Multi-factor Authentication (MFA) for GAMMIS

Frequently Asked Questions (FAQs)

Table of Contents

MFA (Multi-factor Authentication) for GAMMIS

Frequently Asked Questions

1. **What is MFA as it applies to the Georgia Medicaid Management Information System (GAMMIS)?**
   Currently you need only a user ID and password to log into GAMMIS.

   After MFA is activated for your user ID, whenever you log in, you will also need to use an authenticator application on an Android, iOS device or on your computer. It will give you a 6-digit code that you need to enter into GAMMIS to verify that it really is you trying to log in.

2. **What do you mean by an authenticator app?**
   An authenticator app is an application found in the Google Play Store, the Apple App Store, or the Microsoft Store. It's written by a third party such as Google, Microsoft, or Twilio.

   The GAMMIS MFA is designed to make it as flexible as possible for you to choose an authenticator app. If you already use an authenticator app, there's a good chance it also will work for GAMMIS.

   You should make certain that your authenticator app is from a secure source, and that you are downloading the genuine software and not a counterfeit.

3. **Which apps does GAMMIS MFA work with?**
   GAMMIS MFA will work with any authenticator app that supports the time-based one-time passcode (TOTP) algorithm.

   That means it will work with popular authenticator apps like Google Authenticator, Microsoft Authenticator, Twilio Authy, Duo Mobile, and Okta Verify.

   Warning: Not all authenticator apps are free to use, so be sure to read the details about the app before you install it.

4. **Must I install an authenticator app on my smart phone?**
   No, you can choose an authenticator app that works on a different device: a Windows PC, a MacBook, or a tablet. Most people keep their smart phones close by, so they find it more convenient to use a smart phone; however, the choice is up to you. We recommend that you plan this step **before** the MFA rollout begins.

5. **Do I need to take any precautions with a smart phone or tablet where I install my authenticator app?**
   Yes, if you install it on a smart phone or tablet:

   - Make certain the device requires a log-in or fingerprint or face recognition. You don't want anyone who happens to pick up that device to be able to start your authenticator app.
   - Don't install any apps of any kind on the same device you use for your GAMMIS authenticator app unless you know the apps are from a reputable organization. You don't want any malware or spyware running on that device.
   - Never give any app on your device more permissions than it needs to do its job. If it refuses to run without those permissions, then don't trust it.

6. **Do I need to take any precautions with a computer where I install my authenticator app?**
   Yes, if you install it on a computer:

   - Make certain the computer requires a password, PIN, or fingerprint in order to log in.
   - Set up the computer to automatically apply the latest operating systems updates from Microsoft or Apple
   - Run anti-virus software on it that automatically keeps your virus signatures up to date.
   - Don't install software on the same computer unless you know it's from a reputable organization.

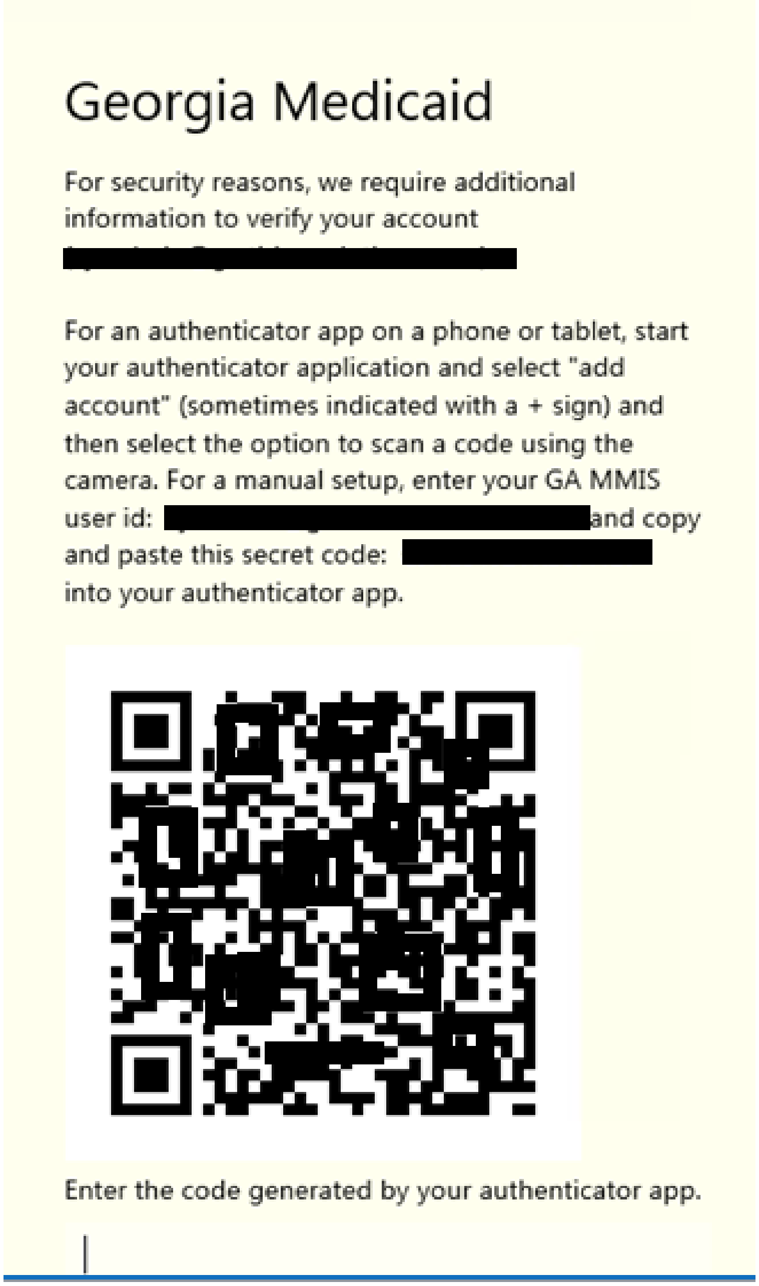
7. **When will MFA be rolled out?**
   Starting the evening of November 29, 2022, all **newly created GAMMIS user IDs** will be required to set up MFA when they are created.

