

ARHOCH PRODUCT MANUALS

ARHOCH IAM

Account, team and administration manual

Understand each area of the system and follow the procedures, from initial setup to everyday operations.

How to use this manual

Follow the quick start to prepare your environment. Then look up individual tasks in the chapters. Screenshots use demonstration data; available menus and actions depend on your permissions.

Contents

About this manual	3
Quick start	3
1 Account and security	4
1.1 Create an account and verify your email	4
1.2 Sign in with password, email code or Google	5
1.3 Recover or change your password	6
1.4 Edit profile, language, time zone and theme	6
1.5 Review and end sessions	7
1.6 Create and manage API tokens	8
1.7 Close your own account	9
2 Organization, branches and team	10
2.1 Choose organization and branch	10
2.2 Start in another application	10
2.3 Invite a person to the team	10
2.4 Accept and review invitations	11
2.5 Add, review and remove access	12
2.6 Rename the organization and manage branches	12
3 Platform administration	14
3.1 Navigate platform administration	14
3.2 Create application	14
3.3 Edit application	15
3.4 Activate, disable or delete application	16
3.5 Create permission	16
3.6 Edit permission	17
3.7 Activate, disable or delete permission	18
3.8 Create access role	18
3.9 Edit access role	19
3.10 Activate, disable or delete access role	20
3.11 Create feature	20
3.12 Edit feature	21
3.13 Activate, disable or delete feature	22
3.14 Create organization	22
3.15 Edit organization	23

3.16 Activate, disable or delete organization	23
3.17 Create branch	24
3.18 Edit branch	25
3.19 Activate, disable or delete branch	25
3.20 Create a global user	26
3.21 Edit a user and resend activation	26
3.22 Change status and administratively verify email	27
3.23 Set a new password for a person	28
3.24 Create and manage user memberships	28
3.25 Assign user roles	29
3.26 Enable features for a context	29
3.27 Send, resend and revoke administrative invitations	30
3.28 Assign platform administrators	31
3.29 Manage publisher token	31
3.30 Manage provisioning token	32
3.31 Rotate a signing key	32
3.32 Retire a key or flag compromise	33
4 Glossary	34
5 Help and next steps	34

About this manual

IAM centralizes identity and access for ARHOCH products. You maintain one account and use only the organizations, branches and applications you are authorized to access.

Team routines also appear inside TV, SGA and Todo. Platform administration has separate permissions and differs from managing your organization. Images show the real Portuguese interface with demonstration data and simulated local responses.

Quick start

1. Create the account, read the conditions and verify email.
2. Sign in and choose the application organization/branch.
3. Review language, time zone and theme; invite people with the required access.
4. Use Applications to open TV, SGA or Todo.

1 Account and security

1.1 Create an account and verify your email

What it is for Start with your identity, an organization and its first branch.

Where to find it Sign-in page → Create account

Fields and options

Your name	Name of the person using the account; required.
Email	Valid accessible address for verification and recovery.
Password / Confirm password	Both entries must match. At least 15 characters and the other displayed criteria; common passwords or passwords tied to the entered data are rejected.
Organization name	Team workspace name; not your personal name.
Organization identifier	3-63 letters, digits or hyphens. Review the suggestion before creating the account.
Branch name	First location/working group, for example Main office.

Step by step

1. Open Create account. In Your details, complete Your name, Email, Password and Confirm password.
2. Use at least 15 characters, up to the maximum displayed. A phrase with spaces is allowed. Avoid personal details, the organization name and common passwords.
3. Select Continue. In Organization, enter Organization name, Organization identifier and Branch name. Review the suggested identifier: 3-63 letters, numbers or hyphens.
4. Read the displayed documents. Accept the conditions after reviewing them, then select Create account. The Privacy Policy is a separate notice; this acceptance does not authorize commercial use of data.
5. Open the verification message in your inbox or spam folder. Follow its link before it expires and select Confirm my email when requested. Then sign in.

Expected result

Registration stays pending until verification. The organization and branch are created after verification; verifying email does not replace signing in.

ARHOCH IAM

Criar conta

Etapa 2 de 2

Agora, organize seu espaço de trabalho.

1 Seus dados 2 **Organização**

Seu espaço de trabalho

A organização reúne sua equipe. A filial identifica o primeiro local ou grupo de trabalho.

Nome da organização

New unit

Identificador da organização

new-unit

Sugerido a partir do nome; você pode editar. Use de 3 a 63 letras, números ou hífens. Ex.: minha-equipe.

Nome da filial

Main

Por exemplo: Matriz, Escritório ou Equipe principal.

Condições para criar sua conta IAM

Consulte os documentos nas versões definidas para este cadastro. Os links abrem o Licenses em outra aba.

- [Termos de uso - 17/10/2026 - revisão 1](#)
- [Licença de uso - 17/10/2026 - revisão 1](#)
- [Condições específicas do IAM - 17/10/2026 - revisão 1](#)
- [Uso aceitável e moderação - 17/10/2026 - revisão 1](#)
- [Conteúdos e uploads - 17/10/2026 - revisão 1](#)
- [Condições comerciais - 17/10/2026 - revisão 1](#)

Informações sobre o tratamento de dados: [Política de privacidade - 17/10/2026 - revisão 1](#)

☐ Aceito as condições de uso e estou ciente da Política de Privacidade.

O uso básico é gratuito. Eventual uso comercial de dados ou conteúdos depende das condições e autorizações específicas; este aceite não concede essa autorização.

Todos os campos são obrigatórios. Você precisará confirmar seu e-mail antes de entrar.

[Voltar](#) [Criar conta](#)

Já possui uma conta? [Entrar](#)

Real Portuguese registration, Organization step; demonstration data and locally simulated submission.

Important information

Use Resend verification if needed. A registration conflict can mean an existing account or an unavailable identifier: review the identifier or use Sign in or recover password. You do not need a new identity for each application.

1.2 Sign in with password, email code or Google

What it is for Authenticate the identity shared by the applications.

Where to find it Sign-in page

Fields and options

Email	Identity used with each sign-in method.
8-digit code	Use the latest code sent to that address; do not share it.

Step by step

1. Enter Email. For password access, choose Continue with password, enter Password, then Sign in. Use Change email if the address is incorrect.
2. Alternatively, choose Send email code. Enter the latest 8-digit code and select Confirm code. If it expires, use Resend code.

