Configuration Guide
Revision A

McAfee® Firewall Enterprise Control Center 5.3.2

FIPS 140-2

Contents

Enabling FIPS on Control Center

Enabling FIPS on managed firewalls through Control Center

1 Introduction to FIPS 140-2

The Federal Information Processing Standard (FIPS) 140-2 is a U.S. government computer security standard used to accredit cryptographic modules.

Contents

About FIPS 140-2

The Cryptographic Module Validation Program (CMVP) validates cryptographic modules to Federal Information Processing Standard (FIPS) 140-2 and other cryptography-based standards.

The CMVP is a joint effort between the U.S. National Institute of Standards and Technology (NIST) and the Communications Security Establishment Canada (CSEC). Validated products that conform to FIPS 140-2 are accepted by the federal agencies of both countries for the protection of sensitive information (United States) or Designated Information (Canada). The goal of the CMVP is to promote using validated cryptographic modules and provide federal agencies with a security metric to use in procuring equipment containing validated cryptographic modules.

Control Center is validated as a cryptographic module at the platform level and provides FIPS 140-2-compliant cryptographic services. These services include:

- Symmetric key encryption and decryption
- Public key cryptography
- Hashing
- Random number generation

FIPS 140-2 and Control Center

The FIPS 140-2 standard provides various increasing levels of security.

- Virtual appliances are certified to FIPS 140-2 Level 1.
- Hardware appliances (with the addition of a FIPS 140-2 Level 2 kit) are certified to FIPS 140-2 Level 2.

A FIPS 140-2-compliant Control Center can manage both FIPS-compliant and non-compliant firewalls.

Enabling FIPS on Control Center

This section enables you to make Control Center FIPS compliant.

2 Configuring Control Center for FIPS 140-2 compliance

FIPS 140-2 validated mode (hereinafter FIPS mode) is a separate operational state for Control Center. Configuration changes are necessary to put your Control Center in FIPS mode and make it compliant with FIPS 140-2 requirements.

Contents

Make sure your model is supported

Make sure your Control Center model supports FIPS compliance.

Task

1. Go to www.mcafee.com/us/support/support-eol-appliances.aspx.
2. Click **Firewall**.
3. Search for your model.
4. Check the **Hardware End of Life** column. If the date has not yet passed, or if there is no date listed, your model is supported.

Download documentation

Download the documents you will need to complete your FIPS 140-2-compliant setup.

Task

1. Go to support.mcafee.com.
2. Click **Product Documentation**.

3 Download the following documents:

- *McAfee Firewall Enterprise Control Center Quick Start Guide*, version 5.3.2
- *McAfee Firewall Enterprise Control Center Product Guide*, version 5.3.2
- [Physical and Virtual appliances]*McAfee Firewall Enterprise Control Center Installation and Migration Guide*, version 5.3.2
- [FIPS 140-2 Level 2 only]*McAfee Firewall Enterprise Control Center FIPS 140-2 Level 2 Kit Installation Guide*

Install Control Center software

Install the Control Center to the correct version and patch level.

Install version 5.3.2 of the Control Center Management Server and Client application. See the *McAfee Firewall Enterprise Control Center Product Guide*, version 5.3.2 or the *McAfee Firewall Enterprise Control Center Installation and Migration Guide*, version 5.3.2 for installation or re-imaging instructions.

Task

1 Install the Control Center Management Server from the installation CD or the installation USB drive, or as a new VMware image.

2 Upgrade to 532P06 patch. You can download the patch from http://www.mcafee.com/us/downloads/downloads.aspx.

Additional software updates are not certified for FIPS 140-2.

If you are a 5.2.x user, migrate to 5.3.0 and upgrade to 5.3.1, and then upgrade to 5.3.2 Patch 02. Use the README.txt file to install 5.3.2 Patch 06 and enable FIPS as detailed in this guide.

3 Configure the appliance manually. Do not use the Control Center Initialization Tool to configure the Control Center.

Do not configure the Remote Management Module (RMM3) on a FIPS 140-2-compliant Control Center.

If ePolicy Orchestrator is configured before moving to FIPS mode, you have to regenerate the ePO certificate after Control Center Management Server is on FIPS mode. This makes sure that Control Center and McAfee ePO communicate seamlessly.

Configuring appliance BIOS settings

For information on the hardware and BIOS modifications required for FIPS 140-2 Level 2 compliance, see the FIPS 140-2 Level 2 Kit installation guide for your hardware model.

Enable FIPS 140-2 processing

Enable FIPS 140-2 processing on your Control Center.

When FIPS 140-2 processing is enabled, the system uses FIPS 140-2-approved cryptographic modules and key lengths, and runs FIPS 140-2 self-tests. Users can still log on using all the operating system-level user accounts.

Task

1 Start the Control Center Client application and log on to the Control Center Management Server.

2 Select **Control Center** | **Settings** | **FIPS**. The FIPS window appears.

3 Select **Require FIPS 140-2 processing**, then click **OK**. A message appears with information that the Control Center will restart.

