



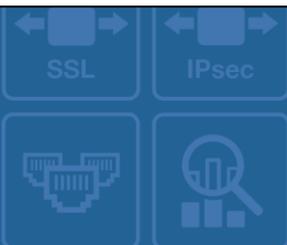
**FORTINET**

High Performance Network Security



# FortiVoice™ Phone System Release Notes

VERSION 5.3.14 GA



**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>

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



July 11, 2018

FortiVoice™ Phone System 5.3.14 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
What's New .....	7
iOS Softclient support .....	7
Android softclient support .....	7
Jitter Buffer support .....	7
Firmware Upgrade/Downgrade .....	8
Before and after any firmware upgrade/downgrade .....	8
Upgrade path for FVE-200D and 200D-T .....	8
For any older 2.x.x/3.0.x/4.0.x release .....	8
For any older 5.0.x release prior to 5.0.5 .....	8
For 5.0.5 and 5.3.x release .....	8
Upgrade path for FVE-2000E-T2 .....	8
For any older 3.0.x/4.0.x release .....	8
For any older 5.0.x release prior to 5.0.5 .....	9
For 5.0.5 and 5.3.x release .....	9
Upgrade path for other FVE models .....	9
For any older 5.0.x release .....	9
For 5.0.5 and 5.3.x release .....	9
Firmware downgrade for FVE-200D and 200D-T .....	9
Downgrading from 5.3.14 to 5.x.x release .....	9
Downgrading from 5.3.14 to 4.0.x/3.0.x/2.0.x release .....	10
Firmware downgrade for FVE-2000E-T2 .....	10
Downgrading from 5.3.14 to 5.x.x release .....	10
Downgrading from 5.3.14 to 4.0.x release .....	10
Downgrading from 5.3.14 to 3.0.x release .....	10
Firmware downgrade for other FVE models .....	11

Downgrading from 5.3.14 to 5.x.x release .....	11
Resolved issues .....	12
Image Checksums .....	14

# Introduction

This document provides a list of new and changed features, upgrade instructions and caveats, resolved issues, and known issues for FortiVoice release 5.3.14, build0386.

## Supported Platforms

FortiVoice 5.3.14 release supports the following platforms:

- FVE-20E2 & FVE-20E4
- FVE-50E6
- FVE-100E
- FVE-200F
- 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 and later)
- FVE-VM (Citrix XenServer v5.6sp2, 6.0 and higher)
- FVE-VM [AWS (BYOL)]
- FVE-VM [Azure (BYOL)]
- FVG-GO08
- FVG-GS16
- FVG-GT01
- FVG-GT02

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 11 and Edge 40, 41
- Firefox 52.7.2 ESR, 59
- Safari 10, 11
- Chrome 65
- Adobe Flash Player 9 or higher plug-in required to display statistics charts

# What's New

The following list highlights some of the new features or enhancements introduced in the FortiVoice Phone System 5.3.14 release. For more information, see the FortiVoice Phone System Administration Guide.

## iOS Softclient support

FortiFone iOS Softclient for the iPhone is supported. This new application enables enterprise mobility for FortiVoice phone system users, and provides an essential feature-set such as Visual Voicemail, Contacts, and Call History to simplify how users make and receive calls.

## Android softclient support

Introducing new push notification framework to support Google Firebase Cloud Messaging (FCM). FCM provides a more reliable and battery-efficient implementation to deliver call events to the FortiFone Softclient running on Android or iOS mobile platforms.

## Jitter Buffer support

Jitter Buffering is supported on the FortiVoice phone system to better handle network and device impairment conditions, especially when using IP SIP phones or softphones from external networks to make or receive calls using PSTN lines.

Use the following CLI to configure jitter buffer support:

```
config system advanced-config
set jitter-buffer-receive-status sip pstn set jitter-buffer-max-size 200 end
```

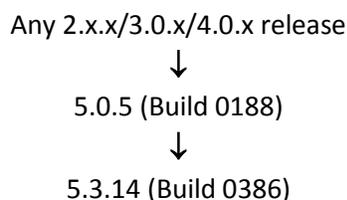
# Firmware Upgrade/Downgrade

## Before and after any firmware upgrade/downgrade

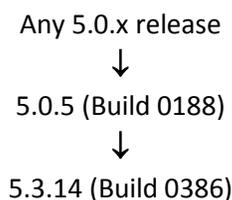
- Before any firmware upgrade/downgrade, save a copy of your FortiVoice configuration (including replacement messages and user data) by going to System > Maintenance > Configuration.
- After any firmware upgrade/downgrade, if you are using the web UI, clear the browser cache prior to login on the FortiVoice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

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

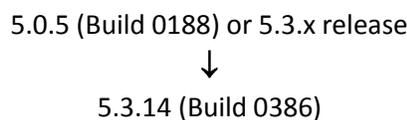
### For any older 2.x.x/3.0.x/4.0.x release



