Multifamily Multifactor Authentication (MFA) - Frequently Asked Questions (FAQs)

Multifactor Authentication (MFA)

Q1:   What is MFA?

Multifactor Authentication (MFA) refers to an additional layer of security that is added to the login process when accessing a tool. It increases security by requiring you to use both something you know (e.g., your username and password) and something you have (e.g., email address, mobile phone number) when you log into our user interface. This makes it more difficult for an unauthorized person to access your account.

Q2:   What tools and systems will be protected with MFA?

All external facing Freddie Mac technology tools accessed via a user interface that require users to log in and authenticate are protected with MFA.

Q3:   Does MFA apply to system-to-system (S2S) accounts?

No, MFA does not apply to S2S accounts.

Q4:   What if our organization uses RPA, or bots, with a human user account to access Freddie Mac tools?

A robotic process automation (RPA), also known as a "bot," refers to functions that have been programmed to perform repetitive activities without human interaction. Some RPAs include automated steps to log into an account with user credentials to perform the functions a human would normally execute. If your organization uses RPAs to log into Freddie Mac tools, your process may require additional programming to accommodate MFA.

While MFA doesn't need to be applied to bot accounts currently, we continue to review our policies and may later determine whether MFA will be extended to bot accounts. Prior to making the change to have MFA extended to bot accounts, we will provide advance notice and details to allow sufficient time for development, testing and adoption.

Q5:   Will MFA make my sign-on experience more difficult?

No, MFA will add one additional step to your sign-on process and will be quick and easy. The experience should be a familiar process that you may already be using for other online accounts to increase security.

Q6:   How often do I have to re-authenticate?

You'll need to re-authenticate and complete your MFA verification every 24 hours on each trusted device (computer or phone) and each browser you use (e.g., Google Chrome, Microsoft Edge or Mozilla Firefox). You'll also need to re-authenticate whenever you clear your cache.

Q7:   Where do I find more information on getting started with MFA?

June 2024

For additional information about MFA as well as setup requirements and guidelines, refer to the MFA user guide.

Q8: What are my authentication options?

The following table describes the methods currently available for MFAs. Starting June 30, 2024, the only supported MFA methods will be email address and PingID® Mobile.

Verification Method	Description
Email Address	A six-digit, one-time passcode notification is sent to the email address on your user profile that you will enter to complete the authentication process.
Text Message*	A text message with a six-digit, one-time passcode is sent to your mobile device that you will enter to complete the authentication process.
Phone Calls*	A call is placed to the phone number provided and the six-digit, one-time passcode will be verbally communicated for you. Enter this code to complete the authentication process.
PingID**	The PingID mobile application is a user-friendly solution designed to improve the security of logins and verify an end user's identity through multifactor authentication.

*Effective June 30, 2024, this option will no longer be supported.
**Starting June 30, 2024, this will be a newly available option.

Q9: How many devices should I register?

It is highly recommended that you enable a secondary authentication method in the event your primary device is not available at the time you are attempting to access a Freddie Mac tool.

Q10: Can I use my personal device for MFA?

Freddie Mac allows the use of your personal devices for MFA. You are responsible for ensuring that any such use complies with your employer's policies, procedures and requirements.

Q11: How do I change or update my authentication method?

You can make changes to your authentication settings for each registered device by visiting the MFA Management portal. For instructions, please refer to the MFA user guide.

Q12: What if I do not receive a security passcode to the cell phone number in my profile?

Please request that the one-time passcode be resent. If you still encounter issues, please contact the Multifamily Service Desk by phone at 866-MULTIFM (866-685-8436) or send an email to the Multifamily Service Desk.

Q13: What if I do not receive emails with a security passcode?

Please check your junk or quarantine folders within your mailbox. If you encounter issues receiving emails during the registration process, you can click "Cancel" to exit the email registration, close your browser, and then log back into the application and elect to register SMS and/or Voice.

If you encounter issues receiving emails after the registration process is complete, you can elect to "Change Method" and select another method to send the security passcode (OTP). You may need to speak with your IT staff to determine if they are able to allow emails from NoReplyMFA@freddiemac.com. If these methods do not resolve your issue, please contact the Multifamily Service Desk.

Q14: What if I experience issues with MFA?

If you encounter issues, please contact the Multifamily Service Desk.

Q15: What if I lose my MFA device?

If you forget or lose one of your MFA devices, you can use an alternative MFA method that you've established. You should also make sure to remove that method of contact from the MFA Management portal. If you encounter issues, please contact the Multifamily Service Desk.

Q16: Can I opt out of MFA?

No. Freddie Mac views MFA as an important additional layer of security. If you have concerns with how this may impact you, please contact the Multifamily Service Desk.

Q17: What is the MFA Management portal?

It's a self-service portal that allows you to manage your devices. To access the management portal, select your user icon on the top right and a drop-down list will appear. From there, select "Devices" to be directed to your Manage Devices page where you can add, delete and change your primary or secondary MFA device.

Q18: I registered PingID mobile application device through the management portal. Why can't I use it for authenticating?

PingID mobile application for authenticating into Freddie Mac tools will not begin until June 30, 2024.

June 2024