



Zbix CRM Administrator Technical Manual

Product release 1.2.0

Zbix Technologies

Documentation edition 1.2.0-r1

28 October 2026

Administration, permission management, automation, security and integration configuration for customer administrators and IT teams.

Use the contents to find a task, then review its prerequisites and expected result. Screenshots show demonstration data and preserve the original interface. Your permissions, organization layouts and enabled capabilities can change the controls you see.

Private review edition. Source-reviewed procedures have not been executed against a CRM installation as part of this documentation project. Platform acceptance and provider configuration require their stated qualification.

Contents

Create and maintain Users	3
Manage Teams and legacy role policies.....	4
Design customer document templates.....	5
Import CSV and Excel records.....	6
Set up authenticator protection	7
Use the Settings hub and preferences.....	9
Configure Pipelines and stages	10
Workflows	11
Approvals.....	13
Blueprints	15
Assignment Rules	16
Business Calendars	17
Sales Cadences	18
SLA Policies	20
Escalation Rules	21
Fields and Layouts.....	22
Module Permissions.....	24
Authentication and sign in architecture	26
Manage sessions and sign out other devices	27
Password change and account recovery	29
Authenticator enrollment and organization MFA policy.....	29
Authorization and permission evaluation	30
Integration interfaces and provider boundaries.....	31
Configure and use the scoped integration API	33
Configure SMTP email delivery	35
Connect Microsoft 365 mail and calendar.....	35
Microsoft synchronization and conflict handling.....	36
Activate and review a self hosted license	37
Renew licenses transfer installations and manage seats	38
Read System Health and verify service readiness	39
Troubleshoot import validation and execution	42
Troubleshoot attachment upload and download	43

Create and maintain Users

Zbix CRM 1.2.0 | Source reviewed | Reviewed 28 October 2026

Users defines CRM identities, their active state and legacy role. Team memberships and a custom module-role assignment add separate access controls. Named-user licensing can constrain creation or reactivation.

Give each person an individual account with the intended level of access.

Before you begin

- An administrator identity; a custom manage-settings grant alone is not identity administration.
- An available licensed seat where enforced.
- The person's approved email, role and team memberships.

Procedure

1. Open Administration > Users and search the email before creating an account.
2. Select Create user. Enter Full name, Email, Role and a suitable Temporary password; choose the active state.
3. Select the intended team memberships where available, then save the user.
4. Open Teams and Module Permissions to review memberships and any explicit module-role assignment. Verify effective access rather than relying on the role name.
5. Provide the sign-in details through your approved secure handover process and direct the person to change the temporary password and enroll MFA when required.
6. For a departing user, review record ownership and background work before deactivating the account. Preserve history and ensure another active administrator remains.

Expected result

The person has an individual identity with deliberate role, membership and activation settings.

Name	Email	Role	Is Active
AD Administrator	admin@zbitextech.com	Admin	Yes
AN Anjali Varma	anjali.varma@zbitextech.com	Sales	Yes
AR Arjun Menon	arjun.menon@zbitextech.com	Manager	Yes
DI Divya Krishnan	divya.krishnan@zbitextech.com	Sales	Yes
FA Fatima Al-Sayed	fatima.alsayed@zbitextech.com	Sales	Yes
ME Meera Suresh	meera.suresh@zbitextech.com	Manager	Yes
MU Muzammil YS	musammilys@zbitextech.com	Admin	Yes
PR Priya Nair	priya.nair@zbitextech.com	Admin	Yes
RA Rahul Pillai	rahul.pillai@zbitextech.com	Sales	Yes

Figure 1 Users list SS-038

Important considerations

- Roles are admin, manager, sales and readonly. A custom module role replaces the action/scope policy instead of adding a union of multiple roles.
- Membership in a team does not itself grant create, edit, export or administrator actions.
- Do not confuse inactive users with inactive Accounts or Products.
- Record reassignment and user deactivation are separate operations.

Troubleshooting

- Seat limit reached: review active named users and License Management.
- User cannot see a module: inspect effective module access, capability and visibility.
- User cannot administer identities: confirm the identity role is admin.
- Cannot deactivate the final administrator: keep an approved active administrator available.

Related knowledge base articles: Manage Teams and legacy role policies; Module Permissions; Activate and review a self-hosted license; Set up authenticator protection.

Manage Teams and legacy role policies

Zbix CRM 1.2.0 | Source reviewed | Reviewed 28 October 2026

Teams group people for record visibility and reporting. A user can belong to several teams and can be a manager in a membership. Team membership and action permissions are evaluated separately.

Organize account coverage and manager visibility without granting unintended administrative actions.

Before you begin

- Administrator identity.
- Active users from the same organization.
- An agreed ownership and team-scope policy.

Procedure

1. Open Administration > Teams & permissions. Review the existing teams before creating another group.
2. Create a team with a descriptive name and save it.
3. Choose the team, add its intended active members, and mark the relevant team managers.
4. Save membership changes and refresh the team details. Resolve a version conflict by reviewing the latest membership rather than overwriting it.
5. Review legacy role permissions and visibility if your organization uses them. Check Module Permissions for users with an explicit custom role because that assignment replaces legacy action/scope policy.
6. Test access through a representative authorized user account during an approved access review.

Expected result

Teams reflect the intended organization structure and effective visibility uses the current memberships.

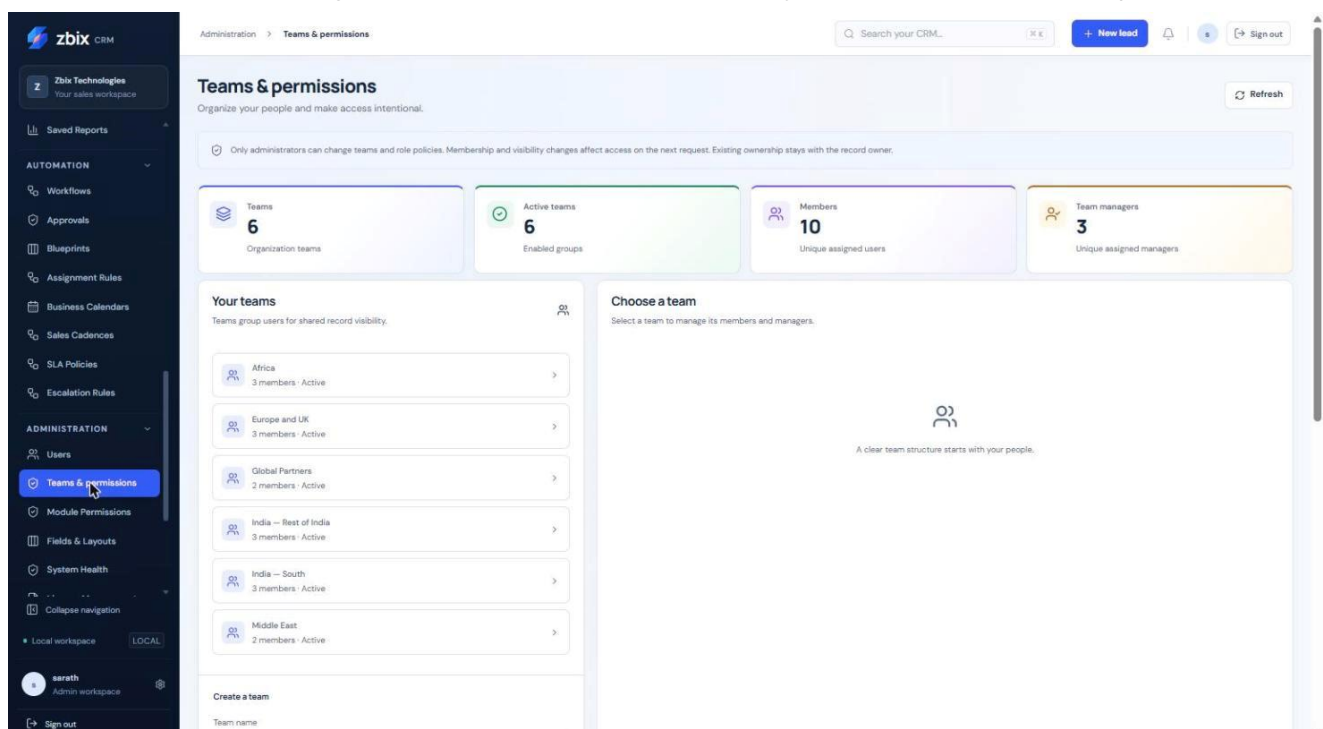


Figure 2 Teams & permissions SS-039

Important considerations

- Existing record ownership stays with the owner when membership changes.
- Multiple team memberships can produce overlapping reporting groups.
- A team manager flag does not turn a user into an administrator.

Troubleshooting

- Member cannot be added: confirm the user is active and belongs to this organization.
- Team records are absent: the module visibility may be own rather than team.
- Totals overlap: do not sum teams as disjoint business units.

Related knowledge base articles: Create and maintain Users; Module Permissions; Analyze performance with Reports.

Design customer document templates

Zbix CRM 1.2.0 | Source reviewed | Reviewed 28 October 2026

Document Templates provides a visual PDF designer for Quotes, Sales Orders and Invoices. The gallery includes Modern Business, Classic Corporate, Minimal and Executive starters, plus a blank-page option.

Create consistent customer-facing documents while preserving already finalized artifacts.

Before you begin

- Document-template management access.
- Approved organization branding and a permitted sample record for preview.
- A clear choice of document type.

Procedure

1. Open Administration > Document Templates and choose Quotes, Sales Orders or Invoices.
2. Select a starter, Blank page or a permitted clone to create a draft.
3. Edit the supported blocks and properties. Arrange their order with the provided controls, and add supported merge fields and validated local image assets.
4. Open Organization branding to maintain approved company information and logos where your permissions allow.
5. Preview against a suitable record. Review long line tables, page breaks, headers, footers and totals before publishing.
6. Publish the version and set it as the default where required. Select the published design on an editable document before finalization.
7. Use history and retirement controls to manage older designs without deleting historical commercial evidence.

Expected result

New documents can use the published design, while finalized artifacts retain their captured version and bytes.

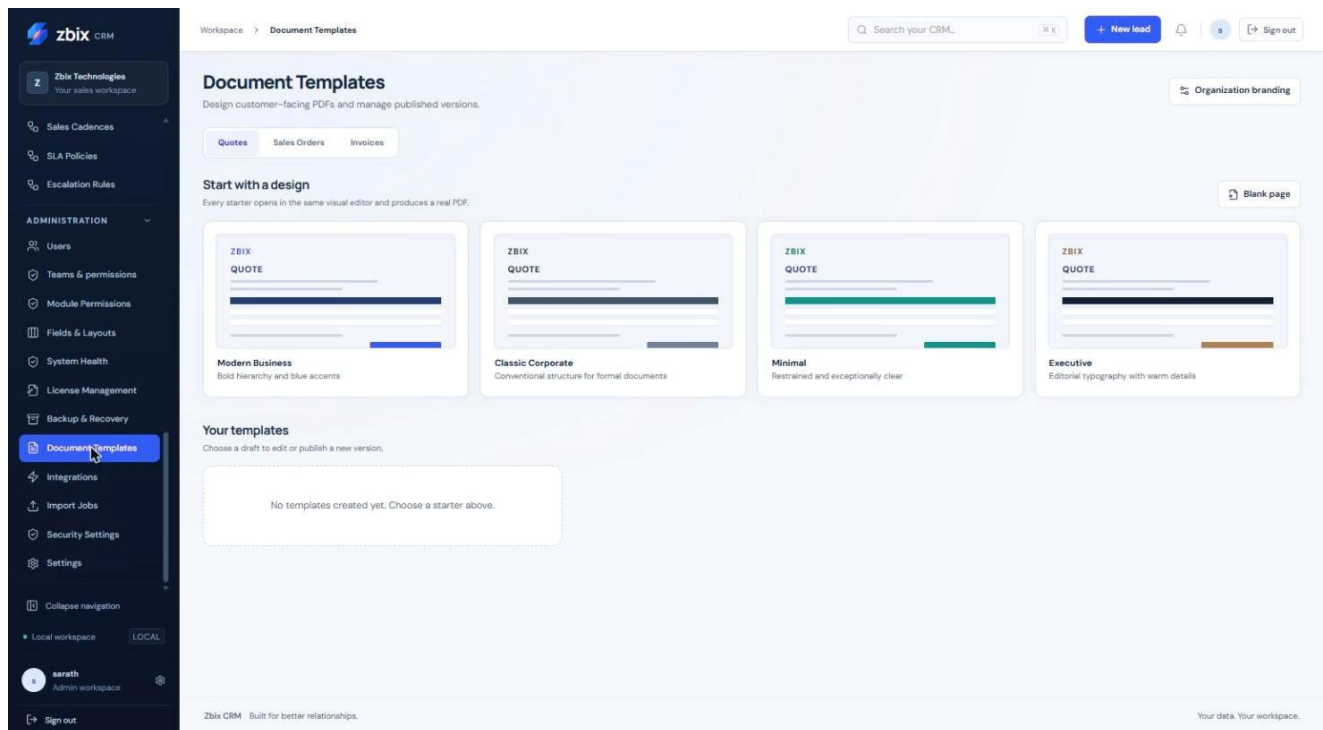


Figure 3 Document template gallery SS-046

Important considerations

- The editor is a constrained document designer; arbitrary HTML, JavaScript and remote resources are not supported.
- Hidden or unauthorized fields cannot be exposed merely by adding a merge field.
- Approved Quotes, confirmed Orders and issued Invoices capture document artifacts. Changing a template does not rewrite those artifacts.
- The supplied capture shows the gallery, not the full editor canvas.

Troubleshooting

- A merge field is rejected: use an allowed field available to the document type and role.
- A logo is missing or distorted: use a validated PNG/JPEG and inspect the preview dimensions.
- Published changes do not alter an old invoice: use the retained historical artifact as intended.

Related knowledge base articles: Prepare and manage Quotes; Create and progress Sales Orders; Issue Invoices and record payments; Fields and Layouts.

Import CSV and Excel records

Zbix CRM 1.2.0 | Source reviewed | Reviewed 28 October 2026

Import Jobs uploads a durable CSV or XLSX source, maps its columns, validates rows and waits for confirmation before importing. Background processing records progress and row outcomes. The original small synchronous import path is separate.

Load a reviewed dataset while identifying validation and duplicate problems before committing records.

Before you begin

- Import access and the required create/edit rights on the target module.
- A clean CSV/XLSX file for a supported module such as Leads, Accounts, Contacts or Products.
- Approved duplicate handling and field mapping.

Procedure

1. Open Administration > Import Jobs and choose Upload import file.
2. Select the target module and source file. Review detected columns and sample rows.
3. Map source columns to supported CRM fields and choose the available duplicate handling policy. Save the mapping to queue validation.

4. Wait for Ready for confirmation. Inspect validation counts and row-level issues; correct the file or mapping if the preview does not match your intention.
5. Confirm the validated import only after review. Monitor processed, successful and rejected rows as the worker commits batches.
6. Download available error results with appropriate export permission. Correct rejected rows in a new source when necessary.
7. If you cancel, verify the terminal state and existing success count before deciding whether retry is appropriate.

Expected result

Validated rows are imported with durable job history and explicit row outcomes.

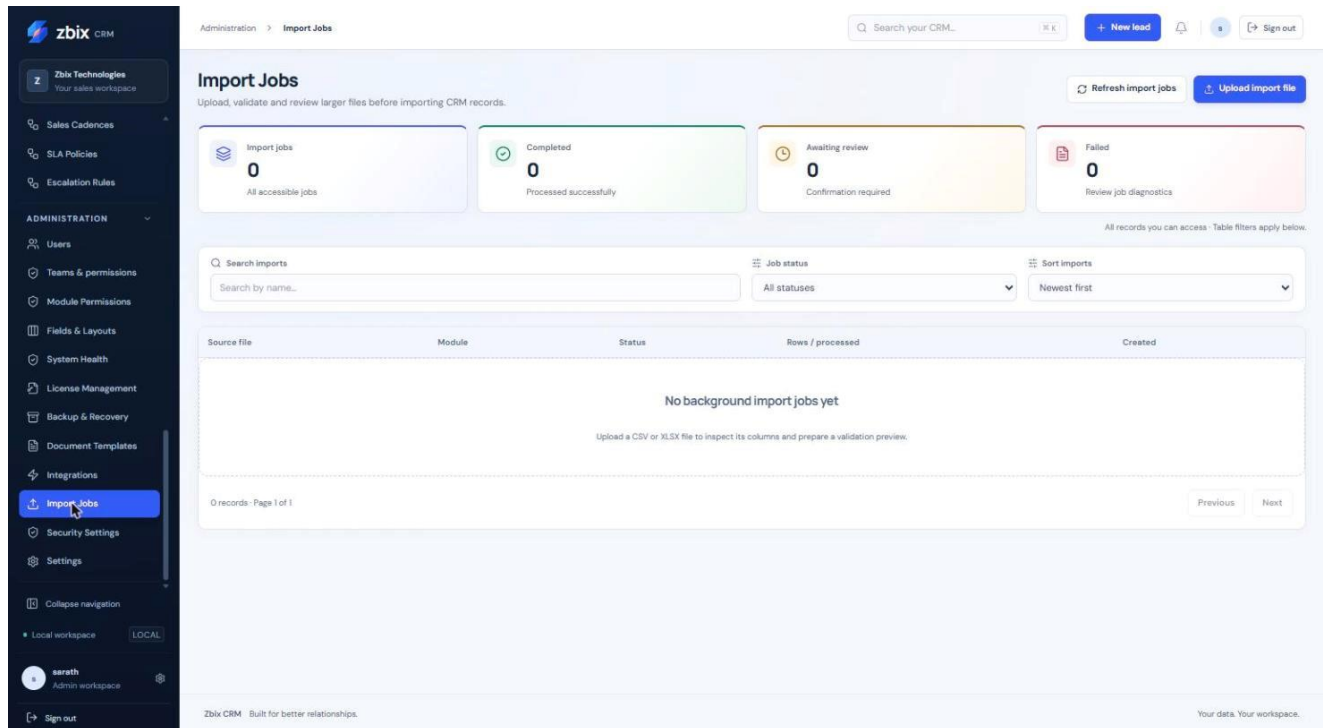


Figure 4 Import jobs (empty) SS-048

Important considerations

- Background imports are bounded to 10000 rows and 50 columns, with the configured upload-byte limit. The legacy synchronous import retains its smaller limit.
- Batches can commit up to 100 rows. Cancellation stops future processing; it does not undo already committed records.
- Changed mapping invalidates the prior preview and requires a new review.
- Completed histories are retained; a completed job cannot simply be reset.

Troubleshooting

- Validation does not progress: inspect worker health.
- Required field errors: check mapping, format and the published custom-field rules.
- Duplicate errors: apply the approved duplicate policy or correct the source.
- Retry risks duplicates: read prior row outcomes and committed counts before resubmitting.

Related knowledge base articles: Create and update CRM records; Manage Leads; Maintain the Products catalog; Read System Health and verify service readiness.

Set up authenticator protection

Zbix CRM 1.2.0 | Source reviewed | Reviewed 28 October 2026

Security Settings manages personal authenticator enrollment and recovery codes. Administrators can configure an organization MFA policy and assist another user with recovery under the required verification controls.

Add a second sign-in factor and retain a controlled recovery path.

Before you begin

- Your current CRM password.
- An authenticator application and a protected place for one-use recovery codes.
- Administrator identity for organization policy or administrator-assisted recovery.

