



# FortiAuthenticator Agent for Microsoft OWA - Install Guide

Version 2.3

**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/training-certification>

**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)



March 30, 2022

FortiAuthenticator Agent for Microsoft OWA 2.3 Install Guide

23-230-710315-20220330

# TABLE OF CONTENTS

<b>Change Log</b>	<b>4</b>
<b>Introduction</b>	<b>5</b>
FortiAuthenticator Agent for Microsoft OWA	5
System requirements	5
Minimum operating system requirements	5
Required ports	6
Third-party trademark notice	6
<b>FortiAuthenticator configuration</b>	<b>7</b>
<b>Agent installation procedure</b>	<b>8</b>
Agent configuration	10
<b>Appendix A — Licenses</b>	<b>11</b>
pGina license	11

## Change Log

Date	Change Description
2022-03-30	Initial release.

# Introduction

This document introduces FortiAuthenticator Agent for Microsoft OWA (Outlook Web Access), a plugin for the Microsoft Outlook Web Access running on Microsoft IIS web server which allows a FortiAuthenticator OTP (One Time Passcode) requested during Microsoft Outlook Web Access authentication.

This document covers the installation and configuration of the FortiAuthenticator Agent for Microsoft OWA on supported Microsoft Windows Server, IIS, running Outlook Web Access and configuration of the FortiAuthenticator.

## FortiAuthenticator Agent for Microsoft OWA

Once installed, the modified login process requires a Username and OTP to be validated via the FortiAuthenticator, and the username and password validated as normal via AD (Active Directory).

FortiAuthenticator Agent for Microsoft OWA validates the OTP prior to the AD password which prevents any possibility of brute forcing the password.



FortiAuthenticator Agent for Microsoft OWA supports SMS, email, and FortiToken Mobile push methods for 2FA.

---

## System requirements

FortiAuthenticator Agent for Microsoft OWA 2.3 has the following system requirements:

- 20 MB of free disk space
- TCP/IP networking
- Microsoft .Net Framework 4.8.0
- Visual Studio C++ 2019 redistributable packages



The installation process checks and attempts to install the appropriate .NET runtime version. FortiAuthenticator Agent for Microsoft OWA 2.3 currently does not test for the IIS/Exchange presence or for the appropriate .NET runtime versions. This will be resolved in a future revision.

---

## Minimum operating system requirements

FortiAuthenticator Agent for Microsoft OWA 2.3 has the following minimum operating system requirements:

## Operating systems

- Microsoft Windows Server 2012 and later

## Applications

- Microsoft IIS 8.5 and later
- Microsoft Exchange Server 2013 and up

## Required ports

The following ports must be allowed between the Client operating system and the specified system:

Port	Destination	Description
<b>TCP/443</b>	FortiAuthenticator	Used by the FortiAuthenticator Agent for Microsoft OWA to validate the entered two-factor authentication token.
<b>TCP/389</b>	Windows Domain Controller	Indirectly used by the FortiAuthenticator Agent for Microsoft OWA to verify group membership of the user in order to identify if two-factor authentication should be applied.

## Third-party trademark notice

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

# FortiAuthenticator configuration

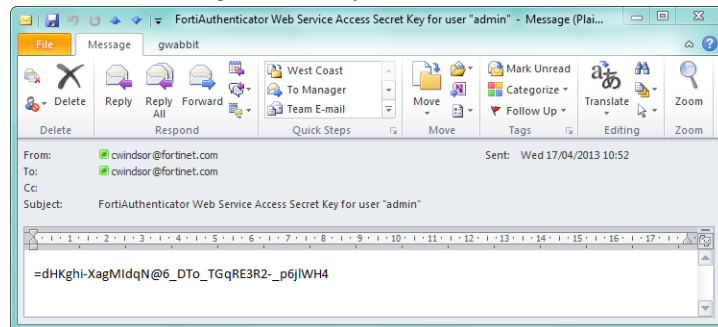
To enhance the Microsoft Windows operating system login with the use of a OTP (i.e. the two-factor authentication token), FortiAuthenticator Agent for Microsoft OWA uses the FortiAuthenticator REST API. To use the REST API, a key is required which must be generated before installing the desktop agent software.

