FortiAuthenticator - Agent for Microsoft Windows Administration Guide

VERSION 4.3

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

FORTICAST

http://forticast.fortinet.com

CLI REFERENCE

http://cli.fortinet.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

3/21/2017

FortiAuthenticator 4.3 Agent for Microsoft Windows Administration Guide

23-430-264234-20170321

TABLE OF CONTENTS

Change Log

Date	Change Description
2013-10-23	Initial release.
2013-12-09	Amended supported OS list.
2014-02-04	Updated release.
2016-11-24	Updated Agent installation screenshots and supported OS for Agent v.1.7.0.
2017-03-21	Updated for new feature: Offline Token Configuration (applicable only to FortiAuthenticator 4.3 and newer). Updated Agent installation version to 2.0.2.

Introduction

This document introduces FortiAuthenticator Agent for Microsoft Windows, a plugin for Windows domain PCs that allows a FortiAuthenticator OTP to be inserted into the Windows authentication process.

The document covers the installation and configuration of the FortiAuthenticator Agent on a supported Microsoft Windows system and configuration of the FortiAuthenticator.

FortiAuthenticator Agent for Microsoft Windows

FortiAuthenticator Agent for Microsoft Windows is a Credential Provider plugin for Windows operating systems that allows a FortiToken OTP, validated by FortiAuthenticator, to be inserted into the Windows authentication process.

The modified login process requires Username and OTP (One Time Passcode) to be validated via the FortiAuthenticator, and the Username and Password validated as normal via AD (Active Directory).

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

This administration guide is based on FortiAuthenticator Agent for Microsoft Windows v.2.0.2.

Supported Operating Systems

Server Operating System	
Windows Server 2008	• DataCenter (x86/x64) • Enterprise (x86/x64)
Windows Server 2010	• R2 DataCenter (x86/x64) • Enterprise (x86/x64)
Windows Server 2012	• Standard (x64) • DataCenter (x64)
Desktop Operating System	
Windows Vista	• Ultimate (x86/x64) • Business (x86/x64) • Enterprise (x86/x64)
Windows 7	• Professional (x86/x64) • Ultimate (x86/x64) • Enterprise (x86/x64)

Windows 8	• Professional (x86/x64) • Enterprise (x86/x64)
Windows 10	• Professional (x86/x64) • Enterprise (x86/x64)

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

Microsoft Windows XP is not currently supported as it has reached end of support with Microsoft. Please contact your Fortinet Account Manager if this is an issue.

System Requirements

FortiAuthenticator Agent for Microsoft Windows v.2.0.2 has the following system requirements:

- 20 MB of free disk space
- TCP/IP networking
- Microsoft .NET Framework 4 Client Profile or later
- Visual Studio C++ 2012 redistributable packages

Microsoft .NET Framework and Visual Studio C++ redistributable packages will be automatically downloaded and installed if required. An internet connection is required, otherwise these packages can be installed manually before proceeding with the installation.

Required Ports

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

Port	Destination	Description
TCP/443	FortiAuthenticator	Used but the FortiAuthenticator Agent for Microsoft Windows to validate the entered Two-Factor Authentication Token.
TCP/389	Windows Domain Controller	Indirectly used by the FortiAuthenticator Agent for Microsoft Windows to verify group membership of the user in order to identify if Two-Factor Authentication should be applied.

Third Party Trademark Notice

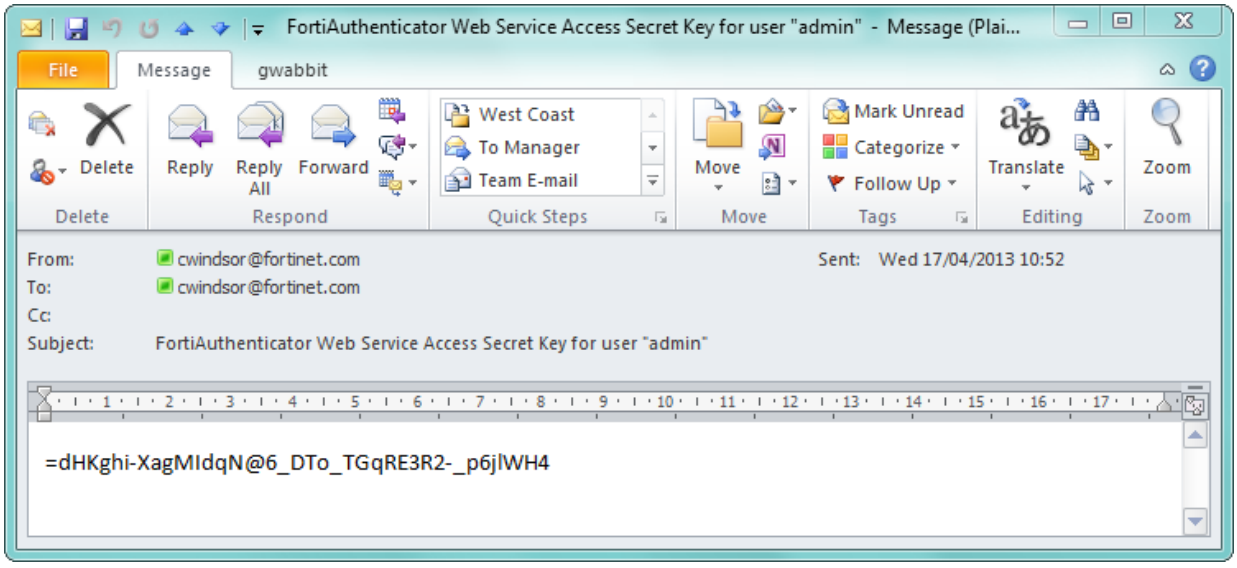
Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

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 Windows 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* > *Messages* > *SMTP Servers* and set it as active in *System* > *Messages* > *Email Services*.

1. Log into the FortiAuthenticator.
2. Edit the admin user in *Authentication* > *Local User Management* > *Local Users* and enable *Web Service Access* in the *Role* section. Click *OK* and an email containing the API Key for that user will be sent.

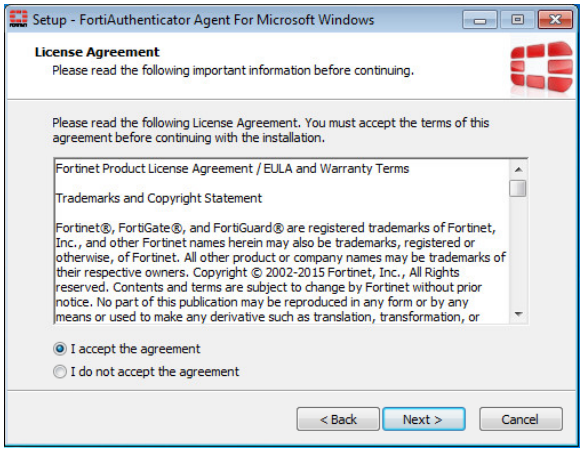


The required users should be imported via LDAP and assigned a FortiToken with which to authenticate before proceeding.

