2. How to Configure Security and Authentication

A robust security and authentication setup is fundamental to protecting sensitive customer data and ensuring that only authorized personnel can access your CRM. In the **Settings > Configurations > General** tab, you'll define who can reach your system (via IP restrictions) and how users prove their identity (via session policies and multi-factor checks). Properly configuring these options helps you meet compliance requirements, reduce the risk of unauthorized access, and tailor the login experience to your organization's security posture.

Use Cases

1. **Office-Only Access**
   Limit CRM access to your corporate network by whitelisting office IP ranges, preventing external login attempts from unknown locations.
2. **High-Security Environments**
   Require both password and biometric authentication (WebAuthn) for administrators or finance teams to meet stringent internal policies or regulatory frameworks.
3. **Adaptive Session Management**
   Enforce shorter session timeouts for contractors or guest users, while allowing longer idle periods for full-time staff—striking a balance between security and productivity.
4. **Automated Bot Prevention**
   Enable invisible reCAPTCHA on login screens to block scripted attacks without interrupting the legitimate user experience.

The **General** tab under **Settings > Configurations** is where you define your system's core access and login policies. Here you'll find two sections:

1. **Security**: Restrict which IP addresses can access the CRM.
2. **Authentication**: Control session duration, password-attempt limits, and multi-factor requirements.

Below is a detailed, step-by-step guide—complete with screenshots—on how to locate and configure each option.

Navigating to the General Configuration

Click the ⚙ **Settings** icon in the sidebar.
Select **Configurations**.
Ensure the **General** tab (next to "Statuses" and "Languages") is active.

Security: IP Whitelisting

Click “+ New IP”.
Enter a valid IP address (IPv4 or IPv6). Invalid entries highlight in red.
Press **Enter** to confirm the IP. Repeat steps to add more IPs.
Remove an IP by hovering and clicking **×**.
Click **Save** to save the list.

> Note: IP addresses are usually expressed in dotted decimal notation as four numbers separated by dots, e.g., *172.16.255.2*, or as a set of 16-bit hexadecimals separated by colons, e.g., *2001:0000:130F:0000:0000:09C0:876A:130B* If the field turns red, you have entered an invalid IP address.

Authentication: Session & Login Policies

The **Authentication** section allows you to set logon and usage rules, including limited session times and additional logon checks.

To configure authentication:

1. Fill in the following fields:
   Session time minutes: Enter how many minutes after login the user is automatically unlogged from the system when idle. If the field is left blank, the default value of 60 minutes will be applied.
   Login attempts: Enter the number of times the user can enter an incorrect password before being temporarily locked out (for 2 minutes). The default is 3.
2. Check one of the options (or leave them all blank):
   Internal login or WebAuthn: If you want the user to use a choice of password or WebAuthn (biometric data) to log in.
   Internal login and WebAuthn: If you want the user to use both a password and biometrics for additional security to log in.
   Google TFA: If you want the user to use two-factor authentication through Google for additional security.
   Phone TFA: If you want the user to use two-factor authentication via phone number for additional security.

   Get more information about authentication types in Wifox Business Core Solution [here].
3. Check the box next to **Recaptcha on login** to use reCAPTCHA. We use reCAPTCHA v3, which means users will not notice this additional check.
4. Click **Save** to save your settings.

> **Note**: If you select one of the options, the others will be automatically disabled. Uncheck the selected box to enable other authentication options.

By leveraging IP whitelisting and advanced authentication controls, you can significantly bolster your CRM’s defenses against unauthorized access and automated attacks. Regularly revisit these settings—especially after network changes or user-role updates—to maintain an optimal balance between security and usability.

Revision #13
Created 3 October 2024 10:05:15
Updated 25 January 2026 13:47:15