FortiAuthenticator Agent for Microsoft Windows - Install Guide

Version 3.2.0

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://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

January 29, 2021
FortiAuthenticator Agent for Microsoft Windows 3.2.0 Install Guide
23-320-641529-20210129

TABLE OF CONTENTS

Change Log

Date	Change Description
2020-09-16	Initial release.
2020-11-09	Added information about enabling REST API access on an interface to FortiAuthenticator configuration on page 7.
2021-01-29	Added Appendix D - FortiAuthenticator Agent for Microsoft Windows registry files on page 35.

Introduction

This document has been produced for FortiAuthenticator Agent for Microsoft Windows 3.2, 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 One Time Passcode (OTP), validated by FortiAuthenticator, to be inserted into the Windows authentication process.

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

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 3.2.

System requirements

FortiAuthenticator Agent for Microsoft Windows 3.2 has the following system requirements:

- 20 MB of free disk space
- TCP/IP networking
- Microsoft .NET Framework 4.6 Client Profile or later
- Visual Studio C++ 2019 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.

Minimum operating systems requirement

FortiAuthenticator Agent for Microsoft Windows 3.2 has the following minimum operating system requirements:

- **Server operating system**: Windows Server 2012
- **Desktop operating system**: Windows 8

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 FortiAuthenticator Agent for Microsoft Windows to validate the entered Two-Factor Authentication Token.
TCP/389	Windows Domain Controller	Indirectly used by 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

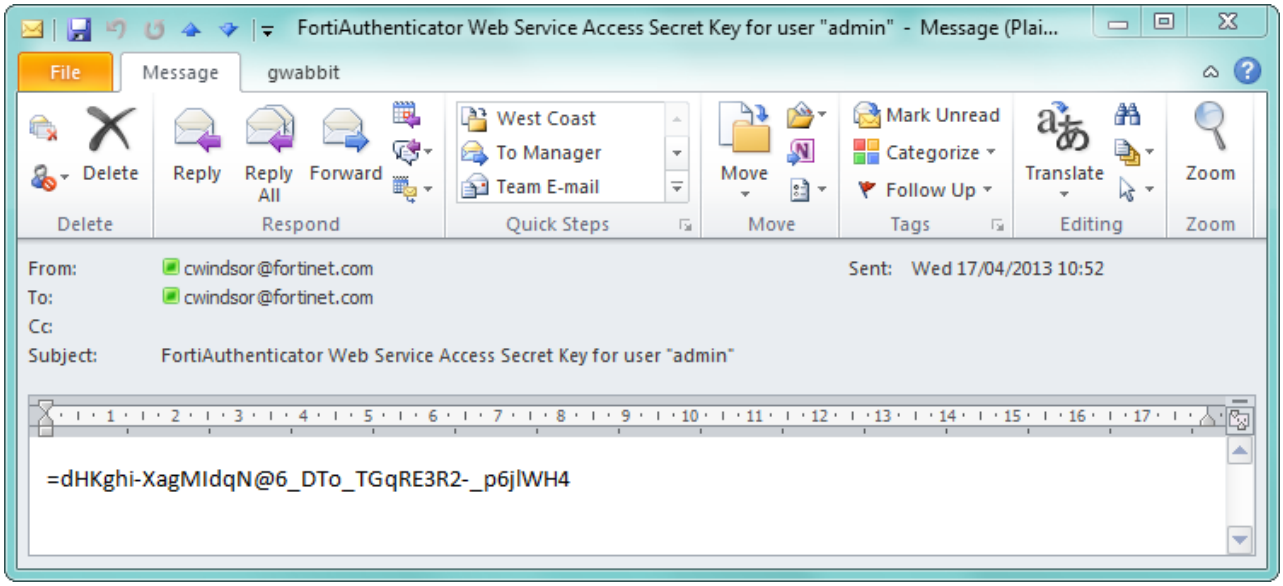
To enhance the Microsoft Windows operating system login with the use of a OTP (i.e. the two-factor authentication token), FortiAuthenticator Agent for Microsoft Windows uses the FortiAuthenticator REST API. To use the REST API, a key is required which must be generated before installing the desktop agent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

REST API admin access must be enabled on the FortiAuthenticator interface. To enable REST API on an interface, go to *System* > *Network* > *Interfaces*, edit the interface, and enable the *REST API (/api)* option.

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*.

To generate an API key:

1. Log into 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.

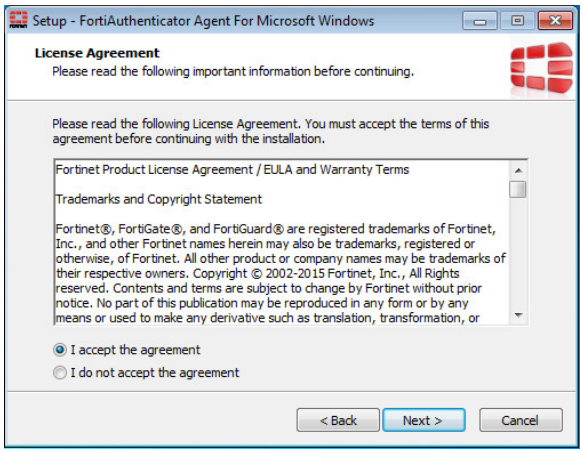
All network communications take place over TLS 1.2. As a result, the minimum required version of .NET Framework is 4.6.0. The Agent's installer will offer to install this when necessary.

To install FortiAuthenticator Agent for Microsoft Windows:

1. On the desktop you wish to perform two-factor enhanced login run the FortiAuthenticator Agent install file as a Domain Administrator.

   The Agent can also be installed via GPO. As the MSI file is not yet available, this can be done using the CLI install options /`VERYSILENT` and /`SUPPRESSMSGBOXES`.

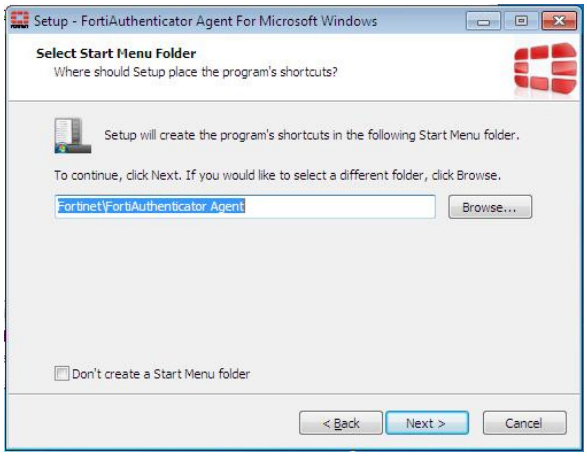
2. Read and accept the *License Agreement* and either install to the default installation location or select a more suitable location.



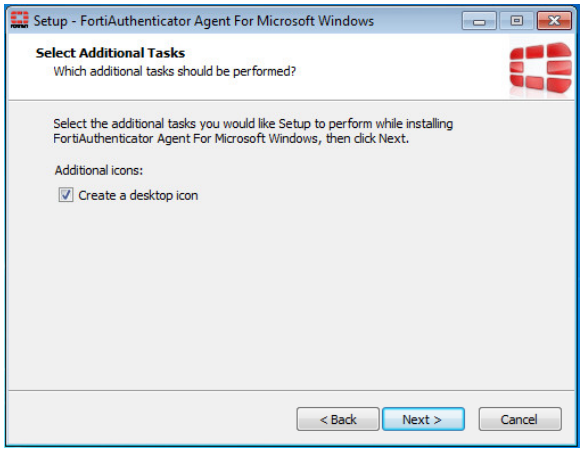
3. The .Net 4.6.0 Framework and Visual Studio C++ redistributable packages are required and will be downloaded and installed as part of the process.
   FortiAuthenticator Agent for Microsoft Windows will now begin to install.

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

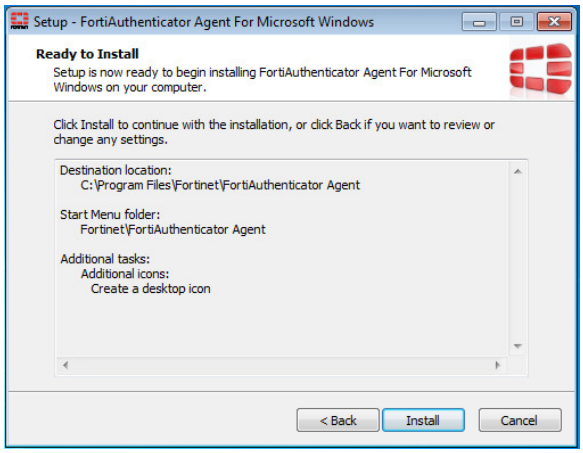
5. Select the appropriate installation location.



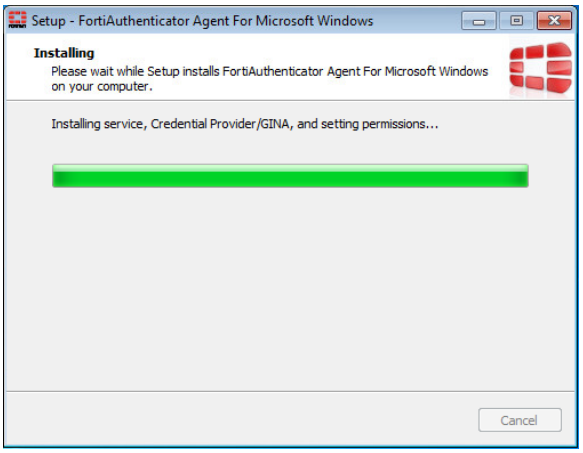
6. Select the appropriate start menu folder.



