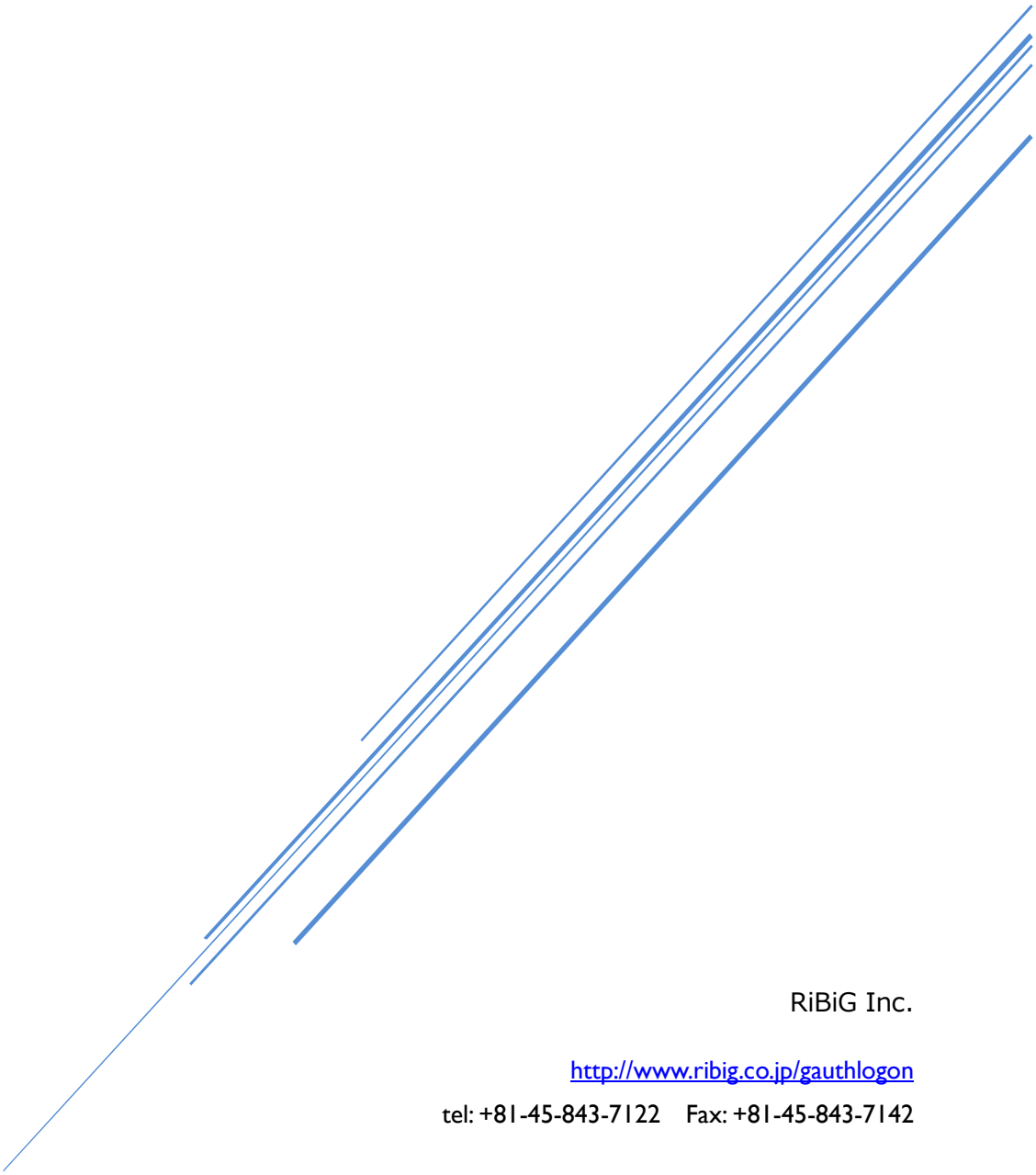
# GAUTHLOGON MANUAL

## Installation & Operation

Ver. 1.0.11



RiBiG Inc.

http://www.ribig.co.jp/gauthlogon

tel: +81-45-843-7122 Fax: +81-45-843-7142

# Contents

# About GAuthLogon

GAuthLogon is Windows sign-in software with 2 factor authentications. In the first stage, it authenticates a user by Username/Password. A successfully authenticated user will be prompted for an authentication code from Google Authenticator in the second step. GAuthLogon displays different screens for Username/Password entry and an authentication code entry.

A terminal service client user will also be asked to provide an authentication code by GAuthLogon in the remote desktop screen, after the user is successfully authenticated via network level authentication by providing UserName and Password in CredUI on the client side.

On Windows 8/10/ 2012 Server, GAuthLogon is installed as a V2 credential provider ( CP ) newly introduced with the release of Windows 8 and Windows 2012 Server. On the previous versions of Windows (Windows 7 / Vista, Windows 2008 Server ) , it is installed as a V1 credential provider. They do not support V2 CP.

**Installation Requirements**

A. Installation requires administrative privileges

B. You should have Android/iOS devices with Google Authenticator app installed.

C. The computer to install GAuthLogon on and the device running Google Authenticator must have their clocks synchronized. Each authentication code is time-based and, if they are out of sync beyond a certain limit, GAuthLogon will not be able to authentication a code as valid. It is recommended that you configure your computer / devices to synchronize automatically with a NPT server, if they have not be so configured, yet. Refer to Appendex 1 for Widows configuration for Internet time synchronization.

## About QRCode

One utility program, AddToke.exe, uses libqrencode library to generate QR bitmap data. Please refer to the author's page on the library.

http://fukuchi.org/works/qrencode/index.html.en

## LICENSING INFORMATION

Copyright (C) 2006-2012 Kentaro Fukuchi

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA

## About Evaluation Version

GAuthLogon will run as the evaluation version while no license file is installed. The evaluation version has the following limitations;

1. GAuthLogon will generate and accept several pre-defined Google Authenticator keys only.
2. The maximum number of credential providers that can be filter is two(2).

Google Authenticator keys are critical to the authentication security. Different users must have a different keys. But the evaluation version of GAuthLogon recycles the same pre-defined keys and different users can have the same secret key. When they do have the same keys, their authentication codes will be always the same.