3. Continue with Google appears only when enabled. Complete authentication with Google. If Complete your registration appears, provide the organization, identifier and branch, review the documents, then choose Create organization and continue.
4. Wait for the session check. An existing valid session may take you directly to your account. Then select the organization and branch context required by the application.

Expected result

Your account becomes authenticated; this does not automatically grant access to every organization or application.

If something goes wrong**Password, code or link rejected**

Check the email, use the latest code and request another if needed. Respect the displayed wait time instead of repeated clicks. Do not share codes or links.

1.3 Recover or change your password

What it is for Recover access or update a known password.

Where to find it Sign-in → Continue with password → Forgot my password; or account menu → Account security → Password

Step by step

1. To recover, enter your email, open the password step and select Forgot my password. The response does not publicly confirm whether the account exists.
2. Wait for the message and open the valid link. In Recover password, enter New password and Confirm new password, then Save password. A further request requires waiting 1 minute when indicated.
3. To change it while signed in, open Password. Enter Current password when requested, New password and confirmation. Save and follow the displayed authentication guidance.

Expected result

The new password is submitted only through IAM's dedicated operation. A recovery link must not be reused or disclosed.

1.4 Edit profile, language, time zone and theme

What it is for Maintain your account presentation and date display preferences.

Where to find it Account menu → My profile or Preferences

Fields and options

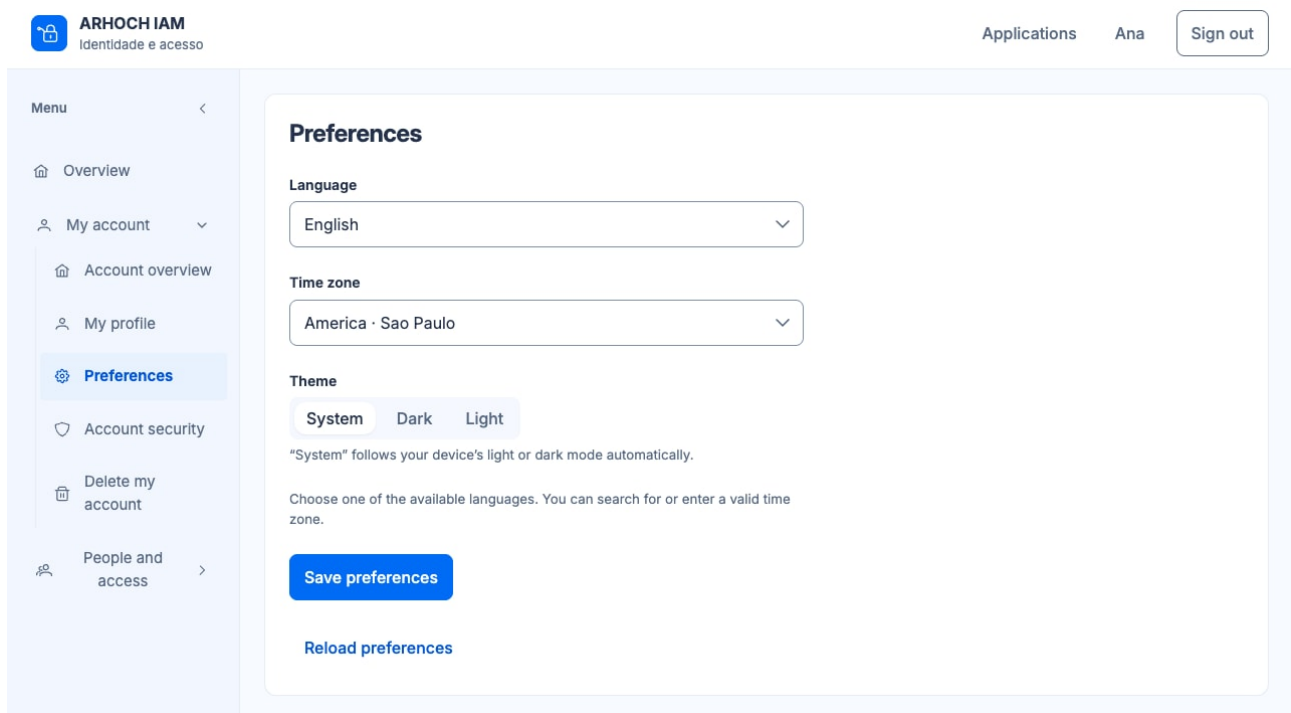
Name	Editable in My profile; email is not editable in this panel.
Language	Actual options: Portuguese (Brazil), English, English (United States) and Spanish.
Time zone	Select or enter a valid identifier; affects displayed dates.
Theme	Light, Dark or System; System follows the device.

Step by step

1. In My profile, change Name and select Save profile. Email is displayed as non-editable in this panel.
2. In Preferences, choose Language among Português, English and Español. Search for or enter a valid Time zone.
3. Choose light, dark or System theme. System follows the device setting. Select Save preferences and check the success message.
4. If another screen changed the same data, use Reload profile or Reload preferences, review the current values and reapply only the intended change.

Expected result

IAM saves shared preferences; consuming applications present them through the official components.



Preferences in the real English interface with a demonstration account.

1.5 Review and end sessions

What it is for Identify connected devices and revoke access that should not continue.

Where to find it Account menu → Account security → Sessions

Step by step

1. Open My sessions and review client names, dates and the current-session marker. Use Refresh sessions to reload the list.

2. Use Items per page, Next sessions and Back to start for additional results; the maximum is 200 per page.
3. To end a session, select Close on the correct row and confirm. To retain only the current session, select Revoke other sessions and confirm.
4. Use Sign out in the account menu when finishing on a shared device. Wait for server-side revocation to complete.

Expected result

A revoked session can no longer be used. Ending the current session may require signing in again.

1.6 Create and manage API tokens

What it is for Grant limited programmatic access to an application without sharing your password.

