:
6b66e5748233d9d5edb19f8112ef20d8834872717dfe6a9d528e3696c76dc5e7

SHA512SUM:
48d22acac593673a2a0fa0b50949d8b6
cd615bdf9b9b137654fb28b1aa05494a
de6c65eb975dffaa672cc21fad52a62b
60f53bd0b588e51f1c63c073723614c5
```

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 6.5 can manage all compatible Forcepoint NGFW Engine versions up to and including version 6.5.

Important: Some versions of Forcepoint NGFW have reached end-of-life status. Maintenance releases that contain security updates are no longer provided for Forcepoint NGFW versions that have reached end-of-life status. Even though these Forcepoint NGFW versions are compatible with the SMC, we recommend that you use a Long-Term Support version that is still supported. For more information about the Forcepoint NGFW lifecycle policy, see https://support.forcepoint.com/ProductSupportLifeCycle.

SMC 6.5 is compatible with the following component versions.

- Forcepoint™ Next Generation Firewall (Forcepoint NGFW) 6.2 or higher
- Stonesoft® Next Generation Firewall by Forcepoint (Stonesoft NGFW) 6.0 and 6.1
- McAfee® Next Generation Firewall (McAfee NGFW) 5.7, 5.8, 5.9, and 5.10
- Stonesoft Firewall/VPN Express 5.5
- McAfee® ePolicy Orchestrator® (McAfee ePO™) 5.0.1 and 5.1.1
- McAfee® Enterprise Security Manager (McAfee ESM) 9.2.0 or higher (9.1.0 CEF only)

New features

This release of the product includes these new features. For more information and configuration instructions, see the *Forcepoint Next Generation Firewall Product Guide* and the *Forcepoint Next Generation Firewall Installation Guide*.

SD-WAN dashboard

The SD-WAN dashboard makes the software-defined wide area network (SD-WAN) features that are already part of Forcepoint NGFW more visible. The SD-WAN dashboard allows you to monitor SD-WAN features, such as outbound Multi-Link and Multi-Link VPNs, and to view statistics and reports related to SD-WAN features.

Application routing

You can now apply different NAT rules to traffic, select which VPN traffic uses, and redirect traffic to different proxy servers depending on the network applications detected in the traffic.

Route metrics, ECMP, and route monitoring

You can now define multiple static routes to the same destination and apply metrics to the routes. The routes with a lower metric value can be used as backup routes. When you enable the equal-cost multi-path (ECMP) feature on the routes, there is a potential increase in bandwidth as traffic is balanced between the routes. In addition, you can use probes to monitor the status of a route. If a route is unavailable, the route is removed from the routing table and traffic is automatically sent over another route.

Enhancements

This release of the product includes these enhancements.

Enhancements in SMC version 6.5.0

Enhancement	Description
Viewing log data on the SMC Appliance command line	A new option “log-view” for the smca-system command line tool allows you to view the contents of log files in the SMC Appliance log data directory /var/log and in any of its subdirectories.
Audit data storage	For new installations, audit data is stored on its own partition.
Integrated User ID Service on NGFW Engines	You can now use the Integrated User ID Service on the NGFW Engines to provide transparent user identification for access control by user. The Integrated User ID Service is primarily meant for demonstration purposes and proof-of-concept testing of user identification services.
LDAP authentication for administrators	You can now authenticate administrators using simple password authentication against integrated external LDAP databases.
VPN tunnels can remain established	You can now set specific VPN tunnels to always remain established even when no traffic is sent through the VPN tunnel.
Improved sorting options in the Home view	You can now organize Active Alerts by Severity and Type, and organize User Behavior Events by Activity, User, User Alert Check Type, User Alert, and Severity.
IPv6 support for DHCP relay	You can now use DHCP relay on interfaces that have IPv6 addresses.
Node-initiated contact to Management Server for clustered NGFW Engines	Firewall Clusters and Master NGFW Engines in the Firewall/VPN role now support node-initiated contact to the Management Server. The clustered NGFW Engine opens a connection to the Management Server and maintains connectivity.