## License File

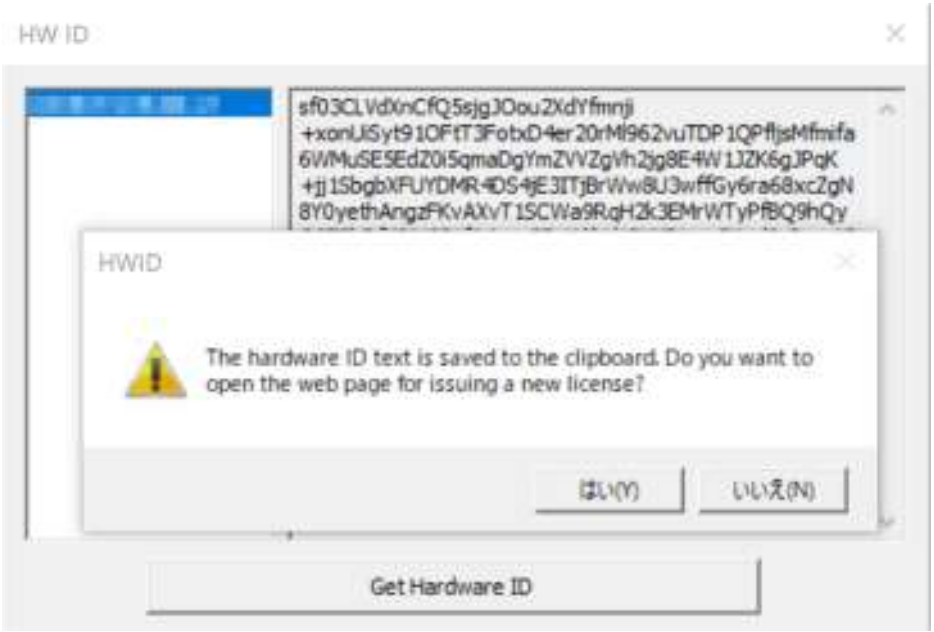
To obtain a license file, run "hwid.exe". It will generate a hardware ID that identifies the PC that is running hwid.exe. A license file is created using the hardware ID text; the license is valid only on the computer identified by the hardware ID.

Hwid.exe generates the hardware ID by acquiring unique properties of PC hardware components. One of them is MAC address of network adaptor / Bluetooth adaptor. A PC could have multiple MAC addresses; it may have multiple network cards, network and Bluetooth adaptors, hardware and virtual network adaptors. To lock down the license to MAC address, Hwid.exe wants one address that stays permanent and always visible. When you disable a network adaptor, MAC address will not be detected.

You can list PC's MAC address by issuing "ipconfig /all" in the command prompt. If your PC has multiple MAC addresses, take note of a permanent one that is always visible.

After running "hwid.exe", click on "Get Hardware ID" button. When only one MAC address is found, it will generate the hardware ID based on the MAC address. When it finds multiple MAC addresses, they are displayed in the list box on the left. Select one and click on "Get Hardware ID" button again.

The list box must always indicate MAC address used to generate the hardware ID. If you do not find anything in the list, please obtain a new version of the program.




**Hwid.exe detects MAC addresses and other hardware properties to calculate a hash from them. It is this hash that is fed to generate the hardware ID. The hash is irreversible to the original data; it cannot be manipulated/exploited to identify your hardware**

Once the hardware ID of the computer is generated, it will be shown in the right edit box and is also saved to the clipboard. To issue a license, open the web page. The page will accept a hardware ID and create a license file.

URL of the web site to issue GAuthLogon license:

https://www.ribig.co.jp/gauthlogon/license/

On the page, paste the hardware ID into the HWID field.

To issue a license file, you must have an account. You can create an account on "Create Account" page. When creating an account, you must buy licenses and pay via Paypal.  An account will be ready to issue a license upon completion of

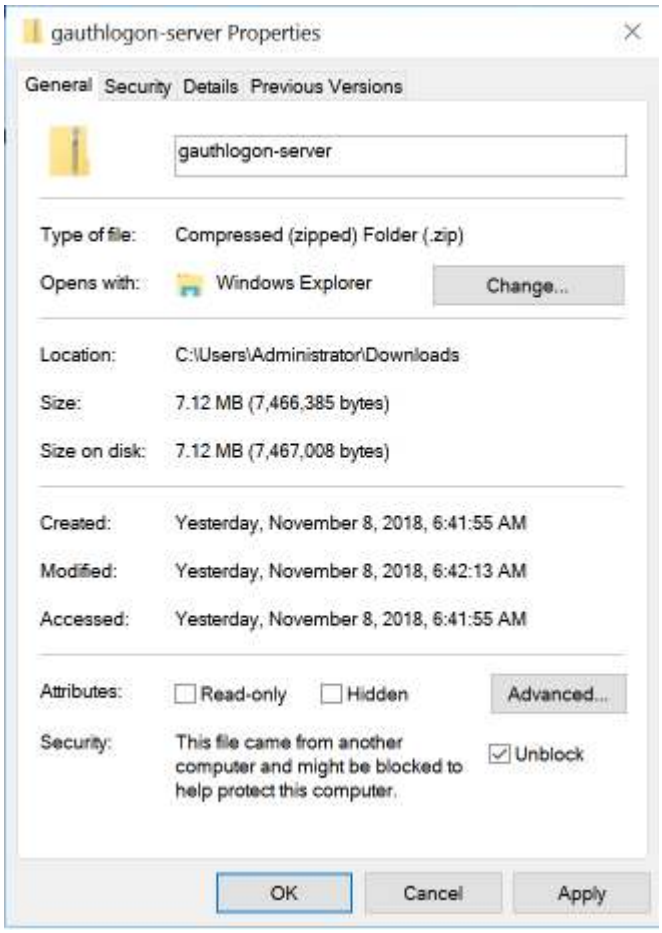
payment.

The web page creates a license and a license file named "license.txt" will be downloaded. Place this license file in GAuthLogon folder. In the folder, you should find a file named "GAuthLogon.DLL".

GAuthLogon Folder: %ProgramFiles%\RiBiG\GAuthLogon"

## About Downloaded ZIP File Security

After you downloaded ZIP file, it is flagged as blocked. Right-click the downloaded ZIP file and select "Property". At the bottom of [General] tab, you will find "Unblock" checkbox. Enable the checkbox to unblock the file protection.




Or you can unblock the individual files after expanding the ZIP file. Windows Server OS will show a warning message when you run a blocked program.

# Installation

## Distribution Files

There are distribution files for the client OS and the server OS.
The client distribution file contains 2 folders for Win7 and Win8. Use Win7 files for Vista. They each have 32bit(x86) and 64bit(x64) version.

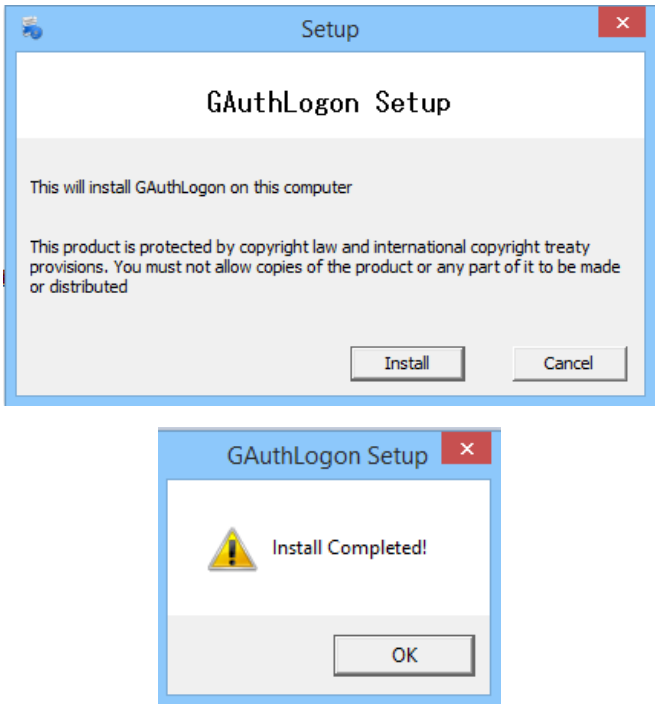
- Client.ZIP
  - Auto-setup.exe
  - Hwid.exe
  - Win7
    - X86 32bit version
    - X64 64bit version
  - Win8
    - X86 32bit version
    - X64 64bit version

The server distribution files contains 2 folders for Win2008 and Win2012.