### For any older 5.0.x release prior to 5.0.5



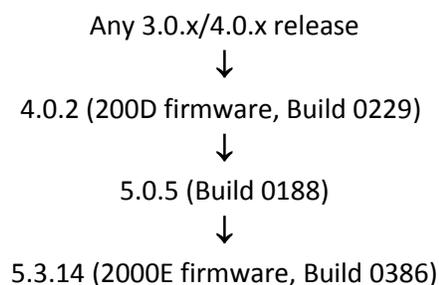
### For 5.0.5 and 5.3.x release



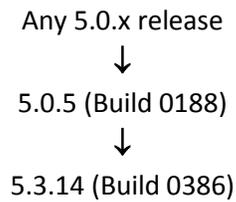
After every upgrade, verify that the build number and version number match the image that was loaded. To do so, go to *Status > Dashboard > Dashboard*.

## Upgrade path for FVE-2000E-T2

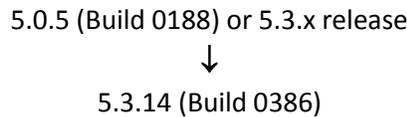
### For any older 3.0.x/4.0.x release



#### For any older 5.0.x release prior to 5.0.5



#### For 5.0.5 and 5.3.x release

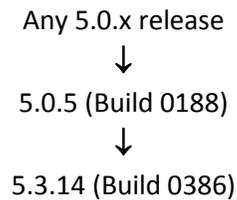


After every upgrade, verify that the build number and version number match the image that was loaded. To do so, go to *Status > Dashboard > Dashboard*.

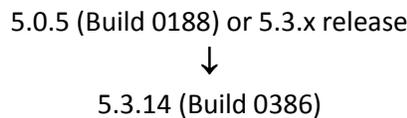
**Note:** For FortiVoice 2000E-T2 with serial number prefix of FO2HDD, if upgrade is done through "G" option of boot loader, FVE-200D platform image should be used.

## Upgrade path for other FVE models

#### For any older 5.0.x release



#### For 5.0.5 and 5.3.x 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 5.3.14 to 5.x.x release

Downgrading from 5.3.14 to 5.x.x release is not fully supported and may cause data loss. If you have to downgrade, follow these steps:

1. Back up the 5.3.14 configuration.
2. Install the older 5.x.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.x.x backup configuration saved before upgrading to 5.3.14.

### Downgrading from 5.3.14 to 4.0.x/3.0.x/2.0.x release

Downgrading from 5.3.14 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:

1. Back up the 5.3.14 configuration.
2. Install the older 4.0.x/3.0.x/2.0.x image.
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 4.0.x/3.0.x/2.0.x backup configuration saved before upgrading to 5.3.14.

## Firmware downgrade for FVE-2000E-T2

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

### Downgrading from 5.3.14 to 5.x.x release

Downgrading from 5.3.14 to 5.x.x release is not fully supported and may cause data loss. If you have to downgrade, follow these steps:

1. Back up the 5.3.14 configuration.
2. Install the older 5.x.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.x.x backup configuration saved before upgrading to 5.3.14.

### Downgrading from 5.3.14 to 4.0.x release

Downgrading from 5.3.14 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 5.3.14 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 5.3.14.

### Downgrading from 5.3.14 to 3.0.x release

Downgrading from 5.3.14 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 5.3.14 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 5.3.14.

## Firmware downgrade for other FVE models

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

### Downgrading from 5.3.14 to 5.x.x release

Downgrading from 5.3.14 to 5.x.x release is not fully supported and may cause data loss. If you have to downgrade, follow these steps:

1. Back up the 5.3.14 configuration.
2. Install the older 5.x.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.x.x backup configuration saved before upgrading to 5.3.14.

## Resolved issues

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

Bug ID	Description
498788	Enhancement to Call Reports to support Virtual Number queries.
480799	Enhancement to User Call Handling to support selective call routing based on schedule or type of call.
492357	Enhancement to Agent Console's call Pickup (Waiting Caller) function to provide better user experience.
437800	Enhancement to Call Center Reporting to reflect call transfers from Agent Console.
477401	Enhancement to Access Control to provide System Directory for FortiPhones only.
447012	Provide the ability to set a priority queue for agents who sign into multiple queues.
489314	Provide separate parameter settings for QR Code and Voicemail expiry timers.
450773	Provide more precise statistics for Queue Agent summary.
477947	Provide support for new FON475 phones.
477482	Provide function in Agent Console to allow users to manually override Wrap-Up time when ready to receive calls.
297334	Provide Wrap-Up timer display in Agent Console.
497413	Provide FortiVoice Survivability support for H25 phones.
497596	Provide FortiVoice Survivability support for C70/C71 conference phones.
477950	Provide FortiVoice Survivability support for FON-870 phones.
495552	Extend line appearance support for Managed Gateways.
498457	Increase the maximum number of DHCP servers supported on the respective FortiVoice platforms.
493860	Call Center console displays incorrect Agent status on logout.
492061	Configuring overflow call handling in Call Queue generates error pop-up message.
495624	Missing PAI header in 180 Ringing message when the called extension is configured with an auxiliary device using a SoftClient phone type.
494112	Configuring General Voicemail greeting generates error pop-up message.
493251	Cannot add members to an existing department or a new department.
495866	CDR upload to restful service misses call leg when call is transferred.
497402	Voicemail deletion from Web console generates an out-of-sync MWI condition on phone.

