



# FortiAuthenticator Agent for Microsoft Windows - Release Notes

Version 3.5

**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://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

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

**FEEDBACK**

Email: [techdoc@fortinet.com](mailto:techdoc@fortinet.com)



August 11, 2021

FortiAuthenticator Agent for Microsoft Windows 3.5 Release Notes

23-350-691237-20210811

# TABLE OF CONTENTS

- Change log** ..... 4
- FortiAuthenticator Agent for Microsoft Windows 3.5 release** ..... 5
- What's new** ..... 6
- Product integration and support** ..... 7
  - FortiAuthenticator Support ..... 7
  - Operating systems ..... 7
- Resolved issues** ..... 9
- Known issues** ..... 10

## Change log

Date	Change Description
2021-02-03	Initial release.
2021-08-11	Updated <a href="#">Product integration and support on page 7</a> .

# FortiAuthenticator Agent for Microsoft Windows 3.5 release

This document provides a summary of new features, enhancements, support information, installation instructions, caveats, and resolved and known issues for FortiAuthenticator Agent for Microsoft Windows 3.5.

## What's new

FortiAuthenticator Agent for Microsoft Windows version 3.5 includes the following new features and enhancements:

- You can now set up realm-based authentication by default during installation.
- Implemented Unlock and CredUI scenarios for push.

# Product integration and support

## FortiAuthenticator Support

FortiAuthenticator Agent for Microsoft Windows 3.5 supports the following FortiAuthenticator versions:

- FortiAuthenticator 6.2.1
- FortiAuthenticator 6.2
- FortiAuthenticator 6.1
- FortiAuthenticator 6.0

## Operating systems

Server Operating System	
Windows Server 2012	<ul style="list-style-type: none"><li>• Standard (x64)</li><li>• DataCenter (x64)</li></ul>
Windows Server 2012 R2	<ul style="list-style-type: none"><li>• Standard (x64)</li><li>• DataCenter (x64)</li></ul>
Windows Server 2016	<ul style="list-style-type: none"><li>• Standard (x64)</li><li>• DataCenter (x64)</li></ul>
Windows Server 2019	<ul style="list-style-type: none"><li>• Standard (x64)</li><li>• DataCenter (x64)</li></ul>
Desktop Operating System	
Windows 8	<ul style="list-style-type: none"><li>• Professional (x86/x64)</li><li>• Enterprise (x86/x64)</li></ul>
Windows 10	<ul style="list-style-type: none"><li>• Enterprise (x86/x64)</li><li>• Pro (x86/x64)</li></ul>



---

Microsoft Windows 8 Standard is unsupported as it is not designed to be connected to a Windows Domain.

Microsoft Windows XP and Microsoft Windows Vista are not currently supported as they have reached end of support with Microsoft. Please contact your Fortinet Account Manager if this is an issue.

Other versions of Microsoft Windows may also work, but have not been validated.

---



## Resolved issues

The resolved issues listed below may not list every bug that has been corrected with this release. For inquiries about a particular bug, please visit the [Fortinet Support](#) website.

Bug ID	Description
<b>660392</b>	500 error if you send the REST API call for /v1/auth/ when a duplicate user name is present.
<b>661203</b>	FortiAuthenticator Agent for Microsoft Windows push auth fails if the realm name is different from the server name.
<b>668916</b>	Subdomain users can authenticate over the FortiAuthenticator Agent for Microsoft Windows installed on a workstation in the main domain without the token code.
<b>671345</b>	Fixed bad password scenario for push.
<b>673306</b>	FortiAuthenticator Agent for Microsoft Windows cannot initiate connection towards the secondary FortiAuthenticator for 2FA validation.
<b>683298</b>	Agent exception error occurred when OTP is delivered by SMS.

## Known issues

This section lists the known issues of this release, but is not a complete list. For inquiries about a particular bug, please visit the [Fortinet Support](#) website.

Bug ID	Description
<b>676199</b>	Blank screen issue on the Windows Server 2012 and 2012 R2.



**FORTINET®**



Copyright© 2021 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.