



FORCEPOINT

NGFW Security Management Center Appliance

Release Notes

6.6.2

Revision D

Contents

- [About this release](#) on page 2
- [Build number and checksums](#) on page 2
- [System requirements on virtualization platforms](#) on page 3
- [Compatibility](#) on page 3
- [New features](#) on page 3
- [Enhancements](#) on page 5
- [Resolved issues](#) on page 7
- [Install the SMC Appliance](#) on page 11
- [Upgrade the SMC Appliance](#) on page 12
- [Known issues](#) on page 13
- [Find product documentation](#) on page 13

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 6.6.2 is 10720. This release contains Dynamic Update package 1186.

Use checksums to make sure that files downloaded correctly.

- 6.6.2U002.sap

```
SHA1SUM:
339c56b9594ae0d149ac0deafd33758134f2ae20

SHA256SUM:
c1be1d031050ec704895c5dc23e3c88524e6a251875f579017467ee1172c0a23

SHA512SUM:
37edfc4338277ec0bd01b2a35789214d
86f1764896771eef22102f159cc5b07f
7f2506a5b1b45fa266ded3ba0052b150
1aa26d0550af0e34f09f65a3c2938f20
```

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 6.6 can manage all compatible Forcepoint NGFW Engine versions up to and including version 6.6.



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 6.6 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*.

Dynamic link selection for SD-WAN

The VPN links that are used for Multi-Link traffic from applications and protocols, and traffic associated with QoS classes are now automatically selected based on quality metrics defined for the network applications, protocols, and QoS classes. You can now also specify how different types of ISP connections are used for specific types of traffic. For each type of ISP connection, you can specify that:

- The ISP connection is used for the specified type of traffic unless an ISP connection with significantly higher quality is available.
- The ISP connection is used for the specified type of traffic only if the quality of the other ISP connections is too low or the other ISP connections are not available.
- The ISP connection must not be used for the specified type of traffic.

Storage and browsing of log data locally on NGFW Engines

You can now save copies of the most recent log entries locally on the NGFW Engine. Alert entries are also saved locally on the NGFW Engine. You can browse the saved log and alert entries on the command line of the NGFW Engine even if the log and alert entries have already been sent to the Log Server. The length of time for which the log and alert entries are stored depends on the size of the NGFW Engine's disk and the volume of log data. You can also set limits for how long log entries are stored, and how much disk space can be used for storage.

LLDP support

NGFW Engines can now use the Link Layer Discovery Protocol (LLDP) to send information, such as information about interfaces and MAC addresses on the NGFW Engine, to directly connected devices on the network. The NGFW Engines can also receive information that other devices on the network send. In the Management Client, you can now monitor information that the NGFW Engine has received about devices in directly connected networks.


Support for LTE modems on NGFW Engines in the Firewall/VPN role

You can now use LTE modems for mobile broadband connections on 4G networks with NGFW Engines in the Firewall/VPN role. Support for LTE modems is only available on specific purpose-built NGFW appliance models (NGFW 50 Series).

Enhancements

This release of the product includes these enhancements.

Enhancements in SMC version 6.6.0


Enhancement	Description
Easier forwarding to a proxy	You can now configure forwarding traffic to a proxy or host directly in the Access rules rather than in the NAT rules.
Shared interfaces on Master NGFW Engines	<p>Layer 3 physical interfaces on Master NGFW Engines in the Firewall/VPN role can now be shared interfaces.</p> <ul style="list-style-type: none"> You can now connect Virtual Firewalls to the same network without dedicating one physical interface or VLAN for each Virtual Firewall. The Virtual Firewalls can now communicate with each other without an external switch or router. Link aggregation is supported on Virtual Firewalls.
IPv6 support for user authentication	User authentication now supports IPv6 addresses. Communication between NGFW Engines and TACACS+ authentication servers now also supports IPv6 addresses.
Server Pool enhancements	<p>The following enhancements have been made for the Server Pool feature:</p> <ul style="list-style-type: none"> You can now use Server Pool elements in NAT rules to apply both source and destination NAT for Server Pool load balancing. The Server Pool feature now supports IPv6.
New URLs for dynamic updates and engine upgrades	<p>To improve the performance of automatic dynamic updates and engine upgrades, the following new URLs are available in SMC 6.5.0 and higher:</p> <ul style="list-style-type: none"> https://autoupdate.ngfw.forcepoint.com/dynup.rss https://autoupdate.ngfw.forcepoint.com/ngfw.rss <div>  <p>Note: The SMC automatically starts using the new URLs when you upgrade to SMC 6.5.0 or higher and activate the dynamic update package that includes the new URLs.</p> </div> <p>The new URLs use a content distribution network (CDN) to allow the SMC to download dynamic update packages and engine upgrade files from the geographically closest server. The legacy https://update-pool.stonesoft.com/index.rss URL remains available for backward compatibility and as a backup for the new URLs.</p>
Configurable update services for dynamic updates and engine upgrades	<p>New Update Service elements define sets of URLs for automatic dynamic updates and engine upgrades. In SMC 6.5.0 and higher, the SMC automatically uses Update Service elements that include both the new URLs and the legacy URL. No action is needed to start using the Update Service elements that include the new URLs.</p> <p>Starting from SMC 6.5.2, you can optionally change which Update Service element is used for automatic dynamic updates and engine upgrades. For more information, see Knowledge Base article 16589.</p>