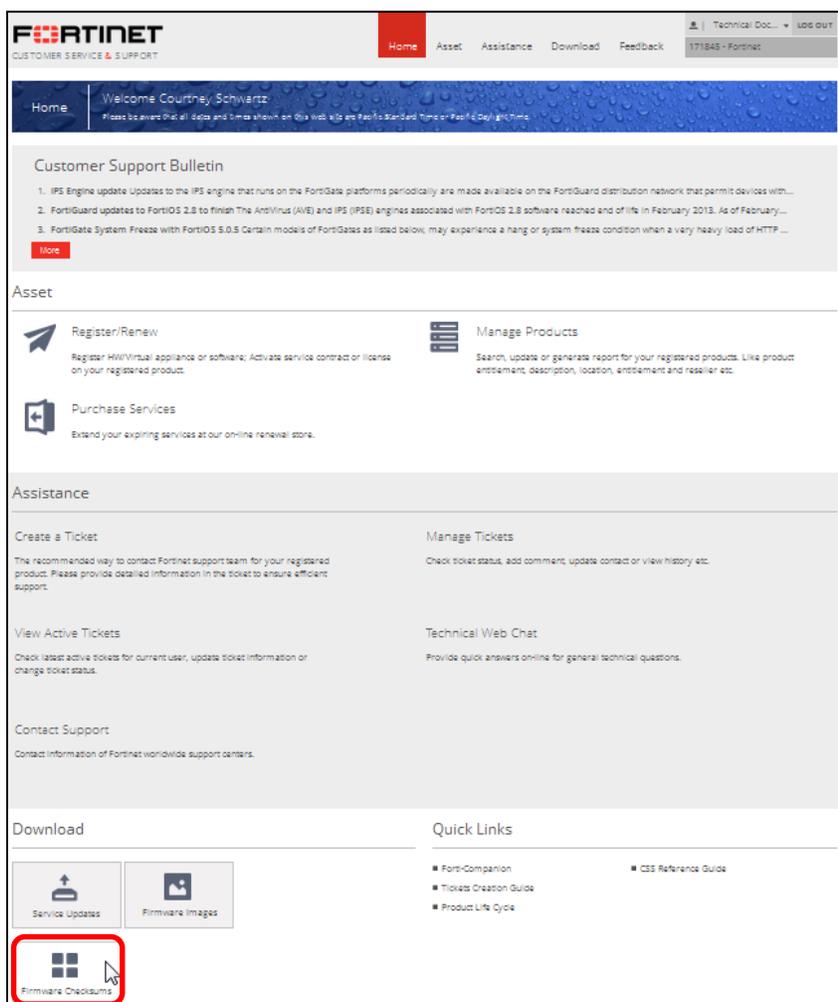
Bug ID	Description
492925	Display name change when extension is disabled/enabled does not reflect changes in system/user portal directories.
493552	Queue Callback feature fails to route call when Caller ID formatting is enabled.
489583	HTML report has issue if a second report is generated within a minute.
492701	System callback feature ends call after callback is answered and prompt plays.
489312	In Agent Call Summary Report, report format/structure is inconsistent based on agent queue membership.
497927	FortiFone-375i fails to register when phone "Display Name" field contains double quote character(s).
499103	CDR Disposition is not accurate when voicemail call handling is configured.
501755	System does not follow holiday schedule and does not revert back to the original schedule the following day.
439222	"Apply to All" does not change the profiles on any of the selected extensions when using Batch Edit.
491405	Agent Summary Report does not match Agent Activity detail report.
492995	Agent skill set changes are not applied to database.
497146	Paging Group prompts to "Please add at least one member" when trying to edit.
492365	When enabling the checkbox for the queue entry announcement, all of the recordings are grayed out.
462220	In Call Reporting, Agent Detail report misses log out information.
496874	Downloaded CSV files first cell has changed from "No" to "Id" and this creates an error.
497143	Department drop down list misses the "None" option.
496742	Calls cannot be completed when "Call Restriction" is set to "Allow with personal code" or "Allow with account code".
444106	Follow Me incorrectly uses multiple trunks when routing calls.
490901	Call Center Queue Agent selection list incorrectly displays members in both list when selected.

# 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





Copyright© 2018 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.