Agent Installation Procedure

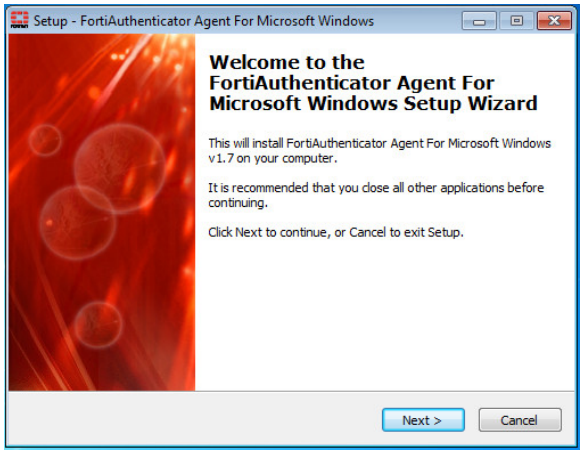
FortiAuthenticator Agent for Microsoft Windows is designed for installation onto a Domain connected system. On the desktop you wish to perform two-factor enhanced login:

1. Run the FortiAuthenticator Agent 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.
2. Read and accept the *License Agreement* and either install to the default installation location or select a more suitable location.

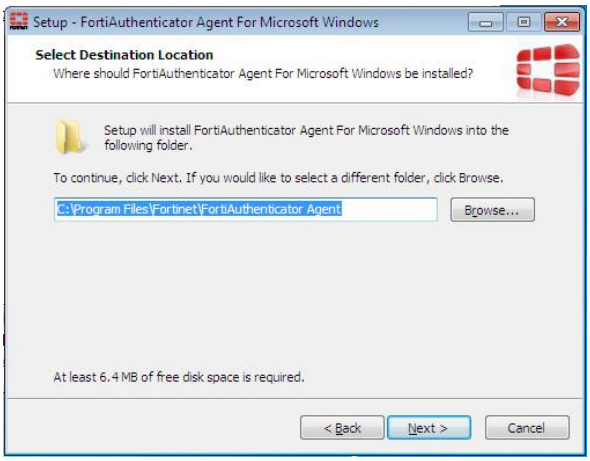


1. The .Net 4.0 Framework and Visual Studio C++ redistributable packages are required and will be downloaded and installed as part of the process.

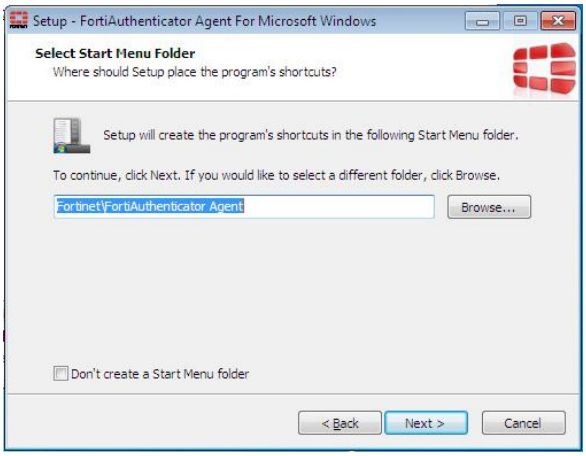
   FortiAuthenticator Agent for Microsoft Windows will now begin to install.



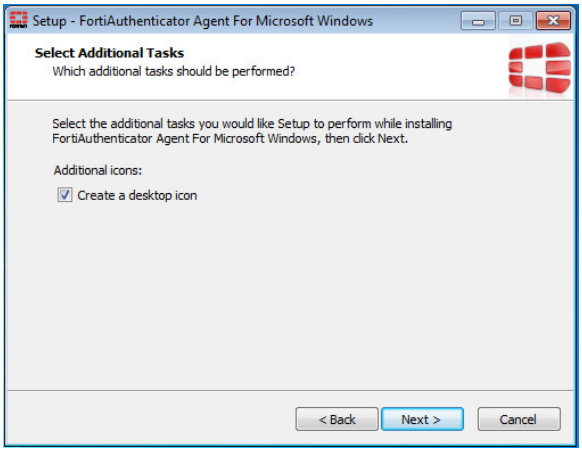
2. Select *Next* to continue with the installation.



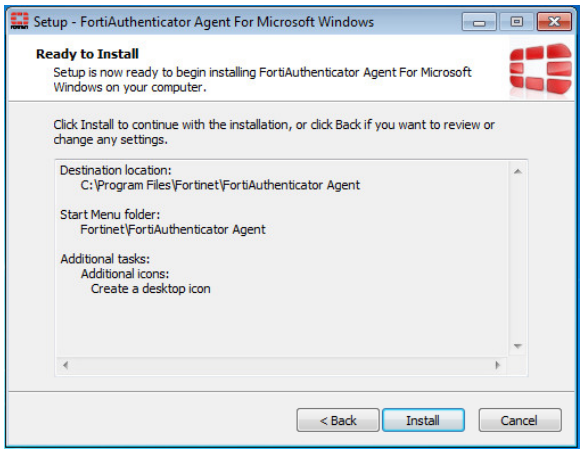
3. Select the appropriate installation location.



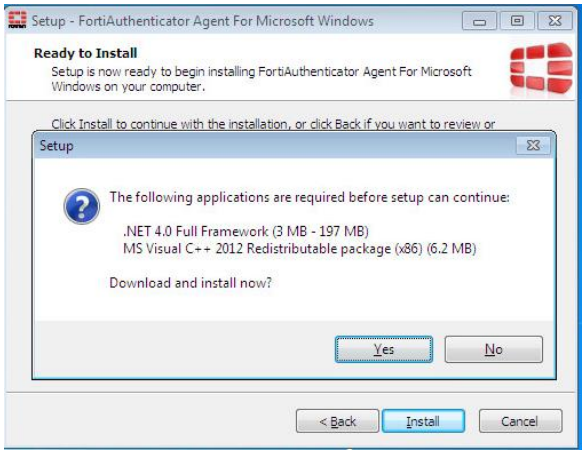
4. Select the appropriate start menu folder.

