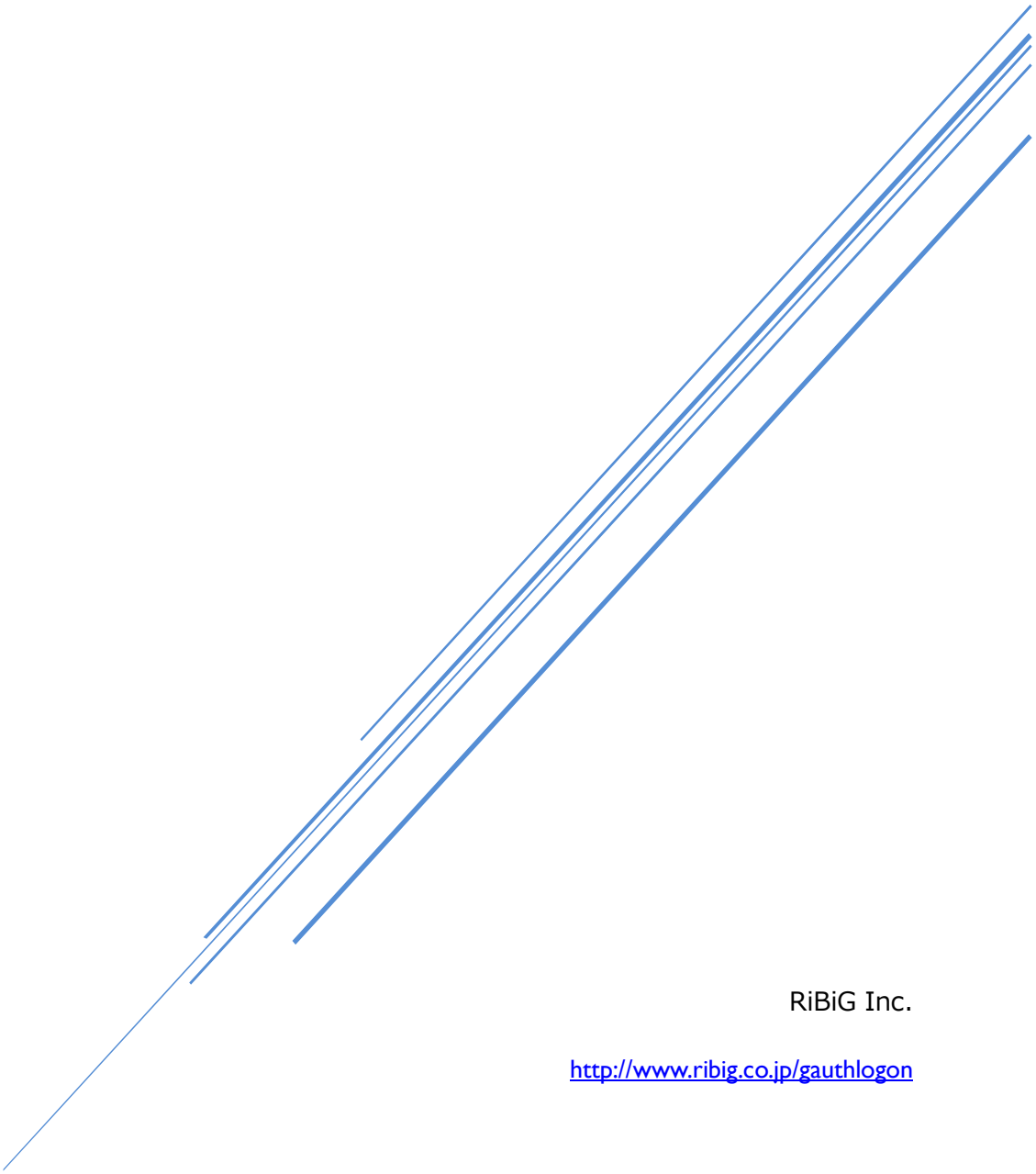
GAUTHLOGON MANUAL

Installation & Operation

Ver. 2.1.0.2



RiBiG Inc.

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

Contents

1. About GAuthLogon

GAuthLogon is a 2-factor authentication solution for Windows. A sign-in to Windows with GAuthLogon requires you to provide a valid user credential first and then to enter one-time code from an authenticator app. The process is similar to that of logging in to two factor authentication enabled Web applications.

1. User Credential Entry

2. One-Time Code Entry

A remote sign-in to GAuthLogon installed Windows will be also two-factor authentication enabled. When the remote server is properly set up, a remote desktop client will be asked to enter one-time code in the server's login screen after the network level authentication (NLA).

1.1 Installation Requirements

A. Installing GAuthLogon requires the administrative privileges

B. You should have Android/iOS devices with an authenticator app installed. Any RFC 6238 TOTP(time-based one-time password) compliant apps like Google Authenticator or Microsoft Authenticator will do.

C. Since one-time code is generated based on the current time, the computer GAuthLogon runs on and the device running an authenticator app must have their clocks synchronized. GAuthlogon will never authenticate a one-time code successfully unless PC or devices running an authenticator app have the correct time. PC should be configured to adjust the time automatically using Internet timer server. Do not forget to adjust the clock manually when a PC is without Internet connection

1.2 License Information

GAuthLogon uses the following library and source codes

- Libqrencode library for QR code bitmap generation

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

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

- Sha1

```
/*
* Copyright 2010 Google Inc.
* Author: Markus Gutschke
*
* Licensed under the Apache License, Version 2.0 (the "License");
* you may not use this file except in compliance with the License.
* You may obtain a copy of the License at
*
*     http://www.apache.org/licenses/LICENSE-2.0
*
* Unless required by applicable law or agreed to in writing, software
* distributed under the License is distributed on an "AS IS" BASIS,
* WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
* See the License for the specific language governing permissions and
* limitations under the License.
*
*
* An earlier version of this file was originally released into the public
* domain by its authors.  It has been modified to make the code compile and
* link as part of the Google Authenticator project.  These changes are
* copyrighted by Google Inc. and released under the Apache License,
* Version 2.0.
*
* The previous authors' terms are included below:
*/

/*****************************************************************************
*
* File:    sha1.c
*
```

```
* Purpose: Implementation of the SHA1 message-digest algorithm.
*
* NIST Secure Hash Algorithm
*   Heavily modified by Uwe Hollerbach <uh@alumni.caltech edu>
*   from Peter C. Gutmann's implementation as found in
*   Applied Cryptography by Bruce Schneier
*   Further modifications to include the "UNRAVEL" stuff, below
*
* This code is in the public domain
*
************************************************************************
*/
```

- Hmac

```
/ HMAC_SHA1 implementation
//
// Copyright 2010 Google Inc.
// Author: Markus Gutschke
//
// Licensed under the Apache License, Version 2.0 (the "License");
// you may not use this file except in compliance with the License.
// You may obtain a copy of the License at
//
//      http://www.apache.org/licenses/LICENSE-2.0
//
// Unless required by applicable law or agreed to in writing, software
// distributed under the License is distributed on an "AS IS" BASIS,
// WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
// See the License for the specific language governing permissions and
// limitations under the License.
```

- Base32

```
// Base32 implementation
//
```

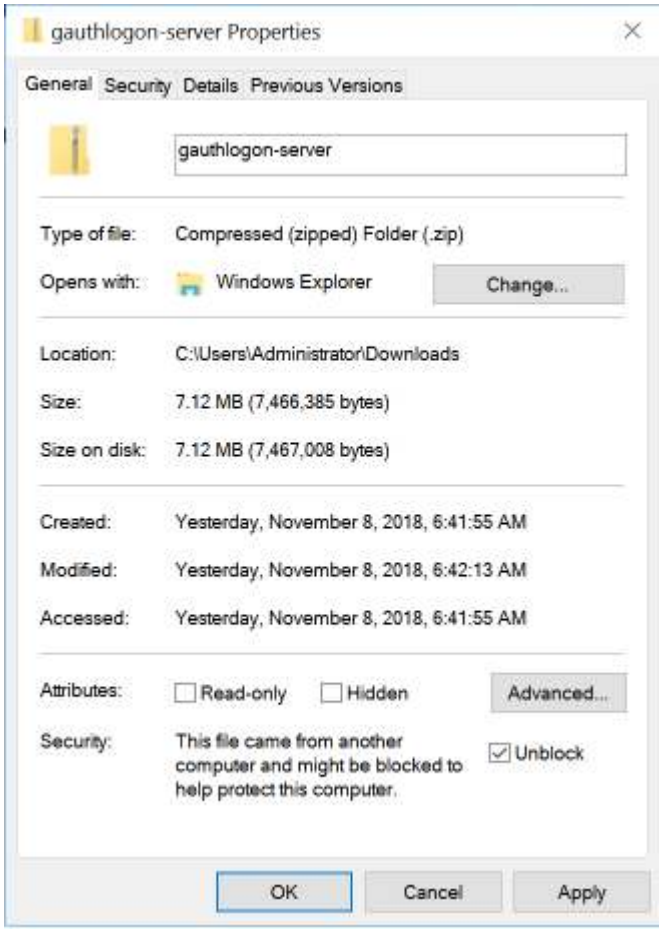
```
// Copyright 2010 Google Inc.
// Author: Markus Gutschke
//
// Licensed under the Apache License, Version 2.0 (the "License");
// you may not use this file except in compliance with the License.
// You may obtain a copy of the License at
//
//      http://www.apache.org/licenses/LICENSE-2.0
//
// Unless required by applicable law or agreed to in writing, software
// distributed under the License is distributed on an "AS IS" BASIS,
// WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
// See the License for the specific language governing permissions and
// limitations under the License.
```

GAuthLogon v2.x does not rely on OpenSSL library

2. Installing GAuthLogon

2.1 GAuthLogon ZIP File

The downloaded GAuthlogon ZIP file is probably flagged as blocked. Right-click the file and select "Property". If it is blocked, turn on "Unblock" check-box on [General] tab.



