Network Security Platform

7.3

How to install Forcepoint Network Security Platform in FIPS mode

Revision A

Contents

- Introduction on page 2
- Installing the SMC Appliance in FIPS mode on page 3
- Installing the SMC in FIPS mode on page 11
- Installing the Security Engine in FIPS mode on page 19

Introduction

You can use the Forcepoint Network Security Platform in FIPS mode to comply with Federal Information Processing Standards (FIPS).

The Forcepoint Network Security Platform solution includes Security Engines, Forcepoint 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 SMC Clients. The SMC Client is the user interface for the SMC. You use the SMC Client for all configuration and monitoring tasks.

There are two main ways to deploy the SMC:

- You can use a Security Management Center appliance that ships with a Management Server and a Log Server pre-installed on it.
  You can also install the SMC Appliance as a virtual machine on virtualization platforms such as VMware ESX. For more information, see *Installing SMC Appliance software on a virtualization platform* in the *Forcepoint Network Security Platform Installation Guide*.
- You can install the SMC components on Windows or Linux platforms.

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

FIPS mode restrictions

When FIPS mode is enabled, the following restrictions are enforced:

- The Security Engine local console, command line interface, and SSH access are not available
- The available cryptographic algorithms and configuration options in the SMC are restricted:
  - RSA key sizes of 2048 bits or greater are used for digital signature generation
  - ECDSA key sizes of 256 bits or greater are used for digital signature generation
  - SHA-1 cannot be used for digital signature generation
  - The minimum password length for SMC backup encryption is 14 characters

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 SMC Client.

Related tasks

Enable FIPS mode on the SMC Appliance on page 3
Check the SMC Appliance self-tests on page 6
Install the SMC Client on page 16

Enable FIPS mode on the SMC Appliance

You must enable FIPS mode and enable 256-bit encryption as the security strength when you install the SMC Appliance.

Before you begin

Prepare the appliance for installation:

- Determine the appliance networking information:
  - IPv4 network address and network mask
  - (Optional) Default gateway address
  - (Optional) DNS server addresses
- Install the SMC Appliance as a virtual appliance in ESXi. Follow the guidelines in the Installing SMC Appliance software on a virtualization platform appendix in the *Forcepoint Network Security Platform Installation Guide*.
- Access the appliance using the virtual machine console in the VMware Host Client.

The password is not shown while logging on to the local console. No configuration or preparatory steps are required.

When 256-bit encryption is enabled, the SMC TLS Client and Server settings are automatically configured to use:

- TLS 1.2 as the protocol
- ECDSA P-521 with SHA-512 in digital signatures in connections between the SMC and the Security Engines.

Note

ECDSA P-384 with SHA-384 when using ECDSA P-384 certificates issued by an external CA.

- P-521 NIST curve in TLS key establishment in connections between the SMC and the Security Engines.

  Note

  P-384 NIST curves when using ECDSA P-384 certificates issued by an external CA.

- P-256, P-384, and P-521 NIST curves, in TLS key establishment, with SHA-256, SHA-384, or SHA-512 in digital signatures, in Web Access and in connections to external servers.

The Management Server and Log Server only accepts the TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 cipher suites when acting as TLS server for connections from Security Engines.

Use the main network interface for management for the connection to the Security Engine, and for the connection to the SMC Client and external syslog server.

Steps

1) After SMC Appliance reboots following the installation, please proceed by accepting the End User License Agreement (EULA).

2) Select **Begin**, then press **Enter**.

3) Select the keyboard layout for accessing the SMC Appliance on the command line.

4) Enter the administrator account name and password.

   Note

   The administrator account and password are used for command line access to the SMC Appliance and for access to the SMC Client. The administrator account is created with unrestricted permissions (superuser).

   a) Enter the account name.

   This field is case sensitive and limited to eight characters.

   b) Enter the password.

   The password is case sensitive. The password must be at least ten characters long and contain at least one number.

   c) Enter the password again.

5) (Optional) Configure a bootloader password.

