



FortiManager 5.6.6

Common Criteria EAL4 Technote

FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET KNOWLEDGE BASE

<http://kb.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET NSE INSTITUTE (TRAINING)

<https://training.fortinet.com/>

FORTIGUARD CENTER

<https://fortiguard.com>

FORTICAST

<http://forticast.fortinet.com>

END USER LICENSE AGREEMENT AND PRIVACY POLICY

<https://www.fortinet.com/doc/legal/EULA.pdf>

<https://www.fortinet.com/corporate/about-us/privacy.html>

FEEDBACK

Email: techdoc@fortinet.com



Wednesday, June 12, 2019

Common Criteria EAL4 Technote for FortiManager 5.6.6

02-566-486071-20190604

TABLE OF CONTENTS

Introduction	5
References	5
Certified Models	5
Installing the CC Certified Firmware	6
Verifying secure delivery	6
Registering the unit	6
Installation Requirements	6
Installing the unit	7
Downloading the FIPS-CC certified firmware and MD5 check sums	7
Verifying the integrity of the firmware build	7
Installing the FIPS-CC firmware build	8
Potential Firmware issues	8
Potential Hardware issues	8
Entropy	9
The Fortinet Entropy Token	9
Installing the entropy token	9
Configuring the entropy token settings	9
RBG Seeding and Reseed Interval	10
The FIPS-CC Mode of Operation	11
Enabling FIPS-CC mode	11
Disabling FIPS-CC mode	12
Key Destruction	12
Common Criteria compliant operation	13
Use of non-CC evaluated features	13
Install Updated Certificates	13
Trusted Hosts	13
Administration	14
Remote access requirements	14
Web browser requirements	14
Enabling administrative access	14
Disabling JSON API access	15
Configuration backup	15
Self-tests	15
FIPS Error Mode	15

Miscellaneous administration related changes16

Introduction

Fortinet performs FIPS 140-2 and Common Criteria certifications on specific FortiManager versions in combination with specific FortiManager family hardware models. This technote applies to the Common Criteria EAL4 certification of FortiManager 5.6.6 build 7352.

The documentation set for FortiManager units operated in FIPS-CC mode consists of this document and the standard FortiManager 5.6.6 documentation set. This document covers Common Criteria specific installation instructions and explains the FortiManager FIPS-CC mode of operation. The standard documentation is available from the Fortinet Technical Documentation web site (<http://docs.fortinet.com>).

For detailed information on the FortiManager 5.6.6 Common Criteria certification refer to the FortiManager 5.6.6 EAL4 Security Target.

References

EAL4 Security Target: Fortinet FortiManager 5.6.6, Version 1.10, 30 May 2019

FortiManager [Documentation Set](#)

Model specific [Hardware Information Supplements](#)

Certified Models

FMG-400E	FMG-2000E	FMG-3900E	FMG-4000E
FMG-1000D	FMG-3000F	FMG-4000D	

Installing the CC Certified Firmware

This section describes how to install the CC certified firmware on your FortiManager unit.

Verifying secure delivery

Before installing the FortiManager unit, you should take steps to ensure the unit has not been tampered with during transit. Perform the following checks to verify the integrity of the unit prior to installation.

- Courier - Fortinet only uses bonded couriers such as UPS, FedEx or DHL. Verify the shipment was received using a bonded courier.
- Shipping information - Verify the shipment information against the original purchase order or evaluation request. Verify the shipment has been received directly from Fortinet.
- External packaging - Verify the Fortinet branded packing tape sealing the packaging is intact and the packaging has not been cut or damaged to allow access to the unit.
- Internal packaging - Verify the unit is sealed in an undamaged, clear plastic bag for non-blade units. For blade units, verify the internal box packaging is intact.
- Warranty seal - For non-blade units, verify the unit's warranty seal is intact. The warranty seal is a small, grey sticker with the Fortinet logo and is normally placed over a chassis access screw. The chassis cannot be opened without destroying the warranty seal.

If you identify any concerns while verifying the integrity of the unit, contact your supplier immediately.

Registering the unit

Register your product in order to access firmware builds, customer support, etc. You can register your FortiManager unit through the [Fortinet Support Website](#). Refer to the [Fortinet Support Website User Guide](#) for details on registering your product.

