

FortiVoice™ Phone System Release Notes

VERSION 5.3.1 GA

FORTINET TDOCUMENT 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>

FORTINET 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



July 22, 2016

FortiVoice™ 5.3.1 GA Release Notes

TABLE OF CONTENTS

Introduction	5
Supported Platforms	5
Special Notices	6
TFTP firmware install	6
Monitor settings for web UI	6
Recommended web browsers	6
Firmware Upgrade/Downgrade	7
Before and after any firmware upgrade/downgrade	7
Upgrade path for FVE-200D and 200D-T	7
For any older 2.x.x/3.0.x/4.0.x release	7
For any older 5.0.x release prior to 5.0.5	7
For 5.0.5 release	7
Upgrade path for FVE-2000E-T2	7
For any older 3.0.x/4.0.x release	7
For any older 5.0.x release prior to 5.0.5	8
For 5.0.5 release	8
Upgrade path for other FVE models	8
For any older 5.0.x release	8
For 5.0.5 release	8
Firmware downgrade for FVE-200D and 200D-T	8
Downgrading from 5.3.1 to 5.0.x release	8
Downgrading from 5.3.1 to 4.0.x/3.0.x/2.0.x release	9
Firmware downgrade for FVE-2000E-T2	9
Downgrading from 5.3.1 to 5.0.x release	9
Downgrading from 5.3.1 to 4.0.x release	9
Downgrading from 5.3.1 to 3.0.x release	9
Firmware downgrade for other FVE models	10
Downgrading from 5.3.1 to 5.0.x release	10
Resolved issues	11

Image checksums 12

Introduction

This document provides a list of new and changed features, upgrade instructions and caveats, resolved issues, and known issues for FortiVoice release 5.3.1, build0288.

Supported Platforms

FortiVoice 5.3.1 release supports the following platforms:

- FVE-20E2 & FVE-20E4
- FVE-100E
- FVE-300E-T
- FVE-500E-T2
- FVE-1000E
- FVE-1000E-T
- FVE-2000E-T2 (compatible with FVC 2000E-T2)
- FVE-3000E
- FVE-VM (VMware vSphere Hypervisor ESX/ESXi 5.0 and higher)
- FVE-VM (Microsoft Hyper-V Server 2008 R2 and 2012)
- FVE-VM (KVM qemu 0.12.1)
- FVE-VM (Citrix XenServer v5.6sp2, 6.0 and higher)

Old platforms:

- FVE 200D
- FVE 200D-T

Special Notices

TFTP firmware install

Using TFTP via the serial console to install firmware during system boot time will erase all current FortiVoice configurations and replace them with factory default settings.

Monitor settings for web UI

To view all objects in the web UI properly, Fortinet recommends setting your monitor to a screen resolution of at least 1280x1024.

Recommended web browsers

- Internet Explorer 7 or higher
- Firefox 3.5 or higher
- Safari 4 or higher
- Adobe Flash Player 9 or higher plug-in required to display statistics charts

Firmware Upgrade/Downgrade

Before and after any firmware upgrade/downgrade

- Before any firmware upgrade/downgrade, save a copy of your FortiVoice configuration (including replacement messages and user data) by going to System > Maintenance > Configuration.
- After any firmware upgrade/downgrade, if you are using the web UI, clear the browser cache prior to login on the FortiVoice unit to ensure proper display of the web UI screens.

Upgrade path for FVE-200D and 200D-T

For any older 2.x.x/3.0.x/4.0.x release

Any 2.x.x/3.0.x/4.0.x release



5.0.5 (Build 0188)



5.3.1 (Build 0288)

For any older 5.0.x release prior to 5.0.5

Any 5.0.x release



5.0.5 (Build 0188)



5.3.1 (Build 0288)

For 5.0.5 release

5.0.5 (Build 0188)



5.3.1 (Build 0288)

After every upgrade, verify that the build number and version number match the image that was loaded. To do so, go to *Status > Dashboard > Dashboard*.

Upgrade path for FVE-2000E-T2

For any older 3.0.x/4.0.x release

Any 3.0.x/4.0.x release



4.0.2 (200D firmware, Build 0229)

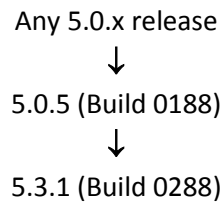


5.0.5 (Build 0188)

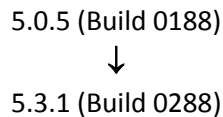


5.3.1 (2000E firmware, Build 0288)

For any older 5.0.x release prior to 5.0.5



For 5.0.5 release

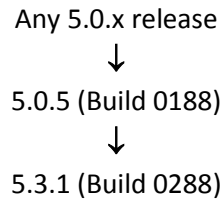


After every upgrade, verify that the build number and version number match the image that was loaded. To do so, go to *Status > Dashboard > Dashboard*.

