



FORCEPOINT

Next Generation Firewall

**How to install
Forcepoint NGFW in FIPS mode**

6.7
Revision A

Contents

- [Introduction](#) on page 2
- [Installing the SMC Appliance in FIPS mode](#) on page 2
- [Installing the SMC in FIPS mode](#) on page 6
- [Installing the NGFW Engine in FIPS mode](#) on page 13

Introduction

You can use the Forcepoint Next Generation Firewall (Forcepoint NGFW) in FIPS mode to comply with Federal Information Processing Standards (FIPS).

The Forcepoint NGFW solution includes NGFW Engines, Forcepoint NGFW Security Management Center (SMC) server components, and SMC user interface components. The basic SMC components are the Management Server, Log Server, and one or more Management Clients. The Management Client is the user interface for the SMC. You use the Management Client for all configuration and monitoring tasks.

There are two main ways to deploy the SMC:

- You can use a Forcepoint NGFW Security Management Center Appliance (SMC Appliance) that ships with a Management Server and a Log Server pre-installed on it.
- You can install the SMC on Windows or Linux platforms.

In a FIPS environment, you must use NGFW Engines that run on purpose-built Forcepoint NGFW appliances.

Installing the SMC Appliance in FIPS mode

To use the SMC Appliance in a FIPS environment, you must install the SMC Appliance in FIPS mode.

You must complete the following main steps:

- 1) Enable FIPS mode on the SMC Appliance.
- 2) Check the SMC Appliance self-tests.
- 3) Install the Management Client.

Related tasks

[Enable FIPS mode on the SMC Appliance](#) on page 3

[Check the SMC Appliance self-tests](#) on page 4

[Install the Management Client](#) on page 11

Enable FIPS mode on the SMC Appliance

You must enable FIPS mode when you install the SMC Appliance.

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 administrator account name and password.
 - a) Enter the administrator account name.
This field is case sensitive and limited to eight characters.
 - b) Enter the password.
The password is case sensitive and must have a minimum of ten characters.
 - c) Enter the password again.



Note: The administrator account and password are used for command line access to the SMC Appliance and for access to the Management Client.

- 5) (Optional) Configure a bootloader password.
 - a) Enter `y` to configure a bootloader password.
 - b) Enter the password.
 - c) Enter the password again.
- 6) Make your security selections.
 - a) Select FIPS 140-2 mode.
 - b) (Optional) Select 256-bit encryption as the security strength.
- 7) Select whether to configure a secondary management interface.
- 8) Complete the network interface and network setup fields.
 - a) Select the main network interface for management.
 - b) Complete the network setup fields for the interface.
- 9) (Secondary management interface only) Complete the network interface and network setup fields for the second network interface for management.

- 10) Enter a host name for the Management Server.
- 11) Select the time zone.
- 12) Set the time.
- 13) (Optional) Configure NTP server settings.

Result

When the installation is complete, the SMC Appliance restarts.

Check the SMC Appliance self-tests

The SMC Appliance contains several modules that run self-tests when the SMC Appliance starts. Known answer tests (KAT) and pairwise consistency tests (PCT) are run.

Bouncy Castle FIPS Java API software module self-tests

Algorithm	Type
Software Integrity	KAT
AES	KAT
CCM	KAT
AES-CMAC	KAT
FFC KAS	KAT
DRBG	KAT, Continuous, Health Checks
DSA	KAT, PCT
ECDSA	KAT, PCT
GCM/GMAC	KAT
HMAC	KAT
ECC KAS	KAT
RSA	KAT, PCT
SHS	KAT
TDES	KAT
TDES-CMAC	KAT
Extendable-Output functions (XOF)	KAT
Key Agreement Using RSA	KAT
Key Transport Using RSA	KAT
NDRNG	Continuous
DH	PCT

Algorithm	Type
SP 800-56A	Assurances

OpenSSL FIPS Object Module self-tests

Algorithm	Type
Software Integrity	KAT
HMAC	KAT
AES	KAT
AES CCM	KAT
AES GCM	KAT
XTS-AES	KAT
AES CMAC	KAT
TDES	KAT
TDES CMAC	KAT
RSA	KAT, PCT
DSA	PCT
DRBG	KAT, Continuous
ECDSA	PCT
ECC CDH	KAT

Check the self-test results in the console.