Procedure

1. Open Security Settings and choose Set up authenticator app.
2. Reauthenticate as prompted. Scan the displayed QR code in your authenticator and submit a current code to confirm enrollment.
3. Save the displayed recovery codes in your approved protected location. They are shown only through the designated recovery-code flow.
4. Sign out and sign in again to verify the challenge works.
5. Administrators should check that the affected active users are enrolled before changing the organization policy to require MFA.
6. For a lost factor, use an unused recovery code or contact another administrator. Administrator-assisted reset revokes sessions and requires reenrollment.

Expected result

The account has verified authenticator protection and a known recovery route.

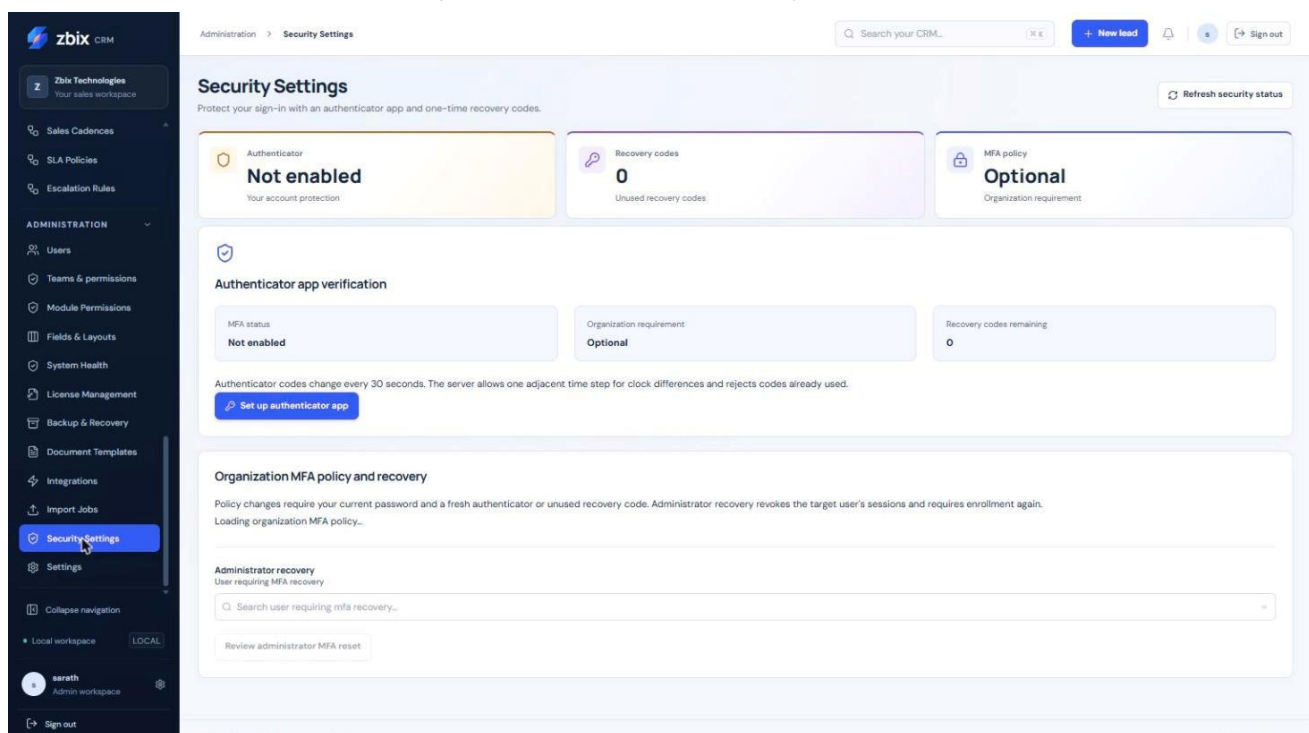


Figure 5 Security settings (MFA) SS-049

Important considerations

- Never place QR codes, setup secrets or recovery codes in a support ticket or screenshot.
- Authenticator codes change on a short time interval. Already-used codes are rejected and adjacent clock steps are bounded.
- Personal MFA enrollment and an organization requirement are separate states.
- The screenshot shows a not-enabled example; it does not establish your current policy.

Troubleshooting

- Code rejected: use a fresh code and check the device clock.
- Policy change blocked: complete the enrollment prerequisites for affected users.
- Recovery required: do not share a code with support; follow the authenticated recovery flow.

Related knowledge base articles: Sign in and manage your session; Create and maintain Users; Use the Settings hub and preferences; Read System Health and verify service readiness.

Use the Settings hub and preferences

Zbix CRM 1.2.0 | Source reviewed | Reviewed 28 October 2026

Settings is a directory of personal and organization configuration. It groups Workspace, CRM configuration, Access & security and Operations links, including preferences, users, teams, pipelines, document templates, email, Microsoft 365, imports, health and backup.

Find the correct configuration page without treating every setting as available to every role.

Before you begin

- An authenticated account.
- The appropriate administrative permissions for organization changes.

Procedure

1. Open Administration > Settings and choose the relevant group.
2. For personal changes, open Personal preferences and review profile, timezone and reminder choices.
3. For access changes, use Users, Teams, Module permissions or Security according to the task.
4. For sales configuration, open Fields & layouts, Pipelines or Document templates.
5. For delivery and operations, open Email & communications, My Microsoft 365 account, Integrations, Import jobs, System health or Backup & Recovery.
6. Save in the destination page and verify its resulting status. Return to Settings for the next configuration area.

Expected result

You reach the specialized configuration screen and can verify the relevant change there.

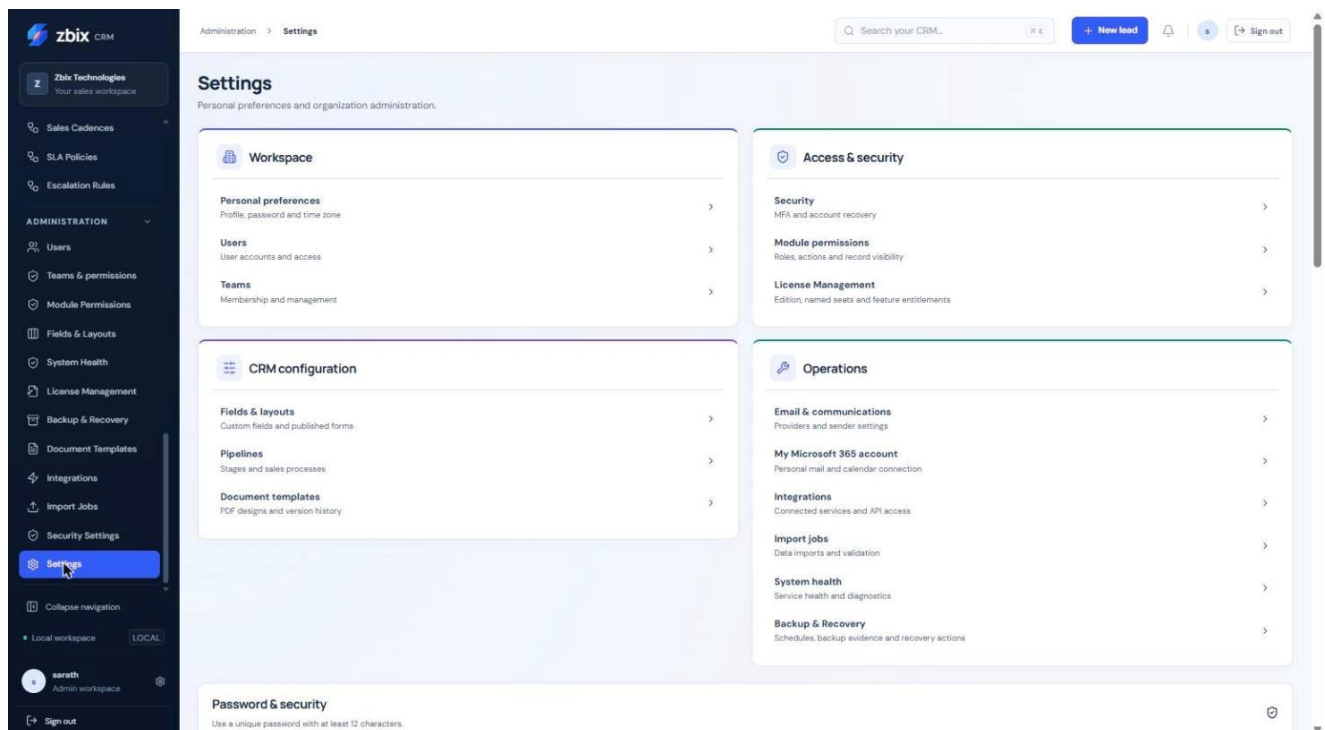


Figure 6 Settings hub SS-050

Important considerations

- The hub links to dedicated pages; it is not a single global Save form.
- A personal Microsoft connection is distinct from the organization's Microsoft application registration.
- Timezone preferences affect display and scheduling inputs, while stored timestamps and some report boundaries use UTC.

Troubleshooting

- A settings link is absent: check identity role, module grants and enabled capability.
- A personal preference appears unchanged: save in the destination page and refresh.
- Unexpected meeting time: compare personal timezone and the meeting's explicit timezone.

Related knowledge base articles: Create and maintain Users; Set up authenticator protection; Configure and use the scoped integration API; Configure Pipelines and stages; Design customer document templates.

Configure Pipelines and stages

Zbix CRM 1.2.0 | Source reviewed | Reviewed 28 October 2026

Pipelines define the ordered stages used by Deals, including probabilities, open/won/lost kinds and information required on stage entry. The demonstration has 12 stages, while a newly created pipeline starts with the standard eight-stage set.

Model the organization's sales process and make forecast probabilities and required information consistent.

Before you begin

- Deal manage-settings permission.
- An approved stage model and awareness of Deals already using the existing pipeline.

Procedure

1. Open Pipelines in the Sales sidebar, or use the Settings shortcut. In this release the breadcrumb reads Automation even though the sidebar placement is Sales.
2. Enter New pipeline name and select Create pipeline, or choose an existing pipeline from Your pipelines.
3. Review Pipeline name, Active pipeline and Default pipeline, then select Save pipeline. The default must remain active.
4. Select Add stage or Edit on an existing stage. Enter Stage name, Stage kind, Stage probability (%), color and active state.
5. Choose the required fields for stage entry: Account, Contact, Amount, expected close date, description, next action or won/lost reason as appropriate. Save the stage.
6. Use the move-up and move-down controls to arrange stages. Review the complete order and retain active open, won and lost stages.
7. Open a permitted Deal in a training/review context and verify the intended stage choices and requirements before adopting the revised process.

Expected result

Deals use stable configured stage identities, while reporting reads the stage kind and probability.

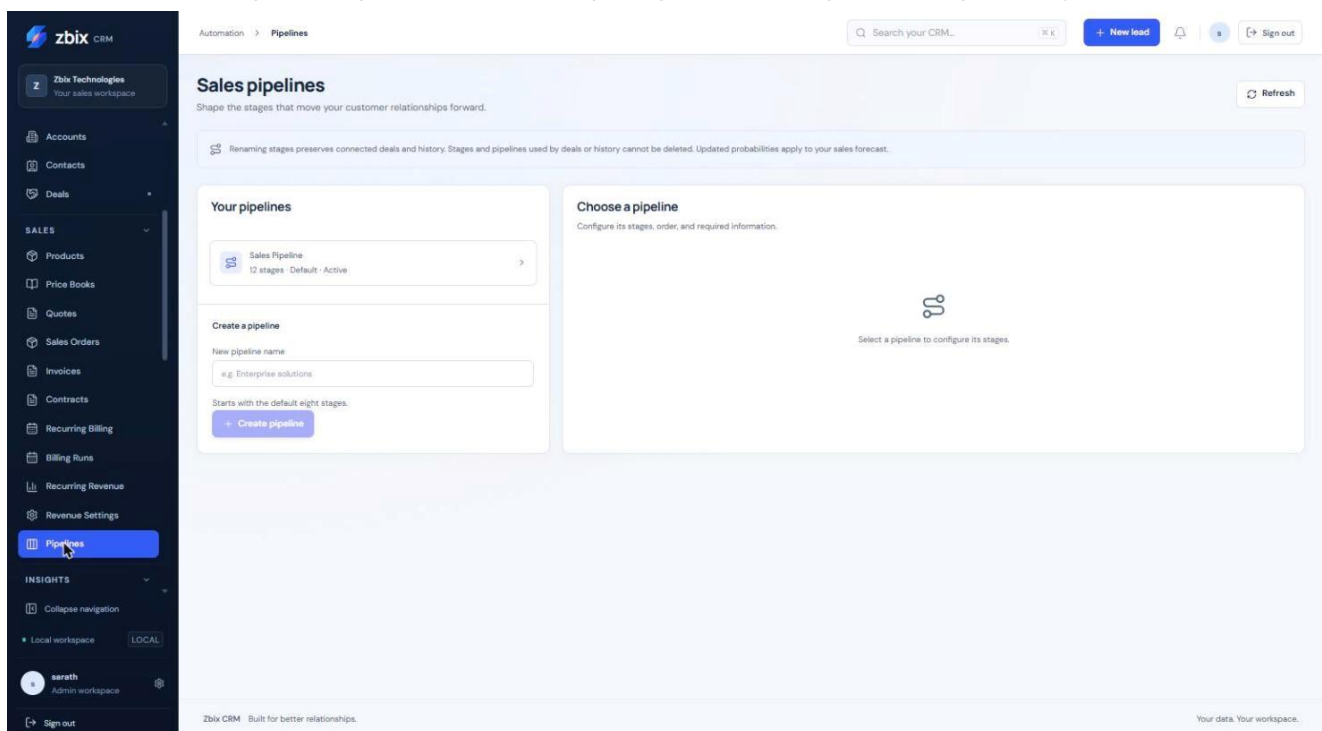


Figure 7 Pipelines overview SS-025

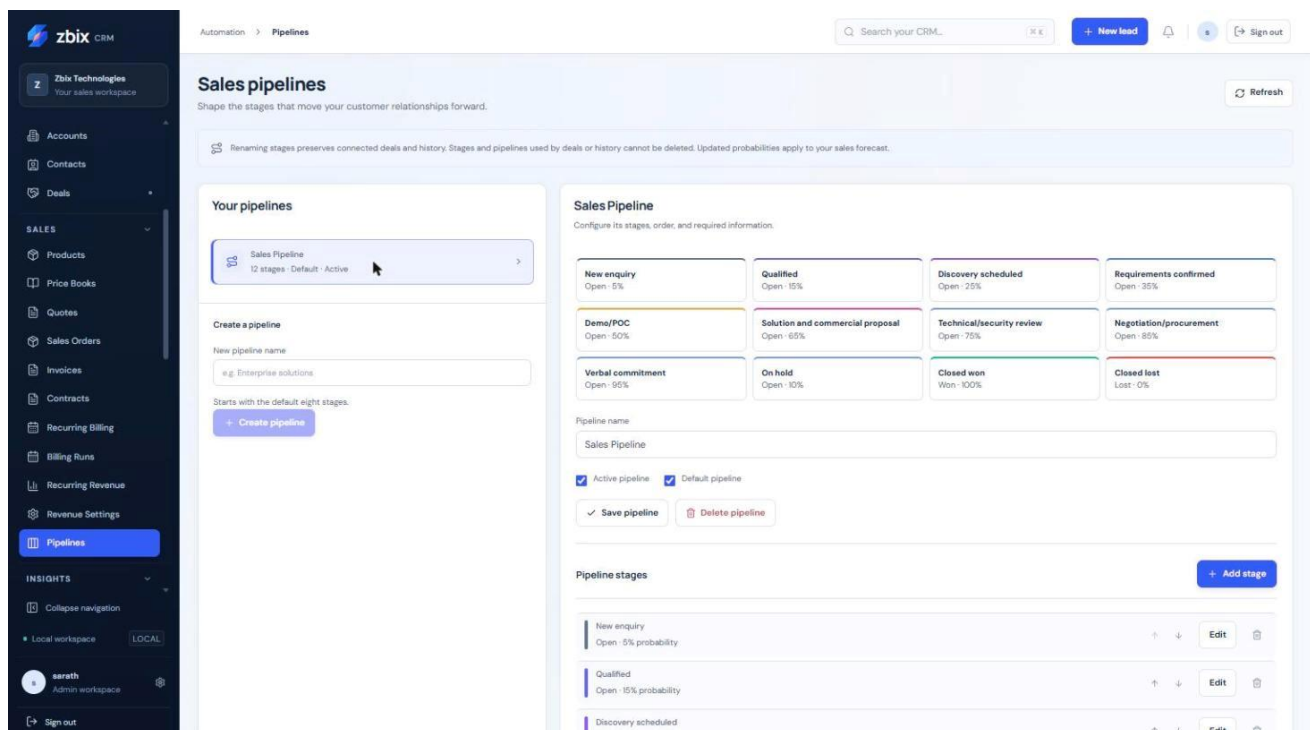


Figure 8 Pipeline stage editor SS-026

Important considerations

- Probabilities range from 0 to 100. Won stages use 100 and lost stages use 0. A pipeline supports at most 50 stages.
- Referenced stages cannot be disabled or have their kind changed. Pipelines/stages used by Deals or history cannot be deleted.
- Renaming preserves existing references and historical labels. Probability changes affect the current forecast.
- A Blueprint may impose additional transition controls beyond these stage requirements.

Troubleshooting

- Cannot delete a stage: it may be referenced by a Deal or history; revise the process without removing that evidence.
- Cannot save the structure: keep active open, won and lost stages and an active default pipeline.
- Concurrent modification: refresh and review the latest stage order before retrying.

Related knowledge base articles: Manage Deals and pipeline stages; Analyze performance with Reports; Blueprints.

Workflows

Zbix CRM 1.2.0 | Source reviewed | Reviewed 28 October 2026

Conditional workflow automation creates versioned rules for Leads, Deals, Accounts and Contacts. Rules evaluate an actual record event and optional conditions, then queue ordered internal actions. Existing simple workflows are shown below the conditional rules and are a separate mechanism.

Use a conditional rule to make follow-up tasks and in-app notifications consistent, or to enroll an eligible Lead or Deal into a published sales cadence. A saved draft has no operational effect until it is published and activated.

Before you begin

- The deployment must enable conditional automation and the user must be allowed to view and manage Workflows, with the create or edit action for the change.
- The triggering user and action recipients must retain access to the source record. Task creation also requires applicable Activity permissions and required task fields.

Procedure

1. Open Automation > Workflows. Under Conditional workflow automation, select Create conditional rule.
2. Select Module and enter Rule name. Select Workflow trigger. The catalog offers triggers appropriate to the module, including Record created, Status changes, Deal stage changed, Deal owner changed and Selected fields changed.

- For a Deal stage trigger, select Pipeline and To stage; optionally restrict From stage. For Selected fields changed, select the fields that must actually change. For a Lead status rule, choose Target status and decide whether Also match Leads created in this status should be enabled.
- Enable Require conditions if necessary. Build the allowed field predicates and AND/OR groups. Review the plain-language condition summary. Deal amount predicates need the matching currency equality in each branch.
- Enter Elapsed delay (minutes), Task due-date timezone and whether to Recheck status and conditions before actions.
- Add task action, Add notification action, or, for Leads and Deals when available, Add cadence enrollment. Enter titles and the required action details. Select the current owner, triggering user or explicit authorized user as recipient. Arrange the action order with Move action up.
- Use Read-only condition check with an Authorized source record ID and select Explain conditions without actions. This evaluates conditions without creating tasks or notifications.
- Select Save conditional draft. Review the saved definition, select Publish saved draft, then Activate published rule.
- After a qualifying record event, select History for the rule. Inspect status, pinned version, source record, action outcomes, attempts and next retry. Open a created task through its link.