Enhancement	Description
Audit log improvements	<p>Audit entries now include information as text about the changes made to elements when the following configurations are modified:</p> <ul style="list-style-type: none"> • VLAN interfaces on Master NGFW Engines • Virtual Resources on Master NGFW Engines • IP addresses on Virtual NGFW Engines • Antispoofing on Virtual NGFW Engines • Announced Networks for dynamic routing on Virtual NGFW Engines • External BGP Peers on Virtual NGFW Engines • Matching Conditions in Route Maps on Virtual NGFW Engines • Route Entry Settings in Route Maps on Virtual NGFW Engines • IP prefix lists on Virtual NGFW Engines • Comments on Virtual NGFW Engines
Improvements in the Pending Changes feature	Improvements in the Pending Changes feature prevent an element from appearing in the Pending Changes list when an administrator clicks OK without modifying the properties of the element.
User interface rendering on macOS	The Management Client now detects the operating system in use. On macOS, for example, the appropriate window control icons and special characters in keyboard shortcuts are shown.

Enhancements in SMC version 6.6.1

Enhancement	Description
Details of User Behavior Events	In the User Dashboard, you can now view related log entries for entries in the User Behavior Events pane.
New option to show disabled tunnels in the SD-WAN dashboard	A new option for viewing disabled tunnels has been added in the SD-WAN dashboard. The new Show Disabled Tunnels option is available in the Tunnels pane on branch home pages and VPN home pages.
Possibility to define the OSPF Area ID as an IP Address	You can now define the OSPF Area ID as an IP address instead of converting it to a decimal number as previously instructed in Knowledge Base article 16319 .
Endpoint Information shows the user's computer name	The Endpoint Information pane in the User Dashboard can now show the computer name from which the user is connected.
ECMP option for BGP	You can now set an equal cost multi path (ECMP) value in the BGP configuration using the Management Client.

Enhancements in SMC version 6.6.2

Enhancement	Description
EasyConnect forwarding to the Forcepoint Web Security Cloud	<p>You can now configure EasyConnect to forward web traffic from Forcepoint NGFW to Forcepoint Web Security Cloud. For more information, see Knowledge Base article 10582.</p> <div>  CAUTION: This feature requires NGFW Engine version 6.5.6, 6.6.3, 6.7.0, or higher. </div>

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 6.6.2

Description	Issue number
VPN validation warns about disabled tunnels even though it is normal for Multi-Link VPNs to have disabled tunnels.	SMC-1234
Rules in a policy are shown in different colors to indicate the different template levels that the rule is inherited from. The rule template that the rule is inherited from is not shown in text format.	SMC-1279
VPN validation incorrectly gives warnings about disabled tunnels.	SMC-2405
The automatic rule for Endpoint Context Agent (ECA) does not allow the necessary traffic when the Source Networks field is left blank. The default value, Internal Zone, is not used correctly.	SMC-9117
The certificate request for browser-based user authentication does not include the Subject Alternative Name attribute. The Google Chrome web browser does not accept server certificates that do not have this attribute.	SMC-9163
Deleting custom Endpoint Application elements is slow.	SMC-12900
If the Management Server does not have access to Forcepoint servers, the following alert is sent constantly regardless of the specified update check interval: "Management Server: Update server not available".	SMC-16638
Expression element translation values are not updated until the element is revalidated. If an element within an Expression element is updated, the change is not reflected in the Network Details view in the policy editor. The Expression element is revalidated when the policy is installed or if the Expression element is edited.	SMC-17851
When searching for rules in a large policy that produces many matches, not all the matching rules are shown. You must click Next to show all the matching rules.	SMC-18333
When you create an additional VPN gateway for a firewall, the list of endpoints shown in the Engine Editor does not match under the different gateways.	SMC-18400
When dragging and dropping elements between rules, or adjusting column widths, the performance of the Policy Editor decreases.	SMC-19672