   If you configure a bootloader password, you must enter the bootloader password to edit the options that appear in the bootloader menu of the SMC Appliance.

   a) Press the space bar to configure a bootloader password.

   b) Enter the password.

   c) Enter the password again.

6) Make your security selections.

a) Select FIPS mode.

b) Select 256-bit encryption as the security strength.

c) (Optional) Select Use External Certificate Authority.

Note

- When you install the SMC, you can use certificates issued by an external CA for internal TLS communication between system components.
- You must complete the following actions after installation before you can start using the SMC:
  - Import the external CA certificate.
  - Generate and export certificate requests.
  - Sign the certificates using the external CA.
  - Import the signed certificates.

  Note

  Only the ECDSA public key algorithm is supported.

7) To enable network interface configuration, select **Disabled**, then press **Enter**.

8) Complete the network interface configuration for the primary network interface for management.

a) Select **Enable interface**.

b) Select **Primary**.

c) Complete the network configuration fields for the interface.

9) (Optional) Complete the network interface configuration for the secondary network interface for management.

a) Select **Enable interface**.

b) Select **Secondary**.

c) Complete the network configuration fields for the interface.

10) Enter a host name for the Management Server.

11) (Optional) Enter one or more IPv4 or IPv6 addresses in the DNS server fields.

Note

When using an external CA, it is necessary to configure at least one DNS server.

12) (Optional) If you do not want to use NTP, disable it in the NTP settings.

Note

We recommend that you configure an NTP server when using an external CA so that the time settings for the SMC are accurate when checking validity times for certificates, CRLs, and OSCP server responses.

13) Select the time zone.

14) Set the date and time.
You are prompted to review the configuration.

15) Select **Confirm**, then press **Enter**.

Result

When the installation is complete, select one of the following options:

- Reboot
- Shutdown.

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 for the software cryptographic modules.

Integrity check verifies the ECDSA signature of a catalog file of the SHA-256 hashes of all binaries.

Noise source health tests include a Repetition Count Test and an Adaptive Proportion Test as specified by NIST SP 800-90B.

SMC FIPS Java API self-tests

Algorithm	Type	Test Method
HMAC-SHA2-256	Software Integrity	Message Authentication
AES-ECB Encryption	CAST	KAT
AES-ECB Decryption	CAST	KAT
AES-CCM Encryption	CAST	KAT
AES-CCM Decryption	CAST	KAT
AES-CMAC Generation	CAST	KAT
AES-CMAC Verification	CAST	KAT
KAS-ECC Primitive “Z” Computation	CAST	KAT
KAS-FFC Primitive “Z” Computation	CAST	KAT
HASH_DRBG SHA2-256	CAST	KAT

Algorithm	Type	Test Method
HMAC-DRBG HMAC-SHA2-256	CAST	KAT
CTR_DRBG AES-CTR 256 bits	CAST	KAT
DSA Signature Generation	CAST	KAT
DSA Signature Verification	CAST	KAT
ECDSA Signature Generation	CAST	KAT
ECSDA Signature Verification	CAST	KAT
AES-GCM Encrypt	CAST	KAT
AES-GCM Decrypt	CAST	KAT
HMAC-SHA2-256	CAST	KAT
HMAC-SHA2-512	CAST	KAT
HMAC-SHA3-256	CAST	KAT
KDA OneStep	CAST	KAT
KDA TwoStep	CAST	KAT
KBKDF	CAST	KAT
PBKDF	CAST	KAT
SHA-3	CAST	KAT
RSA Signature Generation	CAST	KAT
RSA Signature Verification	CAST	KAT
RSA Encryption	CAST	KAT
RSA Decryption	CAST	KAT
SHA-1	CAST	KAT
SHA2-256	CAST	KAT
SHA2-512	CAST	KAT
SHAKE256	CAST	KAT
ANS 9.63 KDF	CAST	KAT
IKEv2 KDF	CAST	KAT
SNMP KDF	CAST	KAT
SRTP KDF	CAST	KAT
SSH KDF	CAST	KAT
TLS 1.0 KDF	CAST	KAT
TLS 1.1 KDF	CAST	KAT
TLS 1.2 KDF	CAST	KAT
HMAC	CAST	KAT