- If the Bouncy Castle FIPS Java API cryptographic module self-test fails, the server application fails to start and an error message is shown on the console. The error message is also sent to SMC Appliance syslog.

```
Starting Forcepoint NGFW Management Server: [FAILED]
SMC: Cryptographic self-tests failed. Try restarting the server
Starting Forcepoint NGFW Log Server: [FAILED]
SMC: Cryptographic self-tests failed. Try restarting the server
```

- If a power-up self-test fails, an error message is shown on the console and the appliance turns off and is not remotely accessible.

```
fipstest: Performing FIPS RNG selftest...
Fatal FIPS Error: fipstest:ERROR:FIPS RNG selftest failed.
Failed tests: /lib/fips/fipstest-rng.sh: 1
fipstest: Performing FIPS OpenSSL crypto selftests...
Fatal FIPS Error: fipstest:ERROR:FIPS OpenSSL crypto selftest failed: /lib/fips/fipstest-openssl: 1
```

- If the file system integrity check fails, an error message is shown on the console and the appliance turns off and is not remotely accessible.

```
fipscheck: Performing FIPS integrity check...
Fatal FIPS Error: fipscheck:ERROR:FIPS check failed. /lib/fips/fipscheck: 1
```

Next steps

- If the self-tests succeed, continue configuring the SMC Appliance.
- If a self-test fails, and the SMC Appliance does not restart automatically, restart it manually.

- If a self-test continues to fail, reset the SMC Appliance to factory settings.

Related tasks

[Install the Management Client](#) on page 11

Reset the SMC Appliance to factory settings

If a self-test fails on the SMC Appliance, reset the SMC Appliance to factory settings.

Steps

- 1) Connect to the SMC Appliance command line using one of these options.
 - Connect a keyboard to a USB port and a monitor to the VGA port, then press **Enter**.
 - Connect to the IP address of the iDRAC port, then start the virtual console on the **Server Properties** tab.
- 2) Turn on the SMC Appliance, and at the boot menu, select **Virtual CD**.
- 3) Press **N** to start a new installation.
- 4) Press **I** to start the installation.
- 5) Enter **Erase**, then press **Enter** to erase the disk.
- 6) When prompted, press **Y** to reboot the SMC Appliance.
- 7) Install the SMC Appliance in FIPS Compatible Mode.

Installing the SMC in FIPS mode

If you do not have a pre-installed SMC Appliance, you must enable FIPS restrictions on the Management Server, the Log Server, and the Management Client when you install them.

For detailed installation instructions and information about hardware requirements for third-party hardware, see the *Forcepoint Next Generation Firewall Installation Guide* and the *Forcepoint NGFW Security Management Center Release Notes*.



CAUTION: In Linux, cryptographic modules use `/dev/random` as the randomness source, and that may block installation, startup, or even execution. We recommend that you install and run an entropy daemon, such as `jitterentropy-rngd` or `haveged`.

You must complete the following main steps:

- 1) Download the SMC software from <https://support.forcepoint.com>, then check the file integrity.
- 2) Obtain licenses for all the SMC servers and the Forcepoint NGFW Engine in the License Center at <https://stonesoftlicenses.forcepoint.com>.

Generate the licenses based on your Management Server proof-of-license (POL) code.

- 3) Install the Management Server, the Log Server, and the Management Client.
Enable FIPS restrictions during the installation.
- 4) Start the Management Client.
- 5) Install the licenses for the Management Server and Log Server,

Start the installation

Start the Installation Wizard on the computer where you want to install the SMC components.

