Setting up your Account

Registering as a User

> The User Registration Process outlines how new parkers create an account to access the user portal, purchase permits, and manage their vehicles. Its primary purpose is to capture essential user data while offering organizations flexible onboarding through either immediate access or email validation workflows. This article is intended for OPSCOM administrators to help them understand and support the end-user registration experience.

Setup and Configuration

Administrators can dictate how users access the system upon initial sign-up by configuring one of two primary registration workflows:

- **Auto Login:** Users are automatically logged in immediately after signing up, without requiring them to verify their account or email address first.
- **Email Verification Required:** Users are barred from logging in until they have successfully received an email, clicked the validation link, and created their password.

Admin Side: Ensure your portal settings are configured to your organization's preferred registration method (Auto Login vs. Email Verification).

User Side: Users will initiate the setup process directly from the main portal login page.

Using this Feature

Administrators can use the following workflow to guide new users through the portal registration process or troubleshoot onboarding issues.

Step-by-Step Instructions

1. Choose the preferred language and click **Continue**.
2. Click the **Create Account** button located on the login page.
3. Complete the initial profile registration questions.
4. Click the **Create Account** button to submit the details.
5. Review the on-screen prompt, which varies based on the system configuration:
   - If Auto Login is enabled, the user is automatically logged in, directed to their user profile page, and shown a green message prompting them to check their email for an activation link.
   - If Email Verification is required, the user is not logged in and is shown a message indicating that an email has been sent for validation.
6. Check the associated email inbox and locate the activation email from OPSCOM.
7. Click the **Create Password** link within the email.
8. Enter a new password into the provided fields and click **Confirm** to save the credentials to the system.
9. Log in to the account using the newly created password (if redirected to the login page).
10. Fill out any missing or mandatory details on the user profile page.
11. Click the **Save Changes** button to lock in the profile information and gain full access to the portal.

> If Auto Login is enabled, clicking the **Create Password** link in the email simply allows the user to establish a permanent password for future sessions, as they are already temporarily logged in. If Email Verification is required, clicking this link is a mandatory step to gain any access to the system.

Best Practices and Considerations

- **Mandate profile completion: Users must finish completing their profile before they can explore other features of the portal.** Administrators should communicate this requirement clearly, as users cannot purchase permits or appeal violations until their mandatory profile fields are saved.
- **Determine the best workflow for your operations: Organizations should establish a clear business rule regarding portal security.** Use Auto Login to reduce onboarding friction for new users, or use Email Verification Required to prevent spam accounts and ensure all registered email addresses are accurate and deliverable.
- **Provide support contacts:** Ensure your parking office contact information is easily accessible on the portal login page in case users fail to receive their activation emails or encounter errors during the password creation step.

Multi-Factor Authentication - User Portal

> The User Portal Multi-Factor Authentication (MFA) feature adds an essential layer of security to user accounts by requiring a One-Time Password (OTP) during the login process. Its primary purpose is to protect sensitive user data and ensure that only authorized individuals can access the parking portal. This article is intended for OPS-COM administrators to help them understand the user MFA workflow and support their clients.

Setup and Configuration

This feature requires the organization to have MFA support enabled on their system. Once available, the configuration is primarily handled on the User Side, where individual users opt-in and manage their own security settings.

Admin Side: Ensure that your system's email templates are properly configured, as the OTP emails will utilize the standard system email formatting designated for your account.

Using this Feature

Administrators can use the following instructions to guide users through enabling MFA on their accounts and logging in with One-Time Passwords.

Enabling Multi Factor Authentication

1. Log in to the User Portal and click your name in the top corner of the screen.

2. Click **Security** from the drop-down menu.
3. Scroll to the Multi-Factor Authentication section and click the **Change Multifactor Authentication Settings** button.
4. Choose **Enable One-Time Passwords** from the available settings.
5. Click the **Send One-Time Password To Email** button.
6. Navigate to your registered email inbox and copy the generated OTP.
7. Return to the portal and enter the OTP alongside your current account password in the provided fields.
8. Click the **Submit** button to confirm your changes and activate MFA.

> One-Time Passwords are only valid for 15 minutes. If the user's password expires before they enter it, they must generate a new one. Generating a new OTP automatically invalidates any previously unused passwords.

Logging In with MFA Enabled

Once MFA is successfully enabled, the standard login workflow will change to include the OTP validation step.