Installation Requirements

Common Criteria compliant operation requires that you use the FortiManager unit in its FIPS-CC mode of operation and that you follow secure procedures for installation and operation of the unit. You must ensure that:

- The FortiManager unit is installed in a secure physical location.
- Physical access to the FortiManager unit is restricted to authorized operators.
- A Fortinet entropy token is used to seed the RBG and the Fortinet entropy token remains in the USB port during operation (to allow for periodic reseeding of the RBG).

Installing the unit

The documentation shipped with your unit includes a FortiManager QuickStart Guide and a model specific Hardware Supplement. The FortiManager Admin Guide includes a Getting Started chapter that provides additional installation and configuration details. These documents provide instructions on the physical installation and initial configuration of your unit. When you have completed these procedures you will be able to access both the web-based manager and Command Line Interface (CLI).

Downloading the FIPS-CC certified firmware and MD5 check sums

To download the firmware and MD5 check sums

1. With your web browser, go to <https://support.fortinet.com/> and log in using the name and password you received when you registered your unit with Fortinet Support.
2. Navigate to the FortiManager 5.6.6. FIPS-CC Certified download page. Download the firmware build for your specific hardware model. Save the file on the management computer or on your network where it is accessible from the FortiManager unit.
3. Download the md5sum.txt file from the same directory as the firmware. This file contains MD5 check sums for the firmware builds.



Note that upgrading a FortiManager unit running a FortiManager 5.2 (or earlier) certified build in FIPS-CC mode to FortiManager 5.6 is not officially supported. Back up your configuration and contact Fortinet Support before starting.

Verifying the integrity of the firmware build

There are two methods you can use to verify the integrity of the firmware build. A manual method using the MD5 hashes downloaded from the support site and an automatic method using RSA signatures.

You can use a hashing utility to create an MD5 hash for each firmware build you download. Compare the resulting hash to the corresponding hash from the `md5sum.txt` file. If the hashes match, the downloaded build is uncorrupted and unmodified.

However, MD5 is not a FIPS 140-2 or Common Criteria approved integrity check method, which is why the FIPS-CC mode of operation includes an automatic firmware integrity test using RSA signatures. When FIPS-CC mode is enabled, FortiOS uses a public key to verify the signatures applied to the core system files. The integrity test takes place automatically during the boot process. If the test fails, the FortiManager unit will halt. See the FIPS-CC Mode section for more details.

Installing the FIPS-CC firmware build

Install the FIPS-CC firmware build on your FortiManager unit. There are several methods to do this. Refer to the FortiManager Administration Guide and FortiManager CLI Reference Guide for more information.

Verifying the firmware version of the unit

Execute the following command from the command line:

```
get system status
```

The version line of the status display shows the FortiManager model number, firmware version, build number and date. For example:

```
Version: FortiManager-2000E v5.6.6,build7347,190328
```

Verify in the relevant security target or security policy document that your firmware version, build number and date are correct.

Potential Firmware issues

If the unit is not booting correctly and power cycling the unit does not clear the problem, then it may be necessary to reinstall the firmware. The firmware can be reinstalled using the FortiManager BIOS boot menu and a remote tftp server. The BIOS can also be used to format the boot device prior to reinstalling the firmware to ensure a clean installation.

Refer to the following FortiGate Cookbook recipe for more details: [Navigating the FortiGate BIOS](#). Although the document is titled "Navigating the FortiGate BIOS", the content is equally applicable to FortiManager.

You may want to contact Fortinet's technical support group before attempting to use the FortiManager BIOS tools. You can open a support ticket on the support website.

Potential Hardware issues

If the unit fails any of the startup hardware checks or displays a hardware fault during operation, contact Fortinet technical support.

Entropy

Generation of strong encryption keys requires a strong source of random data, also referred to as entropy. FortiManager 5.6.6 uses the Fortinet Entropy Token as a strong entropy source. FortiManager also includes a basic, software based entropy source that is used if the entropy token is not installed or if the entropy token is installed, but not enabled.

The Fortinet Entropy Token

Based on a wide band, Gaussian white noise generator, the Fortinet Entropy Token provides users with a simple, FIPS 140-2 and NDPP CC validated source of entropy.

The Fortinet Entropy Token is compatible with FortiManager 5.2 or higher.

Installing the entropy token

Plug the entropy token into an available USB port on the FortiManager unit. Note that the entropy token requires a USB-A port.