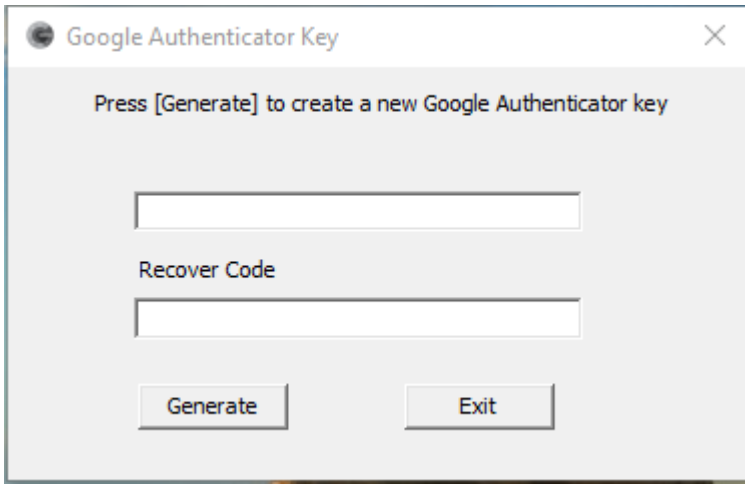
- Server.ZIP
  - Auto-setup.exe
  - Hwid.exe
  - Win2008
    - X86 32bit version
    - X64 64bit version
  - Win2012 64bit version only

## Installation

Run Auto-setup.exe in the root folder of the distribution ZIP file. It will detect the current OS and run Setup.exe in an appropriate folder. Alternatively, you can select the right folder that matches your target OS and run Setup.exe in the folder. Setup.exe will complete in a few seconds.




When you see "Install Completed", press [OK] button to close Setup.exe. Before exiting, Setup will run another program that will help you generate a seed key for Google Authenticator. This key is critical both for Authenticator to create a time-based authentication code and for GAuthLogon to authenticate the code.




When you see the window above, press [Generate] button. A key will be generated and, at the same time, a window with QR code encoding the key will be displayed.


You need

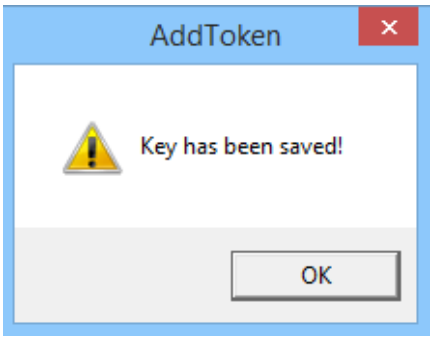
1. To scan QR code with your Google Authenticator app or to register the key to Authenticator app manually.
2. To set at least 32 character long recover code of your own choice
3. To save the key to the computer.

When you scan QR code, Authenticator will automatically save it under the label named "Win:(username)@(domain)". Alternatively, you can manually enter the key along with a label (an account name) to identify it. Make certain to save it as "time-based" which is Authenciator's default. After scanning the QR code, close the window by pressing close[x] button

You must also save the key to the computer. Before pressing [Save] button, be sure that you have entered a recovery code. The recovery code is a code you can

use once instead of an authentication code displayed by Google Authenticator. You can use the recovery code in cases like you have lost your authenticator device.

By pressing [Save] button, the auto-generated key and the recovery code are saved in your home folder. Now Google Authenticator and your user account are configured to share the same key. If their clocks are synchronized, GAuthLogon should be able to sign you in.




Press [OK] to close the dialog and quit the program by clicking on [X].

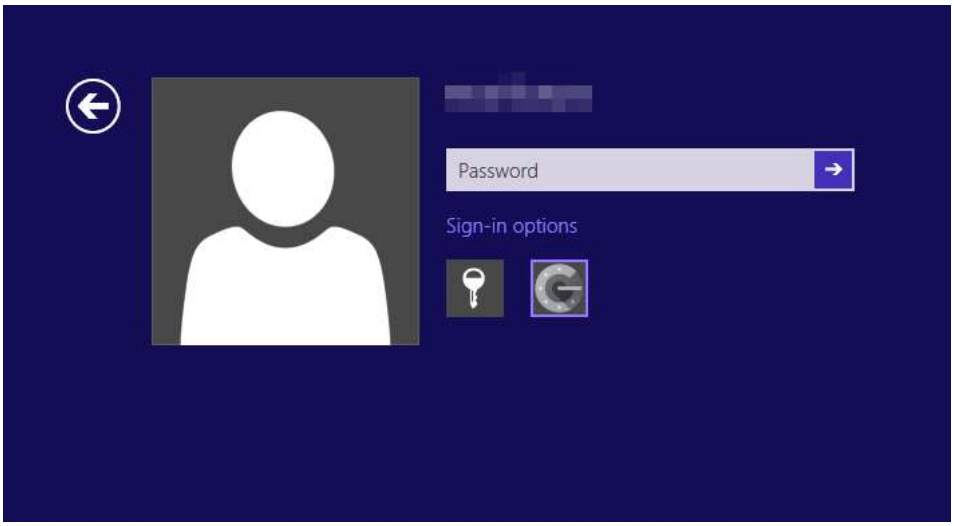
You can now sign out and try to sign in to Windows via GAuthLogon.

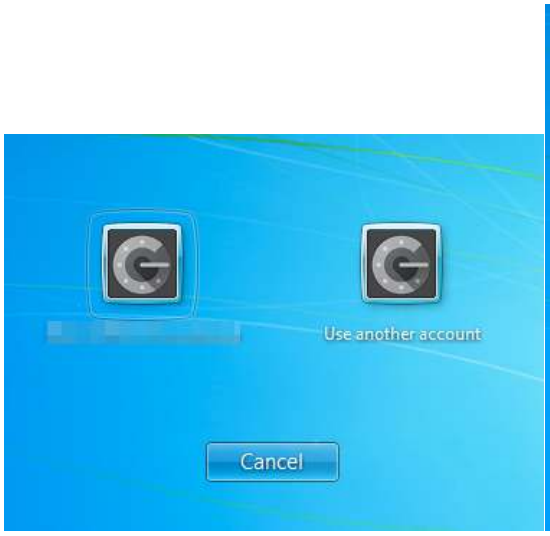
Please note that you have configured GAuthLogon only for your account. The other users have not yet set up their Authenticator keys. Each user is responsible of generating a key and save it both to their Authenticator app and to their computer account with AddToken.exe utility. You find the detail in the section "Authenticator Key Generation".