Where to find it Account security → API tokens

Fields and options

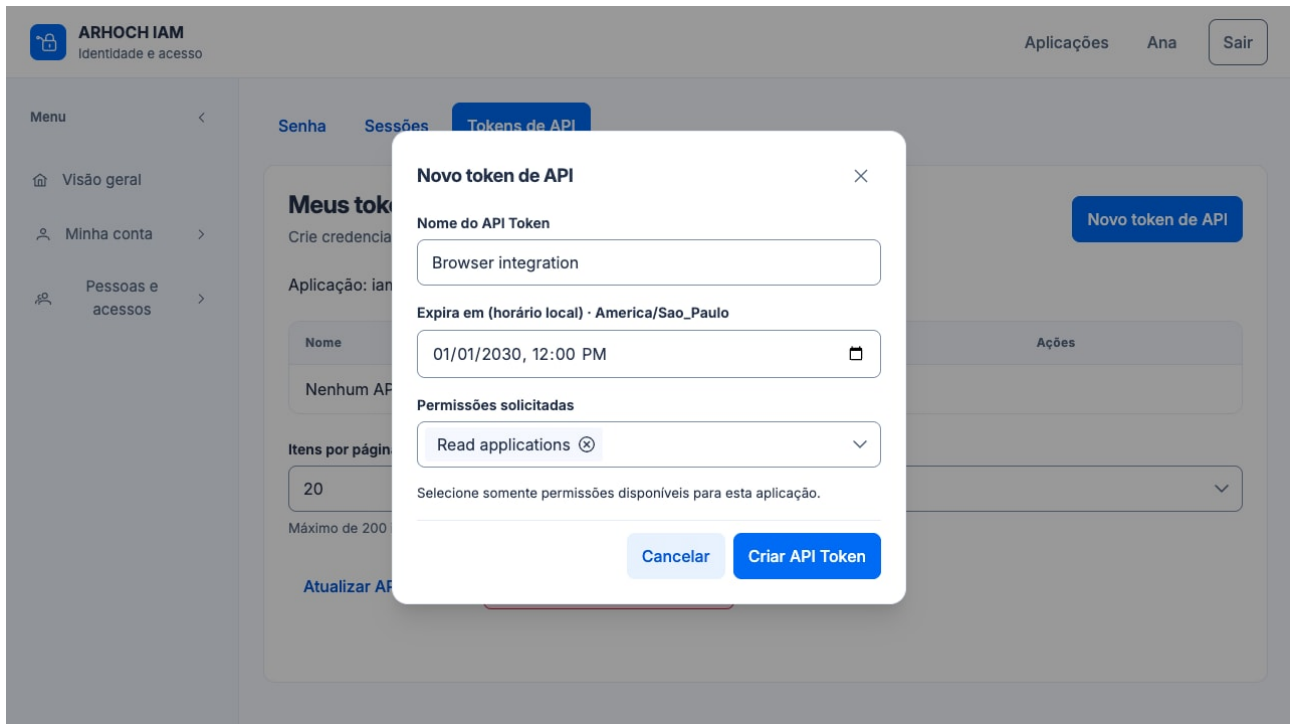
API token name	Required; identify the consuming integration.
Expires at (local time)	Required; check the displayed time zone and the server-accepted expiry.
Requested permissions	Only permissions available in the active application/context; does not grant rights your account lacks.

Step by step

1. Select the application organization and branch if requested. Open New API token. Enter API token name and Expires at (local time), checking the displayed time zone.
2. In Requested permissions, select only the necessary options available for this application. Load more options if needed. Select Create API token.
3. The secret is displayed once. Store it securely and select Hide secret after transferring it. The list shows metadata and cannot retrieve the secret.
4. In Edit, change the name with Save name. For other changes, use Change permissions or rotate; review permissions and confirm Rotate secret. Update the integration using the previous secret.
5. Use Revoke for one token or Revoke all API tokens, reviewing the confirmation. Refresh API tokens and pagination let you review the state.

Expected result

Each token retains its authorized scope and permissions. Revocation or rotation may interrupt existing integrations.



Real token-creation form before generating any secret; simulated local API.

Important information

Personal, publisher and provisioning tokens serve different purposes. Never include secrets in screenshots, public support requests or manuals.

1.7 Close your own account

What it is for Close the identity and its connected access with explicit confirmation.

Where to find it Account → Delete my account; IAM /account-deletion address

Step by step

1. Read the impact: sessions and API tokens lose access across connected applications. The operation preserves history and other data; it is not complete erasure of personal data.
2. Check the account email. Select Delete my account and confirm only if you intend to close this identity.
3. If you are blocked because you are the only organization or platform owner, assign another authorized owner before trying again.

Expected result

The account is closed. A new account can use the same email or Google identity, but previous access is not automatically restored.

2 Organization, branches and team

2.1 Choose organization and branch

What it is for Choose where application actions will take place.

Where to find it Header → Organization and branch

Step by step

1. Open the header selector. Select an available pair or choose Organization and then Branch. Use More options for further results.
2. Check both names and choose Use this context. Wait for the application to reload its data for that context.
3. Use Refresh options if an access change is not yet visible. An active session without context does not authorize an unknown or unlinked organization.

Expected result

The header shows the active organization and branch. Check this context before editing people, media or tasks.

2.2 Start in another application

What it is for Reuse your identity and, when authorized, an existing organization.

Where to find it Header → Applications; context selector → Use another organization

Step by step

1. Open Applications and choose a product. The destination opens in a new tab and checks access again.
2. In Start in this application, choose Use existing organization when available. Select an organization you administer and choose Branches for this application.
3. For a separate workspace, choose Create new organization and enter its name, identifier and branch. Review and select Confirm and continue.
4. Use Use another organization in the selector to enable another existing organization when available. This does not transfer data between organizations.

Expected result

The application receives the authorized context. A shared account does not provide universal access.

2.3 Invite a person to the team

What it is for Let a person receive and accept an invitation with the correct scope.

Where to find it Application → People with access → Send invitation / New invitation

Before you start

- People-management access in the context. Visible options depend on permissions and ownership.

Fields and options

Email	Required and valid; verify the person before sending or granting access.
Initial name	Used for direct addition when requested; an existing account keeps its name.
Organization roles / Branch roles	Independent selections within allowed scopes; check the permissions described by each option.

Step by step

1. Check the active application, organization and branch. Open Send invitation or New invitation and enter Invitee email.
2. Select the required Organization roles and Branch roles. Read each description and its permissions; grant only the intended access.
3. Check the recipient and select Send invitation. The list shows status and expiry. Use Refresh invitations and Filter status to follow up.
4. If necessary, use Resend on an eligible invitation. Revoke or Delete invitation prevents its use; it is not the deletion of an existing account. Confirm the target before acting.