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



8. 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.



9. 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.

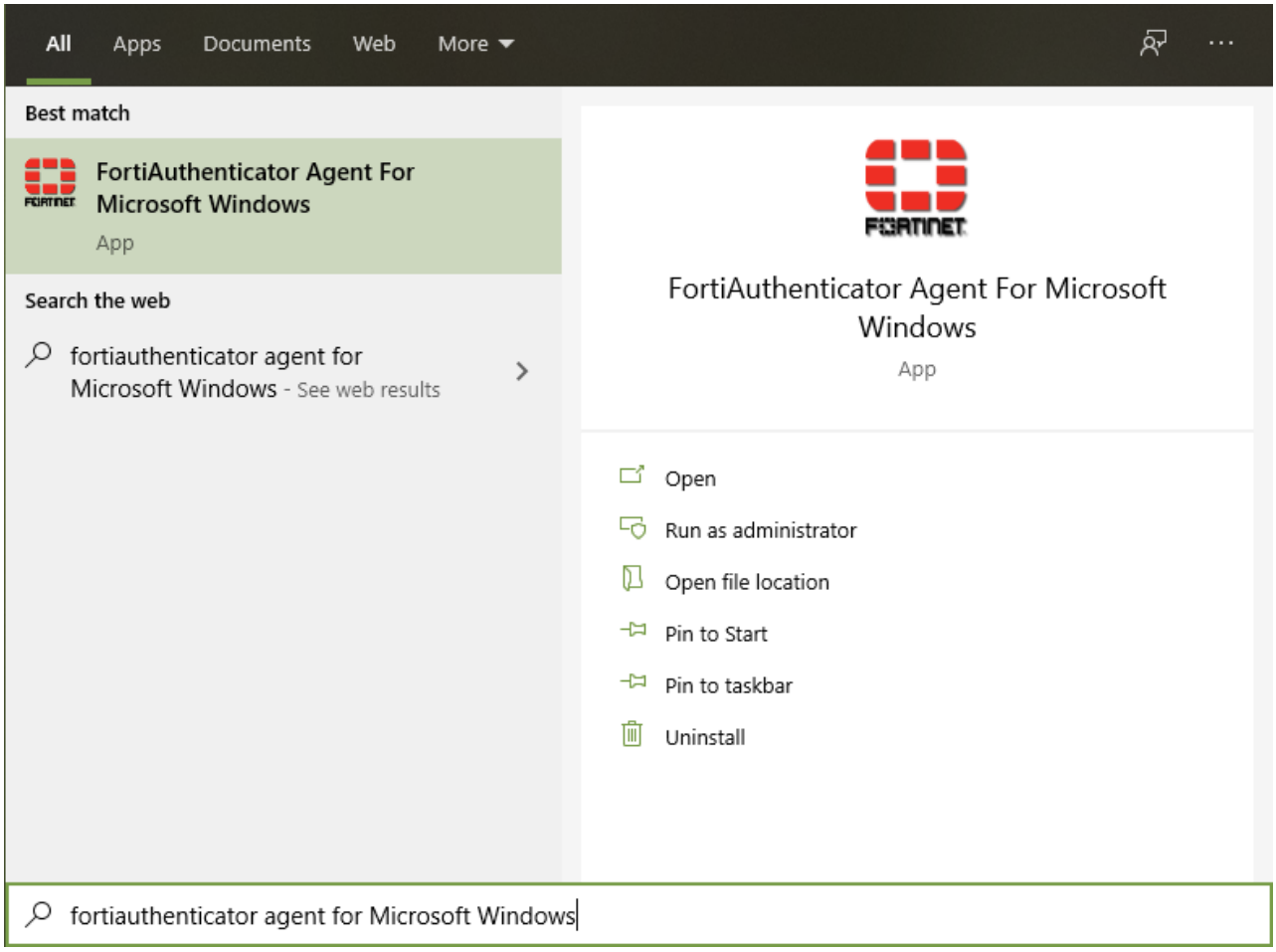
The installation is now complete. Launch the FortiAuthenticator Agent for Microsoft Windows configuration utility to configure the specifics of your setup.

Agent configuration

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

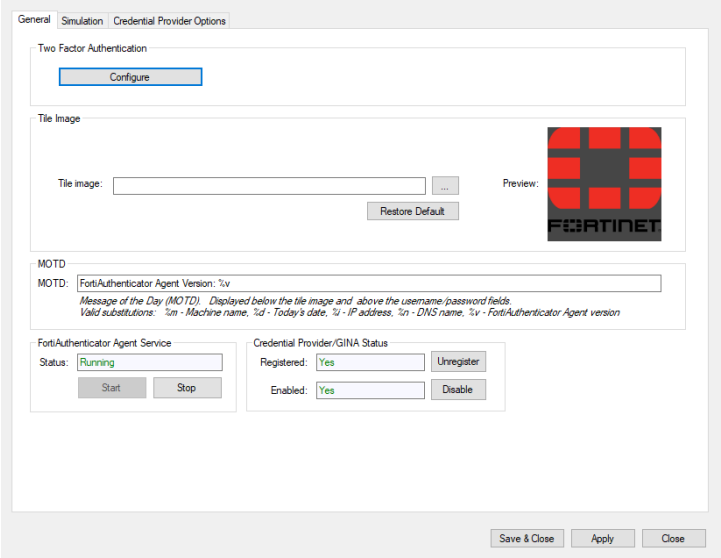
To configure FortiAuthenticator Agent for Microsoft Windows:

1. Launch the FortiAuthenticator Agent for Microsoft Windows.

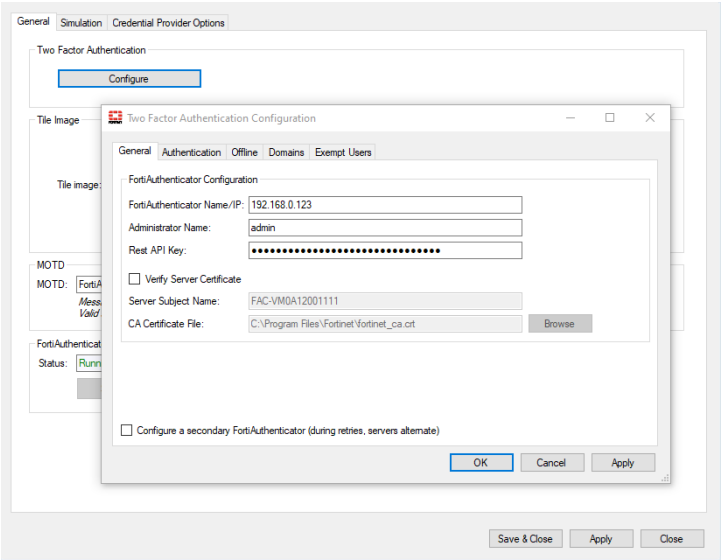


2. Select the *General* tab, and click the *Two Factor Authentication* > *Configure* button.

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*.



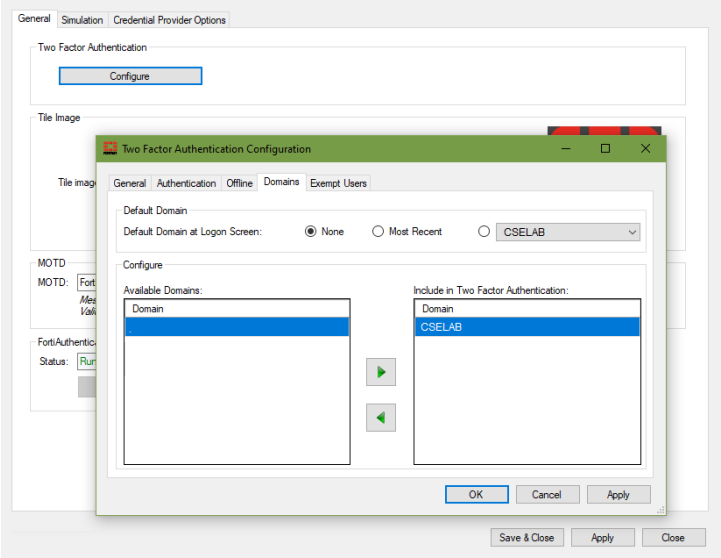
4. For test purposes, disable *Verify Server Certificate*. This can be configured once the installation has been tested and proven working.

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.

5. Select the *Domain* tab and select the domains you want to include in the two-factor authentication process by clicking the arrow.

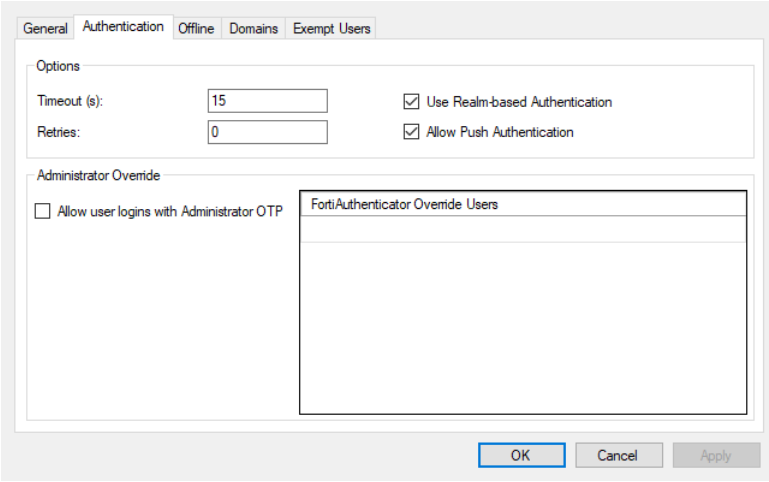
FortiAuthenticator Agent for Microsoft Windows contains the default domain "." which represents the local user. You can disable local user login by including the "." domain in the list of domains included in two factor authentication. When the "." domain is not included, login is enabled for local users.

