# Logging In and Password Security

05/19/2026 9:33 am CDT

## First-Time Login Instructions

When someone creates a user account for you in service**minder**, you should get an email prompting you to set your password. If that email does not come through to your inbox right away, you can follow these steps:

1. Navigate to serviceminder.com.
2. Click **Log In** at the top right.
3. Enter your email address and click **Forgot Password**.
4. Follow the link in the password reset email to create your password.
5. Once your password is set, return to the login page and sign in with your email and new password.

If you do not receive a reset email or experience issues logging in, contact your Owner or Brand Administrator. You can also submit a support ticket

---

## Each User Should Have Their Own Login

Each user should log in with their own unique credentials. Sharing logins can cause several issues, including:

- **Loss of Accountability**: Activities such as creating contacts or scheduling appointments are logged under the user's name. If multiple people share a login, there's no way to identify who completed which action.
- **Audit and Permissions Management**: service**minder** tracks user actions for reporting, troubleshooting, and administrative review. Shared logins compromise this tracking and limit your ability to assign role-based access and restrictions.

**Please do not share credentials.** If a new user needs access, create a dedicated account for them under **Control Panel > Users.**

---

## Ongoing Password Requirements

For security and PCI compliance, service**minder** requires users to update their passwords every 90 days, unless you have Multi-Factor Authentication (MFA) enabled. You'll receive in-app reminders when your password is nearing expiration.

If you forget your password, use the **Forgot Password** option on the login screen.

Your account may be locked due to multiple failed login attempts, if that happens please reach out to your Owner

or Brand Administrator for assistance.

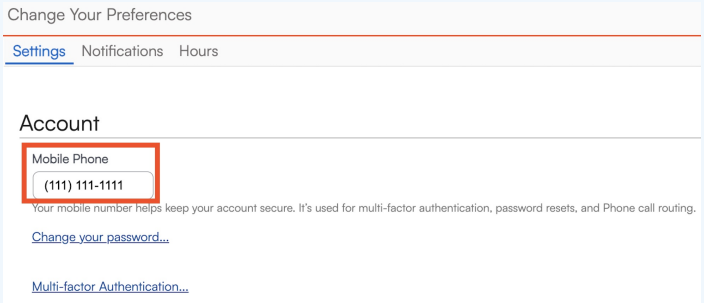
---

# Multi-Factor Authentication (MFA) Settings

Multi-Factor Authentication (MFA) provides an added layer of security by requiring users to verify their identity with a code in addition to their password.

- **Required MFA:** Users must complete MFA every time they log in. By default, codes are sent by text or email. If the user has set up an authenticator app, codes will come from the app instead. MFA cannot be bypassed when required.
- **Enabled MFA:** This indicates a user has successfully linked an authenticator app and opted themselves in to MFA. If the user loses access to the app, an admin can uncheck "Enabled" to reset MFA. This forces the system to fall back to text/email codes until the app is re-enrolled.

If you want to receive MFA codes via text message, make sure to **enter your mobile phone number** on your user preferences page, accessed via the **gear icon** in the top right corner of the website.




Typically, your password will expire and must be changed every 90 days. If MFA is enabled for your user account, your password will not expire.

## Setting Up a Multi-Factor Authentication App (Web)

1. Go to **User Preferences**.
2. Select **Multi-Factor Authentication Setup**.
3. Scan the QR code (or manually enter the code) into your authenticator app.
4. Enter the 6-digit validation code to complete setup.

## Login Experience (Web & Mobile)

1. Enter your email and password as normal.

2. Enter the 6-digit code from your authenticator app (or from text/email if fallback is in use).
    - If the code is incorrect, you'll see the error: *"Incorrect code. Regenerate and try again."*
    - If correct, you'll be logged in automatically.

MFA setup on web carries over to mobile. If MFA is active, you'll be prompted to enter your code when logging in on either platform.

---

# FAQs

**Why am I not receiving a password reset email?**

This could be happening for a few reasons:

- The email is going to your junk or promotional folder. Check all folders in your inbox.
- An email from our system to your email address bounced, preventing further email delivery. Check with a Brand Administrator to get the bounce cleared.
- Your user account in service**minder** has been marked as **Inactive**, preventing further logins. Check with your Owner or Brand Administrator to review your account status.

---