FORTINET

High Performance Network Security

FortiVoice™ Phone System Release Notes

VERSION 5.3.9 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

November 9, 2017

FortiVoice™ Phone System 5.3.9 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 5.3.9, build0362.

Supported Platforms

FortiVoice 5.3.9 release supports the following platforms:

- FVE-20E2 & FVE-20E4
- FVE-50E6
- 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)
- AWS
- Azure
- FVG-GO08
- FVG-GS16

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 5.3.9 release. For more information, see the FortiVoice Phone System Administration Guide.

Reports

Call reports are enhanced by adding new reports on account code, extensions, lines, number search, queue ring Time, and Top30.

Phone management

Phone management for phone firmware is enhanced by adding the ability to distinguish different hardware revisions.

Operator console

Support operator console for FVE-20E/50E/VM50.

Auto attendant

Support changing auto attendant greetings remotely by phone.

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)

↓

5.3.9 (Build 0362)

For any older 5.0.x release prior to 5.0.5

Any 5.0.x release

↓

5.0.5 (Build 0188)

↓

5.3.9 (Build 0362)

For 5.0.5 and 5.3.x release

5.0.5 (Build 0188) or 5.3.x release

↓

5.3.9 (Build 0362)

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)

↓

5.3.9 (2000E firmware, Build 0362)

For any older 5.0.x release prior to 5.0.5

Any 5.0.x release

↓

5.0.5 (Build 0188)

↓

5.3.9 (Build 0362)

For 5.0.5 and 5.3.x release

5.0.5 (Build 0188) or 5.3.x release

↓

5.3.9 (Build 0362)

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)

↓

5.3.9 (Build 0362)

For 5.0.5 and 5.3.x release

5.0.5 (Build 0188) or 5.3.x release

↓

5.3.9 (Build 0362)

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 5.3.9 to 5.x.x release

Downgrading from 5.3.9 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 5.3.9 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 5.3.9.

Downgrading from 5.3.9 to 4.0.x/3.0.x/2.0.x release

Downgrading from 5.3.9 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 5.3.9 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 5.3.9.

Firmware downgrade for FVE-2000E-T2

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

Downgrading from 5.3.9 to 5.x.x release

Downgrading from 5.3.9 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 5.3.9 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 5.3.9.

Downgrading from 5.3.9 to 4.0.x release

Downgrading from 5.3.9 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 5.3.9 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 5.3.9.

Downgrading from 5.3.9 to 3.0.x release

Downgrading from 5.3.9 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 5.3.9 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 5.3.9.

Firmware downgrade for other FVE models

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

Downgrading from 5.3.9 to 5.x.x release

Downgrading from 5.3.9 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 5.3.9 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 5.3.9.

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
452540	Invalid extension displays when you do not enter an option in auto attendant.
458134	After daylight savings time changes, extensions status all display "Not Registered".
452467	Extensions with an auxiliary devices will not be paged when being part of Paging Group.
444475	Analog line appearance is incorrect for outbound calls and does not reflect the actual line being used.
448637	Pressing # via an auto attendant makes calls get stuck under some conditions.
456800	Add warning message when quota size is changed to a smaller value.
456118	Only 20 From Trunk entries can be added in call routing Inbound Rule.
453601	The announcement selection drop down list is not populated with announcements when being configured at the extension level.
453923	Auto attendant timeout action does not route calls to Ring Group.
447038	When caller dials feature code *40, call drops and extension is placed on hold..
413857	CDR data is missing when calls are parked and picked up from another extension.
445858	Need to prevent calls from being transferred to a Page Group via User Privileges.
454649	Service call queue display names are not updated on reports.
446658	Call center data service has incomplete output and requires enhancement.
452480	Call Detail Report misses call data and requires report structure change.
417255	Need to include paging calls in CDR.
453421	In Call Center, configured query name is not used in the agent performance report.
452969	IOT registration failed error message has a typo.
441789	Agent console displays data under the wrong owner/queue.
453162	FortiVoice AVS registration error displays "Invalid Credentials" when firewall blocks communication.
452736	In Inbound Call Routing, changing from Dial Number to Endpoint action makes routing change impossible.
452666	Unable to edit Match Patterns in the Dialed Number Match field of an outbound call routing.
414619	Need to improve Call Center callback prompts.

Bug ID	Description
453401	Renaming prompt files via CLI changes file size to zero.
458427	Extensions in a Page Group cannot receive a page if "Disconnect ongoing call" is enabled under Emergency call option.
457672	Operator Console search window loses focus with new inbound calls.
456740	Enhance PRI kill switch mechanism to send email alert notification when PRI module is unloaded if Critical Event alert is enabled.
445845	Need department-only administration.
435806	Add auto attendant key option to support recording of weekly announcements.
454140	User portal on the SMB system in GA build 355 and current GA build 360 is accessible.
453164	Operator Console is not available on FVE-50E.
417203	Add VM option to disable prompt that states caller's phone number.
305813	Add search capability for FortiFone- 470i remote phonebook.
423831	Incorrect PRI D channel setting causes system to become unresponsive after about 10 minutes.
455192	Agents are auto logged out of call queues due to business hour.
448196	Ring group call handling issue when more than one external number is used.
442723	Parked calls can be reparked by the original extension, even if the calls are unparked by another extension.
455556	CDR displays incorrect log.
453930	C70 conference phone outbound volume is distorted for the remote party.
384956	CDR call flow misses steps when call is parked or handled with extension appearance.
453122	Line appearance key allows an unparked call in progress to be stolen by another extension.

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