4 Click **OK**. The Control Center Management Server restarts with FIPS 140-2 processing enabled.

When you log on to the Control Center Management Server again, *FIPS 140-2 processing enabled* appears on the Client application title bar.

Place the Control Center in FIPS mode

Replace existing certificates and lock OS accounts to put the Control Center in FIPS mode.

In FIPS mode, *administrator* user can define their user account name and log on to the Control Center Management Server at the console or through SSH. Operating system commands requiring the root account (such as certain Linux networking commands) are not available in FIPS mode.

Tasks

- *Replace certificates and SSH server keys* on page 11
- *Lock operating system-level accounts* on page 12

Replace certificates and SSH server keys

Critical security parameters cannot be shared between non-FIPS and FIPS mode. Existing critical security parameters need to be deleted before entering FIPS mode. Deleted critical security parameters are created when the system restarts in FIPS mode.

The following certificates are recreated with a FIPS 140-2-approved key length (2048 bits) and a FIPS 140-2-approved algorithm (SHA-2 with RSA digital signature):

- Built-in CA certificate
- Tomcat TLS certificate
- UTT Server TLS certificate
- PostgreSQL TLS certificate
- Apache TLS certificate

In addition, the Tomcat TLS certificate is recreated with an X.509v3 Key Usage extension. SSH server keys are re-created with FIPS 140-2-approved key lengths.

Delete critical security parameters, certificates, and SSH server keys before entering FIPS mode.

Task

1 On the command line, log on to the Management Console as an *administrator* user.

2 Type the following command, then press **Enter**:

```
su root
```

3 Type the following command, then press **Enter**:

```
/usr/local/bin/fips_rmcerts
```

This command performs the following commands.

```
rm -rf /usr/local/tomcat/JavaCA
rm -rf /usr/local/tomcat/ssl
rm /usr/local/common/dcserver/conf/uttserver.req
rm /usr/local/common/dcserver/conf/uttserver.key
rm /usr/local/common/dcserver/conf/uttserver.crt
rm /usr/local/common/dcserver/conf/cacert.pem
rm /etc/httpd/conf/tomcat.cer
rm /etc/httpd/conf/tomcat.key
rm /etc/httpd/conf/cacert.pem
rm /var/lib/pgsql/data/server.crt
rm /var/lib/pgsql/data/server.req
rm /var/lib/pgsql/data/server.key
rm /etc/ssh/ssh_host_dsa_key
rm /etc/ssh/ssh_host_dsa_key.pub
rm /etc/ssh/ssh_host_rsa_key
rm /etc/ssh/ssh_host_rsa_key.pub
```

The system generates the certificates and keys in FIPS mode.

Critical security parameters, certificates, and SSH server keys are deleted. New certificates and keys are generated in FIPS mode.

Lock operating system-level accounts

Make sure only the administrator operating system-level account has access to the command line interface when the system is in FIPS mode. Make sure the system is running in the release kernel.

Task

1 On the command line, log on to the Management Console as an administrator user.

2 Type the following command, then press **Enter**:

```
su root
```

3 Type the following command, then press **Enter**

```
/usr/local/bin/fips_lock_accounts
```

4 Exit from the root shell. Type `exit`, then press **Enter**.

5 As an administrator user, type the following command and press **Enter**.

```
sudo reboot
```

The Control Center Management Server restarts in FIPS mode.

Applying tamper-evident seals

Apply the tamper-evident seals to your Control Center appliance. Refer to the McAfee Firewall Enterprise Control Center FIPS 140-2 Level 2 Kit Installation Guide for your appliance.

Verify the Control Center is in FIPS mode

Examine server configuration and log files to make sure the Control Center Management Server is in FIPS mode.

Task

1 Start the Control Center Client application and log on to the Control Center Management Server.

2 Make sure *FIPS 140-2 processing enabled* appears on the Client application title bar.

3 Check the server logs.

a Select **Control Center** | **Logs** | **Server Logs**. The **Server Logs** window appears.

For option descriptions, press **F1**.

b Expand **Tomcat Web Server Logs (catalina)**. Make sure the log has a line containing *Completed FIPS 140 self checks successfully*.

c Expand the **Secure Alerts Server (dcserver_log)**. Make sure the log has a line containing *Completed FIPS 140 self checks successfully*.

d Click **Close**.

4 Check the cryptography logs.

a Select **Control Center | Logs | Crypto Logs**. The **Crypto Logs** window appears.

b Make sure there is an SSH Server entry that shows *** *IN FIPS MODE* ***.

c Make sure there is a FIPS Software Integrity entry that shows *STATUS:PASSED: FIPS hmac integrity check succeeded*.

d Make sure there is a HTTPD Server entry that shows *Operating in SSL FIPS mode*.

e Click **Close**.

5 Make sure operating system-level accounts are locked.

a Log on to the console as an administrator user.

b Type the following command, then press **Enter**:

```
su root
```

c Enter the root password. It should fail.