6.



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 five seconds and three 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.

Allow Realm-based authentication

Allow Realm-based authentication is disabled by default and can be enabled to allow FortiAuthenticator Agent for Microsoft Windows to use Realm-based authentication methods.

To create a realm in FortiAuthenticator, go to *Authentication* > *User Management* > *Realms* and select the *Create New* button. The realm listed in the *Offline* tab of FortiAuthenticator Agent for Microsoft Windows two-factor authentication settings must match the realm created in FortiAuthenticator.

Allow Push Authentication

Allow Push Authentication is enabled by default and allows FortiAuthenticator Agent for Microsoft Windows to use two factor authentication push notifications.

To use FTM push authentication with FortiAuthenticator Agent for Microsoft Windows, enable *FortiToken Mobile API (/api/v1/pushauthresp)* on the configured FortiAuthenticator interface.

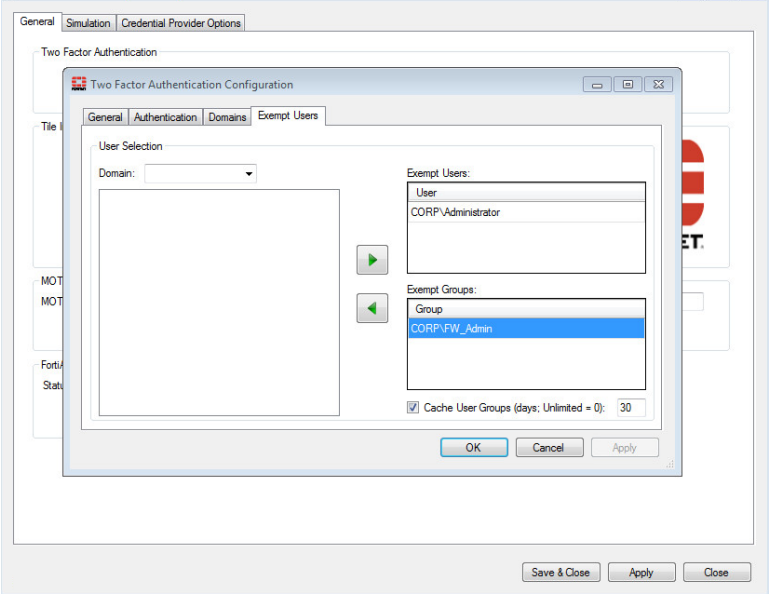
Override users

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.

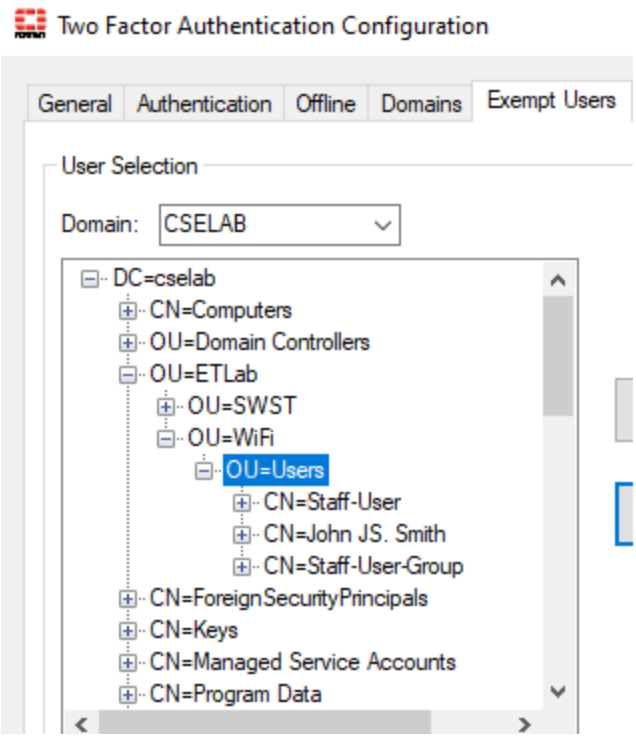
Exempt users and groups

If local administrators are removed from Windows and all domain users are protected by two factor authentication, but the Agent/FortiAuthenticator are incorrectly configured, 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.

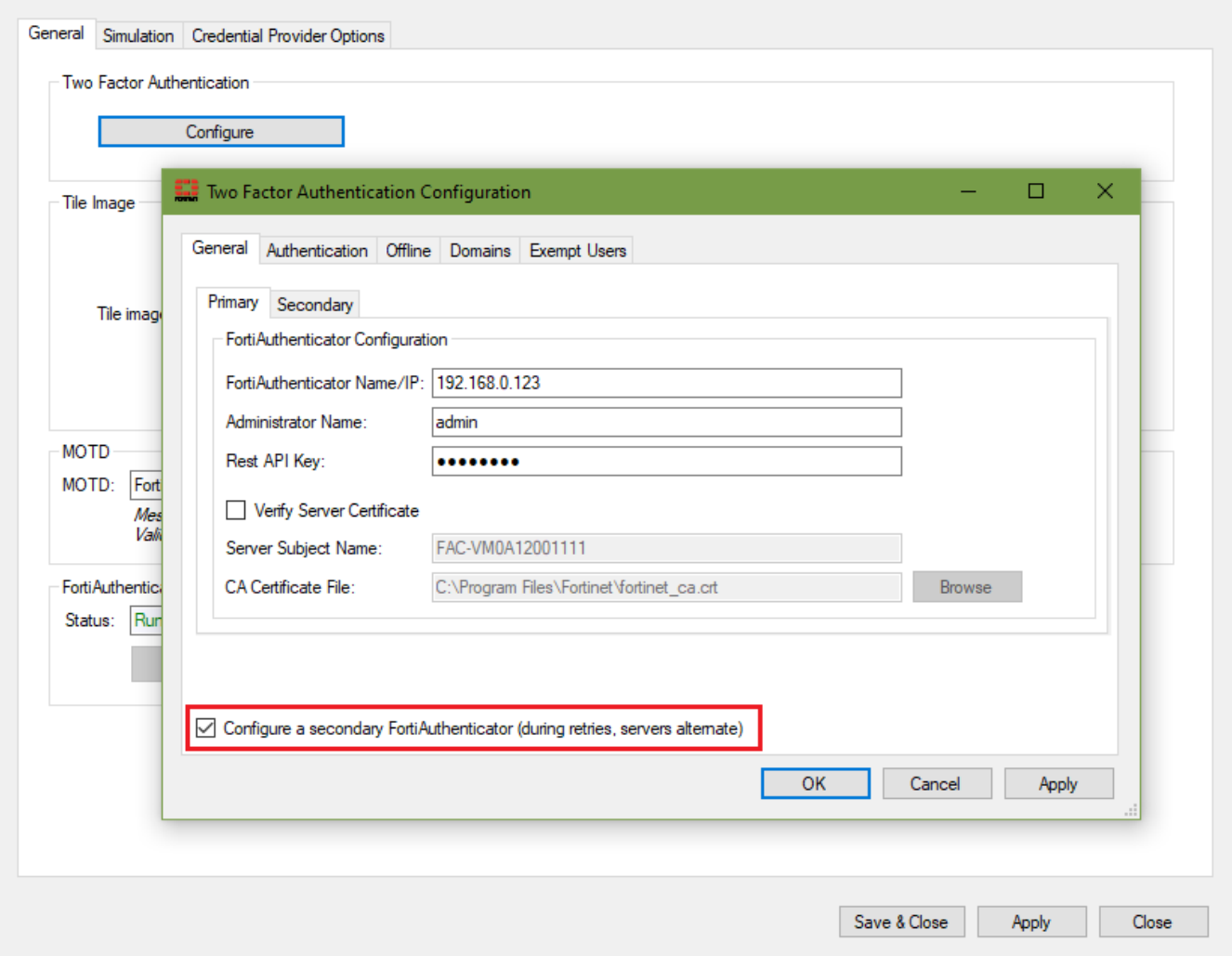
Exempt users can be selected from the domain in the *Exempt Users* tab when configuring two factor authentication settings.



Although the option to enter an OTP is displayed for exempted users, it is not required. When an exempt user clicks *Login* without submitting an OTP, they are automatically logged in.

