



FortiSwitch ATCA - Release Notes

VERSION v5.0.6

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



April 24, 2015

FortiSwitch ATCA v5.0.6 Release Notes

11-520-276410-20150424

TABLE OF CONTENTS



Change Log	4
Introduction	5
Supported models	5
What's new in v5.0.6	5
Special Notices	6
General	6
	6
Upgrade Information	7
Upgrading from FortiSwitch-ATCA v5.0.3 or later	7
Upgrading from FortiSwitch-ATCA v4.3.3 or later	7
ELBC v3 cluster upgrades	7
Downgrading to previous firmware versions	7
Firmware image checksums	8
Product Integration and Support	9
FortiSwitch-ATCA v5.0.6 support	9
Resolved Issues	10
Known Issues	11

Change Log

Date	Change Description
2014-04-24	Initial release.

Introduction

This document provides the following information for FortiSwitch-ATCA v5.0.6 build 0034:

- [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 v5.0.6 supports the following models:

FortiSwitch	FS-5003A, FS-5003B and FCTL-5103B
--------------------	-----------------------------------

What's new in v5.0.6

The following is a list of enhancements in v5.0.6:

- SNMPv3 support
- Added `forward-rule` to allow sending traffic to specific slots

Special Notices

General

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

Upgrade Information

Upgrading from FortiSwitch-ATCA v5.0.3 or later

FortiSwitch ATCA v5.0.6 supports upgrade from v5.0.3 or later.

Upgrading from FortiSwitch-ATCA v4.3.3 or later

FortiSwitch ATCA v5.0.6 supports upgrade from v4.3.3 or later.

ELBC v3 cluster upgrades

To upgrade an ELBCv3 cluster from FortiSwitch-ATCA v4.3 to v5.0.6, the following procedure is advised:

1. Upgrade your FortiSwitch-ATCA and FortiGate devices to the latest v4.3 firmware release. For more information, see the [FortiOS 4.0 MR3 Release Notes](#) for the upgrade procedure.
2. Disable the graceful upgrade feature on your FortiSwitch-ATCA devices using the following CLI command:

```
config system ha
  set graceful-upgrade disable
end
```



FortiGate supports graceful upgrade from FortiOS v4.3 to FortiOS v5.0. You do not need to disable this feature on your FortiGate devices.

3. Load the FortiGate v5.0 image to the ELBC master FortiGate.
4. Wait until all FortiGates have completed the upgrade. You may use the CLI command `diagnose system ha force-slave-state` to trigger chassis HA fail-over during the FortiGate upgrade if you have a dual chassis setup.
5. Load the FortiSwitch-ATCA v5.0.5 image to the master device.
6. All devices will start to upgrade simultaneously. You will experience a traffic interruption during this time.
7. After all devices have completed the upgrade you can re-enable the graceful upgrade feature using the following CLI command:

```
config system ha
  set graceful-upgrade enable
end
```

Downgrading to previous firmware versions

Downgrading from FortiSwitch-ATCA v5.0.6 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

FortiSwitch-ATCA v5.0.6 support

The following table lists v5.0.6 product integration and support information.

Web browser	<ul style="list-style-type: none">• Microsoft Internet Explorer version 10• Mozilla Firefox version 33• Google Chrome version 37 <p>Other web browsers may function correctly, but are not supported by Fortinet.</p>
FortiOS	<ul style="list-style-type: none">• 5.0.8 and later• 5.2.1 and later

Resolved Issues

The following issues have been fixed in v5.0.6. For inquiries about a particular bug, please contact [Customer Service & Support](#).

NTP

Bug ID	Description
264304	NTP settings may cause a <code>confsync</code> failure.

Upgrade

Bug ID	Description
256157	Improved handling of FPGA upgrade to prevent FPGA upgrading failure.

Known Issues

The following issues have been identified with v5.0.6. For inquires about a particular bug or to report a bug, please contact [Fortinet Customer Service & Support](#).

IPv6

Bug ID	Description
265591	IPv6 address is not supported by the <code>forward-rule</code> .



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.