

Release Notes

FortiBranchSASE 7.6.2



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO LIBRARY

<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/training-certification>

FORTINET TRAINING INSTITUTE

<https://training.fortinet.com>

FORTIGUARD LABS

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com



Jun 23, 2025

FortiBranchSASE 7.6.2 Release Notes

TABLE OF CONTENTS

Change log	4
Introduction	5
What's new	6
Supported hardware models	7
Special notes	8
Firmware upgrade procedures	9
Product integration and support	10
Compatibility matrices	10
Supported Web browsers	10
Resolved issues	11
Known issues	12

Change log

Date	Change Description
2025-05-14	Initial release.
2025-06-23	Updated What's new on page 6 .

Introduction

FortiBranchSASE is a member of the FortiExtender product family. The FortiBranchSASE firmware can be found on the [Fortinet Support](#) website under the FortiExtender category.

While FortiExtender and FortiBranchSASE share many features, this document provides release information specific to FortiBranchSASE 7.6.2 (Build 0441).

What's new

FortiBranchSASE 7.6.2 offers the following new features and enhancements:

- Support for wired 802.1X authentication on FortiBranchSASE models (Standalone).
- Enhance RADIUS authentication with support for FQDN servers (Standalone).
- Support for importing third-party certificates through an SCEP server (Standalone).
- All FortiBranchSASEs with valid support contracts and FortiEdge Cloud licenses can establish a tunnel to FortiEdge Cloud. FortiBranchSASE must be provisioned as the OBM type in the FortiEdge Cloud portal so that the cloud OBM session can be established in the FortiGate mode to provide remote OBM console capability.
- Add Bluetooth button control on BLE capable models (Standalone).

```
config system bluetooth
  set status {enable | disable}
end
```



For more information on managed features, refer to the FortiBranchSASE 7.6.2 [Admin Guide](#) (Managed).

For more information on standalone features, refer to the FortiExtender 7.6.2 [Admin Guide](#) (Standalone)

Supported hardware models

FortiBranchSASE 7.6.2 supports the following hardware models:

Model	Market
FortiBranchSASE-10F-WiFi	Global
FortiBranchSASE-20G	Global
FortiBranchSASE-20G-WiFi	Global

Special notes

- Upon reboot, FortiBranchSASE will try to discover the FortiGate, FortiSASE, or FortiEdge Cloud that manages it, depending on your existing configuration. Because of this, there might be a short delay before the device reconnects to the FortiGate, FortiSASE, or FortiEdge Cloud.
- In order for FortiBranchSASE to forward syslog messages to a remote syslog server, the syslog server and the FortiBranchSASE LAN port must be part of the same subnet.

Firmware upgrade procedures

You can download and install the FortiBranchSASE firmware using the FortiGate GUI or CLI, or the FortiBranchSASE GUI or CLI.

To upgrade using the FortiBranchSASE GUI:

1. Log into your FortiBranchSASE device.
2. On the navigation bar on the left, click *Settings*.
3. From the top of the page, select *Firmware*.
4. Select *Extender Upgrade > Local*, and then upload the firmware.

Product integration and support

Compatibility matrices

As FortiBranchSASE is a member of the FortiExtender product family, FortiBranchSASE hardware and firmware compatibility information can be found under the [FortiExtender documentation](#) category. The following compatibility matrices are available:

- [FOS & FortiExtender OS Compatibility Matrix](#)
- [FortiExtender OS-Hardware Compatibility](#)
- [FortiExtender Hardware and FOS Compatibility Matrix](#)

Supported Web browsers

FortiBranchSASE 7.6.2 supports the latest versions of the following web browsers:

- Google Chrome
- Mozilla Firefox

Resolved issues

The following issues have been resolved in FortiBranchSASE 7.6.2. For inquiries about a particular bug, visit the [Fortinet Support](#) website.

Bug ID	Description
0949548	FortiExtender stops responding to SNMP monitoring after a few hours.
1089690	When FortiExtender is in LAN extension mode with split tunneling configured, le-switch clients sometimes fail to access services.
1110949	Read-only users are able to make system changes.
1134971	FortiExtender does not send the correct hostname to the syslog server.

Known issues

There are no known issues in this release.



www.fortinet.com

Copyright© 2025 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., 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 Chief Legal Officer, 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. 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.