6 Check the configuration files. Make sure each of the following configuration files contains the content needed for FIPS mode:

- **java.security**

  1 Type the following command, then press **Enter**:

```
vi /usr/java/jre1.6.0_45/lib/security/java.security
```

2 Make sure the following lines are present and are not commented out:

```
com.rsa.cryptoj.jce.fips140initialmode=FIPS140_MODE
cc.fips140.mode=true
```

3 Close the file.

- **openssl.cnf**

1 Type the following command, then press **Enter**:

```
vi /etc/pki/tls/openssl.cnf
```

2 Make sure the following lines are present:

```
#FIPS configuration options
openssl_conf = openssl_options

[ openssl_options ]
alg_section = algs

[ algs ]
fips_mode = yes
```

3 Close the file.

- **JavaCA.cnf**

1 Type the following command, then press **Enter**:

```
vi /usr/local/tomcat/JavaCA/JavaCA.cnf
```

2 Make sure the following lines are present:

```
#FIPS configuration options
openssl_conf = openssl_options

[ openssl_options ]
alg_section = algs

[ algs ]
fips_mode = yes
#end FIPS configuration options
```

3 Close the file.

- **openssl.cnf**

1 Type the following command, then press **Enter**:

```
vi /usr/local/tomcat/JavaCA/openssl.cnf
```

2 Make sure the following lines are present:

```
#FIPS configuration options
openssl_conf = openssl_options

[ openssl_options ]
alg_section = algs

[ algs ]
fips_mode = yes
#end FIPS configuration options
```

3 Close the file.

- **fips140**
  1. Make sure the fips140 file exists. Type the following command, then press **Enter**:

     ```
     ls -l /etc/sysconfig/gcc/fips140
     ```

- **pgstartup.log**
  1. Type the following command, then press **Enter**:

     ```
     sudo vi /var/lib/pgsql/pgstartup.log
     ```

  2. Make sure the file contains the line *** *FIPS mode enabled* ***.
  3. Close the file.

- **uttlog**
  1. Type the following command, then press **Enter**:

     ```
     vi /usr/local/common/dcserver/logs/uttlog
     ```

  2. Make sure the file contains the line *FIPS mode—enabled*.
  3. Close the file.

- **ssl-conf**
  1. Type the following command, then press **Enter**:

     ```
     vi /etc/httpd/conf.d/ssl.conf
     ```

  2. Make sure the following lines are present.

     ```
     ## Begin FIPS
     SSLFIPS on
     ## End FIPS
     …
     SSLProtocol -all +TLSv1
     …
     SSLCipherSuite FIPS
     ```

  3. Close the file.

3 Using Control Center in FIPS mode

Perform common administrator tasks when Control Center is in FIPS mode.

When running Control Center High Availability in a FIPS 140-2 environment, both Control Center Management Server nodes must be configured for FIPS mode.

Contents

Reset database user passwords and operating system-level user passwords

Reset the passwords of the database user, operating system level user, and Control Center administrator passwords.

Task

1. On the command line, log on to the Management Console as an administrator user.
2. Type the following command, then press **Enter**:

   ```
   sudo /usr/local/bin/fips_reset_passwords
   ```

3. When prompted to proceed, type `yes`, then press **Enter**.
4. At the password prompt, carefully type the new values for the password.
5. As an administrator user, type this command and press **Enter**.

   ```
   passwd
   ```

6. At the password prompt, type the current password for the administrator. Carefully type the new values for the passwords.
7. As an administrator user, type this command and press **Enter**.

   ```
   sudo passwd < Firewall Audit Export Account >
   ```

8 At the password prompt, carefully type the new values for the password.

If any audit export or configuration backup objects in the Control Center Client use the < *Firewall Audit Export Account* >, update them with the new password.

9 As an administrator user, type the following command and press **Enter**.

```
sudo reboot
```

The Control Center Management Server restarts.

Reset the Control Center administrator password

Reset the password of the Control Center administrator.

Task

1 Start the Control Center Client application, and log on to the Control Center Management Server.

2 Select **Control Center** | **Administrators**. Select the administrator password. The **Control Center Administrator** window appears.

For option descriptions, press **F1**.

3 Enter and confirm the new password.

4 Click **OK**.

The administrator password is reset.

Enable Control Center backup encryption

Each time a you create a Control Center backup, perform these steps to enable backup encryption and provide a custom passphrase.

Task

1 Start the Control Center Client application, and log on to the Control Center Management Server.

2 Select **Control Center** | **Maintenance** | **Backup System**. The **Backup Control Center System** window appears.

3 Enter a name for the backup.

4 Select **Use the following custom passphrase**.

5 Enter the passphrase in the **Use the following custom passphrase** field.

6 Enter the same passphrase again in the **Confirm** field.

7 Click **Add** to initiate the backup.

The FIPS 140-2 configuration is complete.

Leaving FIPS mode

To take a Control Center out of FIPS mode, you must re-image the Control Center Management Server using the Control Center CD or installation USB drive.

For re-imaging instructions, see the *McAfee Firewall Enterprise Control Center Product Guide*.

