2018/3

Ver. 1.0

GAuthLogonV

Protecting VMWare VDI Windows Session

With Google Authenticator OTP

RiBiG Inc.

http://www.ribig.co.jp

Content

About GAuthLogonV

GAuthLogonV is a software solution to protect VMWare VDI Windows virtual machine session by adding an additional authentication layer before you can begin to use your Windows desktop. The authentication layer asks you to enter 6 digits one-time password(OTP) to be generated by the time-based one-time password algorithm defined in RFC 6238. Unless you enter a valid OTP, Windows login session will not be available for you to use.

GAuthLogonV is not a credential provider (CP) that signs you in to Windows. You can log in to Windows with any one of CPs available such as username/password, smartcard, face, finger-print authentications. Once you are logged in to Windows, GAuthhLogonV will lock the screen that prompts for OTP entry. The screen will be unlocked with a successful entry of OTP.

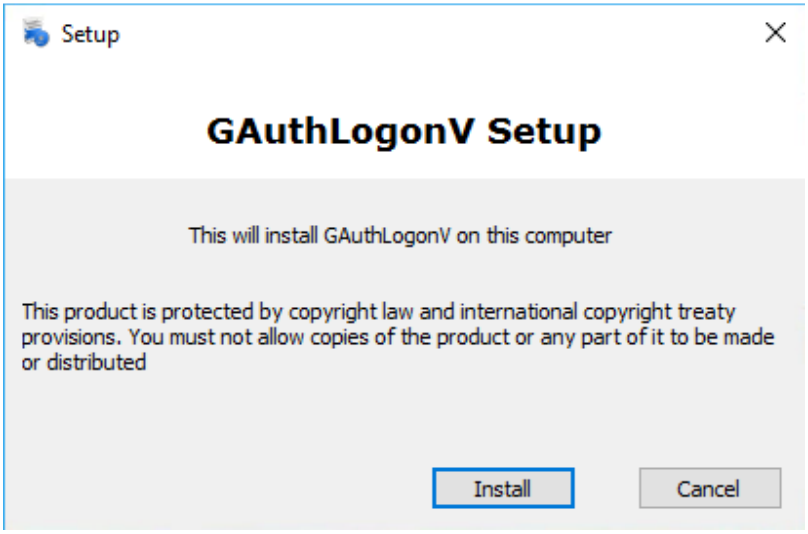
GAuthLogonV is designed for use with VMWare VDI Windows virtual machines. Under VMWare VDI, you authenticate to a connection server with a domain credential, not directly to a virtual machine. Once authenticated to a connection server, the single sign-on mechanism will automatically log you in to a virtual machine. CPs are disabled for the single sign-on to work. GAuthhLogonV comes to work immediately after you are logged in and to prevent you from using your desktop without a valid OTP entry.

GAuthLogonV may be installed on AWS WorkSpace machines. For GAuthLogonV to work, you must sign out each time you finish using a virtual machine. If you just disconnect your client, GAuthLogonV will not lock your session next time you connect to the virtual machine. This is because there is no way for GAuthLogonV on WorkSpace virtual machine to detect a client disconnection or connection. In WorkSpace documents, it says that WorkSpace machines on a domain network

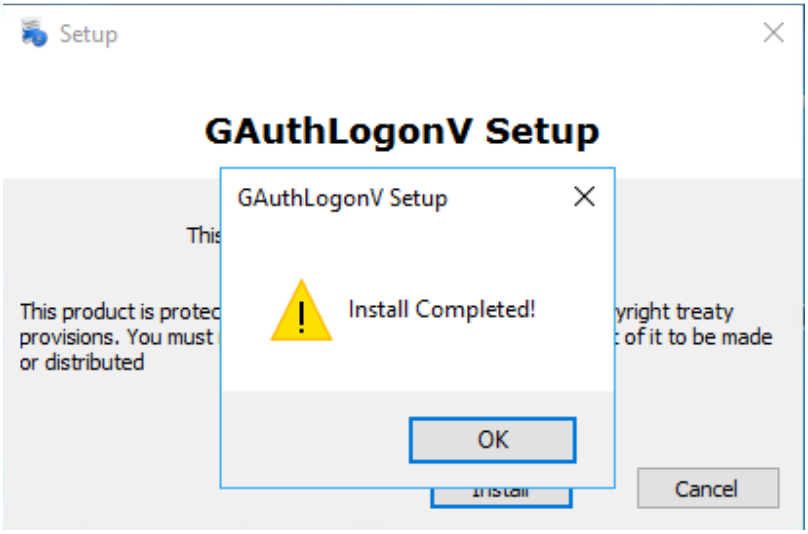
may automatically sign you out when you disconnect the client when a domain policy setting is applied.