Expected result

The request appears in the list. Sending does not prove that the person opened the email or accepted the invitation.

2.4 Accept and review invitations

What it is for Complete joining the invited context.

Where to find it Email invitation link → Accept invitation

Step by step

1. Open the received link. Review the organization, branch, masked email and expiry before proceeding.
2. If an account needs to be created, enter Your name when requested. If authentication is required, sign in with the invited identity. Select Accept invitation.
3. After confirmation, use the offered destination or explicitly sign in to the application. Accepting an invitation does not necessarily start a session.
4. Team managers can use Review invitation to inspect details and Confirm invitation when that action is available and authorized.

Expected result

Authorized membership can be used in its context. Invalid, expired or revoked links require a replacement from the manager.

2.5 Add, review and remove access

What it is for Maintain people and roles without changing application business data.

Where to find it Application → People with access

Fields and options

Email	Required and valid; verify the person before sending or granting access.
Initial name	Used for direct addition when requested; an existing account keeps its name.
Organization roles / Branch roles	Independent selections within allowed scopes; check the permissions described by each option.

Step by step

1. Review people, invitations, states and the Organization owner marker. Use Refresh people, filters and pagination as needed.
2. For authorized immediate access, select Add access now, enter Person email and Initial name, and review roles. An existing account keeps its current name. Confirm with Add access.
3. Open Edit roles or View roles for the correct person. Review organization and branch scope, select available roles and use Save roles.
4. Remove from this branch removes access in that branch; Remove from organization is broader. Read the confirmation and check the email. This is not the deletion of the global account.

Expected result

The list reflects authorized memberships and roles. Restrictions may prevent removing the last owner or editing people without verified email.

2.6 Rename the organization and manage branches

What it is for Maintain the structure shared by the applications.

Where to find it Application → Organization / Organization branches

Fields and options

Organization name	Renames the shared workspace; requires organization-management authority.
New branch name	Name of the created/renamed location/group; does not copy another branch's data.

Step by step

1. In Organization, verify the context, edit Organization name and select Save name. Use Refresh organization to reload.

2. In Organization branches, enter New branch name and select Create branch. Wait for it to appear in the list.
3. To rename, choose Rename, enter New branch name and select Save name. Cancel abandons that edit. Use Refresh branches or More branches to continue browsing.

Expected result

IAM manages the names and branches. Creating a branch does not mean copying business data from another branch.

Important information

These consumer screens allow creating and renaming. Platform administration offers separate status actions; do not confuse the access levels.

3 Platform administration

Use this part only if the administrative menu and authorization are available for your account. Creating applications, permissions or keys is not required for daily TV use.

3.1 Navigate platform administration

What it is for Review global records only with administrative authorization.

Where to find it IAM → Administration

Step by step

1. Sign in with an authorized account. Administration differs from managing your team; screens and operations are checked by the server.
2. Open the desired section. Use Filter status and, when available, Filter application. Search this page searches loaded items only, not the whole catalog.
3. Use Items per page (maximum 200), Next page and Back to start to browse results. Refresh reloads current records.
4. When editing, save or explicitly discard changes before leaving. On a version conflict, reload and check the current state before reapplying.

Expected result

Lists preserve browsing context and show permitted controls. Denied access requires review by an authorized administrator.

3.2 Create application

What it is for Create an administrative record with correct fields and scope.

Where to find it Administration → Applications and features → Applications

Before you start

- Account with platform administration and the area's read/write permissions; organization or branch ownership alone does not grant this authorization. The server decides each operation.

Fields and options

Application key	Required, at most 128 characters; starts with a lowercase letter and allows lowercase letters, digits and hyphens.
Name / Description	Name is required; description optionally explains the purpose.
Trusted domains	Optional. One exact arhoch.com subdomain per line; no protocol, port or wildcard. accounts.arhoch.com is reserved.
URL after email confirmation or invitation acceptance	Optional, at most 2048 characters. HTTPS with a host listed in Trusted domains; no port, username, password or # fragment.

Step by step

1. Open Applications and features → Applications. Check filters and select the target organization or application when required.
2. Select New application and complete the fields described in this table. Correct inline field messages before saving.
3. Review the scope and select Create application. Wait for confirmation; do not close or repeat while processing.
4. Refresh the list and check the new record name and state. Review duplicate or invalid identifiers according to the server response.

Expected result

The record is created without automatically granting access to all users.

3.3 Edit application

What it is for Update the existing record while preserving identity and revision.

Where to find it Administration → Applications and features → Applications → Edit

Before you start

- Account with platform administration and the area's read/write permissions; organization or branch ownership alone does not grant this authorization. The server decides each operation.

Fields and options

Application key	Required, at most 128 characters; starts with a lowercase letter and allows lowercase letters, digits and hyphens.
Name / Description	Name is required; description optionally explains the purpose.
Trusted domains	Optional. One exact arhoch.com subdomain per line; no protocol, port or wildcard. accounts.arhoch.com is reserved.
URL after email confirmation or invitation acceptance	Optional, at most 2048 characters. HTTPS with a host listed in Trusted domains; no port, username, password or # fragment.

Step by step

1. Find the record, verify its name and select Edit. Review current values before changing them.
2. Change only enabled fields. Do not circumvent locked identifiers or associations. For roles, recheck selected permissions after changing scope.
3. Select Save changes and wait. Cancel abandons editing, with discard confirmation for pending drafts.
4. On version conflict, reload the record and compare current content. Reapply only the necessary change.

Expected result

Allowed fields are updated; server authorization remains enforced.

3.4 Activate, disable or delete application

What it is for Control record lifecycle without confusing disabling with renaming.

Where to find it Administration → Applications and features → Applications → Actions

Before you start

- Account with platform administration and the area's read/write permissions; organization or branch ownership alone does not grant this authorization. The server decides each operation.

Step by step

1. Check the row state and open Actions. Activate is eligible for a disabled record; Disable for an active one; Delete is not a new operation for an already deleted record.
2. To disable, select Disable followed by the name and read the access-interruption notice. Confirm Disable only for the correct target.
3. To reactivate, select Activate on the disabled record and check the result. This does not replace reviewing required memberships, permissions or features.
4. To delete, choose Delete and read the irreversible-action confirmation. Cancel if you intended only a temporary interruption. Dependencies or restrictions may cause server rejection.