Algorithm	Type	Test Method
SHS	CAST	KAT
DH	Pair-Wise Consistency Test	PCT
DSA	Pair-Wise Consistency Test	PCT
EC DH	Pair-Wise Consistency Test	PCT
ECDSA	Pair-Wise Consistency Test	PCT
RSA	Pair-Wise Consistency Test	PCT

SMC FIPS Library self-tests

Algorithm	Type	Test Method
HMAC-SHA2-256	Software integrity	Message Authentication
SHA2-512	CAST	KAT
SHA3-256	CAST	KAT
AES-ECB	CAST	KAT
AES-GCM	CAST	KAT
KBKDF	CAST	KAT
KDA OneStep	CAST	KAT
HKDF	CAST	KAT
ANS X9.42 KDF (CVL)	CAST	KAT
ANS X9.63 KDF (CVL)	CAST	KAT
SSH KDF (CVL)	CAST	KAT
TLS 1.2 KDF (CVL)	CAST	KAT
TLS 1.3 KDF (CVL)	CAST	KAT
PBKDF2	CAST	KAT
CTR_DRBG	CAST	KAT
Hash_DRBG	CAST	KAT
HMAC_DRBG	CAST	KAT
KAS-FFC-SSC	CAST	KAT
KAS-ECC-SSC	CAST	KAT
RSA	CAST	KAT
ECDSA	CAST	KAT
ECDSA	Pair-Wise Consistency Test	PCT
RSA	Pair-Wise Consistency Test	PCT
Safe Primes	Pair-Wise Consistency Test	PCT

SMC FIPS Cryptographic Module for NTP self-tests

Algorithm	Type	Test Method
HMAC-SHA-256	Software integrity	Message Authentication

Algorithm	Type	Test Method
SHA-1	CAST	KAT
SHA-224	CAST	KAT
SHA-256	CAST	KAT
SHA-384	CAST	KAT
SHA-512	CAST	KAT
AES-ECB	CAST	KAT
AES-CBC	CAST	KAT
AES-GCM	CAST	KAT
AES-CMAC	CAST	KAT
HMAC SHA-224	CAST	KAT
HMAC SHA-256	CAST	KAT
HMAC SHA-384	CAST	KAT
HMAC SHA-512	CAST	KAT
KBKDF	CAST	KAT
HKDF	CAST	KAT
TLS 1.0/1.1 KDF	CAST	KAT
TLS 1.2 KDF	CAST	KAT
IKEv2 PRF	CAST	KAT
PBKDF2	CAST	KAT
Hash_DRBG	CAST	KAT
KAS-FFC-SSC	CAST	KAT
KAS-ECC-SSC	CAST	KAT
RSA	CAST	KAT
DSA	CAST	KAT
ECDSA	CAST	KAT
Safe Primes	Conditional Pairwise Consistency Self-Test	PCT
ECDH	Conditional Pairwise Consistency Self-Test	PCT
RSA	Conditional Pairwise Consistency Self-Test	PCT
ECDSA	Conditional Pairwise Consistency Self-Test	PCT

Check the self-test results in the console. The self-test messages are also sent to the SMC Appliance syslog.

- If the SMC FIPS Java API cryptographic module self-test fails, the server application fails to start, and an error message is shown on the console and the appliance halts its execution automatically.

```
fipssmc: ERROR: FIPS SMC Bouncy Castle
fipssmc: FIPS System Shutdown
```

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

```
fipstest:Performing FIPS NSS crypto selftests...
Fatal FIPS Error: fipstest:ERROR:FIPS NSS crypto selftest failed: /lib/fips/fipstest-ossl: 255
```

```
fipstest: Performing FIPS OpenSSL crypto selftests…
Fatal FIPS Error: fipstest:ERROR:FIPS OpenSSL crypto selftest failed: /lib/fips/fipstest-ossl: 1
```

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

```
fipscheck: Performing FIPS integrity check…
Fatal FIPS Error: fipscheck:ERROR:FIPS integrity check failed. /usr/bin/smca-fipscheck: 255
```

- If a noise source health test fails, an error message is shown on the console and the appliance halts and is not remotely accessible.

```
fipsrngdtest: Performing FIPS rngd self test...
Fatal FIPS Error: fipsrngdtest:ERROR:FIPS rngd self test failed: 1
```

If a self-test fails, see the *Reset the SMC Appliance to factory settings* topic.