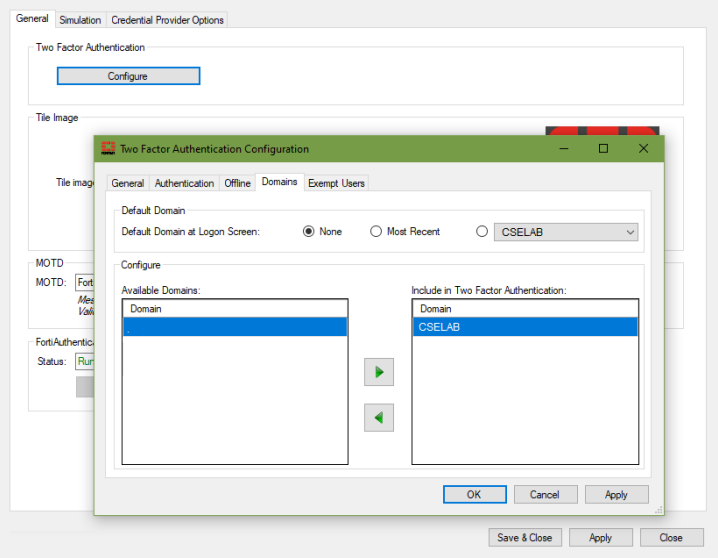
Contact secondary FortiAuthenticator for load-balancing HA

The agent can be set to try to reach a secondary FortiAuthenticator if the primary is unreachable. When configured, the primary and secondary are used round-robin style (for retries) upon each authentication.



Default domain for logon

The log on screen can be set to a default domain. Select from either *None*, *Most Recent*, or select a specific domain from the dropdown list available on the computer. For more information, see the Installation parameters.



Agent testing

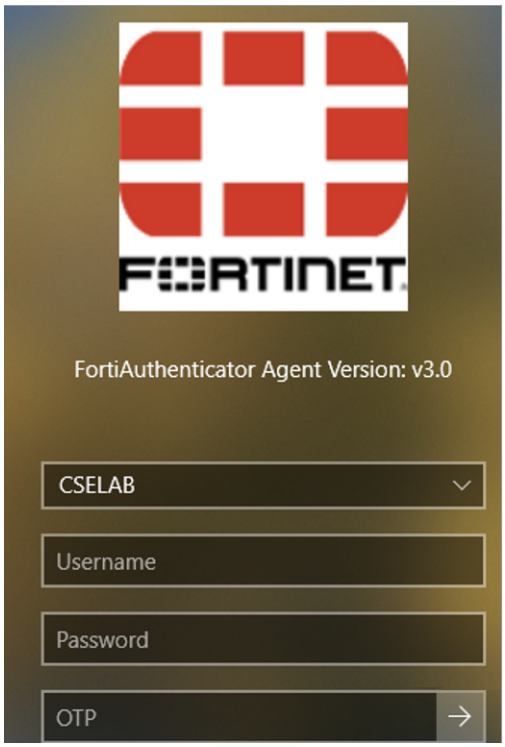
Once installation and configuration is complete, log out from the account and attempt to log in using the FortiAuthenticator two-factor authentication enhanced service.

To test the agent:

1. Select the FortiAuthenticator agent login application.
2. Use the dropdown box to select the domain of which you are a member.
   The dropdown is not mandatory and the user may supply usernames in the form `DOMAIN\Username` or `Username@domain.com`.

   If a domain is identified in both the username and dropdown, the agent will use the domain from the username by default.

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.
   When using push notifications, click the arrow next to *OTP* to send the push notification to your device.



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

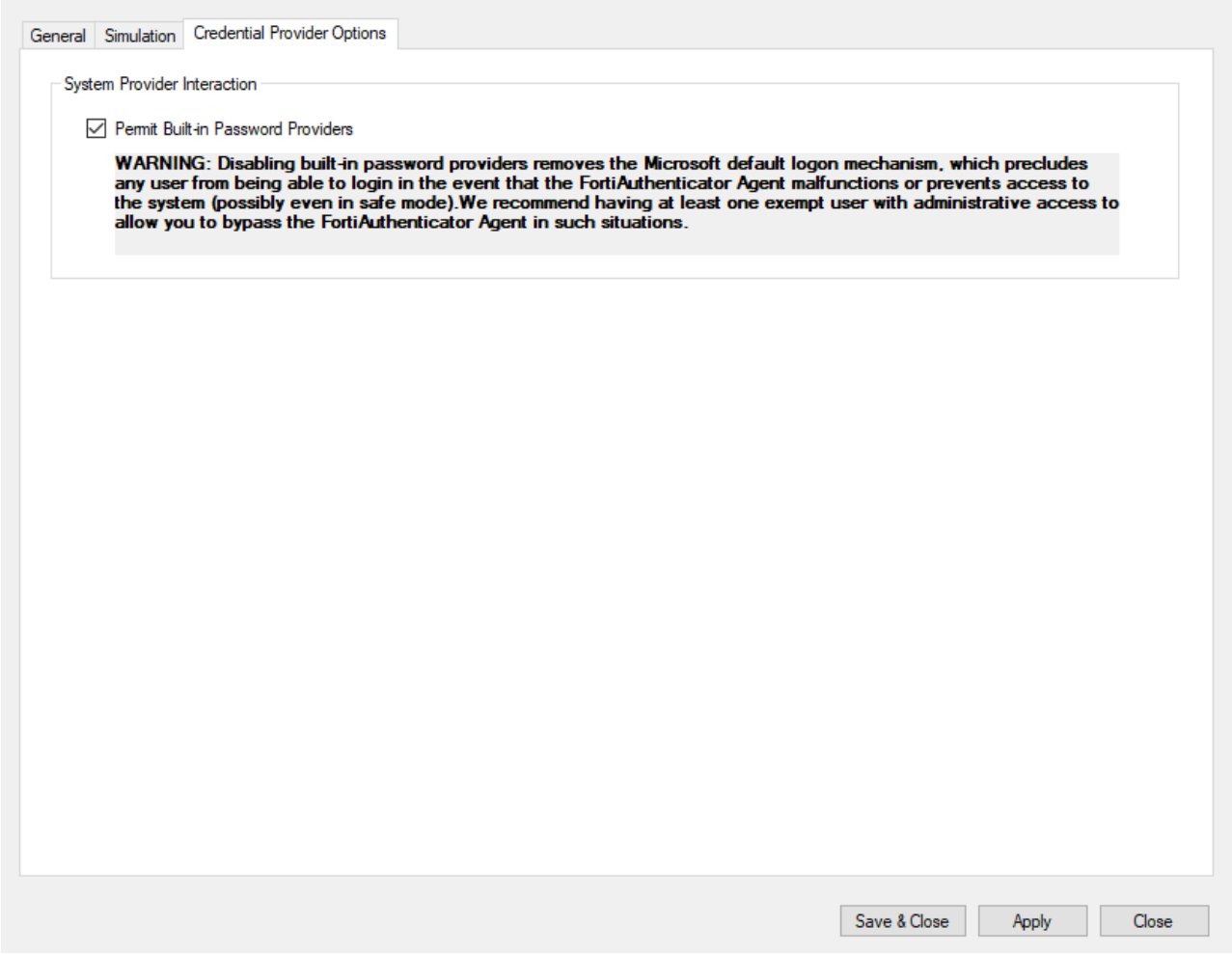
Live deployment

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 and groups.

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 *Permit Built-in Password Providers* option.



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

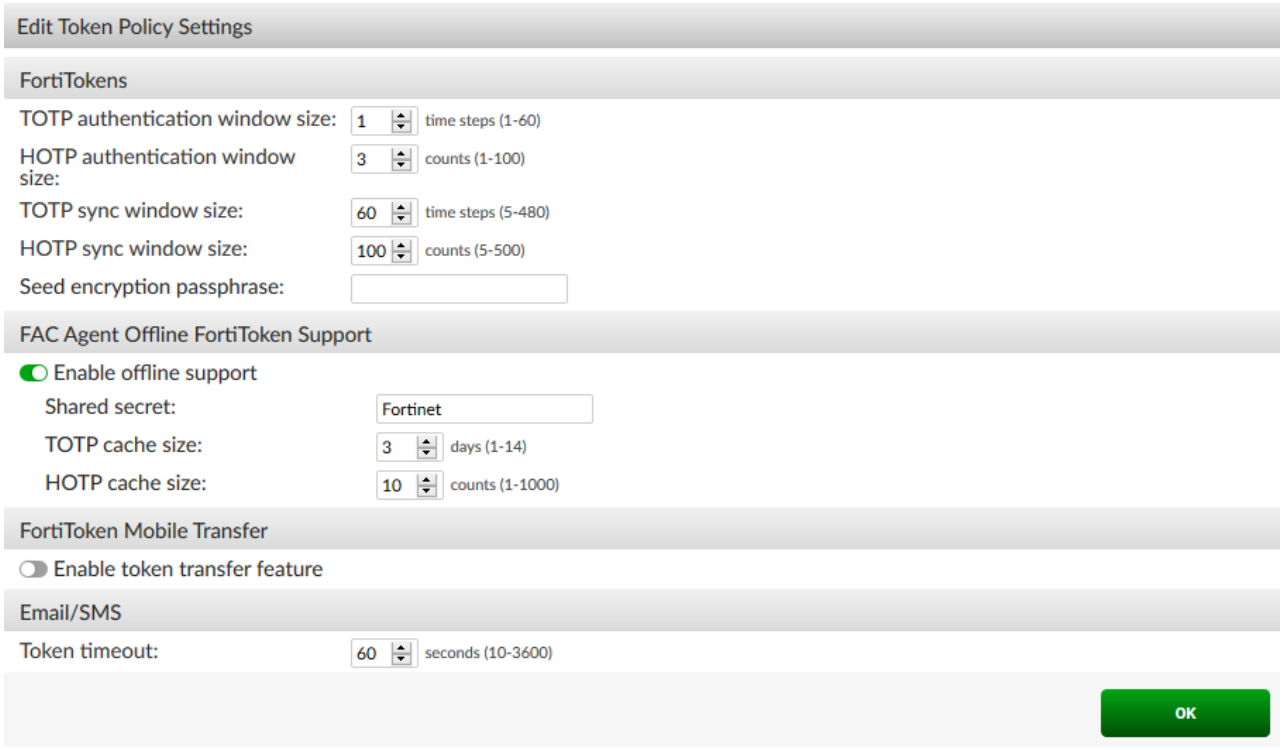
Offline token configuration

The instructions below describe how to configure FortiAuthenticator Agent offline token support. Offline tokens allow the Windows Agent to cache future tokens for users when they are offline or the FortiAuthenticator is unreachable