Enabling FIPS on managed firewalls through Control Center

You can use Control Center to enable FIPS on managed firewalls. Firewalls deployed on Crossbeam and CloudShield platforms are managed by Control Center and this section helps you to enable FIPS on these firewalls.

4 Prepare managed firewalls for FIPS mode

Prepare managed firewalls for FIPS 140-2 validated mode (hereinafter FIPS mode) and use the Control Center to bring managed firewalls to the necessary software version.

Contents

Steps for FIPS 140-2 compliance

Software updates and configuration changes are necessary to put a managed firewall in FIPS mode and make it compliant with FIPS 140-2 Level 2 requirements. In order to make a managed firewall compliant with FIPS 140-2 Level 2 requirements, hardware modifications are also needed.

The high-level steps for FIPS 140-2 compliance are:

- Set up for FIPS mode
  - Download documentation
  - Make sure requirements are met
  - Upgrade the firewall to a FIPS 140-2-certified version
- [FIPS 140-2 Level 2 only] Prepare the appliance
- Enable FIPS 140-2 processing
- Verify FIPS 140-2 compliance
  - Replace certificates and keys
  - Verify use of allowed cryptographic services
  - Verify use of approved cryptographic algorithms and key lengths

- Verify SSH client and server configurations
- Restrict administrator access

Download documentation

Use this procedure to download the needed documentation.

1 Go to support.mcafee.com.

2 Click **Product Documentation**.

3 Download the following documents:

- *McAfee Firewall Enterprise Control Center Product Guide, version 5.3.2*
- *McAfee Firewall Enterprise Quick Start Guide, version 8.3.2*
- *McAfee Firewall Enterprise FIPS 140-2 Configuration Guide, version 8.3.2*
- *McAfee Firewall Enterprise Release Notes, version 8.3.2*

Make sure your requirements are met

Use this procedure to make sure the managed appliance meets the minimum requirements for FIPS 140-2 compliance.

1 Make sure the managed firewall model is supported.

2 If the managed firewall has not been configured yet, perform the initial configuration.

3 Make sure the managed firewall is registered to the Control Center and that all firewall objects have been retrieved.

4 If you are configuring the managed firewall for FIPS 140-2 Level 2 compliance, make sure you have the FIPS 140-2 Level 2 Kit.

Refer to the *McAfee Firewall Enterprise Product Guide, version 8.3.2* for more details.

Upgrade the firewall to a FIPS 140-2-compliant version

Upgrade a managed firewall to FIPS compliant version.

The FIPS 140-2-compliant versions include software features that add system integrity checking to software configurations and cryptography. Managed firewalls must be running version 8.x or 7.0.1.03 to be FIPS 140-2 compliant. A managed firewall must be upgraded to one of these two versions before FIPS 140-2 processing is enabled and the firewall configuration is updated.

Perform the appropriate procedure to bring your firewall to a FIPS 140-2-compliant version. Refer to the *McAfee Firewall Enterprise Release Notes* for upgrade instructions.

Prepare the appliance

For information on the hardware modifications required for FIPS 140-2 Level 2 compliance, see the *McAfee Firewall Enterprise FIPS 140-2 Level 2 Kit Installation Guide* for your hardware model.

5 Configure FIPS mode on managed firewalls

Use Control Center to enable and configure managed firewalls to comply with FIPS 140-2.

Contents

Enable FIPS 140-2 processing

Use this procedure to enable FIPS 140-2 processing on a managed firewall.

Task

1. From the Control Center Client application, select **Policy**.
2. From the **Policy** tree, double-click the firewall you want to enable FIPS 140-2 processing on. The Firewall window is displayed.
3. From the navigation tree, select **Settings** | **Other**. The **Other** tab of the Settings area is displayed.
4. Make sure the **Apply Global Settings** checkbox is deselected.
5. From **Other Settings** options, select the **Require FIPS 140 processing** checkbox.
6. Click **OK** to the save the configuration changes.
7. Click **Apply**. The configuration is pushed out to the managed firewall.
8. Restart the firewall.

The firewall restarts with FIPS 140-2 processing enabled.

Replace critical security parameters

Replace and verify critical security parameters to ensure FIPS 140-2 compliance.

You must replace critical security parameters (CSP): Firewall certificates and private keys for several services must be regenerated, and each administrator password must be changed.

To comply with FIPS 140-2 requirements, these certificates, keys, and passwords must be created after FIPS 140-2 processing is enabled.

The high level steps are:

1. Create the new parameter — certificate, key, or password.
2. Select the new parameter where needed.
3. Delete the old parameter.

The following table shows the service, the associated CSP, the required change, and the actions needed to make the change.