Generating an API key requires a working email configuration. Before proceeding, configure and test an email server in **System > Messaging > SMTP Servers** and set it as active in **System > Messaging > Email Services**.

## To generate an API key:

1. Log into FortiAuthenticator.
2. Go to *Authentication > User Management > Local Users* and click the admin user.
3. Under *User Role*, select *Web service access*.
4. Click **OK**.

An email containing the API Key for that user will be sent.



The required users should be imported via LDAP and assigned a FortiToken with which to authenticate before proceeding.

# Agent installation procedure



Before proceeding, please backup your system and all configurations files.

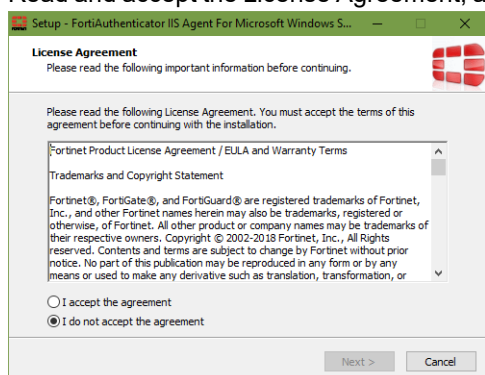
FortiAuthenticator Agent for Microsoft OWA Agent for Microsoft OWA is designed for installation onto a Domain connected system.

On the IIS/OWA system you wish to perform two-factor enhanced login:

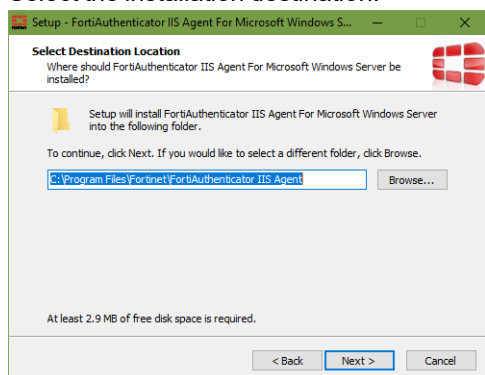
1. Ensure that your system meets the prerequisites as defined in [System requirements](#).
2. Run the FortiAuthenticator Agent for Microsoft OWA install file as a Domain Administrator (e.g. either as a logged in Domain Administrator or by right-clicking and select *Run as Administrator*). Note that the Agent can also be installed via GPO, however that process is not covered in this document.

FortiAuthenticator Agent for Microsoft OWA Agent for Microsoft Windows will now begin to install.