Steps

- 1) Log on to the operating system with administrator rights in Windows or as the root user in Linux.
- 2) Start the Installation Wizard from a .zip file or the Installation DVD.
Decompress the .zip file.
 - On Windows, the executable is `\Forcepoint_SMC_Installer\Windows-x64\setup.exe`
 - On Linux, the executable is `/Forcepoint_SMC_Installer/Linux-x64/setup.sh`

If the DVD is not automatically mounted in Linux, use the following command:

```
mount /dev/cdrom /mnt/cdrom
```

- 3) Select the language for the installation, then click **OK**.
The language that you select is also set as the default language of the Management Client.
- 4) Read the information on the **Introduction** page, then click **Next**.



Tip: Click **Previous** to go back to the previous page, or click **Cancel** to close the wizard.

- 5) Select **I accept the terms of the License Agreement**, then click **Next**.
- 6) (Optional) Select where to install the SMC, then click **Next**.
The default installation directory in Windows is `C:\Program Files\Forcepoint\SMC`. Click **Choose** to browse to a different installation folder.



Note: If you install the SMC in `C:\Program Files\Forcepoint\SMC`, the installation creates an extra `C:\ProgramData\Forcepoint\SMC` folder, which duplicates some of the folders in the installation directory and also contains some of the program data.

- 7) (Linux only) Read the instructions about the hosts file, make any necessary configuration changes, then click **Next**.


- 8) Select where to create shortcuts, then click **Next**.
These shortcuts can be used to manually start components and to run some maintenance tasks.
- 9) Select **Typical** as the installation type, then click **Next**.

Install the Management Server


Continue the installation in the Installation Wizard to configure the options for the Management Server.

Steps


- 1) Configure the settings, then click **Next**.

Option	Description
Select Management Server IP Address	Select the Management Server's IP address from the drop-down list. The Management Server's license must be generated using this IP address.
Log Server IP Address	Enter the IP address of the Log Server to which this server sends its log data.
Advanced Management Server Options	<p>When selected, you can configure additional options on another page. Select this option if you want to:</p> <ul style="list-style-type: none"> Disable the use of 256-bit encryption for communication between the Management Server and the NGFW Engines. Enable alternative methods to access the Management Client, such as Java Web Start or using SMC Web Access to run the Management Client in a web browser. (Linux only) Enable integrating NSX with Forcepoint NGFW. <div>  Note: NSX integration with Forcepoint NGFW is not yet supported. </div>
Install as an Additional Management Server for High Availability	When selected, you can configure additional options on another page.
Enable FIPS 140-2 Configuration Restrictions	You must enable this option to use the SMC in FIPS mode.
Install the Management Server as a Service	When selected, the server starts automatically.


- 2) If you selected **Advanced Management Server Options** on the previous page, select the features to enable, then click **Next**.

Option	Description
Enable and Configure Web Start Server	When enabled, administrators can download and start the Management Client from a web page instead of installing the Management Client locally.
Enable and Configure SMC Web Access	When enabled, administrators can access the SMC in a web browser. You can run the Management Client in a web browser instead of installing the Management Client locally. On Linux platforms, xvfb-run must be installed under <code>/usr/bin</code> . You can specify another path in the Management Server properties after the installation has completed.
Enable NSX Service (Linux only)	When enabled, allows integrating NSX with Forcepoint NGFW.  Note: NSX integration with Forcepoint NGFW is not yet supported.
256-bit Security Strength	When enabled, 256-bit encryption is used for communication between the Management Server and the NGFW Engines. This option is selected by default.

- 3) If you enabled the Web Start Server, configure the settings, then click **Next**.

Option	Description
Port Number	Enter the TCP port number that the service listens to. By default, the standard HTTP port numbers (80 on Windows, 8080 on Linux) are used. Linux does not allow the use of reserved ports for this type of service.  Note: Make sure that the listening port is not in use on the server.
Host Name (Optional)	Enter the host name that the service uses. Leave the field blank to allow requests to any of the server's host names.

- 4) If you enabled SMC Web Access, configure the settings, then click **Next**.

