FortiAuthenticator Agent for Microsoft OWA - Install Guide

Version 1.6

F⊡RTINET®

TABLE OF CONTENTS

Change Log

Date	Change Description
2020-06-11	Initial release.

FortiAuthenticator Agent for Microsoft OWA 1.6 Install Guide
Fortinet Technologies Inc.

4

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.

Due to the fact that the username, password, and token need to be simultaneously put into the login prompts, two-factor authentication methods that require a trigger to obtain the token (email and SMS) are not supported. However, other methods including FortiToken and FortiToken Mobile are supported.

System requirements

FortiAuthenticator Agent for Microsoft OWA 1.6 has the following system requirements:

- 20 MB of free disk space
- TCP/IP networking
- Microsoft .Net Framework 4.6.0
- Visual Studio C++ 2012 redistributable packages

FortiAuthenticator Agent for Microsoft OWA 1.6 currently does not test for the IIS/Exchange presence or for the appropriate .NET runtime versions. This will be resolved in a future revision.

Required ports

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

Port	Destination	Description
TCP/443	FortiAuthenticator	Used by the FortiAuthenticator Agent for Microsoft OWA to validate the entered two-factor authentication token.
TCP/389	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.
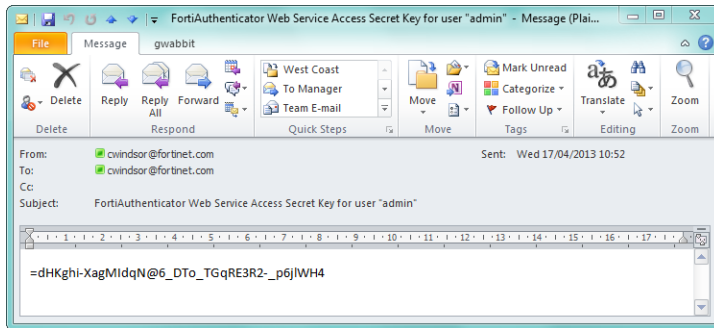
FortiAuthenticator configuration

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*.

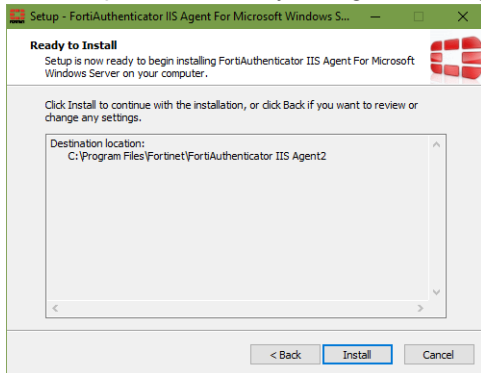4. Select the installation destination.

FortiAuthenticator Agent for Microsoft OWA 1.6 Install Guide
Fortinet Technologies Inc.

8
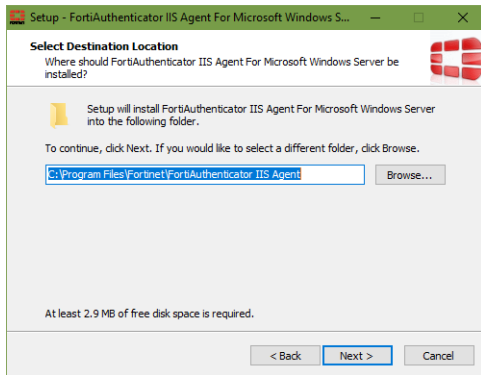
5. Select a start menu folder for the program shortcut, or select *Don't create a Start Menu folder*.
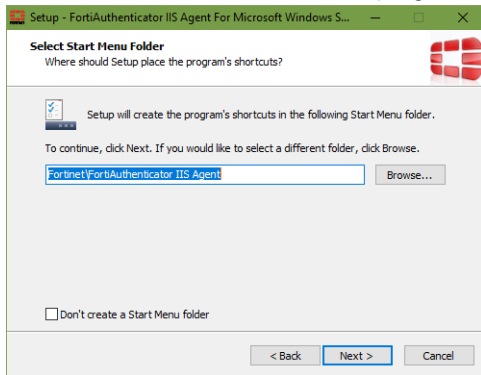
6. Select *Create a desktop shortcut* if you would like to create a shortcut on your desktop.
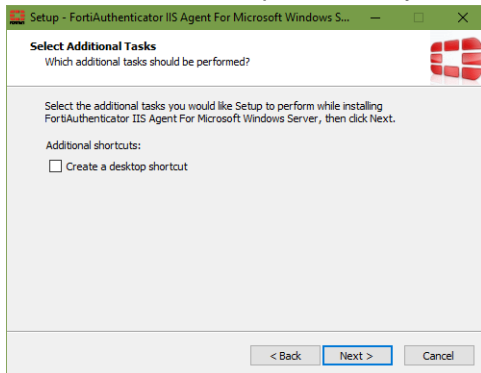
**7.** The setup wizard is ready to begin installing.