3. Read and accept the License Agreement, and click *Next*.

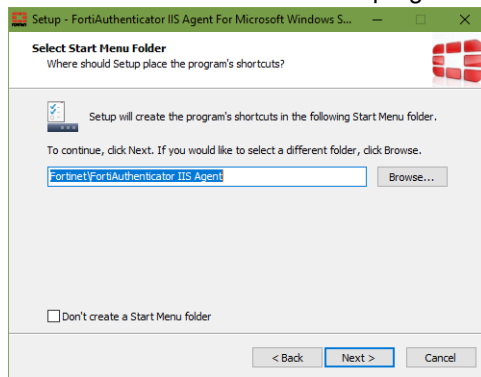


4. Select the installation destination.

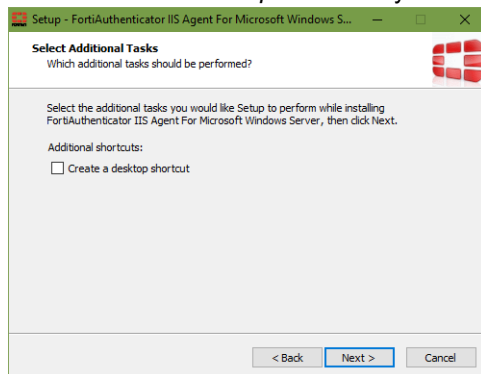




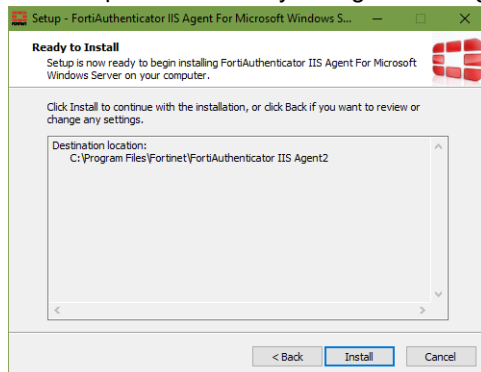
5. Select a start menu folder for the program shortcut, or select *Don't create a Start Menu folder*.



6. Select *Create a desktop shortcut* if you would like to create a shortcut on your desktop.



7. The setup wizard is ready to begin installing.



8. Click *Install* to begin the installation process.



- Once the installation has completed, select *Review 2FA Configuration* and click *Finish*.  
The configuration dialogue should open. If it does not, or if you wish to reconfigure your agent, run the FortiAuthenticator Agent for Microsoft OWA configuration utility to configure the specifics of your setup.

## Agent configuration

- After the FortiAuthenticator Agent for Microsoft OWA configuration utility opens, click the *General* tab.
- Under *FortiAuthenticator Configuration*, configure the IP address, username, and API key obtained.
- Under *Web Configuration*, configure the specifics of your Web Server and OWA installation.

The screenshot shows the 'FortiAuthenticator 2FA Configuration' dialog box with the 'General' tab selected. The 'FortiAuthenticator Configuration' section includes fields for 'FortiAuthenticator Name/IP' (192.168.0.123), 'Administrator Name' (admin), and 'Rest API Key' (masked with dots). There is a checkbox for 'Verify Server Certificate' which is unchecked. Below it, 'Server Subject Name' is set to 'FAC\VM0A12001111' and 'CA Certificate File' is set to 'C:\Program Files\Fortinet\FortiAuthenticator IIS Agent\Fortinet\_ca' with a 'Browse' button. The 'Web Configuration' section includes 'Public Server Hostname' (192.168.150.21), 'Internal Server Hostname' (192.168.150.21), 'OWA Path' (/owa/), and 'Fortinet 2FA Path' (/fortinet/login2fa). At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

- Click the *Authentication* tab and configure the required timeout, retry parameters, and push timeout, as well as the action to take should the FortiAuthenticator become unavailable (*Allow* or *Block*).

The screenshot shows the 'FortiAuthenticator 2FA Configuration' dialog box with the 'Authentication' tab selected. The 'Options' section includes 'Timeout (s)' (5), 'Retries' (3), and 'Push Timeout (s)' (20). There are two radio button options for 'Action to take on authentication failure (timeout/unavailable):' and 'Action to take when no token has been assigned to user:', both with 'Allow' and 'Block' choices. The 'Block' option is selected for both. Below this is a 'Disable 2FA Protection' section with a checkbox and explanatory text. At the bottom is a 'Realms for Domains' table.

Domain	Realm
FORTINET-US	FORTINET-US
MERUNETWORKS	MERUNETWORKS
ACCELOPS	ACCELOPS

At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

You can use the realm included in the login request to process the authentication. Realms configured in FortiAuthenticator Agent for Microsoft OWA must exactly match the one configured on FortiAuthenticator. Select **OK** to save changes.

## Appendix A — Licenses

FortiAuthenticator utilizes elements of Open Source technology including:

pGina - <http://pgina.org/>

License for use of such software is reproduced below as per the terms of use.

### pGina license

Copyright (c) 2013, pGina Team

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- \* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

- \* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

- \* Neither the name of the pGina Team nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.



**FORTINET®**



Copyright© 2022 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.