A user without their Authenticator keys set up can sign in via GAuthLogon but only several times. GAuthLogon will not ask for an authenticator code for those users, but this can only last for several sign-ins. After an upper limit of this special sign-in is reached, GAuthLogon will start asking for an authentication code.

## Sign In

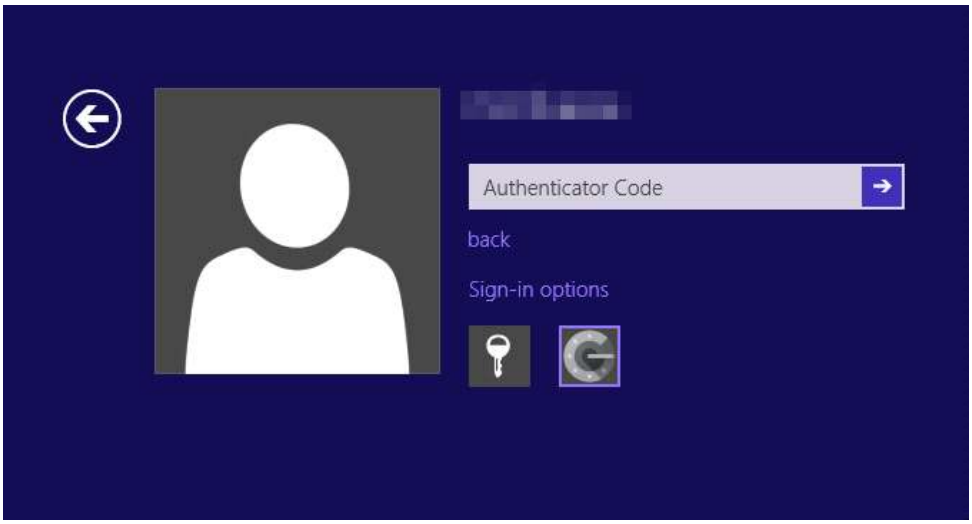
Sign out and select a tile. Clicking on "Sign-in options" link should display GAuthLogon icon.





Enter the correct password for the user. When the user is successfully authenticated, GAuthLogon will prompt for an authentication code. It may take a few seconds for the screen to switch to the code entry.



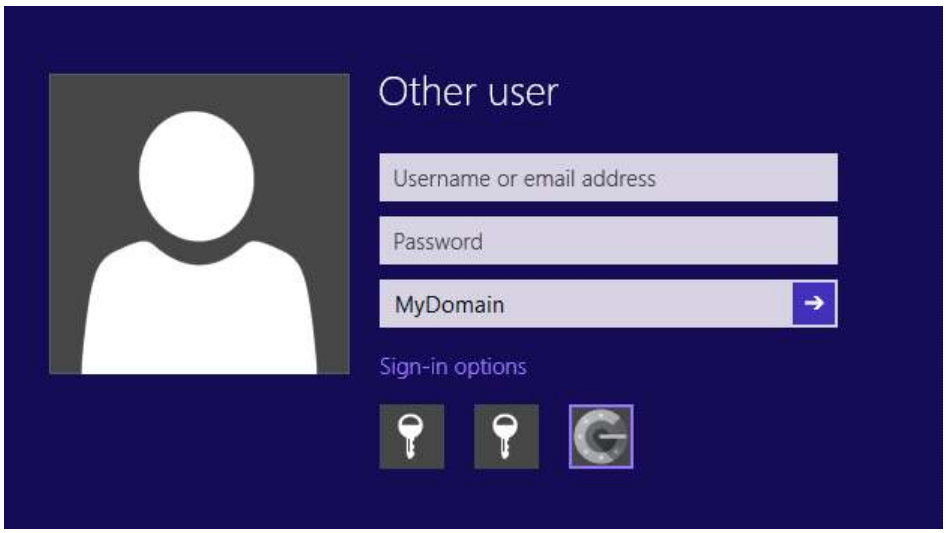


Type in the authentication code displayed on your Google Authenticator app. and press Enter key. A correct authentication code will sign you in to Windows.

Instead of an authentication code, you may enter the recovery code. Once you use the recovery code for a login, the registration information on the computer will be deleted and you must configure your authentication device and a new recovery code again, using AddToken utility.

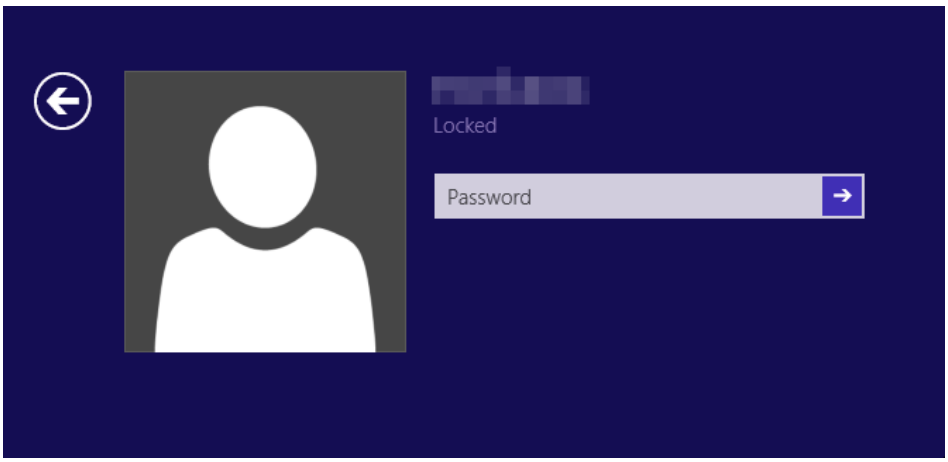
You can go back to the previous screen by pressing Enter key while the code field is empty or by clicking on “back” link.

In [Other User] tile, fill in User Name, Password and Domain fields. On Windows 8, if you want to set a LiveID mail address in Username field, the domain name must be "MicrosoftAccout". You can type in "MicrosoftAccout". Or just key in ~(tilde) when the domain field is empty. A Tilda will be automatically expanded to "MicrosoftAccount". For a local user, you can leave the domain field blank.



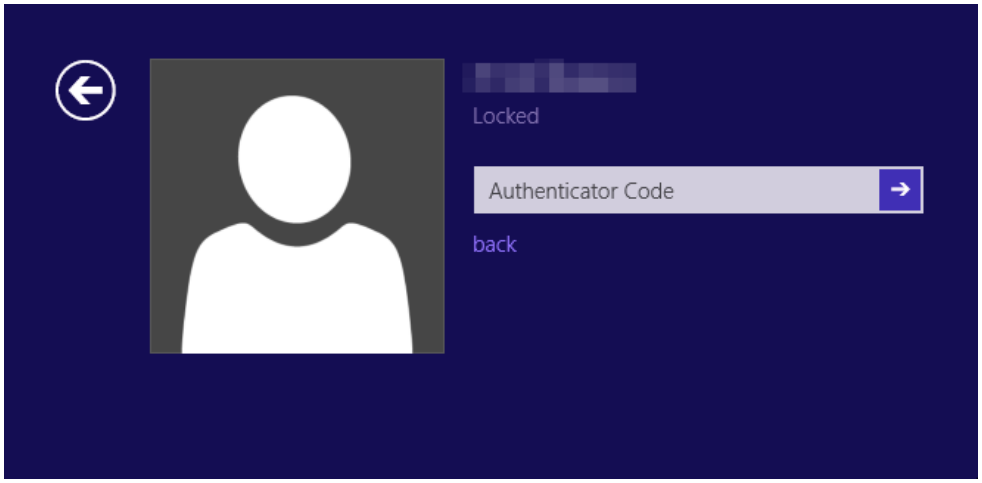

The correct credential information will take you to the next screen for the authentication code entry.

