FAQs

Multi-factor Authentication (MFA) Login

Q: Why is Auto/Mate Implementing MFA?
A: MFA improves security, and it is a required security feature under the Gramm-Leach-Bliley Act.

Q: What is the Gramm-Leach-Bliley Act?
A: The Gramm-Leach-Bliley Act (GLBA) is a United States federal law that applies to a variety of companies and includes many car dealerships. The Act has two separate rules. The Privacy Rule requires, among other things, covered companies to explain their information sharing practices to their customers. The Safeguards Rule includes security requirements to protect nonpublic personal information. The Federal Trade Commission added provisions to the Safeguards Rule that become effective December 9, 2022.

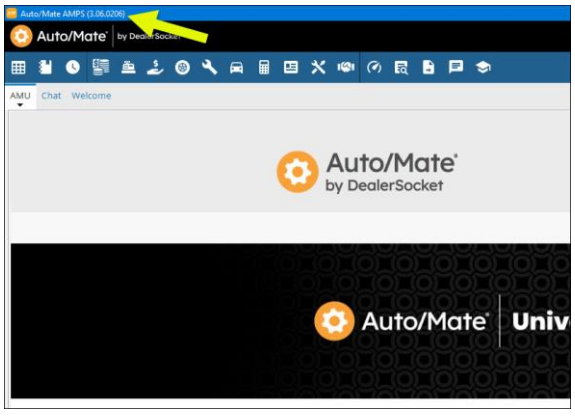
A summary of how Auto/Mate complies with the Rule can be found here.

Additional information regarding Auto/Mate's privacy practices can be found by accessing our Privacy Policy.

Q: What if my dealership doesn't want to participate in this change?
A: All Auto/Mate users will need to participate as MFA has been adopted to increase the security of data available in our product.

Q: When will I be required to start using the Multi Factor Authentication login?
A: The software release containing MFA login will start rolling out to dealers starting on November 7th, 2022, as an AMPS update. The release will be introduced gradually to a group of dealers each night until all dealer customers receive the update.

Q: How will I know when I have received this update?
A: You will receive a pop up when your server is updated asking you to download the update. On the top left of your Auto/Mate screen it will say Auto/Mate AMPS (3.6.0210) after the update



Q: What do I need to do before I get this update?
A: Please do the following:

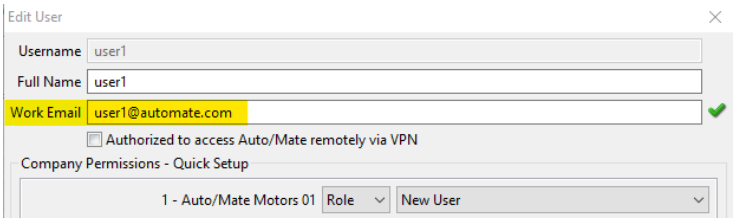
- Make sure all users that login to Auto/Mate have a working email setup in System Utilities (i.e., that there are no active users with email missing).
- Make sure there aren't any duplicate emails in system utilities on multiple users.
- Make sure all users can receive text messages install the Authenticator App on their cell phone to be able to setup the authentication for MFA-based login.
- Check to see who your system administrator is in case you have any issues logging in after this update and need to verify your email. You can see who your system administrators are by clicking on the shield icon on the top right of your screen.

Q: Are users that only use Time/Mate to clock-in required to login using MFA?
A: No, users that only use Time/Mate for clocking-in are not required to login using MFA-based login process. They will not be required to perform additional authentication during the login.

Q: How do I add email for users that currently don't have it?
A: System Admin can add any missing emails by following these steps:

- Go to System Utilities
- Highlight the user that is missing the email
- Select Edit user on the bottom left and add the user email

This change can only be done by System Admins.



Q: What will happen after I receive this update?
A: Once the update is received, all users will be requested to Authenticate their username upon login. For more details on how this will work, please see the user instructions document.

Any users that receive the following error message during login process: "Email is missing, please contact your admin to verify" during the first attempt to login, will need to check with their system administrator to add an active email to their user record in system utilities.

Q: If I login to two servers through one login how will this affect me?
A: You will be asked to Authenticate only once based on your default server. It will act the same as if you are logging into a single server and you will still have access to both servers.

Q: What if my employee doesn't have a cell phone?
A: If an employee does not have a cell phone or prefers not using it for authentication, they have an option of using tablet or PC (laptop or desktop) devices for that purpose. To use those devices, they will be required to select the authenticator app as an authentication method during the MFA setup process. For more details on how to setup authenticator app method for authentication, please refer to user instructions document. Setting up authenticator app on PC devices is described in detail in the FAQ section of that document.

Q: Can more than one person use the same device to authenticate their login?
A: Multiple users can use the same device, but each user will be required to pass authentication during login.

Q: How can a user avoid providing their cell phone number to be used in authentication if they don't want to share it?
A: Utilizing authenticator app does not require the user to provide their cell phone number.

Q: Can an email be used for authentication in MFA-based login?
A: No, email cannot be used for authentication. Only cell phone text messaging (SMS) or authenticator app can be used for authentication.