FortiController-5000 v5.2.7 Release Notes

VERSION 5.2.7

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

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTINET COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING AND CERTIFICATION PROGRAM

https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE

https://training.fortinet.com/

FORTIGUARD CENTER

https://fortiguard.com

FORTICAST

http://forticast.fortinet.com

END USER LICENSE AGREEMENT

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

July 30, 2018

FortiController-5000 v5.2.7 Release Notes

11-527-439178-20180730

TABLE OF CONTENTS

Change log

Date	Change description
July 30, 2018	Initial release.

Introduction

This document provides the following information for FortiController-5000 5.2.7 build 0182:

- Supported models
- Special Notices
- Upgrade Information
- Product Integration and Support
- Resolved Issues
- Known Issues

See the Fortinet Document Library for FortiController-5000 documentation.

Supported models

FortiController-5000 5.2.7 supports the following models:

FortiController	FCTL5103B, FCTL5903C, and FCTL5913C.

Special Notices

General

The TFTP boot process erases all current switch configuration and replaces it with the factory default settings.

FortiGate-5001D operating in FortiController or Dual FortiController mode

When upgrading a FortiGate-5001D operating in FortiController or dual FortiController mode from 5.0.9 to FortiOS 5.2.2 and later, you may experience a backplane interface connection issue. After the upgrade, you will need to perform a factory reset and then re-configure your device.

Upgrade Information

Upgrading from FortiController-5000 5.2.5

FortiController-5000 5.2.7 supports upgrading from FortiController-5000 5.2.5 and above.

Downgrading to previous firmware versions

Downgrading from FortiController-5000 5.2.7 to previous releases is not supported.

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal, https://support.fortinet.com. After logging in select **Download > Firmware Image Checksums**, enter the image file name including the extension, and select **Get Checksum Code**.

Product Integration and Support

FortiController-5000 5.2.7 support

The following table lists FortiController-5000 5.2.7 product integration and support information.

Web browser	• Microsoft Internet Explorer version 10 • Mozilla Firefox version 33 • Google Chrome version 37 Other web browsers may function correctly, but are not supported by Fortinet.
FortiOS	• 5.2.10 and later

Resolved Issues

The following issues have been fixed in FortiController-5000 5.2.7. For inquires about a particular bug, please contact Customer Service & Support.

Bug ID	Description
502916	Resolved an issue that prevented FortiManager from accessing an SLBC cluster after upgrading the FortiControllers in the cluster to FortiController v5.2.6.
500675	Resolved an issue that caused the /var/log/wtmp file to use excessive amounts of disk space.

Known Issues

The following known issues have been identified with FortiController-5000 5.2.7. For inquires about a particular bug or to report a bug, please contact Fortinet Customer Service & Support.

Bug ID	Description

483105	SHA1 weak certificate signature may be vulnerable. This certificate encrypts HTTPS administrator login sessions.
	
	Workaround:
	
	Upload your own more secure certificate from the GUI:
	1. Go to **System > Certificate > Import > Import Certificate**.
	2. Under *Certificate file (*.crt)*, select the certificate to import.
	3. Under *Key file (*.key)*, select the key for import.
	
	Upload your own certificate from the CLI:
	`execute user certificate upload tftp <file.crt> <file.key> <tftp_ipv4>`
	
	Us this certificate instead of the default certificate. To activate your certificate, use the following CLI commands:
	
	`config system global`
	`set admin-server-cert <cert>`
	`set strong-crypto enable`
	`end`