

FortiVoice Phone System - Release Notes

Version 5.3.25

FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/support-and-training/training.html>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://fortiguard.com/>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



January 31, 2020

FortiVoice Phone System 5.3.25 Release Notes

26-5325-585435-20190923

TABLE OF CONTENTS

Change log	4
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
Directory Name Lookup Service	7
Phone Directory Enhancement	7
Firmware upgrade/downgrade	8
Before and after any firmware and downgrade	8
Upgrade path for FVE-200D and 200D-T	8
Upgrade path for FVE-2000E-T2	9
Upgrade path for other FVE models	10
Firmware downgrade for FVE-200D and 200D-T	10
Firmware downgrade for FVE-2000E-T2	11
Firmware downgrade for other FVE models	12
Resolved issues	13

Change log

Date	Change description
2020-01-29	Initial release of the FortiVoice 5.3.25 Release Notes.

Introduction

This document provides a list of new and changed features, upgrade instructions and caveats, resolved issues, and known issues for FortiVoice release 5.3.25, build 0462.

Supported platforms

FortiVoice release 5.3.25 supports the following platforms:

- FVE-20E2 and 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, 5
- 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 this release. For more information, see the FortiVoice Phone System Administration Guide.

Directory Name Lookup Service

- Dial by name feature enhancement to provide a more refined directory listing for business groups.
- Additional caller option to skip directory name playback using the DTMF "*" key.
- Directory name playback to support menu group listing of names.

Phone Directory Enhancement

Provide separate phone directories on the FortiFones for accessing contacts from the local branch office directory and another from the global system directory.

Firmware upgrade/downgrade

This section includes the following topics:

- [Before and after any firmware and downgrade on page 8](#)
- [Upgrade path for FVE-200D and 200D-T on page 8](#)
- [Upgrade path for FVE-2000E-T2 on page 9](#)
- [Upgrade path for other FVE models on page 10](#)
- [Firmware downgrade for FVE-200D and 200D-T on page 10](#)
- [Firmware downgrade for FVE-2000E-T2 on page 11](#)
- [Firmware downgrade for other FVE models on page 12](#)

Before and after any firmware and downgrade

- Before any firmware upgrade and 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)



5.3.25 (Build 0462)

For any older 5.0.x release prior to 5.0.5

Any 5.0.x release



5.0.5 (Build 0188)



5.3.25 (Build 0462)

For 5.0.5 and 5.3.x releases

5.0.5 (Build 0188) or 5.3.x release



5.3.25 (Build 0462)

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)



5.3.25 (2000E firmware, Build 0462)

For any older 5.0.x release prior to 5.0.5

Any 5.0.x release



5.0.5 (Build 0188)



5.3.25 (Build 0462)

For 5.0.5 and 5.3.x release

5.0.5 (Build 0188) or 5.3.x release



5.3.25 (Build 0462)

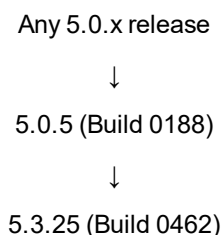
After every upgrade, verify that the build number and version number match the image that was loaded. To do so, go to **Status > Dashboard > Dashboard**.



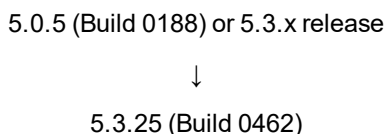
For a FortiVoice 2000E-T2 upgrade with the serial number prefix of FO2HDD.
If the upgrade is done through the "G" option of the boot loader, then use the FVE-200D platform image.

Upgrade path for other FVE models

For any older 5.0.x release



For 5.0.5 and 5.3.x release



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 5.3.25 to 5.x.x release

Downgrading from 5.3.25 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 5.3.25 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 5.3.25.

Downgrading from 5.3.25 to 4.0.x/3.0.x/2.0.x release

Downgrading from 5.3.25 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 5.3.25 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 5.3.25.

Firmware downgrade for FVE-2000E-T2

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

Downgrading from 5.3.25 to 5.x.x release

Downgrading from 5.3.25 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 5.3.25 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 5.3.25.

Downgrading from 5.3.25 to 4.0.x release

Downgrading from 5.3.25 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 5.3.25 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 5.3.25.

Downgrading from 5.3.25 to 3.0.x release

Downgrading from 5.3.25 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 5.3.25 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 4.0.x backup configuration saved before upgrading to 5.3.25.

Firmware downgrade for other FVE models

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

Downgrading from 5.3.25 to 5.x.x release

Downgrading from 5.3.25 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 5.3.25 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 5.3.25.

Resolved issues

The resolved issues listed below do not list every bug that has been corrected with this release. For inquiries about a particular bug, contact [Fortinet Customer Service & Support](#).

Bug ID	Description
606276	Phone directory needs to be enhanced to provide different directory source for local and remote directories.
568996	Outbound dialplan needs to trigger next call handling action immediately when a monitored SIP trunk becomes unavailable.
586549	Log message has a typo where "registriation" should be "registration".
586036	Softclient configuration should always be generated regardless of the auto provisioning status.
595183	Call Center Agent option only displays 500 agents.
591611	Caller ID Modification needs to be enabled when managed gateway trunks are generated by the system.
594243	PRI trunk should have configurable Screening Indicator options.
604397	Missing validation check for unique extension group name identifier results in DB query failures when duplicate names exist.
587294	Entry level phone system administrator with custom access profile cannot view CDR detail.
551042	FortiVoice DST setting does not apply to FortiFones.



FORTINET[®]



Copyright© 2020 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.