FortiVoice™ Phone System Release Notes

VERSION 5.3.4 GA

FORTINE 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

November 9, 2016

FortiVoice™ 5.3.4 GA Release Notes

TABLE OF CONTENTS

Introduction

This document provides a list of new and changed features, upgrade instructions and caveats, resolved issues, and known issues for FortiVoice release 5.3.4, build0317.

Supported Platforms

FortiVoice 5.3.4 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 and later)
- FVE-VM (Citrix XenServer v5.6sp2, 6.0 and higher)

Old platforms:

- FVE-200D
- FVE-200D-T

What's New

The following list highlights some of the new features or enhancements introduced in the FortiVoice Phone System 5.3.4 release. For more information, see the FortiVoice Phone System Administration Guide.

New phones

FortiFone-375 and FortiFone-H25 are supported.

New virtual machine offerings

FVE-VM-1000, FVE-VM-3000, FVE-VM-5000 and FVE-VM-10000 are introduced to support more extensions.

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)

↓

5.3.4 (Build 0317)

For any older 5.0.x release prior to 5.0.5

Any 5.0.x release

↓

5.0.5 (Build 0188)

↓

5.3.4 (Build 0317)

For 5.0.5 and 5.3.x release

5.0.5 (Build 0188) or 5.3.x release

↓

5.3.4 (Build 0317)

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)

↓

5.3.4 (2000E firmware, Build 0317)

For any older 5.0.x release prior to 5.0.5

Any 5.0.x release
↓
5.0.5 (Build 0188)
↓
5.3.4 (Build 0317)

For 5.0.5 and 5.3.x release

5.0.5 (Build 0188) or 5.3.x release
↓
5.3.4 (Build 0317)

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

Any 5.0.x release
↓
5.0.5 (Build 0188)
↓
5.3.4 (Build 0317)

For 5.0.5 and 5.3.x release

5.0.5 (Build 0188) or 5.3.x release
↓
5.3.4 (Build 0317)

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 5.3.4 to 5.x.x release

Downgrading from 5.3.4 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 5.3.4 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 5.3.4.

Downgrading from 5.3.4 to 4.0.x/3.0.x/2.0.x release

Downgrading from 5.3.4 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 5.3.4 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 5.3.4.

Firmware downgrade for FVE-2000E-T2

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

Downgrading from 5.3.4 to 5.x.x release

Downgrading from 5.3.4 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 5.3.4 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 5.3.4.

Downgrading from 5.3.4 to 4.0.x release

Downgrading from 5.3.4 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 5.3.4 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 5.3.4.

Downgrading from 5.3.4 to 3.0.x release

Downgrading from 5.3.4 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 5.3.4 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 5.3.4.

Firmware downgrade for other FVE models

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

Downgrading from 5.3.4 to 5.x.x release

Downgrading from 5.3.4 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 5.3.4 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 5.3.4.

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
374517	FortiFone-370i with 2x FF-70E becomes unresponsive.
389889	FortiFone -870i configuration files are not populated with extension details.
389915	FortiFone-870i phone time is one hour off.
366728	Retaining original caller ID setting does not save.
381721	Virtual number call handling is overridden by local extension call handling.
393468	*63 and *64 feature codes have no feedback from TTS.
386088	Personal recording (*3) does not work when calls are routed to Ring Group.
389709	When hot-desking into an extension configured for French language profile, the hot desk prompts are a mixture of English and French.
395042	User web portal is accessible on FVE-20E when user privilege is set to none.
393111	An error appears when trying to load logo onto FVE-20E.
390079	An error appears when adding an extension with auxiliary SIP device to a User Group.
387395	Request to add Call Center configuration review option.
389242	Exception handling does not work properly if restful query times out.
388876	Call Center agent detail reports show inaccurate call time.
388878	Query for "outbound calls per hour" option is requested.
385866	On Waiting Caller widget, all agents are able to view queued callers for queues that the agent is not a member of.

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