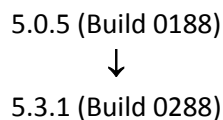
Note: For FortiVoice 2000E-T2 with serial number prefix of FO2HDD, if upgrade is done through "G" option of boot loader, FVE-200D platform image should be used.

Upgrade path for other FVE models

For any older 5.0.x release



For 5.0.5 release



After every upgrade, verify that the build number and version number match the image that was loaded. To do so, go to *Status > Dashboard > Dashboard*.

Firmware downgrade for FVE-200D and 200D-T

Firmware downgrade is not recommended. Before downgrading, consult Fortinet Technical Support first.

Downgrading from 5.3.1 to 5.0.x release

Downgrading from 5.3.1 to 5.0.x release is not fully supported and may cause data loss. If you have to downgrade, follow these steps:

1. Back up the 5.3.1 configuration.
2. Install the older 5.0.x.
3. In the CLI, enter `execute factoryreset` to reset the FortiVoice unit to factory defaults. Note that you will lose all of the FortiVoice configurations by doing so.

4. Configure the device IP address and other network settings.
5. Reload the 5.0.x backup configuration saved before upgrading to 5.3.1.

Downgrading from 5.3.1 to 4.0.x/3.0.x/2.0.x release

Downgrading from 5.3.1 to 4.0.x/3.0.x/2.0.x release is not fully supported and may cause data loss. If you have to downgrade, follow these steps:

6. Back up the 5.3.1 configuration.
7. Install the older 4.0.x/3.0.x/2.0.x image.
8. In the CLI, enter `execute factoryreset` to reset the FortiVoice unit to factory defaults. Note that you will lose all of the FortiVoice configurations by doing so.
9. Configure the device IP address and other network settings.
10. Reload the 4.0.x/3.0.x/2.0.x backup configuration saved before upgrading to 5.3.1.

Firmware downgrade for FVE-2000E-T2

Firmware downgrade is not recommended. Before downgrading, consult Fortinet Technical Support first.

Downgrading from 5.3.1 to 5.0.x release

Downgrading from 5.3.1 to 5.0.x release is not fully supported and may cause data loss. If you have to downgrade, follow these steps:

1. Back up the 5.3.1 configuration.
2. Install the older 5.0.x.
3. In the CLI, enter `execute factoryreset` to reset the FortiVoice unit to factory defaults. Note that you will lose all of the FortiVoice configurations by doing so.
4. Configure the device IP address and other network settings.
5. Reload the 5.0.x backup configuration saved before upgrading to 5.3.1.

Downgrading from 5.3.1 to 4.0.x release

Downgrading from 5.3.1 to 4.0.x release is not fully supported and may cause data loss. If you have to downgrade, follow these steps:

1. Back up the 5.3.1 configuration.
2. Install the older 4.0.2 image.
3. Back up the 4.0.2 configuration.
4. Install the older 4.0.x image.
5. In the CLI, enter `execute factoryreset` to reset the FortiVoice unit to factory defaults. Note that you will lose all of the FortiVoice configurations by doing so.
6. Configure the device IP address and other network settings.
7. Reload the 4.0.x backup configuration saved before upgrading to 5.3.1.

Downgrading from 5.3.1 to 3.0.x release

Downgrading from 5.3.1 to 3.0.x release is not fully supported and may cause data loss. If you have to downgrade, follow these steps:

1. Back up the 5.3.1 configuration.
2. Install the older 4.0.2 image.

3. Back up the 4.0.2 configuration.
4. Install the older 3.0.x image.
5. In the CLI, enter `execute factoryreset` to reset the FortiVoice unit to factory defaults. Note that you will lose all of the FortiVoice configurations by doing so.
6. Configure the device IP address and other network settings.
7. Reload the 3.0.x backup configuration saved before upgrading to 5.3.1.

Firmware downgrade for other FVE models

Firmware downgrade is not recommended. Before downgrading, consult Fortinet Technical Support first.

Downgrading from 5.3.1 to 5.0.x release

Downgrading from 5.3.1 to 5.0.x release is not fully supported and may cause data loss. If you have to downgrade, follow these steps:

1. Back up the 5.3.1 configuration.
2. Install the older 5.0.x.
3. In the CLI, enter `execute factoryreset` to reset the FortiVoice unit to factory defaults. Note that you will lose all of the FortiVoice configurations by doing so.
4. Configure the device IP address and other network settings.
5. Reload the 5.0.x backup configuration saved before upgrading to 5.3.1.