Files unzipped from the blocked ZIP file will be flagged as blocked. Windows Server OS will show a warning message when you run a file flagged as blocked. You can unblock such files individually.

2.2 Do not display last username in Logon/Locked Screen

The installation program does not automatically set the following two(2) security options. GAuthLogon assumes that username information is not displayed either in Logon or Locked screen. Set the 2 security options so that username is not displayed in either screens.

Interactive logon: Don't display last signed-in
https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/interactive-logon-do-not-display-last-user-name

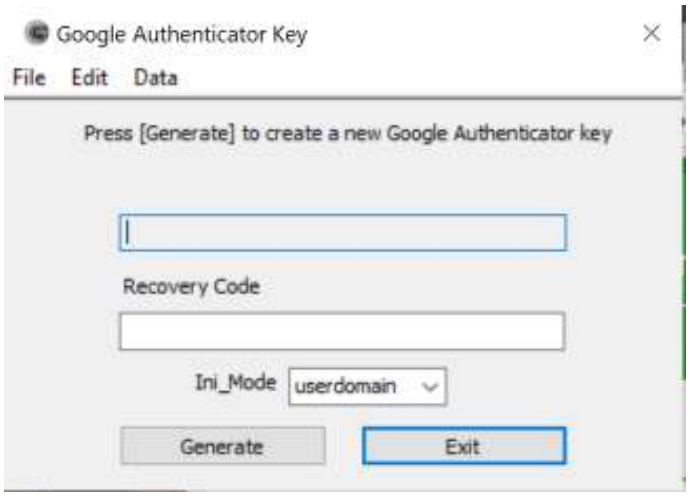
Interactive logon: Display user information when the session is locked
https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/interactive-logon-display-user-information-when-the-session-is-locked

2.3 Running Setup

Log in as an administrative user and run Auto-setup.exe in the root folder of the distribution ZIP file. It will detect the current OS and run the right Setup.exe.

Click on [Install]. Set-up will complete in a few seconds.

Pressing [OK] button will close Setup.exe.
Right after setup terminates, another program is automatically started. With this program, you set up your authenticator app

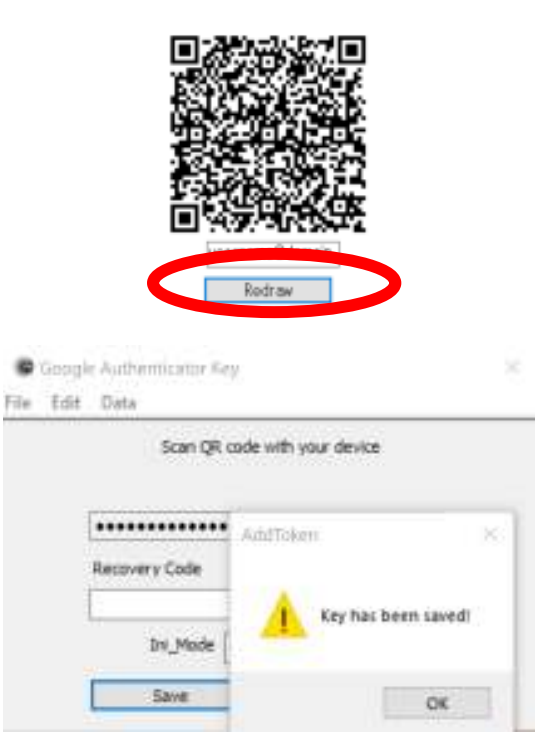


If you are logged in as a standard user but are elevated as an administrative user to run "auto-setup", exit this program. This program must set up the authenticator app for the currently logged-in user, not for the elevated user. If you are elevated as an administrative user, this program will arrange the setup for the administrative user, not for the logged in user. If you are an administrative user and are elevated as the same user, you do not have to re-run the program.

You can run the program from Start Menu.
[Start Menu]-[GAuthLogon]-[AddToken]

Or you can run the program file
%Program Files%\RiBiG\GAuthLogon\AddToken.exe

Press [Generate] button. QRCode will be displayed in a separate window. The password field in the main window is filled and the setting is saved automatically.



Press [Ok]. Scan QRCode with your authenticator app.

Before scanning, you can change the text in the edit box in the QRCode window. The default text is the login username plus the user domain. If you are elevated as another user, you will see the elevated username. In that case, clear the setting, exit the program and re-start the program. QRCode encodes this text. Your authenticator app uses the text as the label to identify whose account the one-time code is for.

After you change the text, you must press "redraw" so that the new text will be encoded in the QRCode.

Recovery Code

This is a 16 or more characters long arbitrary string that can be used instead of one-time code in the login screen. If you have lost a device with the authenticator app, you can enter the recovery code for one-time code entry field. After you enter a recovery code, press [Save]. The edit box becomes the password field.

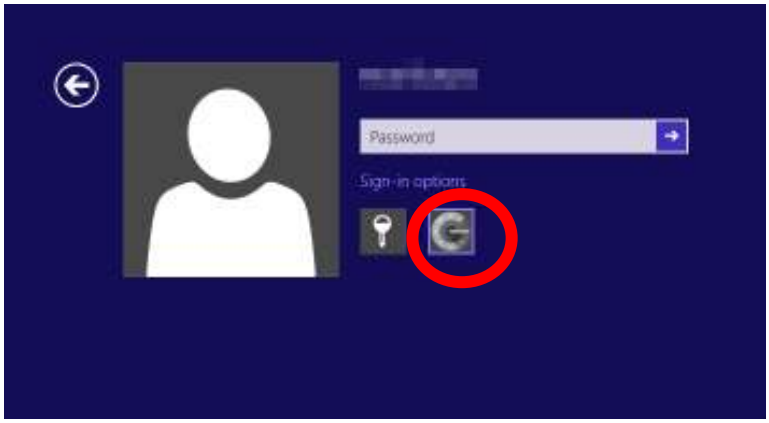
Clear the field and press [Save]. The edit box becomes a normal field and the characters are readable again. When the recovery code field is empty, double-clicking the edit box will fill it with an auto-generated code.

Now GAuthlogon setup is complete for the current user.

3. Sign In / Unlock

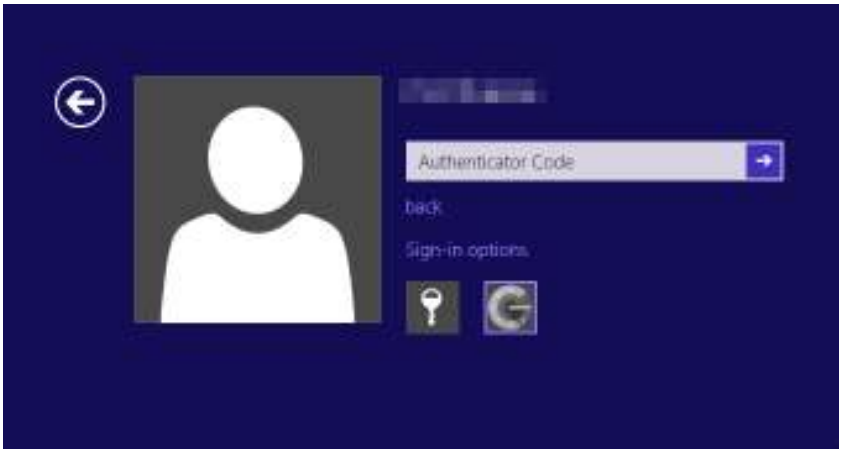
Sign out or lock the session.

In the login screen, click on “Sign-in options” link. You will find GAuthLogon icon.



