

Account Creation Preferences

OPSCOM allows administrators to configure user account creation preferences, choosing between immediate auto-login or requiring email verification upon registration. Understanding and setting this preference is crucial for managing your user base effectively, balancing user convenience with security and data integrity needs.

Please refer to the [Registering as a User](#) article for the user-side documentation.

Setup & Configuration

Account creation preferences are configured within the **User Profile** settings under **System Settings**.

1. Hover over **System Configuration**, then **System Settings**, and click the **User Profile** tab.
2. Toggle the **Auto Login After Register** setting, which controls the account creation flow.

Using this Feature

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

Immediate Login (Auto Login After Register: ON)

- **Configuration:** Toggle the **Auto Login After Register** setting to **ON**.

- **Behavior:** This method allows users to instantly access their account immediately upon completing registration, without requiring them to verify their email address.
- **Reasons to Use:**
 - **Limited Email Access:** Ideal for scenarios where users might not have immediate access to their email, such as in kiosk setups or for individuals without constant mobile email access.
 - **Reduced Friction:** Provides a smoother, quicker onboarding experience, especially if your target audience is less tech-savvy or if you aim to minimize any barriers to entry.

Email Verification (Auto Login After Register: OFF)

- **Configuration:** Toggle the **Auto Login After Register** setting to **OFF**.
- **Behavior:** This method requires users to click a unique verification link sent to their registered email address before they can fully access their account.
- **Reasons to Use:**
 - **Verifying Legitimate Users:** This is generally the **preferred method** as it immediately confirms that the registration originates from a real user with a valid email address, significantly reducing bot registrations or fake accounts.
 - **Account Security and Recovery:** Email verification establishes a reliable communication channel crucial for secure password resets, account recovery procedures, and sending important notifications, thereby enhancing overall account security.

- **Maintaining Data Integrity:** By ensuring valid email addresses from the outset, you improve the quality and accuracy of your user data in the system.
-

Best Practices & Considerations

- **Balance Security and Convenience:** Carefully weigh the trade-offs between user convenience (immediate login) and enhanced security/data integrity (email verification) based on your organization's risk tolerance and user base.
 - **Communication:** Clearly inform users about the account creation process, especially if email verification is required. Provide instructions on checking spam folders for verification emails.
 - **Email Deliverability:** If using email verification, ensure your system's email sending configurations are robust to guarantee that verification emails are delivered promptly and reliably.
 - **Target Audience Analysis:** Consider the technical literacy and typical access methods of your target audience when deciding on the preferred setting.
 - **Compliance:** Some data privacy regulations may implicitly favor email verification as it contributes to better data quality and user consent verification.
-