FORTINET

High Performance Network Security

FortiVoice™ Phone System Release Notes

VERSION 5.3.23 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

July 26, 2019

FortiVoice™ Phone System 5.3.23 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 5.3.23, build 0449.

Supported Platforms

FortiVoice 5.3.23 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, 2012, 2012 R2, 2016)
- FVE-VM (KVM qemu 0.12.1 and later)
- FVE-VM (Citrix XenServer v5.6sp2, 6.0 and higher, Open source XenServer 7.4 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 5.3.23 release. For more information, see the FortiVoice Phone System Administration Guide.

New phone support

FON-575 is supported. FON-575 has a built-in LCD expansion module and can support up to 106 programmable keys.

Survivable branch enhancement

Speed dial support is added for survivable branch, which allows users in central site or survivable branch to connect external paging system in survivable branch using speed dial.

Message group template enhancement

More variables are added to the message template of message delivery group to display more information in the delivered text message using message group.

Business group enhancement

Abbreviated dialing from Auto-Attendant is supported for business groups.

.

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)

↓

5.3.23 (Build 0449)

For any older 5.0.x release prior to 5.0.5

Any 5.0.x release

↓

5.0.5 (Build 0188)

↓

5.3.23 (Build 0449)

For 5.0.5 and 5.3.x release

5.0.5 (Build 0188) or 5.3.x release

↓

5.3.23 (Build 0449)

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)

↓

5.3.23 (2000E firmware, Build 0449)

For any older 5.0.x release prior to 5.0.5

Any 5.0.x release

↓

5.0.5 (Build 0188)

↓

5.3.23 (Build 0449)

For 5.0.5 and 5.3.x release

5.0.5 (Build 0188) or 5.3.x release

↓

5.3.23 (Build 0449)

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)

↓

5.3.23 (Build 0449)

For 5.0.5 and 5.3.x release

5.0.5 (Build 0188) or 5.3.x release

↓

5.3.23 (Build 0449)

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 5.3.23 to 5.x.x release

Downgrading from 5.3.23 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 5.3.23 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 5.3.23.

Downgrading from 5.3.23 to 4.0.x/3.0.x/2.0.x release

Downgrading from 5.3.23 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 5.3.23 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 5.3.23.

Firmware downgrade for FVE-2000E-T2

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

Downgrading from 5.3.23 to 5.x.x release

Downgrading from 5.3.23 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 5.3.23 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 5.3.23.

Downgrading from 5.3.23 to 4.0.x release

Downgrading from 5.3.23 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 5.3.23 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 5.3.23.

Downgrading from 5.3.23 to 3.0.x release

Downgrading from 5.3.23 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 5.3.23 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 5.3.23.

Firmware downgrade for other FVE models

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

Downgrading from 5.3.23 to 5.x.x release

Downgrading from 5.3.23 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 5.3.23 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 5.3.23.

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
537106	FortiVoice Enterprise 5.3.23 is no longer vulnerable to the following CVE-Reference: CVE-2019-0190, CVE-2018 17199, and CVE-2018 17189
568645	FortiVoice Enterprise 5.3.23 is no longer vulnerable to the following CVE-Reference: CVE-2019-0211, CVE-2019-0217, CVE-2019-0215, CVE-2019-0197, CVE-2019-0196, and CVE-2019-0220.
571799	Forwarded call is sent back to PBX by FortiVoice Gateway.
569897	Adjusted FON-570 adjust voice audio volume to default values.
565003	Support Diffserv in phone profile.
564969	Enhanced Message Group for additional message information.
565331	Auto-Attendant setting of Ring Group for invalid input action fails validation length check when RG name/ID exceeds 15 characters.
554731	CDR shows wrong disposition when call is routed to virtual number with IVR setting after auto attendant times out.
571383	Restricted Area Code/Number under Call Restrictions in the user privilege profile does not work.
571384	Transfer calls directly from LSG to analog phone on other end of FXO intercom system.
571988	Specified default user password is not applied to new extensions.
572579	brand new FON-375 with MAC address e8:1c:ba cannot get unassigned phone configuration.

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