More precise controls for endpoint use	You can now define which VPN endpoints can communicate with each other, and how the endpoints are used in a Multi-Link configuration.
Dynamic routing with active-active clustering	You can now use dynamic routing in Firewall Clusters that use load-balancing mode. In load-balancing mode, all nodes in the cluster are online at the same time and traffic is balanced between the nodes, increasing performance for inspection and VPN traffic.
Support for ECA Evaluation deployment	It is now easier to deploy the Endpoint Context Agent to a limited set of users for evaluation. The ECA client and all necessary certificates can be downloaded from the ECA Evaluation web application and installed on endpoints. For details, see Knowledge Base article 16193.
Dynamic elements specific to cloud platforms	You can use a specific naming scheme with Domain Name elements in Access rules to run a script on the NGFW Engine that resolves dynamic element names specific to a cloud platform to IP addresses. The IP addresses are resolved through API calls rather than regular network DNS queries. For more information, see Knowledge Base article 16290.

Enhancements in SMC version 6.5.1

Enhancement	Description
TLS Profile for connecting to Forcepoint servers	The Management Server now uses a custom TLS Profile element for automatically downloading license updates, dynamic updates, and NGFW Engine upgrades from Forcepoint servers. The TLS Profile element defines the settings for cryptography, trusted certificate authorities, and the TLS version used in TLS-protected traffic.

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.

Resolved issues in SMC Appliance 6.5.1

Description	Issue number
Special characters specific to macOS are not displayed correctly in Management Client menus.	SMC-1296
The status icons for NGFW Engines in the Home view blink when log reception from any of the NGFW Engines is in an error state. This issue might happen when an NGFW Engine is sending log entries that were spooled on the NGFW Engine.	SMC-12584
When you use an HTTPS Service element in the policy for NGFW Engines running version 6.3 or lower, policy validation shows the following warning: "Service with Protocol Agent HTTPS contains parameter 'Redirect connections to Proxy Server'. This parameter is not supported by engine version X. The parameter is ignored."	SMC-13535
When you edit a policy-based VPN, changes on the Mobile VPN tab are saved even if you do not save the VPN. However, these changes might not be shown on the Tunnels tab until you save the VPN.	SMC-13872
If the User monitoring view is kept open for a long time, it might not be stable when showing all users.	SMC-14605
The Administration | Tasks | History branch does not show the progress of running tasks.	SMC-14772
You cannot select an interface that has a dynamic IP address as one of the Listening Interfaces in the ECA Connection Settings on the Endpoint Integration tab of the Engine Editor. The Engine Editor incorrectly allows you to select Zone elements that are associated with interfaces that have dynamic IP addresses. This configuration causes policy installation to fail.	SMC-15412
An administrator whose logon is delayed due to the password policy is shown as being disabled. See Knowledge Base article 16422.	SMC-15433
You cannot enable or disable user database replication using the SMC API.	SMC-15576
If you duplicate a Network Application element that has a Context with multiple nested conditions, the new Network Application element does not match traffic correctly.	SMC-15915
When you use temporary filters in reports, report sections are empty even though data is available.	SMC-16112
When you change the interface ID of a physical interface, the VLAN IDs under the interface might not be updated in the routing tree.	SMC-16117
Policy generation is slow when hundreds of tunnel interfaces are configured.	SMC-16244

Description	Issue number
New tasks such as policy upload do not start if an administrator begins to import elements, but does not click Continue to proceed with the import.	SMC-16247
The SD-WAN dashboard shows VPN gateways and VPNs even after the VPN configuration has been removed.	SMC-16275
In some cases, the license database might become corrupted during an SMC upgrade. After upgrading the SMC, all policy installations fail and the following message is shown: "Upload failed: License database integrity check failed".	SMC-16280
Administrators with restricted permissions cannot reply to messages sent by other administrators.	SMC-16292
If you have created a Log Data Context in an administrative Domain, you cannot delete the Domain even if there are no other elements in the Domain.	SMC-16322
When you select the Analyze option in the Logs view, you might see the message "Server lost, reconnecting".	SMC-16328
