FortiController-5000 - Release Notes

Version 5.2.6

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

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

FORTINET BLOG
https://blog.fortinet.com

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

FORTIGATE COOKBOOK
http://cookbook.fortinet.com

FORTINET TRAINING SERVICES
http://www.fortinet.com/training

FORTIGUARD CENTER
http://www.fortiguard.com

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

FEEDBACK
Email: techdocs@fortinet.com

May 22, 2018
FortiController-5000 (FortiSwitch ATCA) 5.2.6 Release Notes
11-526-439178-2018022

TABLE OF CONTENTS

Change Log

Date	Change Description
May 22, 2018	Initial release.

Introduction

This document provides the following information for FortiController-5000 5.2.6 build 0180:

See the Fortinet Document Library for FortiController-5000 documentation.

Supported models

FortiController-5000 5.2.6 supports the following models:

FortiController	FCTL-5103B, FCTL-5903C, and FCTL-5913C.

What's new in 5.2.6

The following is a list of enhancements in 5.2.6:

- Added support for VLAN masking in load balancing flow-rules.

Special Notices

General

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

FG-5001D operating in FortiController or Dual FortiController mode

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

Upgrade Information

Upgrading from FortiController-5000 5.2.4

FortiController-5000 5.2.6 supports upgrade from 5.2.4 and above.

Downgrading to previous firmware versions

Downgrading from FortiController-5000 5.2.6 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 5.2.6 support

The following table lists 5.2.6 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 5.2.6. For inquires about a particular bug, please contact Customer Service & Support.

Bug ID	Description
412760	Automatic daylight savings time adjustment now works correctly.
392441	Fixed an issue that blocked broadcasting IP fragmented packets when `load-distribution-method` was set to any L3 algorithm.
421210	Fixed an issue that caused traffic to be dropped for a few seconds when rebooting a FortiController in a backup chassis.
309358	The backup chassis now correctly updates the bridge table of the active chassis with valid information.
423333	The FortiController-5903C and 5913C models now support interdependent split ports.
408384	FortiController LAG link-status now appears in the worker-blade GUI.
411140	Fixed an issue that caused HA heartbeat packets to be lost during normal operation. The same issue would cause traffic loss during firmware upgrades.
442333	Fixed a DP processor routing table driver memory leak.
423649	Fixed an issue that caused FortiController sessions to be displayed as out of sync.
442127	New GUI pages added for uploading and managing SSL certificates used for administrator sessions.
480380	Fixed an issue that prevented FortiController from forwarding IS-IS Ethertypes in L2 mode.
484281	Fixed an issue that caused the FortiController to discard VDOM information from the DP processor routing table, resulting in asymmetric routing errors.
490993	Fixed an issue that sometimes caused the FortiController to forward multicast traffic to all workers even though no the configuration did not include multicast flow rules.

Common vulnerabilities and exposures

Bug ID	Description
470966	FortiController 5.2.6 is no longer vulnerable to the following CVE references: CVE-2017-3737 CVE-2017-3738

Known Issues

The following known issues have been identified with 5.2.6. 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`