   We will turn on the MFA requirement gradually for existing user IDs starting the week of November 29, 2022 and ending February 28, 2023.

8. **Do you have a schedule for when MFA will be required for my user ID?**
Below is a chart of when we expect MFA to be activated, based on the first letter of the last name on the user account, as of November 28, 2022. This chart may change as the rollout proceeds, so be sure to check the latest version of this FAQ document.

Week of	**Last Name Field on Accounts Beginning With**
11/29/2022	A-B
12/4/2022	B-C
12/11/2022	C-F
12/18/2022	<Holidays>
12/25/2022	<Holidays>
1/3/2023	F-G
1/8/2023	G-J
1/17/2023	J-L
1/22/2023	L-N
1/29/2023	N-R
2/5/2023	R-S
2/12/2023	S-W
2/19/2023-2/28/2023	W-Z
3/1/2023	All provider accounts will be required to use MFA

9. **How will I know it's time to set up MFA for my GAMMIS user ID?**
When you try to log into GAMMIS, a new screen will appear asking you to set up MFA on your authenticator application.



Georgia Medicaid

For security reasons, we require additional information to verify your account [redacted]

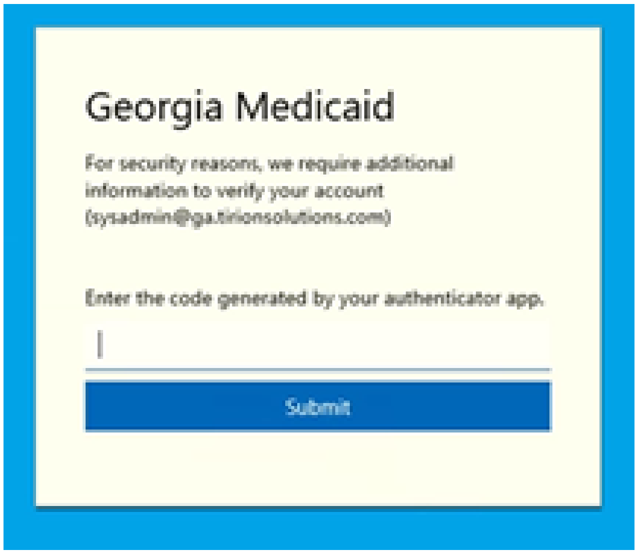
For an authenticator app on a phone or tablet, start your authenticator application and select "add account" (sometimes indicated with a + sign) and then select the option to scan a code using the camera. For a manual setup, enter your GA MMIS user id: [redacted] and copy and paste this secret code: [redacted] into your authenticator app.

Enter the code generated by your authenticator app.

WARNING: Take care when this code is being displayed on your computer. Do not print it out or save a picture of it.

Note: We recommend that you select an authenticator application and install it on your device **before** the MFA rollout.

10. **Must I set this up on my phone, computer, or tablet every time I log in?**
No, the set up only needs to happen once. After that, whenever you log in, after you enter your user ID and password, you will be prompted to enter a 6-digit code that you will receive from your authenticator app.



Georgia Medicaid

For security reasons, we require additional information to verify your account (sysadmin@ga.tirionsolutions.com)

Enter the code generated by your authenticator app.

