



# 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

|  |           |
|--|-----------|
| <b>Change log</b> .....  | <b>4</b>  |
| <b>Introduction</b> .....  | <b>5</b>  |
| Supported models.....  | 5         |
| <b>Special Notices</b> .....   | <b>6</b>  |
| General.....   | 6         |
| FortiGate-5001D operating in FortiController or Dual FortiController mode..... | 6         |
| <b>Upgrade Information</b> .....   | <b>7</b>  |
| Upgrading from FortiController-5000 5.2.5.....                                 | 7         |
| Downgrading to previous firmware versions.....                                 | 7         |
| Firmware image checksums.....  | 7         |
| <b>Product Integration and Support</b> .....                                   | <b>8</b>  |
| FortiController-5000 5.2.7 support.....  | 8         |
| <b>Resolved Issues</b> .....   | <b>9</b>  |
| <b>Known Issues</b> .....  | <b>10</b> |

# 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:

|                        |                                      |
|------------------------|--------------------------------------|
| <b>FortiController</b> | 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.

|                    |   |
|--------------------|---|
| <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>• 5.2.10 and later</li></ul>  |

# Resolved Issues

The following issues have been fixed in FortiController-5000 5.2.7. For inquiries 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 inquiries about a particular bug or to report a bug, please contact [Fortinet Customer Service & Support](#).

| Bug ID | Description  |
|--------|--|
| 483105 | <p>SHA1 weak certificate signature may be vulnerable. This certificate encrypts HTTPS administrator login sessions.</p> <p><b>Workaround:</b></p> <p>Upload your own more secure certificate from the GUI:</p> <ol style="list-style-type: none"><li>1. Go to <b>System &gt; Certificate &gt; Import &gt; Import Certificate</b>.</li><li>2. Under <i>Certificate file (*.cert)</i>, select the certificate to import.</li><li>3. Under <i>Key file (*.key)</i>, select the key for import.</li></ol> <p>Upload your own certificate from the CLI:</p> <pre>execute user certificate upload tftp &lt;file.crt&gt; &lt;file.key&gt; &lt;tftp_ipv4&gt;</pre> <p>Use this certificate instead of the default certificate. To activate your certificate, use the following CLI commands:</p> <pre>config system global   set admin-server-cert &lt;cert&gt;   set strong-crypto enable end</pre> |



**FORTINET®**



Copyright© (Undefined variable: FortinetVariables.Copyright Year) 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.