Table 5-1 Critical security parameter (CSP) replacement

Service	CSP	Action to take
• Admin Console (TLS) • Control Center (TLS) • SSL Content Inspection (TLS) • Firewall cluster management (TLS) • Audit log signing • IPsec/IKE certificate authentication • Passport authentication • Realtime Audit • McAfee® Firewall Reporter (Firewall Reporter) • McAfee® Firewall Profiler Communication • McAfee® Endpoint Intelligence Agent (McAfee EIA) (Endpoint Intelligence Agent) • Secure Alerts • SmartFilter Admin	Firewall certificate/ private key	1 Generate or import a new firewall certificate and private key. a From the Control Center Client application, select **Policy**. b From the Policy tree, double-click the firewall you are configuring for FIPS mode. The Firewall window appears. c From the navigation tree, select **Certificates** | **Firewall Certificates**. The Firewall Certificates tab of the Certificates area appears. d Click **Add Certificate**. The Certificate Request Wizard appears. e Use the Certificate Request Wizard to create or import a new certificate. The certificate Distinguished Name should include the full machine name. 2 Replace the certificate used by each service with the new firewall certificate and private key. See *Replace certificates* for the steps to replace the certificates. 3 Delete the old certificate and private key. a Select From the Control Center Client application, select **Policy**. b From the Policy tree, double-click the firewall you are configuring for FIPS mode. The Firewall window appears. c From the navigation tree, select **Certificates** | **Firewall Certificates**. The **Firewall Certificates** tab of the Certificates area appears. d Select the old certificate, then click **Delete Certificate**. e Click **OK** to save your configuration changes. 4 Click **Apply**. 5 Select the firewalls to apply the changes to, then click **OK**.
Global Threat Intelligence (TLS)	Firewall certificate/ private key	1 Delete the old certificate and private key. a From the Control Center Client application, select **Policy**. b From the Policy tree, double-click the firewall you are configuring for FIPS mode. The Firewall window appears. c From the navigation tree, select **Certificates** | **Firewall Certificates**. The **Firewall Certificates** tab of the Certificates area appears. d Select the certificate that begins with **MFE_Communication_Cert**, then click **Delete Certificate**. e Click **OK** to save your configuration changes.

Table 5-1 Critical security parameter (CSP) replacement *(continued)*

Service	CSP	Action to take
		2 Re-activate the firewall license. a From the Control Center Client application, select **Maintenance | Firewall License**. The Firewall License window appears. b From the **Firewall** drop-down list, select the firewall you are configuring for FIPS mode. c Click **Activate Firewall**. A message appears. d Click **OK**. 3 Click **Apply**. 4 Select the firewalls to apply the changes to, then click **OK**.
IKE	IKE pre-shared keys	Find and replace IKE pre-shared and IPsec manual keys. 1 From the Control Center Client application, select **Policy**. 2 From the Rule Objects tree, select **VPN | VPN Communities**. 3 Double-click the VPN community for the firewall you are configuring for FIPS mode. The VPN Community window appears. 4 Click **Authentication**. The Authentication tab appears. 5 In the **Pre-Shared key** field, type a new key. 6 Click **OK** to save your configuration changes.

Table 5-1 Critical security parameter (CSP) replacement *(continued)*

Service	CSP	Action to take
SSH server	SSH host key	Generate a new SSH server host key. 1 From the Control Center Client application, select **Policy**. 2 From the Policy tree, expand the **Firewalls** node. 3 Double-click the firewall you are configuring for FIPS mode. The Firewall window appears. 4 From the navigation tree, select **Certificates | Keys**. The Keys tab of the Certificates area appears. 5 Click **Add**. The Add SSH Key window appears. 6 Enter a name for the key, then click **OK**. 7 Click **OK**. 8 Replace the SSH keys. a Select **Policy** | **Rule Objects** | **Application Defenses** | **SSH**. The SSH Application Defense window is displayed. b Check all the application defenses. Click the **Client Advanced** tab to select the new DSA and RSA keys. Click **OK**. 9 Go back to firewall settings. From the navigation tree, click **Certificates | Keys**. Select the old keys and click **Delete**. 10 Select the firewalls to apply the changes to, then click **OK**.
Local Certificate Authority	Local CA private key	Delete local CAs. 1 From the Control Center Client application, select **Policy**. 2 From the Policy tree, expand the Firewalls node. 3 Double-click the firewall you are configuring for FIPS mode. The Firewall window appears. 4 From the navigation tree, select **Certificates | Local CA Certificates**. The **Local CA Certificates** tab of the Certificates area appears. 5 Select each listed CA, and click **Delete Certificate**. A message appears. 6 Click **Yes**.

Replace certificates

These following procedures enable you to regenerate firewall certificates and private keys.

To comply with FIPS 140-2 requirements, these certificates and keys must be created after FIPS 140-2 processing is enabled.

In order to delete the old certificates, you must remove all uses like:

- Admin console
- Audit log signing
- SmartFilter Admin
- Firewall reporter

- CAC authenticator
- Passport authentication
- Realtime audit
- Profiler communication
- Endpoint Intelligence Agent
- Secure alerts

If you fail to remove all uses of a certificate, the procedure to create a new certificate, replace the existing certificate, and delete the old certificate will be unsuccessful.