Configuring the entropy token settings

Use of the entropy token is required for FIPS 140-2 and Common Criteria compliance. It is possible to disable the use of the token in FIPS-CC mode, but doing so means the unit is not operating in a FIPS or CC compliant manner. There are three options for the entropy token setting:

- `enable` — token required
- `disable` — token is not required and is not used even if present
- `dynamic` — token is not required, but is used if present

To enable FIPS-CC mode with use of the entropy token enter the following commands from the FortiManager console.

```
config system fips
  set status enable
  set entropy-token enable
end
```

See the FIPS-CC Mode of Operation section for complete details on enabling the FIPS-CC mode of operation.



The FIPS-CC mode of operation can only be enabled from the FortiManager console.

RBG Seeding and Reseed Interval

The RBG is seeded from the entropy token during the boot process and then reseeded periodically. The default reseed period is once every 24 hours (1440 minutes) and is configurable using the `self-test-period` CLI command.

To set the reseed interval to 60 minutes, enter the following commands from the FortiManager CLI.

```
config system fips
    set re-seed-interval 60
end
```



The entropy token must be present to allow the RNG to seed or reseed from the token.

When FortiManager is configured in FIPS-CC mode with the entropy token enabled, if the token is not present at boot time or the reseed interval, the boot process will pause until the token is inserted. The following message is displayed on the console:

```
Please insert entropy-token to complete RNG seeding
```

The message is repeated until the token is inserted.

If the entropy token is set to dynamic and the token is not present at boot time or the scheduled reseed interval, the unit will use the default, internal FortiManager seed method instead.

The FIPS-CC Mode of Operation

If you have verified the firmware version, you are ready to enable FIPS-CC mode.



When you enable FIPS-CC mode, the existing configuration is cleared and restrictive default settings are implemented.

The new password must be at least 8 characters long and must contain at least one each of:

- upper-case-letter
- lower-case-letter
- numeral
- non-alphanumeric character

Enabling FIPS-CC mode

Use the following steps to enable FIPS-CC mode:

1. If required, plug the entropy token into a USB port on the FortiManager unit.
2. Log in to the CLI through the console port. Use the default admin account or another account with a super_admin access profile. Enter the following commands.

```
config system fips
  set status enable
  set entropy-token [enable|disable|dynamic]
  set re-seed-interval [1 to 1440]
end
```

3. In response to the following prompt, enter the new password for the administrator:
Please enter administrator password:
4. When prompted, re-enter the administrator password. The CLI displays the following message:
Warning: most configuration will be lost,
do you want to continue? (y/n)
5. Enter y. The FortiManager unit restarts and is now running in FIPS-CC mode.
6. A series of self-tests are performed during the boot process when FIPS-CC mode is enabled. You should see output similar to the following. If any of the tests fail, the FortiManager unit will halt.

```
FIPS-CC mode: Starting self-tests.  
Running Configuration Bypass test...      passed  
Running AES test...                      passed  
Running SHA1 HMAC test...                 passed  
Running SHA256 HMAC test...               passed  
Running SHA384 HMAC test...               passed  
Running RSA test...                      passed  
Running Firmware integrity test...         passed  
Running RBG-instantiate test...            passed  
Running RBG-reseed test...                passed  
Running RBG-generate test...              passed  
Self-tests passed
```

7. Verify FIPS-CC mode is enabled. The `get system status` CLI command output should include "FIPS mode: Enabled".

Disabling FIPS-CC mode

To disable the FIPS-CC mode of operation, reset the unit to the factory default configuration using the following CLI command:

```
execute reset all-settings
```

Disabling FIPS-CC mode erases the current configuration and destroys most keys and critical security parameters. To completely destroy all keys and wipe the configuration data, refer to the instructions in the next section.

Key Destruction

All keys and CSPs are destroyed by erasing the unit's boot device and then power cycling the unit. To erase the boot device, execute the following command from the CLI:

```
execute erase-disk <boot device>
```

The command erases the boot device by overwriting it with random data.

The boot device ID may vary depending on the FortiManager module. The following command will output a list of the available internal disks:

```
execute erase-disk ?
```



Erasing the unit's boot device will leave the unit unbootable. The firmware can be reinstalled using the FortiManager BIOS boot menu tools and a tftp server.

Common Criteria compliant operation

Use of non-CC evaluated features

FIPS-CC mode does not prevent you from using features that were not part of the evaluated configuration. However, if you use these features, you may not be operating the FortiManager unit in strict compliance with the Security Target. Refer to the Security Target for more information.