FortiAuthenticator configuration

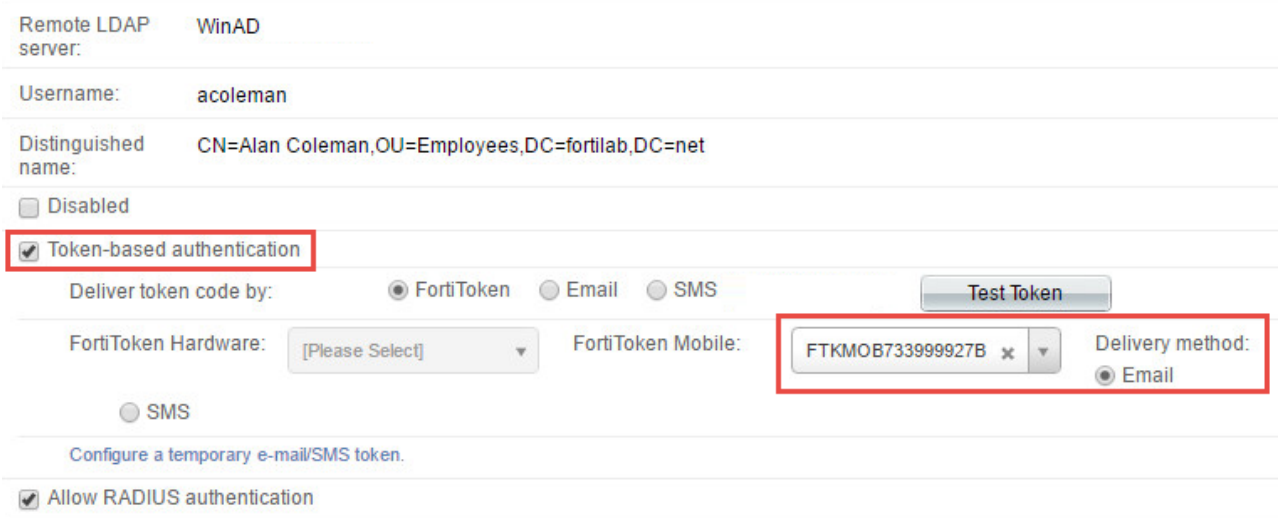
To configure the FortiAuthenticator to enable offline token support:

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

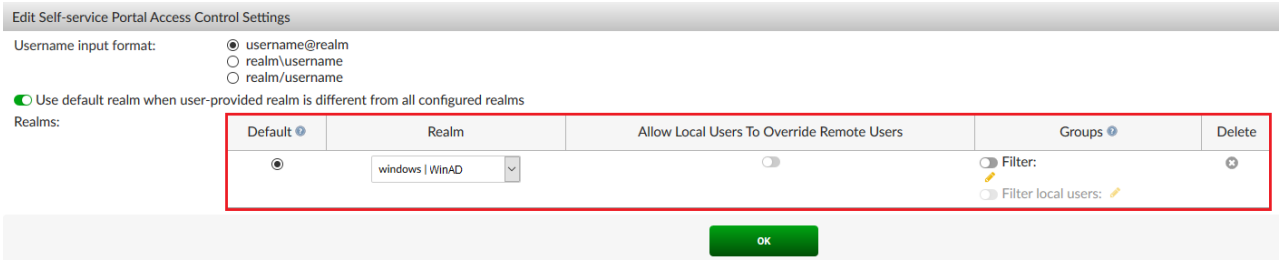


Now we need to generate the web service key for the Windows agent to talk to FortiAuthenticator with an associated administrative account. Once enabled on the account, the key will be emailed to the email address in the account details from FortiAuthenticator.

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.

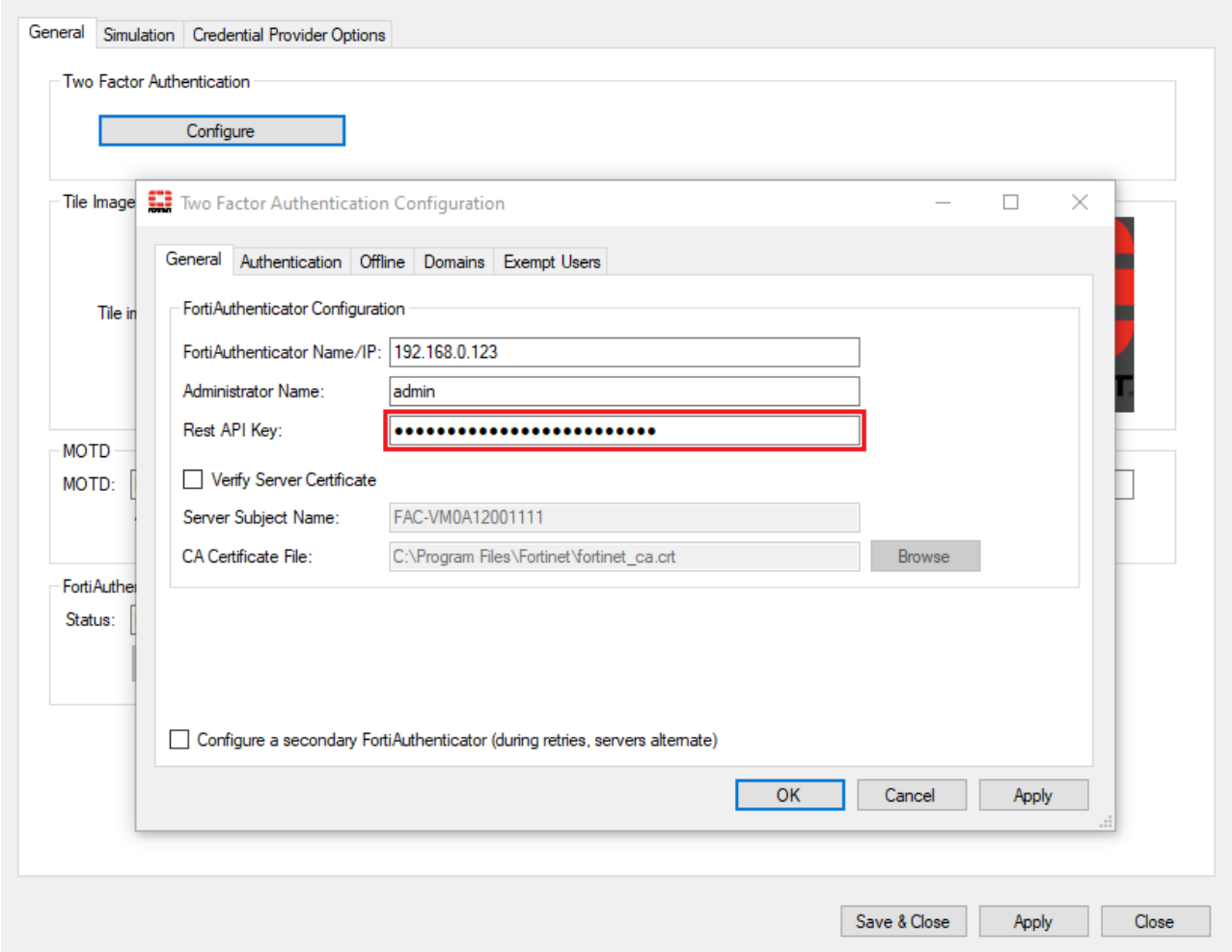


FortiAuthenticator Agent for Windows configuration

To set up FortiAuthenticator Agent for Microsoft Windows:

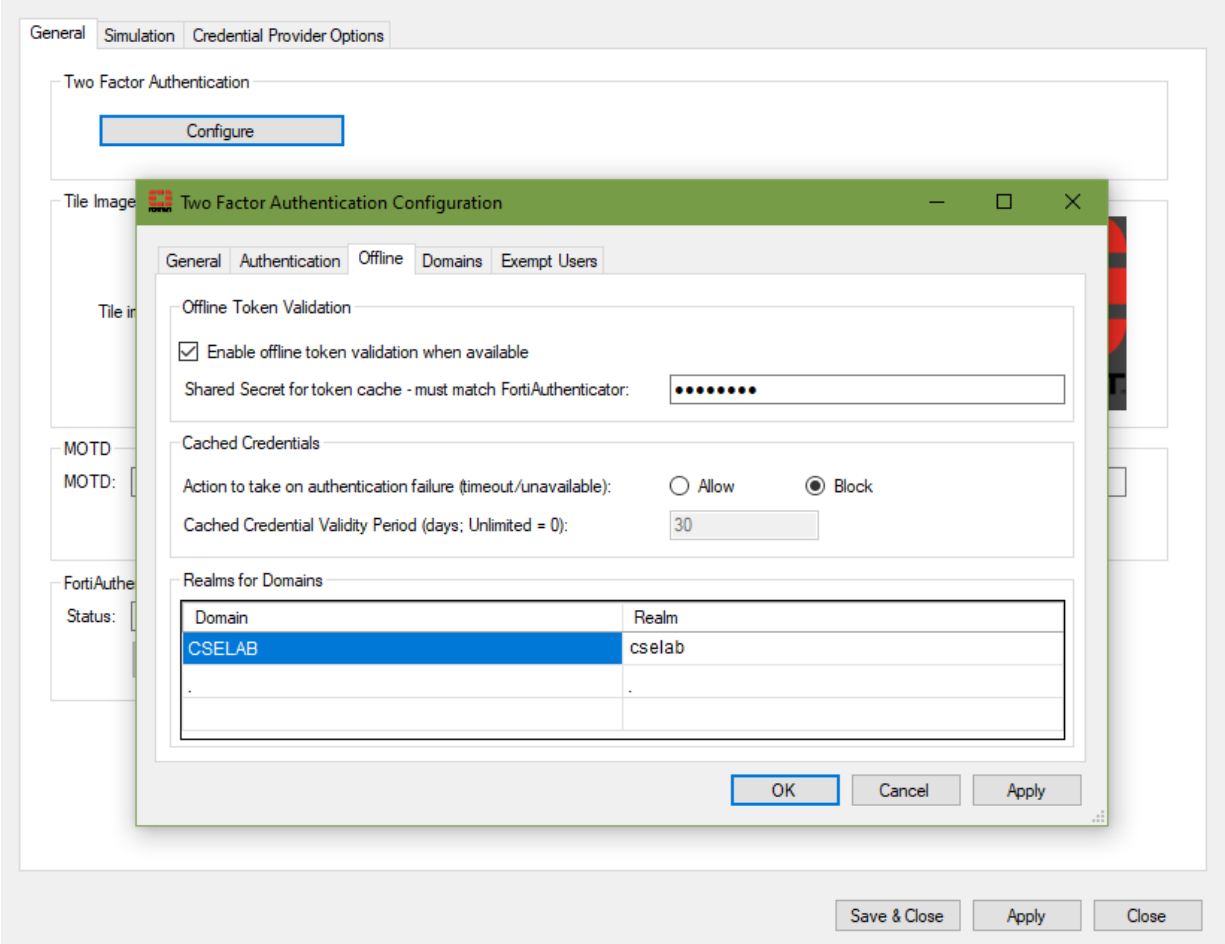
1. Log on to the host system where the Windows agent has been installed.
2. Select the *General* tab and select the *Configure* button to load the configuration settings.
3. Verify the IP address of the FortiAuthenticator server and the administrator account name.

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



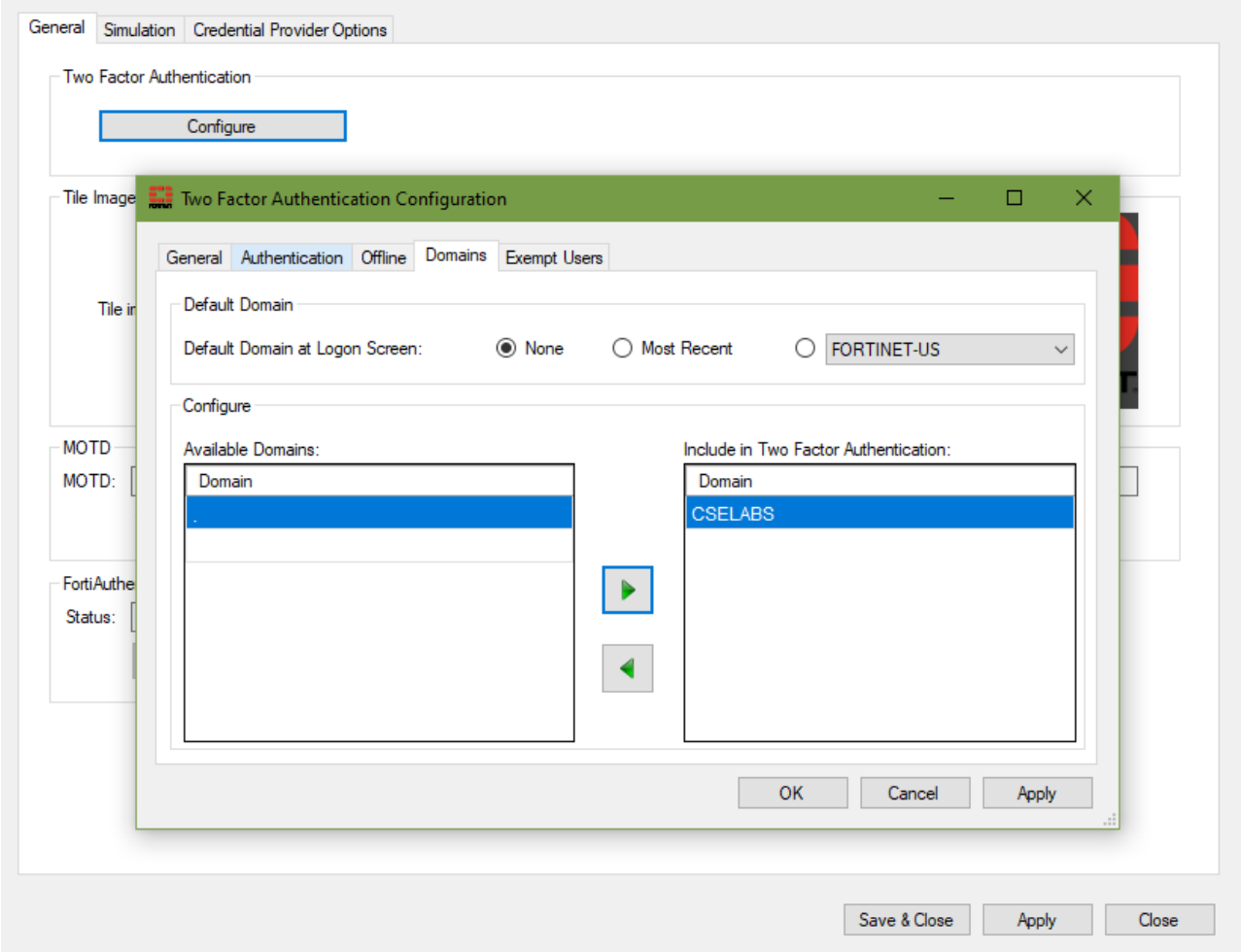
5. Next, select the *Offline* tab and verify the following:
   - Check the *Enable offline token when available…* box.
   - Enter the *Shared Secret* that was set on the FortiAuthenticator (*Authentication* > *User Account Policies* > *Tokens*).
   - Verify that the *Domain* is the correct AD Domain and the *Realm* is an exact match to the realm setup in

FortiAuthenticator that points to the LDAP directory (*Authentication* > *User Management* > *Realms*).



6. In the *Domains* tab, select a domain and move it into the *Include in Two Factor Authentication* column. The specified *Realm* name must match the one configured on FortiAuthenticator exactly for offline tokens to work.

FortiAuthenticator Agent for Microsoft Windows contains the default domain "." which represents the local user. You can disable local user login by including the "." domain in the list of domains included in two factor authentication. When the "." domain is not included, login is enabled for local users.



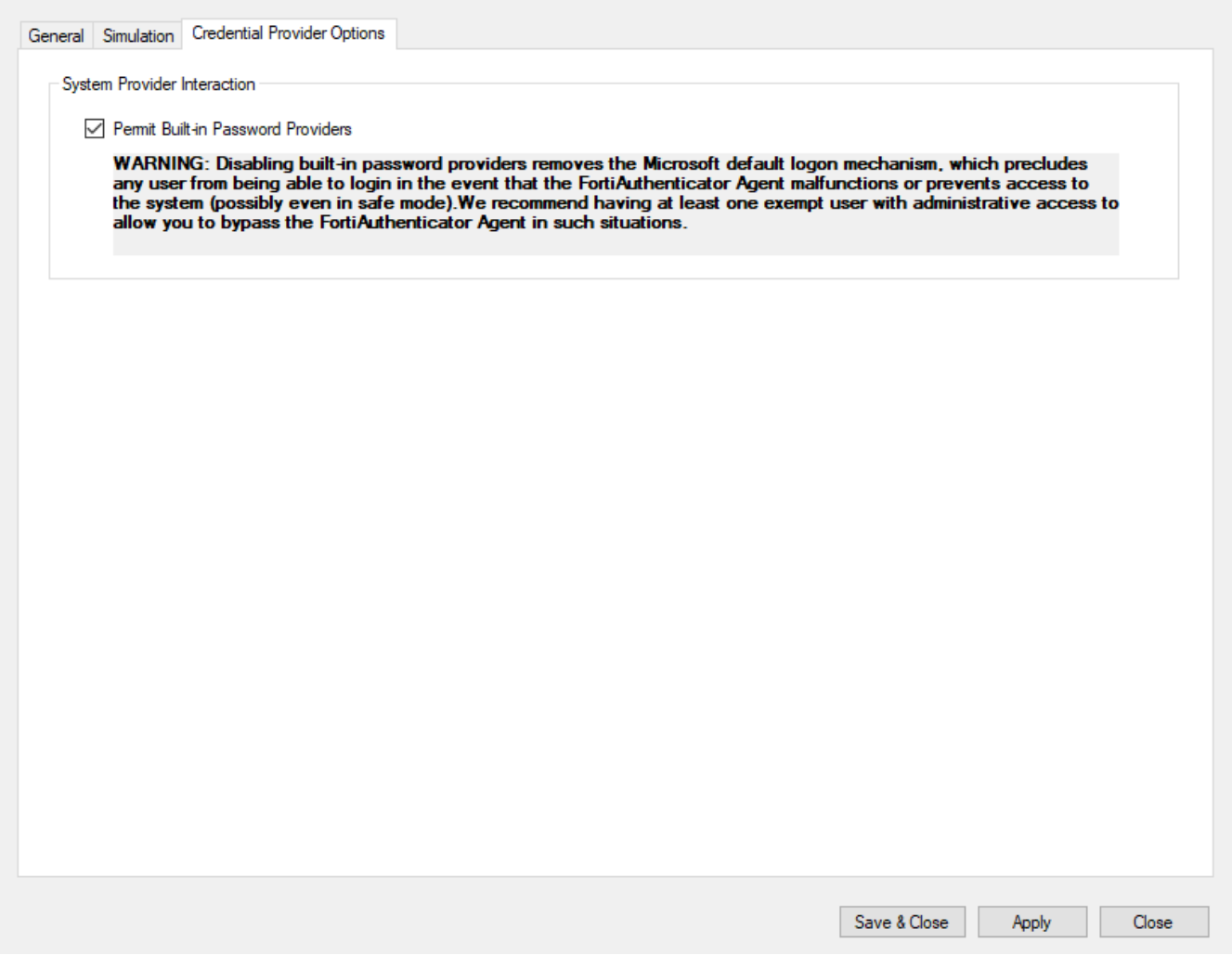
This completes the configuration of the Windows agent.