Table 5-2 Steps to replace certificates for listed services

Service	Action to take
Admin Console	Replace the certificate used by the Admin Console with the new firewall certificate. 1 From the Control Center Client application, select **Policy**. 2 From the Policy tree, double-click the firewall you are configuring for FIPS mode. The Firewall window appears. 3 From the navigation tree, select **Certificates | Settings**. The Settings tab of the Certificates area appears. 4 Under **SSL Certificates**, next to the Admin Console entry, select the new certificate from the drop-down list. 5 Click **OK**. The certificate is replaced.
Control Center	Replace the Control Center certificate used by a managed firewall. 1 From the Control Center Client application, select **Policy**. 2 From the Rule Objects tree, double-click the firewall you are configuring for FIPS mode. The Firewall window appears. 3 From the navigation tree, select **Certificates | Settings**. The Settings tab of the Certificates area appears. 4 Under **SSL Certificates**, next to the Control Center Server (in) entry, select the new certificate from the drop-down list. 5 Click **OK**. The certificate is replaced.

Table 5-2 Steps to replace certificates for listed services *(continued)*

Service	Action to take
SSL Content Inspection (8.x firewalls)	You have two options for SSL rules. **Option 1**: 1 Go to **Policy | <firewall> | Certificates | Settings | SSL Rule Settings**. 2 From the **Default RSA Certificate**, **Default RSA Key**, and **Default Local CA** drop-down lists, select a default certificate to use for all the SSL rules that apply to the firewall. 3 Click **OK**. **Option 2**: Use this option only when a rule uses **Override Certificate Settings**. 1 Select **Policy | Other Rules | SSL Rules**. Select the SSL rule that applies to the firewall. **Scenario 1** a If **Type** shows **Inbound** and Action shows **Decrypt only** or **Decrypt and re-encrypt**, click **SSL decryption settings (Client to Firewall)**. b Click **Override Certificate Settings...**. c Change the Key and Certificate for the firewall. **Scenario 2** a If **Type** shows **Outbound** and **Action** shows **Decrypt and re-encrypt** , click **SSL decryption settings (Client to Firewall)** . b Click **Override Certificate Settings...**. c Change the Key and Certificate for the firewall. 2 Click **OK**.
HTTPS Application Defenses (7.x firewalls)	You have two options for HTTPS defenses. **Option 1**: 1 Go to **Policy | <firewall> | Certificates | Settings | SSL Rule Settings**. 2 From the **Default RSA Certificate**, select a default certificate to use for all the HTTPS application defenses. 3 Click **OK**. **Option 2**: 1 From the Rule Objects tree, select **Application Defenses | HTTPS**. 2 Double-click an HTTPS Application Defense that is applied to the firewall you are configuring for FIPS mode. The HTTPS Application Defense window appears. 3 Under **SSL Settings**, deselect the **SSL2** and **SSL3** checkboxes. 4 If the HTTPS Application Defense is set to **Decrypt Web Traffic**, under **Firewall Certificates** change the firewall certificate. 5 Click **OK**.

Table 5-2 Steps to replace certificates for listed services *(continued)*

Service	Action to take
Firewall cluster management	1 Remove the firewall from the cluster and restore it to standalone status. a Right-click the firewall you are configuring for FIPS mode, then select **Demote to Standalone**. The Cluster Wizard appears. b Click **Finish**. The Apply Configuration window appears. c Click **OK**. 2 Replace the certificate. a From the Control Center Client application, select **Policy**. b From the Rule Objects tree, double-click the firewall you are configuring for FIPS mode. The Firewall window appears. c From the navigation tree, select **Certificates | Settings**. The Settings tab of the Certificates area appears. d Under **SSL Certificates**, next to the Cluster Registration Server entry, select the new certificate from the drop-down list. e Click **OK**. 3 Reconfigure the High Availability cluster. a Right-click the firewall, then select **Create/Join Cluster**. The Cluster Wizard appears. Click **Next**. b Select **Join existing cluster**, then click **Next**. c Click **Finish**. The Apply Configuration window appears. d Click **OK**
Audit log signing	1 From the Control Center Client application, select **Policy**. 2 Double-click a firewall and from the navigation tree, select **Offbox**. The Offbox area appears. 3 In the **Audit Export** area, from the **Certificate** drop-down list, select the new certificate.
IPSec/IKE	1 From the Control Center Client application, select **Policy**. 2 From the Rule Objects tree, select **VPN | VPN Peers**. 3 Double-click the firewall you are configuring for FIPS mode. The VPN Peer window appears. 4 Click **Authentication**. The Authentication tab appears. 5 From the **Certificate to present** drop-down list, select the new certificate. The certificate is replaced.
Realtime Audit	From the command line, enter this command: `cf ssl set proxy=realtime_audit firewall_certs=<name>` Where *name* is your new firewall certificate.