Option	Description
Port Number	Enter the TCP port number that the service listens to. By default, port 8085 is used when SMC Web Access is enabled on the Management Server and port 8083 when enabled on the Web Portal Server.  Note: Make sure that the listening port is not in use on the server.
Host Name (Optional)	Enter the host name that the service uses. Leave the field blank to allow requests to any of the server's host names.
Certificate Distinguished Name	Administrators must use an HTTPS connection to access and use the Management Client. Enter the distinguished name for the certificate used to secure the HTTPS connection.
Certificate Algorithm	Select the algorithm and key length for the certificate used to secure the HTTPS connection.
Certificate Signer	Select the signer for the certificate used to secure the HTTPS connection. You can use the Internal Certificate Authority or the certificate can be self-signed.

- 5) Enter a user name and password to create a superuser account, then click **Next**.



Important: This is the only account that an administrator can use to log on after the installation has been completed.

Install the Log Server

Continue the installation in the Installation Wizard to configure the options for the Log Server.

Steps

- 1) Configure the settings, then click **Next**.

Option	Description
Select Log Server IP Address	Select the server's IP address from the drop-down list. If IP address binding is used, the server's license must be generated with this IP address as the binding.
IP Address(es) of the Management Server(s) that will control this Log Server	Enter the IP address of the Management Server that controls this server. If there are multiple Management Servers, enter the IP addresses as a comma-separated list.
Certify the Log Server during the installation	When selected, the server is automatically certified. If the components are installed on different computers and the Management Server is not immediately contactable, deselect this option to avoid connection attempts after installation. Certifying is mandatory for running the server.
Port on which the Log Server will receive data	Enter the port number that the server receives data on.
Enable FIPS 140-2 Configuration Restrictions	You must enable this option to use the SMC in FIPS mode.
Install the Log Server as a Service	When selected, the server starts automatically.

- 2) (Optional) Click **Choose** to browse to a different storage folder for log data.



Note: Remote locations are not suitable for active storage, as quick and reliable access is required.

- 3) Click **Next**.

Finish the installation

Review the configuration options that you set in the Installation Wizard, then finish the installation.

Before you begin

If you are installing any server components as a service on a Windows system, make sure that the Services window is closed before you proceed.



Important: This is the last chance to cancel the installation or make changes. Click **Previous** to adjust your selections.

Steps

- 1) Check that the information in the **Pre-Installation Summary** is correct, then click **Install**.
Depending on the options, you selected, you might be prompted to generate certificates during the installation.
- 2) When the installation has completed, click **Done**.



Note: If any Log Server or Web Portal Server certificate was not retrieved during the installation, retrieve a certificate manually before starting the server.

Install the Management Client

If you did not install the Management Client on the same computer as the Management Server or if you are using the SMC Appliance, you must separately install the Management Client in FIPS mode on each administrator's computer.

For system requirements, see the SMC release notes for your version.




As an alternative to installing the Management Client, you can use SMC Web Access or use Java Web Start. You can enable these features when installing the Management Server, or you can enable them later. SMC Web Access is not supported on the SMC Appliance.

Steps

- 1) Log on to the operating system with administrator rights in Windows or as the root user in Linux.
- 2) Start the Installation Wizard from a .zip file or the Installation DVD.
Decompress the .zip file.
 - On Windows, the executable is `\Forcepoint_SMC_Installer\Windows-x64\setup.exe`
 - On Linux, the executable is `/Forcepoint_SMC_Installer/Linux-x64/setup.sh`

If the DVD is not automatically mounted in Linux, use the following command:

```
mount /dev/cdrom /mnt/cdrom
```