Next steps

- If the self-tests succeed, continue configuring the SMC Appliance.
- If a self-test fails, restart the SMC Appliance manually. It does not restart automatically.
- If a self-test continues to fail, reset the SMC Appliance to factory settings. For more details, refer to the *Reset the SMC Appliance to factory settings* topic.

Related tasks
Install the SMC Client on page 16

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) Access the virtual SMC Appliance using the virtual machine console in the VMware Host Client.
2) Reboot the SMC Appliance, then at the boot menu, select **VCDROM**.
3) Select **Manual Installation** and **Begin**.
4) Select **Fresh Install**, then press **Enter**.
5) (Optional) Highlight **Securely wipe drive**, then press the space bar.
6) Select **Next**, then press **Enter**.
   You are prompted to review the configuration.

7) Select **Confirm**, then press **Enter**.

8) Install the SMC Appliance in FIPS 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 SMC Client when you install them.

For detailed installation instructions and information about hardware requirements for third-party hardware, see the *Forcepoint Network Security Platform Installation Guide* and the *Forcepoint Network Security Platform Release Notes*.

CAUTION

In Linux, cryptographic modules use /dev/random as the source of randomness. Using /dev/random as the source of randomness can 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 Security 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 SMC Client.
Enable FIPS restrictions during the installation.

4) Start the SMC 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 SMC 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`. The default installation directory in Linux is `/usr/local/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 server's IP address from the drop-down list. If you use IP address binding, the server's license must be generated with this IP address as the binding.
Log Server IP Address	Enter the IP address of the Log Server to which this server sends its log data.
Advanced Management Server Options	When selected, you can configure additional options on another page. Select this option if you want to: ■ Disable the use of 256-bit encryption for communication between the Management Server and the Security Engines. ■ Disable the use of Web Access to run the SMC Client in a web browser.
Install as an Additional Management Server for High Availability	When selected, you can configure additional options on another page.
Enable FIPS Configuration Restrictions	You must enable this option to use the SMC in FIPS mode.
Use External Certificate Authority	Select when you need to use certificates issued by an external CA for internal TLS communication between system components.
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 Access	When enabled, administrators can access the SMC in a web browser. You can run the SMC Client in a web browser instead of installing the SMC Client locally. On Linux platforms, xvfb-run must be installed under `/usr/bin`. You can specify another path in the Management Server properties after the installation has completed. This option is selected by default.
Enable OWASP encoding	When enabled, the SMC API uses the OWASP encoder in responses. Using the OWASP encoder reduces the risk of cross site scripting (XSS) attacks when you use the SMC API in a web browser. **Note** When you enable this option, some strings in data returned by the SMC API, such as special characters inside JSON payloads, are also encoded. We recommend enabling this option only if you use the SMC API in a web browser.
256-bit Security Strength	When enabled, 256-bit encryption is used for communication between the Management Server and the Security Engines. This option is selected by default.

3) If you enabled 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 Web Access is enabled on the Management Server and port 8083 when enabled on the Web Access 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 SMC Client. Enter the distinguished name in LDAP string format for the certificate used to secure the HTTPS connection. Example: `dn=smc,dc=demo,dc=com`
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.

4) 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 you use IP address binding, 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 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.

   When the installation has completed, the unique installation identifier (UIID) for the SMC is shown. If you plan to use UIID-bound licenses for SMC servers, make a note of the UIID for the SMC. You will need the UIID to generate licenses.

2) When the installation has completed, click **Done**.

Note

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

Install the SMC Client

Optionally you can install a stand-alone SMC Client application in FIPS mode on a Windows or Linux workstation.