UnLock





There is no “Sign-in options” link on the screen. Just input the correct password for the locked session user and the right authentication code in the next screen.


Locked
Authenticator Code
back

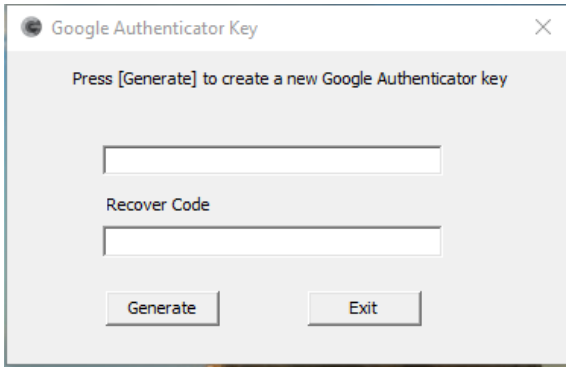

Authenticator Code
back
Switch User

## Authenticator Key Generation

Users are responsible of setting up their Authenticator key on their own device. After GAuthLogon is installed, it will not ask a user to enter an authentication code when it finds that the user has not set up Authenticator key. But it keeps the user's sign-in count and starts asking for an authentication code after the count reaches a specified upper limit. Note that Unlock and CredUI authentications via GAuthLogon will increment the sign-in counter.

A. Sign in to Windows

B. Run AddToken.exe utility. You can find the program in「Program Files」—「RiBiG」—「GAuthLogon」folder。




C. Press [Generate] to generate a new Authenticator key. You can type in or paste an encrypted Authenticator key you have obtained on another computer. When you start filling in the text box, the message in the window is changed as below.

D. [Generate] button will create a new Authenticator key and show a window with QR code.


The part "Win:(username)@(domain)" is used as the account name to identify the key. You are free to change it to any text to suit your purpose.

E. Scan QR code with your Authenticator app. Also save the key along with a recover code of your own choice to the computer by pressing [Save]. Instead of scanning the QR code, you may manually set the key to your Authenticator. Be sure to check the key as "time-based"

F. [Save] button saves the key and the recovery code to your home folder on the computer. (GAuthLogon will seek a user key in their home folder). [Save] button will also save the corresponding encrypted key in the clipboard.

G. When you set an encrypted Authenticator key ( generated on another computer ) in the text box, AddToken utility will detect it as valid only when the destination user account has the same user name as the source user account. This way, your accoun can share the same key on multiple computers.

H. Please handle encrypted keys as confidential information.

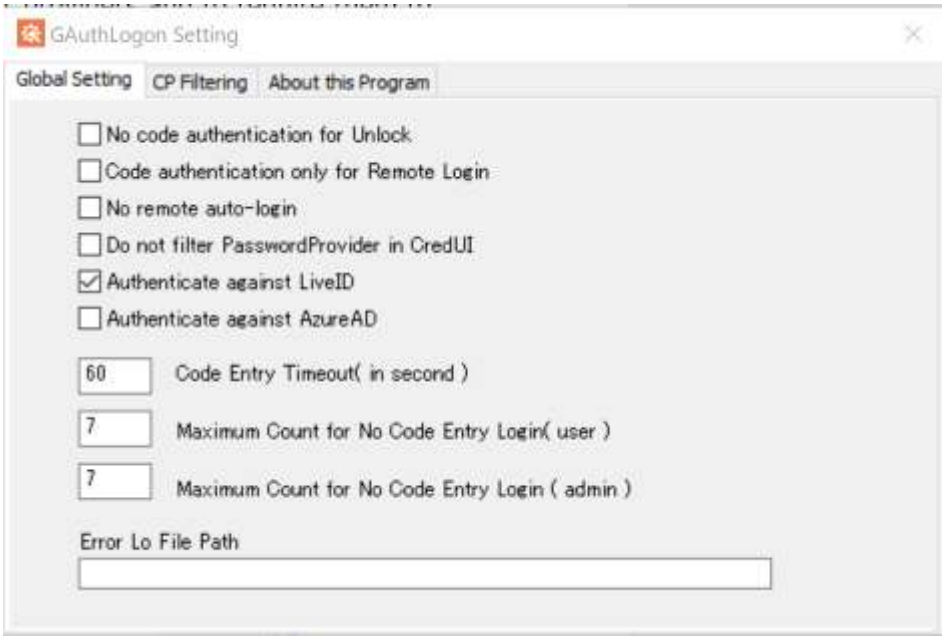
## Filtering out Credential Providers

After you install GAuthLogon, you can use GAuthLogon for sign-in but also select the other providers, using “Sign-in options” link. When you select to use the password provider, you do not have to enter an authentication code.

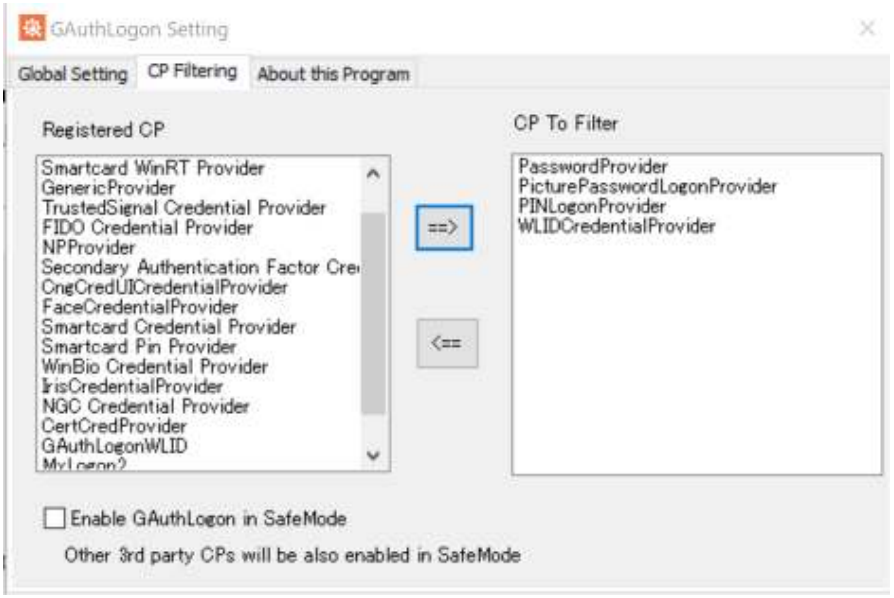
In order to prevent users from selecting other providers and to require them to provide valid authentication code for sign-in, you need to filter out the providers that you do not want to be displayed in the sign-in screen.