Table 5-2 Steps to replace certificates for listed services *(continued)*

Service	Action to take
Firewall Reporter	1 From the Control Center Client application, select **Policy**. Expand the **Firewalls** node. 2 Double-click the firewall and select **Offbox**. 3 In the McAfee Firewall Reporter / Syslog area, select **Encrypt traffic to McAfee Firewall Reporter**. 4 From the **Certificate** drop-down list, select a new certificate, then click **OK**. The certificate is replaced.
Firewall Profiler Communication	1 From the Control Center Client application, select **Policy**. Expand the **Firewalls** node. 2 Double-click the firewall and select **Offbox | McAfee Firewall Profiler** . 3 From the **Certificate** drop-down list, select a new certificate, then click **OK**. The certificate is replaced.
Endpoint Intelligence Agent	1 From the Control Center Client application, select **Policy**. Expand the **Firewalls** node. 2 Double-click the firewall and select **EIA**. 3 From the **CA Certificate** drop-down list, select a new certificate. The certificate is replaced.
Secure Alerts	From the command line, enter this command: `cf ssl set proxy=secure_alerts firewall_certs=<name>` Where *name* is your new firewall certificate.

Verify allowed cryptographic services

Allowed and prohibited cryptographic services for firewalls in FIPS mode are listed below. Examine your firewall configuration and make adjustments as necessary.

Task

1 Examine the firewall configuration for prohibited cryptographic services.

2 Make sure services use the appropriate SSL settings.

Do not configure FIPS 140-2-prohibited algorithms while FIPS 140-2 processing is enabled. All requests to use FIPS 140-2-prohibited algorithms will be rejected and audited.

Tasks

- *Modify SSL Rule settings* on page 35
  Services that use SSL or TLS must use TLSv1.1, TLSv1.2, or TLSv1. SSLv2 and SSLv3 are not allowed. To make sure a service is using the appropriate SSL settings, perform this procedure for SSL rules.

Allowed cryptographic services

These cryptographic services are allowed on firewalls in FIPS mode.

- Admin Console management
- Audit log signing and validation
- CAC authentication
- Certificate and key management
- Control Center management
- Cluster management (entrelayd)
- Firewall license management
- Firewall package signature validation and decryption
- Geo-Location, Virus Scanning, and IPS downloads
- IPsec and IKE VPNs
- McAfee® ePolicy Orchestrator communication
- McAfee® Global Threat Intelligence™ queries
- McAfee® Endpoint Intelligence Agent (McAfee EIA) communication
- Microsoft NT authentication (MD5, DES, RC4) (*cannot be used for administrator logon*)
- NTP (*cannot be used with MD5 authentication*)
- Passive Passport (MLC)
- RADIUS authentication (MD5) (*cannot be used for administrator logon*)
- RIPv2 and OSPF (*cannot be used with MD5 authentication*), other routing protocols
- Safeword authentication (DES) (*cannot be used for administrator logon*)
- Secure Sendmail (using STARTTLS)
- SNMPv3 (requires SHA-1 for message authentication)
- SSH client and server
- SSL content inspection (SSL Rules)

Prohibited cryptographic services

These cryptographic services are not allowed on firewalls in FIPS mode.

- Hardware acceleration (Cavium SSL and Crypto Offload)
- McAfee® SmartFilter®
- NTP with MD5 authentication
- RIPv2 and OSPF with MD5 authentication
- SCEP certificate enrollment
- Secure DNS
- SSH proxy

Modify SSL Rule settings

Services that use SSL or TLS must use TLSv1.1, TLSv1.2, or TLSv1. SSLv2 and SSLv3 are not allowed. To make sure a service is using the appropriate SSL settings, perform this procedure for SSL rules.

Task

1 From the Control Center Client application, select **Policy**.

2 **For 7.0.1.03 firewalls**

a From the Rule Objects tree, select **Application Defenses > HTTPS**.

b Double-click an HTTPS Application Defense that is applied to the firewall you are configuring for FIPS mode. The HTTPS Application Defense window appears.

c If the HTTPS Application Defense is set to decrypt web traffic, make sure the **TLS1** checkbox is selected.

d Deselect the **SSL2** and **SSL3** checkboxes.

3 **For 8.x firewalls**

a Click **Other Rules** and select **SSL Rules**. The SSL Rules window appears.

b For each rule, click **Modify**. The SSL Rule Editor window appears.

c Replace the certificate or key depending on the instance.

- For each rule that mentions the **Action** as **Decrypt** or **Decrypt / re-encrypt**, click **SSL Decryption Settings (Client to Firewall)** and make sure **TLSv1** is selected, and **SSLv2** and **SSLv3** are deselected.
- For each rule that mentions the **Action** as **Decrypt / re-encrypt**, click **SSL Re-encryption settings (Firewall to Server)**and make sure **TLSv1** is selected, and **SSLv2** and **SSLv3** are deselected.

4 Click **OK** to save the configuration changes.

5 Click **Apply**.

6 Select the firewalls to apply the changes to, then click **OK**.

Verify use of approved cryptographic algorithms and key lengths

Make sure all FIPS 140-2 cryptographic services use only these approved algorithms.

Service	Approved algorithm
Symmetric encryption	• AES128 • AES192 • AES256 • 3DES
Asymmetric encryption	• RSA (minimum 2048-bit key length) • DSA (minimum 2048-bit key length)
Hash algorithms	SHA2 (256, 384, 512)
HMAC algorithms	HMAC-SHA2 (256, 384, 512)

Tasks

- *Certificate authorities* on page 36
  Make sure certificate authorities use approved cryptographic algorithms.
- *Remote certificates* on page 36
  Make sure remote certificates use approved cryptographic algorithms.
- *IPsec and IKE* on page 37
  Make sure IPsec and IKE use approved cryptographic algorithms.
- *Passive Passport (MLC)* on page 37
  Make sure Passive Passport certificates use the RSA signature algorithm.