1. Enter your username and password on the main portal login page.
2. Check your registered email address for the automatically generated OTP.
3. Enter the OTP into the prompt on the screen.
4. Click the **Submit** button to complete the login process and access the site.

> When MFA is active, the system restricts access to the portal. Users will be forcibly redirected to the OTP entry screen if they attempt to navigate

> to any other internal pages (such as their profile or vehicle management) before submitting a valid One-Time Password.

Understanding OTP Session Settings

When guiding users through their MFA settings, administrators should be aware of how the system handles active OTP sessions:

- **Session Storage:** Once a user enters an OTP, the validation is stored in their browser's local session data. If they clear their browser's local storage or cache, they will be forced to enter a new OTP upon their next login.
- **Different Devices:** OTP session data does not persist across different browsers or hardware. If a user logs in from a new computer, a secondary mobile device, or a different web browser, they will be prompted to enter a new OTP.

Best Practices and Considerations

- **Educate users on OTP expiration: Always remind users that One-Time Passwords strictly expire after 15 minutes.** If a user complains about invalid codes, ensure they are not attempting to use an expired OTP or one that was invalidated when they clicked the send button multiple times.
- **Assist with device switching: Inform users that they will need access to their email whenever they switch devices.** Because OTPs are tied to local session storage, attempting to log in on a new phone or public computer will always trigger a new OTP request.

Manage your Account

> The User Profile Management feature allows end-users to update their personal details, addresses, and account passwords directly from the user portal. Its primary purpose is to empower users to maintain accurate account information autonomously, reducing the administrative burden on parking staff. This article is intended for OPS-COM administrators to help them understand the user experience and assist with profile troubleshooting.

Setup and Configuration

This feature is a core component of the user portal and requires no specialized setup to enable.

Admin Side: Administrators determine which profile fields are mandatory for users to complete before they can successfully save their profile and access other portal features.

User Side: Users access these management features directly from their portal dashboard upon logging in.

Using this Feature

Administrators can use the following instructions to guide users through updating their profile details, address, or password.

Editing Profile Details

1. Log in to the User Portal and click the user's name in the top left corner of the page.
2. Click **Your Profile** from the drop-down menu.
3. Modify any editable fields on the **Profile Page**. Fields that are greyed out cannot be changed by the user.
4. Click the **Save Changes** button to apply the updates.

> Users must complete all required fields determined by your organization before the system will allow them to save their changes and navigate to other areas of the portal.

Updating the Address

1. Click **Address** located below the main profile information.
2. Click **Edit** to open the address input fields.
3. Enter the updated address information into the necessary fields.
4. Click the **Save Changes** button to save the new address.

Changing the Password

1. Click **Security** located below the address section.
2. Click **Change Password** to begin.
3. Enter the current password in the **Current Password** field.
4. Enter a new password and re-enter it in the **Confirm Password** field.
5. Click the **Change Password** button to save the new security credentials.

Additional Profile Actions

Users may also have access to the following features from their profile menu, depending on your organization's configuration:

- **Payment Methods:** Allows users to store credit cards for seamless future purchases. Detailed instructions can be found on the *Manage your Payment Methods & Subscriptions* page.
- **User History:** Click **History** to view past transactions, citations, and permit records. Detailed instructions can be found on the *Viewing your History* page.
- **Forms and Documents:** Access custom forms and file uploads, if supported by the parking provider. Detailed instructions can be found on the *Using Forms on the User Portal* and *Uploading Files* pages.

Best Practices and Considerations

- **Communicate mandatory fields: Organizations should ensure that all mandatory fields are clearly communicated to users.** Users cannot save their profile or proceed to purchase permits if required fields are left blank, which can cause confusion during peak registration periods.
- **Lock specific data fields: If your organization requires strict control over certain user data (such as student ID numbers or primary email addresses), ensure these fields are configured as read-only.** This ensures they appear greyed out on the user side, preventing unauthorized modifications that could disrupt integrations with single sign-on (SSO) or external student information systems.

Recovering a Password

> The Password Recovery Process allows end-users to securely reset their account access credentials if they have forgotten their password. Its primary purpose is to enable self-service password management, reducing administrative support requests and ensuring users can quickly regain access to the portal. This article is intended for OPSCOM administrators to help them understand and support the recovery workflow.

Setup and Configuration

This feature is a standard component of the user portal and requires no specialized administrative setup to function for local accounts.

> If a user's login source is configured using Single Sign-On (SSO), they cannot use the standard OPSCOM password recovery tool. They must reset their password directly through your organization's designated SSO provider. Only users with a local system login can utilize this password recovery option.