Expected result

A matching event produces a durable execution linked to the published rule version. The worker applies the action group using current permissions. History separates successful, failed, waiting and cancelled execution outcomes.

Fields and controls

Field or control	Rule
Rule name	Required; maximum 200 characters
Elapsed delay	0-525,600 minutes
Conditions	Maximum 24 nodes; depth 3; 10 rules per group
Ordered actions	Maximum 5
Task due calendar days	0-365
Notification message	Maximum 1,000 characters

The screenshot displays the 'Workflows' section of the Zbix CRM interface. The left sidebar contains navigation links for Invoices, Contracts, Recurring Billing, Billing Runs, Recurring Revenue, Revenue Settings, Pipelines, Reports, Saved Reports, and Automation. The 'Automation' section is expanded, showing 'Workflows' as the active item. The main content area is titled 'Workflows' and 'Manage CRM automation rules.' It features a 'Conditional workflow automation' section with a summary of rule counts: 1 Conditional rule (Accessible versioned rules), 0 Active rules (Enabled definitions), 1 Draft rule (Unpublished definitions), and 0 Inactive rules (Disabled definitions). Below this is a search and filter section for conditional rules, including a search bar, a 'Create conditional rule' button, and filters for Module (All modules), Status (All states), and Sort (name). A table lists the rules, with one rule 'Lead Contacted - Create Follow-up Task (DEMO)' in 'Draft' status. The table columns include Name, Module / draft trigger, Status, Published version, Last attempt / success, Executions / failures, and Actions. At the bottom, there is a section for 'All workflows' with a search bar and a 'Create workflow' button.

Figure 9 Conditional workflows & legacy rules SS-029

Important considerations

- At most five ordered actions are allowed. Conditions are bounded to 24 nodes, depth three and ten conditions per group; related-record conditions are unavailable.
- Delay is elapsed time. Task due days are calendar days in the selected timezone, not business days. Zero delay still queues the worker.
- Task titles allow up to 200 characters; task descriptions up to 2,000; notification messages up to 1,000. Delay is 0-525,600 minutes and task due days 0-365.
- One failed internal action rolls back the action group. An unchanged field does not create a new event. Subsequent genuine transitions do.
- Publishing does not rewrite pending executions. Deactivate and cancel pending cancels pending work. Cadence enrollment references the selected immutable version and retains an already-open enrollment.
- These workflow actions do not send arbitrary external HTTP requests, execute scripts or deliver external email.

Troubleshooting

- Rule does not run: verify publication, activation, the actual triggering change and condition result, then inspect execution history and worker health.
- Execution fails after an access change: review the triggering user, source-record visibility, recipients and Activity required fields.
- A version conflict preserves unsaved editor inputs: use Edit to reload deliberately, then reapply the intended change before publishing.

Related knowledge base articles: Sales Cadences; Record tasks calls and meetings; Review notifications and scheduled jobs; Read System Health and verify service readiness.

Approvals

Zbix CRM 1.2.0 | Source reviewed | Reviewed 28 October 2026

Approvals provide a sequential review process for Deals. Each request pins a submitted business snapshot, policy version and intended purpose. The Approvals workspace separates My Approvals, My Requests and Approval History; users with configuration rights also see Approval Policies and All Requests.

Use approvals when a Deal or a protected Blueprint transition requires a recorded decision. Approval is tied to the submitted state; editing the Deal cannot silently carry an older authorization into a changed transaction.

Before you begin

- Process automation is enabled. The requester can view and edit the Deal and can use an applicable active policy.
- Approvers must be currently assigned, active, have Deal approve permission and be authorized for the Deal and required fields. The submitter cannot decide their own request.
- Policy administrators need Workflows view and manage_settings plus appropriate create/edit rights.

Procedure

1. To configure a policy, open Approvals > Approval Policies and select Create approval policy. Enter Process name, optional Pipeline and Description. Approval policies use the Deals module.
2. Set Eligibility conditions. Add one to ten Sequential approval levels. Name each level and choose a Named user or Explicit CRM role. A role level can be decided by one eligible assigned member; it is not a quorum vote.
3. Choose whether to Require comments for approval decisions. Select Save process draft, Validate saved draft, Publish saved draft and Activate published process.
4. To submit a Deal, open its Business process panel. Choose Approval policy and Resubmission cycle, then Submit for Approval. For a protected transition use Request approval for the named transition.
5. In My Approvals, search or filter the requests and select Review request. Inspect Submitted values, the requester, policy, record version and Sequential approval steps.
6. Enter a Decision reason. Select Approve current level, Reject request or Return for changes. Rejection and return require a reason. The requester can use Cancel request with a reason.
7. Follow Decision history. If returned or superseded, update the Deal and submit a new linked cycle. If approval protects a transition, return to the Deal and perform that exact transition against the approved version.

Expected result

The request records each decision and advances one level at a time. A completed approval can authorize only its matching, current purpose. The transition consumes that authorization once.

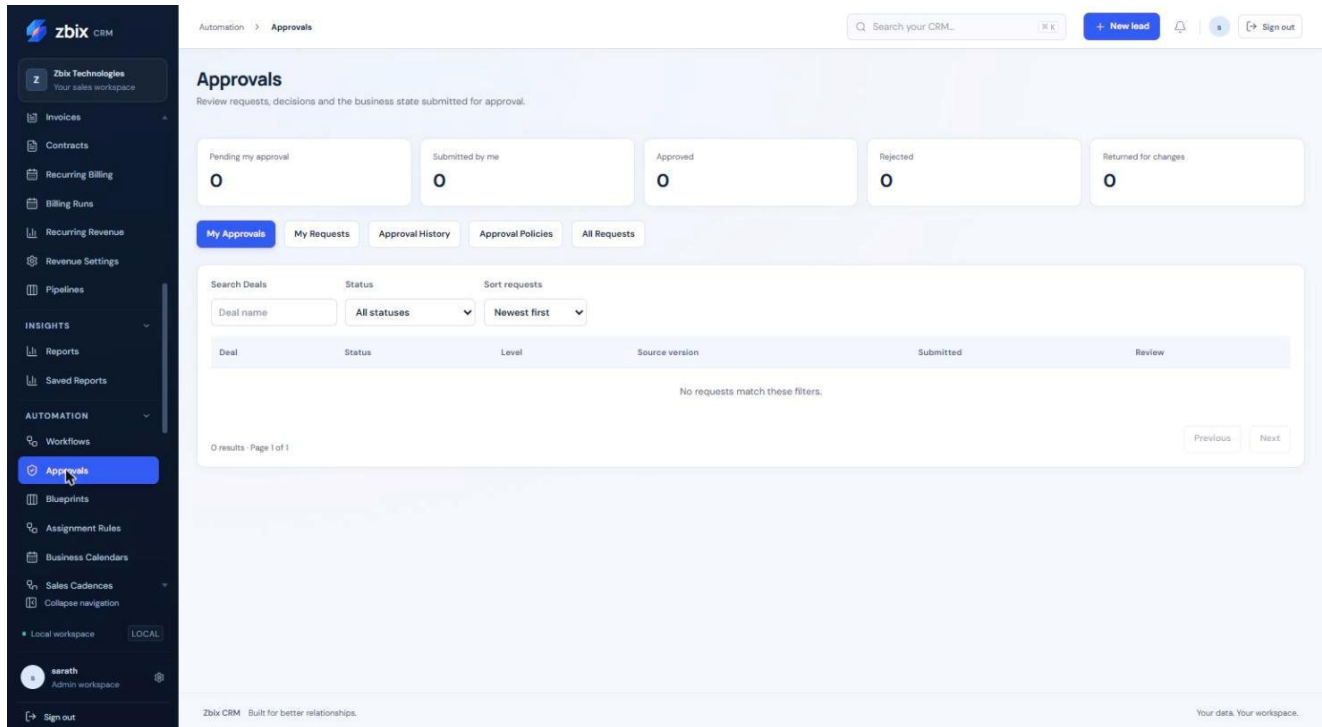


Figure 10 My Approvals tab SS-030

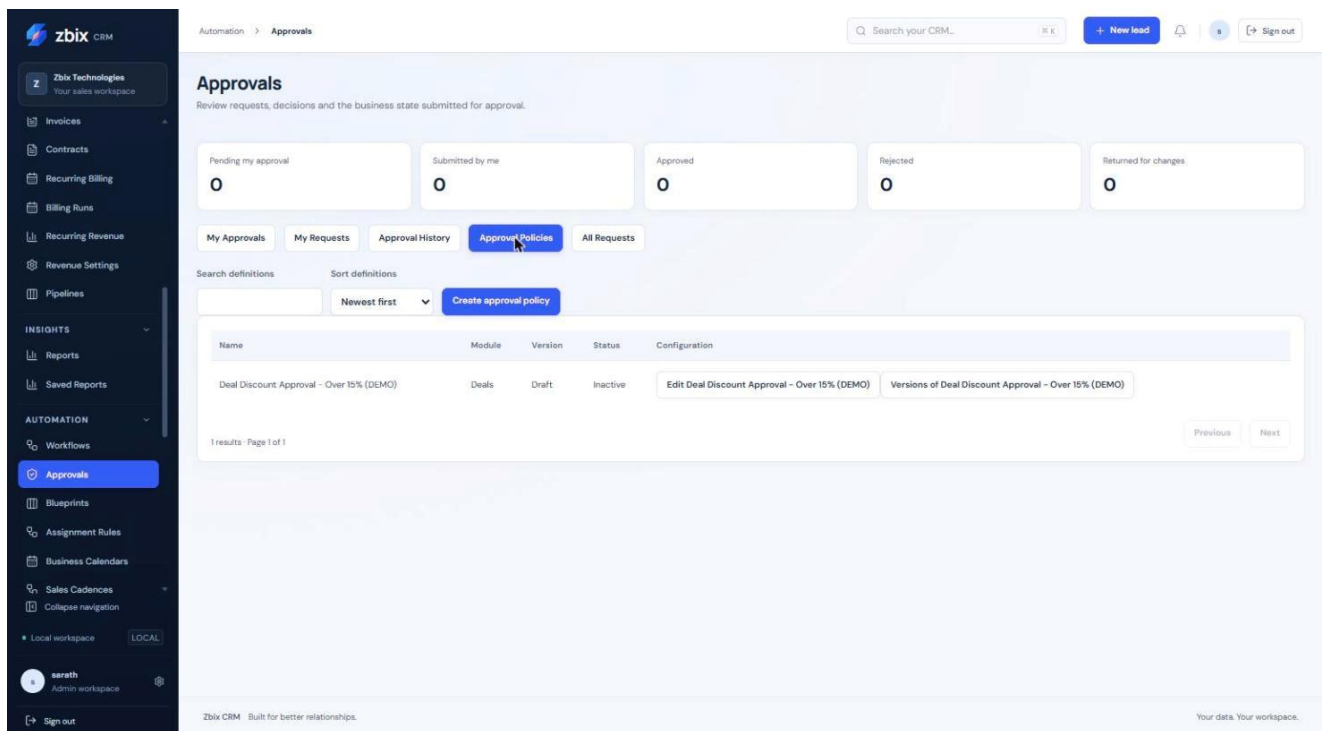


Figure 11 Approval Policies tab SS-031

Important considerations

- A stale snapshot cannot authorize a transition. Source edits invalidate old pending or approved authorization.
- No administrator fallback allows self-approval or substitutes for an unavailable eligible approver.
- Current configurable approvals are Deal policies. Existing commercial Quote approval is a different mechanism.
- Parallel approvals, quorum voting and inferred manager hierarchies are not exposed. Decision reasons are limited to 2,000 characters.

Troubleshooting

- No eligible approver: repair the selected user or explicit role membership and source/field permissions, or have the requester cancel; do not assume an administrator override.
- Source changed: review the current Deal and submit a fresh cycle. Do not retry a stale approval as if its snapshot were current.

- A decision button is missing: verify that the request is pending at your level and that you are not its submitter.

Related knowledge base articles: Blueprints; Manage Deals and pipeline stages; Module Permissions.

Blueprints

Zbix CRM 1.2.0 | Source reviewed | Reviewed 28 October 2026

Blueprints govern actual Lead statuses and Deal pipeline stages through named, authorized transitions. A Blueprint defines who may perform each transition, its required inputs and preconditions, and whether a Deal transition also needs approval.

Use a Blueprint to enforce a repeatable sales process at the record boundary. The control also applies to supported direct, bulk and import paths, so a board move cannot bypass a governed transition.

Before you begin

- Process automation is enabled; administrators have Workflows view/manage_settings and create/edit rights.
- A Deal Blueprint needs an active pipeline. Its transitions must reference real distinct states. Users performing transitions need current record edit access and the configured performer membership.

Procedure

1. Open Automation > Blueprints and select Create Blueprint.
2. Enter Process name, Module and Description. For Deals, select Pipeline before saving; module and pipeline are fixed after creation.
3. Set Eligibility conditions. Select Add transition and enter Transition name, From state and To state.
4. Select each Performer as a Named user or Explicit CRM role. Add any Required fields, Transition preconditions and Require transition comment. For Deals, optionally choose a Required approval policy.
5. Select Save process draft, Validate saved draft, Publish saved draft and Activate published process. Use Versions of the definition to review immutable versions and configuration history.
6. Open a governed Lead or Deal. In Business process, choose an available transition. If required, save the Deal inputs first and request approval for that transition.
7. Complete the required inputs and Transition comment in the dialog, then select Complete transition. Review the new business state and Process history.

Expected result

The record moves through a permitted transition with a recorded history entry. It retains the Blueprint version to which it was enrolled.

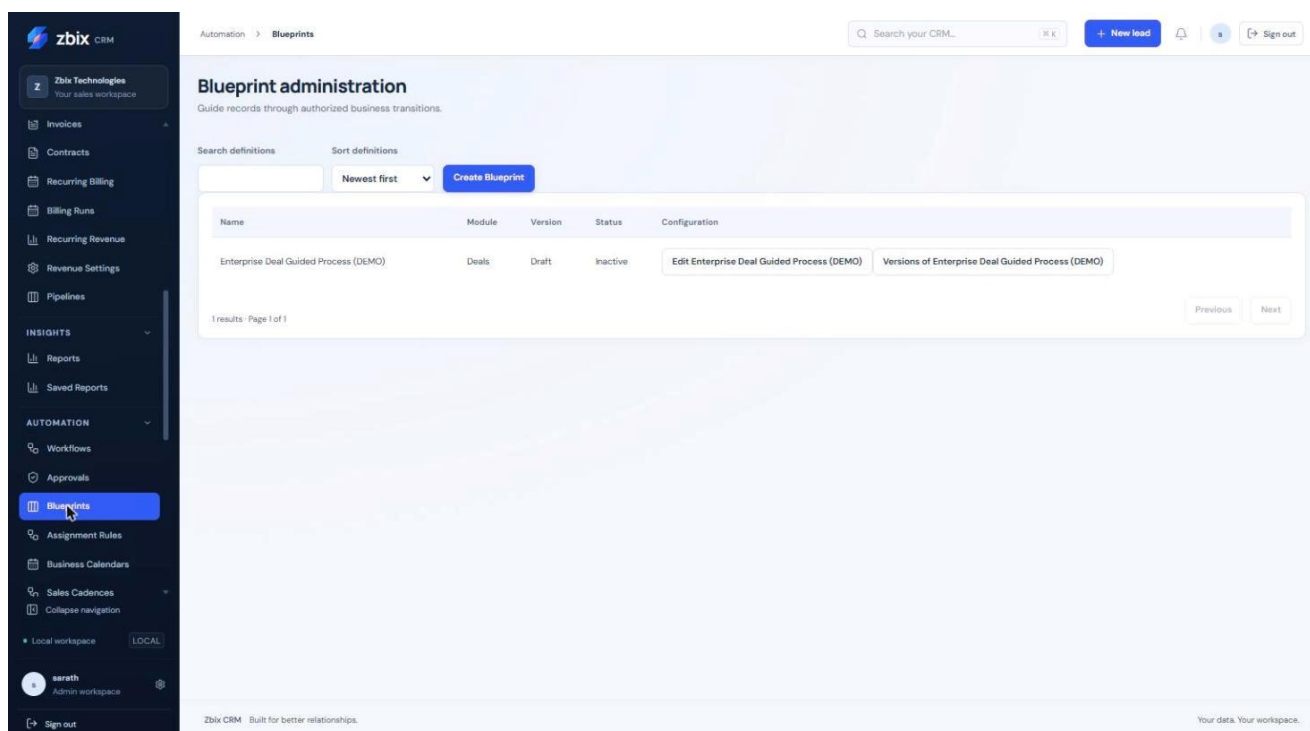


Figure 12 Blueprint administration SS-032

Important considerations

- Existing records enroll on their first authorized save or transition. Already enrolled records retain their version after deactivation; publishing a new version does not migrate them.
- A matching new record must start in a configured entry state. Root source states are the default; cyclic graphs need explicit entry-state configuration through the API.
- Only one active Blueprint may govern the same scope. The UI allows at most 40 transitions and 20 performers per transition.
- Existing pipeline forward/reopen/lost-state rules still apply. A graph edge does not override them.
- Lead conversion remains blocked while a Lead is governed. Multiselect transition inputs are unsupported.

Troubleshooting

- Direct status or stage edit is rejected: use the named Business process transition.
- Transition is unavailable: check current state, performer membership, eligibility/preconditions and current field access.
- Approval cannot authorize the action: confirm the policy, Blueprint version, transition and Deal version all match the approved request.

Related knowledge base articles: Approvals; Configure Pipelines and stages; Manage Leads; Manage Deals and pipeline stages.

Assignment Rules

Zbix CRM 1.2.0 | Source reviewed | Reviewed 28 October 2026

Assignment Rules distribute new Leads and Deals to authorized representatives. Named-user, ordered round-robin and team round-robin strategies are supported. A rule can run on record creation or through an explicit reassignment command.

Use assignment rules for consistent intake ownership while keeping explicit record owners authoritative.

Before you begin

- Sales automation is enabled. Configuration requires Workflows management access and assign/view access to the target module.
- Recipients belong to the same organization; a team strategy requires an active team. Runtime allocation checks current eligibility.

Procedure

1. Open Automation > Assignment Rules and select Create rule.
2. Enter Name and choose Module. Set Priority (lower first). Select Named user, Round-robin or Team round-robin.
3. For a named user, select one recipient. For round-robin, select recipients in allocation order. For a team, choose Team.
4. Choose Record created or Explicit reassignment command as Trigger. Add Eligibility conditions when the rule should target only part of the intake.
5. Select Save draft, Publish saved draft and Activate published version. Use Preview published allocation order to inspect the pool without allocating a record.
6. For a manual rule, open a Lead or Deal and use Apply manual assignment rule in Assignment history. Review the previous owner, new owner, rule version and result.

Expected result

The first matching rule by priority assigns the record to an eligible recipient. Assignment history records committed outcomes.

