



GAP Access Two-Factor Authentication

Contents:

- Authentication Application Selection & Set Up**
- Application Download and Installation**
- Adding GAP Access Account to Authenticator**
- Logging in to GAP Access**
- Administration Functions**

GAP Access Two-Factor Authentication

Two-Factor Authentication, a security measure that requires both a password and a single-use verification code, is required every time a user logs in to the Gift Assistance Program (GAP) Access portal. The GAP Access portal is used for online data inquiries and submission, eligibility announcements and payment requests for Illinois Student Assistance Commission (ISAC) programs.

Two Factors:

1. GAP Access User ID and Password
2. Single-use verification code obtained through an authentication application (unique code generated for each login)

Authentication Applications

The single-use verification code required for GAP Access login is obtained through an authentication application. ISAC recommends one of the following free applications that can be used. ISAC does not endorse or recommend one product over another.

1. Google Authenticator
2. Microsoft Authenticator
3. Authy Authenticator

Colleges may choose to use an authentication application other than those options listed above, as long as the application is compatible with GAP Access. Please note that the application used by the U. S. Department of Education **is not** a compatible option. Contact a School Services Representative to confirm whether an alternative application is compatible.

Authentication Application Selection & Set Up

Log in to the GAP Access portal using your GAP Access User ID and Password.

Select the two-factor authentication application you have opted to use.

The screenshot shows the 'Two-Factor Authentication Setup' page in the GAP ACCESS portal. At the top left is the 'GAP ACCESS ISAC Gift Assistance Programs' logo. At the top right is the text 'JB Pritzker, Governor, State of Illinois'. Below the header is a 'User Login' section. The main content area is titled 'Two-Factor Authentication Setup' and contains three tabs: 'Options', 'Install', and 'Verify'. The 'Options' tab is active. Underneath, the heading 'Authenticator App Options' is followed by a paragraph: 'Two-factor authentication is necessary to make your account truly secure. To access your GAP account you must choose one of the following authentication apps to download and install on your Android or iPhone device:'. Below this are three radio button options: 'Authy Authenticator' (with a red icon), 'Microsoft Authenticator' (with a blue icon), and 'Google Authenticator' (with a grey icon). The 'Google Authenticator' option is selected. A 'Next' button with a right-pointing arrow is located to the right of the options. At the bottom of the page is a navigation bar with links for 'Contact ISAC', 'FAAs', 'MAP Program', 'MTI Program', 'ING Program', and 'IVG Program'.

Application Download and Installation

Clicking on the authenticator application, follow the instructions on the [Two-Factor Authentication Setup](#) screen. This process will sync the application to your GAP Access account.

If you have already downloaded the application to your device (cell phone, tablet, other), click the Next button.

The screenshot shows the 'Two-Factor Authentication Setup' screen on the GAP ACCESS website. At the top left is the 'GAP ACCESS ISAC Gift Assistance Programs' logo. At the top right is the text 'JB Pritzker, Governor, State of Illinois'. Below the logo is a 'User Login' header. The main content area is titled 'Two-Factor Authentication Setup' and features three buttons: 'Options', 'Install' (which is highlighted in a darker blue), and 'Verify'. Below these buttons is the section 'Download + Install App' with the following text: 'If you're using an **Android** device, find the Google Authenticator on the **Google Play** app and install it. If you have an **Apple iOS** device, use the **App Store**. Once you have the Google Authenticator installed, return to this screen and click the "Next" button below.' At the bottom of this section are 'Back' and 'Next' buttons. The footer contains a navigation bar with links for 'Contact ISAC', 'FAAs', 'MAP Program', 'MTI Program', 'ING Program', and 'IVG Program'.

Adding GAP Access Account to Authenticator

Following the instructions on the screen, open the application on your device. If your device has a camera option, point the camera at the QR code on the screen or, instead, the code that is provided under the QR code box may be manually entered.

GAP ACCESS
ISAC QR Assistance Program

JD Pritzker, Governor,
State of Illinois

User Login

Two-Factor Authentication Setup

Options **Install** **Verify**

Add GAP Account to Authenticator

Open the Google Authenticator app on your device, click the "+" button at the bottom of the screen, and point the camera at the QR code below or manually enter the key code provided.



Manual Key Code: EU72BD63HPSATWMN

Enter the Verification code displayed in your Google authenticator app.