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

As an alternative to installing the SMC Client, you can use Web Access. You can enable these features when installing the Management Server, or you can enable them later. By default, the SMC Web Access is enabled.

When logging on to the SMC Client, the fingerprint of the Management Server certificate is verified.

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 SMC 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`. The default installation directory in Linux is `/usr/local/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 **SMC Client Only** as the installation type, then click **Next**.

10) When prompted to select the cryptographic algorithms, select **Restricted Cryptographic Algorithms Compatible with FIPS**.

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 SMC Client

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

Steps

1) If you installed the SMC 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 Web Access to run the SMC Client in a web browser, do the following:

   a) In a web browser, browse to the URL of the Management Server or SMC Appliance.

   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. The default port for Web Access is 8085.

   For example, if the SMC Appliance is configured with the IP address 192.0.2.1, the SMC Client can be accessed using the URL `https://192.0.2.1:8085/` in a web browser.

b) Enter your user name and password, then click **Log On**.

Configure administrative settings in the SMC

After you start the SMC Client, review the administrative settings in the SMC. These settings are located in the global system properties, Management Server properties, and Log Server properties. Select the values according to the security policy of your organization.

Steps

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

1) Configure the password policy in the global system properties.

   a) In the SMC Client, select **Settings** > **Global System Properties**.

   b) Click the **Password Policy** tab.

   c) Select **Enforce Password Settings for All the Administrators and Web Portal Users**.

   d) In the **Logon Options** section, review the following settings:

   - **Temporarily Lock Account After Failed Logon Attempts** — Select the option, then define the maximum number of failed logon attempts and the length of time to lock the account.
   - **Lock the Management Client Window After the User Session is Idle for** — Select the option, then define the length of idle time. To close the SMC Client when the window is locked, select Close the SMC Client.

   e) In the **Password Complexity Requirements** section, review the following settings:

   - **Minimum Number of Characters in Password** — Define the minimum password length.
   - **Minimum Number of Required Characters** — Define the minimum number of uppercase letters, lowercase letters, special characters, and numbers. The total number of required characters must not be larger than the minimum password length.

   f) Click **OK**.

2) Configure the audit storage setting for the Management Server.

   a) Select **Network Elements**, then browse to **Servers**.

   b) Right-click the Management Server, then select **Properties**.

   c) On the **General** tab, review the **Audit Storage Full** setting, then select the action that the Management Server takes when the audit storage is full:
      - **Stop Management Server** — The Management Server writes an audit entry, stops all processes, and shuts down. This is the default.
      - **Overwrite Oldest Audit Entries** — The Management Server overwrites audit entries, starting with the oldest entries.

   d) Click **OK**.

3) Configure the log storage setting for the Log Server.

   a) Select **Network Elements**, then browse to **Servers**.

   b) Right-click the Log Server, then select **Properties**.

   c) On the **General** tab, review the **Log Storage Full** setting, then select the action that the Log Server takes when the log storage is full:
      - **Stop Receiving** — The Log Server stops receiving log entries. This is the default.
      - **Overwrite Oldest** — The Log Server overwrites log entries, starting with the oldest entries.

   d) Click **OK**.

   For more information about these settings, see the *Enable and define password policy settings* and the *Overwrite old log or audit entries when log storage is full* topics in the *Forcepoint Network Security Platform Product Guide*.

Installing the Security Engine in FIPS mode

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

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

You must complete the following main steps:

1) Create an element for the Security Engine in the SMC Client.

2) Enable FIPS mode in the properties of the Security Engine element.

3) Create a policy for the Security Engine.

4) Install the Security Engine in FIPS mode.

5) Check the results of the self-tests on the Forcepoint Network Security Platform appliance.

6) Install the policy on the Security Engine.

Create an element for the Security Engine

Use the SMC Client to create the Security Engine element.

These steps are the high-level tasks. For more information, see the *Forcepoint Network Security Platform Product Guide*.

Steps

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

1) In the SMC Client, create a Security Engine, then define the properties in the Engine Editor.

   Follow the normal process to define the properties of a Security 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) Review the settings for Automatic rules on the **Policies** > **Automatic Rules** branch. Select the values according to the security policy of your organization, including the **Log Level for Automatic Rules**.

