

SAKUL ACCOUNT

Sakul Account User Manual

The central account for Sakul websites and applications

Application and manual version: 1.0.3

Language: English

Contents

1. How Sakul Account works	3
2. Registration and e-mail verification	3
3. Sign-in and password	4
4. Two-factor authentication	4
5. Profile and personal data	5
6. Sessions and devices	6
7. Authorized applications and permissions	6
8. Features, benefits, and connected accounts	7
9. Privacy, export, and deactivation	7
10. Troubleshooting and safe use	7

This guide explains how to create, secure, and use an account. It also covers application permissions, connected services, privacy, and troubleshooting.

1. How Sakul Account works

One account provides identity to multiple services without disclosing your password to them.

Central identity

Sakul Account keeps sign-in credentials and the basic profile in one place. Connected websites and applications redirect you to the Sakul Account authorization page and receive only the data you approve.

Every account has a private internal record and a stable public ID. Applications can recognize the same person by this ID without using the e-mail address as a technical identifier.

- The password is never passed to a client application.
- Access can be revoked from the profile at any time.
- The data scopes are listed before consent is confirmed.

Language and version

The interface and manual are available in Czech and English. The stored choice and browser language are evaluated first; unsupported languages fall back to English. A manual choice takes precedence.

Signed-in users see the application version in the footer. The same version is printed in the PDF manual, making it possible to confirm that the document matches the system.

2. Registration and e-mail verification

An account becomes active only after the e-mail address is confirmed.

Create an account

- 1 Choose account creation on the sign-in page.
- 2 Enter a display name and a valid e-mail address.
- 3 Submit the form and wait for the verification message.
- 4 Open the one-time link and set a secure password.

Note: If an administrator pauses new registrations, existing accounts can still sign in.

Registration form protection

The system uses timing and frequency limits, a hidden control field, and optionally Cloudflare Turnstile. These checks distinguish normal visitors from automated registrations.

The registration score is intended for administrators. A higher score is not proof of abuse; it is a signal for review.

Warning: Do not submit the form repeatedly in rapid succession. A temporary limit protects the service and clears automatically after its window expires.

Missing or expired verification link

- 1 Check the spam folder and the spelling of the address.
- 2 Open the verification resend page from the sign-in screen.
- 3 Enter the same e-mail and use only the newest delivered link.

Note: The system does not reveal whether a particular e-mail exists. The same generic response protects user privacy.

3. Sign-in and password

Sign-in is protected by sessions, attempt limits, and secure cookies.

Normal sign-in

- 1 Open the Sakul Account sign-in page.
 - 2 Enter the verified e-mail and password.
 - 3 If two-factor authentication is enabled, enter a code from the authenticator.
 - 4 After success, the profile opens or authorization continues in the original application.
- The session uses a secure HttpOnly cookie.
 - The session identifier is renewed after sign-in.
 - Suspicious or excessive attempts can be temporarily limited.

Forgotten password

- 1 Choose Forgot password.
- 2 Enter the account e-mail.
- 3 Open the newest one-time link from the message.
- 4 Set a new password of at least 12 characters.

Warning: The link expires and stops working after use. Never share the password or the complete link.

Change the password

Password change is available under Account security and requires the current password. Other sessions and persistent sign-ins are revoked after a successful change.

Use a unique password stored in a password manager. Reusing a password from another service increases takeover risk.

4. Two-factor authentication

TOTP adds a one-time code from a phone or password manager to the password.

Enable with a QR code

- 1 Open Account security and the 2FA setup from the profile.

- 2 Scan the QR code with a compatible authenticator, or enter the secret manually.
- 3 Enter the current six-digit code and confirm activation.
- 4 Store the one-time recovery codes securely and separately from the authenticator device.

Warning: The QR code and secret are as sensitive as a password. Do not save a screenshot in a public gallery or unsecured cloud.

Recovery codes

Each recovery code works once. Generating a new set invalidates the entire old set.

If both the authenticator and recovery codes are lost, contact the operator. Ownership verification may not be immediately possible.

Note: Enabling, disabling, or regenerating codes creates a security audit event.

5. Profile and personal data

Required information is limited; the extended profile is optional.

Basic profile

The display name can be changed in profile settings. E-mail is used for sign-in and communication; changing it requires confirmation of the new address.