Expected result

The list reflects the permitted state. This catalog action does not promise physical erasure of personal data.

3.5 Create permission

What it is for Create an administrative record with correct fields and scope.

Where to find it Administration → Applications and features → Permissions

Before you start

- Account with platform administration and the area's read/write permissions; organization or branch ownership alone does not grant this authorization. The server decides each operation.

Fields and options

Permission key	Required, at most 128 characters; at least three lowercase dot-separated segments, such as app.resource.action. Start with the selected application key followed by a dot.
Application	Required. The permission key must belong to this application namespace.
Where it can be granted	Platform, Organization, Branch or Organization or branch. Defines valid grant scopes.
Name / Description	Required name and optional description; explain the allowed action.

Step by step

1. Open Applications and features → Permissions. Check filters and select the target organization or application when required.
2. Select New permission and complete the fields described in this table. Correct inline field messages before saving.
3. Review the scope and select Create permission. Wait for confirmation; do not close or repeat while processing.
4. Refresh the list and check the new record name and state. Review duplicate or invalid identifiers according to the server response.

Expected result

The record is created without automatically granting access to all users.

3.6 Edit permission

What it is for Update the existing record while preserving identity and revision.

Where to find it Administration → Applications and features → Permissions → Edit

Before you start

- Account with platform administration and the area's read/write permissions; organization or branch ownership alone does not grant this authorization. The server decides each operation.

Fields and options

Permission key	Required, at most 128 characters; at least three lowercase dot-separated segments, such as app.resource.action. Start with the selected application key followed by a dot.
Application	Required. The permission key must belong to this application namespace.
Where it can be granted	Platform, Organization, Branch or Organization or branch. Defines valid grant scopes.
Name / Description	Required name and optional description; explain the allowed action.

Step by step

1. Find the record, verify its name and select Edit. Review current values before changing them.
2. Change only enabled fields. Do not circumvent locked identifiers or associations. For roles, recheck selected permissions after changing scope.
3. Select Save changes and wait. Cancel abandons editing, with discard confirmation for pending drafts.
4. On version conflict, reload the record and compare current content. Reapply only the necessary change.

Expected result

Allowed fields are updated; server authorization remains enforced.

3.7 Activate, disable or delete permission

What it is for Control record lifecycle without confusing disabling with renaming.

Where to find it Administration → Applications and features → Permissions → Actions

Before you start

- Account with platform administration and the area's read/write permissions; organization or branch ownership alone does not grant this authorization. The server decides each operation.

Step by step

1. Check the row state and open Actions. Activate is eligible for a disabled record; Disable for an active one; Delete is not a new operation for an already deleted record.
2. To disable, select Disable followed by the name and read the access-interruption notice. Confirm Disable only for the correct target.
3. To reactivate, select Activate on the disabled record and check the result. This does not replace reviewing required memberships, permissions or features.
4. To delete, choose Delete and read the irreversible-action confirmation. Cancel if you intended only a temporary interruption. Dependencies or restrictions may cause server rejection.

Expected result

The list reflects the permitted state. This catalog action does not promise physical erasure of personal data.

3.8 Create access role

What it is for Create an administrative record with correct fields and scope.

Where to find it Administration → Applications and features → Access roles

Before you start

- Account with platform administration and the area's read/write permissions; organization or branch ownership alone does not grant this authorization. The server decides each operation.

Fields and options

Role key	Required, at most 128 characters; at least two lowercase dot-separated segments. Must start with the application key followed by a dot.
Application / Name / Description	Application and name required; description optional.
Where it can be assigned	Platform, Organization, Branch or Organization or branch. Selection filters compatible permissions.
Role permissions	Load available permissions and select required ones. A platform role accepts platform permissions; organization/branch roles accept their respective scopes; a mixed role accepts Organization or branch permissions.

Step by step

1. Open Applications and features → Access roles. Check filters and select the target organization or application when required.
2. Select New access role and complete the fields described in this table. Correct inline field messages before saving.
3. Review the scope and select Create access role. Wait for confirmation; do not close or repeat while processing.
4. Refresh the list and check the new record name and state. Review duplicate or invalid identifiers according to the server response.

Expected result

The record is created without automatically granting access to all users.

3.9 Edit access role

What it is for Update the existing record while preserving identity and revision.

Where to find it Administration → Applications and features → Access roles → Edit

Before you start

- Account with platform administration and the area's read/write permissions; organization or branch ownership alone does not grant this authorization. The server decides each operation.

Fields and options

Role key	Required, at most 128 characters; at least two lowercase dot-separated segments. Must start with the application key followed by a dot.
Application / Name / Description	Application and name required; description optional.
Where it can be assigned	Platform, Organization, Branch or Organization or branch. Selection filters compatible permissions.
Role permissions	Load available permissions and select required ones. A platform role accepts platform permissions; organization/branch roles accept their respective scopes; a mixed role accepts Organization or branch permissions.

Step by step

1. Find the record, verify its name and select Edit. Review current values before changing them.
2. Change only enabled fields. Do not circumvent locked identifiers or associations. For roles, recheck selected permissions after changing scope.
3. Select Save changes and wait. Cancel abandons editing, with discard confirmation for pending drafts.

4. On version conflict, reload the record and compare current content. Reapply only the necessary change.

Expected result

Allowed fields are updated; server authorization remains enforced.

3.10 Activate, disable or delete access role

What it is for Control record lifecycle without confusing disabling with renaming.

Where to find it Administration → Applications and features → Access roles → Actions

Before you start

- Account with platform administration and the area's read/write permissions; organization or branch ownership alone does not grant this authorization. The server decides each operation.

Step by step

1. Check the row state and open Actions. Activate is eligible for a disabled record; Disable for an active one; Delete is not a new operation for an already deleted record.
2. To disable, select Disable followed by the name and read the access-interruption notice. Confirm Disable only for the correct target.
3. To reactivate, select Activate on the disabled record and check the result. This does not replace reviewing required memberships, permissions or features.
4. To delete, choose Delete and read the irreversible-action confirmation. Cancel if you intended only a temporary interruption. Dependencies or restrictions may cause server rejection.