3) Save the initial configuration.

Note

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

Create a Security Engine policy

You must create a policy for the Security Engine and install the policy on the Security Engine after you have installed it. Each policy is based on a template policy. Use one of the following template policies:

- The default **Firewall Template** or **Firewall Inspection Template policy**.
- A customized template policy, if necessary. Rules inherited from the default template policies cannot be edited directly, so create a copy of a default template policy and customize the copy.

In addition to the rules in the template policy, the default template policies use Automatic rules. Automatic rules are created for the necessary traffic to and from theSecurity Engine, including the management communications between the SMC and the Security Engine. Automatic rules are created only if the installed policy contains the Automatic Rules Insert Point. The default template policies contain the insert point. If you use a customized template policy, include the Automatic Rules Insert Point to use Automatic rules.

Automatic rules are not shown in the rule tables of the policy. You can view a summary of the Automatic rules and change their settings in the Engine Editor.

Steps

1) Select the template policy for the Security Engine policy.

   a) To use a default template policy, select the **Firewall Template** or the **Firewall Inspection Template** policy.

   b) If necessary, create a customized template policy. Open a default template policy for editing, save it as a new template policy, then add the rules that you need. To use Automatic rules, include the Automatic Rules Insert Point in the customized template policy.

2) In the SMC Client, create a policy for the Security Engine that uses the template policy.

3) Add the Access rules that are required according to the security policy of your organization, then save the policy.

   For more information, see the *Automatic rules and how they work*, the *Configure settings for Automatic rules*, and the *Creating and managing policy elements* topics in the *Forcepoint Network Security Platform Product Guide*.

Install the Security Engine in FIPS mode

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

The Security Engine uses TLS 1.2 and the TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 cipher suite for management connections with the SMC.

Note

If the Security Engine is installed as a Virtual Machine in ESXi, the same ESXi entropy configuration caveats apply as in the *Enable FIPS mode on the SMC Appliance* topic.

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

Note

Forcepoint Network Security Platform appliances come with Security Engine software pre-installed. Before setting the Security Engine to use FIPS mode, upgrade the Security Engine software to the version that you want to use.

Steps

1) Download the Security Engine software from https://support.forcepoint.com/s/download, then validate the checksums.

   Note

   Save the Security 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 Network Security Platform Installation Guide*.

2) Upgrade the Security Engine software to the version that you want to use.

   a) In the Security Engine Configuration Wizard, select **Upgrade**.

   b) In the **Select Source Media** dialog box, select the appropriate media type, then click **OK**.
   The software update signature is verified.

   c) Click **OK**.
   The upgrade starts.

   d) Select **Set kernel in FIPS mode after reboot**.

   e) Click **OK**.

   Forcepoint Network Security Platform appliance restarts and displays the upgraded version.

3) Configure the Security Engine with the Security Engine Configuration Wizard.
   Follow the normal process to define the Security Engine properties, with these exceptions:

   - Select **Restricted FIPS-Compatible Operating Mode**.
     This option enables the FIPS 140-3 cryptographic module.
   - Ensure that the **256-bit security strength** is selected in the Management Server configuration settings.

   Note

   This option is selected by default.

4) To verify FIPS-Approved mode of operation, verify that the following messages are shown on the console when the Forcepoint Network Security Platform appliance restarts:

   ```
   FIPS: rootfs integrity check OK
   ```

   This message confirms that the module's integrity test has been executed successfully. The integrity test verifies an ECDSA P-521 signature with SHA-512 over the root file system. If the integrity test fails, an error message is displayed and the module restarts.

   ```
   FIPS power-up tests succeeded
   ```

   This message confirms that the FIPS power-up self-tests have been executed successfully. If the power-up tests fail, a power-up test error message is shown and the module restarts.

   If the connection with the Management Server is not established successfully, verify the following:

   - The one-time generated password is correct.
   - The Management Server IP address is correct.
   - The certificate fingerprint is correct.
   - The 256-bit encryption is used for the connection to the Management Server.

