NDcPP Common Criteria and FIPS 140-2 Technote

FortiManager 6.2

Document version:	1.5
Publication date:	Friday, July 22, 2022
Firmware version:	v6.2, build 9589

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

FortiManager 6.2 NDcPP Common Criteria and FIPS 140-2 Technote
02-628-740959-20210818

TABLE OF CONTENTS

Introduction

Fortinet performs FIPS 140-2 and NDcPP Common Criteria certifications on specific FortiManager OS versions in combination with specific FortiManager family hardware models. At the publication date of this document, the latest NDcPP CC certified version of the FortiManager OS is 6.2.

The documentation set for FortiManager units operated in FIPS-CC mode consists of this document and the standard FortiManager 6.2 documentation set. This document covers NDcPP 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 6.2 NDcPP Common Criteria certification, including the certified hardware models, refer to the FortiManager 6.2 NDcPP Security Target. The Security Target can be found on the Fortinet Support web site in the FortiManager 6.2 FIPS-CC certified firmware download directory (http://support.fortinet.com).

References

Security Target: FortiManager 6.2
FIPS 140-2 Security Policy: FortiManager 6.2
FortiManager 6.2.8 Administration Guide
FortiManager 6.2.8 CLI Reference
FortiManager 6.2.8 Log Reference (Combined FAZ/FMG document)
Model specific Hardware Information Supplements

Certified Models

FortiManager-300F	FortiManager-3000F
FortiManager-1000F	FortiManager-3700F

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.
- Warranty seal - 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.
- An Araneus Alea II entropy token is used to seed the RBG, if required, and the token remains in the USB port during operation (to allow for periodic reseeding of the RBG). See the Entropy Section for details on which models require an entropy token as a strong entropy source.

Installing the unit

The documentation shipped with your unit includes a QuickStart Guide and a model specific Hardware Supplement. The FortiManagerAdministration includes a "Setting up FortiManager" 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

The validated firmware version is FortiManagerv6.2, build 9589.

To download the firmware

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 6.2 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.

Verifying the integrity of the firmware build

Download the model specific FIPS validated firmware image and checksum from the Fortinet Support site at https://support.fortinet.com/. Use a hashing utility on the downloaded firmware image to compare and verify the output against the result from the checksum listing. If the hashes match, the downloaded build is uncorrupted and unmodified.

In addition to the above, FIPS validated firmware images are digitally signed via an RSA key. Any FIPS validated firmware image that is installed or updated will automatically be verified with this signature.

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 or FortiManager CLI 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 firmware version and build number. For example:

```
Version: v6.2.8-build9498 210713
```

Verify in the relevant security target or security policy document that your firmware version and build number are correct. Note that YYMMDD is the build date, but the date is not relevant for verifying the firmware version.

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.

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 6.2 uses the Araneus Alea II entropy token as its strong entropy source.

The Araneus Alea II entropy token

Based on a wide band, Gaussian white noise generator, the Alea token provide users with a FIPS 140-2 and cPP CC validated source of entropy for FortiManager models that do not have an internal strong entropy source. The Alea token is generically referred to as the entropy token.

Installing the token

Plug the token into an available USB port on the FortiManager unit.

Configuring the entropy token settings

Use of the 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.

RBG Seeding and Reseed Interval

The RBG is seeded during the boot process and then reseeded periodically. The default reseed period is once every 24 hours (1440 minutes) and is configurable using the `re-seed-interval` 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.

You must use a console connection to enable FIPS-CC mode. Enabling FIP-CC mode is not supported via the GUI or SSH.

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

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

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. Verify FIPS 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 zeroizes most keys and critical security parameters. To completely zeroize the unit, refer to the instructions in the next section.

Key Zeroization

All keys and CSPs are zeroized 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 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 CA Certificate

A CA certificate must be installed before any new, CA signed certificates can be installed.

The CA cert must have the following basic attributes set:

- Basic Constraint X509 certificate extension set to true
- cRLSign set to true

To import the CA certificate, use the CLI commands:

```
config system certificate ca
   edit <ca-cert-name>
   set ca <CA-cert-content-PEM-format>
end
```

When creating a CRL for an intermediate CA by using "config system certificate crl", the following warning message may occur:

```
   "Cannot read certificate file d25f96a3.r2"
```

Despite the warning, the CRL for intermediate CA can be created successfully. The warning message may be ignored.