Expected result

The list reflects the permitted state. This catalog action does not promise physical erasure of personal data.

3.11 Create feature

What it is for Create an administrative record with correct fields and scope.

Where to find it Administration → Applications and features → Features

Before you start

- Account with platform administration and the area's read/write permissions; organization or branch ownership alone does not grant this authorization. The server decides each operation.

Fields and options

Feature key	Required, at most 128 characters; at least two lowercase dot-separated segments with the selected application prefix.
Application / Name / Description	Application and name required; description optional. A record describes an existing capability, not new feature code.

Step by step

1. Open Applications and features → Features. Check filters and select the target organization or application when required.
2. Select New feature and complete the fields described in this table. Correct inline field messages before saving.
3. Review the scope and select Create feature. Wait for confirmation; do not close or repeat while processing.
4. Refresh the list and check the new record name and state. Review duplicate or invalid identifiers according to the server response.

Expected result

The record is created without automatically granting access to all users.

3.12 Edit feature

What it is for Update the existing record while preserving identity and revision.

Where to find it Administration → Applications and features → Features → Edit

Before you start

- Account with platform administration and the area's read/write permissions; organization or branch ownership alone does not grant this authorization. The server decides each operation.

Fields and options

Feature key	Required, at most 128 characters; at least two lowercase dot-separated segments with the selected application prefix.
Application / Name / Description	Application and name required; description optional. A record describes an existing capability, not new feature code.

Step by step

1. Find the record, verify its name and select Edit. Review current values before changing them.
2. Change only enabled fields. Do not circumvent locked identifiers or associations. For roles, recheck selected permissions after changing scope.
3. Select Save changes and wait. Cancel abandons editing, with discard confirmation for pending drafts.
4. On version conflict, reload the record and compare current content. Reapply only the necessary change.

Expected result

Allowed fields are updated; server authorization remains enforced.

3.13 Activate, disable or delete feature

What it is for Control record lifecycle without confusing disabling with renaming.

Where to find it Administration → Applications and features → Features → Actions

Before you start

- Account with platform administration and the area's read/write permissions; organization or branch ownership alone does not grant this authorization. The server decides each operation.

Step by step

1. Check the row state and open Actions. Activate is eligible for a disabled record; Disable for an active one; Delete is not a new operation for an already deleted record.
2. To disable, select Disable followed by the name and read the access-interruption notice. Confirm Disable only for the correct target.
3. To reactivate, select Activate on the disabled record and check the result. This does not replace reviewing required memberships, permissions or features.
4. To delete, choose Delete and read the irreversible-action confirmation. Cancel if you intended only a temporary interruption. Dependencies or restrictions may cause server rejection.

Expected result

The list reflects the permitted state. This catalog action does not promise physical erasure of personal data.

3.14 Create organization

What it is for Create an administrative record with correct fields and scope.

Where to find it Administration → Organizations and branches → Organizations

Before you start

- Account with platform administration and the area's read/write permissions; organization or branch ownership alone does not grant this authorization. The server decides each operation.

Fields and options

Name	Required organization name.
Identifier	Required identifier; the server validates format and availability. It differs from the display name.

Step by step

1. Open Organizations and branches → Organizations. Check filters and select the target organization or application when required.
2. Select New organization and complete the fields described in this table. Correct inline field messages before saving.

3. Review the scope and select Create organization. Wait for confirmation; do not close or repeat while processing.
4. Refresh the list and check the new record name and state. Review duplicate or invalid identifiers according to the server response.

Expected result

The record is created without automatically granting access to all users.

3.15 Edit organization

What it is for Update the existing record while preserving identity and revision.

Where to find it Administration → Organizations and branches → Organizations → Edit

Before you start

- Account with platform administration and the area's read/write permissions; organization or branch ownership alone does not grant this authorization. The server decides each operation.

Fields and options

Name	Required organization name.
Identifier	Required identifier; the server validates format and availability. It differs from the display name.

Step by step

1. Find the record, verify its name and select Edit. Review current values before changing them.
2. Change only enabled fields. Do not circumvent locked identifiers or associations. For roles, recheck selected permissions after changing scope.
3. Select Save changes and wait. Cancel abandons editing, with discard confirmation for pending drafts.
4. On version conflict, reload the record and compare current content. Reapply only the necessary change.

Expected result

Allowed fields are updated; server authorization remains enforced.

3.16 Activate, disable or delete organization

What it is for Control record lifecycle without confusing disabling with renaming.

Where to find it Administration → Organizations and branches → Organizations → Actions

Before you start

- Account with platform administration and the area's read/write permissions; organization or branch ownership alone does not grant this authorization. The server decides each operation.

Step by step

1. Check the row state and open Actions. Activate is eligible for a disabled record; Disable for an active one; Delete is not a new operation for an already deleted record.
2. To disable, select Disable followed by the name and read the access-interruption notice. Confirm Disable only for the correct target.
3. To reactivate, select Activate on the disabled record and check the result. This does not replace reviewing required memberships, permissions or features.
4. To delete, choose Delete and read the irreversible-action confirmation. Cancel if you intended only a temporary interruption. Dependencies or restrictions may cause server rejection.

Expected result

The list reflects the permitted state. This catalog action does not promise physical erasure of personal data.

3.17 Create branch

What it is for Create an administrative record with correct fields and scope.

Where to find it Administration → Organizations and branches → Branches

Before you start

- Account with platform administration and the area's read/write permissions; organization or branch ownership alone does not grant this authorization. The server decides each operation.

Fields and options

Organization	First select the target organization; New branch requires it.
Name / Code	Both required. The code identifies the branch within its organization.

Step by step

1. Open Organizations and branches → Branches. Check filters and select the target organization or application when required.
2. Select New branch and complete the fields described in this table. Correct inline field messages before saving.
3. Review the scope and select Create branch. Wait for confirmation; do not close or repeat while processing.
4. Refresh the list and check the new record name and state. Review duplicate or invalid identifiers according to the server response.

Expected result

The record is created without automatically granting access to all users.

3.18 Edit branch

What it is for Update the existing record while preserving identity and revision.

Where to find it Administration → Organizations and branches → Branches → Edit

Before you start

- Account with platform administration and the area's read/write permissions; organization or branch ownership alone does not grant this authorization. The server decides each operation.