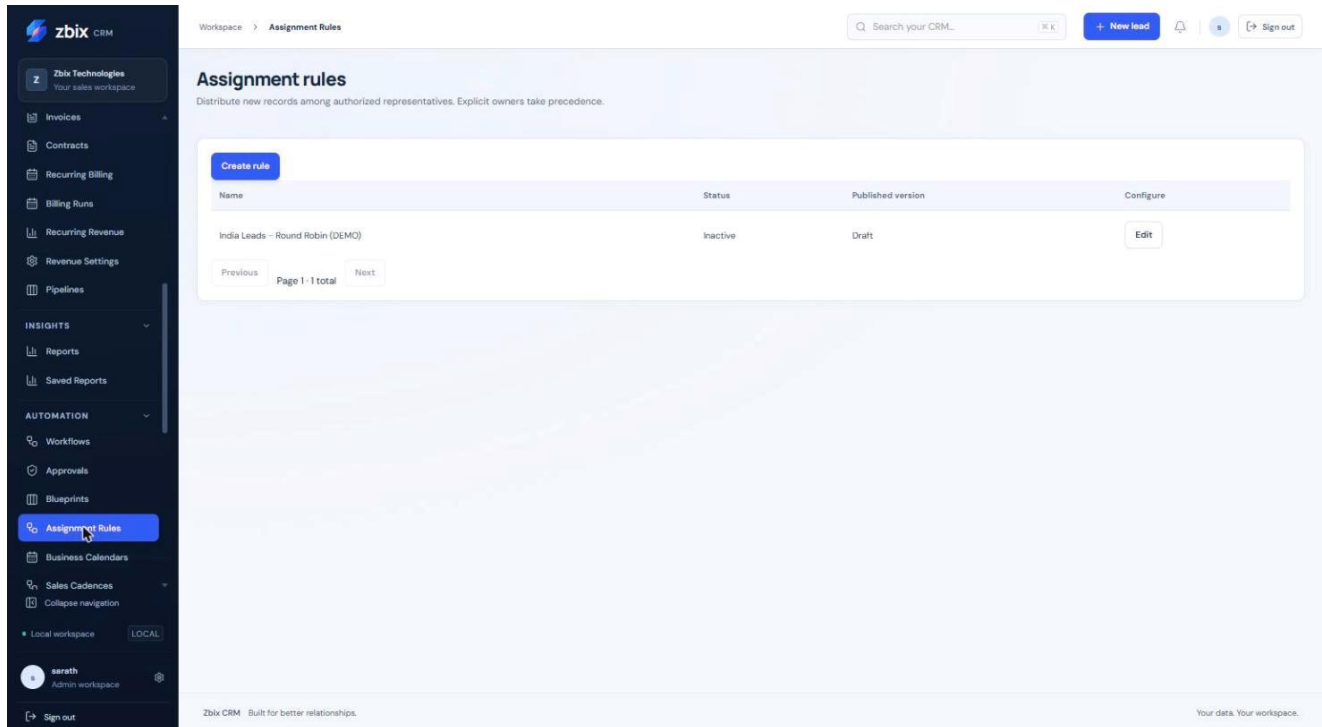


Figure 13 Assignment rules list SS-033

Important considerations

- Explicit owners take precedence. If nobody qualifies, the configured fallback retains the existing owner; this does not create an unassigned queue.
- Priority ranges from 0 to 10,000. Duplicate recipients are rejected; a named strategy requires exactly one user and round-robin requires a nonempty pool.
- No weighted, workload-aware or availability-based routing is claimed. A preview is not a committed allocation.
- Module is fixed after the initial save. Published versions are retained separately from draft edits.

Troubleshooting

- Unexpected owner: check whether creation specified an owner, rule priority and the matching condition set.
- No recipient qualifies: review active team membership, module grants and record visibility, then inspect the rule version.
- Conflict on manual assignment: reload the record so the command uses its current version.

Related knowledge base articles: Manage Teams and legacy role policies; Module Permissions; Manage Leads; Manage Deals and pipeline stages.

Business Calendars

Zbix CRM 1.2.0 | Source reviewed | Reviewed 28 October 2026

Business Calendars define working intervals in an IANA timezone, holidays, closures and dated exceptions. Sales cadences and SLA policies reference a published calendar version so their deadlines remain reproducible.

Use a calendar when a response commitment or follow-up delay should count working time rather than elapsed clock time.

Before you begin

- Sales automation is enabled and the user can manage Workflows.
- Choose the organization's approved working timezone and intervals before publishing.

Procedure

1. Open Automation > Business Calendars and select Create calendar. Enter Name and IANA timezone.
2. Enter Minutes per business day for calculations expressed in business days. Optionally set Effective from and Effective until; the latter is inclusive.
3. For each weekday, use Add interval and enter Start and End in HH:MM format. Use Remove interval to make a day nonworking.

4. In Holidays and closures choose Closed date and Add closure. For a special working date, enter Exception start and Exception end and select Add working exception interval.
5. In Deadline preview, enter a Start timestamp with UTC offset and Business minutes, then select Preview deadline. Check Due and Next working time.
6. Select Save draft, Publish saved draft and Activate published version. In a cadence or SLA select the intended Calendar version explicitly. Review Version history before replacing an existing reference.

Expected result

The published calendar provides bounded, server-calculated working deadlines. Existing references remain tied to the selected version.

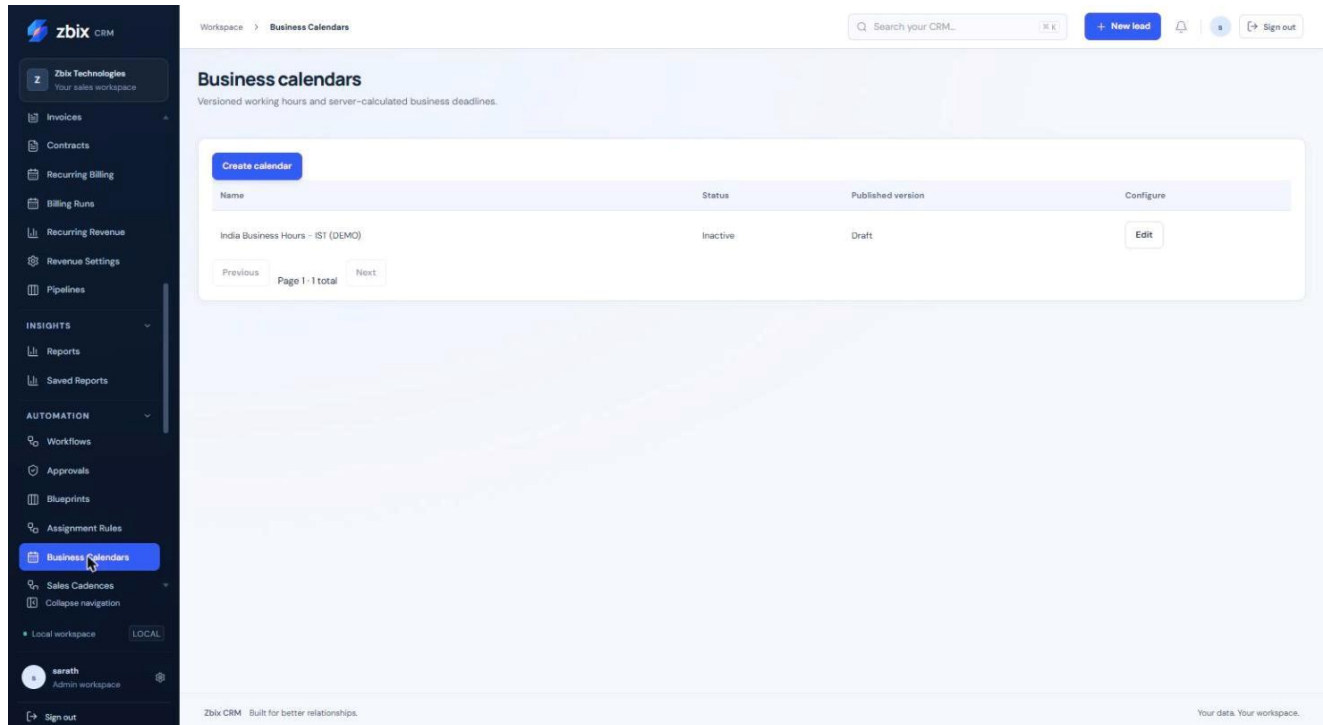


Figure 14 Business calendars list SS-034

Important considerations

- Intervals must be ordered, nonoverlapping and contained in one local date. Split an overnight shift across its two dates.
- At least one weekly working interval is required; at most eight intervals per date and 1,000 exceptions are accepted.
- Minutes per business day must be 1-1,440. The calendar calculation horizon is ten years.
- Dated exceptions replace that date's weekly schedule. No automatic public-holiday feed or inferred team/user calendar is provided.
- The default editor values are examples to review, not a statement of the organization's business hours.

Troubleshooting

- Unknown timezone: use a valid IANA identifier such as Africa/Kampala.
- No working instant or deadline exceeds horizon: check effective dates, closures and available weekly intervals.
- Unexpected deadline across a clock change: inspect the timezone and actual working intervals; calculations resolve local boundaries to actual instants.

Related knowledge base articles: Sales Cadences; SLA Policies; Escalation Rules.

Sales Cadences

Zbix CRM 1.2.0 | Source reviewed | Reviewed 28 October 2026

Sales Cadences run an ordered sequence of internal tasks, in-app notifications and waits for Leads or Deals. Enrollment is stored separately from the definition, and each instance records its progress and pinned version.

Use cadences for a repeatable new-lead or Deal follow-up sequence, with optional completion gates and business-time delays.

Before you begin

- Sales automation and Workflows configuration rights are available.
- Business-time steps require a published calendar version. Task creation and enrollment require current source and Activity permissions.

Procedure

1. Open Automation > Sales Cadences and select Create cadence. Enter Name and Module.
2. Choose Calendar version when using business time. Set Owner changes to Pause for review or Use new owner for future actions.
3. Configure Eligibility conditions. Enable Explicitly enroll matching new records on creation only when all matching new records should enter automatically.
4. For each step choose Create task, In-app notification or Wait, enter Title and Delay after preceding step (minutes), and optionally enable Use business time.
5. For task steps, enable Wait for this task to be completed when the next step must wait for a recorded task completion. Use Move up, Remove and Add step to order the sequence.
6. Select Save draft, Validate saved draft, Publish saved draft and Activate published version.
7. To enroll an existing record, open its Sales automation activity panel, select Cadence and Enroll. The conditional workflow editor can also enroll a pinned published cadence version.
8. Monitor Sales automation activity. Filter Status, inspect History and follow View task links. Use Pause, Resume or Stop when appropriate and authorized.

Expected result

An enrollment advances through the stored steps. Task completion gates display Awaiting task completion and resume only when the qualifying task completion is recorded.

The screenshot displays the Zbix CRM interface. On the left is a dark sidebar with navigation options: Invoices, Contracts, Recurring Billing, Billing Runs, Recurring Revenue, Revenue Settings, Pipelines, INSIGHTS (Reports, Saved Reports), AUTOMATION (Workflows, Approvals, Blueprints, Assignment Rules, Business Calendars, Sales Cadences), and Local workspace. The 'Sales Cadences' menu item is highlighted. The main content area is titled 'Sales cadences' with a subtitle 'Configure versioned internal sales follow-up and monitor persisted execution.' It features a 'Create cadence' button and a table with columns: Name, Status, Version, and Configure. A single row is visible: 'New Lead Follow-up Cadence (DEMO)' with status 'Inactive' and version '0'. Below this is a 'Sales automation activity' section with a 'Status' dropdown set to 'All' and a table with columns: Record, Kind, Status, Due, and Actions. The table shows '0 enrollments'. The footer includes 'Zbix CRM Built for better relationships.' and 'Your data. Your workspace.'

Figure 15 Sales cadences & automation activity SS-035

Important considerations

- A cadence has 1-30 steps. Delay is 0-525,600 minutes. Only task steps can have a completion gate.
- Business-time steps require a published calendar; elapsed-time steps do not. A newly published definition does not rewrite an existing instance.
- These steps create internal CRM tasks and notifications; they do not constitute an external email or SMS campaign.
- Owner changes follow the chosen policy for future actions. Stop is different from Pause: it ends the instance.
- Closed-record exit and current authorization are checked by runtime execution. Monitor the worker as well as the instance status.

Troubleshooting

- Awaiting task completion persists: open the linked task and verify its actual Completed state.
- Enrollment fails: check eligibility, module, source access and any existing open enrollment.
- No step executes: inspect History, due time, paused status, calendar version and System Health worker status.

Related knowledge base articles: Workflows; Business Calendars; Record tasks calls and meetings; Read System Health and verify service readiness.

SLA Policies

Zbix CRM 1.2.0 | Source reviewed | Reviewed 28 October 2026

SLA policies measure an initial response commitment on eligible new Leads or Deals. A business calendar determines the deadline; an eligible completed CRM activity satisfies the commitment.

Use a policy to track first-response timeliness and expose overdue work. Recording an activity is not evidence that a real customer interaction occurred.

Before you begin

- Sales automation is enabled and the user can manage Workflows.
- A published Business Calendar version exists. Choose the activity types that count as response evidence.

Procedure

1. Open Automation > SLA Policies and select Create sla. Enter Name and Module.
2. Choose Calendar version. Set Owner changes to Pause for review or Use new owner for future actions.
3. Configure Eligibility conditions, Target business minutes and Priority. Select at least one Qualifying completed activity type: call, meeting, visit or task.
4. Select Save draft, Validate saved draft, Publish saved draft and Activate published version.
5. After eligible record creation, inspect the SLA instance under Sales automation activity. Open or create the appropriate related activity and record completion when the work is actually finished.
6. Review History for met or breached outcomes. Use Sales service commitments reporting to filter the cohort, module, owner and team and compare Active, Due within 24 hours, Breached, Met and Compliance.

Expected result

The instance retains a deadline, response outcome and execution history. The summary reports measured compliance for its stated denominator.

Fields and controls

Field or control	Rule
Target business minutes	1-525,600
Priority	0-10,000; lower first
Qualifying types	One or more of call, meeting, visit, task
Calendar version	Required published calendar
Owner changes	Pause for review or follow the new owner

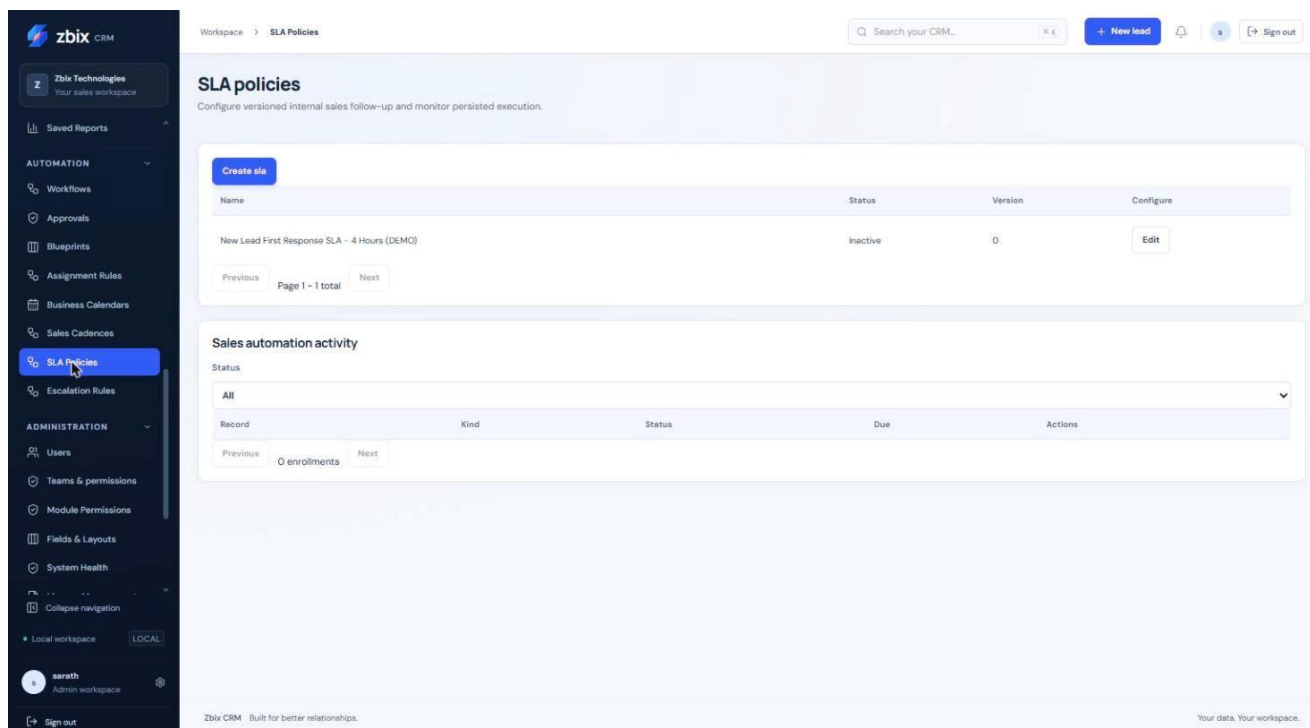


Figure 16 SLA policies list SS-036

Important considerations

- Target business minutes is 1-525,600 and priority is 0-10,000. Creating an activity without completing it does not satisfy the SLA.
- Starts are based on eligible record creation. Arbitrary follow-up event/reset policies are not exposed.
- Historical late responses remain distinguishable from timely performance. Active, paused and unbreached cancelled instances are excluded from the displayed compliance denominator.
- Cohort date filters are UTC and the end date is exclusive. An empty measured denominator is shown as No measured results.

Troubleshooting

- An activity did not satisfy the SLA: verify the source association, completion state, qualifying type and relevant instance history.
- Deadline appears wrong: inspect the pinned calendar, timezone and working exceptions.
- Policy does not attach to existing records: the documented automatic start is record creation; do not assume activation backfills old records.

Related knowledge base articles: Business Calendars; Escalation Rules; Record tasks calls and meetings; Analyze performance with Reports.

Escalation Rules

Zbix CRM 1.2.0 | Source reviewed | Reviewed 28 October 2026

Escalation Rules attach ordered task or notification levels to a published SLA version. Thresholds can occur before, at or after the SLA deadline, measured in business minutes.

Use escalation for due-soon reminders and missed-response follow-up to the record owner or a named authorized colleague.

Before you begin

- An SLA policy has a published version for the same module.
- Sales automation is enabled and the configuration user can manage Workflows. Recipients must remain authorized and active.

Procedure

1. Open Automation > Escalation Rules and select Create escalation. Enter Name and Module.
2. Choose the exact SLA version to monitor.

- For each level choose Create task or In-app notification and enter Title and Business minutes after deadline. A negative offset is a reminder before the deadline; zero is at the deadline.
- Select Escalation recipient as Current record owner or a named user. Use Add level, Move up and Remove to keep the thresholds in increasing order.
- Select Save draft, Validate saved draft, Publish saved draft and Activate published version.
- Inspect the related SLA or sales automation History after a threshold is due. Open generated tasks and review notifications through their normal modules.

Expected result

The runtime records escalation outcomes against the pinned SLA/definition and avoids duplicate internal actions for the same scheduled effect.

