



# FortiSwitch ATCA - Release Notes

**VERSION v5.2.0**

**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](mailto:techdocs@fortinet.com)



April 22, 2015

FortiSwitch ATCA v5.2.0 Release Notes

11-520-261933-20150422

# TABLE OF CONTENTS



<b>Change Log</b> .....	<b>4</b>
<b>Introduction</b> .....	<b>5</b>
Supported models .....	5
What's new in v5.2 .....	5
<b>Special Notices</b> .....	<b>6</b>
General .....	6
FG-5001D operating in FortiController or Dual FortiController mode .....	6
<b>Upgrade Information</b> .....	<b>7</b>
Upgrading from FortiSwitch-ATCA v5.0.5 or earlier .....	7
Upgrading from FortiSwitch-ATCA v5.0.6 or later .....	7
Downgrading to previous firmware versions .....	7
Firmware image checksums .....	7
<b>Product Integration and Support</b> .....	<b>8</b>
FortiSwitch-ATCA v5.2.0 support .....	8
<b>Resolved Issues</b> .....	<b>9</b>
<b>Known Issues</b> .....	<b>10</b>

# Change Log

Date	Change Description
2014-12-02	Initial release.
2015-02-13	Added FTCL-5913C to supported models.
2015-04-22	Updated Upgrade Information chapter.

# Introduction

This document provides the following information for FortiSwitch-ATCA v5.2.0 build 0128:

- [Supported models](#)
- [Special Notices](#)
- [Upgrade Information](#)
- [Product Integration and Support](#)
- [Resolved Issues](#)
- [Known Issues](#)

See the [Fortinet Document Library](#) for FortiSwitch-ATCA documentation.

## Supported models

FortiSwitch-ATCA v5.2.0 supports the following models:

**FortiController**

FTCL-5103B, FTCL-5903C, FTCL-5913C

## What's new in v5.2

The following is a list of enhancements in v5.2:

- FortiController 5903C support
- FortiController 5913C support

# 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 v5.0.7 (build 4625) to FortiOS v5.2.2, you may experience a back-plane interface connection issue. This is due to a change to the ELBC interface mapping ID. After the upgrade, you will need to perform a factory reset and then re-configure the device.

# Upgrade Information

## Upgrading from FortiSwitch-ATCA v5.0.5 or earlier

FortiController units running v5.0.5 or earlier must first upgrade to v5.0.6 or later prior to upgrading to v5.2.0 in order to receive a necessary update to the FPGA firmware.

## Upgrading from FortiSwitch-ATCA v5.0.6 or later

FortiSwitch-ATCA v5.2.0 introduces an enhanced heartbeat packet that contains more information. As a result, users must upgrade their FortiGate blades from FortiOS v5.0.x to v5.2.3 or later before upgrading their FortiController units from FortiSwitch ATCA v5.0.6 or later to v5.2.0.

## Downgrading to previous firmware versions

Downgrading from FortiSwitch-ATCA v5.2.0 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

## FortiSwitch-ATCA v5.2.0 support

The following table lists v5.2.0 product integration and support information.

<b>Web browser</b>	<ul style="list-style-type: none"><li>• Microsoft Internet Explorer version 10</li><li>• Mozilla Firefox version 33</li><li>• Google Chrome version 37</li></ul> <p>Other web browsers may function correctly, but are not supported by Fortinet.</p>
<b>FortiOS</b>	<ul style="list-style-type: none"><li>• v5.2.2 and later</li><li>• v5.0.9 and later</li></ul>

## Resolved Issues

The following issues have been fixed in v5.2.0. For inquiries about a particular bug, please contact [Customer Service & Support](#).

Bug ID	Description
0255452	UDP traffic used by IKE NAT-T is load-balanced to multiple blades in SLBC, preventing tunnel from getting established.

# Known Issues

The following issues have been identified with v5.2.0. For inquires about a particular bug or to report a bug, please contact [Fortinet Customer Service & Support](#).

Bug ID	Description
0246369	FortiController 5903C/5913C do not currently support IPsec VPN traffic.
0246422	<p>Random connection issue on backplane interfaces.</p> <p>Workaround:</p> <p>When back-plane connections are 10G:</p> <ul style="list-style-type: none"><li>• On the FortiGate: Enforce the interface speed of elbc-ctrl/1 and elbc-ctrl/2 to 10000full.</li><li>• On the FortiController 5903C/5913C: enable fabric-backplane-port-10g-mode in global setting.</li></ul> <p>When back-plane connections are 40G:</p> <ul style="list-style-type: none"><li>• On the FortiGate: Enforce the interface speed of elbc-ctrl/1 and elbc-ctrl/2 to 40000full.</li><li>• On the FortiController 5903C/5913C: disable fabric-backplane-port-10g-mode in global setting and then enforce the related fabric-channel physical ports to 40000full.</li></ul>
0259215	The traffic log is not accurate.
0261570	<p>After FortiGates have finished the graceful upgrade, FortiController fails to perform graceful upgrade in chassis redundancy mode.</p> <p>Workaround:</p> <p>Use the diagnose system ha force-slave-state clear CLI command to clear the force-slave mode on the master FortiController after all FortiGates have finished upgrading.</p>
0264621	Neither the static nor LACP trunks are supported by the FortiController 5913C.



Copyright© 2015 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.