Fields and options

Organization	First select the target organization; New branch requires it.
Name / Code	Both required. The code identifies the branch within its organization.

Step by step

1. Find the record, verify its name and select Edit. Review current values before changing them.
2. Change only enabled fields. Do not circumvent locked identifiers or associations. For roles, recheck selected permissions after changing scope.
3. Select Save changes and wait. Cancel abandons editing, with discard confirmation for pending drafts.
4. On version conflict, reload the record and compare current content. Reapply only the necessary change.

Expected result

Allowed fields are updated; server authorization remains enforced.

3.19 Activate, disable or delete branch

What it is for Control record lifecycle without confusing disabling with renaming.

Where to find it Administration → Organizations and branches → Branches → Actions

Before you start

- Account with platform administration and the area's read/write permissions; organization or branch ownership alone does not grant this authorization. The server decides each operation.

Step by step

1. Check the row state and open Actions. Activate is eligible for a disabled record; Disable for an active one; Delete is not a new operation for an already deleted record.
2. To disable, select Disable followed by the name and read the access-interruption notice. Confirm Disable only for the correct target.
3. To reactivate, select Activate on the disabled record and check the result. This does not replace reviewing required memberships, permissions or features.
4. To delete, choose Delete and read the irreversible-action confirmation. Cancel if you intended only a temporary interruption. Dependencies or restrictions may cause server rejection.

Expected result

The list reflects the permitted state. This catalog action does not promise physical erasure of personal data.

3.20 Create a global user

What it is for Create and maintain identities with verification and security safeguards.

Where to find it Administration → People and access → Users

Before you start

- Account with platform administration and the area's read/write permissions; organization or branch ownership alone does not grant this authorization. The server decides each operation.

Fields and options

Email / Name	Required; valid email. Changing address requires verification.
Initial password / New password	Initial password is optional during creation; if supplied, at least 15 characters. Administrative new password is required, at least 15 characters, with a matching confirmation.

Step by step

1. Locate the person or open New user. Verify identity and authorization before changing someone else's data.
2. Use New user. Enter Email, Name and, if appropriate, Initial password (optional); review and select Create user. Never use real credentials in training material.
3. Wait for completion, refresh and check state/email. Cancel preserves the previous record if no save was confirmed.

Expected result

The global identity is updated; memberships and roles remain separate controls.

3.21 Edit a user and resend activation

What it is for Create and maintain identities with verification and security safeguards.

Where to find it Administration → People and access → Users

Before you start

- Account with platform administration and the area's read/write permissions; organization or branch ownership alone does not grant this authorization. The server decides each operation.

Fields and options

Email / Name	Required; valid email. Changing address requires verification.
--------------	--

Initial password / New password

Initial password is optional during creation; if supplied, at least 15 characters. Administrative new password is required, at least 15 characters, with a matching confirmation.

Step by step

1. Locate the person or open New user. Verify identity and authorization before changing someone else's data.
2. In Edit, update the name or email and save. Changing email requires verification before the person can sign in again. Resend activation is available for eligible accounts.
3. Wait for completion, refresh and check state/email. Cancel preserves the previous record if no save was confirmed.

Expected result

The global identity is updated; memberships and roles remain separate controls.

3.22 Change status and administratively verify email

What it is for Create and maintain identities with verification and security safeguards.

Where to find it Administration → People and access → Users

Before you start

- Account with platform administration and the area's read/write permissions; organization or branch ownership alone does not grant this authorization. The server decides each operation.

Fields and options**Email / Name**

Required; valid email. Changing address requires verification.

Initial password / New password

Initial password is optional during creation; if supplied, at least 15 characters. Administrative new password is required, at least 15 characters, with a matching confirmation.

Step by step

1. Locate the person or open New user. Verify identity and authorization before changing someone else's data.
2. Use status controls or Actions to activate, disable or delete when permitted. Confirm the target and impact. Administrative email confirmation, when available, bypasses the email link and requires additional care.
3. Wait for completion, refresh and check state/email. Cancel preserves the previous record if no save was confirmed.

Expected result

The global identity is updated; memberships and roles remain separate controls.

3.23 Set a new password for a person

What it is for Create and maintain identities with verification and security safeguards.

Where to find it Administration → People and access → Users

Before you start

- Account with platform administration and the area's read/write permissions; organization or branch ownership alone does not grant this authorization. The server decides each operation.

Fields and options

Email / Name	Required; valid email. Changing address requires verification.
Initial password / New password	Initial password is optional during creation; if supplied, at least 15 characters. Administrative new password is required, at least 15 characters, with a matching confirmation.

Step by step

1. Locate the person or open New user. Verify identity and authorization before changing someone else's data.
2. For Set new password, enter New password and Confirm new password, review and choose Save new password. For organization access, choose Manage memberships for the selected person.
3. Wait for completion, refresh and check state/email. Cancel preserves the previous record if no save was confirmed.

Expected result

The global identity is updated; memberships and roles remain separate controls.

3.24 Create and manage user memberships

What it is for Maintain the global structure and users' context memberships.

Where to find it Administration → People and access → User memberships

Before you start

- Account with platform administration and the area's read/write permissions; organization or branch ownership alone does not grant this authorization. The server decides each operation.

Fields and options

User	Person whose memberships will be consulted.
Organization / Branch (optional)	Organization required; without a branch, the operation is organization-scoped.

Step by step

1. In User memberships, select User, review Existing memberships and open Manage membership. Add membership lets you choose an organization and an optional branch.

2. In details, use Create membership if absent, Reactivate membership if disabled, or Disable membership / Delete membership when authorized. Without a branch, the change is organization-scoped.
3. Refresh Existing memberships afterwards and check organization, branch and state. Do not remove membership merely to change a role.

Expected result

Membership is an access control separate from the account and application data.

3.25 Assign user roles

What it is for Grant existing roles in the chosen scope without editing the role catalog.

Where to find it Administration → People and access → User roles

Before you start

- Platform superadministrator for this central screen; own-team role management remains inside the product according to its rights.

Fields and options

Application / Organization	Select the context before loading and saving roles.
/ Branch / User	

Step by step

1. In User roles, select Application, Organization, Branch and User as requested. Review organization and branch roles and use Save roles.
2. Review each description/permission before selecting a role. Organization and branch roles are separate sets.
3. Wait for Save roles and verify the loaded selection. If a user is missing, load More users or check membership in the context.