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

9. 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

1. After the FortiAuthenticator Agent for Microsoft OWA configuration utility opens, click the *General* tab.
2. Under *FortiAuthenticator Configuration*, configure the IP address, username, and API key obtained.
3. Under *Web Configuration*, configure the specifics of your Web Server and OWA installation.
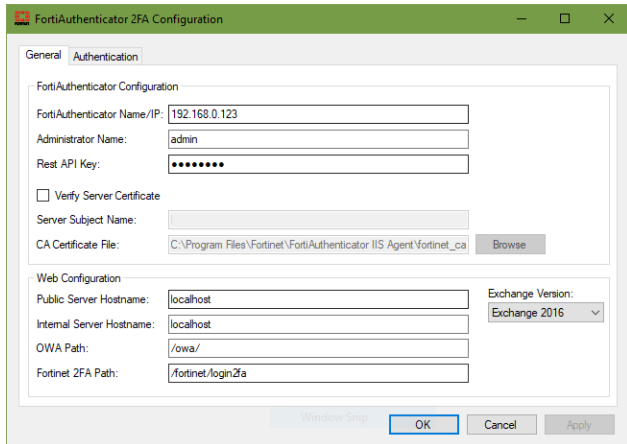
4. Click the *Authentication* tab and configure the required timeout and retry parameters, as well as the action to take should the FortiAuthenticator become unavailable (*Allow* or *Block*). Click *OK* to save.
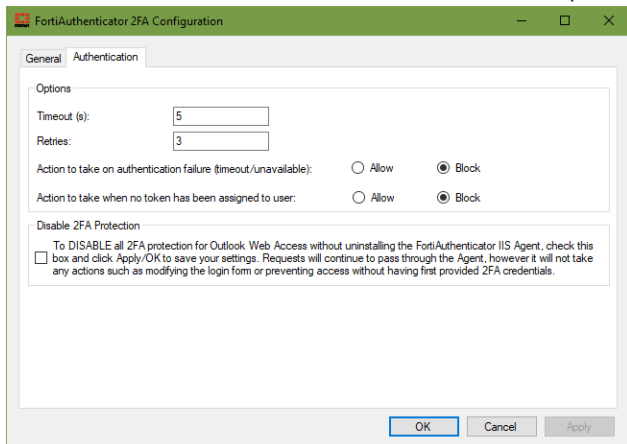
User two-factor login

The default installation creates a modified version of the OWA login page as shown below which is enhanced with an OTP login dialogue. Users should enter their username and password as usual but add the OTP code from their FortiToken or FortiToken Mobile as the second factor.
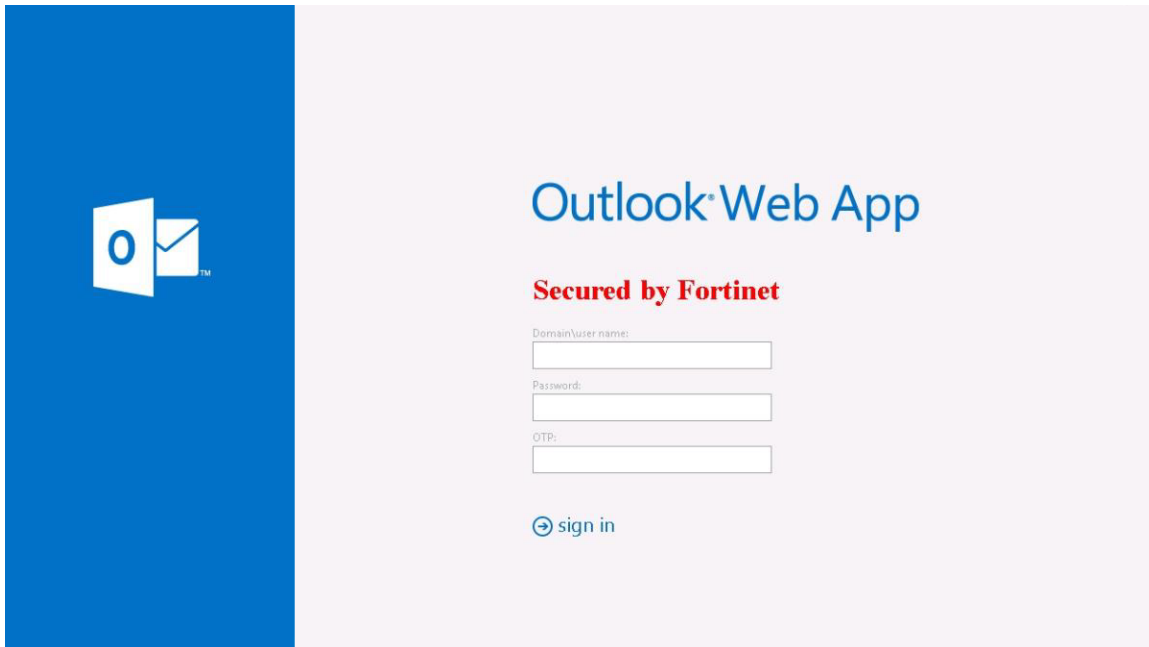
This template can be modified by editing the webpage CSS/JS if required.

While this plugin protects Microsoft IIS with Outlook Web Access, two-factor authentication will not be applied to other protocols such as POP3/IMAP traffic.

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.

FÜRTINET.