American Arbitration Association®

Multi Factor Authentication FAQ

1. What is multi-factor authentication (MFA)?

Multi-factor authentication (MFA) is a security mechanism that requires users to provide two or more credentials to verify their identity when logging into an account or service. The goal of MFA is to add an extra layer of security beyond just a username and password.

2. Why is the AAA-ICDR® requiring MFA?

Using MFA helps protect your accounts from unauthorized access even if your password is compromised. It makes it much harder for hackers or bad actors to log in as you, since they would need access to your additional factors like a one-time code sent to your phone. Enabling MFA greatly improves your account security.

3. What are the different types of MFA credentials used on the AAA-ICDR sites?

a. One-time passcodes sent via text message to your mobile device

b. An automated voice call made to the phone number registered by the user. To complete the sign-in process, the user is prompted to press # on their keypad.

c. One-time passcodes generated by an authenticator app (*e.g.* Google Authenticator, Duo Mobile, Microsoft Authenticator, Twilio Authy, Okta Verify, Entrust Identity). Note that an authenticator app is a program installed on your mobile device; it will generate a code for you to enter as a secondary authentication method when logging in to an AAA-ICDR site.

4. Why is email not included as a form of MFA credential?

Email accounts can be compromised by hackers using automated bots and therefore are not as secure as secondary authentication methods requiring a separate physical device such as a phone.

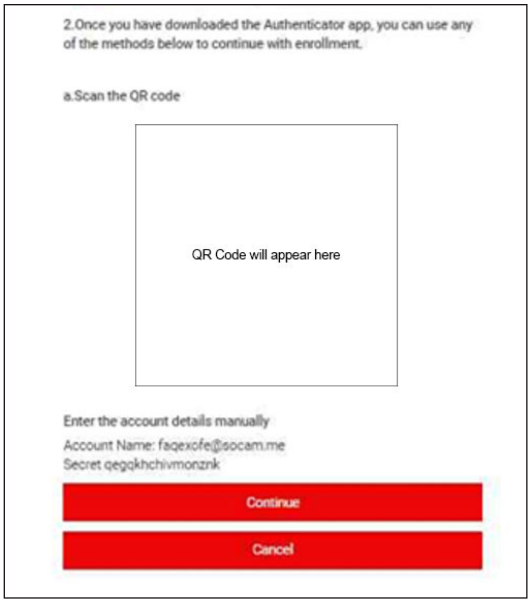
5. How do I enable MFA for my AAA WebFile®/Panelist eCenter®/AAA Mediation.org®/Consumer Clause Registry account?

- You will be prompted to register your phone number to receive text messages or phone calls.
- Or you can choose to install an authenticator app such as Google Authenticator, Duo Mobile, Microsoft Authenticator, Twilio Authy, Okta Verify or Entrust Identity. You can then generate time-limited, one-time passcodes from the authenticator app when logging in.

6. How do I set up an authenticator app?

As many authenticator apps are available for use, please refer to your preferred authenticator app directly, for their guide on usage.

After downloading the app from the App Store or the Google Play Store, you need to open the app. You will be able to add an account for AAA WebFile/Panelist eCenter authentication by using your phone to scan a QR code, as shown below.



2.Once you have downloaded the Authenticator app, you can use any of the methods below to continue with enrollment.

a.Scan the QR code

Enter the account details manually

Account Name: faqexofe@socam.me
Secret qegqkhchivmonznk

The Authenticator App setup screens will look slightly different depending on which authenticator app you are using and the type of phone you have (*e.g.* iPhone, Android).

7. If I choose to receive a phone call for MFA, what will my caller ID indicate as the source of the call?

The AAA-ICDR is using Microsoft software for MFA, so, depending on the phone carrier, the call you receive may appear on your caller ID as "Microsoft", or +1 855-330-8653, or perhaps some other number, depending on how your phone carrier routed the call from Microsoft. Regardless of how the call was routed, the message you will hear on the call is "This is Microsoft. If you are trying to sign in, please press the pound key to finish signing in."

8. Do I need to have a mobile device to enable MFA?

No, you can receive an automated voice call. To confirm the sign in, you will need to press # on the phone keypad.

9. What should I do if I don't receive the one-time passcode sent to my mobile device?

Try the below steps.

a. Restart your mobile device – Sometimes your device just needs a refresh. When you restart your device, all background processes and services are shut down and then refreshed.

b. Make sure your mobile device has notifications turned on. Ensure the following notification modes are allowed:

- Phone calls
- Your authentication app
- Your text messaging app
- Ensure these modes create an alert that is visible on your device.
- Make sure you have a device signal and Internet connection
- Turn off "Do not disturb"
- Unblock phone numbers

10. What if I lose access to my mobile device or change my phone number?

If you are logged in, you can change the MFA phone number by clicking "My Profile" and then clicking the "Multi-Factor Authentication Phone Number Update" button. If you are unable to login, please contact AAA® Customer Service at 800-778-7879 or email customerservice@adr.org for assistance in changing your MFA credentials.

11. What else do I need to know about MFA to keep my AAA WebFile/Panelist eCenter/AAA Mediation.org/ Consumer Clause Registry account secure?

In recent cyberattacks in the news, cyber criminals have compromised accounts protected with MFA by getting an unsuspecting person to complete the MFA login for the criminal. Here are a few tips to keep in mind.

- Just like you wouldn't give out your password to someone who requests it, you should never share a code you receive as part of your MFA login. The AAA-ICDR will never ask for the code in a text message, email, or phone call.
- Never act on a MFA notification if you did not initiate the request first. Cyber criminals in recent breaches have used a technique called "MFA prompt-bombing" where a MFA push is repeatedly sent to a user's legitimate device until the user approves the authentication, which they eventually did to stop the annoying and repeating notifications, which in turn allowed the bad actor to gain access to the account. If you do get a MFA notification that you did not request, don't complete the process and please notify AAA Customer Service at 800-778-7879 or email customerservice@adr.org.