Contact ISAC FAAs MAP Program MTI Program ING Program IVG Program

Logging in to GAP Access

Once the QR code is submitted, a 6-digit verification code will be sent to your application. This code expires very quickly. You will need to enter the verification code on the [Two Factor Authentication Setup](#) screen. When you click Submit, you are officially logged into your GAP Access account.

After the GAP Access account has been added to the authentication application on the selected device, a new verification code must be obtained from the authentication application and entered at the time of every login.

The screenshot displays the 'Two-Factor Authentication Setup' page on the GAP ACCESS website. At the top, there is a navigation bar with the 'GAP ACCESS' logo and the text 'ISAC QR Assistance Program' on the left, and 'JB Pritzker, Governor, State of Illinois' on the right. Below the navigation bar is a 'User Login' header. The main content area is titled 'Two-Factor Authentication Setup' and features three tabs: 'Options', 'Install', and 'Verify'. Under the 'Install' tab, there is a section titled 'Add GAP Account to Authenticator' with instructions: 'Open the Google Authenticator app on your device, click the "+" button at the bottom of the screen, and point the camera at the QR code below or manually enter the key code provided.' A QR code is displayed in the center, with the 'Manual Key Code: EU72BD63HPSATWMN' listed below it. A red rectangular box highlights the input field for the verification code, which contains the text 'Enter the Verification code displayed in your Google authenticator app.', and a 'Submit' button. A 'Back' button is located in the bottom left corner. The footer contains links for 'Contact ISAC', 'FAAs', 'MAP Program', 'MTI Program', 'ING Program', and 'IVG Program'.

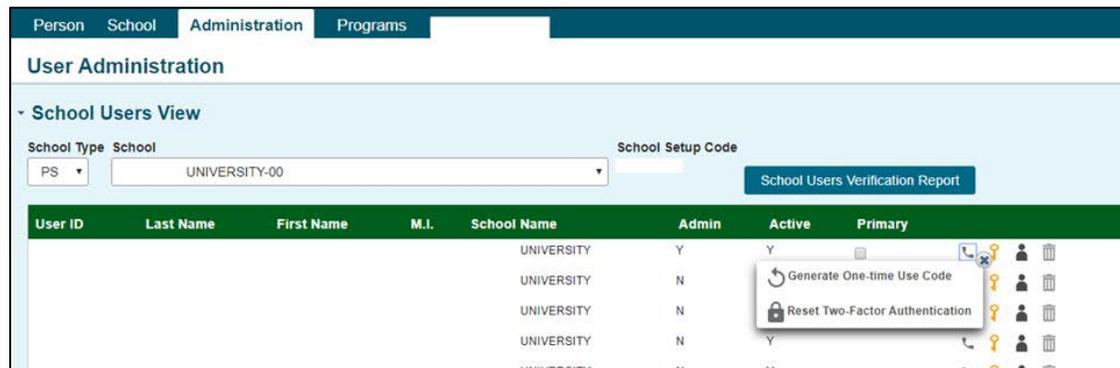
Administration Functions

A phone icon appears on the [Administration – School Users View](#) screen.

School Name	Admin	Active	Primary	
UNIVERSITY	N	Y		   
UNIVERSITY	N	C		   
UNIVERSITY	Y	Y	<input type="checkbox"/>	   

The icon has two options:

- **Generate One-time Use Code** - If a user does not have access to the application, they can notify their school administrator or School Services to request an authenticator code be sent to their e-mail. This code can only be used one time. A new code would need to be requested if the user needs to login again later.
- **Reset Two Factor Authentication** – If a user changes to a new device (cell phone, tablet, other) or has decided to use a different application after the initial setup, the existing account will require a school administrator or ISAC to “Reset the Two-Factor Authentication” QR Code that is stored in the user profile in GAP Access. Once the QR code has been reset, the user will be able to re-register the account in GAP Access.



The screenshot shows the 'Administration' tab selected in the top navigation bar. Below it, the 'User Administration' section is visible, with a sub-section for 'School Users View'. The 'School Type' is set to 'PS' and the 'School' is 'UNIVERSITY-00'. A 'School Setup Code' field is also present. A 'School Users Verification Report' button is located to the right of the table. The table has columns for 'User ID', 'Last Name', 'First Name', 'M.I.', 'School Name', 'Admin', 'Active', and 'Primary'. A context menu is open over one of the rows, showing two options: 'Generate One-time Use Code' and 'Reset Two-Factor Authentication'.