1. Installation

To install GAuthLogonV, run Setup.exe in the distribution files.



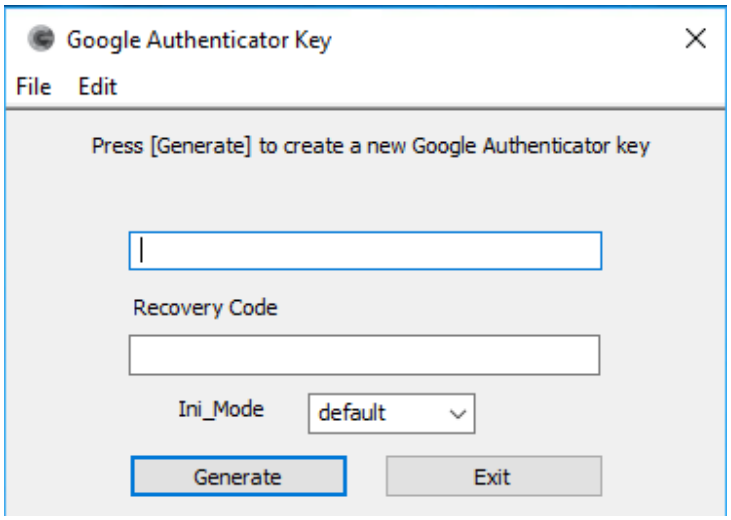
Click on [Install] button to start the installation. It will complete in a few seconds



GAuthLogon Installation Folder:

32bit Windows	%ProgramFiles%\RiBiG\GAuthLogonV
64bit Windows	%Program Files% (x86)\RiBiG\ GAuthLogonV

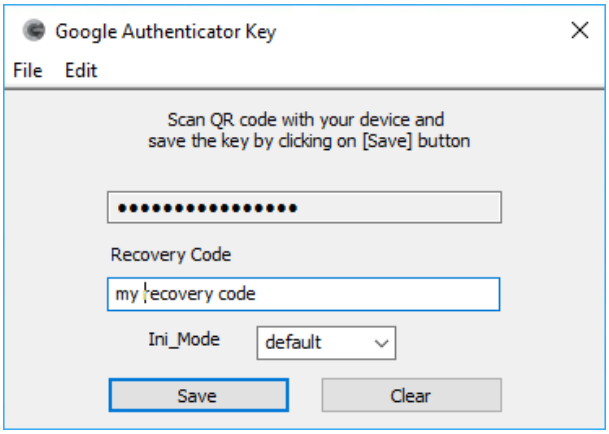
After the installation is complete, another program is run to configure your authentication device to protect the current user's session. It is not mandatory to configure your device at this time. You can exit the program if you choose to configure it later.



How to configure:

1. Click on [Generate] button

2. A window with QR code will be shown. The label below the QR code will be displayed on your authentication device to identify the OTP. Edit the string to be unique enough to distinguish it from the other.
3. Click on [Redraw] button. This will encode the new label in QR code
4. Scan the redrawn QR code
5. Close the window with QR code



6. Enter Recovery code. This must be at least 32 digits long. You can use this recovery code once instead of OTP
7. Click on [Save] button
8. Close the window

Once configured, GAuthLogonV will lock the screen prompting you for 6 digits OTP entry.

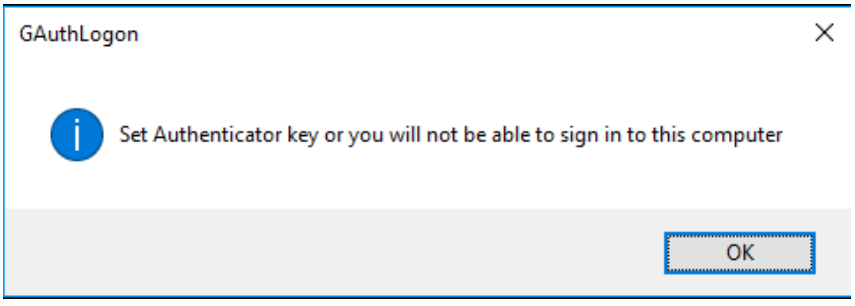
** Demo Version **

Any authenticator devices will generate the same OTP at any time for the demo version. The recovery code