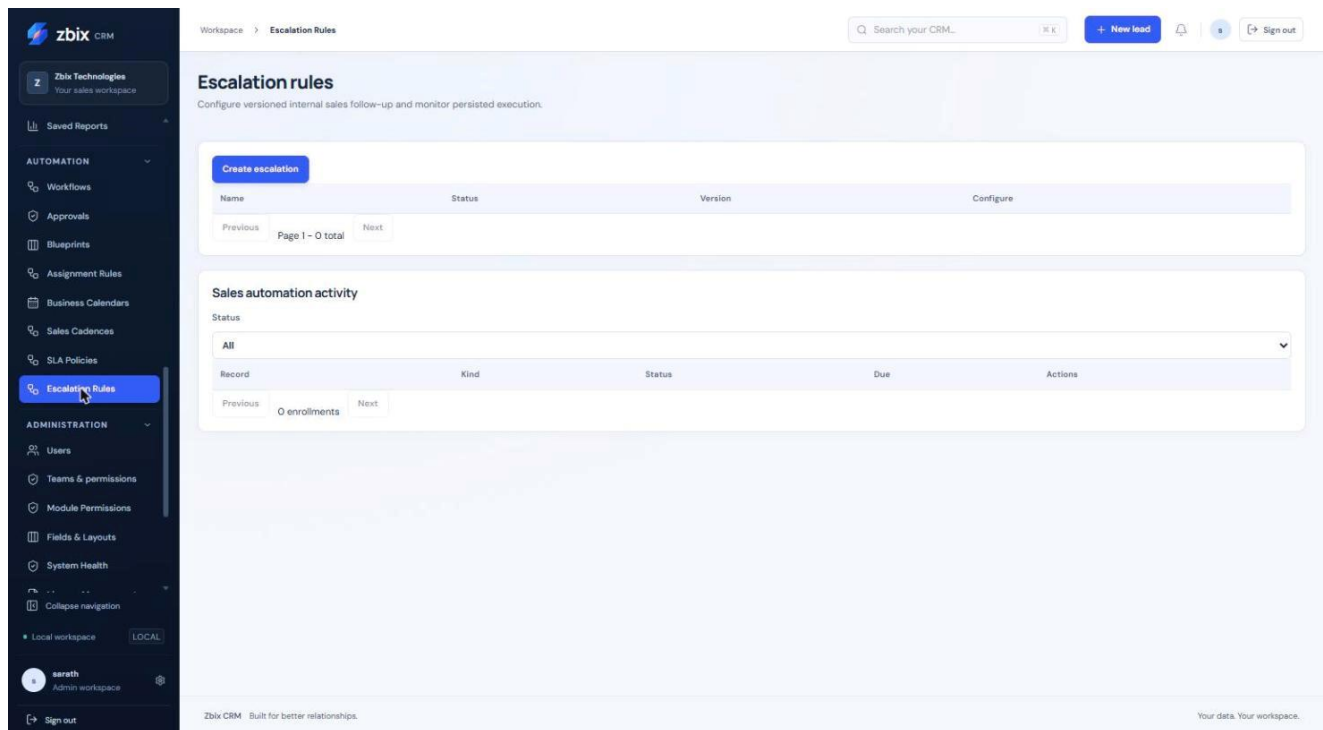


Figure 17 Escalation rules (empty) SS-037

Important considerations

- A rule contains 1-10 levels. Thresholds must be unique and ordered, between -525,600 and 525,600 minutes.
- A negative reminder cannot precede the SLA's start. The selected SLA module must match the rule module.
- Named recipients are available in the current editor. No manager hierarchy or role fan-out is inferred.
- An empty rule list in the screenshot is a genuine unconfigured state, not evidence that the feature lacks an implementation.

Troubleshooting

- Validation rejects thresholds: remove duplicate offsets, order them ascending and ensure reminders fall after SLA start.
- Delivery is absent: inspect the instance status, worker history, current recipient permissions and whether the SLA was already met or cancelled.
- SLA version is not listed: publish the SLA and verify configuration visibility first.

Related knowledge base articles: SLA Policies; Business Calendars; Review notifications and scheduled jobs; Record tasks calls and meetings.

Fields and Layouts

Zbix CRM 1.2.0 | Source reviewed | Reviewed 28 October 2026

Fields & Layouts extends existing CRM modules with typed custom fields and a published default form layout. Field definitions and layouts have separate version histories. Contracts and Subscriptions also appear in the module selector.

Use fields to capture organization-specific information, and layouts to organize forms without changing the database schema manually.

Before you begin

- An administrator identity is required for the Fields & Layouts interface.
- Decide the field's stable API name, data type, validation and legacy-role visibility/editability before creation.

Procedure

1. Open Administration > Fields & Layouts and choose Module. Wait for its Field catalog and Default form layout to load.
2. Select Add custom field. Enter API name, Label and Type. Use a lower-case cf_ name, for example cf_service_region.
3. Enter Description and optional Default value. For Select or Multiselect, enter Options, one per line. Set applicable Maximum length, Decimal precision and Decimal scale.
4. Set Required, Exportable, Searchable, Filterable and Sortable as needed. Review Visible to and Editable by; selecting no roles means all otherwise permitted users.
5. Select Save field. To make it visible in a form, add it to a section in Default form layout. Use the up/down controls to reorder sections or fields, and Add section to group related information.
6. Select Preview layout. Select Save draft to retain unpublished work or Publish layout to make the layout current. Open a record form in the chosen module and check the resulting form.
7. Use History or Published history to review prior definitions. If a custom field is no longer needed, select Retire and confirm that historical values are to be preserved.

Expected result

The saved field is validated by the server. Published layout changes appear in record forms; unpublished layout drafts do not change the current published form.

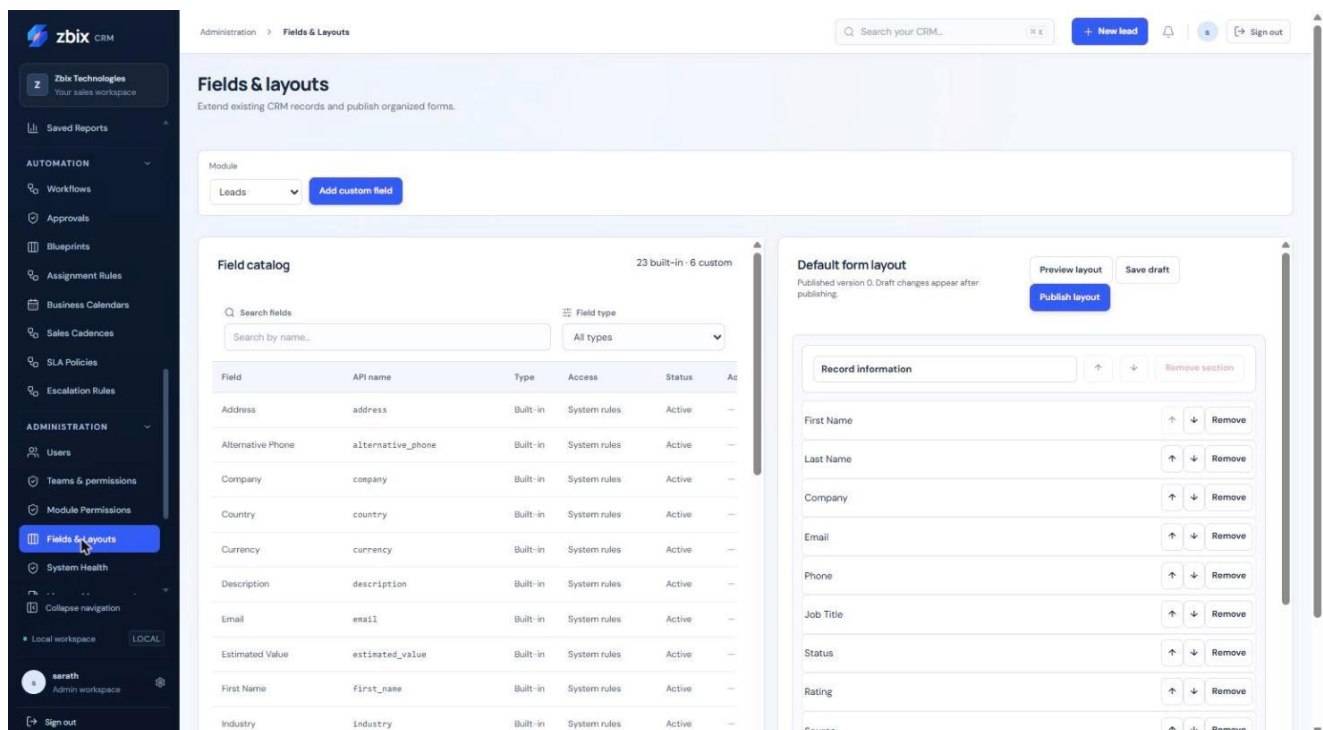


Figure 18 Field catalog & form layout editor SS-042

Important considerations

- API name and field type are immutable after creation. Labels are 1-120 characters; descriptions are at most 1,000. API names follow cf_ plus a lower-case letter, then lower-case letters, digits or underscores.
- There are 12 types: text, multiline, integer, decimal, boolean, date, datetime, email, phone, url, select and multiselect.
- Layout removal does not delete the field or its data. Retiring preserves historical values.
- The source uses explicit up/down controls; it does not implement drag-and-drop layout ordering despite the earlier screenshot inventory description.

- Per-field role restrictions use the legacy role identifiers admin, manager, sales and readonly. A custom module role does not substitute for a new field-role identifier.

Troubleshooting

- A field is hidden: check its active status, placement in the published layout, module permissions and field role visibility.
- Save rejects a value: check type, allowed options, length/precision and whether a datetime contains an offset.
- A required field blocks automation: supply a suitable default or configure the task action's required custom-field values.

Related knowledge base articles: Module Permissions; Workflows; Contracts; Recurring Billing.

Module Permissions

Zbix CRM 1.2.0 | Source reviewed | Reviewed 28 October 2026

Module Permissions assigns a complete custom permission matrix to a user. Eight actions and Own records, Team records or Organization records are configured for each module. One explicit assignment replaces the user's legacy module grants.

Use a custom module role when the standard admin, manager, sales or readonly defaults do not match an operational role. Review access as a whole before assignment.

Before you begin

- An administrator identity is required. A manage_settings grant alone does not authorize identity or role administration.
- Identify the required modules, actions and visibility scope, including source modules used by reports, documents and automation.

Procedure

1. Open Administration > Module Permissions. Select a role to inspect its matrix or select Create module role. A copy of a known role can be created with Create role copy.
2. Enter the role name and set View, Create, Edit, Delete, Assign, Export, Approve and Manage settings for each module. Choose its record visibility.
3. Select Save module role. A complete matrix is required; omitted newly introduced revenue grants remain denied.
4. In User assignment and effective access, choose the user and Assigned module role. Review the displayed effective access and assignment version.
5. Select Review role assignment. Check the replacement warning and proposed access, then Apply module role assignment.
6. Reopen effective access and verify the role and visibility. Where necessary, test with the intended user in a permitted review session.
7. Before deactivating a role, remove all user assignments. Removing an assignment restores legacy policy, which may grant more or different access.

Expected result

The server evaluates the single assigned role on subsequent requests. Related resources continue to require their source-record and field access as well as the module action.

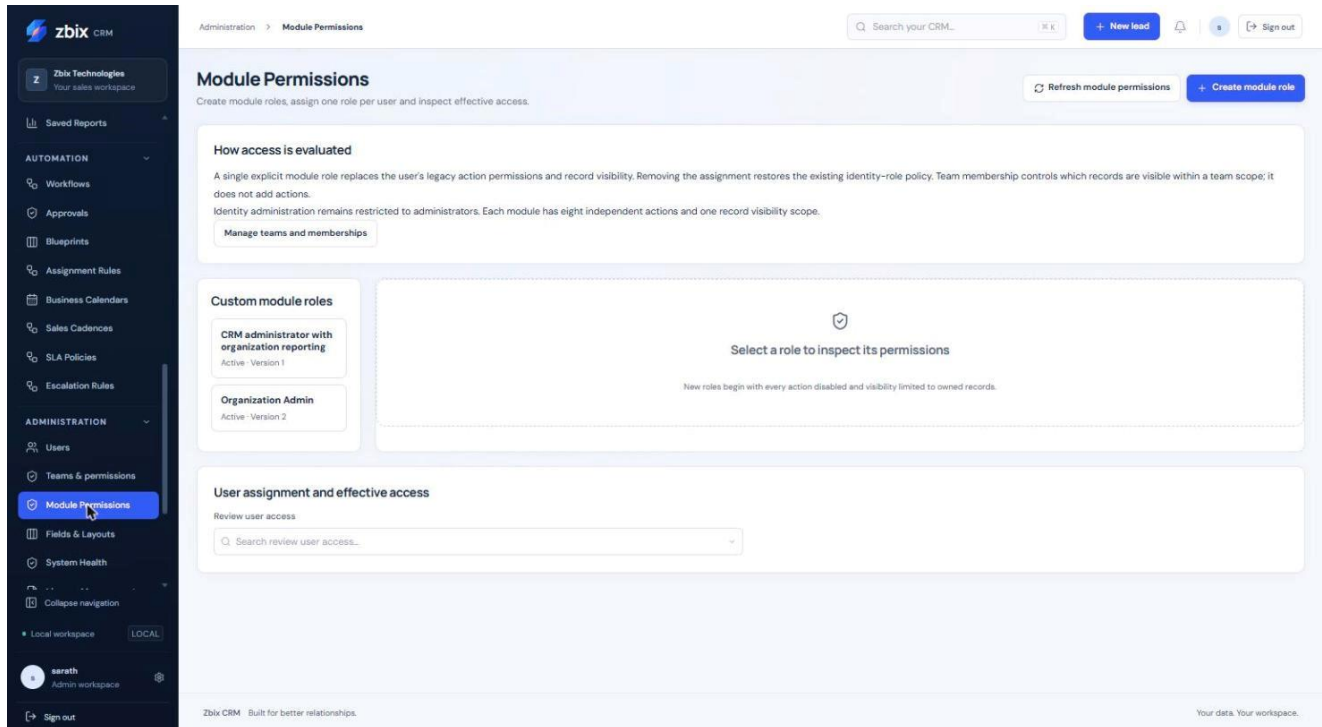


Figure 19 Module permissions overview SS-040

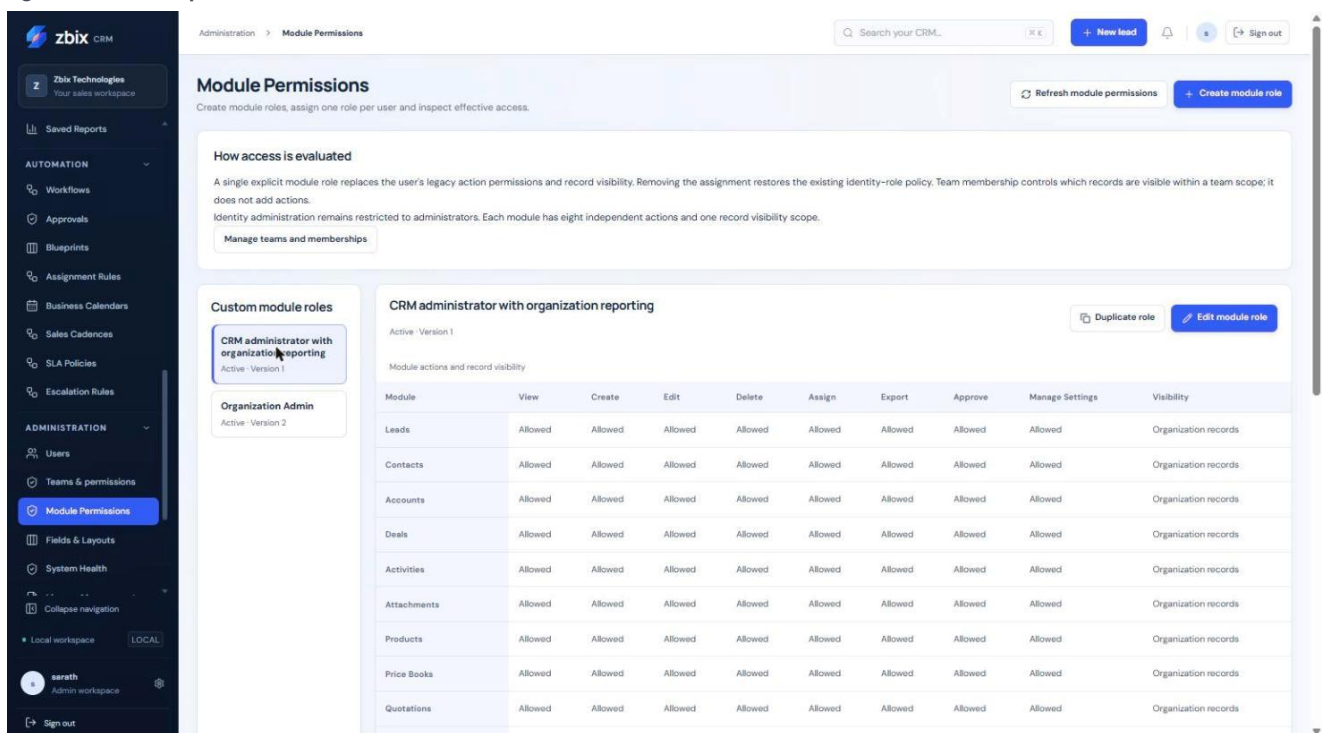


Figure 20 Role permission matrix SS-041

Important considerations

- Custom roles do not union together. An inactive or invalid assigned role fails closed rather than silently restoring legacy grants.
- Team membership does not itself grant actions. Organization visibility does not cross organization boundaries.
- Report sharing, document links and automation history do not override source permissions.
- Legacy administrator identity remains separate from the module role. Record and action rights can still be restricted by an explicit role.

Troubleshooting

- A user lost access after assignment: compare the entire assigned matrix with the prior legacy policy; assignments replace rather than add grants.
- A report is visible but cannot run/export: check the source module's view/export grants and record/field scope.

- Role deactivation is rejected: remove every assignment first, reviewing the legacy access that each removal restores.

Related knowledge base articles: Manage Teams and legacy role policies; Create and maintain Users; Analyze performance with Reports; Fields and Layouts.

Authentication and sign in architecture

Zbix CRM 1.2.0 | Source reviewed | Reviewed 28 October 2026

CRM login uses an email address and password, with an additional authenticator or recovery-code challenge when MFA is enabled. Passwords are verified with Argon2. Successful authentication creates a server-side session and an HTTP-only browser cookie. The database stores a hash of the session token. Microsoft 365 connection authorizes mailbox/calendar access and does not replace this CRM sign-in flow.

Use this reference to understand login, enrollment requirements and the relationship between application identity and provider connections.

Before you begin

- An active CRM user account.
- The enrolled authenticator or an unused recovery code when the account requires MFA.