If a rule that references an unused element was overwritten when a policy was imported, the deletion of the unused element might fail when you try to delete the element. A "Database problem" message is shown.	SMC-16340
You cannot select a port group interface on an integrated switch as the Listening Interface in the ECA Connection Settings. Saving the configuration fails and the following message is shown: "Incorrect ECA settings. NIC X Interface is not a valid interface for ECA."	SMC-16413
When you set a custom MTU value for a Layer 3 Physical Interface on a Master NGFW Engine, a message that recommends setting the same MTU value for VLAN interfaces on the physical interface is shown. When you remove a custom MTU value from a Layer 3 Physical Interface on a Master NGFW Engine, this message is not shown.	SMC-16415
When the "Show only matching rules" option is selected, rule searches do not show matching rules in sub-policies even though the total number of matching rules includes these rules.	SMC-16614
On the Logs tab of the Web Portal, the Print PDF option might fail and an error message might be shown.	SMC-16631
Release notes for engine upgrades and dynamic update packages are not available directly from the Management Client.	SMC-16704
When there are several simultaneous log reading operations, such as browsing log entries, generating reports, and archiving log entries, that cover long time periods, the Log Server might suddenly allocate a large amount of memory and run out of memory.	SMC-16738
The ECA evaluation deployment described in Knowledge Base article 16193 does not work on the SMC Appliance.	SMC-16755
On the Routing pane of the Engine Editor, you cannot add the same Dynamic NetLink element to both an interface that has an IPv4 address and an interface that has an IPv6 address to use the same Dynamic NetLink for IPv4 and IPv6 traffic.	SMC-16837
Validation for the IKE Phase-1 ID in VPN endpoints does not allow domain names where one part of domain name is only numbers.	SMC-16838
Automatic rules that allow NetLink probing are not generated for Server Pools that have dynamic DNS updates enabled.	SMC-16841
When you add several users or user groups to the Authentication cell in an SSL VPN Portal Policy, the cell does not show the users or user groups correctly.	SMC-16871

Description	Issue number
When an IKE Phase-1 ID exception is defined for a VPN endpoint, the exception is not applied to the configuration of other NGFW Engines that are used as gateways in the VPN.	SMC-16881
If you select a loopback IP address as a listening IP address for SNMP on the General | SNMP branch of the Engine Editor, the NGFW Engine element cannot be saved.	SMC-16890
When you change the VPN Profile of a route-based tunnel to a VPN Profile that contains settings that are not supported for route-based VPN tunnels, VPN validation does not detect the issue. When you open the properties of the route-based VPN tunnel again, VPN validation detects the issue.	SMC-16911
Automatic deployment of an NGFW Engine in Microsoft Azure using the SMC API fails if the NGFW Engine uses the Bring Your Own License (BYOL) licensing model and the same SMC also manages an NGFW appliance. The correct license is not bound to the NGFW Engine element.	SMC-16987
You cannot remove individual custom color filters from Administrator elements. You can only use the Set to Default option to remove all custom color filters.	SMC-17003
The performance of the Management Client is slow if there is a large number of pending changes on a large number of elements.	SMC-17027
When you activate Dynamic Update 1101 or higher, the "All Cloud Elements" Access Control List is removed from the Granted Elements list of any Administrator elements in which it was selected.	SMC-17037
The same message might appear multiple times in the task pane, such as when collecting sgInfo or upgrading an NGFW Engine.	SMC-17045
You cannot browse users that belong to the InternalDomain user group using the SMC API.	SMC-17084
When you delete an Access Control List element, references to it are automatically removed from administrator permissions but not from administrator account replication. As a result, the list of administrators might be empty even though administrators can log on to the Management Client.	SMC-17109
When you view policies in the Web Portal, disabled rules are shown in the same way as active rules.	SMC-17186
Policy validation shows validation warnings for Exception rules in the Inspection Policy even though rule validation has been disabled for the rules.	SMC-17221
At the beginning of the policy installation process, VPN validation might prevent policy installation from progressing. Policy installation takes much longer than usual.	SMC-17280
The "Use Client Certificates for Authentication" option in the User Authentication branch of the Engine Editor is deselected when you save changes in the Engine Editor.	SMC-17290