A. Sign in to Windows

B. Run config.exe. You can find the program in「Program Files」—「RiBiG」—「GAuthLogon」folder or in [Start]-[GAuthLogon]-[Setting]. You must have administrator privileges to execute it.




C. Select [CP Filtering] tab.




D. The left list box shows all the providers available on the system. You move those to filter out to the right list box by selecting a provider and pressing [=>] button. To enforce GAuthLogon authentication only, filter out the following 4 providers like above.

1. PaswordProivder ( User/password )
2. PicturePasswordLogonProvider ( Picture Password )
3. PINLogonProvider ( PIN )
4. WLIDCredentialProvider (LiveID )

When Windows is AzureAD joined, PIN logon is always available unless you filter out the following provider

5. NGC Credential Provider

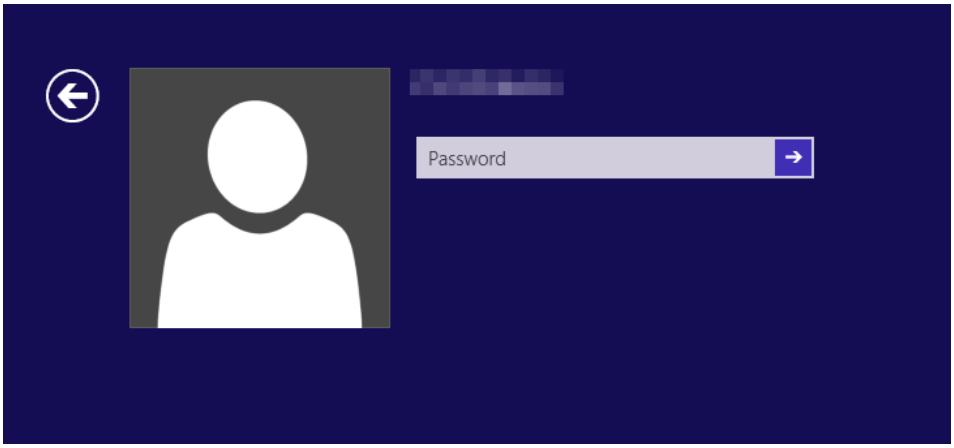
Changes will be automatically saved.

* The evaluation copy can accept only up to two credential providers to filter.

＊Please try to filter out those providers you whose role you understand. Leave untouched those you do not.

Sign out and you should find no “Sign-in options” link or “Sign-in options” link

that does not show Password, PIN, Picture Password, LiveID provider icons.




Enable GAuthLogon in SafeMode

Unless you know what this means, do not check the box.

By default, all the third-party credential providers are disabled in Safe Mode. This way, you can always sign in to Windows via Password provider in Safe Mode for the maintenance purpose, even when third-party credential providers fail to sign you in.

If you enable third-party credential providers in Safe Mode, be prepared for the worst scenario where third-party credential providers do not sign you in. This is particularly relevant when you filter out providers and can sign in via only one provider.

But enabling third-party credential providers in Safe Mode makes your Windows secure. When you enable GAuthLogon in Safe Mode,

1. Do not filter out PassProvider first. This way, if you cannot log in via GAuthLogon, you can still log in via PasswordProvider.
2. Be sure that you can remove GAuthLogon by setting a recovery code.

After making sure that you can log in via GAuthLogon in Safe Mode several times and you can remove it with the recovery code, filter out

PasswordProvider.

To disable GAuthLogon using Recovery console, delete gauthlogon.dll
( %ProgramFiles%\ribig\gauthlogon\gauthlogon.dll )

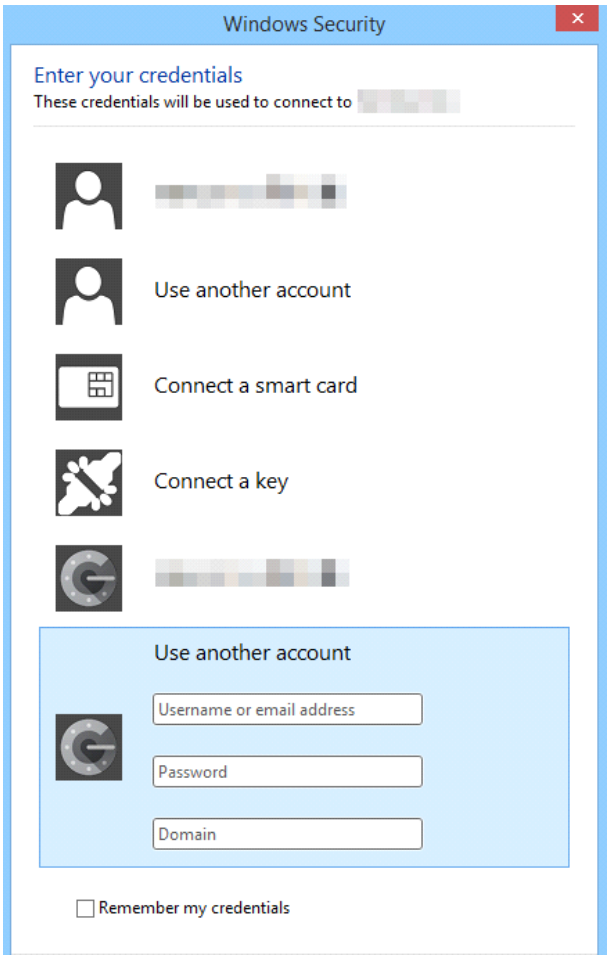
## Remote Desktop

When you filter out Password provider on Windows running the terminal service, a remote desktop client will display a screen for the authentication cod entry after the network level authentication completes ( you have provide your credential information in CredUI on the client side ).

*Microsoft Password provider automatically sign you in to Windows after the network level authentication succeeds, preventing GAuthLogon from prompting for an authentication code. GAuthLogon on the terminal server starts receiving the user credential information you enter on the client side and asking for an authentication code, only when Microsoft Password provider is filtered. When GAuthLogon is configured to receive the client credential information, we recommend that you also filter any other credential providers that require the credential information from the client ( they do not receive them and you have to re-enter the credential on the terminal side ).*

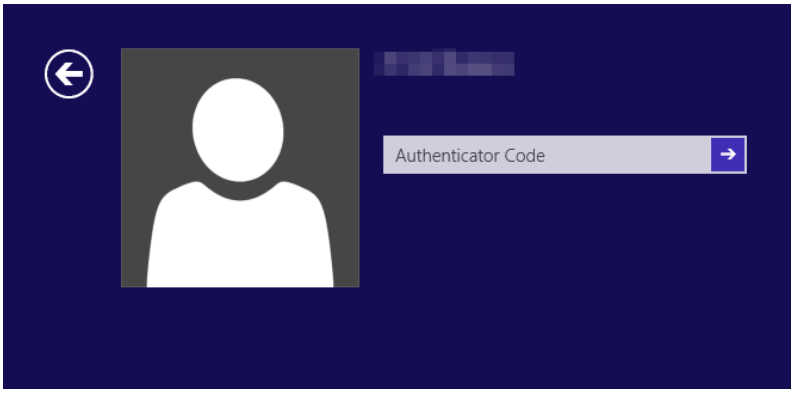
GAuthLogon may be installed to a template VM to be provisioned as virtual desktops on VDI. It should work in the same way, regardless of whether it is installed to a physical machine or a virtual machine.