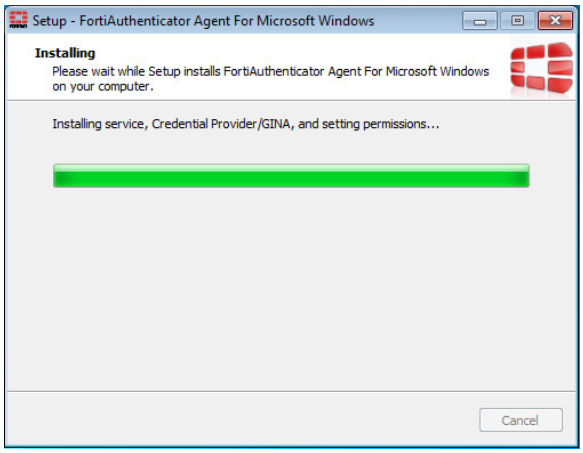


5. Select to create a desktop icon to open the FortiAuthenticator Agent configuration utility (disabled by default).



6. The setup is now ready to proceed. If there are any unfulfilled dependencies such as the need for the .NET Framework of MS Visual C++ libraries, they will be displayed here. Select *Install* to continue.





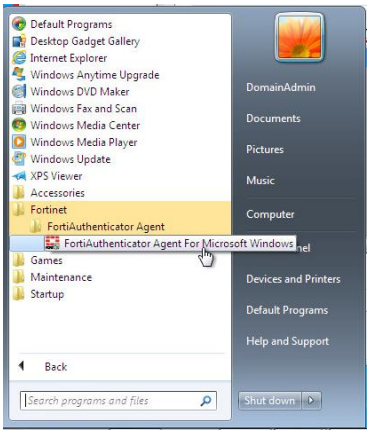
7. The required dependencies will be automatically downloaded at this point, so ensure the system has internet access before proceeding. Alternatively, these packages can be downloaded and manually installed.

The installation is now complete. Launch the FortiAuthenticator Agent for Microsoft Windows configuration utility to configure the specifics of your setup.

Agent Configuration

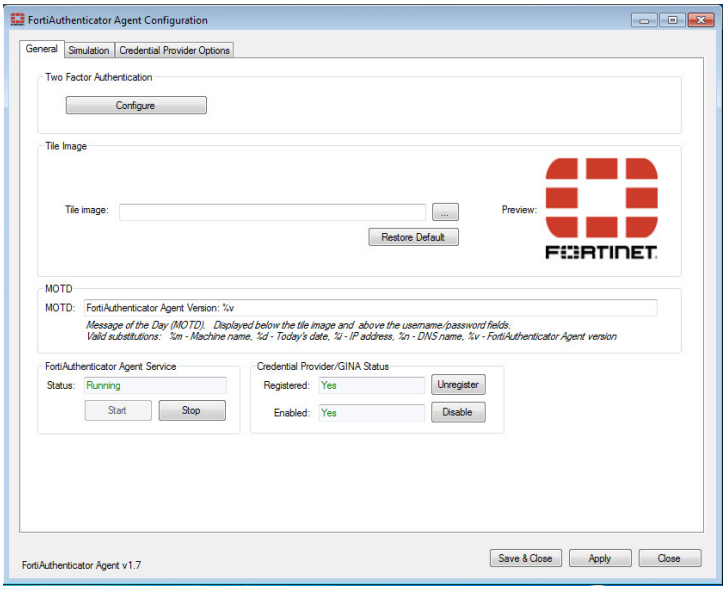
Once installed the FortiAuthenticator Agent Configuration utility will automatically open. This can also be started via the *Start* menu.

1. Go to *Start* > *All Programs* > *Fortinet* > *FortiAuthenticator Agent* > *FortiAuthenticator Agent for Microsoft Windows*.

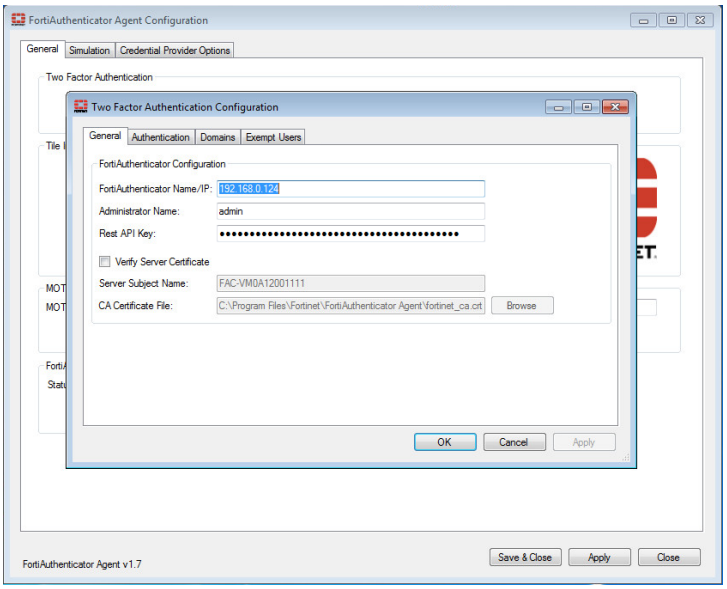


2. Select the *General* tab, and click the *Two Factor Authentication* > *Configure* button.

The *Simulation* tab, shown in the image below, is used for the testing of the login process and is not used in normal operation.



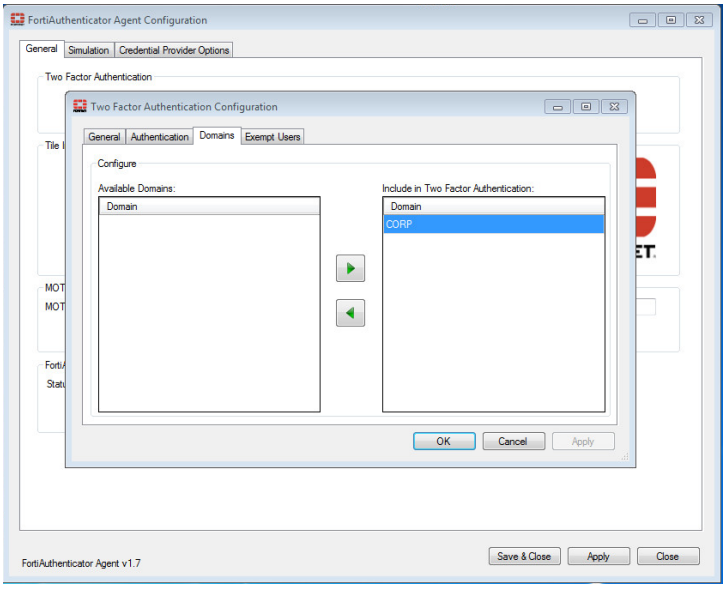
3. In the *Two Factor Authentication configuration* screen, configure the IP address, username and API key obtained in *FortiAuthenticator Configuration*.