Description	Issue number
When a VPN endpoint has Phase-1 ID exceptions configured, the VPN Client configuration always uses the default Phase-1 ID even if the VPN Client is included in a VPN for which an exception is defined.	SMC-19775
Automatic IPv6 Access rules for ping monitoring of Server Pool members are not correctly generated.	SMC-20158
If AES-GCM-256 and AES-GCM-128 are the only cipher algorithms set in the VPN profile for mobile VPN, the client configuration is not generated. When installing the policy, you see the following message: "The Configuration for FORCEPOINT IPsec VPN Client has not been generated for the Gateway: <name>. The FORCEPOINT IPsec VPN Client does not support one or more settings in the VPN Profile".	SMC-20463
Only one contact address is included in the initial configuration for an NGFW Engine, even if several contact addresses have been defined for the Management Server. In a high availability (HA) SMC environment, all Management Server IP addresses are included.	SMC-20596
When editing a large VPN, it is useful to select Tools > Filter by Gateway. However, when you select Tools > No Filtering, the filter is not removed correctly.	SMC-20798
When you use SMC Web Access in Linux, sgInfo files are saved on the Management Server even though you select the option to save the files on your local workstation.	SMC-20990
An MSSP report might show the date 01/01/1970 for an expired license.	SMC-21039
When there are three Management Servers, excluding one standby Management Server from database replication also causes a database mismatch for the other standby Management Server.	SMC-21040
If QoS Class elements are used for link selection for outbound traffic, when the policy is installed, the NAT entry identification changes unnecessarily. The NGFW Engine considers this to be a network configuration change, even if the configuration has not changed.	SMC-21294
When you search an external LDAP server, you might see the message: "Failed to refresh Folder Search. Could not search an entry from base dn". This might happen if there is a large number of users and groups on the external LDAP server.	SMC-21307
In the Active Alerts view, the Details option might not be available after you change the way the view is sorted or aggregated.	SMC-21398
When you remotely upgrade an NGFW Engine cluster, the upgrade does not proceed after "Waiting for all the nodes to come back online..." is shown on the progress tab even though the upgrade is successful to all nodes.	SMC-21405
If a loopback interface is used as the interface for DHCP relay in the VPN Client settings for a VPN gateway, the automatic rules do not allow these relayed DHCP packets.	SMC-21683
You cannot create an SSID interface that uses a custom MAC address.	SMC-21705
The Where Used? option might not find a user or group used in a configuration if the Base DN configured on an Active Directory server uses one case (lower case, for example), but the SMC element that represents that Active Directory server is configured to use the same Base DN, but uses a different case (upper case, for example).	SMC-21717
The system alias \$\$ Local Cluster(NDI addresses only) does not include loopback NDI addresses.	SMC-21766
When you configure protocol-independent multicast (PIM) on a tunnel interface, the CVI address on the tunnel interface must be saved before you continue configuring PIM in the Routing view.	SMC-21799
The performance of the Routing view is decreased when there is a large number of tunnel interfaces.	SMC-21800

Description	Issue number
It is possible to use an SMC API Client name and authentication key to log on to the Management Client.	SMC-21817
If the certificate for SMC Web Access is created without a common name (CN), you cannot set the host name in the Management Server properties.	SMC-21832
If you right-click a VPN Site, then select New Site, the new VPN Site might replace the existing VPN Site.	SMC-21854
Policy installation fails on a Master NGFW Engine in the Firewall/VPN role that hosts a Virtual Firewall that has only a Layer 2 interface configured.	SMC-21865
It is not possible to delete a blacklist entry for a Virtual NGFW Engine.	SMC-21887
An audit entry is not created when there is a failed SMC API logon attempt and the password policy locks the account.	SMC-21928
It is not possible to set the Location option for Active Directory Server and LDAP Server elements.	SMC-21965
When you add an NGFW element to a Location element that has already been saved, the change is not saved unless you also modify the comment or name of the Location element.	SMC-21986
When you search for rules, only the rule ID for sub-policy rules is shown. If there are several levels of sub-policies, it can be difficult to see the location of the rule.	SMC-22002
When you search in rules, the search can match against a sub-policy rule, even if the jump rule to that sub-policy rule does not match.	SMC-22004
You cannot sort the Routing monitoring view by the Network column.	SMC-22028
When you set the pre-shared key for an SSID interface, the key is not saved.	SMC-22040
When you compare a policy snapshot from an audit entry to the current policy, the comparison indicates that every rule has been changed, even when the policy has not been modified.	SMC-22058
Automatic license updates or dynamic update downloads might fail.	SMC-22093
Upgrading the Management Server might take up to an hour if there are several larger policies.	SMC-22104
In rare circumstances, when you refresh the policy on a Virtual NGFW Engine while an earlier policy refresh is still in progress for other Virtual NGFW Engines on the same Master NGFW Engine, the policy refresh might fail.	SMC-22110
When you create a backup to a local workstation, instead of storing to the user-specified path, the backup is always stored in the default folder.	SMC-22123
When you create a new VPN site from the Engine editor, the VPN Site Properties dialog box might not open or the list of available elements might be empty.	SMC-22136
The snapshot comparison view can take a long time to open.	SMC-22158
When using the SMC API, a rule can be created by specifying a rule insert point. It is not possible to query an existing rule insert point.	SMC-22166
You cannot select the VPN type in additional VPN Gateway elements that have an endpoint with a dynamic IP address. All types of VPNs are automatically selected.	SMC-22270
When you use the Management Client on a computer with multiple displays, popup menus might open on a different display than the main Management Client window.	SMC-22283

