FORTINET

High Performance Network Security

FortiVoice™ Phone System Release Notes

VERSION 5.3.13 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

May 15, 2018

FortiVoice™ Phone System 5.3.13 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 5.3.13, build0378.

Supported Platforms

FortiVoice 5.3.13 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 5.3.13 release. For more information, see the FortiVoice Phone System Administration Guide.

FortiVoice survivability solution

This solution is designed to provide branch resiliency for centralized deployments with multi-sites. It is delivered and supported by a selected line of enterprise-class appliances through a firmware upgrade and enables system administrators to seamlessly connect multiple locations with an easy-to-deploy solution.

Gateway management

Gateway Management is an innovative part of the FortiVoice management framework to enable auto-discovery of other FortiVoice gateways on the network and offer remote device management from a centralized FortiVoice phone system. This feature is designed to enhance the management of increasing FortiVoice gateway devices and provide system administrators with an improved user experience when managing a FortiVoice enterprise ecosystem.

New phones

Hotel phone H35 with LCD screen and FortiFone-475 are supported.

New PRI gateway platforms

FVG-GT01 (1 PRI port) and GT02 (2 PRI ports) are supported.

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)

↓

5.3.13 (Build 0378)

For any older 5.0.x release prior to 5.0.5

Any 5.0.x release

↓

5.0.5 (Build 0188)

↓

5.3.13 (Build 0378)

For 5.0.5 and 5.3.x release

5.0.5 (Build 0188) or 5.3.x release

↓

5.3.13 (Build 0378)

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)

↓

5.3.13 (2000E firmware, Build 0378)

For any older 5.0.x release prior to 5.0.5

Any 5.0.x release

↓

5.0.5 (Build 0188)

↓

5.3.13 (Build 0378)

For 5.0.5 and 5.3.x release

5.0.5 (Build 0188) or 5.3.x release

↓

5.3.13 (Build 0378)

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)

↓

5.3.13 (Build 0378)

For 5.0.5 and 5.3.x release

5.0.5 (Build 0188) or 5.3.x release

↓

5.3.13 (Build 0378)

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 5.3.13 to 5.x.x release

Downgrading from 5.3.13 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 5.3.13 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 5.3.13.

Downgrading from 5.3.13 to 4.0.x/3.0.x/2.0.x release

Downgrading from 5.3.13 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 5.3.13 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 5.3.13.

Firmware downgrade for FVE-2000E-T2

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

Downgrading from 5.3.13 to 5.x.x release

Downgrading from 5.3.13 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 5.3.13 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 5.3.13.

Downgrading from 5.3.13 to 4.0.x release

Downgrading from 5.3.13 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 5.3.13 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 5.3.13.

Downgrading from 5.3.13 to 3.0.x release

Downgrading from 5.3.13 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 5.3.13 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 5.3.13.

Firmware downgrade for other FVE models

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

Downgrading from 5.3.13 to 5.x.x release

Downgrading from 5.3.13 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 5.3.13 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 5.3.13.

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.

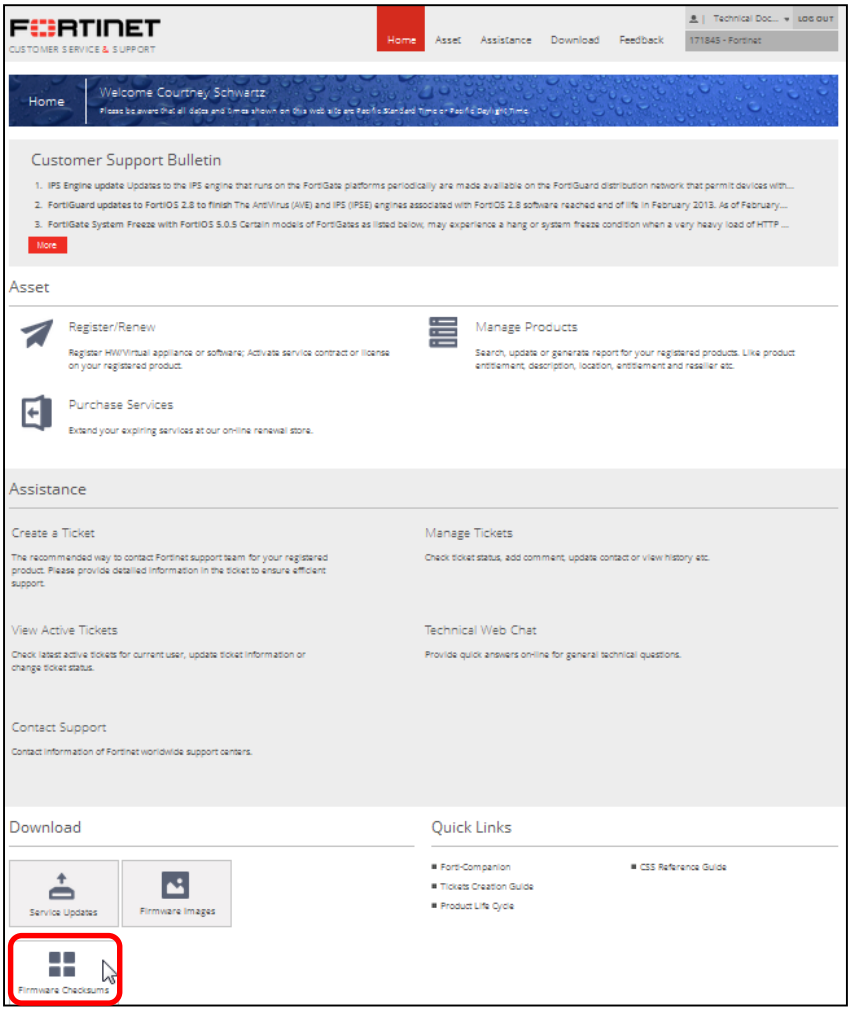
Bug ID	Description
486547	GS16 FXS gateway has an issue with T.38 which prevents fax being relayed to the fax machine on the gateway.
485819	After testing a page call to a group with a large number of extensions, the PBX CPU is stuck running at 50%.
487670	+1 DID Mapping rule for call recording does not work.
480110	Outbound calls are rejected by some remote SIP servers when the "X-FV-FORWARD-COUNT" is on INVITE message.
488608	FortiFone SoftClient does not receive calls consistently.
478424	Schedule profiles with "&" in their names are lost after upgrading to b367.
489563	Calls cannot be hung up for FON175 FON375 if a connected call lasts 5 minutes and primary outbound proxy was down.
482717	911 alert email does not include caller ID of extension making the 911 call.
478608	DST/Timezone is incorrectly set when (GMT-6:00)Saskatchewan is selected.
477143	FXO alarm is triggered at the end of call when external party hangs up.
476909	Call recording policy is not followed when calls are transferred between queues.
478922	When FortiFone-375i is configured for Data VLAN, the configuration file is correct for the Data VLAN but the port is disabled.
489831	Agent login to Call Center Queue results in agent status set to Invalid.
483174	FortiFON-375i does not display CID from Ring Group on internal calls to Ring Group.
483591	The orange icon of MAC address in extension displays wrong MAC address (FortiFone-375/175/H25).
437798	Need to enhance error handling for blind transfers and invalid option selection.
476976	In Call Center, calls to IVR with ticket information fall through to customer service. CS attempts a supervised transfer to another queue but no popup appears in Agent Console and callers lose priority.
489137	The configuration file pushed to phones uses term "No fucntion" instead of "No function".
486829	Disabling “Coach” from “Agent” profile under “Manager Privilege” removes the “Pickup” and “Transfer” buttons from the Call Center Console.

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.