”12345678901234567890123456789012”

will be automatically set. Anyone using the demo version will be able to unlock your GAuthLogonV screen

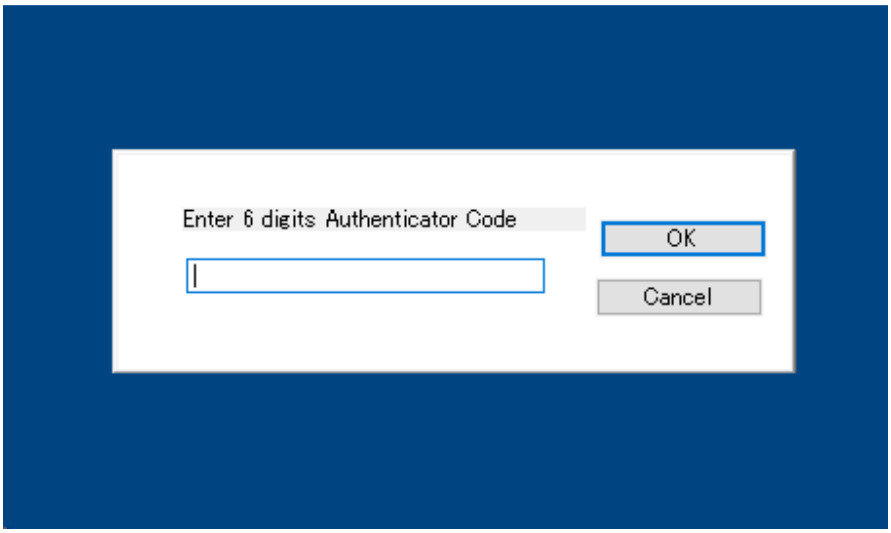
If not configured, you can log in without OTP for up to 7 sign-in/unlock. While you are permitted to sign in without OTP, GAuthLogonV will display the following window.

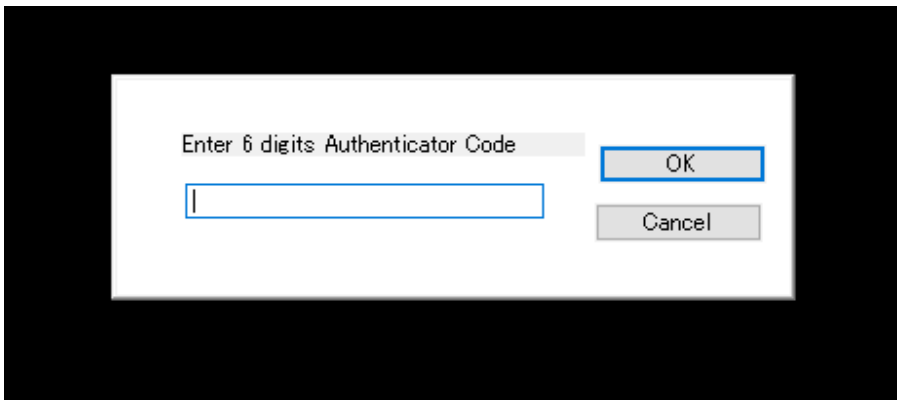


Clicking [Ok] will unlock the screen and run the configuration program. Be sure to set your authentication device before you will lose the access to your desktop.

2. Login / Unlock

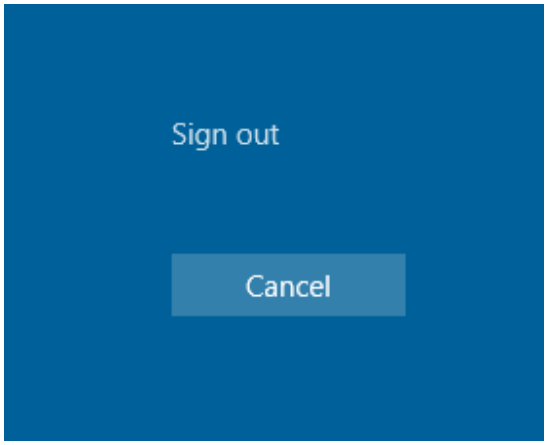
When you have configured your device, GAuthLogonV will lock the screen immediately after you are logged in. Your desktop screen may be displayed momentarily before the screen lock.