11. **My authenticator app allows me to send the 6-digit MFA codes to my phone in a text message. Is there an issue with using this for GAMMIS MFA?**
Current federal guidance does not recommend the use of text messages (SMS) as an MFA method because they are not secure.

12. **I use my GAMMIS user ID to work on behalf of several providers. Will I have to re-enter my authenticator code every time I switch providers?**
No, you will only need to enter the MFA code when you first log in. You won’t need to enter it again unless you log out or close all your browser windows.

13. **I have a different user ID for each provider, must I have a different MFA code for each one?**
Yes, each user account must be set up with its own MFA code. There is no way to set up more than one GAMMIS user ID to use the same MFA code.

14. But it's not practical to set up hundreds of MFA accounts on a phone.   What should I do if my office staff work on behalf of many providers?

We recommend that you change your GAMMIS user IDs ***before*** the MFA rollout starts:

- Each person who will be working on behalf of any of the providers should create a Billing Agent user ID, if they don't already have one.
- Log in with each provider user ID you maintain. Delegate Super Agent permission to at least two of the office/organization administrators' user IDs.
- This will allow those Super Agents to delegate and remove permissions to the other users who work on behalf of those providers.
- Each person should have only one GAMMIS user ID. That way, each person only has to keep track of one MFA code.
- Once the Billing Agent users IDs have been created and the provider user IDs have delegated Super Agent access to at least two accounts, the provider user IDs do not need to be maintained. ***The Super Agents can perform most needed tasks.*** (If you perform this reorganization of your user IDs before the MFA rolls out, you won't even need to set up MFA for all of the provider user IDs.)

Note: Refer to the "Web Portal User Account Management Guide" found under Provider Information >> Web Portal Training (https://www.mmis.georgia.gov/portal/Default.aspx?TabName=Web%20Portal%20Training) for detailed instructions on setting up and using Billing Agent accounts with the Super Agent role.

15. If I install the authenticator app on my phone for GAMMIS and the phone becomes inoperable, can I restore it to a new phone from my phone's cloud backup?

This depends on the authenticator app. Please read the documentation for the authenticator app carefully before you decide to use it.

16. What if the phone that has the authenticator set up for GAMMIS is lost or stolen?

If you can't find your phone, contact the Gainwell Technologies Helpdesk. They will reset the MFA account associated to the GAMMIS user ID. The next time you log in, it will display a new QR code and you can set up your user ID again in an authenticator app on your new phone.

Please note that you will still need to know your password to do this. If you don't, please see below.

17. **If I forget my password, can I still use the link that lets me reset my GAMMIS password?**
    Yes, that process has not changed. Using the password reset link does not require your 6-digit MFA code; however, you cannot reset your MFA code using this link. It's only for resetting passwords.

    In case you're not familiar with the process, this is how it works: on the GAMMIS sign-on screen, there is a link "Having Trouble Logging In?" If you click it, it will ask you to submit your user ID and the email address on file for that GAMMIS user ID. It will then send an email to that email address that has a link in it. If you click the link, you then need to enter the correct answer to your security question. This will allow you to reset your password if it has not been more than 180 days since you last changed it.

    If it has been more than 180 days since you last reset your password or if your user ID has locked due to 60 days of inactivity, then you need to call the Gainwell Technologies Helpdesk. Please see the question below.

18. **What if I need a password reset but I never set up a security answer? Or what if I don't remember the security answer?**
    You will need to contact the Gainwell Technologies Helpdesk. They will send a password reset email to the email address on file in the system for that user ID. This email will not allow you to reset your MFA, however.

19. **What if my user ID has locked due to more than 60 days of inactivity?**
    You will need to contact the Gainwell Technologies Helpdesk. They will unlock your account and send a password reset email to the email address on file in the system for that user ID.

20. **What if I have forgotten my password, never set up a security answer, and I lost my phone that has the authenticator app installed and I have no backup?**
    You will need to contact the Gainwell Technologies Helpdesk and they will help you start the process of having a new GAMMIS user ID created.

21. **What if my office administrator leaves suddenly and I don’t have access to their GAMMIS user ID, and the authenticator app set up for that user ID?**
    The email address on the GAMMIS user ID must be changed, and the Georgia Technologies Helpdesk can only do this if the person calling in has the correct 6-digit MFA code for that user ID along with other pertinent information to help us verify your identity.

    If this happens, and there is no backup Super Agent user ID that’s still working, then we will need to set up a new user ID for you to use. If this is the master provider user ID, then all of the role delegations must be repeated which is a time-consuming task.

    It’s always been important for the provider user ID to delegate Super Agent permission to at least two office administrator user IDs. Now that MFA is being rolled out, it’s **essential** to avoid situations like this by having a backup in the system.