Install Updated Certificates

By default, FortiManager units use a certificate signed by a Fortinet Certificate Authority (CA). Administrators should install a new, signed certificate from a trusted CA. Consult the FortiManager Administration Guide for additional information on replacing the default certificate.

Trusted Hosts

Trusted hosts should be configured for Administrators to improve security. FortiManager supports up to three trusted hosts per Administrator account. Refer to the FortiManager Administration Guide for details on how to configure trusted hosts.

Administration

This section describes administration specific issues and changes to the way FortiManager should be configured or how it functions in the FIPS-CC mode of operation.

Remote access requirements

In FIPS-CC mode, remote administration via HTTP or Telnet is disabled. HTTPS, SSH or the console should be used. The FIPS-CC mode of operation restricts the cipher suites used by HTTPS and SSH to a subset of the NDCPP compliant suites. Refer to the Security Target for additional information. The administrator does not need to take any specific actions to ensure compliance when using HTTPS or SSH as long as the FIPS-CC mode of operation has been enabled.

Web browser requirements

To use the web-based manager in FIPS-CC mode, your web browser application must meet the following requirements:

- Authentication algorithm: PKCS1 RSA
- Connection security: TLS 1.1 or higher

To configure FortiManager to enforce the use of TLS 1.1 or higher, enter the following CLI commands:

```
config system global
  set enc-algorithm high
  set fgfm-ssl-protocol tlsv1.1
  set oftp-ssl-protocol tlsv1.1
  set webservice-proto tlsv1.1
end
```

Enabling administrative access

In FIPS-CC mode, remote administrative access is disabled by default. You can enable use of the web-based manager using CLI commands on the console. This example adds HTTPS and SSH administrative access on the port1 interface:

```
config system interface
  edit port1
    set allowaccess https ssh
  end
```

For detailed information about accessing the web-based manager, see “Connecting to the GUI” in the FortiManager Administration Guide.

Disabling JSON API access

In FIPS-CC mode, the JSON API must be disabled by setting `rpc-permit` to `none` for all administrative user accounts. The following example shows how to set `rpc-permit` to `none` for the default admin user account:

```
config system admin user
  (user)# edit admin
    (admin)# set rpc-permit none
    (admin)# end
```

Configuration backup

Configuration backup files created in FIPS-CC mode are not compatible with backup files created in non-FIPS-CC mode. A FIPS-CC mode configuration backup cannot be restored in non-FIPS-CC mode and vice-versa.

You can create FIPS-CC configuration backup files to use for disaster recovery. They are valid on a replacement FortiManager unit or to restore configuration after you exit and then re-enter FIPS-CC mode.

Refer to the FortiManager Administration Guide for detailed information about creating configuration backup files.

Self-tests

The FIPS-CC mode of operation includes a set of startup and conditional self-tests. The tests include algorithm known answer tests (KATs), a firmware integrity test and a configuration bypass test. Refer to the FortiManager 5.6.6 Security Policy for a complete list of the self-tests.

The administrator can run self-tests manually at any time. To run all of the tests, enter the following CLI command:

```
execute fips kat all
```

To run an individual test, enter `execute fips kat <test_name>`. To see the list of valid test names, enter `execute fips kat ?`

FIPS Error Mode

If one or more of the self-tests fail, the FortiManager unit switches to FIPS Error mode. The unit shuts down all interfaces including the console and blocks traffic. To resume normal FIPS-CC mode operation, power cycle the unit. If the self-tests pass after the reboot, the unit will resume normal FIPS-CC operation. If a self-test continues to fail after rebooting, there is likely a serious firmware or hardware problem and the unit should be removed from the network until the problem is solved.

Miscellaneous administration related changes

- By default, after three failed attempts to log on to an administrator account the account is locked out for one minute. You can change the number of attempts permitted and the length of the lockout.
- When configuring passwords or keys, the FortiManager unit requires you to enter the password or key a second time as confirmation.
- The `maintainer` account, which allows you to reset the admin password, is disabled.
- The local FortiManager TFTP servers is disabled by default. TFTP can be re-enabled using the `tftp` keyword in the `config system global` CLI command, but this is not FIPS-CC compliant operation.
- USB auto-install options are disabled.



High Performance Network Security



Copyright© 2019 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.