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.

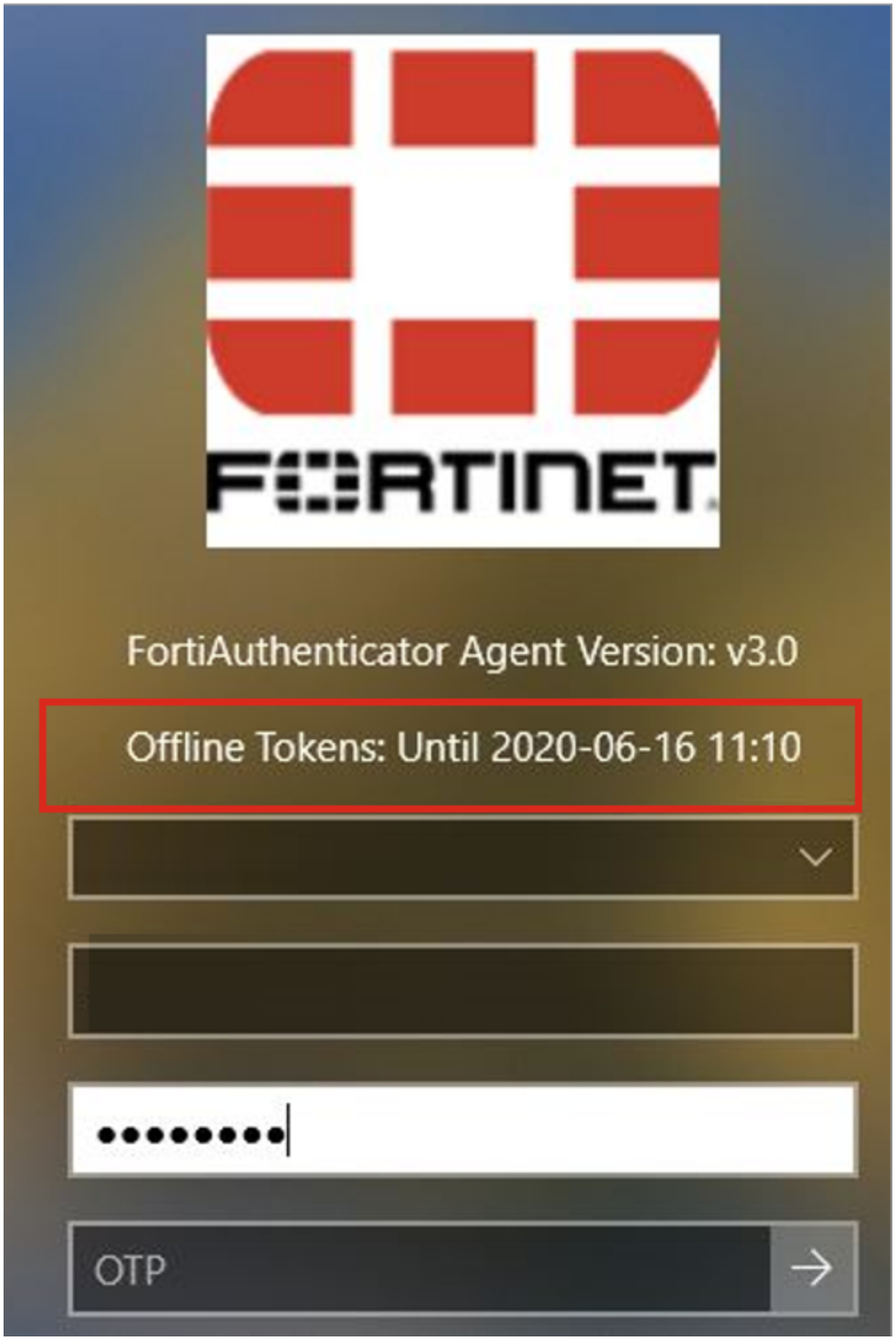
Credential provider options

By un-checking the option for the default *Permit Built-in Password Providers*, you 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 completed, the default Windows credentials provider (e.g., "Other User" option) will no longer be available.



Offline token time/count size

The time/count remaining for offine token validation can be viewed when logging in. All tokens downloaded have enough offline tokens for the configured cache size plus the authentication window size. For example, if the HOTP cache size is 50, and the HOTP window is 10, you initially have 60 tokens. Note that when tokens are displayed but not submitted to the FortiAuthenticator, this can be fewer than 60 authentication attempts.


FORTINET
FortiAuthenticator Agent Version: v3.0
Offline Tokens: Until 2020-06-16 11:10
OTP

Appendix A - Debugging

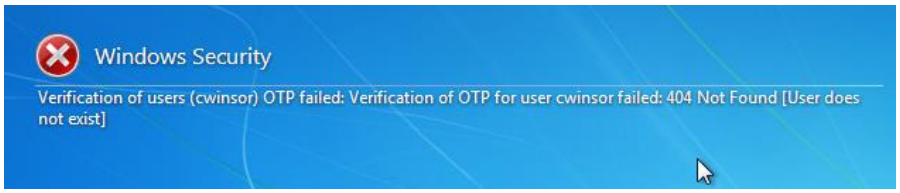
Common login errors

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

Username + OTP	→	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:

FortiAuthenticator Agent installer commands are case-sensitive and are required to be all uppercase.

`/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.

`/OFFLINEENABLED`

Turns offline mode on, will also disable "cached credential" support.

`/OFFLINESHAREDSECRET=<secret>`

Sets shared secret value to this (encrypted at the end of the install).

`/OFFLINEREALMS=domain1:realm1,domain2:realm2`

Sets domain-realm mappings, invalid entries cleared.

`/TILEIMG="C:\path\to\file.bmp"`

The login tile image.

`/MOTD="Here is a custom MOTD"`

Overrides the default MOTD which contains version information.

`/DEFAULTDOMAINMODE=`

Enter after the equals (=) sign either `0` for none, `1` for most recent, or `2` for a specific domain.

`/DEFAULTDOMAIN=DOMAIN`

Enter the domain's down-level/NETBIOS name. For example, for `sub.example.com`, enter `SUB`.

Installing secondary FortiAuthenticator for HA

In order to configure a secondary FortiAuthenticator with the same installation commands as the primary, the following command must be entered:

`/ALTFACENABLED`

Now all relevant existing commands can be used to configure the secondary unit provided they are prefaced with "ALT" (meaning "alternate"), for example:

`/ALTFACHOST...`

`/ALTFACRESTADMIN=...`

`/ALTFACRESTKEY=...`

`/ALTFACVERIFYSERVERCERT...`

`/ALTFACSERVERSUBJNAME...`

`/ALTFACCACERTFILE...`

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.

`/AUTHREALMBASED`

Enable Realm-based authentication. This is disabled by default to retain legacy behavior.

```
/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.

FortiAuthenticator Agent for Microsoft Windows includes the "." domain which represents the local machine. When listed as an included domain for two factor authentication, local user login is disabled.

