

Multi-Factor Authentication (MFA) – Frequently Asked Questions

What is Multi-Factor Authentication?

Multi-Factor Authentication (MFA) is a security measure that requires two or more methods of verification during the login process—typically your password and a one-time code generated by an authentication app.

Why is MFA being implemented?

MFA is being introduced to comply with New York State Law 23 NYCRR Part 500, which establishes industry-wide cybersecurity requirements. This regulation applies to all organizations operating in New York and supports broader efforts to strengthen digital security in the insurance and financial services sectors.

Who will be affected?

All users, including portal users, will be prompted to set up MFA when logging in.

What authentication methods are supported?

At this time, only Google Authenticator, Microsoft Authenticator and Authy Apps are supported.

How do I set up MFA (Multi-Factor Authentication)?

You'll be guided through the setup process after entering your username and password. Follow these steps:

Google Authenticator

1. Download **Google Authenticator** app on your mobile device.
2. Scan the **QR code** displayed on the login screen.
3. Enter the **six-digit code** from the Google Authenticator app.

Microsoft Authenticator

1. Download **Microsoft Authenticator** app on your mobile device.
2. Open the app and tap +, then choose **Work or school account**.
3. Scan the **QR code** displayed on the login screen.
4. The account will auto-add and begin showing a **six-digit verification code**.

Authy

1. Install the **Authy Authenticator** app on your mobile device.
2. Open the app and choose **Add Account**.
3. Select the option to **scan a QR code**, then scan the code on your computer screen.
4. Authy will automatically start generating verification codes.
5. Enter the **first code** when prompted to complete the setup.

What if I lose access to my authenticator app or device?

If you lose access to your device or app, you have several recovery options:

- You can use your **recovery email** and **security question** to receive a one-time code by email.
- **Company admins** can reset your MFA settings, allowing you to reconfigure MFA from scratch.
- If you've connected Google Authenticator to your **Google account**, your authentication setup will transfer to a new device.
(See Google's guide for details.)

New MFA Reset Permissions

Company Admins can reset an employee's MFA setup by navigating to:

Settings > System Setup > Employees

Select the employee, click **Reset MFA**, and confirm the action. A success notification will confirm the reset.

In addition, there are **three new permissions** available for admins to enable, allowing designated employees to reset MFA for various portal users. These permissions are **not enabled by default** and can be assigned as needed.

Where can I get help setting up MFA?

If you need assistance, please contact our Technical Support team at:

servicesoftwaresupport@verisk.com