Account Creation Preferences

> The Account Creation Preferences feature allows administrators to choose between granting users immediate portal access or requiring explicit email verification upon registration. Its primary purpose is to balance user convenience with system security and data integrity by controlling the onboarding flow. This article is intended for OperationsCommander (OPSCOM) administrators responsible for managing the user registration experience.

Setup and Configuration

This feature is a global system setting that immediately dictates the onboarding workflow for all new users.

Admin Side: Administrators must have the appropriate system role permissions to access the configuration menus and modify the registration parameters.

User Side: Depending on the configured preference, new users will either be logged in immediately after creating an account or prompted to check their email for a verification link before they can access the portal. For complete user-side documentation, please refer to the *Registering as a User with OPSCOM-Go!* article.

Using this Feature

Administrators can use the following instructions to locate the registration setting and toggle the desired onboarding workflow.

Configuring the Account Creation Flow

1. Hover over **System Configuration**, click **System Settings**, and click the **User Profile** tab.
2. Locate the **Auto Login After Register** setting.
3. Enable the **Auto Login After Register** toggle to allow immediate login, or disable it to require email verification.

Available Configuration States

The **Auto Login After Register** setting has two distinct states, each with specific implications for user experience and system security:

- **Immediate Login (Enabled):** This configuration allows users to instantly access their account immediately upon completing registration, bypassing email verification entirely. This method reduces friction and provides a quicker onboarding experience. It is ideal for scenarios where users might not have immediate access to their email, such as dedicated lobby kiosk setups.
- **Email Verification (Disabled):** This configuration requires users to click a unique verification link sent to their registered email address before they can fully access their account. This is generally the preferred method, as it immediately confirms the registration originates from a real user with a valid email address, significantly reducing bot registrations and fake accounts.

> While immediate login reduces friction, requiring email verification establishes a reliable communication channel from day one. This is crucial for securely processing future password resets, executing account recovery procedures, and delivering important system notifications.

Best Practices and Considerations

- **Balance security and convenience: Carefully weigh the trade-offs between user convenience (immediate login) and enhanced security (email verification) based on your organization's risk tolerance.** Consider the technical literacy and typical access methods of your target audience when deciding on the preferred setting.
- **Ensure robust email deliverability: If you require email verification, verify that your system's global email sending configurations are properly established.** This guarantees that verification emails are delivered promptly and reliably, preventing users from getting stuck during registration.
- **Communicate the registration process: Clearly inform users about the account creation process on your portal homepage.** If email verification is required, provide explicit instructions reminding users to check their spam or junk folders for the activation link.
- **Maintain regulatory compliance: Consider that data privacy regulations often implicitly favor email verification.** Forcing users to verify their email contributes to better data quality and acts as a verifiable record of user consent.

Revision #10
Created 11 June 2025 07:32:22

Updated 25 August 2026 13:43:26