- 3) Select the language for the installation, then click **OK**.
The language that you select is also set as the default language of the Management Client.
- 4) Read the information on the **Introduction** page, then click **Next**.
 **Tip:** Click **Previous** to go back to the previous page, or click **Cancel** to close the wizard.
- 5) Select **I accept the terms of the License Agreement**, then click **Next**.
- 6) (Optional) Select where to install the SMC, then click **Next**.
The default installation directory in Windows is `C:\Program Files\Forcepoint\SMC`. Click **Choose** to browse to a different installation folder.
 **Note:** If you install the SMC in `C:\Program Files\Forcepoint\SMC`, the installation creates an extra `C:\ProgramData\Forcepoint\SMC` folder, which duplicates some of the folders in the installation directory and also contains some of the program data.
- 7) (Linux only) Read the instructions about the hosts file, make any necessary configuration changes, then click **Next**.
- 8) Select where to create shortcuts, then click **Next**.
These shortcuts can be used to manually start components and to run some maintenance tasks.
- 9) Select **Management Client Only** as the installation type, then click **Next**.
- 10) When prompted to select the cryptographic algorithms, select **Restricted Cryptographic Algorithms Compatible with FIPS 140-2**.
- 11) Check that the information in the **Pre-Installation Summary** is correct, then click **Install**.
 **Important:** This is the last chance to cancel the installation or make changes. Click **Previous** to adjust your selections.
- 12) When the installation has completed, click **Done**.

Start the Management Client

After you have started the Management Server, start the Management Client.

Steps

- 1) If you installed the Management Client locally on the workstation, do the following:
 - (Windows) Use the shortcut icon or run the script `<installation directory>/bin/sgClient.bat`.
 - (Linux) Run the script `<installation directory>/bin/sgClient.sh`. A graphical environment is needed.

- 2) If you enabled or installed a Web Start Server, do the following:



Note: Java Web Start is enabled by default on the SMC Appliance.

- a) In a web browser, browse to `http://<server address>:<port>`.
Enter the port only if the server is configured to run on a different port from the HTTP standard port 80.
- b) (Windows or Linux) Click **Start Management Client** to download and start the Management Client.
Web Start automatically checks if the Management Client version on the server is already on your local computer. If not, the new client is automatically downloaded to your computer. This check is done every time to make sure that the latest version is used.
- c) (Mac OS X) Download the `smcclient.jnlp` file.
Open a terminal window in the folder where you saved the file, then run the following command:

```
javaws -Xnosplash smcclient.jnlp
```

- d) When the Management Client starts, log on with your account credentials.

- 3) If you enabled SMC Web Access to run the Management Client in a web browser, do the following:



Note: This feature is not supported on the SMC Appliance.

- a) In a web browser, browse to the URL of the server that you configured the SMC Web Access feature on.
The URL can be the IP address of the server or the host name that you defined in the properties of the server. Make sure that you include the port number at the end of the URL.
Example where SMC Web Access is enabled on the default port 8085 on the Management Server:
`https://127.0.0.1:8085`
- b) Enter your user name and password, then click **Log On**.

Installing the NGFW Engine in FIPS mode

To use the NGFW Engine in a FIPS environment, you must install the NGFW Engine in FIPS mode.

In a FIPS environment, you must use NGFW Engines that run on purpose-built Forcepoint NGFW appliances.

You must complete the following main steps:


- 1) Create an element for the NGFW Engine in the Management Client.
- 2) Enable FIPS mode in the properties of the NGFW Engine element.
- 3) Install the NGFW Engine in FIPS mode.

- 4) Check the results of the self-tests on the Forcepoint NGFW appliance.

Create an element for the NGFW Engine

Use the Management Client to create the NGFW Engine element.

These steps are the high-level tasks. For more information, see the *Forcepoint Next Generation Firewall Product Guide*.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) In the Management Client, create an NGFW Engine, then define the properties in the Engine Editor. Follow the normal process to define the properties of an NGFW Engine, with these exceptions:
 - On the **Advanced Settings** branch, select **FIPS-Compatible Operating Mode**.
 - On the **Advanced Settings > Log Handling** branch, select a suitable setting for the **Log Spooling Policy** option, depending on your network environment.
- 2) Save the initial configuration.



Note: Handle the configuration files securely. They include the one-time password that allows establishing trust with the Management Server.

Install the NGFW Engine in FIPS mode

Use the NGFW Configuration Wizard to install the NGFW Engine in FIPS mode.

These steps are the high-level tasks. For complete installation instructions, see the *Forcepoint Next Generation Firewall Installation Guide*. Before upgrading, read the *Forcepoint Next Generation Firewall Release Notes* for the version you are upgrading to.