Resolved issues

The resolved issues listed below do not list every bug that has been corrected with this release. For inquires about a particular bug, please contact [Fortinet Customer Service & Support](#).

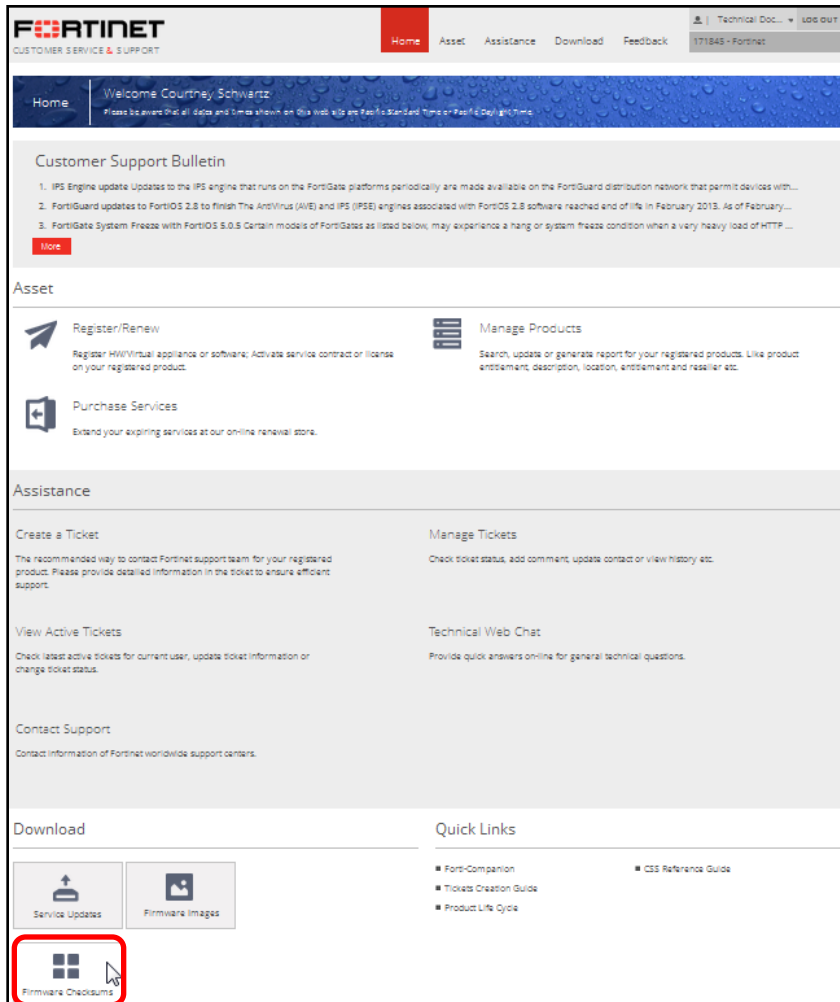
Bug ID	Description
381022	Interfaces are lost after upgrading from v5.0.0 to v5.3.0 on some old FVE 2000E-T2 platforms.
380822	Upgrade from v5.0.5 to v5.3.0 fails for systems with customized system speed dial pattern.
379937	Extension will not ring when being part of ring group if auxiliary device is programmed.
380127	DSS keys with line/extension appearance are configured with wrong labels.
366549	There is no state information for office peer using IAX.
379934	Email relay host test is not working as expected.

Image checksums

To verify the integrity of the firmware file, use a checksum tool and compute the firmware file's MD5 checksum. Compare it with the checksum indicated by Fortinet. If the checksums match, the file is intact.

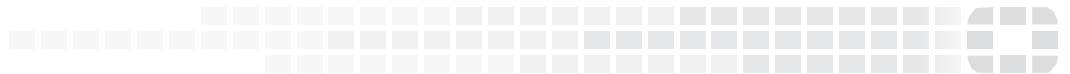
MD5 checksums for Fortinet software and firmware releases are available from [Fortinet Customer Service & Support](#). After logging in to the web site, near the bottom of the page, select the *Firmware Image Checksums* button. (The button appears only if one or more of your devices have a current support contract.) In the File Name field, enter the firmware image file name including its extension, then select *Get Checksum Code*.

Figure 1: Customer Service & Support image checksum tool



FORTINET

High Performance Network Security



Copyright© 2016 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.