Select GAuthLogon and enter your user credential. The user must be the same as the one who has installed GAuthLogon. The other users have not yet set up

their authenticator app. When your credential is successfully authenticated, the screen prompts for one-time code.



Type in the one-time code displayed on your authenticator app. If the code is correct, you will be able to sign in to Windows.

3.1 Log in by a user without an authenticator app set up

Sign out again. This time, try to sign in as another user. An authenticator app is not set up for this user, yet. GAuthLogon will not ask for one-time code; it just displays a warning that GAuthLogon has not been set up for the user and that the user should set it up.

GAuthLogon provides for the "grace" period. The default is 7 sign-ins for each user. Each user can log in 7 times without an authenticator app set up. Once the grace period is over, the entry of a valid one-time code is required.

It is each user's responsibility to set up an authenticator app.

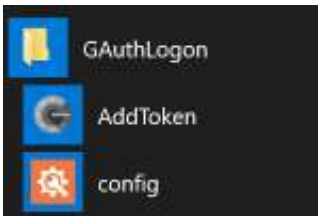
3.2 Log in using Recovery Code

If you have set up a recovery code, enter it in the one-time code field in the login screen. GAuthLogon displays a message that you have used the recovery code and that it has erased the current setting. Once logged in, generate and scan a new QRCode and set a new recovery code.

4. Setting up your authenticator app

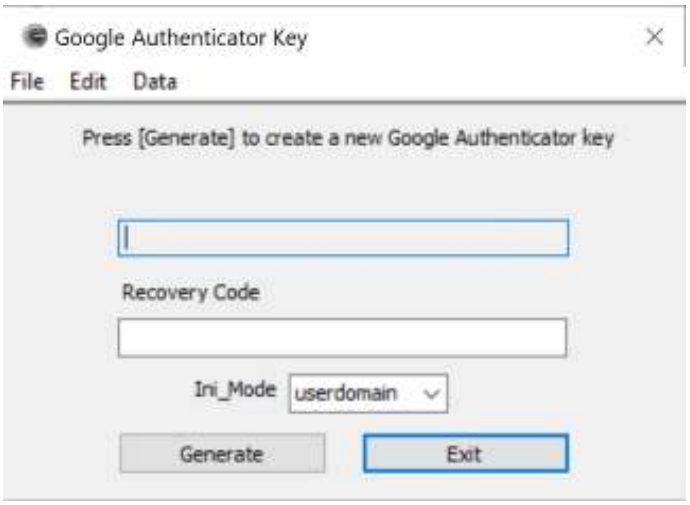
To set up an authenticator app, run AddToken

1. You can run it from the start menu.
   [Start Menu]-[GAuthLogon]-[AddToken]

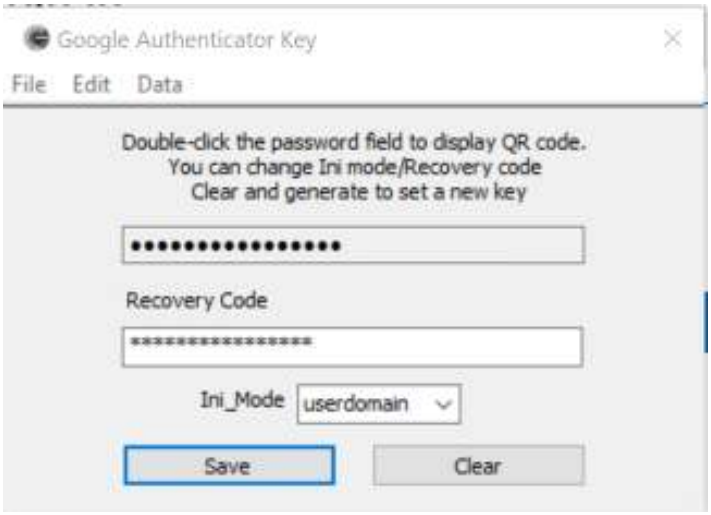


2. You can run the program file
   %Program Files%\RiBiG\GAuthLogon\AddToken.exe

The program prompts to generate a new QRCode when it find no setting data.



When it finds one, it reads it and sets the fields to reflect the current setting.



Double-clicking the password field will display QRCode for the current setting.

You can change the recovery code by clearing the field and pressing [Save] button. The characters you enter will be readable again. Be sure to [Save] the new recovery code.

Ini_Mode specifies how the program saves the setting data.

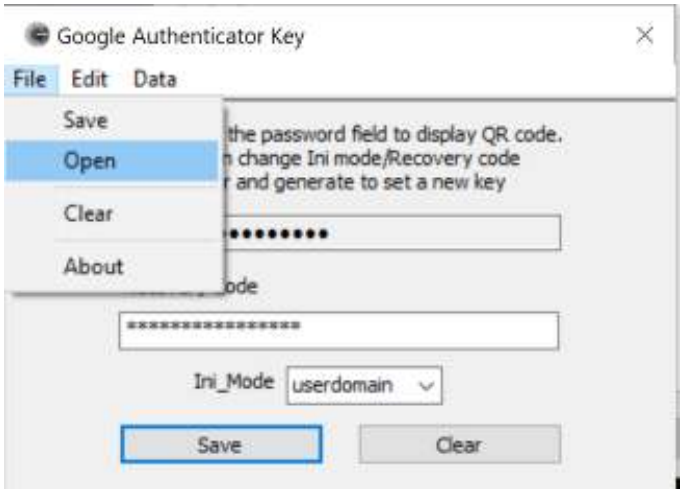
unique	the setting data is saved such that only the current user on the current computer can read
userdomain	The same domain user or local users with the same username can copy the setting data
share	The setting data can be copied among users.

The default mode is “userdomain”.

The setting data is saved as a text file in the user’s profile folder.

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

Selecting [File]-[Open] will open the setting file in Notepad.



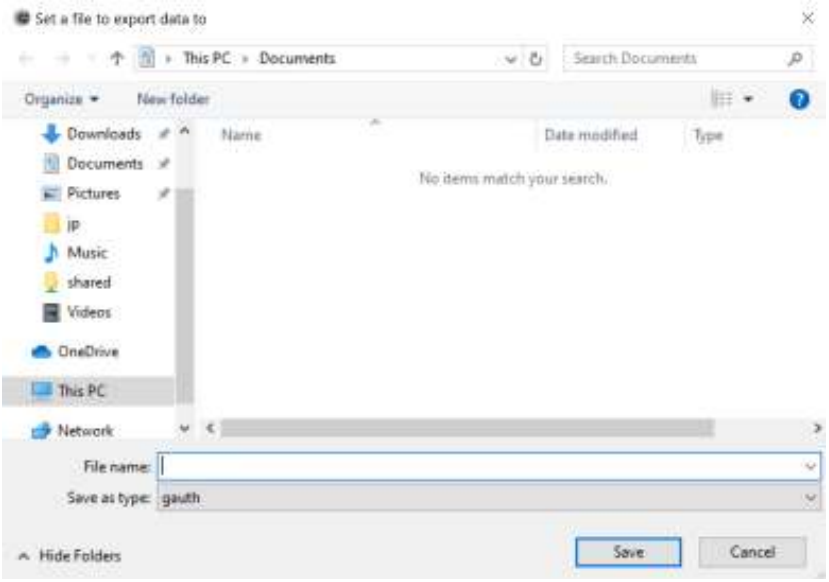
When Ini_Mode is set to "unique" or "userdomain", the important data is encrypted in a way that only the user who encrypted it can decrypt. You cannot just copy the setting file to another user's profile folder.

When it is set to "share", the setting file may be copied among the users on the same computer. The setting file cannot be copied to another computer; the important data is encrypted in a way that only the computer that encrypted the data can decrypt. You need to export the setting and import it on another computer.

Userdomain

To copy a setting, export it and import the exported file to the same domain user account on a different computer. A local user setting can be exported and imported between local users with the same name.

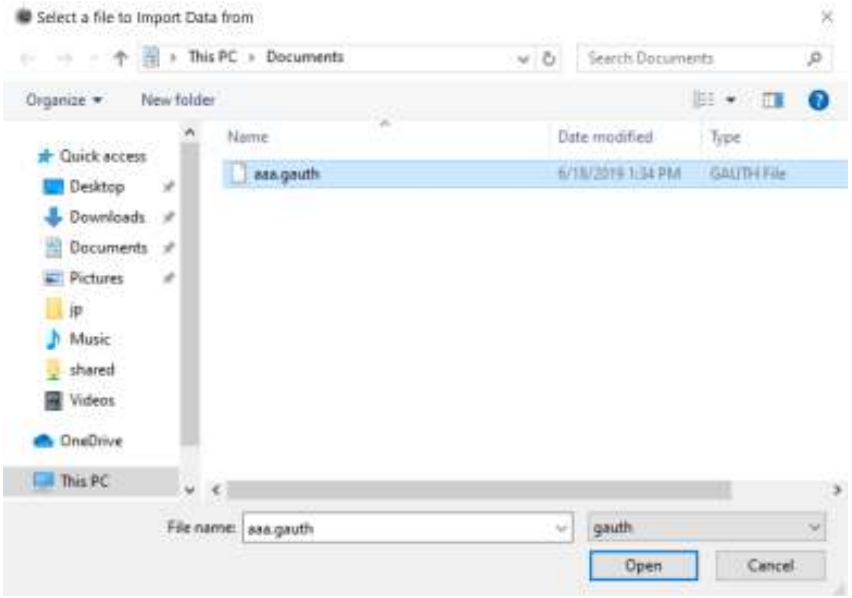
To export, select [Data]-[Export]. In the file dialog, set a file to export the data to.