The background colors may be different in login or unlock scenarios.

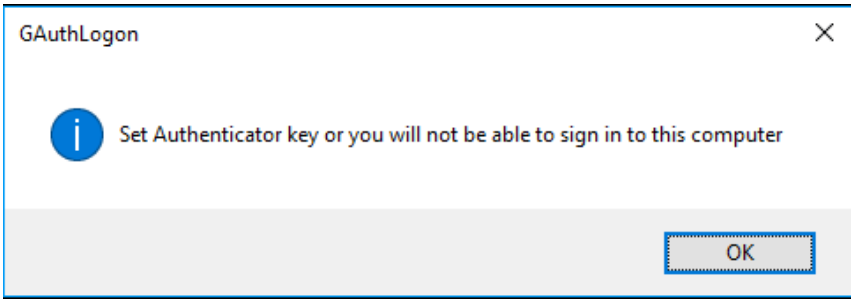
The screen may be automatically switched to the following screen in lieu of the OTP prompt.



This is due to the changes in the security setting made by GAuthLogonV. Pressing on [Cancel] button will return you to the OTP prompt screen.

To unlock he screen, enter 6 digits OTP and press [OK]. Clicking on [Cancel] button or “Sing out” link in a screen show by ALT+CTRL+DEL will sign you out.

When you have not yet configured your authentication device, you will see a warning window. Pressing [Ok] button will unlock the screen.



3. Device Configuration Program - AddToken

You can always configure or re-configure your authentication device using AddToken program.

How to run:

1. [Start] – [GAuthLogonV] – “AddToken”

2. Run AddToken.exe in GAuthLogon installation folder.

Please refer to “1. Installation” section for the detail on device configuration.

4. Optional Setting

4.1 Specifying Users who are not required of OTP Entry

You can specify users who, logged in, will not be prompted for OTP entry.

a. Create a text file named “CodeAuthExcept.user” and specify a user name, one user per line, in down-cast and UPN format.

   Down-cast: Domain\Username

   UPN: user@mydomain.com

b. Copy “CodeAuthExcept.user” to GAuthLogonV installation folder.

   File permission setting on “CodeAuthExcept.user”

   Give Read access to the file only to GAuthLogonV administrator and local “System” to hide the file from other users.

GAuthLogonV will convert the user name to SID and compare it to SID of the login user; it is not making the literal comparisons of user names.

4.2 OTP Entry Not Required on Unlock

Create a key named NoCodeAuthForUnlock under “Google Authenticator” section and set it to “TRUE” or 1 in a file named “gauthlogon.ini” in GAuthLogonV installation folder

“gauthlogon.ini” in GAuthLogonV installation folder

[Google Authenticator]

NoCodeAuthForUnlock=true

This will affect all users. This setting may be enabled on an individual base. For this, create gauthlogon.ini file in AppData\Roaming\RiBiG\GAuthLogon in a profile folder

[Google Authenticator]

NoCodeAuthForUnlock=true

4.3 Maximum Count for Login/Unlock Without OTP Entry

The default count is 7. You can change the value each for Administrative users and standard users.

Set “AdminGraceCount” and “UserGraceCount” under Google Authenticator section in the file “gauthlogon.ini” in GAuthLogonV installation folder

[Google Authenticator]

//Admin users: 3 times

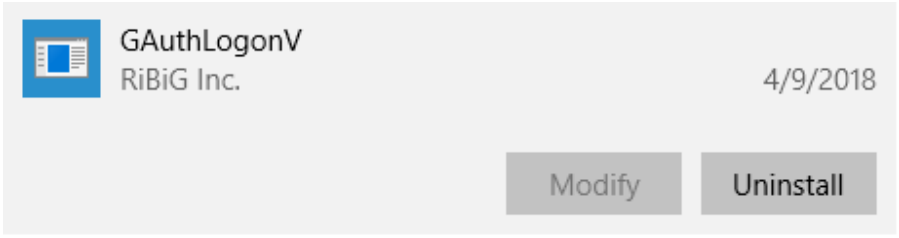
AdminGraceCount =3

//Standard user: just once

UserGraceCount=1

5. Uninstallation

You can uninstall GAuthLogonV in Setting “Apps and Features” or in Control Panel.



Select [Uninstall] button

Clicking on [Uninstall] will remove the program and sign out. You must sign out each time after you uninstall GAuthLogonV to remove it from the computer.