Procedure

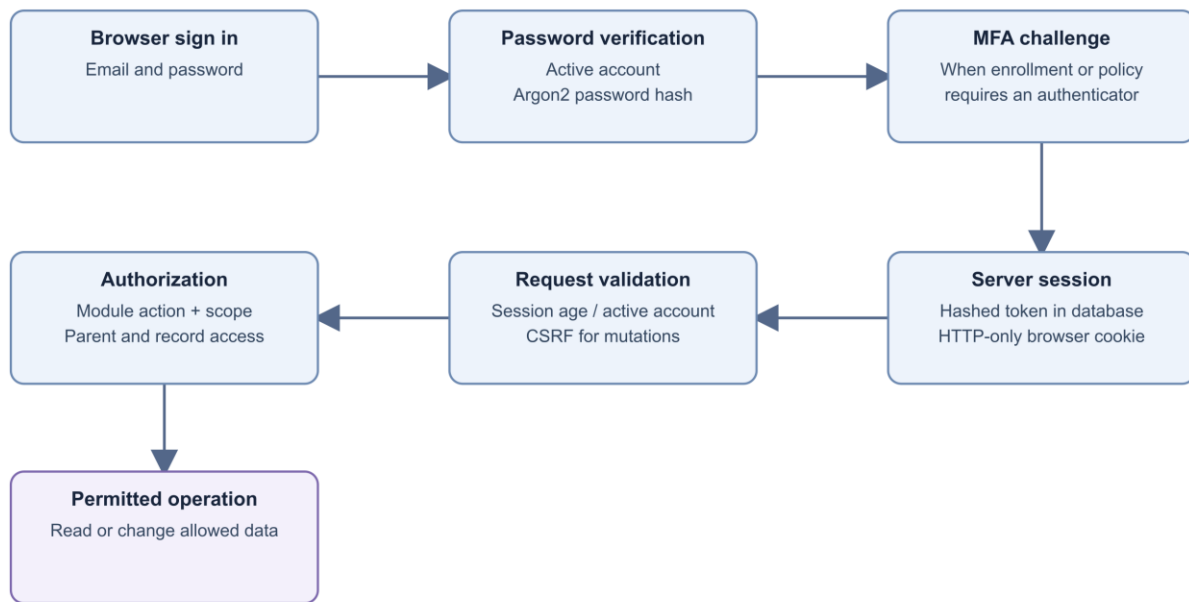
1. Open the approved CRM URL and enter the account email and password. Use Remember me only on a trusted personal device when offered.
2. If an MFA challenge appears, enter a current authenticator code or an unused recovery code. A password-only success does not complete a required MFA challenge.
3. If enrollment is required, complete Security Settings enrollment before expecting normal protected operations to become available.
4. After signing in, confirm the expected account and workspace. Navigation is based on current effective permissions and enabled capabilities.
5. Use Sign out when finished on a shared device. If access is suspected on another device, revoke that session using the session controls.

Expected result

A valid authenticated session is established, subject to the organization's MFA policy, user activity and server-side lifetime limits.

Authentication and access flow

Sign in establishes a session; authorization is checked on requests



Remember me extends session lifetime; idle timeout remains enforced.
Microsoft provider authorization is separate from CRM authentication.

Figure 21 Authentication and access flow

Important considerations

- A session cookie does not carry permanent permission grants. The server reloads the user and effective access policy.
- Mutating browser requests require the matching CSRF token in addition to the session.
- A connected Microsoft mailbox is a separate delegated identity. Disconnection of Microsoft does not itself remove the CRM password account.
- Do not send passwords, authenticator seeds, recovery codes or reset links to support.

Troubleshooting

- Invalid email or password: confirm the address and account activity with the administrator, then use the supported reset path.
- Session expired: sign in again; repeated expiry requires review of inactivity, configured lifetime and browser cookie handling.

Related knowledge base articles: Manage sessions and sign out other devices; Password change and account recovery; Authenticator enrollment and organization MFA policy; Authorization and permission evaluation.

Manage sessions and sign out other devices

Zbix CRM 1.2.0 | Source reviewed | Reviewed 28 October 2026

Sessions have both an inactivity limit and an absolute maximum lifetime. The v1.2.0 defaults are 30 minutes of inactivity, 12 hours of normal lifetime and 30 days for Remember me. Installations can configure these values within bounded ranges. Remember me does not disable the inactivity check. The Active sessions panel shows last activity and maximum expiry for each session.

Use session controls after a lost device, a shared-browser session or an account access review.

Before you begin

- An authenticated account for personal session management.
- Administrator identity for revoking another user's sessions.

Procedure

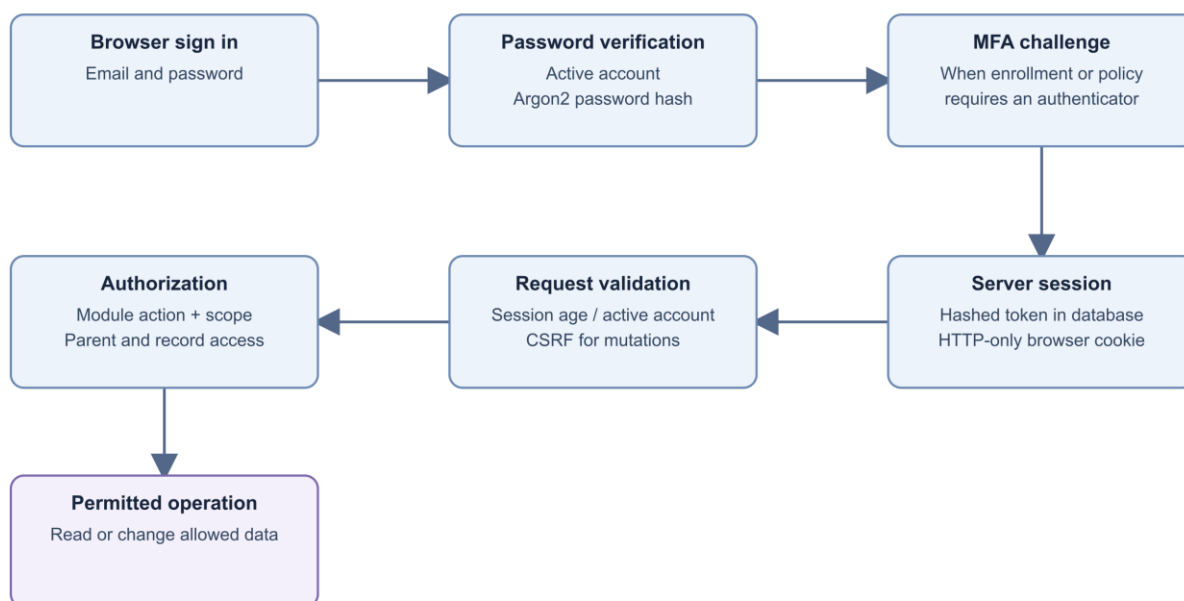
1. Open Settings and locate Active sessions. Review This device and each Other session by last active time and maximum expiry.
2. Choose Revoke beside a specific other session, or choose Sign out other devices to retain the current session while ending the others.
3. Refresh the panel and verify the revoked entries are removed. The other browser will need to authenticate again on its next protected request.
4. For another user, open that user's administration record and use Revoke active sessions. Verify the user identity before confirming the action.
5. When rotating a password, sign in again afterward. Password changes invalidate existing sessions rather than silently keeping them authenticated.

Expected result

Only the intended remaining sessions retain access, and subsequent requests from revoked sessions require sign-in.

Authentication and access flow

Sign in establishes a session; authorization is checked on requests



Remember me extends session lifetime; idle timeout remains enforced.
Microsoft provider authorization is separate from CRM authentication.

Figure 22 Authentication and access flow

Important considerations

- The list identifies sessions by time and current-device status; it is not a complete device inventory or geolocation history.
- The server updates last-seen time periodically rather than on every request.
- Normal lifetime is configurable from 1 to 168 hours; Remember me from 1 to 90 days; inactivity from 5 to 1,440 minutes. Use the installation's approved policy rather than assuming defaults.
- An administrator cannot use the other-user endpoint for their own session; personal controls cover that case.

Troubleshooting

- A session returns after revocation: confirm whether the user signed in again, creating a new session.
- A user still sees a cached page: access is enforced on the next protected server request, so refresh and verify the action rather than relying on already displayed text.

Related knowledge base articles: Authentication and sign in architecture; Password change and account recovery; Authenticator enrollment and organization MFA policy.

Password change and account recovery

Zbix CRM 1.2.0 | Source reviewed | Reviewed 28 October 2026

A signed-in user can change their password using the current password. The login recovery flow can email a short-lived, single-use reset link when outbound SMTP and the recovery configuration are available. The link expires after 30 minutes. A successful reset invalidates outstanding links bound to the previous password and revokes existing sessions.

Use the supported recovery path to restore access without exposing passwords or modifying database hashes.

Before you begin

- For a normal change, the current password and a signed-in session.
- For an email reset, an active account with access to its mailbox and enabled SMTP recovery delivery.

Procedure

1. If signed in, open Settings, locate Password & security, enter the current password and a new password of 12 to 1,024 characters, then save.
2. Sign in again with the new password after the change completes. Complete MFA if the account has an enrolled factor.
3. If unable to sign in, use the password recovery option and enter the account email. The response is deliberately generic and does not confirm account existence.
4. Open the latest reset link in the intended CRM origin before it expires, set the new password, then sign in normally.
5. If no message arrives, ask the workspace administrator to check account activity and SMTP delivery configuration. An administrator can send the supported recovery link or use the authorized user-management password process.

Expected result

The account has a new password, prior sessions are invalidated and normal MFA protection remains in place.

Important considerations

- A reset link is sensitive authentication material. Do not paste it into tickets, screenshots or public documentation.
- The reset response does not prove email delivery. SMTP acceptance and mailbox arrival must be distinguished.
- An expired or already-used link requires a new request. Reusing the old link does not extend its validity.
- Password recovery is separate from MFA recovery; replacing a password does not supply a missing authenticator.

Troubleshooting

- No reset email: check spam/quarantine and ask the administrator to review the configured sender and safe SMTP diagnostic status.
- Invalid or expired reset link: request a new link and use it once within the validity period.

Related knowledge base articles: Manage sessions and sign out other devices; Authenticator enrollment and organization MFA policy; Configure SMTP email delivery.

Authenticator enrollment and organization MFA policy

Zbix CRM 1.2.0 | Source reviewed | Reviewed 28 October 2026

Security Settings supports time-based authenticator verification and one-use recovery codes. Enrollment is tied to the current session and protected by password reauthentication. The organization can keep MFA optional, require it for administrators or require it for all users. Administrative recovery resets another user's factor, revokes their sessions and requires enrollment again.

Use MFA to add a second verification step and maintain a controlled recovery process for lost authenticators.

Before you begin

- An active account and the current password.
- An authenticator application and a protected place to store recovery codes.
- Administrator identity and an enrolled factor for organization policy changes.

Procedure

1. Open Administration > Security Settings and choose Set up authenticator app. Reauthenticate with the current password.
2. Add the displayed enrollment to the authenticator and enter the requested current code to confirm. Keep the enrollment secret private.
3. Store the displayed recovery codes securely. They are shown once and each can be used once. Verify the panel reports the authenticator enabled.
4. For an organization policy change, select Optional for everyone, Required for administrators or Required for all users, then choose Review MFA policy change. Confirm using the current password and a fresh factor.
5. For a verified lost-factor case, select the other user under Administrator recovery, supply the recovery reason and complete the administrator's reauthentication. Have the affected user sign in and enroll again.

Expected result

The account or organization policy is updated with audit history, and recovery revokes affected sessions.

Important considerations

- TOTP secrets require a durable external encryption key. Key custody is an installation responsibility; user recovery codes do not replace that key.
- A code already accepted cannot be replayed. The interface describes a 30-second code cycle and an adjacent time-step allowance.
- Required MFA cannot be disabled by the user while the policy applies.
- Do not publish QR enrollment images, secret text or recovery codes in a support case.

Troubleshooting

- Authenticator codes fail repeatedly: verify the phone clock and use a fresh code; use an unused recovery code if available.
- Organization policy cannot be changed: enroll the administrator first and resolve any user-enrollment prerequisites reported by the application.

Related knowledge base articles: Authentication and sign in architecture; Manage sessions and sign out other devices; Password change and account recovery.

Authorization and permission evaluation

Zbix CRM 1.2.0 | Source reviewed | Reviewed 28 October 2026

Zbix CRM separates identity roles, module actions and record visibility. Legacy identity roles are admin, manager, sales and readonly. A custom module role provides eight independent actions for each module plus own, team or organization visibility. One explicit module-role assignment replaces the legacy action policy; assignments are not combined as a union of multiple roles.

Use this model to design least-privilege access and explain why a user can see a menu but cannot perform a particular operation.

Before you begin

- Administrator identity for managing roles and assignments.
- A written description of the actions and records required by the business role.

Procedure

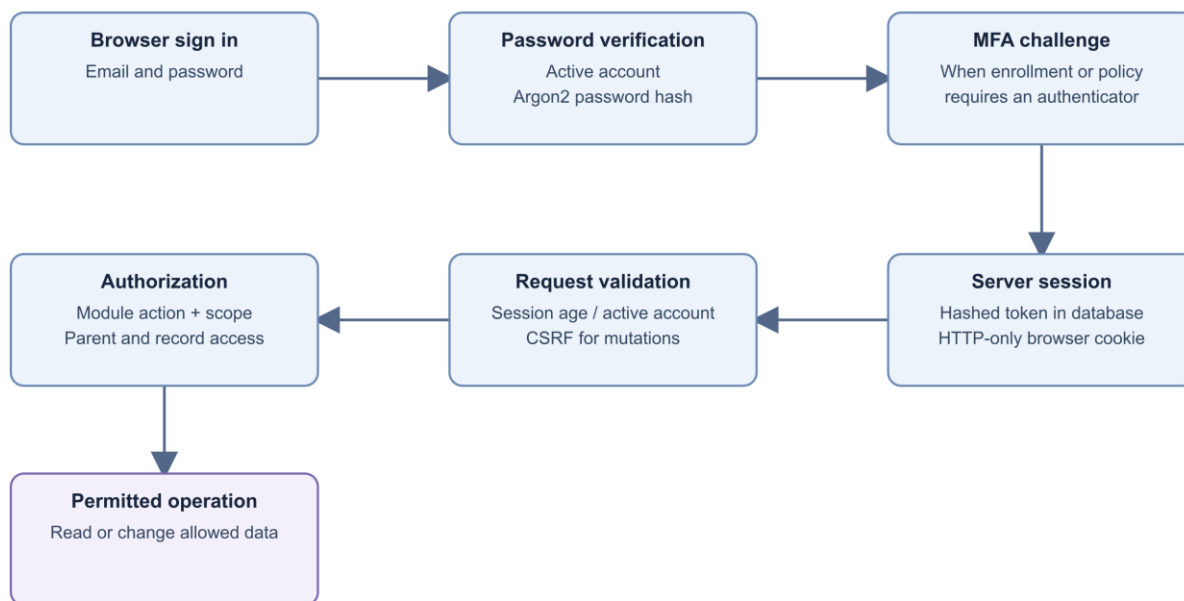
1. Open Module Permissions and inspect the role's complete action matrix. Evaluate View separately from Create, Edit, Delete, Assign, Export, Approve and Manage Settings.
2. Review the visibility scope for each module. Own uses the record owner; Team includes qualifying team membership; Organization remains inside the current organization.
3. Check the user's explicit assignment and effective access. Removing the assignment restores the legacy policy, so review that fallback before removal.
4. Check access to parent and source records as well as the target module. Attachments, documents, related CRM records and report execution intersect these permissions.
5. Verify representative actions with an appropriate test account in an approved test environment, then document the intended role behavior.

Expected result

The role grants only the required actions and record scope, and users understand which permission is missing when an operation is denied.

Authentication and access flow

Sign in establishes a session; authorization is checked on requests



Remember me extends session lifetime; idle timeout remains enforced.
Microsoft provider authorization is separate from CRM authentication.

Figure 23 Authentication and access flow

Important considerations

- Team membership expands eligible team visibility but does not itself grant actions or administrator identity.
- Identity and access administration requires the admin identity role; a custom Manage Settings action is not a substitute.
- A role with an inactive or invalid explicit assignment does not silently regain legacy privileges.
- License and capability checks may further restrict an otherwise permitted action.

Troubleshooting

- A record disappears after a related record is restricted: review the full relationship and source visibility chain.
- A shared report returns fewer records for another user: sharing the definition does not share the owner's data access.

Related knowledge base articles: CRM and commercial data relationships; Troubleshoot report totals and missing records; Authentication and sign in architecture.

Integration interfaces and provider boundaries

Zbix CRM 1.2.0 | Source reviewed | Reviewed 28 October 2026

Zbix CRM has three distinct integration paths: browser APIs secured by the CRM session, a narrow scoped bearer API, and outbound communications through configured providers. SMTP and delegated Microsoft Graph support real external operations. The webhook subsystem in this release is a durable local mock implementation. Enabling the integration API does not turn mock webhooks into HTTP deliveries.

Use this reference before choosing an integration approach or interpreting a successful provider status.

Before you begin

- A defined integration use case and the intended data/action scope.
- Administrator and provider-owner involvement for configuration.

Procedure

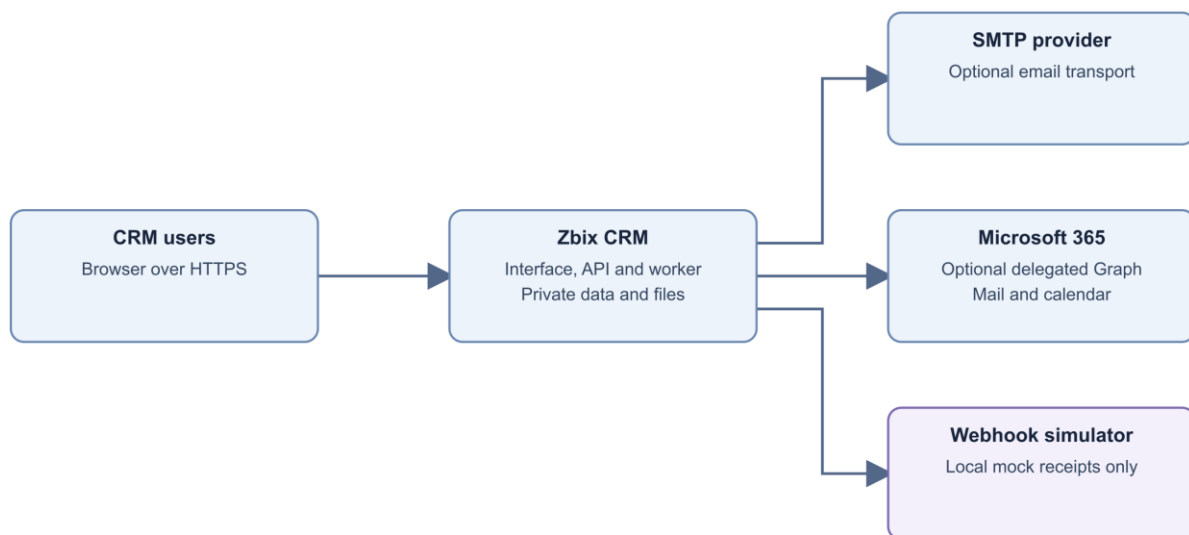
1. Identify whether the integration needs record reads/creates, email, mailbox synchronization or calendar synchronization. Choose the interface that actually supports the operation.
2. For record automation, review the bearer API scopes and the active non-administrator service identity. Its current CRM permissions remain authoritative.
3. For email, configure SMTP or connect Microsoft Graph and explicitly select the provider when queuing a message.
4. For Microsoft synchronization, choose the supported folder/calendar and direction on the personal connection page. Confirm consent and privacy expectations with the user.
5. For webhook testing, treat local receipts as simulation evidence. Do not advertise an external callback delivery until a separately implemented and qualified transport exists.

Expected result

The integration design matches implemented interfaces and distinguishes local simulation, provider acceptance and actual external observation.