After an export file is set, enter the password for the file.

The same domain user as the current domain user or a local user with the same name as the current local user can import the exported file. Any other users can import the exported file but the setting will not be recognized as valid.

To import, select [Data]-[Import]. In the file dialog, select an exported file.



Supply the correct password for file and the import will be complete.

Share

When Ini_Mode is set to "share", the setting file can be copied among the users on the same computer. To copy a setting among users on different computers, export one first and import.

Unique

This is the most secure way to save the setting. The unique setting cannot be exported. A back-up can be created by copying the setting file to another file.

4.1 Set up for Another User

AddToken may be used to set up an authenticator app for another user. Keep pressing [SHIFT] key when running the program. It will display "RunAs" window. Enter the credential of the user to set up for.

The program is run as the specified user and the set-up data is stored to that user's profile folder.

5. Enabling Two Factor Authentication At All Times

Even after you have installed GAuthLogon, two factor authentication is not enforced. You can select any other providers available like the standard PasswordProvider in the login screen.

To enforce two factor authentication, you need to set up the provider filter so that the providers other than GAuthLogon will not be available in the login screen.

5.1 Setting up Provider Filter

Run config.exe. You can find the program in

1. [Start Menu]-[GAuthLogon]-[config]

2. %ProgramFiles\RiBiG\GAuthLogon.

This program changes the system setting and requires the administrator privileges to execute it.

Once the program window is opened, select [CP Filtering] tab

The list box on the left shows the providers available on the system. Select a provider to filter to the right list box and press [=>] button. It will be moved to the right list box. To enforce GAuthLogon's two factor authentication, filter out the following 4 providers.

** The evaluation copy can filter up to two providers.*

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

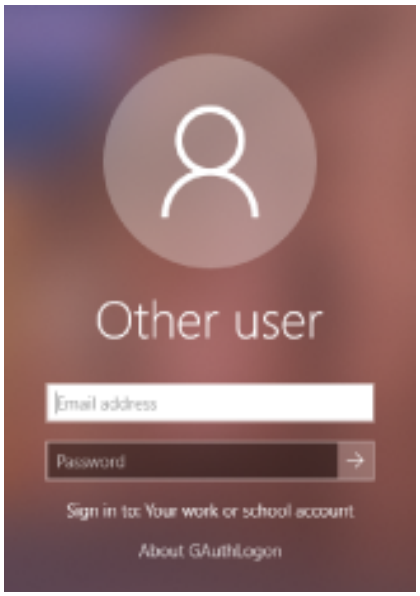
When Windows is AzureAD joined, PIN logon becomes visible. Filter the following

provider to erase it in the login screen.

5. NGC Credential Provider

Filter setting will be automatically saved.

Exit the program and sign out. In the login screen, you will find no “Sign-in options” link or “Sign-in options” link that does not show Password, PIN, Picture Password, LiveID providers’ icons.



5.2 Enabling GAuthLogon in SafeMode

When Windows boots to Safe Mode, all third-party credential providers are disabled by default. Safe Mode exists for the maintenance purpose; you always want to log in to Windows successfully in Safe Mode, even when a third-party credential provider misbehaves and prevents Windows from showing the login screen. Safe Mode exists to correct such issues. By enabling third-party credential providers in Safe Mode, you disable that safety feature.

This risk mentioned, enforcing two factor authentication in Safe Mode (enabling GAuthLogon and filtering PasswordProvider and other providers in Safe Mode) enhances your Windows security.

If you choose to enable third party credential providers, do it carefully.

1. Enable GAuthLogon in Safe Mode, but do not filter out PassProvider at first. Boot to Safe Mode and see if Windows boots successfully and you can log in using GAuthLogon. Only after that, filter out PasswordProvider.

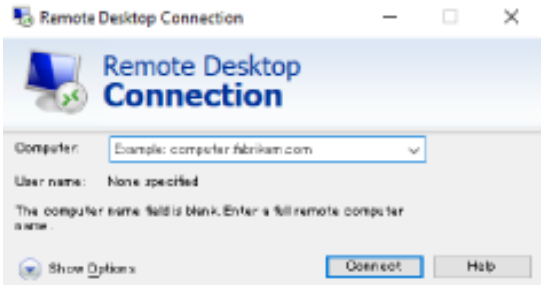
2. Always set a recovery code; you can use it when one-time code authentication fails.

An administrator user can set the private option “DisableGAuthInSafeMode” which enables the user to disable GAuthLogon in Safe Mode at the login time if the recovery code is used.

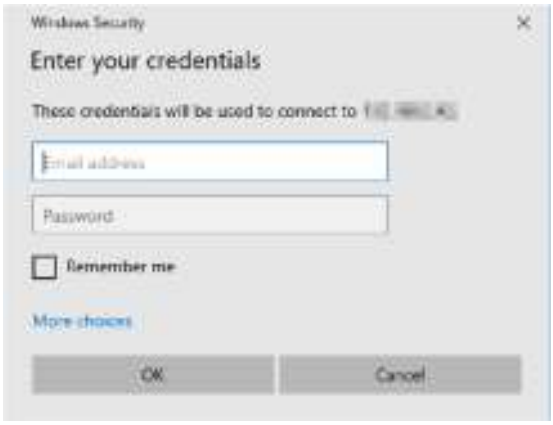
6. Remote Desktop

You can enforce two factor authentication on the remote sign-in to GAuthLogon installed Windows. When you enforce two factor authentication for the local sign-in, it is also enforced for the remote sign-in.

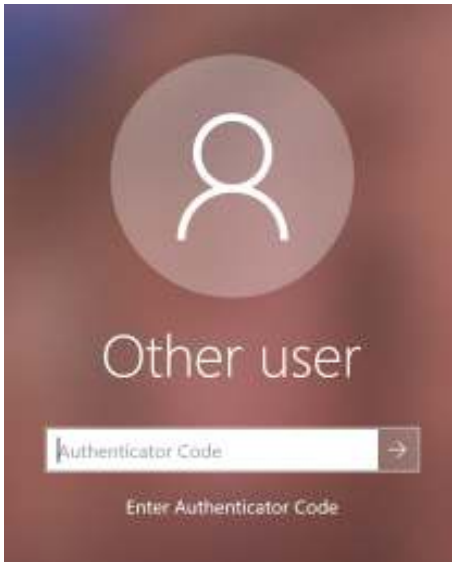
Run the remote desktop client.



Supply your remote credential for NLA (network level authentication)



Enter one-time code for the remote user.



- Windows 10 version 1709 (2017 Fall Update) If the remote desktop server side is running this version, you will be asked to provide your credential in the server login screen again even if NLA is successful. This Windows version does not offer the chance for credential providers to receive a NLA credentials.

7. Redirection of the setting file location

This is GAuthLogon's implementation of the setting file location redirection. We suggest that you use this feature as the last resort when you cannot use the other methods as described in "setting_syncing" manual.

In the domain environment, Windows' roaming user profile / folder redirection may be set up. GAuthLogon user settings are saved on a server. Every time a user tries to log in on a domain computer, GAuthLogon will read the settings on the server. A user can change his settings on a domain computer. When he tries to log in on another domain computers, the changed setting will be read.