Expected result

Authorized roles are assigned; the operation does not make the user a platform administrator.

3.26 Enable features for a context

What it is for Control platform enablement and responsibility.

Where to find it Administration → Organizations and branches → Enabled features

Before you start

- Account with platform administration and the area's read/write permissions; organization or branch ownership alone does not grant this authorization. The server decides each operation.

Fields and options

Target	Application/context for features; organization, branch and application for invitations; user for platform administration.
Feature or role selection	Review displayed rights. Feature enablement differs from a person's permissions.

Step by step

1. Select target data and wait for authorized options. Load more options when the list is paginated.
2. In Enabled features, choose the application and requested context. Select Look up enabled features, then Manage features. Select Available features and Save features.
3. Review the target and full set before saving. Confirm when requested and refresh the query to verify the result.

Expected result

IAM applies enablement and assignments subject to server-side controls.

3.27 Send, resend and revoke administrative invitations

What it is for Control platform enablement and responsibility.

Where to find it Administration → People and access → Invitations

Before you start

- Account with platform administration and the area's read/write permissions; organization or branch ownership alone does not grant this authorization. The server decides each operation.

Fields and options

Target	Application/context for features; organization, branch and application for invitations; user for platform administration.
Feature or role selection	Review displayed rights. Feature enablement differs from a person's permissions.

Step by step

1. Select target data and wait for authorized options. Load more options when the list is paginated.
2. In administrative Invitations, select organization/branch, open New invitation and enter email, application and roles. Send invitation, Resend and Revoke affect real messages and access: check every target first.
3. Review the target and full set before saving. Confirm when requested and refresh the query to verify the result.

Expected result

IAM applies enablement and assignments subject to server-side controls.

3.28 Assign platform administrators

What it is for Control platform enablement and responsibility.

Where to find it Administration → People and access → Platform administrators

Before you start

- Account with platform administration and the area's read/write permissions; organization or branch ownership alone does not grant this authorization. The server decides each operation.

Fields and options

Target	Application/context for features; organization, branch and application for invitations; user for platform administration.
Feature or role selection	Review displayed rights. Feature enablement differs from a person's permissions.

Step by step

1. Select target data and wait for authorized options. Load more options when the list is paginated.
2. In Platform administrators, select User, review available administrative roles and select Save administrators. Retain a capable platform owner.
3. Review the target and full set before saving. Confirm when requested and refresh the query to verify the result.

Expected result

IAM applies enablement and assignments subject to server-side controls.

3.29 Manage publisher token

What it is for Manage an application technical credential, distinct from a personal token.

Where to find it Administration → Applications and features → Applications → Actions

Before you start

- Account with platform administration and the area's read/write permissions; organization or branch ownership alone does not grant this authorization. The server decides each operation.

Fields and options

Expiry (local time)	Check the displayed time zone and accepted expiry. Secret replacement requires updating the previous credential's consumer.
----------------------------	---

Step by step

1. In an application record, open Publisher token or Provisioning token. Check the application and local expiry with the displayed time zone.
2. Generate creates a credential; Rotate replaces the previous one and Revoke removes its use. Read the confirmation, store the one-time secret securely and update the affected integration.

3. Close the dialog after transferring the secret to secure storage. Check the authorized integration; never record the secret in manuals or screenshots.

Expected result

These controls are for authorized operators only. This manual contains no keys, tokens or private infrastructure instructions.

3.30 Manage provisioning token

What it is for Manage an application technical credential, distinct from a personal token.

Where to find it Administration → Applications and features → Applications → Actions

Before you start

- Account with platform administration and the area's read/write permissions; organization or branch ownership alone does not grant this authorization. The server decides each operation.

Fields and options

Expiry (local time)	Check the displayed time zone and accepted expiry. Secret replacement requires updating the previous credential's consumer.
----------------------------	---

Step by step

1. In an application record, open Publisher token or Provisioning token. Check the application and local expiry with the displayed time zone.
2. Generate creates a credential; Rotate replaces the previous one and Revoke removes its use. Read the confirmation, store the one-time secret securely and update the affected integration.
3. Close the dialog after transferring the secret to secure storage. Check the authorized integration; never record the secret in manuals or screenshots.

Expected result

These controls are for authorized operators only. This manual contains no keys, tokens or private infrastructure instructions.

3.31 Rotate a signing key

What it is for Recognize advanced administrative operations and their impact.

Where to find it Administration → Platform security → Signing keys

Before you start

- Account with platform administration and the area's read/write permissions; organization or branch ownership alone does not grant this authorization. The server decides each operation.

Step by step

1. In Signing keys, review state and eligibility. For authorized rotation, select Rotate key, review the guidance and confirm Generate and activate new key.

2. Wait for the new active key. The screen shows identifier, state and dates, not private key material. Refresh the list to check the transition.

Expected result

These controls are for authorized operators only. This manual contains no keys, tokens or private infrastructure instructions.

3.32 Retire a key or flag compromise

What it is for Recognize advanced administrative operations and their impact.

Where to find it Administration → Platform security → Signing keys

Before you start

- Account with platform administration and the area's read/write permissions; organization or branch ownership alone does not grant this authorization. The server decides each operation.

Step by step

1. Locate the exact key identifier. States include prepared, active, verify-only, retired and compromised. Read dates and eligibility.
2. Retire is available only for an eligible key. Discard prepared key and Flag compromise are specific lifecycle/incident actions. Compromise may invalidate associated sessions and tokens; never use it as a test.
3. A verify-only key can be retired only after its eligibility date. A prepared key can offer Discard prepared key. Cancel confirmation if unsure of the target.

Expected result

These controls are for authorized operators only. This manual contains no keys, tokens or private infrastructure instructions.

4 Glossary

Organization

Shared workspace grouping people and branches.

Branch

Location or working group within an organization.

Access role

Set of permissions assignable within the allowed scope.

Context

Application, organization and branch used for the current operation.

5 Help and next steps

If an option is missing, check context, permissions and account state. Your manager can review access.

For errors, retain the message and displayed transaction identifier. Never send passwords, email codes, invitation links or tokens to support.

ARHOCH contact: contact@arhoch.com.