Using this Feature

Administrators can use the following instructions to guide users through the standard password recovery workflow.

Requesting a Reset Link

1. Navigate to the **Login Page** of the user portal.
2. Click the **Forgot Password** link to open the recovery dialog box.

3. Enter the email address associated with the account into the provided field.
4. Click the **Send Reminder** button to trigger the automated system email.

Resetting the Password

1. Locate and open the recovery email sent by the system.
2. Click the secure link within the email body to navigate to the **Update Password** screen.
3. Enter a new password into the provided fields.
4. Click the **Reset Password** button to save the new security credentials.
5. Click the confirmation link provided on the screen to return to the **Login Page**.
6. Log in to the portal using the newly created password.

Best Practices and Considerations

- **Check spam and junk folders: Always advise users to check their spam or junk email folders if they report not receiving the password reset email.** Institutional or personal spam filters will occasionally miscategorize system-generated recovery emails.
- **Verify the registered email address: If a user attempts a password reset but the email never arrives, verify that they are entering the exact email address associated with their active user profile.** The system will not send a reset link to an unregistered or mistyped email address.

Getting Started with Text2ParkMe!

> Text2ParkMe is an SMS-based parking payment system that allows users to initiate, pay for, and extend temporary parking sessions directly from their mobile devices via text message. Its primary purpose is to provide a fast, app-free alternative for transient parkers to secure parking on the go. This article is intended for OPS-COM administrators to help them understand and support the end-user setup and SMS workflow.

Setup and Configuration

Before users can initiate a parking session via text, they must configure their profile and register a vehicle.

Admin Side: Administrators must ensure that the Text2ParkMe module is enabled and a dedicated phone number is provisioned for the organization.

User Side: Users must log in to their portal account and complete a one-time setup process to link their mobile device to their payment profile.

1. Log in to the User Portal and click **Your Profile**.
2. Enter a valid mobile phone number in the **Personal Information** section.
3. Scroll to the **Users Settings** section and locate the **Parking Expiry Reminder** field.
4. Select the preferred SMS reminder timeframe (e.g., 5, 10, or 15 minutes) or select **No reminder**.

5. Register a credit card and ensure the Text2ParkMe subscription is active. Detailed instructions can be found on the *Manage your Payment Methods & Subscriptions* page.
6. Register the vehicle license plate in the **Register the Vehicle(s)** section if one is not already present on the account.

> Not all parking providers support Text2ParkMe. Ensure your organization has the module active and properly configured before communicating this functionality to your end-users.

Using this Feature

Administrators can use the following instructions to guide users through navigating the SMS text prompts to purchase or extend parking.

Initiating a Parking Session

1. Text **ParkMe** to the designated Text2ParkMe phone number provided by your organization using the registered mobile phone.
2. Text **P** to start parking or **Q** to quit the session.
3. Text the number corresponding to the desired parking lot from the provided list.
4. Text the number of minutes required for the parking session.
5. Text **C** to continue if the time is correct, or **L** to go back to the lot selection step.
6. Text the number corresponding to the registered license plate, or type the plate number directly if it is unregistered.
7. Text **C** to confirm the purchase or **L** to go back to the previous options.

8. Check your device for a confirmation text and email detailing the parking expiry time.

Extending a Parking Session

1. Text **E** to the designated Text2ParkMe phone number.
2. Follow the automated SMS prompts to add additional time to the active session.

Managing SMS Communications

Users can text the following system commands at any time to manage their messaging preferences:

- **Opt-out:** Text **STOP**, **STOPALL**, **UNSUBSCRIBE**, **CANCEL**, **END**, or **QUIT** to immediately halt all automated messages from the system.
- **Opt-in:** Text **START**, **YES**, or **UNSTOP** to resume receiving messages.
- **Support:** Text **HELP** or **INFO** for information on controlling messages and interacting with the system.

> The SMS system is conversational. Every time a user texts the access number, the system will reply with clear instructions for the next required step.

Best Practices and Considerations

- **Promote reminder settings: Administrators should encourage users to enable SMS reminders during their initial setup.** Receiving a text 5 minutes before parking expires significantly reduces accidental violations and improves the overall user experience.

- **Ensure profile accuracy: Remind users that their caller ID must exactly match the mobile number entered in their profile.** If a user attempts to text the system from a different phone, the system will not be able to locate their payment profile or registered vehicles.