4. For test purposes, disable *Server Certificate Verification*. This can be configured once the installation has been tested and proven working.

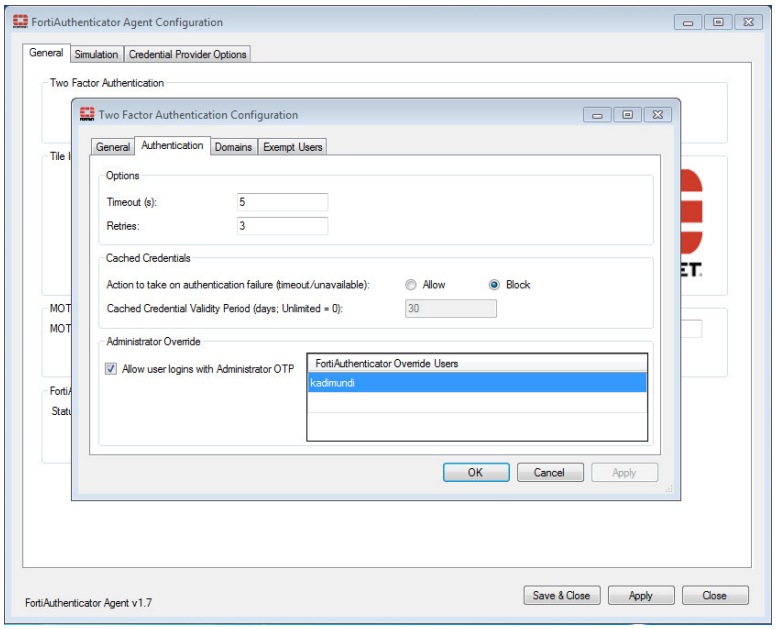
   If there is a Server Subject Name or CA Certificate File Specified, enable *Verify Server Certificate*, delete the entries and disable *Verify Server Certificate*. Authentication may fail in some circumstances if this is not performed. This issue will be resolved in a future release.

5. Select the *Domain* tab and select the domains you want to include in the Two-Factor Authentication process by clicking the arrow.



Optional Configuration Settings

FortiAuthenticator Agent for Microsoft Windows includes a range of settings specific to the behavior in the event of failure and when recovery is required. These features are described below.



Timeout

Timeout configures the behavior to adopt should the FortiAuthenticator become unavailable or slow to respond. The timeout for which a request is considered to be unresponsive is set to 5 seconds and 3 consecutive requests will be made resulting in 15 seconds required for an unavailable system to time out. These default settings can be customized to make the system time out sooner or later if necessary.

Cached Credentials

The Cached credentials configuration details how the system should behave if the device is away from the domain and the domain controller is not available to process the login. In this situation cached credentials can be allowed by the administrator to enable users to continue working, such as when at home. Cached credentials are accepted for the Validity Period specified, after which time the user must return to the domain and properly authenticate.

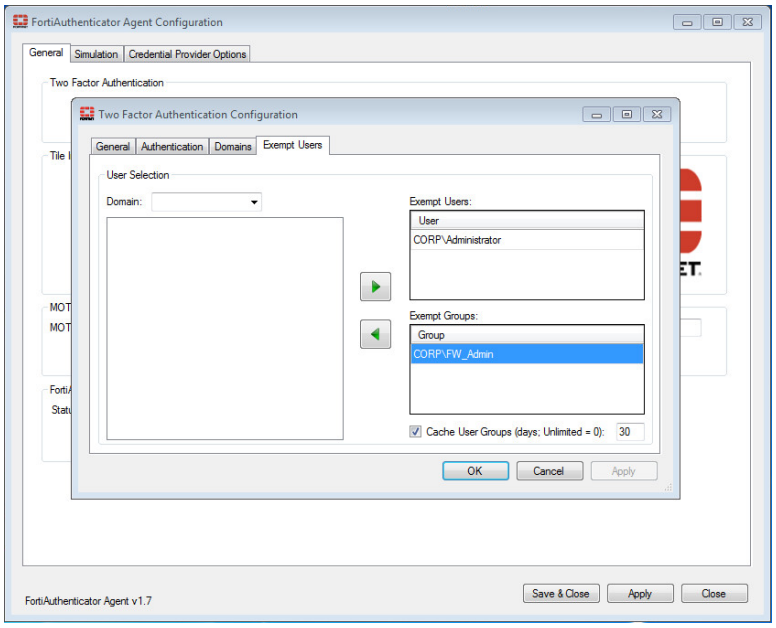
Override Users

Override users are users whose tokens can be used to log other users into their systems. The purpose of such an override is to allow emergency access to a system when a user token is not available (e.g. lost, forgotten, or misplaced).

When this feature is enabled, the user can log in with the *Administrator Override* checkbox enabled. This creates an additional dialog during the login process to enter the Administrator Name that corresponds to the Override OTP Token.

Exempt Users and Groups

If local administrators are removed from Windows, and all domain users are protected by two factor authentication, but the Agent/FortiAuthenticator are misconfigured, this can lead to issues where users are permanently locked out of the system — this may require a system reinstallation. It is therefore recommended that at least one exempt user is configured who can log in without the need to enter a two-factor authentication token. You may also exempt user groups.

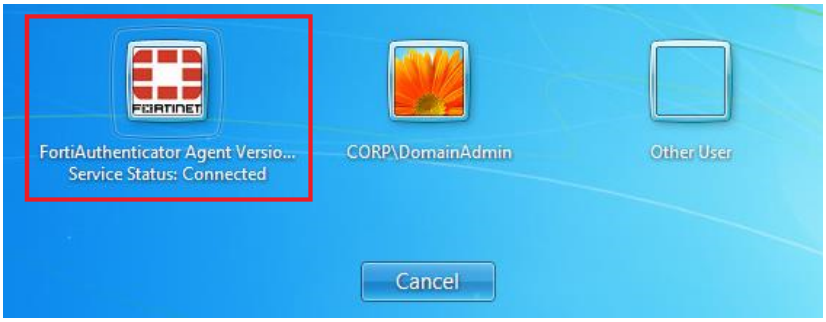


Exempt users can log in and recover any misconfiguration, avoiding the need for reinstallation of the operating system.