```
/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"
```

```
/EXCLUDEDGROUPS="OU=special,DC=domain,DC=com;OU=somethingelse,DC=domain,DC=com"
```

This is a list of groups indicated by their domain, separated by semicolon. These groups 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.

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.

pGina license

Appendix D - FortiAuthenticator Agent for Microsoft Windows registry files

The following registry files are used in FortiAuthenticator Agent for Microsoft Windows:

HKEY_LOCAL_MACHINE\SOFTWARE\Fortinet\FAC_Agent_v1.0

Keys	Description	Type	Default value
27C65014-B660-4141-B9C4-9D35CFE99AE5	A plugin credential provider ID for the FortiAuthenticator Agent for Microsoft Windows, and a binary flag for Windows Agent plugin features. **Note:** This key should not be updated manually.	dword	`0x00000062`

AvailableDomains	List of domains. It can be updated by the user, or it will be updated by the Configuration app.
	Example:
	`ABBY.AD.FACDOM.CA:ABBY`
	`AD.FACDOM.CA:FACDOM`
	.:.
		multi_sz	n/a

CredentialProvidersWhiteList	List of other specific credential providers we allow alongside FortiAuthenticator Agent CP. **Note:** To add multiple values for this key, enter a list of GUIDs in brackets. Optionally, you can use commas to separate the contents of the list. **Example:** Two allowed credential providers for (smartcard credential provider, iris credential provider):	sz	absent

Keys	Description	Type	Default value

	`{1b283861-754f-4022-ad47-a5eaaa618894}{C885AA15-1764-4293-B82A-0586ADD46B35}`
	Alternatively, they can be added as:
	`{1b283861-754f-4022-ad47-a5eaaa618894},{C885AA15-1764-4293-B82A-0586ADD46B35}`		

DisableMSPasswordProvider	Allows to sign-in through Windows Agent only.	sz	`True`
InstallPath	Installation path for the FortiAuthenticator Agent for Microsoft Windows. **Note:** This key should not be updated manually.	sz	`C:\\Program Files\\Fortinet\\FortiAuthenticator Agent`
IPluginAuthentication_Order	Order of plugins to authenticate the user. **Note:** We have only one plugin for now.	multi_sz	`27C65014-B660-4141-B9C4-9D35CFE99AE5`
IPluginAuthorization_Order	Reserved for future.	n/a	empty
IPluginAuthenticationGateway_Order	Reserved for future.	n/a	empty
IPluginFetchTokens_Order	Order of plugins to fetch tokens for the user. **Note:** We have only one plugin for now.	multi_sz	`27C65014-B660-4141-B9C4-9D35CFE99AE5`
IPluginEventNotifications_Order	Reserved for future.	n/a	empty
IPluginPushNotification_Order	Order of plugins for push authentication of the user. **Note:** We have only one plugin for now.	multi_sz	`27C65014-B660-4141-B9C4-9D35CFE99AE5`
MaxClients	Number of connections from the Credential Provider to the (internal) FortiAuthenticator service.	dword	`0x0000019`

Keys	Description	Type	Default value
Motd	(Message Of The Day) Message, appears on the login screen.	sz	`FortiAuthenticator Agent Version: %v`
PluginDirectories	Installation directory for plugins. It is the installation directory for FortiAuthenticator Agent for Microsoft Windows itself. **Note:** We have only one plugin for now.	multi_sz	`C:\Program Files\Fortinet\FortiAuthenticator Agent`
ServicePipeName	Connection/pipe name from the Credential Provider to the (internal) FortiAuthenticator service.	sz	`FAC_AgentPipe`
TileImage	Path to the "Other user" tile image on the login screen.	sz	empty (Fortinet image is shown)
TraceMsgTraffic	Log messages between the Credential Provider and the (internal) FortiAuthenticator service. **Note:** These are not messages from the Agent to the FortiAuthenticator server.	sz	`False`- for investigation only.

HKEY_LOCAL_MACHINE\SOFTWARE\Fortinet\FAC_Agent_v1.0\Plugins\27c65014-b660-4141-b9c4-9d35cfe99ae5

Keys	Description	Type	Default value
The next eight entries are related to authentication.			
Auth_AllowAdminOTP	Allows admin OTP on the login screen. **Example:** `False`	sz	n/a
Auth_CacheCredPeriod	Number of days the user is allowed to login with failed OTP (related to Auth_FailAction).	dword	`0x0000001e`
Auth_FailAction	Allowed to login with a failed OTP (see Auth_CacheCredPeriod and Auth_OfflineEnabled).	dword	`0`
Auth_NumRetries	Number of additional tries to connect to the FortiAuthenticator server after failure (related to Auth_Timeout).	dword	`1` (valid range is `0-3`)

Keys	Description	Type	Default value
Auth_OfflineEnabled	Allow authentication, based on downloaded tokens (or allow logon on failed OTP, if Auth_FailAction is configured).	sz	`True`
Auth_OfflineSharedSecret	Shared secret for the offline storage - must match FortiAuthenticator. **Note:** This key should not be updated manually.	Encrypted string	n/a
Auth_RealmBased	Forces to use realm in addition to the username for authentication (from version 3.0).	sz	`True`
Auth_Timeout	Number of seconds to wait until next retry (related to Auth_NumRetries).	dword	`0x0000000f`
The next four entries are domain-related.			
Dom_DefaultDomain	Domain, selected on the login screen by default (see Dom_DefaultDomainMode). **Example:** `FACDOM`	sz	n/a
Dom_DefaultDomainMode	Mode to save and pick domains (see also Dom_ DefaultDomain): • `0`: No domain should be selected • `1`: last domain • `2`: specific domain **Example:** `1`.	dword	n/a
Dom_IncludedInTFA	List of the domains that require OTP. **Example:** `FACDOM` .	multi_sz	n/a
Dom_RealmMappings	Maps domain names to realm names (usually set up through the configuration app). **Example:** `AD.FACDOM.CA:facdom` .:.	multi_sz	n/a
The next four entries are related to exempt users.			
EU_GroupList	Exempt groups. Members of the group will not need an OTP for login.	multi_sz	empty
EU_ UserGroupCachePeriod	Number of days for which the cached groups are considered valid (related to EU_ UserGroupsCached).	dword	`0x1e`
EU_UserList	Exempt users. **Example:** `FACDOM/Administrator`	multi_sz	n/a

Keys	Description	Type	Default value
	`FACDOM/System`		
EU_UserGroupsCached	Shows if we have cached user groups or not.	sz	`False`
The next seven entries are related to FortiAuthenticator server.			
Gen_HostSpecificSalt	Salt for the offline storage. **Note:** This key should not be updated manually.	Encrypted string	n/a
Gen_AdminName	HTTP basic access authentication user. **Example:** `admin`	sz	n/a
Gen_CACertificateFile	Certificate for the FortiAuthenticator server. **Example:** `C:\\Program Files\\Fortinet\\fortinet_ca.crt`	sz	n/a
Gen_FacHost	FortiAuthenticator server. **Example:** `http://www.facdom.ca`	sz	n/a
Gen_RestAPIKey	HTTP basic access authentication password. **Note:** This key should not be updated manually.	Encrypted string	n/a
Gen_ServerSubjName	FortiAuthenticator server subject name. **Example:** `FAC-VM1`	sz	n/a
Gen_VerifyServerCert	Use certificate validation.	sz	`True`
The next seven entries are related to the alternate FortiAuthenticator server.			
Gen_AltFacEnabled	Alternate FortiAuthenticator server is configured. **Example:** `True`	sz	n/a
Gen_AltAdminName	HTTP basic access authentication user for the alternate FortiAuthenticator server. **Example:** `admin`	sz	n/a
Gen_AltCACertificateFile	Certificate for the alternate FortiAuthenticator server. **Example:** `C:\\Program Files\\Fortinet\\fortinet_ca_alt.crt`	sz	n/a
Gen_AltFacHost	Alternate FortiAuthenticator server. **Example:** `192.168.150.111`	sz	n/a
Gen_AltRestAPIKey	HTTP basic access authentication password for the alternate FortiAuthenticator server. **Note:** This key should not be updated manually.	Encrypted string	n/a
Gen_AltServerSubjName	FortiAuthenticator server subject name for the alternate FortiAuthenticator server. **Example:** `FAC-VM2`	sz	n/a

Keys	Description	Type	Default value
Gen_AltVerifyServerCert	Use certificate validation for the alternate FortiAuthenticator server.	sz	`True`
The next ten entries are either informational or are hints about the last FortiAuthenticator server connection.			
Inf_AllowedDriftHotp	Maximum drift for HOTP tokens. **Note:** This key should not be updated manually.	dword	`0x00000003`
Inf_AllowedDriftTotp	Maximum drift for TOTP tokens. **Note:** This key should not be updated manually.	dword	`0x00000001`
Inf_ApiVersion	API version and date. **Note:** This key should not be updated manually. **Example:** `6.2.0-0525 20200513`	sz	n/a
Inf_ EmailSmsTokenTimeout	Email or SMS token timeout. **Note:** This key should not be updated manually.	dword	`0x0000003c`
Inf_IsOfflineEnabled	Offline validation is enabled or not. **Note:** This key should not be updated manually.	dword	`1`
Inf_IsPushEnabled	Push authentication is enabled or not. **Note:** This key should not be updated manually.	dword	`1`
Inf_MaxDurationTotp	Maximum duration for TOTP. **Note:** This key should not be updated manually.	dword	`0x0000007`
Inf_MaxNumberHotp	Maximum number for HOTP. **Note:** This key should not be updated manually.	dword	`0x0000000a`
Inf_PreferredServer	FortiAuthenticator server that responded faster: `0`: Main FortiAuthenticator `1`: Alternate FortiAuthenticator **Hint:** Agent may prefer this FortiAuthenticator server for the next call.	dword	`0`
Inf_Timestamp	Timestamp when the last 10 entries were updated. **Note:** This key should not be updated manually.	qword	n/a

User-related offline registry settings are not included

Deprecated entries (from version 3.0) are not in the list: all Gina-related entries