Check the Security Engine self-tests

The Security Engine contains the Forcepoint Network Security Platform FIPS Library, Forcepoint Network Security Platform FIPS Cryptographic Module, and Forcepoint Network Security Platform Cryptographic Kernel Module. The modules run several self-tests when the Forcepoint Network Security Platform appliance starts.

The modules perform these tests:

- Cryptographic Algorithm Self-Tests (CAST) implemented as Known Answer Tests (KAT) and Pairwise Consistency Tests (PCT)
- Forcepoint Network Security Platform FIPS Library self-tests
- Forcepoint Network Security Platform FIPS Cryptographic Module self-tests
- Forcepoint Network Security Platform Cryptographic Kernel Module self-tests
- Noise source health tests include a Repetition Count Test and an Adaptive Proportion Test as specified by NIST SP 800-90B.
- The file system integrity check verifies the ECDSA signature over the root file system.

Forcepoint Network Security Platform FIPS Library self-tests

Algorithm	Type	Test Method
HMAC-SHA2- 256	SW/FW Integrity	Message Authentication
AES-ECB	CAST	KAT
AES-GCM Encrypt	CAST	KAT
AES-GCM Decrypt	CAST	KAT
Counter DRBG	CAST	KAT
DSA SigGen (FIPS186-4)	CAST	KAT
DSA SigVer (FIPS186-4)	CAST	KAT
ECDSA SigGen (FIPS186-4) with curve P-224	CAST	KAT
ECDSA SigVer (FIPS186-4) with curve P-224	CAST	KAT
Hash DRBG	CAST	KAT
HMAC DRBG	CAST	KAT
HMAC-SHA2-256	CAST	KAT
KAS-ECC-SSC Sp800-56Ar3	CAST	KAT
KAS-FFC-SSC Sp800-56Ar3	CAST	KAT
KAS-IFC-SSC	CAST	KAT
KDF SP800-108	CAST	KAT
KDA OneStep SP800-56Cr2	CAST	KAT
KDA TwoStep SP800-56Cr2	CAST	KAT
KTS-IFC Encrypt	CAST	KAT
KTS-IFC Decrypt	CAST	KAT
PBKDF	CAST	KAT

Algorithm	Type	Test Method
RSA SigGen (FIPS186-4)	CAST	KAT
RSA SigVer (FIPS186-4)	CAST	KAT
SHA-1	CAST	KAT
SHA2-512	CAST	KAT
SHA3-256	CAST	KAT
KDF ANS 9.42	CAST	KAT
KDF ANS 9.63	CAST	KAT
KDF SSH	CAST	KAT
TLS v1.2 KDF RFC7627	CAST	KAT
TLS v1.3 KDF	CAST	KAT
RSA KeyGen (FIPS186-4)	Pair-Wise Consistency Test	PCT
ECDSA KeyGen (FIPS186-4)	Pair-Wise Consistency Test	PCT
DSA KeyGen (FIPS186-4)	Pair-Wise Consistency Test	PCT
ECDSA SigGen (FIPS186-4) with curve K-233	CAST	KAT
ECDSA SigVer (FIPS186-4) with curve K-233	CAST	KAT

Forcepoint Network Security Platform FIPS Cryptographic Module self-tests

Algorithm	Type	Test Method
ECDSA signature verify with NIST P-224 and SHA2-224	Software Integrity	
SHA-1	CAST	KAT
SHA2-512	CAST	KAT
SHA3-224	CAST	KAT
HMAC-SHA2-256	CAST	KAT
AES-CBC encryption (128-bit key)	CAST	KAT
AES-CBC decryption (128-bit key)	CAST	KAT
AES-CCM encryption (128-bit key)	CAST	KAT
AES-CCM decryption (128-bit key)	CAST	KAT
AES-GCM encryption (128-bit key)	CAST	KAT
AES-GCM decryption (128-bit key)	CAST	KAT
AES-XTS encryption (128-bit key strength)	CAST	KAT