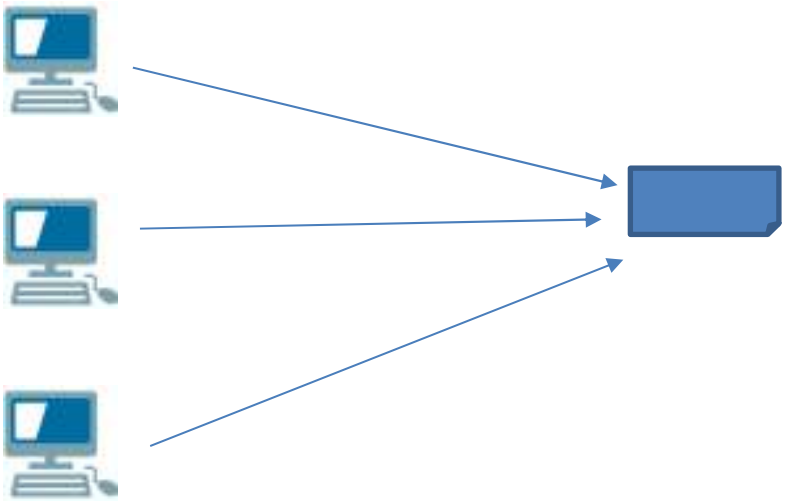
If Windows' roaming user profile / folder redirection is not set up and computers are always connected to Internet, you can save GAuthLogon setting on a cloud storage. The setting on a cloud storage may be shared by users on multiple computers.

Please refer to "setting_syncing" manual for the details

When neither Windows' roaming user profile / folder redirection or cloud storage does not meet your needs, then consider using GAuthLogon's implementation of setting redirection as explained here.

GAuthLogon saves the setting in each user's profile folder by default. The changes in setting by a user will not affect the other users' setting. When you are using multiple computers, you may want to share one setting among them.

The changes you make on one computer can be shared by the others using the same setting file; no need to modify the setting on each computer.

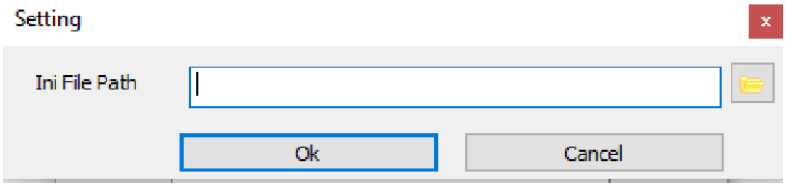


Ini_Mode:

Unique	You cannot share the setting. It is private.
Userdomain	The same domain user on multiple computers can share the setting. Local users with the same username can also share.
Share	A setting can be shared by any users.

To redirect a setting file location, run AddToken and select [Edit]-[Setting].

Specify the redirect destination file.



If you have enabled the redirect, you can disable the redirection by clearing the path field and pressing [Ok].

The current setting is copied to the new redirect destination file.

Select [File]-[Open]. This will open 2 setting files; one is the local file and the other the redirect destination file. The local file has [Redirect] section with the value [to] that points to the destination.

Sharing redirect setting

When a user on a machine enables the redirect, export the setting. The users on the other machine must import the exported setting to share the redirect destination. If another user tries to set the redirect to the same destination, this last user's setting will be effective. The previous user's setting will be nullified.

Sharing requires both the local and the redirect setting

You can specify a network path as the redirect destination. When the redirect is enabled, GAuthLogon always saves the setting in the user's profile folder as well as the redirect destination. Even when GAuthLogon cannot reach the path due to network connection failures, it will successfully authenticate one-time code using the local setting.

When you use the recovery code for login, only the local setting is erased. The redirected setting remains intact. This inconsistent state between the local and the redirect setting is not automatically resolved; you must manually restore the redirected setting to the local setting. For this, run AddToken. It will read the redirected setting. Pressing [Save] will save its local copy.

When the redirect is enabled, you need to pay attentions to the recover code handling.

Userdomain	The redirect destination is shared by the same domain user or the local user with the same name. These users can share the recover code. The recovery code is saved in the redirect destination. This means that, if a user on a machine changes the recovery code, it will be the new recovery code for all users sharing the setting. When a user on a machine logs in with the recovery code, the local setting of the user on the machine is erased. The user must manually synchronize the setting with the redirect destination.
Share	The redirect destination is shared by different users. They should not share the same recover code; the recover code is not saved in the redirect destination. GAuthLgon uses the recovery code stored locally in the user's profile folder. If a user on a machine changes the recovery codes, the new recovery code is good for the user on that particular machine.

8. Configuring GAuthLogon

The global configuration setting is saved to,

%ProgramFiles%\RiBiG\GAuthLogon\gauthlogon.ini

The private setting will be found in.

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

8.1 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.

8.1.1 Configuration Program

Run config.exe. You can find the program in

1. [Start Menu]-[GAuthLogon]-[config]

2. %ProgramFiles\RiBiG\GAuthLogon.

This program changes the system setting and requires the administrator privileges to execute it.

Select [Global Setting] tab.

No Code Authentication for Unlock	When unlocking the locked session, GAuthLogon does not ask for the code authentication.
Code Authentication only for Remote Login	GAuthLogon does not ask for the code authentication for the local login. The code authentication is required only for the remote login
No remote auto-login	The remote client to GAuthLogon installed server will have to enter user credentials in the server's login screen, even after a successful NLA (network level authentication)
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	The user credential you enter is authenticated against the local and domain database first. If not authenticated, GAuthLogon authenticate against LiveID authentications. Enable this option only when necessary
Authenticate against AzureAD	The user credential you enter is authenticated against the local and domain database first. If not authenticated, GAuthLogon tries to authenticate against AzureAD. 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)	Set “Grace” count; the number of log-in a standard user is allowed without setting up an authenticator app.
Maximum Count for No Code Entry Login (admin)	Set “Grace” count; the number of log-in an administrator user is allowed without setting up an authenticator app.
Error Log File Path	Internal error will be written to this file. Give an absolute file path. The specified file must exist (create one manually)

Other Options

These options must be set manually

[Google Authenticator]
NoCodeAuthForUnlock=yes

GAuthLogon will not ask for the one-time authentication code in Unlock screen for all users. The same option exists for the private setting which overwrites the global one.

8.2 Private Optional Setting

To set the private options, you need to edit the private INI file manually. The private options override the global options.

[Google Authenticator]
NoCodeAuthForUnlock=yes

GAuthLogon will not ask for one-time authentication code in Unlock screen.

[Google Authenticator]
ForceCodeAuth=yes

The global option "Code Authentication only for Remote Login" disables the code authentication for the local login. This option will override the option; this user has to enter one-time code in both the remote and the local logins

[Admin]
NoCodeAuth = yes

This option is only for the administrative users. GAuthLogon will not ask for the one-time code authentication for this user. This option setting in a normal user setting will be ignored.

[Admin]
DisableGAuthInSafeMode= yes

This option is only for the administrative users. When this user logs in with the recovery code, GAuthLogon displays a message box asking if GAuthLogon should be disable in Safe Mode. The message box only appears when GAuthLogon is enabled in Safe Mode.

9. Saving and Switching Profiles

The current setting can be saved as a named profile. Up to 8 profiles may be created. A profile may be loaded into the current setting.

Saving the current setting

Enter a label for the current setting in the edit box on the right.
Press [Save the current setting as] button.

Switching to a new profile

Double-click a profile in the left list box.

Overwriting an existing profile

Select a profile name in the list box. The name will be entered in the edit box.
Press [Save the current setting as] button.

Deleting a profile

Select a profile name in the list box and press [Delete Profile] button.

10. Excepted User/IP

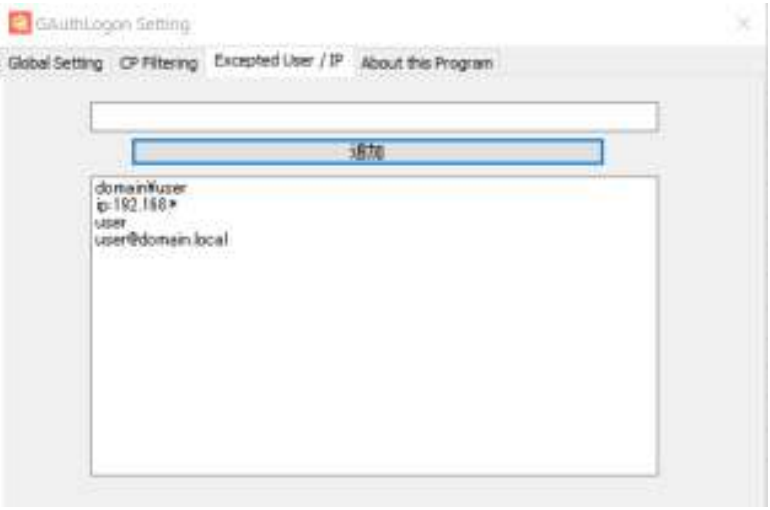
You can exempt any users from the code authentication. Those excepted users will not see the code authentication screen when logging in via GAuthLogon. You can also exempt remote client computers from the code authentication.

Run config.exe.

1. [Start Menu]-[GAuthLogon]-[config]

2. %ProgramFiles\RiBiG\GAuthLogon.

Select [Excepted Users] tab.



The list box shows the currently exempted users/IPs.