Agent Testing

Once installation and configuration is complete, log out from the account and attempt to log in using the FortiAuthenticator Two Factor Authentication enhanced service.

1. Select the FortiAuthenticator Agent Login option.



2. Use the dropdown box to select the domain which you are a member of. The drop down is not mandatory and the user may supply usernames of the form *DOMAIN\Username* or *Username@domain.com*. The user should not do both, however (i.e. select from the dropdown and use DOMAIN\username).
3. Enter your username, AD password, and your FortiToken Passcode. Note that this is a OTP. If it has been used to log in previously on this or any other system, please wait for the next passcode.

If login fails, see Appendix A - Debugging to identify the issue.

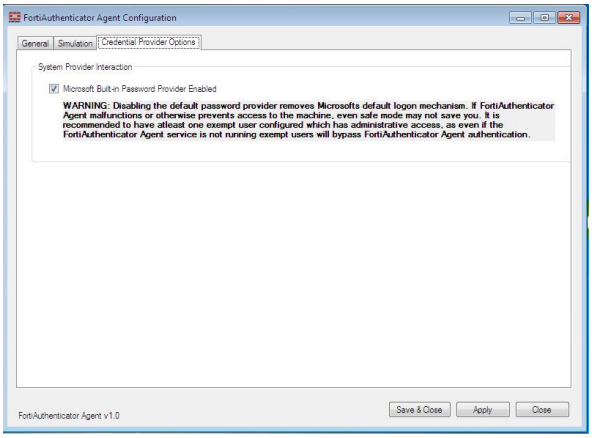
Live Deployment

If incorrectly configured, the following changes could result in being permanently locked out of the system. Please test first on a non-critical system before proceeding.

It is highly recommended that a method to bypass two-factor authentication in the case of misconfiguration is enabled such as that described in Exempt Users.

In the mode shown in Agent Testing, the use of the token code can be bypassed by selecting the *Other User* login method, bypassing the FortiAuthenticator Agent, and the requirement for a OTP. In a live system, it would be necessary to prevent this bypass in order to enforce two-factor authentication. To do this:

- Open the FortiAuthenticator Agent GUI, select *Credential Provider Options*, and uncheck the *Microsoft Built-in Password Provide enabled* option.



When the user attempts to log in again, the login dialog will be restricted to FortiAuthenticator Agent Login only.

Offline Token Configuration

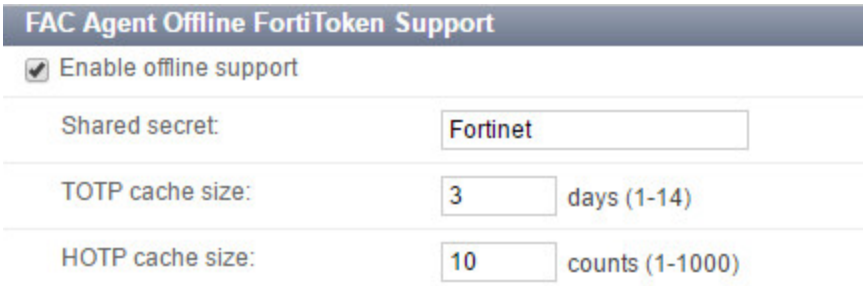
The instructions below describe how to configure FortiAuthenticator Agent offline token support. This functionality is only supported in FortiAuthenticator 4.3. and newer. Testing was based on 4.3.1 GA code.

This section includes:

FortiAuthenticator Configuration

Configure the FortiAuthenticator to enable offline token support:

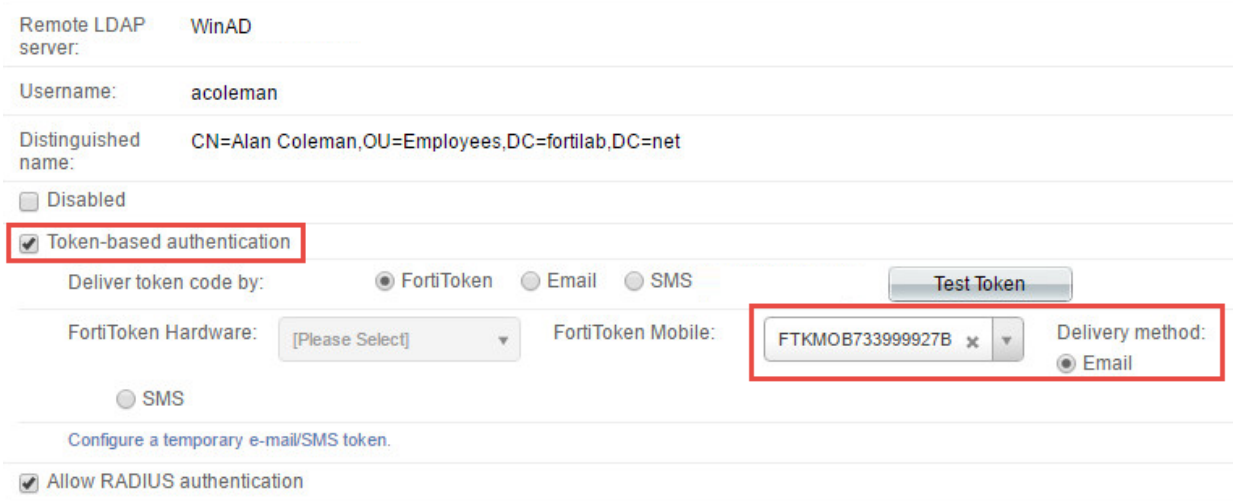
1. Go to *Authentication* > *Tokens*.
2. Under *FAC Agent Offline FortiToken Support*, select *Enable offline support*.



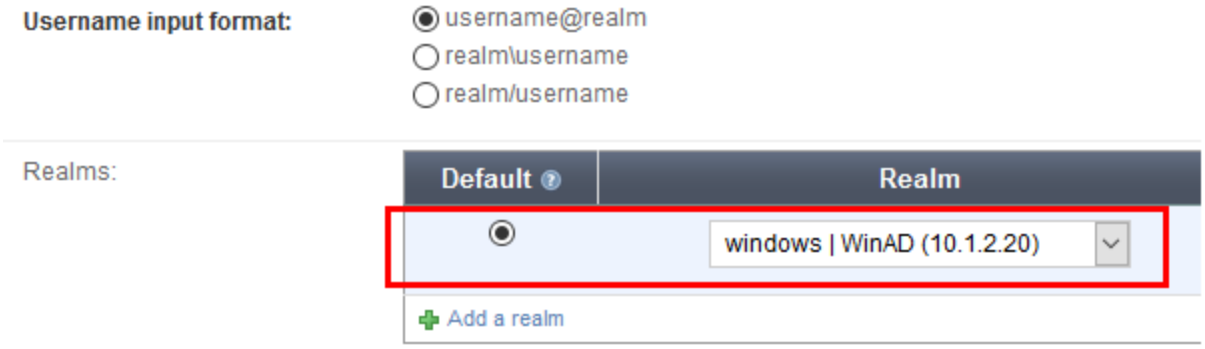
Now we need to generate the Web Service Key for the Windows agent to talk to FortiAuthenticator with an associated administrative account. Once you enable this on the account the key will be emailed to the email address in the account details from FortiAuthenticator.