System context

Core CRM and explicitly configured providers

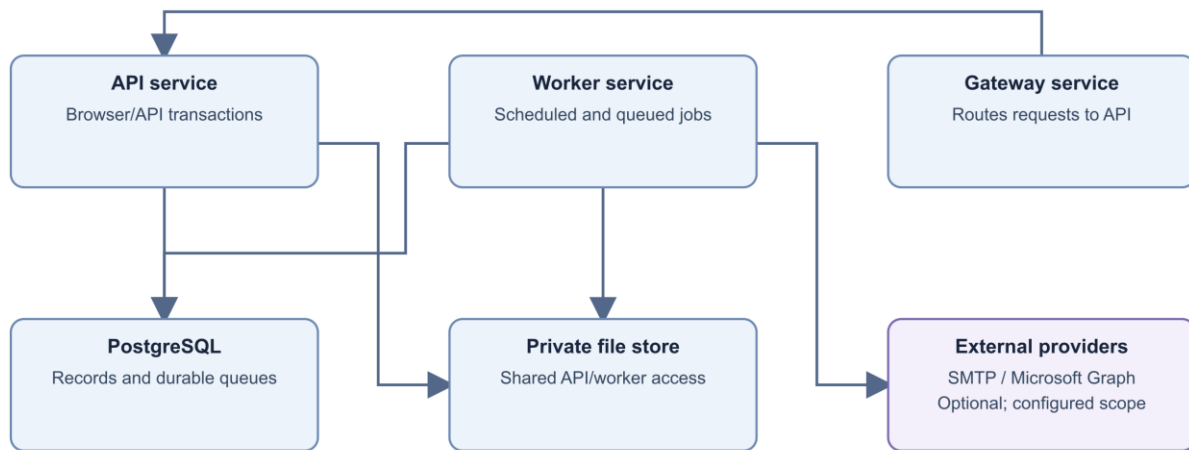


Provider configuration and successful delivery are separate checks.
Microsoft connection does not replace CRM sign in.

Figure 24 System context

Service dependencies

Dependencies to check when only part of the application is healthy



Database readiness does not prove worker progress or provider delivery.
Provider availability depends on configured operation and actor authorization.

Figure 25 Service dependencies

Important considerations

- Microsoft connection does not implement CRM single sign-on. CRM password/MFA authentication remains independent.
- Graph and SMTP acceptance indicate submission to the provider, not recipient delivery.
- No Gmail provider is established by this reviewed implementation.
- Provider configuration and source code are not proof of customer-tenant acceptance. Qualify each intended connection with controlled test data and explicit authorization.

Troubleshooting

- A webhook says delivered but the receiver has no event: inspect the mode; mock delivery creates a local receipt only.
- An API action is unavailable: confirm the endpoint belongs to the narrow bearer surface rather than the broader browser API.

Related knowledge base articles: Configure and use the scoped integration API; Configure SMTP email delivery; Connect Microsoft 365 mail and calendar; Troubleshoot queued failed or uncertain email.

Configure and use the scoped integration API

Zbix CRM 1.2.0 | Source reviewed | Reviewed 28 October 2026

The bearer API supports list, detail and create operations for Leads, Contacts, Accounts and Deals. Each credential is bound to an active non-administrator service identity and explicit read/create scopes. Requests also enforce that user's current module permission and record visibility. Credential creation, rotation and revocation are administrator operations.

Use the scoped API for controlled record ingestion or retrieval without distributing a browser session or administrator password.

Before you begin

- Integration API enabled by the installation owner and a licensed capability where applicable.
- An active non-administrator service identity with the necessary CRM permissions.
- A secure application secret store for the token shown at creation or rotation.

Procedure

1. Open Administration > Integrations and review Local configuration. Resolve disabled API status through the installation owner before creating a credential.
2. Choose Create API credential, name the integration, select its service identity and grant only the required read/create scopes. Set an expiry and request rate limit.
3. Store the returned token securely when shown. Do not place it in source code, documentation, URLs or logs.
4. Call the /api/v1/{module} list or detail endpoint using the Authorization bearer header. Page through results with page and page_size; page_size is limited to 100.
5. For POST creation, provide an Idempotency-Key unique to that logical operation. Retries of identical content retain the same key; changed content requires a different key.
6. Verify the created record and audit result. Rotate credentials before expiry and revoke those no longer required.

Expected result

The integration can perform only the granted read/create actions within its service identity's scope.

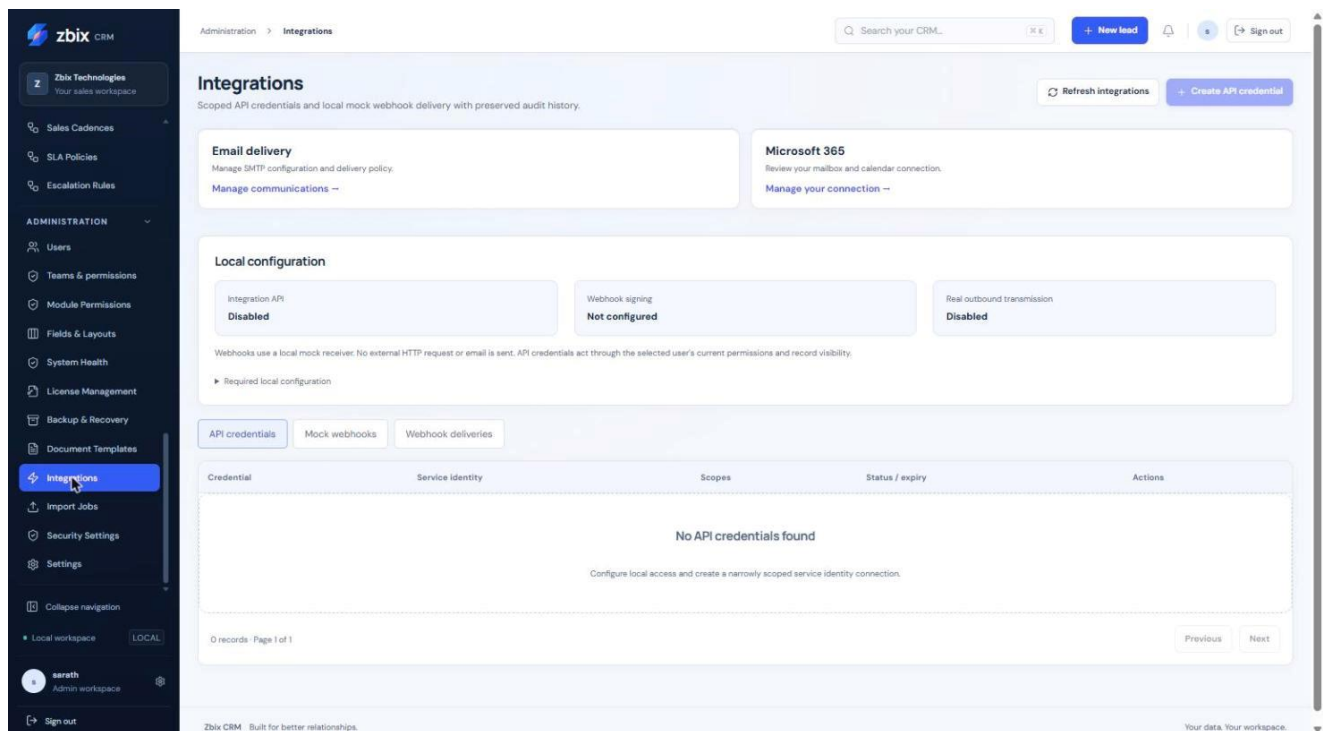


Figure 26 Integrations & API credentials SS-047

Important considerations

- Credential expiry defaults to 30 days and cannot exceed 365 days. Rate limits range from 1 to 600 requests per minute, defaulting to 60.
- Integration-created records must belong to the scoped service identity. Update, delete, bulk export and every browser endpoint are not implied by these scopes.
- Create bodies are bounded to 64 KiB of finite JSON. A reused idempotency key with different content is rejected.
- Rotation invalidates the previous token; revoked credentials cannot be rotated.

Troubleshooting

- 401: check expiry, revocation, token rotation and service-account activity.
- 403: check both explicit credential scope and the service user's current module permissions.
- 429: wait for the next minute window before retrying.
- 409 on a create retry: compare the idempotency key and exact intended request content.

Related knowledge base articles: Integration interfaces and provider boundaries; Authorization and permission evaluation; API validation and safe concurrency.

Configure SMTP email delivery

Zbix CRM 1.2.0 | Source reviewed | Reviewed 28 October 2026

SMTP settings define the organization's outbound server, TLS mode, authentication and sender identity. Saving settings, testing the connection and sending a test email are separate actions. Email Activities queues actual messages through the selected provider. A successful SMTP submission means the server accepted the message; it is not proof that the recipient received it.

Use this procedure to configure and verify the transport before enabling customer-facing email or password recovery.

Before you begin

- Administrator identity and permission to manage communications.
- Approved SMTP host, port, TLS mode, authentication method, sender and test recipient.
- Configured communication-secret encryption when login credentials are stored.

Procedure

1. Open Settings > Email & communications and select the SMTP configuration. Enter the approved hostname and port.
2. Choose STARTTLS or implicit TLS. Select no authentication only for an approved relay, or login authentication with the supplied username and password.
3. Enter the sender address, sender name, optional reply-to and a controlled test recipient. Save the settings before testing.
4. Run Test connection and review its current result and last test time. Correct DNS, TLS or authentication failures through the provider administrator.
5. Use Send test email only for the configured test mailbox. Confirm both the application acceptance result and arrival or provider trace in that mailbox.
6. Enable delivery as intended and create a reviewed Email Activity draft. Select SMTP explicitly when sending and inspect the resulting attempt history.

Expected result

The saved configuration passes the required transport test and a controlled external message has separately verified provider/mailbox evidence.

Important considerations

- Plain unencrypted SMTP is not an offered TLS mode. Ports must match the selected provider mode.
- Stored passwords are not returned to the interface. Keep the external communication encryption key recoverable through the approved process.
- Password recovery requires enabled SMTP and a valid public application origin as well as recovery configuration.
- Never infer delivery from a historical mock Sent state. Current real submission is labeled Accepted.

Troubleshooting

- Connection test fails: review the safe failing stage, hostname, port, TLS mode and provider credentials.
- Accepted but no email arrives: inspect the recipient's quarantine and provider trace before resending.
- A failed send is uncertain: review provider evidence before any retry to avoid a duplicate message.

Related knowledge base articles: Troubleshoot queued failed or uncertain email; Password change and account recovery; Integration interfaces and provider boundaries.

Connect Microsoft 365 mail and calendar

Zbix CRM 1.2.0 | Source reviewed | Reviewed 28 October 2026

Microsoft 365 integration uses a configured Entra web application and a separate delegated connection for each CRM user. The organization registration defines the allowed capabilities; each user connects their own Microsoft identity. Saving the registration alone neither connects a mailbox nor proves mail/calendar delivery. CRM login remains password/MFA based.

Use this procedure to establish the supported personal mailbox and calendar connection with explicit consent.

Before you begin

- Administrator access to CRM integration settings and the intended Microsoft tenant.

- An approved Entra registration and exact redirect URI for the CRM origin.
- A durable communication encryption key and a user authorized to consent to the required delegated scopes.

Procedure

1. In the intended tenant, prepare a web application with the exact callback URI `https://crm.example.com/api/microsoft/callback`, replacing the example origin with the approved CRM origin.
2. In Settings > Email & communications > Microsoft 365, enter the approved tenant/application registration and enable only the required capabilities. Protect the client secret through the provided configuration process.
3. Have each user open My Microsoft 365 account, connect their own identity and consent to the selected scopes. Verify the connected mailbox before enabling background work.
4. Select the desired mailbox folder and calendar synchronization direction. Start with the narrowest scope required for the business process.
5. Validate a controlled mail or calendar operation and review the CRM attempt/synchronization history and Microsoft-side result.
6. Disconnect or reconnect through the personal page when access is no longer required or consent/configuration changes.

Expected result

The user has an explicit delegated connection with selected capabilities and independently observed test results.

Important considerations

- Mail.Send, Mail.Read and calendar permissions serve different operations; avoid granting unused capabilities. The implementation uses the global Microsoft Graph endpoint.
- Disconnect removes the local token cache; underlying tenant consent is managed in Microsoft.
- Shared-mailbox/calendar delegation and CRM single sign-on are not established by this connection.
- Actual tenant acceptance remains an installation-specific test, even when simulator and source tests pass.

Troubleshooting

- Reconnect required: review tenant registration, secret expiry and delegated consent, then reconnect.
- Callback rejected: compare the exact approved redirect URI and tenant/application settings.
- Permission failure: check the user-selected capability and tenant consent before broadening access.

Related knowledge base articles: Microsoft synchronization and conflict handling; Integration interfaces and provider boundaries; Troubleshoot queued failed or uncertain email.

Microsoft synchronization and conflict handling

Zbix CRM 1.2.0 | Source reviewed | Reviewed 28 October 2026

Mailbox synchronization imports a private copy of selected Microsoft messages. Calendar synchronization can read Outlook events, write CRM meetings or operate in two-way mode. Private provider content is not automatically shared as a customer CRM record. The user explicitly associates an imported message or event where supported. Conflicting or uncertain writes are surfaced for review instead of silently replayed.

Use this guide to select synchronization scope and handle discrepancies without overwriting changes or exposing personal mailbox content.

Before you begin

- A connected Microsoft 365 account with the required delegated permissions.
- A chosen folder/calendar and an agreed business purpose for synchronization.

Procedure

1. Open My Microsoft 365 account and verify the connected identity. Select Inbox or Sent Items for mailbox synchronization, then enable the supported Outlook-to-CRM mode.
2. Review imported messages in the personal view. Associate a message with a specific visible CRM record only when the participant email matches that record.
3. For calendar work, select Disabled, Outlook to CRM, CRM to Outlook or Two-way. Confirm the intended personal calendar.
4. Review CRM Calendar alongside private Outlook events. Import or associate provider content explicitly rather than assuming an overlay is a shared CRM Activity.

5. When a link reports Conflict, compare both versions and use the explicit conflict-resolution action. For Uncertain, inspect Microsoft-side state before another write.
6. After reconnecting or resolving a conflict, refresh synchronization history and verify the expected record/event identity.

Expected result

Synchronization has a known scope, private information remains private until explicitly associated, and conflicting writes have a reviewed outcome.

Important considerations

- Initial mailbox synchronization is bounded to the preceding 30 days. The initial calendar window spans 90 days before and 365 days after the first poll.
- CRM-owned event creation intentionally omits invitees, so synchronization does not imply meeting invitations were sent.
- Changing calendars while remote CRM event links exist is blocked for review.
- Graph acceptance, sync completion and customer visibility are separate outcomes.

Troubleshooting

- An event appears twice: compare CRM/import/provider identities and history before deleting either copy.
- Two-way changes conflict: review both changes; do not repeatedly force synchronization.
- Messages are absent from CRM records: private import is separate from explicit association and visibility.

Related knowledge base articles: Connect Microsoft 365 mail and calendar; Troubleshoot queued failed or uncertain email; Authorization and permission evaluation.

Activate and review a self hosted license

Zbix CRM 1.2.0 | Source reviewed | Reviewed 28 October 2026

License Management shows the installation's signed entitlement, edition, validity, named-user seats and enabled capabilities. A self-hosted license is bound to the installation identity and verified with an approved public key. The publisher's signing private key is never installed in CRM.

Activate an approved license and verify that the installation has the intended commercial entitlement before customer use.

Before you begin

- Authorized access to Administration > License Management.
- A self-hosted installation with approved verification trust configured by its operator.
- A signed license issued for this installation through the approved publisher process.

Procedure

1. Open Administration > License Management and review Deployment, Installation identity and current license status.
2. Choose Generate Installation Request. Provide the resulting request to the authorized issuer through the agreed process. It identifies the installation; it is not an activation credential by itself.
3. After receiving the approved signed license file, select it in Signed license file and choose Verify License. Review the result before applying it.
4. Choose Upload / Apply Renewal to apply the verified license. Check the resulting edition, validity dates, licensed users, remaining seats and enabled capabilities.
5. Use Verify Installed when you need to recheck the installed entitlement. Review License history for the corresponding change.
6. If the installation must be moved or recovered, use Transfer / Recovery to load the supported instructions and follow the renewal/transfer procedure rather than editing the license file.

Expected result

The installation reports the intended verified license, validity, seat capacity and capabilities, with an associated history entry.

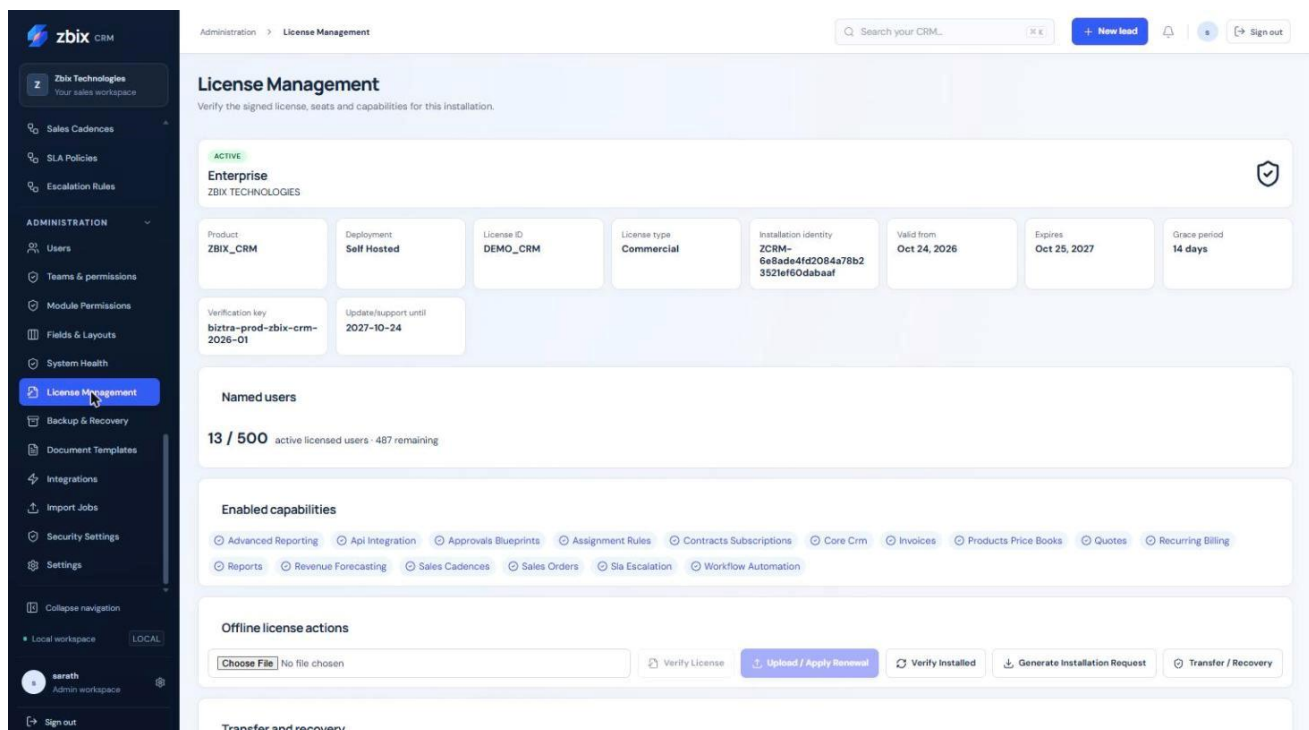


Figure 27 License management SS-044

Important considerations

- A capability being licensed does not mean an integration is configured, authenticated or delivering successfully.
- The installation identity is a durable database value and normally survives upgrades and database restore. It is not tied only to a MAC address or disk serial.
- Supported edition names and capabilities should be taken from the issued entitlement and current screen; do not infer a commercial offer from demo data.
- Backup/recovery and safe data export are recovery controls independent of commercial write entitlement.