When you start a remote desktop connection to a terminal server, the remote desktop client will show CredUI for the network level authentication.



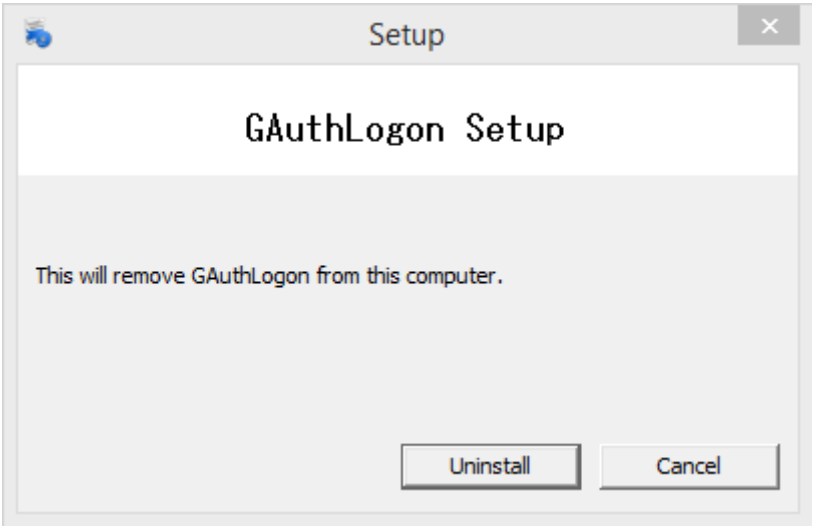

After you are authenticated, the remote desktop client will show the server sign-in screen with one tile for the authenticated user ( multiple tiles may be displayed when smart card provider or other providers are enabled ).


Select the tile. The screen for the authentication code will appear.




## Uninstallation

Press [Programs]-[Uninstall a program] in Control Panel. Select "GAuthLogon" and [Uninstall/change] button




Uninstallation will finish in a few seconds. When done, sign out. Signing out will complete the uninstallation. Do not install GAuthLogon after an uninstallation without a sign-out. If you do, most of the files installed will be erased next time you sign out.

## Updating GAuthLogon

When you have a new GAuthLogon package, just run the right Setup.exe in the same way as you installed GAuthLogon.  Setup.exe will detect if GAuthLogon is already installed and, if it is, then GAuthLogon will over-write the existing files by the new files in the package. No need to uninstall GAuthLogon before updating it.

## Configuration File

By default, the user configuration data is saved to the following file.

%homedir%\AppData\Roaming\RiBiG\GAuthLogon\gauthlogon.ini

The global configuration options may be set in the following file.

%ProgramFiles%\RiBiG\GAuthLogon\gauthlogon.ini

## Global Configuration Options

The global settings affect all users. You can set them by using the configuration program or by editing the global INI file.

### Configuration Program

Run config.exe. You can find the program in「Program Files」—「RiBiG」—「GAuthLogon」folder or in [Start]-[GAuthLogon]-[Setting]. You must have administrator privileges to execute it.

| | |
|---|---|
| No Code Authentication for Unlock | When unlocking the locked session, GAuthLogon does not show the code authentication screen. |
| Code Authentication only for Remote Login | For the console login, the code authentication screen will appear. The code authentication is required only for the remote login |
| No remote auto-login | With Network Level Authentication (NLA) enabled, GAuthLogon lets you log in to a remote server with the credential you enter at the client side and prompts only for a one-time code entry. This option disables NLA auto-login. |
| Do not filter PassProvider in CredUI | When you filter out PasswordProvider, it will not appear in the login screen as well as CredUI. This option will enable PasswordProvider in CredUI even when the provider is filter out. |
| Authenticate against LiveID | When you are not authenticated to a local / domain account, GAuthLogon tries LiveID when this option is set. Enable this option only when necessary |
| Authenticate against AzureAD | When you are not authenticated to a local / domain account, GAuthLogon tries AzureAD when this option is set. Enable this option only when PC is joined to AzureAD |
| Code Entry Timeout | Code entry screen times out and switches back to the user/password entry screen. This option sets the timeout value in seconds |
| Maximum Count for No Code Entry Login ( user ) | When no token is set by using AddToken, GAuthLogon does not prompt the user for code authentication for the first 7 logins by default. This option sets the number of logins GAuthLogon does not prompt |

| | |
|---|---|
| | standard users for code authentication while no token is set. |
| Maximum Count for No Code Entry Login （admin） | This option sets the number of logins GAuthLogon does not prompt administrative users for code authentication while no token is set. |
| Error Log File Path | Internal error will be written to this file. Give an absolute file path. The specified file must exist ( create one before hand ) |

Manual Option Configuration

You must edit the global INI file by hand.

Use Windows' PasswordProvider for the credential entry in Lock Screen

This setting enables GAuthLogon to behave exactly the same as PasswordProvider, except for the authentication code entry.

```
[Google Authenticator]
UsePassProvider=yes
```

Disable Code Authentication in Unlock Screen

GAuthLogon will not ask for one-time authentication code in Unlock screen for all users. The same option in User configuration file can over-writes the global setting.

```
[Google Authenticator]
NoCodeAuthForUnlock=yes
```

Enable Code Authentication only for the remote login

GAuthLogon will ask for one-time authentication code only for remote users. It will not show the authentication code entry page for local logins.

"ForceCodeAuth" option in the user configuration file can override this setting.

```
[Google Authenticator]
EnableRemoteCodeAuthOnly=yes
```

Enable PasswordProvider in Privilege Elevation CredUI
PasswordProvider will not be filtered in Privilege Elevation CredUI.

```
[Google Authenticator]
DontFilterPassProviderInCredUI=yes
```

Show/log File Path for debug purposes.
GAuthLogon will display the path of the user configuration file it loads. When a remote configuration file is set, the file path will be logged in the user configuration file as "ExpandedPath" in [Debug] section. Do not turn on this option in the production environment.

```
[Google Authenticator]
DispIniFilePath=yes
```

## Private Options

To set the private options, you need to edit the private INI file by hand. The private options override the global options where applicable.

Disable Code Authentication in Unlock Screen
GAuthLogon will not ask for one-time authentication code in Unlock screen.

```
[Google Authenticator]
NoCodeAuthForUnlock=yes
```

Enable Code Authentication for the user
"EnableRemoteCodeAuthOnly" disable the code authentication for a local login. This option will make the code authentication for the user mandatory.