3. Go to *Authentication* > *User Management* > *Local Users* and edit the admin account.
4. Under *User Role*, enable *Web service access* and provide the appropriate *Email address* under *User Information*.

5. Go to *Authentication* > *User Management* > *Remote Users* and ensure that LDAP users are imported in FortiAuthenticator and Tokens are enabled.



6. Go to *Authentication* > *Self-service Portal* > *Access Control* and set the Access Control realm to the LDAP server where we want the users to be authenticated.



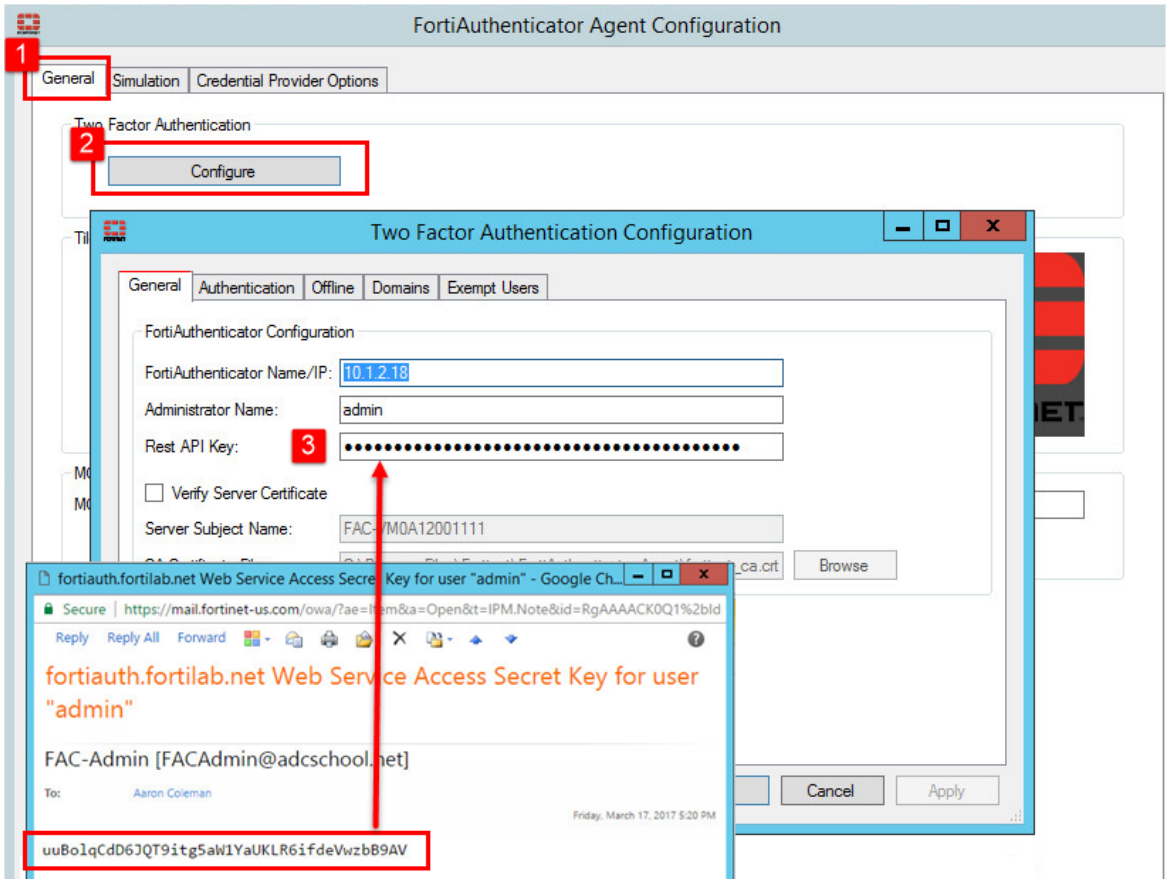
FortiAuthenticator Agent for Windows Configuration

Now we need to setup the FortiAuthenticator Agent for Windows.

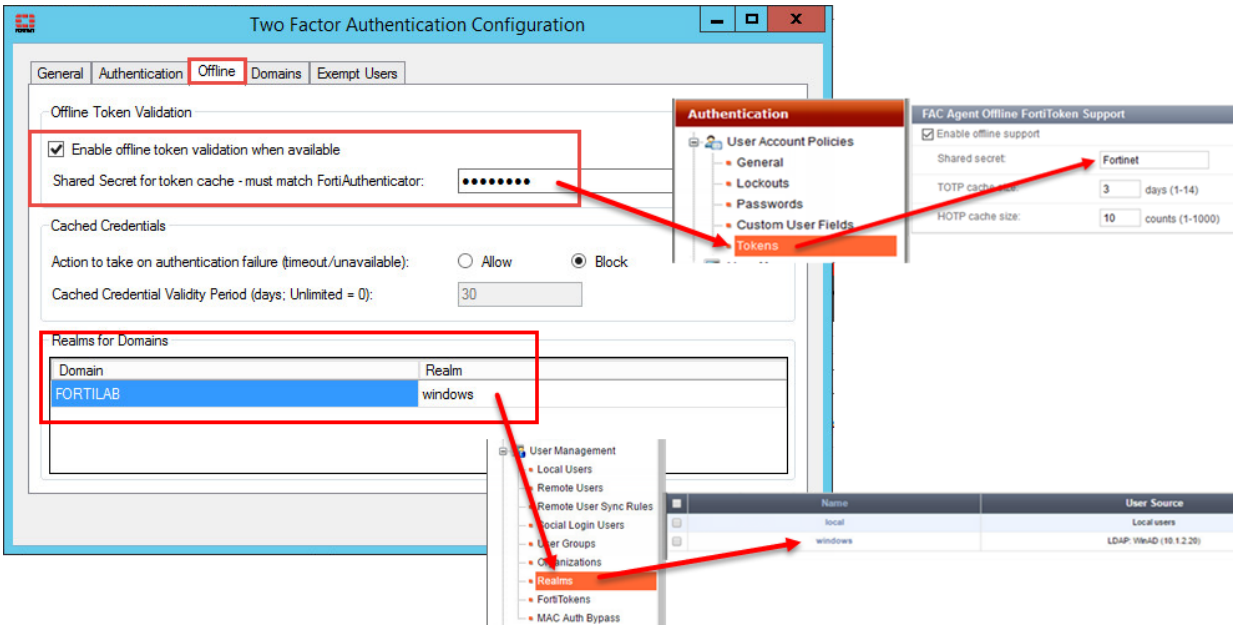
Log on to the host system where the Windows agent has been installed. Follow the steps below to configure the agent to communicate with FortiAuthenticator.