10.1 Adding a new excepted user / IP

Enter the username as you would enter in the login screen in the edit box and press [Add]. Prefix "ip:" for IP(both IPv4 and IPv6) addresses like "ip:192.168.1.1" and "ip: 2001:0DB8:AC10:FE01::1". The remote login from the computer with IPc4 192.168.1.1 / IPv6 2001:0DB8:AC10:FE01::1 will not require the code authentication. The wild character (*) may be specified for IP (e.g. 192.168.1.*)

10.2 Removing from excepted users

Double-click on the username in the list box.

11. About Evaluation Version

GAuthLogon will run as the evaluation version while no license file is installed.

I. The evaluation version generates the same QRCode. This means that all authenticator apps for any users shows the same one-time code all the time.

2. Up to two credential providers can be filtered.

After installing a license file, users must re-generate QRCode and set up their authenticator apps. Only after this will your authenticator app begins to show unique one-time code different from other users'.

12. Installing License File

12.1 Acquiring a License File

To acquire a license file,

1. Generate a hardware ID string using HWID utility
2. Open GAuthlogon license web site and have the license tied to the hardware ID issued
3. You need to have an account with the license web site for it to issue you a license.

12.1.1 Generate a hardware ID string using HWID utility

Run "hwid.exe" in the root folder of the distribution ZIP file. The program will generate the hardware ID that identifies the PC running hwid.exe.

The previous versions used MAC address in generating the hardware ID and, when having detected multiple MAC addresses, prompted you to select one of them. The current version no longer detects MAC address; it generates a hardware ID without user interventions.

HWID.exe generates a hardware ID by calculating a hash from the PC hardware properties. You cannot construct or guess the original value from a hash; the hardware ID cannot be manipulated/exploited to identify your hardware

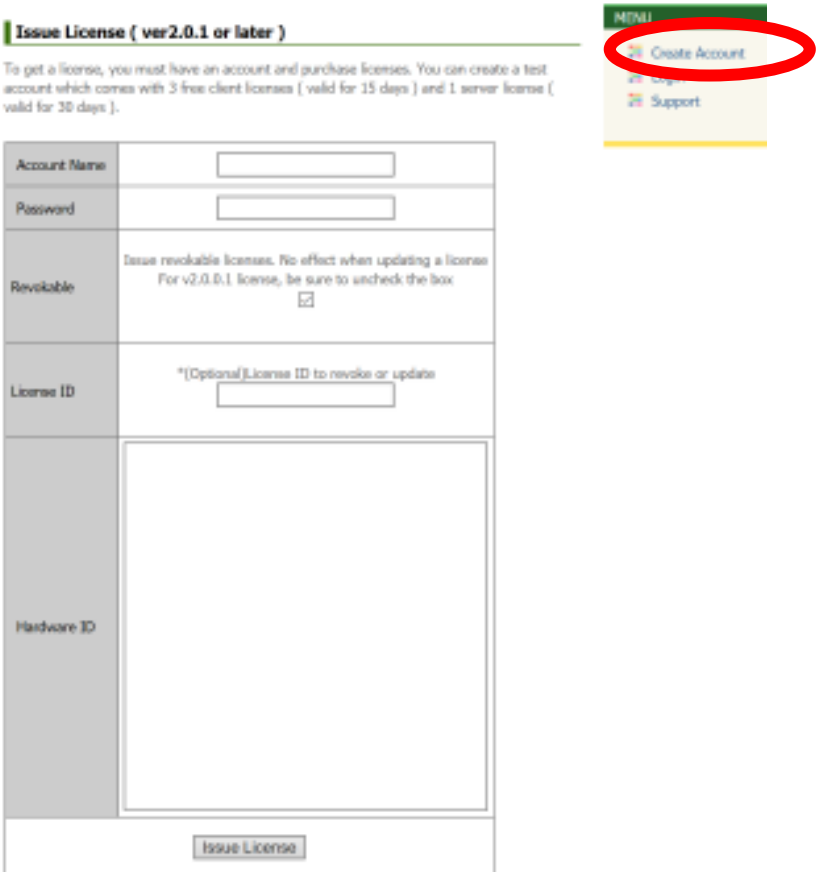
Once the hardware ID of the computer is generated, it will be shown in the right edit box. The previous versions copied the generated hardware ID to the clipboard. The current one does not. Some anti-virus software deems the use of clipboard manipulation API as malicious operations and detects such a program infected. To avoid the false-positive detection, the current version does not call the clipboard copy API. Please manually copy the hardware ID.

12.1.2 Open GAuthlogon license web site and Issue a license tied to hardware ID

With the hardware ID string ready, opent GAuthLogon license page.

https://www.ribig.co.jp/gauthlogon/license/en/index.php

IE on Windows 2008 Server may not be able to open this site due to the license page's TLS/SSL protocol. Use other browsers like Chrome, should this be the case.



Enter username/password, paste the hardware ID text to the HWID field and press [new license] button. This will download a license file.

By default, the revocable check is not enabled. A non-revocable license will be created. When you install this type of license, GAuthLogon locally authenticates the license. No Internet connection is required. GAuthLogon will work on a stand-alone PC. A non-revocable license is tied to a specific PC; you cannot transfer one to another PC.

From ver. 2.1.0.1, a revocable license type is available. When you install this type of license, GAuthLogon programs authenticate the installed licenses against a license server on Internet. If it is authenticated locally but not remotely, then the programs will not run. If there is not license file or the local authentication fails, then, the programs will run in the demo mode.

You can revoke a revocable license. Once a license is revoked, you can create a new license, specifying the ID of the revoked license. The remaining license days

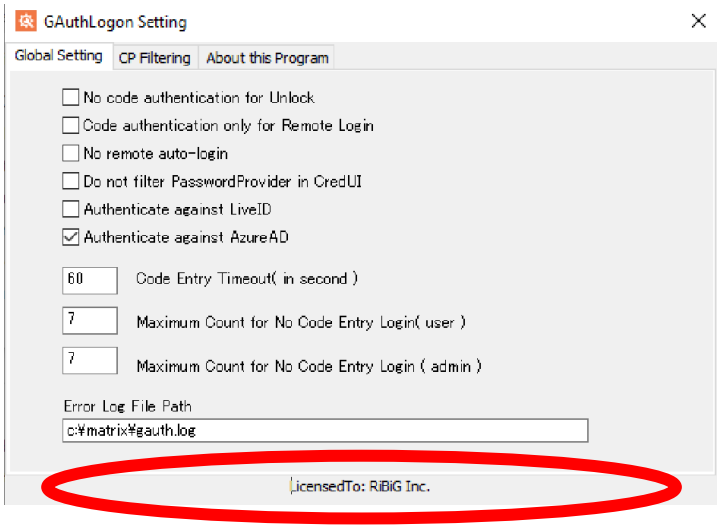
of the revoked license will be set to the new license's license day. If a revoked license has 30 valid days left, then the new license will be valid for 30 days. You can revoke a license tied to a PC and issue a new license tied to another PC.

You can extend a revocable license. Create a new license, specifying the ID of the valid revocable license. The remaining valid license days will be carried over to the new license. If you have a server license expiring in 10 days, extending it will create a new server license whose valid license days will be 365 days plus 10 days.

12.1.3 Creating an account

You must have an account to create a license file. To create an account, select "Create Account" in the menu

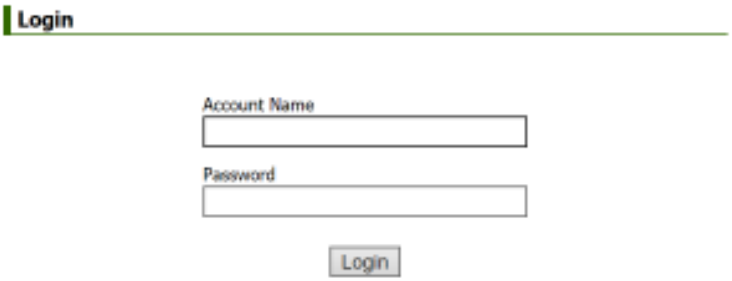
Licensee name will be encoded in the license file and displayed as the licensee name by GAuthLogon programs.



Once an account is created, an email will be sent to the account's email address. The created account is not enabled, yet. The mail contains the link to enable the account.

12.1.4 Login

Once an account has been created and enabled, you can log in.

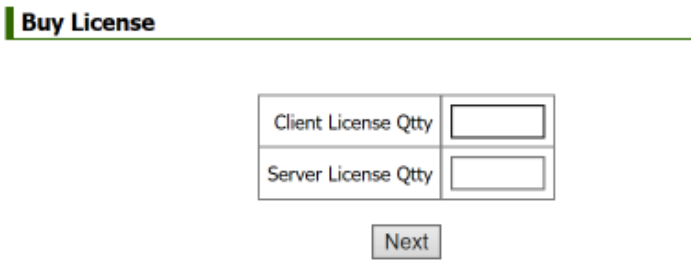


When you log in, the page showing the list of purchased and issued licenses will be displayed. Open "Help" page for the details.

