Identity & Access

1. Identity & Access: General

The **Identity & Access** section controls how users and systems authenticate and access the platform.

The **General** page defines core security and authentication rules for the entire system.

Here you can:

1. Restrict access by **IP whitelist**
2. Set **session duration** and **login attempt limits**
3. Configure authentication methods:
   Internal login
   WebAuthn
   Combined login modes
4. Enable **multi-factor authentication (MFA)**
5. Enable **phone-based TFA**
6. Require **reCAPTCHA on login**

These settings apply globally and help enforce your organization’s security policies.

2. Identity & Access: API Tokens

Identification tokens provide a secure, programmatic way to authenticate and authorize external applications or scripts when interacting with Wifox's API. By generating a token tied to a specific role and (optionally) limiting it to certain IP addresses, you can grant granular access without exposing user passwords.

Use Cases

1. **Server-to-Server API Calls:** Create a token named `BackendAutomation` with the Role "CB Accounts & Transactions" so a nightly batch job can fetch balances and generate reports.
2. **Third-Party Integration:** If you connect an external fraud-detection service, generate a token limited to **Clients**, **Actions**, and **Logs** modules, then whitelist only the IP range where that vendor's servers reside.
3. **Temporary Scripts or Tests:** Use a short-lived token (set an expiration date for 24 hours later) when testing new endpoints via Postman. Once the tests complete, let it expire automatically.
4. **Mobile or Webhooks:** When a webhook receiver needs to fetch client data, create a token named `WebhookListener` with the minimal Role (e.g., read-only "Clients" + "KYC Documents") and restrict it to your webhook server's IP.

Where to Find Identification Tokens

Open the Sidebar Menu: Click the hamburger (☰) icon in the top-left to expand the main navigation.

Navigate to Security → Identification Tokens: Scroll down to the **Security** section and click **Identification tokens**. This opens the **Identification Tokens** list view.

Identification Tokens List View

Once you land on the **Identification Tokens** page, you'll see a table with these columns:

Column	Description
Token	The token's name (a unique identifier you assigned). Clicking it will open the edit panel.
Permissions	A list of modules and API scopes this token can access (e.g., `Clients`, `CB Assets`, `Projects`, etc.).
Whitelisted IPs	0–many IP addresses or CIDR ranges from which the token is valid. Blank means no IP restriction.

Column	Description
Expired Date	(Optional) If set, the token will stop working after this date—use the calendar icon to pick a date.

1. **Permissions** lists each module (e.g., “Clients,” “CB Wallets,” “Projects,” “Desks,” etc.) that the token can access. If there are more than a few scopes, the table will show “+X Show all” to reveal the rest.
2. **Whitelisted IPs** can be individual IPv4/IPv6 addresses or CIDR ranges (e.g., `192.168.31.0/24`). The token will only be accepted when the request originates from one of these allowed IPs.
3. **Expired Date** is blank if no expiration was set. Otherwise, tokens stop working once the date passes.

Click the **token name** itself (e.g., `NewIdentForTest`) to open the **Edit Identification Token** drawer.

Creating a New Identification Token

To generate a brand-new token, click the **+ Add** button in the top-right corner of the list view. This opens the **Add Identification Token** drawer:

1. **Name:**
   Enter a clear, descriptive name for your token (e.g., `MyIntegrationService`, `ReportingScript`, `PostmanUser`, etc.).
   The name must be unique among all existing tokens.
2. **Role:**
   Select the Role that determines which modules and API endpoints the token can access.
   A Role is defined in **Settings → Roles** and groups permissions for specific modules (e.g., “Read-only Clients,” “Full CB Access,” “Analytics Only”).
   When you choose a Role from this dropdown, all modules and scopes assigned to that Role will be inherited automatically.
3. **Expired Date (Optional):**
   Click the **calendar icon** to set an expiration date (DD/MM/YYYY).
   Once the date is reached, the token becomes invalid—useful for short-lived integrations or security best practices.
4. **Whitelist (Range of IPs):**
   If you want to restrict token usage to particular IP addresses, click **+ New IP** to add one or more entries.
   You can enter a single address (e.g., `203.0.113.45`) or a subnet (e.g., `192.168.1.0/24`).
   If your integration only runs from your office or a known server, adding IP restrictions prevents the token from working elsewhere.
5. **Generate Token:**
   Once you’ve filled in **Name**, **Role**, (optional) **Expired Date**, and (optional) **Whitelisted IPs**, click **Generate token**.
   The system will display a newly created alphanumeric token string (e.g., `AbCdEfGhIjKlMnOpQrStUvWxYz1234567890`).
   Be sure to copy and store this token value immediately—this is the only time it’s shown in full.

After generation, the token will appear in the list view with its associated permissions and settings.

Editing an Existing Identification Token

To modify an existing token's properties (e.g., add/remove an IP restriction, update the expiration date, or change its Role), follow these steps:

1. **Click the Token Name** in the list (or click the ✏ pencil icon under "Actions").
2. The **Edit Identification Token** drawer slides out from the right.
3. **Adjust any of these fields**:
   Name (if you want to rename it)
   Role (select a different Role to alter the token's permissions)
   Expired Date (change or clear the date)
   Whitelist (click **+ New IP** to add more addresses, or click the □□ icon next to an IP to remove it)
4. **Save** your changes.

The token's underlying string does not change unless you explicitly delete and recreate the token—a Role or date change does not regenerate the secret value.

After saving, the updated permissions, IP whitelist, or expiration date take effect immediately.

Deleting an Identification Token

If you no longer need a token or suspect it has been compromised, you can permanently remove it:

1. **Locate the Token** in the list view.
2. **Click the □□ Delete icon** in the "Actions" column for that row.
3. A confirmation pop-up appears:
   `Are you sure?`
   `This action cannot be undone.`
   [Cancel] [Delete]
4. **Click Delete** to proceed.

The token is removed instantly—any application using that token string will receive authentication errors going forward.

> **Warning:** Deleted tokens cannot be recovered. If an external system still relies on that token, you'll need to generate a brand new one and update your integration.