1. Select the *General* tab and click the *Configure* button to load the configuration settings.
2. Verify the IP address of the FortiAuthenticator server and the administrator account name.

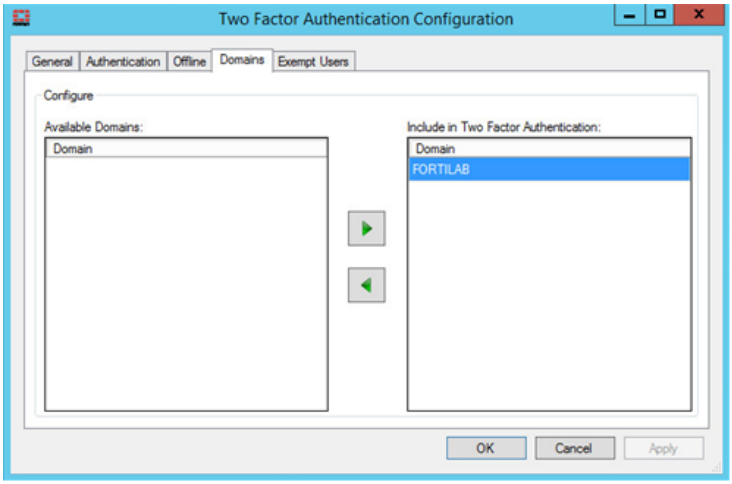
3. Copy the '*Web Service Key*' that was emailed to the administrator account into the *Rest API Key* box .



4. Next, select the *Offline* tab and verify the following:
   - Check the *Enable offline token…* box.
   - Enter the *Shared Secret* that was set on the FortiAuthenticator (*Authentication* > *User Account Policies* > *Tokens*).
   - Verify the *Domain* is the correct AD Domain and the *Realm* **MUST BE** the exact realm setup in FortiAuthenticator that points to the LDAP directory (*Authentication* > *User Management* > *Realms*).



5. In the *Domains* tab, select the AD Domain and move it into the *Include in Two Factor Authentication:* column.



This completes the configuration of the Windows agent.

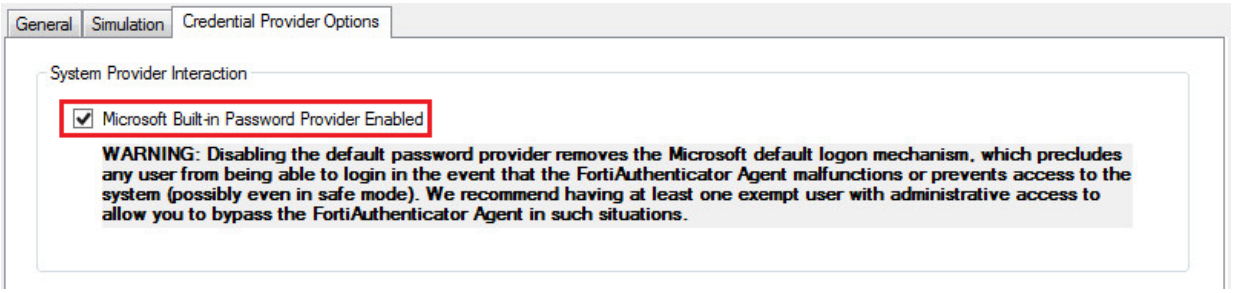
You will need to log in to the host system in an online mode initially so that the agent can sync the offline tokens from FortiAuthenticator. Then the offline tokens will be cached.

Before the agent and FortiAuthenticator sync, make sure the host system time and the time on FortiAuthenticator are in sync. If the time is off by several minutes, the offline tokens will not work.

Credential Provider Options

By un-checking the option for the default *Microsoft Built-in Password Provider*, we eliminate the ability for domain users to bypass the agent when logging in. It is enabled by default on the Agent for safety reasons.

The Administrator has to un-check that option and save changes. Once that's done, the default Windows credentials provider (e.g., "Other User" option) will no longer be available.



Appendix A - Debugging

Common login errors

The authentication order when authenticating a user with FortiAuthenticator Agent for Microsoft Windows is:

Username + One Time Passcode	→	FortiAuthenticator
Username + Password	→	Windows Domain Login

This is important when diagnosing issues with the login process.

Verification of Users OTP failed: 401 Not Authorized

The OTP validation is the first step in the authentication process. The OTP failed error suggests that the FortiAuthenticator is reachable, but the user does not exist on the FortiAuthenticator. This are a few reasons for this to occur:

Cause	Resolution
User mistyped username (will be visible in the login GUI and FortiAuthenticator logs)	*User must reattempt with correct credentials*
User has not been provisioned on the FortiAuthenticator	*Contact your FortiAuthenticator administrator*

Verification of Users OTP failed: 401 Not Authorized

The OTP failed error suggests that the FortiAuthenticator is reachable, but is responding with an authentication error, i.e. the incorrect username/OTP combination has been entered. There are several reasons for this to occur:

Cause	Resolution
User is using a token not assigned to them. Only the token assigned to the user in the FortiAuthenticator database can be used for authentication.	*Use the assigned FortiToken*
The user is configured in FortiAuthenticator but does not have a FortiToken assigned.	*Contact your FortiAuthenticator administrator*
The user is using a FortiToken OTP (the digits from the token) that has been used previously to authenticate. This may include on another system, or in a previous failed attempt to log into the current system.	*Wait for a new OTP to be generated and retry*
Token is out of sync.	*Log into the FortiAuthenticator portal to resynchronize token*

Unknown User / Incorrect Password

The fact that the logon process has reached the point at which the password is being validated means that the Username and FortiToken OTP has been successfully validated. There are several possible reasons for such an error:

Cause	Resolution
User has mistyped their password.	*Retry login with the correct AD password. Remember to wait for a new FortiToken OTP otherwise the OTP validation will fail.* *User should follow organizational password reset procedure if problems persist.*
The user has been deleted from AD since they were imported into FortiAuthenticator.	*Contact the AD administrator.*

Appendix B - Installation CLI Commands

Installation requires AD access - ensure installation user has access to query domain information from AD and the workstation is online. If not FortiAuthenticator Agent may not fully function until the configuration application is manually run and settings fixed.