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 . The basic steps are to create a new local public/private key pair and export the CSR. Get the CSR signed by a CA, import the CA certificate and then import the newly signed local certificate.

Required certificate parameters:

- The local certificate must have the serverAuth extended key usage set to true, if it will be used as the HTTPS (GUI) server certificate
- The local certificate must have the clientAuth extended key usage set to true, if it will be used to connect to a remote log server (e.g. FortiAnalyzer)

All other X509 certificate validation checks are done when a TLS connection is to be established between the TOE and the other entities.

Consult the FortiManager Administration Guide for additional information.

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.

Default Admin User API

For increased security, the default admin user .json API should be disabled. To do so, use the CLI commands:

```
config system admin user
```

```
    edit admin
    set rpc-permit none
end
```

Administration

This section describes administration specific changes to the way FortiManager Administration Guide functions in the FIPS-CC mode of operation and addresses general administration related issues.

Remote access requirements

In FIPS-CC mode, remote administration via HTTP or Telnet is disabled. HTTPS, SSH or the console should be used for remote access to the TOE. 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.

For SSH remote access, the key-board interactive method of authentication should be used with RSA signatures.

Note that the Administrator's credentials (private keys) used to access the TOE must be protected on any other platform on which they reside (e.g. management computers used to remotely access the TOE).

Web browser requirements

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

- Connection security: TLS 1.1 or 1.2
- One of the following TLS cipher suites:
  - TLS_DHE_RSA_WITH_AES_128_CBC_SHA
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHA
  - TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
  - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
  - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA2
  - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
  - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
  - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
  - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

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
```

The Diffie-Hellman group should be set to Group 14 (2048-bit modulus) as per the evaluated configuration:

```
config system global
   set dh-params 2048
end
```

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

Trusted hosts

Trusted hosts for adminstrator remote access should configured. Trusted hosts can be configured through the web-based manager or the CLI. Refer to the FortiManager Administration Guide for more information.

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.

Admin access disclaimer

In order to meet NDcPP (Network Device Protection Profile) compliance, a pre-login disclaimer banner must be enabled.

To enable the disclaimer, log in to the CLI using the default admin account or another account with a super_admin access profile. Enter the following commands:

```
config system global
   set pre-login-banner enable
end
```

Please note that a post-login disclaimer banner is enabled by default. If desired, this disclaimer can be disabled by entering the following command:

```
config system global
   set post-login-banner disable
```

```
end
```

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), and a firmware integrity test. Refer to the FortiManager 6.2 FIPS 140-2 Level 1 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.

Logging out from the GUI and CLI

To log out from the FortiManager Web-Based Manager, click on your username in the top right of the window and select "Log Out".

To logout from the CLI, enter "exit" from the top level of the CLI tree.

Disable NTP

NTP is not claimed in the Security Target. NTP should be disabled to be compliant with the Security Target. Use the following CLI commands to disable NTP.

```
config system ntp
   set status disable
end
```

FortiGuard Labs PSIRT Security Advisories

The administrator is encouraged to keep up to date on security advisories from FortiGuard Labs Product Security Incident Response Team (PSIRT) https://fortiguard.com/psirt and apply fixes where available.

Enabling private data encryption

The administrator must enable private data encrption and load a key for encryption of stored critical security parameters. Use the following CLI commands to enable private data encryption.