The public ID is stable and cannot be changed by the user. Connected applications use it as a safe identifier.

- Display name
- Verified e-mail
- Account status and roles
- Account creation date

Optional information

You may add a profile photo, short biography, interests, birth date, location, and personal website. Every field is optional and can be changed or removed later.

For a website, entering a value such as `www.sakul.cz` is sufficient; the system adds a secure protocol and validates the address.

Warning: Never put passwords, access tokens, or other secrets in the biography or other profile fields.

Profile photo

- 1 Choose a JPEG, PNG, or WebP file within the displayed limit.
- 2 Upload it; the system resizes and stores it in a safe format.
- 3 Use the separate button to remove it.

Note: The image is served through an application route and is not stored as a freely browsable public file.

6. Sessions and devices

The overview helps detect forgotten or unfamiliar sign-ins.

Web sessions

Each active session represents a sign-in in a browser. It shows a device description, approximate IP area, and recent activity, not a precise long-term location.

Revoke an unknown session immediately and change the password. You can also sign out all other sessions at once.

Warning: Always use Sign out on a shared computer; closing a window may not end the session.

Registered application devices

A client application with the devices scope may register an installation. This differs from a web session: it describes an application or installation, not the browser sign-in itself.

A device can be renamed or revoked. Revocation disables further use as supported by the client application.

7. Authorized applications and permissions

Consent defines what a particular application may obtain from the account.

Consent screen

The first sign-in to a client application shows its name, description, and requested permissions. Continue only if you trust both the application and the request.

Sakul Account uses authorization code with PKCE S256. The client receives a short-lived code and exchanges it server-side for a token; the password is never involved.

- openid: stable identity
- profile: basic profile
- email: e-mail and verification state
- features: available features
- devices: registered device management
- offline_access: refresh token permission

Revoke an application

Revocation invalidates access and refresh tokens related to the grant. A new consent is required for later access.

- 1 Open Authorized applications from the profile.
- 2 Review its name, website, granted scopes, and last use.
- 3 Confirm that the application will lose access and revoke it.

Note: An authorized application and a registered device are different records: the first is consent, the second is a specific installation.

8. Features, benefits, and connected accounts

Available features can come from manual assignment or external membership.

Available features

The Benefits page lists effective features for each client application. A feature can have a source, expiry, and change history.

Sakul Account decides entitlement, while the client application decides how that feature is used.

Note: The end of one source does not necessarily remove a feature while another valid source remains.

Patreon and external services

When configured by the operator, Patreon can be connected. Authentication occurs at Patreon and Sakul Account receives authorized membership data and synchronization tokens.

Tokens are encrypted in the database. Disconnecting the service revokes local access and related entitlements are recalculated.

Warning: Sakul Account never asks for a Patreon password. Stop if a page claiming to be Sakul Account requests it.

9. Privacy, export, and deactivation

Users can access their information and deactivate the account.

Personal data export

Profile settings can generate an export of data associated with the account, including profile information and related summaries in a portable format.

Protect the downloaded file like any personal document and do not leave it on a public or shared device.

Note: Security secrets, the password hash, and usable tokens are excluded from the export.

Account deactivation

Deactivation blocks normal sign-in, ends sessions, and invalidates application credentials. It affects every connected service.

Some audit and operational records may remain for a limited time for security, recovery, or legal requirements.

Warning: Download any required export and check the impact on client applications before deactivation.

10. Troubleshooting and safe use

Most problems can be solved by checking the address, time, and newest link.

Common problems

- Expired link: request another and use the newest delivered message.
- 2FA code rejected: enable automatic device time and try the next code.
- Application access rejected: verify the exact redirect address and restart sign-in from the client.
- Feature missing: inspect its source and validity on Benefits.
- E-mail missing: check spam and the address, then wait for resend limits.

Note: When reporting an error, include the time, application, and message. Never send a password, complete authorization code, token, or 2FA secret.

Security recommendations

- Check the Sakul Account domain and HTTPS.
- Use a unique password and enable 2FA.
- Review sessions, devices, and authorized applications regularly.
- Revoke anything unfamiliar or unused.
- Keep the browser, operating system, and authenticator updated.

Warning: The operator will not ask for your password, recovery code, complete reset link, or client token by e-mail.