[Google Authenticator]
ForceCodeAuth=yes

Disable Code Authentication for a user in Administrator group
A user with the administrative privileges may turn on this option to disable one-time code authentication all together.

[Admin]
NoCodeAuth = yes

This option setting in a normal user configuration file will be ignored.

## Configuration File Sharing

By default, GAuthLogon is configured to use the local configuration file for each user. When you have multiple computers, you may want GAuthLogon to use the same user configuration regardless of which computer a user may log in to. One way to achieve this is to copy the user configuration file from a computer to a computer. This may not work when the number of computers increases.

You can configure GAuthLogon to use a specified configuration file by setting the name of the file path. The file can be on a remote computer.

You set the alternative configuration file path in the user configuration file [User home folder]\AppData\Roaming\RiBiG\GAuthLogon\gauthlogon.ini.

[Redirect]
To=\\remote computer\shared folder\user.ini

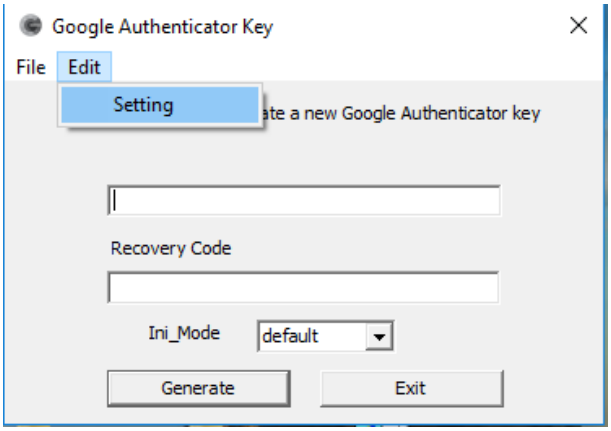
The specified file must have an access permission for the user.

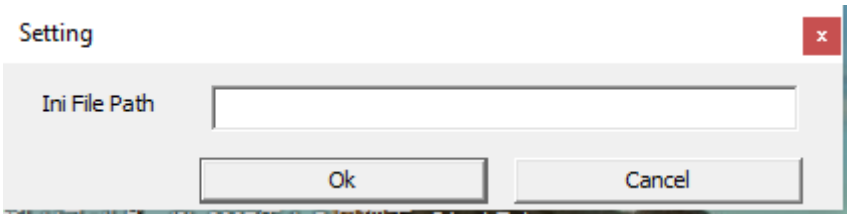
When GAuthLogon detects this option, it always tries to load the configuration data from the specified file instead of the local one. Once it successfully loads the configuration data, it caches them in the local configuration file. GAuthLogon will then use the cached configuration for the login operations.

This ensures that a user could always sign in via GAuthLogon using the cached data even when the redirected configuration file is unreachable or unavailable.

There is no global configuration file sharing scheme available.

You can set the redirected configuration path using AddToken.exe.
Select “Edit” -> “Setting” . It will pop-up a dialog for the path entry.




Enter a file path that the user has the read/write access permission and press [ok]. The path can contain environmental variables like

//remote computer/shared folder/%username%.ini

This will create the redirect section in the local configuration file. AddToken will write the configuration data to the redirected path and to the local configuration file.

## Configuration File Management

Till now, we have assumed that each user is responsible for generating QR code and setting up the device for the code authentication. For a deployment on a large number of computes, you can create configuration files and configure GAuthLogon centrally.

For the configuration file creation, we offer Excel book that has the same functionality as that of AddToken; generate the secret and the encoded strings to save as Key and Key1 in the configuration file.

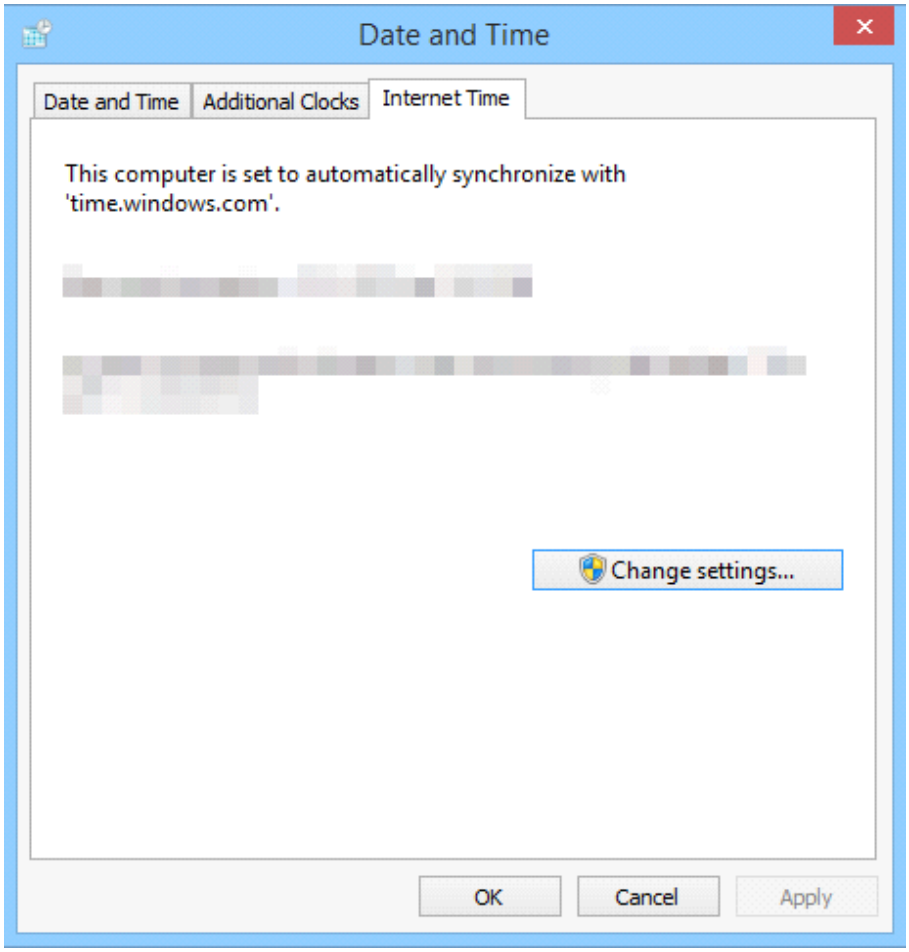
You can then write VBA code to create configuration files.

GAuthLogon installations on individual computers are configured to redirect the configuration files to ones on a remote file server.

We recommend that users have only the read permission ( no write or execute permission ) on the local configuration file to avoid tampering with the user setting.  When the local configuration file is write-protected, AddToken will show an error message and will not run further.

# Appendix 1

In order to synchronize your computer's clock with an external NTP server, select [Date and Time]-[Set the time and date] in Control Panel.




Select "Internet Time" tab. If your computer is set to synchronize with a NTP server, be sure that the synchronization reports no error. You can change NTP server from the default time.windows.com to another.

A domain joined computer synchronizes with the domain controller (DC). Configure DC to have the accurate time. A non-domain joined computer should configured to synchronize with a NTP server periodically.