```
configure system global
   set private-data-encryption enable
end
```

Once private data encryption is enabled, the administrator will be prompted will be prompted to enter, and confirm, a 128bit AES key that will be used for encrypting stored critical security parameters.

Miscellaneous administration related changes

- By default, after three failed attempts to log on to an administrator account, the account is locked out for for a set amount of time (by default, 60 seconds). You can change the number of attempts permitted and the length of the lockout.
- On a CLI session, when an administrator logs out or the session times out, the FortiManager unit sends 300 carriage return characters to clear the screen. Note: if your terminal buffer is large, not all information from the session may be cleared.
- When configuring passwords or keys, theFortiManager 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 server 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.
- Virus attack reporting to FortiGuard Distribution Service (FDS) is disabled.
- Use of the secure shell is not included in the scope of the evaluation and is disabled by default.

Log Specific Settings

This section describes logging specific changes to the way FortiAnalyzer functions in the FIPS-CC mode of operation. For information on how to offload logs to a remote FortiAnalyzer device over SSL, see the System Settings chapter of theFortiManager Administration Guide.

Log messages are cached on the local FortiManager unit before being offloaded to the remote FortiAnalyzer device. The log messages are cached on the local disk or in system memory if the unit does not have disk storage. The log message cache is separate and distinct from local log storage.

If the SSL connection with the FortiAnalyzer is interrupted, one (or both) of the following log messages will be displayed:

SSL connection to <ip address> failed.

SSL connection to <ip address> closed.

Please re-establish the SSL connection between the devices to maintain CC compliance.

FortiAnalyzer configuration

Connections to a remote FortiAnalyzer device in the FIPS-CC mode of operation require the remote FortiAnalyzer's X.509 certificate be loaded onto the local FortiManager device. To configure the remote FortiAnalyzer device connection, use the following CLI commands. Note that the CLI must be used for the remote FortiAnalyzer configuration.

```
config system locallog fortianalyzer setting
   set status realtime
   set status enable
   set secure-connection enable
   set server "192.168.10.1"
   set severity debug
end

config system certificate oftp
   set mode local
   set local "oftp_client_cert"
end
```

This example assumes the address of the remote FortiManager device is 192.168.10.1 and the custom certificate name is oftp_client_cert. Note that the server address can use either ip-address or FQDN to set the reference identifier and FortiManager supports both IP address and DNS name in the certificate's CN or SAN (optional). If the server is identified by IP address, then the SAN must also be configured. The remote FortiManager certificate must be an X.509 certificate.

Note that the oftp client certificate must have the following basic attributes:

- Basic Constraint set to false
- Extended Key Usage extension set to clientAuth
- The CN/SAN set to the server's DNS name
- Key Usage attributes should not be set

Also note that the CA that signs the oftp client certificate must have the clientAuth Extended Key Usage attibute set in its certificate.

Reconnecting to a remote FortiAnalyzer unit

Should communications to the remote FortiAnalyzer be interrupted, the FortiManager is no longer considered to be operating in a CC compliant manner. If an interruption occurs in the communications path between the local and remoteFortiAnalyzer units, the administrator can attempt to re-establish the connection manually by sending a ping to the remote FortiAnalyzer via the local FortiManager's CLI. This can be done in the evaluated configuration by logging in to the GUI via HTTPS and launching the console. Once the console is launched, the administrator may execute the following command:

```
exec ping <FortiAnalyzer IP address>
```

If the ping is successful, the local FortiManager and remote FortiAnalyzer units should re-establish communication and logs should resume flowing to the remote FortiAnalyzer.

If a manual ping does not re-establish the connection, there may be a more serious network problem or problem with the remote FortiAnalyzer unit itself. Contact Fortinet support, if necessary, to resolve the problem.

Local Logging

The default log setting is to overwrite the oldest log entries once the local log capacity is reached.

The System Event Log contains log entries for when:

- Local log files are rolled (new log file created)
- Local log files are deleted (old log files are overwritten)

Clearing local logs

The local logs can be cleared from the GUI or the CLI. Clearing the local logs does not affect cached logs - i.e. logs cached for offloading to a remote FortiAnalyzer unit.

Miscellaneous Logging

- The Common Criteria protection profile requires logging of all traffic and logging of system events, including startup and shutdown of functional components. Logging is enabled by default for:

- new security policies
- interfaces where administrative access is enabled
- attempts to gain administration access on network interfaces where administrative access is not enabled
- failed connection attempts to the FortiManager unit using TCP/IP ports other than 22 (ssh), 23 (telnet), 80 (HTTP), and 443 (HTTPS).
- all configuration changes
- configuration failures
- remote IP lockout due to reaching maximum number of failed login attempts
- log viewing
- interface going up or down
- other traffic: dropped ICMP packets, dropped invalid IP packets, session start and session deletion
- Logging is enabled for all event types at the information severity level.
- Memory logging is enabled on units that do not contain a hard disk. Logging includes traffic logging and all event types. Note that traffic logging to memory is available only in FIPS-CC mode and the log capacity is restricted by the available memory in the unit.
- The diskfull action is set to overwrite.