Certificate authorities

Make sure certificate authorities use approved cryptographic algorithms.

Task

1 From the Control Center Client application, select **Policy**.

2 From the navigation tree, expand the **Firewalls** node.

3 Double-click the firewall you are configuring for FIPS mode. The Firewall window appears.

4 From the navigation tree, select **Certificates**. The Firewall Certificates tab of the Certificates area appears.

5 Select the certificate you want to inspect, then click **Certificate Details**. The Certificate Details window appears.

6 Scroll through the certificate to find the Signature Algorithm line. Make sure it is a FIPS 140-2-approved algorithm.

If the algorithm is not approved:

- Generate or import a new certificate.
- Select the new certificate to replace the old certificate.
- Delete the old certificate.

Remote certificates

Make sure remote certificates use approved cryptographic algorithms.

Task

1 From the Control Center Client application, select **Policy** | **Remote Certificates**. The Remote Certificates window appears.

2 Select the certificate you want to inspect, then click **Certificate Details**. The Certificate Details window appears.

3 Scroll through the certificate to find the Signature Algorithm line. Make sure it is a FIPS 140-2-approved algorithm.

If the algorithm is not approved:

- Generate or import a new certificate.
- Select the new certificate to replace the old certificate.
- Delete the old certificate.

IPsec and IKE

Make sure IPsec and IKE use approved cryptographic algorithms.

Task

1 From the Control Center Client application, select **Policy**.

2 From the Rule Objects tree, select **VPN** | **VPN Communities**.

3 Double-click the VPN Community for the firewall you are configuring for FIPS mode. The VPN Community window appears.

4 Select **Cryptography** | **Cryptographic Properties**. The Cryptographic Properties tab appears.

5 Review the algorithms used. Select different algorithms as necessary.

6 Click **OK**.

7 Click **Apply**.

8 Select the firewalls to apply the changes to, then click **OK**.

Passive Passport (MLC)

Make sure Passive Passport certificates use the RSA signature algorithm.

Task

1 From the Control Center Client application, select **Policy**. Expand the **Firewalls** node.

2 Double-click the firewall that you are configuring passive authentication for. The Firewall window is displayed.

3 In the navigation tree, click **Offbox**. The Offbox area is displayed.

4 In the **McAfee Logon Collector (MLC)** area's **Certificate** field select the certificate that uses RSA algorithm.

   a In the navigation tree, expand **Certificates** and select **Firewall Certificates**.

   b Select the certificate used and click **Certificate Details**.

   c Verify that the certificate uses the RSA signature algorithm.

5 In the **CA certificate** field, make sure a certificate that uses the RSA signature algorithm is specified.

   a From the Control Center Client application, select **Policy** | **Rule Objects** | **VPN** | **CA Certificates**.

   b Select the CA certificate used and verify that it uses the RSA signature algorithm.

Verify SSH client and server configurations

Perform this procedure to make sure the firewall SSH client and server configuration is FIPS compliant.

The firewall server and client are compliant by default. You need to perform this procedure only if you have modified either of the following configuration files:

- `/secureos/etc/ssh/ssh_config`
- `/secureos/etc/ssh/sshd_config`

Verify the following:

- The SSH client and server are using approved cryptographic algorithms.
- Only SSH protocol version 2 is enabled. (SSH protocol version 1 is not allowed for the client or server).
- SSH public key authentication (PubkeyAuthentication) is disabled in the /secureos/etc/ssh/sshd_config file.

If you have problems with SSH or SSHD, view the firewall audit for details on any FIPS-related problems. See the SSH and SSHD man pages for information about configuring SSH and SSHD.

Restrict administrator access

Perform these steps to make the necessary administrator authentication changes for FIPS 140-2 compliance.

Task

1 Check the access control rules list to make sure administrators can only use local password authentication to log on to the managed firewall.

   All other authentication methods are prohibited for administrator logon.

2 [Physical appliances only] Enable authentication for emergency maintenance mode. Authenticated logon is required when the firewall is in emergency maintenance mode.

   a From the Firewall Enterprise Admin Console, use a file editor to open `/etc/ttys`.

   b Make the following change:

Locate this line:	console	none	unknown	off secure
Make this change:	console	none	unknown	off insecure

3 If you have a Telnet rule allowing administrator logon, disable the rule.

4 Change each administrator password.

   a From the Control Center Client application, select **Policy**.

   b From the Rule Objects tree, select **Firewall users > Administrators**.

   c Double-click the administrator for the firewall you are configuring for FIPS mode. The Administrator window appears.

   d In the **Password** field, type a new password.

   e Click **OK**.

   f Click **Apply**.

   g Select the firewalls to apply the changes to, then click **OK**.