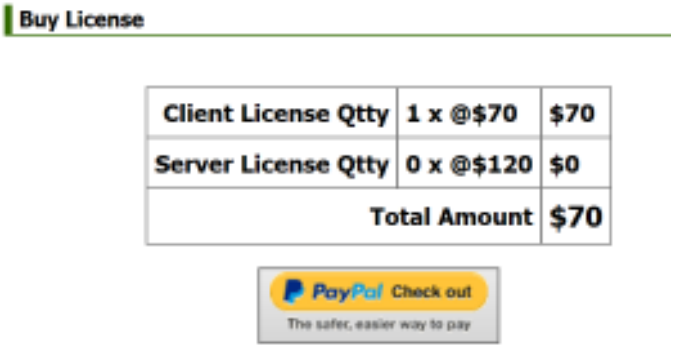
A test account has 3 client licenses and 1 server license automatically assigned. A test account cannot purchase, revoke or extend a license.

12.1.5 License Purchase

A regular account must buy licenses.



Fill the quantity and press [Next].



Clicking on [Paypal Check out] button will open Paypal site. Log in to Paypal account and confirm the purchase. You will be redirected back to our site for the final confirmation. [Confirm] button will complete the transaction. [Cancel] button aborts the order process.

Once the transaction is complete, open the license list page and review the latest status.

12.2 Installing the downloaded license file

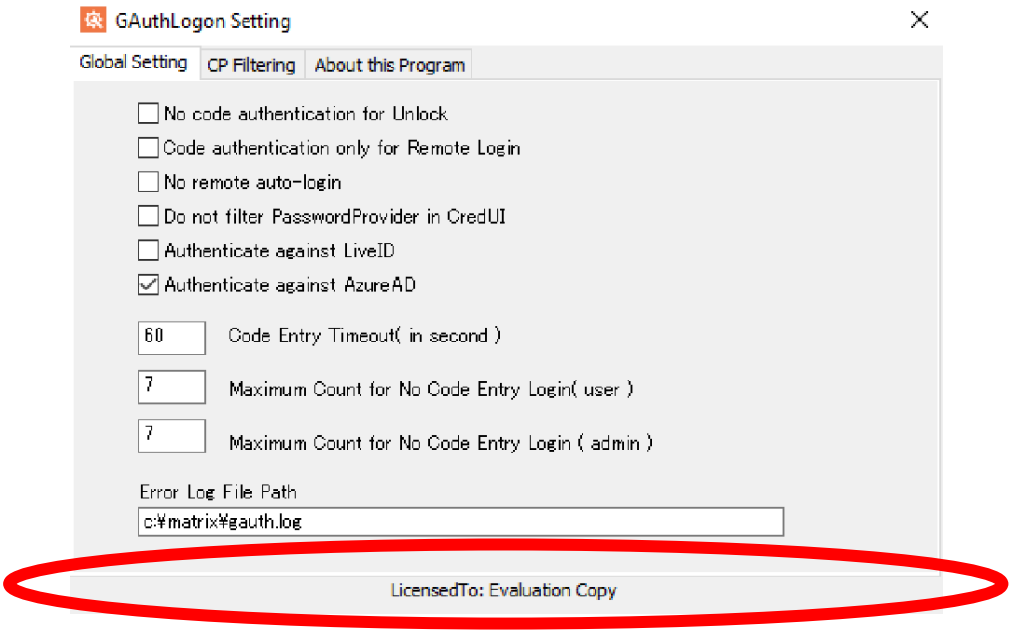
The downloaded license file must be correctly installed.

Run config.exe. You can find the program in

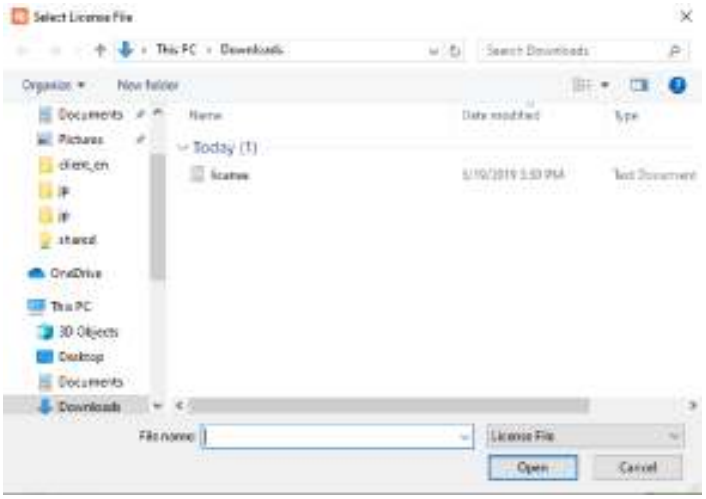
1. [Start Menu]-[GAuthLogon]-[config]

2. %ProgramFiles\RiBiG\GAuthLogon.

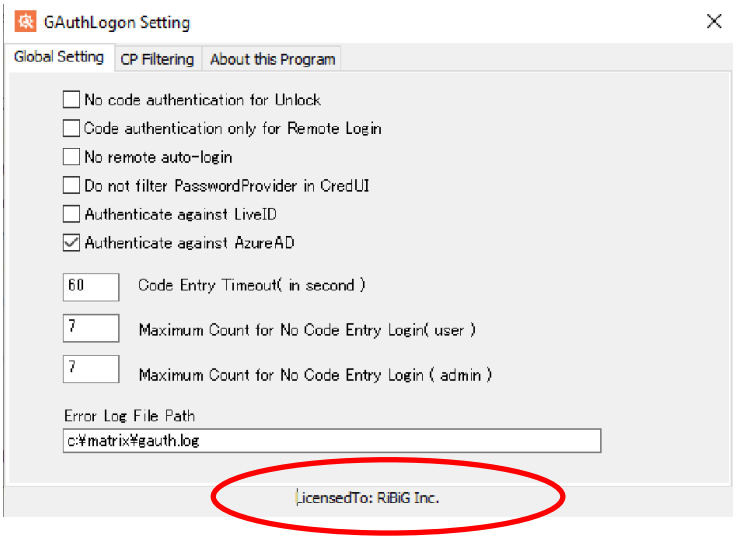
Double-click on the bottom area of the program window where "LicensedTo: Evaluation Copy" is displayed.



The file dialog is opened; select the downloaded license file and press [Open].



This installs the license file. Once it is properly installed, the licensee name that you set while creating your account will be displayed in place of "Evaluation Copy".



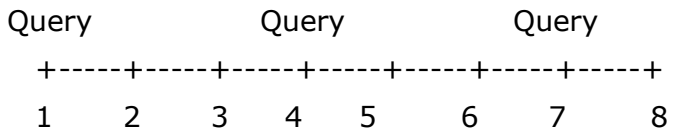
The license is installed as %ProgramFiles%\RiBiG\GAuthLogon\license.txt. Though the file name is the same as the downloaded file, their contents are different.

12.3 Remote Authentication of Revocable License

When you install a revocable license, GAuthLogon programs will try to authenticate the license against our internet license server when they are run. The programs establish a secure connection (HTTPS) to the server and receives responses

12.3.1 License Query

GAuthLogon programs do not query the license server every time they are run; a query takes place once every few days.



In this example, queries are issued to the server on Day 1,4 and 7.

The license revocation takes this into consideration; when you revoke a license, the revocation date will be the next query date. If you revoke a license on Day 2, the revocation date is set to Day 4. The revoked license remains valid on Day 2 and 3. You cannot use the revoked license ID to create a new license before the revocation date.

12.3.2 HTTPS Connection

The query is made by establishing HTTPS connection to the license server. Configure Windows for the connection to succeed.

A login user must be able to open a web page with Windows pre-installed browsers.

If a proxy server is used for the Internet connection, you must configure WinHTTP proxy server. Windows Update uses WinHTTP; if Windows Update is working, then, WinHTTP proxy server has already been correctly set.

You can set WinHTTP proxy server, issuing "netsh winhttp" command in Administrator command prompt

To display the available commands
>netsh winhttp

Try to issue a command using one of the displayed command; you will get the list of available commands for the issued one.

To import IE proxy setting of the login user

>netsh winhttp import proxy source=ie

To set a specific proxy manually

>netsh winhttp set proxy proxy-server="192.168.x.x" bypass-list="*.local"

If you set a wrong proxy server, GAuthLogon will not be able to connect to the license server; it will block till the connection times out.