Description	Issue number
When using Azure automatic scaling, the Management Server creates new NGFW Engine instances automatically. Policy installation might start before initial contact has been successfully made.	SMC-22284
When you use a DNS name as a contact address, the DNS name can include only one dash (-) character.	SMC-22286
When you convert a Firewall Cluster to a Master NGFW Engine cluster, DHCP Relay settings on the VPN > VPN Client branch of the Engine Editor change.	SMC-22339
When a VPN is open in preview mode, changing to edit mode might fail. The following message is shown: "Failed to construct proxy identities".	SMC-22364
Administrators are not notified of changes to the permissions of the administrator role that is assigned to them when they log on to the Management Client.	SMC-22422
When there are several Active Directory Servers, browsing the user tree might fail.	SMC-22428
If the first node of a cluster is not available, adding or deleting blacklist entries from the Management Server fails.	SMC-22434
When you change the MTU setting for a port group interface, the routing configuration for the interface is reset to the default value.	SMC-22456
In environments where an additional Log Server is used for high availability, it is not possible to have more instances of the Blacklist monitoring view open than there are online nodes for the NGFW Engine. The following message is shown: "Message code 203 Internal error".	SMC-22515
If a node for a Master NGFW Engine is disabled, it is not possible to preview the Quagga configuration on a hosted Virtual NGFW Engine.	SMC-22517
Running the Capture Traffic tool on an NGFW Master Engine fails if the first node of the cluster is in the offline state.	SMC-22543
When a new license is installed and license binding changes, the Licenses view does not show the changes until the Management Server service is restarted.	SMC-22560
After you have viewed the details of an alert in the Active Alerts view, the information might not be updated when you view the details of the next alert.	SMC-22590
Adding or editing a valid expression might fail when using the SMC API.	SMC-22598
When you export a report that includes top rate sections as a PDF, some information might not be visible in the PDF. The information is visible if you export the same report in table format.	SMC-22620
When you copy an Access rule that includes the Use VPN action from a policy in one administrative Domain to a policy in another administrative Domain, it is no longer possible to edit the policy to which you copied the rule.	SMC-22696
When there are a large number of Log Servers, viewing logs might fail after you add a new Log Server.	SMC-22705
When a Log Server forwards both active alerts and blacklist entries to the Management Server, the forwarded active alerts and blacklist entries might conflict. Either the active alerts or blacklist entries might be ignored. As a result, alert notifications might not be sent even though an alert is generated and is visible in the Logs view.	SMC-22715
When an SMC API client session times out, the Management Server might return error 404 instead of error 401.	SMC-22738

Description	Issue number
When the Connections monitoring view is open, the NGFW Engine does not remove some old connections from the connections table.	SMC-22783
The --force option for the ambr-install command does not override dependencies on the SMC Appliance.	SMC-22809
Exporting some reports as HTML or PDF might fail on the SMC Appliance.	SMC-22830
It is possible to use characters in the Management Server database password that prevent restoring a Management Server backup.	SMC-22832
You cannot use a fully qualified domain name (FQDN) as the contact address for an Active Directory Server.	SMC-22872

Resolved issues in patch 6.6.2U002.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 Web Start 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 6.6.2.

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: 6.6.1P001
- 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: 6.6.1U001

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 6.6 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 – 6.4.10, 6.5.0 – 6.5.6, 6.5.8 – 6.5.9, and 6.6.0 – 6.6.1.
- 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 6.6.2U001
```

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/6.6.2U001.sap
```

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

```
sudo ambr-install 6.6.2U001
```

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 6.6.2.

Known issues

For a list of known issues in this product release, see Knowledge Base article [16950](#).

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