Note: NGFW appliances come with NGFW Engine software pre-installed. Before setting the NGFW Engine to use FIPS mode, upgrade the NGFW Engine software to the version that you want to use.

Steps

- 1) Download the NGFW Engine software from <https://support.forcepoint.com/Downloads>, then validate the checksums.



Note: Save the NGFW Engine upgrade .zip file to the root directory of the USB drive or DVD media.

For information about obtaining the installation files, see the *Forcepoint Next Generation Firewall Installation Guide*.

- 2) Upgrade the NGFW Engine software to the version that you want to use.
 - a) In the NGFW Configuration Wizard, select **Firewall/VPN** as the role.

- b) Select **Upgrade**.
 - c) In the **Select Source Media** dialog box, select the appropriate media type, then click **OK**.
The software update signature is verified.
 - d) Click **OK**.
The upgrade starts.
 - e) Select **Set kernel in FIPS mode after reboot**.
 - f) Click **OK**.
The NGFW Engine restarts and displays the upgraded version.
- 3) Configure the NGFW Engine with the NGFW Configuration Wizard.
Follow the normal process to define the NGFW Engine properties, with these exceptions:
- Select **FIPS-Compatible Operating Mode**.

Check the NGFW Engine self-tests

The NGFW Engine contains the OpenSSL FIPS Object Module, NGFW Cryptographic Library, and NGFW Cryptographic Kernel Module. The modules run several self-tests when the Forcepoint NGFW appliance starts.

The modules perform these tests:

- Cryptographic algorithm known answer tests (KAT)
- Software integrity tests using HMAC verification
- Conditional self-tests for CTR-DRBG
- Pair-wise consistency test (PCT) on generated RSA, DSA, and ECDSA keys
- File system integrity check using the OpenSSL FIPS Object Module and HMAC

OpenSSL FIPS Object Module self-tests

Algorithm	Type
Software Integrity	KAT
HMAC	KAT
AES	KAT
AES CCM	KAT
AES GCM	KAT
XTS-AES	KAT
AES CMAC	KAT
TDES	KAT
TDES CMAC	KAT
RSA	KAT, PCT

Algorithm	Type
DSA	PCT
DRBG	KAT, Continuous
ECDSA	PCT
ECC CDH	KAT

NGFW Cryptographic Library self-tests

Algorithm	Type
Software Integrity	KAT
AES	KAT
TDES	KAT
DSA	PCT
RSA	KAT, PCT
ECDSA	KAT, PCT
SHS	KAT
HMAC	KAT
DRBG	KAT, Continuous
Diffie-Hellman	KAT, PCT
EC Diffie-Hellman	KAT, PCT

NGFW Cryptographic Kernel Module self-tests

Algorithm	Type
Software Integrity	KAT
AES	KAT
TDES	KAT
HMAC	KAT
SHA	KAT

Check the self-test results in the console.

- If a cryptographic self-test or the file system integrity check fails, an error message is shown on the console and the appliance is restarted automatically.

```
FIPS: OpenSSL self-tests FAILED, rebooting...
FIPS: rootfs integrity check FAILED, rebooting...
```

Next steps

- If the self-tests succeed, continue configuring the NGFW Engine.
- If the problem persists, reset the Forcepoint NGFW appliance to factory settings.

Reset the NGFW appliance to factory settings

If a cryptographic self-test or the file system integrity check fails, you must reset the appliance to factory settings.

If the appliance is otherwise functioning correctly, but you want to destroy all cryptographic keys on the NGFW appliance, you can also reset the appliance to factory settings from the Management Client. For more information, see the *Forcepoint Next Generation Firewall Product Guide*.

Steps

- 1) Restart the Forcepoint NGFW appliance, then select **System restore options** from the boot menu.
- 2) Select **Advanced data removal options**.
- 3) Select the number of overwrite passes.
A larger number of overwrites is more secure, but it might take a considerable amount of time depending on the appliance storage capacity.
 - For one pass, select **1 pass overwrite**.
 - For multiple passes, select **Custom**, then enter the number of overwrite passes.
- 4) Install the NGFW Engine in FIPS mode.