Installation parameters

The following command line parameters are supported during installation:

`/SP-`

Disables the "*This will install... Do you wish to continue?*" prompt at the beginning of Setup.

`/SILENT`

Instructs Setup to be silent. When setup is silent the wizard and the background window are hidden but the installation progress window is displayed.

`/VERYSILENT`

Instructs Setup to be very silent. As per `/SILENT` but the install progress window is also hidden.

`/SUPPRESSMSGBOXES`

Instructs Setup to suppress message boxes. Only has an effect when combined with `/SILENT` and `/VERYSILENT`.

`/DIR="x:\dirname"`

Overrides the default directory name displayed on the Select Destination Location wizard page. A fully qualified pathname must be specified.

`/GROUP="folder name"`

Overrides the default folder name displayed on the *Select Start Menu Folder* wizard page.

`/NOICONS`

Instructs Setup to initially check the *Don't create a Start Menu folder* check box on the *Select Start Menu Folder* wizard page.

General configuration settings

`/DISABLEMSPROVIDER`

Disable the default Microsoft Built-in Password Provider.

Disabling the default password provider removes Microsoft's default logon mechanism. If FortiAuthenticator Agent malfunctions or otherwise prevents access to the machine, even safe mode may not resolve the issue.

When enabling this feature, it is recommended to have at least one exempt user configured who has administrative access. This will mean that even while the FortiAuthenticator Agent service is running, exempt users can bypass FortiAuthenticator Agent authentication.

If the built-in provider remains enabled, users can bypass two factor authentication by using the default provider.

Two Factor Authentication settings

`/FACHOST=host name`

Set the value of the FortiAuthenticator host name/IP address.

`/FACRESTADMIN=admin name`

Set the value of the FortiAuthenticator administrator for which Web Services have been enabled.

`/FACRESTKEY=api key`

Set the value of the key to be used for Web Services access.

`/FACVERIFYSERVERCERT`

Enable verification of the FortiAuthenticator web server certificate.

`/FACSERVERSUBJNAME=subject name`

The web server certificate subject name (e.g. CN=<server subject name>). The default firmware server certificate uses the FortiAuthenticator serial number (e.g. FAC-VM0A12001111).

`/FACCACERTFILE="ca certificate file path"`

The CA certificate which issued the web server certificate. By default this is the Fortinet CA which comes pre-installed in the FortiAuthenticator Agent installation directory.

`/AUTHNUMRETRIES=number of retries`

The number of two factor authentication retries that are made when a timeout occurs/the FortiAuthenticator is unavailable/etc.

`/AUTHTIMEOUT=timeout`

The timeout value for each two-factor authentication attempt in seconds. Upon timeout the next retry is attempted if configured to do so.

`/AUTHFAILACTION=fail action`

The action to take on authentication failure due to timeout/unavailability of the FortiAuthenticator. Allowed integer values are 0 (Block) and 1 (Allow).

`/AUTHCACHECREDPERIOD=validity period`

If the authentication fail action is set to 1 (Allow), users will be allowed to log on without two-factor authentication using cached credentials. This sets the number of days the user is allowed to log on offline without two-factor authentication before being locked out. Once locked out the user must reconnect to the domain and successfully authenticate with two-factor authentication with the FortiAuthenticator before their validity period is reset. Note that if this feature is enabled, the user **must** perform an initial successful two-factor authentication logon against the FortiAuthenticator for the validity period to take effect offline. If not, they will be locked out immediately when offline.

`/AUTHALLOWADMINOTP`

If enabled this allows the configured administrators to use their FortiToken to override the logon for a user. The user will still be required to enter their domain credentials, but instead of their OTP being provided the administrator provides their name along with their OTP (as configured on the FortiAuthenticator and in the administrator override names configuration field in FortiAuthenticator Agent). The administrator name and OTP are authenticated against the FortiAuthenticator, and the users credentials are used to continue the logon process (this also counts as a successful logon for cached credential validity period reset).

`/AUTHADMINOVERRIDENAMES="comma separated list of administrators"`

A list of administrators that will be allowed to perform administrator overrides, if overrides are enabled. These names must correspond directly with users defined on the FortiAuthenticator which are configured with FortiTokens. These can be either local users or imported remote users on the FortiAuthenticator, as long as the proper username is used.

`/INCLUDEDDOMAINS="comma separated list domains"`

This can be either a list of DNS domain names (e.g. domain.corp.com) or NetBIOS names (e.g. domain). Note that these will be validated during installation and need to match up with what the installation program detects directly through AD. If a specified domain is not found it will be ignored. These domains will force users to use two-factor authentication (as configured above, cached credentials when offline do not require a OTP if configured) if they belong to these domains. For all other domains no OTP is required and normal authentication operation takes place.

`/EXCLUDEDUSERS="comma separated list of exempt users"`

This is a list of users in the format "NetBIOS domain name\Username" separated by commas. These users are excluded from two-factor authentication regardless of whether the domain is configured for two-factor authentication. This bypass will occur even if the FortiAuthenticator service is not running.

e.g.

```
FAC_Agent_Setup_v1.0.exe /VERYSILENT /DISABLEMSPROVIDER
/FACHOST=192.168.0.123 /FACRESTADMIN=admin
/FACRESTKEY=X2=ByrYt1CgGyxLixYcZj7IFPT#7X5GSHieTlnwi

/FACVERIFYSERVERCERT /FACSERVERSUBJNAME=FAC-VM0A12000040
/FACCACERTFILE="C:\Program Files\Fortinet\FortiAuthenticator
Agent\fortinet_ca.crt"
```

```
/AUTHNUMRETRIES=2 /AUTHTIMEOUT=3 /AUTHFAILACTION=1
/AUTHCACHECREDPERIOD=23 /AUTHALLOWADMINOTP

/AUTHADMINOVERRIDENAMES="Administrator,Admin2,admin"
/INCLUDEDDOMAINS="de.test.com,BE,TEST,corp.com"
/EXCLUDEDUSERS="TEST\Administrator,TEST\manager3"
```

Appendix C - 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.