After you upgrade the Log Server to version 6.4.2 or higher on a Linux platform, the Log Server fails to start. This issue might occur if you have changed the memory allocation for the Log Server to a value above 6144. The same issue might also occur on the Web Portal Server.	SMC-17421
When two SSL VPN Portal Service elements have the same value in the Title field, only one of the services is included in the NGFW Engine configuration.	SMC-17464
Every time that you modify an element, the validation index for the element in the database increases. When you have made a large number of changes to the same element, the maximum value of the validation index is reached, and the following message is shown: "Cannot increase the sequence value".	SMC-17501
In rare cases, policy installation might fail, and the following message might be shown: "SSL VPN Configuration error: Portal doesn't have any Hostname defined." The next policy installation succeeds.	SMC-17560

Description	Issue number
When you use a custom Network element to represent any network under NetLink elements in the Routing view, the routes for connections that are initiated by the NGFW Engine itself are not generated.	SMC-17618
The value of the down ratio parameter for the Link Status test is not shown in the Management Client. The default value of the down ratio parameter for aggregated link interfaces in load balancing mode is 30. The default value of the down ratio parameter for other types of interfaces is different.	SMC-17696
When Start TLS is selected as the LDAP protocol in an Active Directory Server element, browsing domain users with the Management Client fails.	SMC-17707

Resolved issues in patches 6.5.1P001.sap and 6.5.1U002.sap

Description	Issue number
The SMC Appliance requires all signing certificates to be valid. The trusted update certificate that was used to sign SMC Appliance upgrade patches expired on 18 August 2019. It is not possible to upgrade the SMC Appliance using upgrade patches released before 18 August 2019. For more information, see Knowledge Base article 17745.	SMC-22993

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.

You can use Java Webstart or install the Management Client from a file to allow remote access to the SMC. Java Web Start is enabled by default on the Management Server that is pre-installed on 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 6.5.1.

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: 6.5.1P001
- 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: 6.5.1U001

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*.

CAUTION: Before upgrading the SMC Appliance from version 6.2.0, install the 6.2.0P001 patch. For more information, see Knowledge Base article 14168.

- SMC 6.5 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.
- Upgrading is supported from SMC versions 6.2.0 – 6.2.5, 6.3.0 – 6.3.8, 6.4.0 – 6.4.7, and 6.5.0.
- If you configured SNMP for the SMC Appliance before upgrading to version 6.4.0 or higher, you must configure SNMP again.

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 6.5.1U001
```

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/6.5.1U001.sap
```

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

```
sudo ambr-install 6.5.1U001
```

The installation process prompts you to continue.

5) Enter `Y`.

Result

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 6.5.1.

Known issues

For a list of known issues in this product release, see Knowledge Base article 16274.

Find product documentation

On the Forcepoint support website, you can find information about a released product, including product documentation, technical articles, and more.

You can get additional information and support for your product on the Forcepoint support website at https://support.forcepoint.com. There, you can access product documentation, Knowledge Base articles, downloads, cases, and contact information.

Product documentation

Every Forcepoint product has a comprehensive set of documentation.

- *Forcepoint Next Generation Firewall Product Guide*
- Forcepoint Next Generation Firewall online Help

Note: By default, the online Help is used from the Forcepoint help server. If you want to use the online Help from a local machine (for example, an intranet server or your own computer), see Knowledge Base article 10097.

- *Forcepoint Next Generation Firewall Installation Guide*

Other available documents include:

- *Forcepoint Next Generation Firewall Hardware Guide* for your model
- *Forcepoint NGFW Security Management Center Appliance Hardware Guide*
- *Forcepoint Next Generation Firewall Quick Start Guide*
- *Forcepoint NGFW Security Management Center Appliance Quick Start Guide*
- *Forcepoint NGFW SMC API Reference Guide*
- *Stonesoft VPN Client User Guide* for Windows or Mac
- *Stonesoft VPN Client Product Guide*