Algorithm	Type	Test Method
AES-XTS decryption (128-bit key strength)	CAST	KAT
AES-CMAC (192-bit key)	CAST	KAT
TDES-CBC encryption (192-bit key)	CAST	KAT
TDES-CBC decryption (192-bit key)	CAST	KAT
Counter DRBG AES-256 (instantiate, generate and reseed; includes AES-ECB mode encryption)	CAST	KAT
RSA SigGen 2048-bit with SHA2-256	CAST	KAT
RSA SigVer 2048-bit with SHA2-256	CAST	KAT
DSA SigGen (P=2048/N=256 with SHA2-224)	CAST	KAT
DSA SigVer (P=1024/N=160 with SHA2-224)	CAST	KAT
ECDSA SigGen (NIST P-224 with SHA2-224)	CAST	KAT
ECDSA SigVer (NIST P-224 with SHA2-224)	CAST	KAT
KTS-IFC Key Encapsulation 2048-bit (RSA-OAEP)	CAST	KAT
KTS-IFC Key Un-encapsulation 2048-bit (RSA-OAEP)	CAST	KAT
KAS-FFC-SSC (P=2048/N=224)	CAST	KAT
KAS-ECC-SSC (NIST P-224)	CAST	KAT
KDF SP800-108 (Counter Mode)	CAST	KAT
KDA HKDF (includes KDF SP800-108 Feedback Mode)	CAST	KAT
KDF SP800-108 (Double Pipeline Mode)	CAST	KAT
KDF IKEv1	CAST	KAT
KDF IKEv2	CAST	KAT
TLS v1.2 KDF RFC7627	CAST	KAT
SP 800-90A-r1, (Instantiate/ Generate) health tests for Counter DRBG AES-256	CAST	KAT

Algorithm	Type	Test Method
SP 800-90A-r1, (Reseed) health test Counter DRBG AES-256	CAST	KAT
SP 800-90B, start-up and continuous health tests (RCT and APT) for JitterEntropy ENT (NP)	CAST	Fault Detection Tests

Forcepoint Network Security Platform Cryptographic Kernel Module self-tests

Algorithm	Type	Test Method
HMAC-SHA2-256	Software Integrity	Message Authentication
AES encryption (AES-CBC, AES-CFB128, AES-ECB, AES-OFB 128, 192, 256)	CAST	KAT
AES decryption (AES-CBC, AES-CFB128, AES-ECB, AES-OFB 128, 192, 256)	CAST	KAT
AES-GCM 128 authenticated encryption	CAST	KAT
AES-GCM 128 authenticated decryption	CAST	KAT
SHA (SHA-1, SHA2-256, SHA2- 512)	CAST	KAT
HMAC (HMAC-SHA-1, HMACSHA2-256, HMAC-SHA2- 512)	CAST	KAT

Check the self-test results in the console.

- If a cryptographic self-test or a noise source health test fails, an error message is shown on the console and the appliance is restarted automatically. Noise source health tests are automatically executed as part of the self-tests when Forcepoint Network Security Platform FIPS Library and Forcepoint Network Security Platform FIPS Cryptographic Module are loaded.

```
FIPS: OpenSSL self-tests FAILED, rebooting…
Cryptographic Kernel Module self tests failed
FIPS: Cryptographic module self-tests FAILED, rebooting...
```

```
FIPS: rootfs integrity check FAILED, rebooting…
```

Next steps

- If the self-tests succeed, continue configuring the Security Engine.
- If the problem persists, reset the Security Engine to factory settings.
  To reset the Security Engine, do the following:

  1) Power off the Security Engine.

  2) Power on the Security Engine, and select the **System restore options** option from the local console **boot** menu.

3) Follow the instructions to reset the Security Engine.

Reset the Forcepoint Network Security Platform 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 Forcepoint Network Security Platform appliance, you can also reset the appliance to factory settings from the SMC Client. For more information, see the *Forcepoint Network Security Platform Product Guide*.

Steps

1) Restart the Forcepoint Network Security Platform 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 Security Engine in FIPS mode.

© 2026 Forcepoint
Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint.
All other trademarks used in this document are the property of their respective owners.
Published 28 October 2026