FORTINET

High Performance Network Security

FortiVoice™ Phone System Release Notes

VERSION 5.3.20 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

April 24, 2019

FortiVoice™ Phone System 5.3.20 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
Dial plan enhancement 7
Call center enhancements 7
Ring tones 7
Certificate renewal 7
What's Changed 8
Softclient login 8
Firmware Upgrade/Downgrade 9
Before and after any firmware upgrade/downgrade 9
Upgrade path for FVE-200D and 200D-T 9
For any older 2.x.x/3.0.x/4.0.x release 9
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 FVE-2000E-T2 9
For any older 3.0.x/4.0.x release 9
For any older 5.0.x release prior to 5.0.5 10
For 5.0.5 and 5.3.x release 10
Upgrade path for other FVE models 10
For any older 5.0.x release 10
For 5.0.5 and 5.3.x release 10
Firmware downgrade for FVE-200D and 200D-T 10
Downgrading from 5.3.20 to 5.x.x release 10
Downgrading from 5.3.20 to 4.0.x/3.0.x/2.0.x release 11
Firmware downgrade for FVE-2000E-T2 11
Downgrading from 5.3.20 to 5.x.x release 11

Downgrading from 5.3.20 to 4.0.x release 11
Downgrading from 5.3.20 to 3.0.x release 11
Firmware downgrade for other FVE models 12
Downgrading from 5.3.20 to 5.x.x release 12
Resolved issues 13
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 5.3.20, build 0431.

Supported Platforms

FortiVoice 5.3.20 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 5.3.20 release. For more information, see the FortiVoice Phone System Administration Guide.

Dial plan enhancement

Enhanced dial plan to support third party paging systems.

Call center enhancements

Enhanced Monitor View to:

- provide filtering option to display agents with a "Logged in" status and customization of the queue view columns.
- add configuration option to specify the starting reference time for displaying daily statistics.

Ring tones

Added distinctive ring tone for inbound calls (internal vs. external).

Certificate renewal

Renewed certificate used in Apple push service for iOS Softclient. Old certificate expired on Apr 18, 2019.

What's Changed

The following list highlights the behavior changes in this release.

Softclient login

When user authentication is enabled for LDAP, softclient login will continue to use local password in order to support auto configuration with QR code.

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)

↓

5.3.20 (Build 0431)

For any older 5.0.x release prior to 5.0.5

Any 5.0.x release

↓

5.0.5 (Build 0188)

↓

5.3.20 (Build 0431)

For 5.0.5 and 5.3.x release

5.0.5 (Build 0188) or 5.3.x release

↓

5.3.20 (Build 0431)

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)

↓

5.3.20 (2000E firmware, Build 0431)

For any older 5.0.x release prior to 5.0.5

Any 5.0.x release

↓

5.0.5 (Build 0188)

↓

5.3.20 (Build 0431)

For 5.0.5 and 5.3.x release

5.0.5 (Build 0188) or 5.3.x release

↓

5.3.20 (Build 0431)

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)

↓

5.3.20 (Build 0431)

For 5.0.5 and 5.3.x release

5.0.5 (Build 0188) or 5.3.x release

↓

5.3.20 (Build 0431)

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 5.3.20 to 5.x.x release

Downgrading from 5.3.20 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 5.3.20 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 5.3.20.

Downgrading from 5.3.20 to 4.0.x/3.0.x/2.0.x release

Downgrading from 5.3.20 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 5.3.20 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 5.3.20.

Firmware downgrade for FVE-2000E-T2

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

Downgrading from 5.3.20 to 5.x.x release

Downgrading from 5.3.20 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 5.3.20 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 5.3.20.

Downgrading from 5.3.20 to 4.0.x release

Downgrading from 5.3.20 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 5.3.20 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 5.3.20.

Downgrading from 5.3.20 to 3.0.x release

Downgrading from 5.3.20 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 5.3.20 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 5.3.20.

Firmware downgrade for other FVE models

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

Downgrading from 5.3.20 to 5.x.x release

Downgrading from 5.3.20 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 5.3.20 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 5.3.20.

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.