User Side: Managing Email Preferences

> The Managing User Email Preferences feature allows end-users to opt out of non-essential email communications directly from their portal. Its primary purpose is to improve the user experience, ensure compliance with data privacy regulations, and reduce manual unsubscribe requests for your staff. This article is intended for OPS-COM administrators to help them understand the user-facing email management workflow.

Setup and Configuration

This feature relies on the global unsubscribe functionality being active in your environment.

Admin Side: Ensure the unsubscribe functionality is enabled within your system communications settings. If this feature is disabled globally on the backend, the user-facing management options will not be accessible.

User Side: Users can access and manage their specific email preferences independently from their portal account settings or via direct links in received emails.

Using this Feature

Administrators can use the following information to guide users on how to update their communication settings.

Accessing the Preferences Page

Users can access the management page using one of two methods:

2. Navigate to the account settings on the user portal and click **Email Preferences**.
3. Click the **Unsubscribe** link located in the body or footer of any non-essential system email.

> Disabling the unsubscribe functionality at the system level overrides all user preferences. Always ensure this aligns with your local data privacy regulations (such as CAN-SPAM, CASL, or GDPR) before restricting a user's ability to opt out of non-essential communications.

Key Information Displayed

- **Essential Categories:** A section at the bottom of the page displays a list of essential email categories that users cannot unsubscribe from (e.g., system alerts, financial receipts, password resets).

Available Actions and Buttons

- **Category Checkboxes:** Enable the specific category checkboxes to subscribe, or disable the checkboxes to unsubscribe from those non-essential communications.
- **? Icon:** Click the **?** popover icon next to any checkbox to display a detailed description of that specific email category.
- **Select All / Deselect All:** Click these bulk options to select or deselect all available email category checkboxes at once.
- **Save Changes:** Click the **Save Changes** button to apply the updated preferences. A confirmation message will display once successfully saved.

Best Practices and Considerations

- **Communicate exempt categories: Remind users that system-related emails are strictly exempt from the unsubscribe functionality.** Critical communications such as payment receipts, password resets, and new account creation confirmations cannot be disabled by the user to ensure basic account security and operational integrity.
- **Understand global overrides: If your organization disables the unsubscribe functionality globally after users have already unsubscribed, their individual subscription settings will be ignored.** They will default back to receiving all non-essential emails again, regardless of their past opt-out choices.

Managing Company Users (for Company Managers)

> The Company Manager feature allows designated users to directly access and manage the portal accounts of their associated staff members. Its primary purpose is to empower corporate administrators to update employee parking profiles, purchase permits, and pay violations on behalf of their team, centralizing organizational parking management. This article is intended for OPS-COM administrators to help them support corporate clients and troubleshoot impersonation workflows.

Setup and Configuration

This feature requires explicit permissions and user associations to be configured before a manager can access their team's profiles.

Admin Side: Administrators must grant the correct role permissions to the designated manager account within the system backend. Additionally, administrators must link the applicable staff members (sub-users) to the manager's corporate account so they populate in the management list.

User Side: Designated managers access these impersonation tools directly from their user portal navigation bar upon logging in.

Using this Feature

Administrators can use the following instructions to guide a Company Manager through accessing and managing a staff member's account.

Accessing a Staff Account

1. Log in to the User Portal using the Company Manager credentials.
2. Click **Company Manager** in the navigation bar to open the list of all associated users.
3. Click the **login icon** located next to the specific staff member's name.
4. Review the pop-up message on the screen, which confirms the name of the staff member whose account is currently being accessed.
5. Navigate through the staff member's profile and perform the necessary actions on their behalf.

> Once logged in as a staff member, the Company Manager has the ability to perform all the actions that the staff member themselves can do within their profile. This includes updating profile information, buying parking permits, paying parking violations, and adding or managing registered vehicles.

Available Actions and Buttons

- **Company Manager:** Click this navigation menu item to view the list of associated corporate users.
- **Login Icon:** Click this icon to initiate the impersonation session and access the selected user's portal dashboard.

Best Practices and Considerations

- **Maintain accurate corporate rosters: Organizations must routinely ensure that corporate user associations are kept up to date.** If an employee leaves the company, administrators should promptly unlink their account from the Company Manager to prevent unauthorized access or accidental permit renewals on the former employee's behalf.

- **Audit corporate actions: Remind Company Managers that any actions taken while impersonating a user are recorded in the system.** Payments made for permits or violations will apply directly to the staff member's account, so managers should carefully verify they have selected the correct employee from the list before completing financial transactions.