You can set the timeout values for the license connection in "gauthlogon.ini" in GAuthLogon installation folder(%Program Files%\RiBiG\GAuthLogon)
Set the timeout values under [Remote License Auth] section.

```
[Remote License Auth]
ResolveTimeout=10000
ConnectTimeout=10000        //   10 seconds
SendTimeout=10000
ReceiveTimeout=10000
```

12.3.3 Failure in establishing a connection to the server

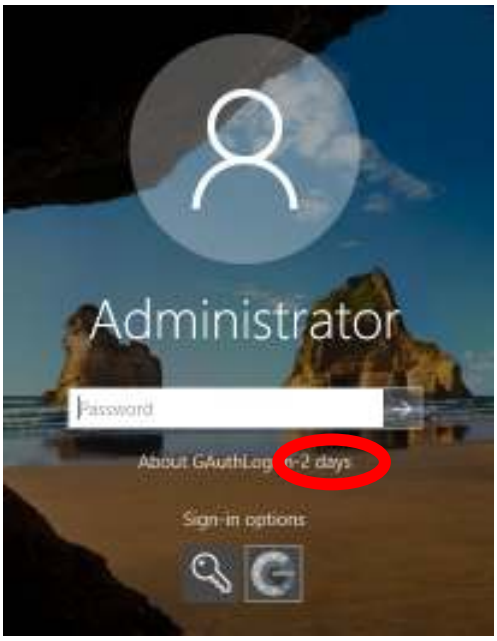
When a valid license is installed but a connection to the license server cannot be established, you cannot log in to Windows. If you permit a login in such a case, manually disabling the network adaptor can bypass the remote authentication and defeats the purpose of the remote authentication.

If a connection error is accidental, boot Windows to Safe Mode; GAuthLogon will not query the license server and there will be no connection error.

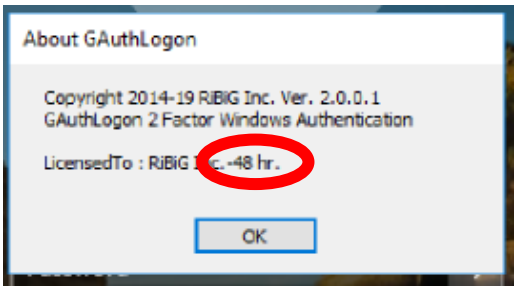
Rename or delete a valid license file; GAuthLogon will work in the demo mode. It will not attempt any remote license query and there will be no connection error.

12.3 License Expiration

The server license is valid for one year by default. When the license expiration is drawing near (about 5 days away), “About GAuthLogon” link will begin to show the remaining time in days.



Click the link and the dialog will display the remaining time in hours.



Once the installed license expires, GAuthLogon runs in the evaluation mode. If it finds the setting by the product version, it does not load it; it does not show the code authentication screen. It displays a message “The evaluation version cannot use the product version code. Code authentication is skipped”. If you want to continue to use the pre-expiry setting, install a new license; GAuthLogn will be in the product mode, load and use the pre-expiry setting. Alternatively, delete the expired license file and use AddToken to create the evaluation version setting.

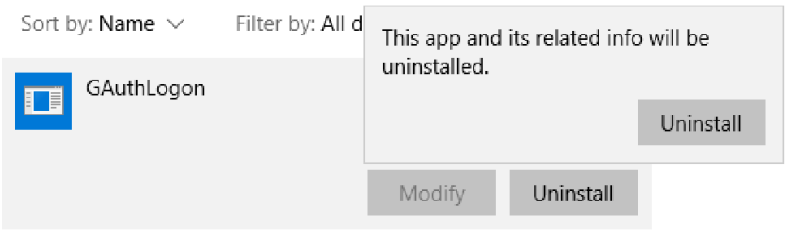
13 Updating GAuthLogon

You may overwrite the program files (DLL/EXE) in GAuthLogon installation folder (%ProgramFiles%\RiBiG\GAuthLogon) with new program files in GAuthLogon ZIP package file. When you find a new GAuthLogon.DLL in the package file, for example, just copy it and overwrite the existing one in the installation folder. This will update the main program, GAuthLogon.DLL.

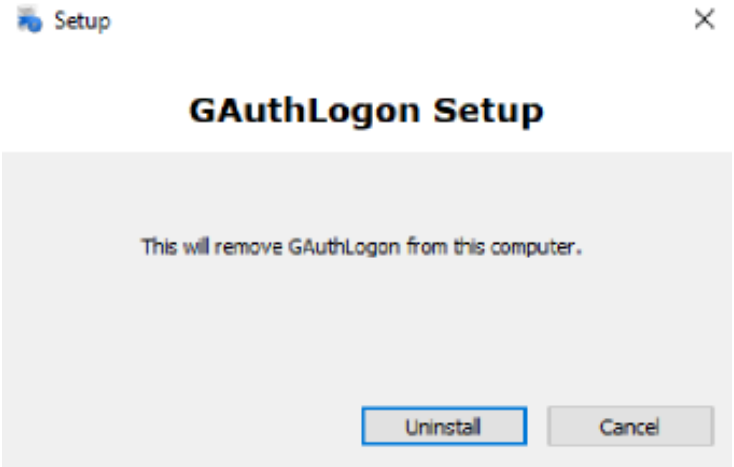
14 Uninstallation

If you have License.txt in GAuthlogon installation folder and want to keep the file, create a back-up for uninstalling GAuthLogon.

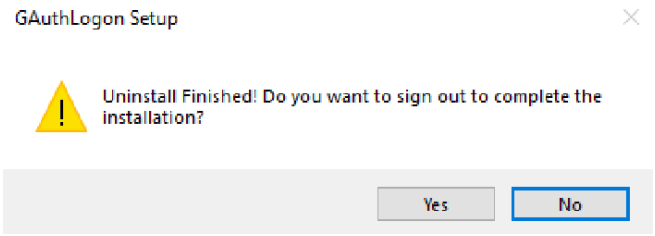
You can remove GAuthLgon in Setting or Control Panel. Select "GAuthLogon" and press [Uninstall] button



The setup program will open. Press [Uninstall].



The uninstallation will finish in a few seconds.

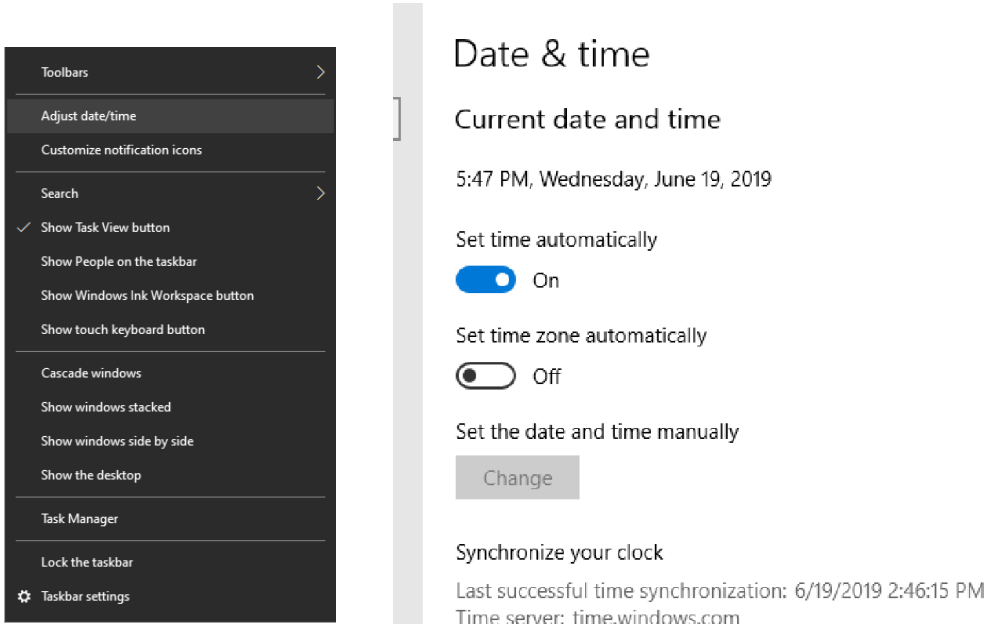


Some files still remain and you must sign out to erase them completely. If there are any other programs with unsaved data, save before signing out.

Appendix 1

An authenticator app generates one-time codes based on the device's clock time. GAuthLogon authenticates a one-time code using the PC's clock time. The clocks of both the device and the PC must have the same time for the code authentication to succeed.

iOS / Android devices with Internet connections have their clocks automatically adjusted and keeps the correct time. When Window PC is connected to Internet, set it to adjust time automatically.



A domain joined computer synchronizes with the domain controller (DC). Configure the DC to have the accurate time.

If you have a PC without Internet connection, be sure that the clock is correctly adjusted. One frequent cause of one-time code authentication failure is PC time's not being correct.