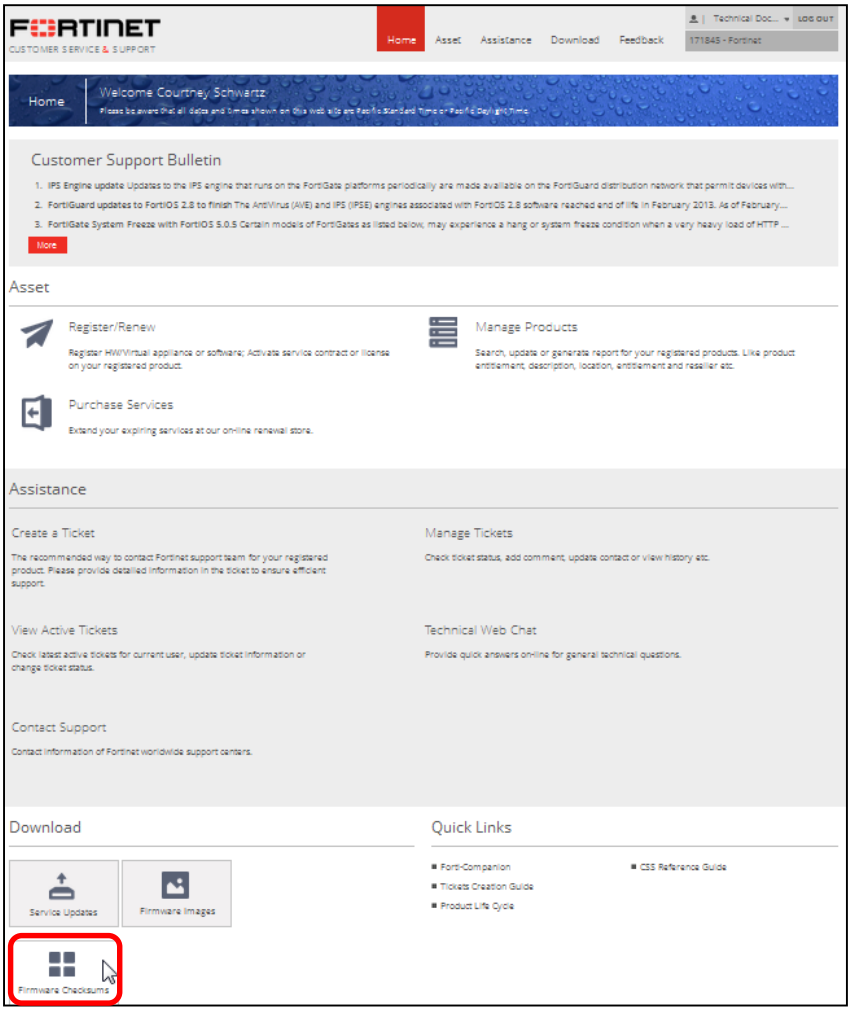
Bug ID	Description
541888	Sending faxes from user web portal causes high memory usage.
542474	Web user portal reminder option configuration for external number has no audio and disconnects the call.
546245	Resolve inbound calls via SIP trunk fails with "404 Not Found" when multiple SIP trunk entries are provisioned using the same proxy and server address.
543220	Call Forward feature *71 does not work on inbound calls.
549182	Managed gateway survivable branch does not show FortiVoice management information.
543238	Registering multiple handsets for D71 results in conflict MAC addresses.
547744	On FortiVoice v5.3.18, unassigned phone menu does not show all the phones.
547137	Downloading filtered CDR pulls oldest logs.
540677	Extension report does not have data on calls from ring groups.
544874	Extension is not listed in directory if voicemail is disabled.
548044	FVG-GS16 auto-provisioning has multiple issues.
537147	Phone does not reboot if user defined profile has setting change.
550047	SoftClient is not able to login when LDAP is used for portal authentication.
544173	Managed GS16 gateway configuration is invalid if PBX ID contains spaces.
548661	When update-pai-header is enabled, FVE sends UPDATE to SIP Peer when a blind transfer is completed.
549502	Fetch directory does not work when a remote sever is configured with FQDN.
550279	GS16 FXS gateway issue with T.38 on outbound faxes.

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© 2019 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.