Troubleshooting

- For a rejected file, confirm the intended product, installation identity, validity interval, issuer and approved verification key with the publisher. Do not alter the signed JSON.
- If a licensed function is still unavailable, distinguish license entitlement from user permission, application configuration and provider connection.
- Escalate using the installation request, non-secret license identity and verification result through the approved support channel. Never send signing private keys.

Related knowledge base articles: Renew licenses transfer installations and manage seats; Complete the installation readiness review; Assess managed SaaS capabilities; Prepare backup access keys and storage.

Renew licenses transfer installations and manage seats

Zbix CRM 1.2.0 | Source reviewed | Reviewed 28 October 2026

Renewal and transfer use newly signed license documents with the correct installation identity and supersession lineage. Named-user licensing counts active user accounts rather than concurrent sessions. Deactivating an account and reactivating it have different seat effects.

Keep entitlement current while avoiding seat-allocation failures or an unsupported transfer to a different installation.

Before you begin

- Authorized License Management and user-administration access for the intended actions.
- The current license identity and a current installation request.
- An approved renewal, seat change or transfer from the issuer.

Procedure

1. Review Named users in License Management. Compare active users with licensed users and remaining seats before creating or reactivating accounts.

2. For additional seats or a renewal, obtain a signed replacement through the approved issuer process. The replacement must preserve the required license lineage and identify the installed license it supersedes.
3. Select the new file, choose Verify License, then Upload / Apply Renewal. Recheck dates, edition, seat capacity and capabilities after application.
4. For a seat reduction, reconcile the legitimate active-user population first. The system rejects a limit below current active use; do not delete business history to make an entitlement fit.
5. For replacement hardware or a new installation identity, generate a request from the replacement installation and follow Transfer / Recovery guidance. Obtain an authorized superseding license rather than copying or editing an old file.
6. After an upgrade or normal restore that preserves the installation identity, verify the installed license and seat count. Retain the approved recovery and entitlement records together for handover.

Expected result

The current installation has a valid replacement entitlement, accurate named-user capacity and a recorded renewal or transfer history.

Important considerations

- Each active user counts once; disabled users do not count, and the number of sessions is irrelevant.
- Creation and reactivation allocate seats on the server. Concurrent administrators cannot safely bypass a full seat limit by submitting at the same time.
- Role changes do not consume another seat. The current CRM has no pending-invitation seat model.
- Offline revocation is governed by replacement and expiry. Do not describe it as immediate online revocation.

Troubleshooting

- If a user cannot be created or reactivated, check available seats and the active-user count before changing role permissions.
- If renewal fails, compare the replacement's installation and superseded-license identity with the current installation and contact the issuer.
- If a restored system has unexpected entitlement state, preserve the recovery evidence and involve the license/recovery owner. Do not generate a new identity merely to bypass validation.

Related knowledge base articles: Activate and review a self-hosted license; Prepare a CRM upgrade; Plan recovery and rollback decisions; Assess managed SaaS capabilities.

Read System Health and verify service readiness

Zbix CRM 1.2.0 | Source reviewed | Reviewed 28 October 2026

System Health provides administrator-visible evidence for database reachability, worker heartbeats, queue state, private storage, backup status and recent HTTP counters. Runtime identity reports the source commit, image identities and database migration when supplied by the installation. These checks describe different layers and must be interpreted together.

Use the health page for routine checks and incident triage before attempting corrective service or data changes.

Before you begin

- Administrator identity.
- The intended release and the time range of the incident.

Procedure

1. Open Administration > System Health and choose Refresh system health. Record the checked time and warnings in the private operations log.
2. Confirm database reachability, then examine worker last-seen and last-success times. The backend considers a running heartbeat healthy when it is no more than 90 seconds old.
3. Inspect queued and failed counts and the oldest due-work age for the affected operation. Open the corresponding job or activity history for details.
4. Review storage availability, writability and free capacity. Escalate a storage warning before uploads, imports or recovery work exhaust the volume.
5. Review runtime identity against the release plan. Treat unreported fields as unavailable evidence rather than proof of a match.

6. Inspect Backup & Recovery for artifact verification, isolated restore and destination evidence. A legacy receipt alone does not establish recoverability.

Expected result

The operator has a dated health assessment with specific follow-up actions for the affected component.

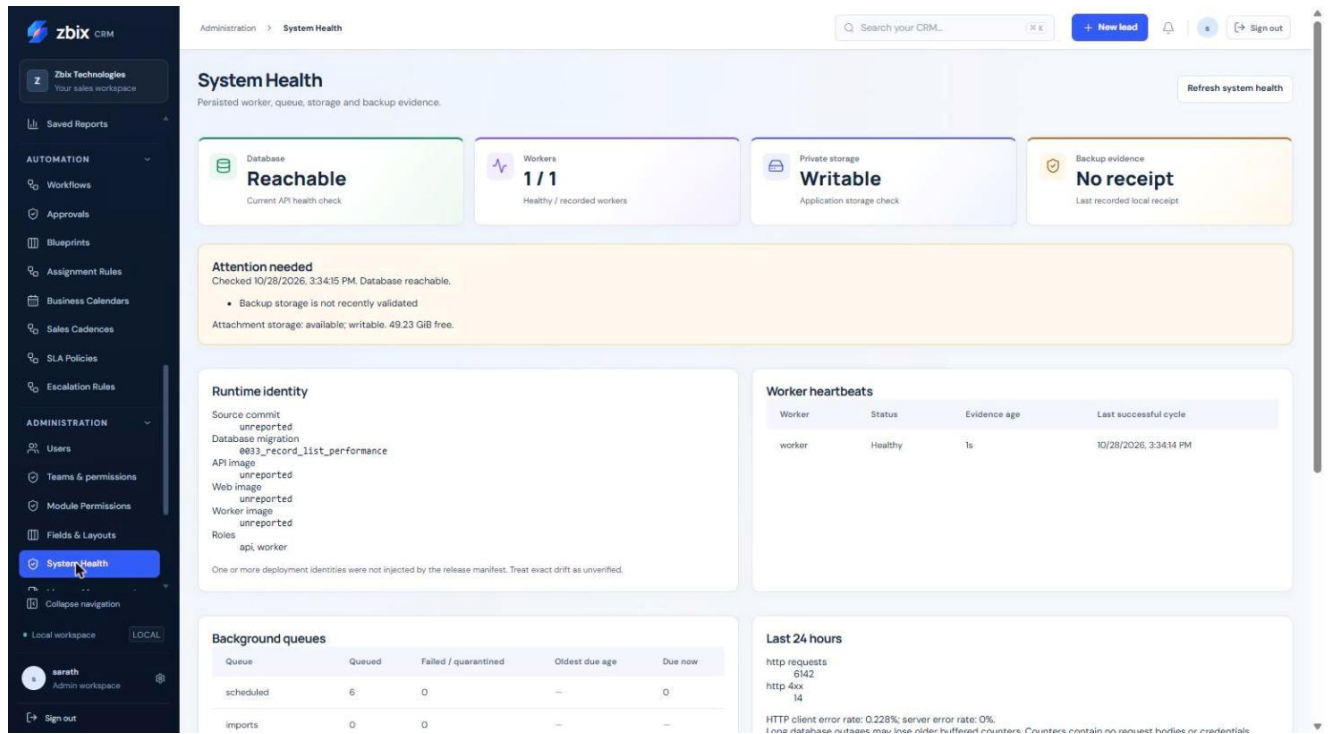
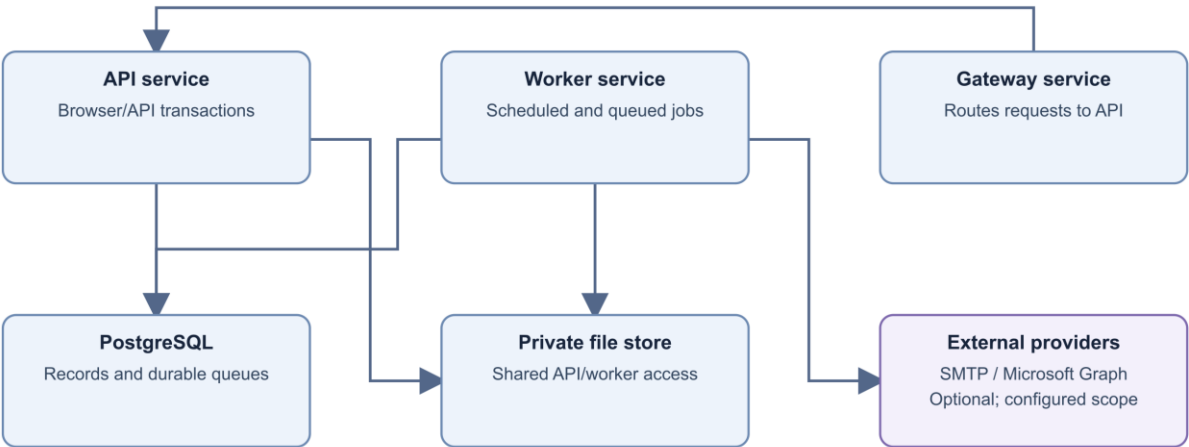


Figure 28 System health dashboard SS-043

Service dependencies

Dependencies to check when only part of the application is healthy

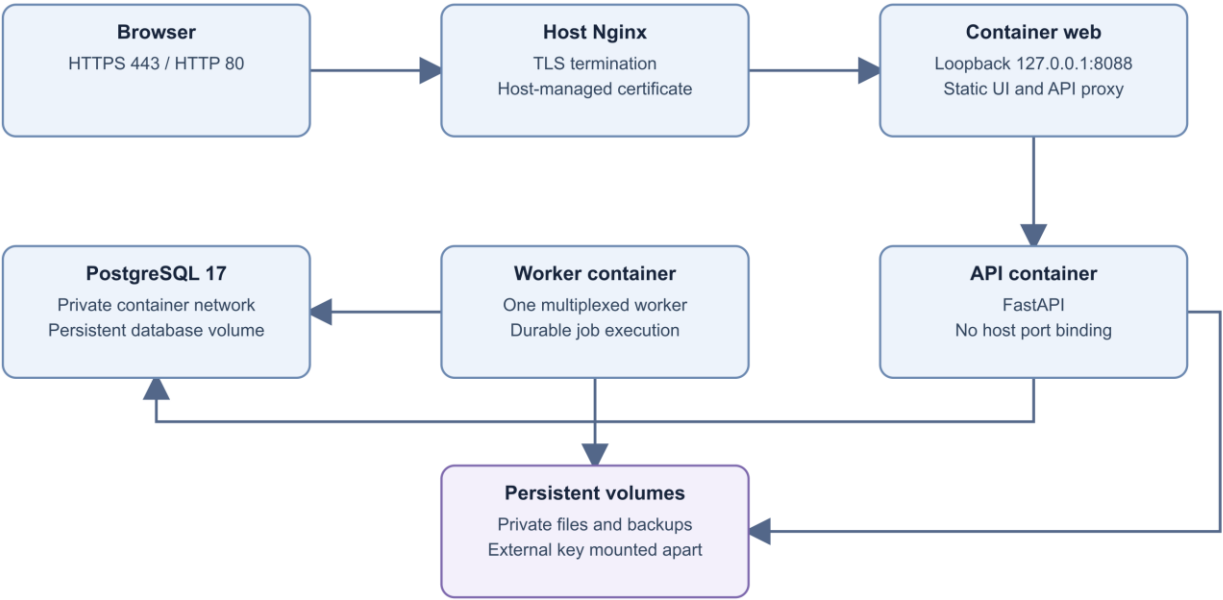


Database readiness does not prove worker progress or provider delivery.
Provider availability depends on configured operation and actor authorization.

Figure 29 Service dependencies

Linux deployment topology

Source-qualified Ubuntu amd64 package; one host

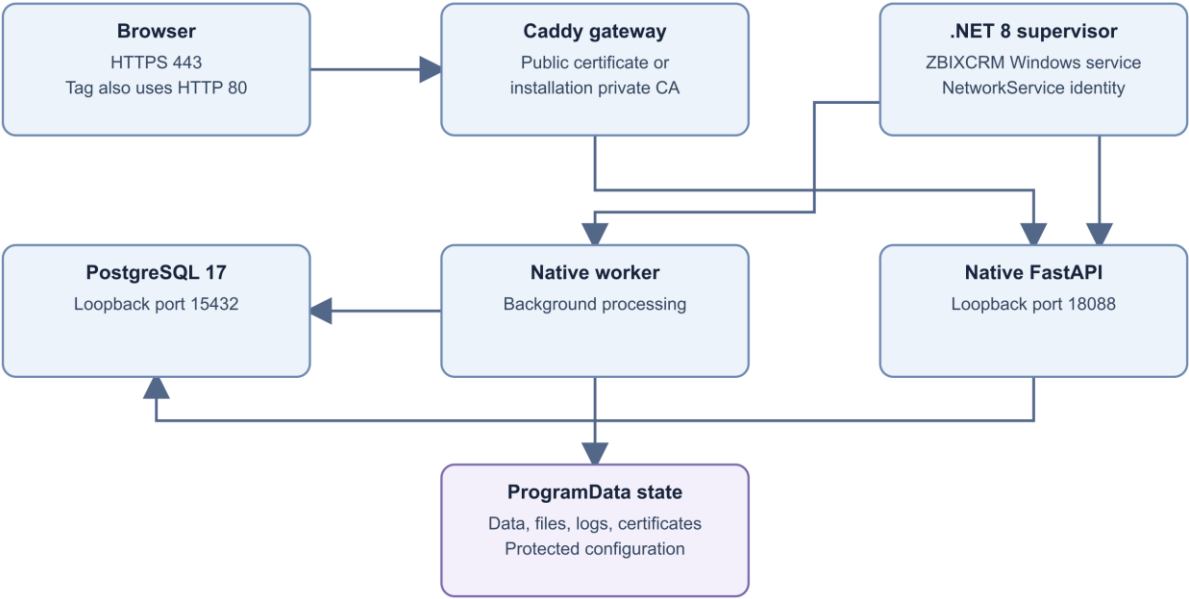


systemd wraps Docker Compose; database and API remain private.
Optional provider egress is configured separately. No HA or external broker is established.

Figure 30 Linux deployment topology

Native Windows topology

Tagged v1.2 runtime; supervised native processes

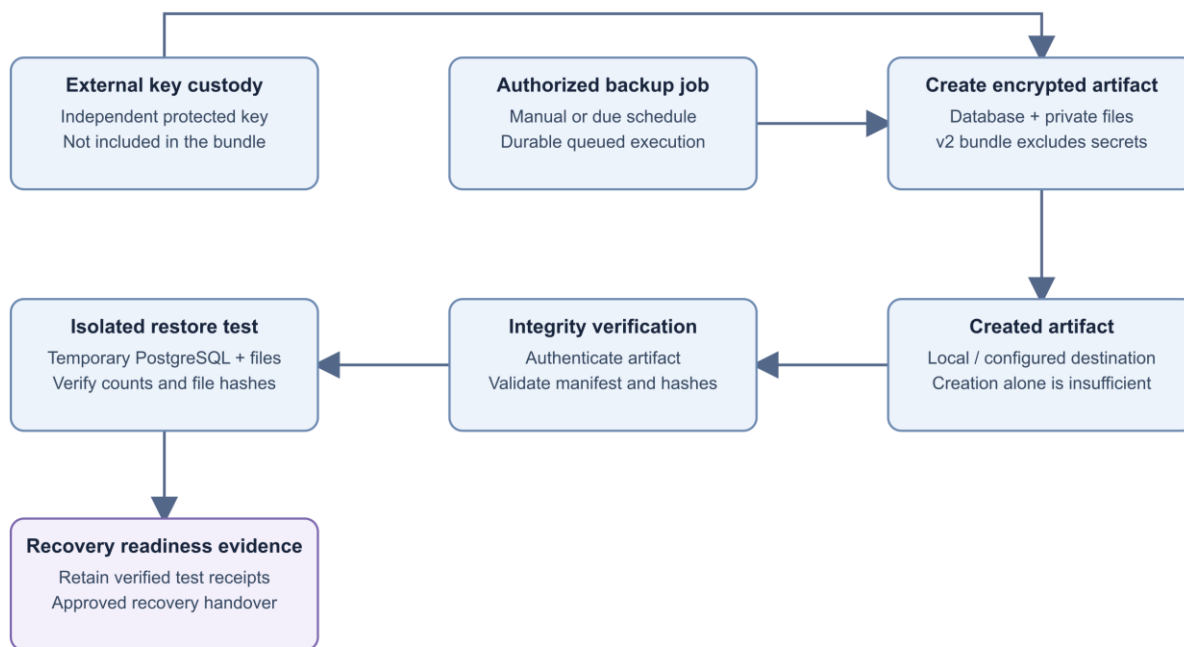


Supervisor also starts PostgreSQL and Caddy; its links illustrate process supervision.
Optional port 80 / IIS coexistence correction is post-tag, not qualified by v1.2 source.

Figure 31 Native Windows topology

Backup verification and recovery readiness

Separate creation, integrity verification and isolated restore evidence



Created, integrity verified and restore tested are distinct states; no live restore UI is provided.
Keep independent key custody and off-host copies; same-host storage is not disaster recovery.

Figure 32 Backup verification and recovery readiness

Important considerations

- GET /api/health is liveness; GET /api/ready checks database readiness. Neither alone proves background work or an external provider works.
- HTTP percentages are derived from bounded recent counters; absent request samples do not establish zero errors.
- Healthy backup status depends on several recorded prerequisites. Do not replace a degraded status with an assumption based on a file existing.

Troubleshooting

- The health page is denied: identity administration access is required.
- Database is reachable but jobs are delayed: investigate worker heartbeat, due work and operation-level history.
- Runtime identity is unreported: have the deployment owner reconcile the artifact and configuration privately.

Related knowledge base articles: Background processing and durable jobs; Operational logging and support evidence; Routine application maintenance checklist.

Troubleshoot import validation and execution

Zbix CRM 1.2.0 | Source reviewed | Reviewed 28 October 2026

Import Jobs stages CSV/XLSX source data, maps columns, validates a preview and requires explicit confirmation before writing CRM records. Validation creates no CRM records. Execution commits bounded batches, so cancellation or a later error does not undo rows already imported. Retry resumes interrupted work; it does not blindly rerun successful rows.

Use this guide to resolve invalid previews, stalled jobs and partial outcomes without duplicating records.

Before you begin

- The original uploader or another user with the required scoped job access and action permissions.
- A retained source file and the intended target module: Leads, Accounts, Contacts or Products.

Procedure

1. Open Administration > Import Jobs and inspect the job phase, processed counts and safe error. Determine whether it is parsing, mapping, validating, awaiting confirmation or importing.
2. If mapping is incomplete, map only supported target fields and select the intended duplicate handling. Validate again and review the current generation.
3. Review invalid and duplicate rows before confirming. Download error report CSV when available and correct the source rather than ignoring rejected relationships or required fields.
4. If confirmation is stale, refresh and validate the latest mapping. Changing mapping invalidates the previous preview token.
5. For a stalled or failed job, inspect worker health and current uploader permissions. Use Retry only for interrupted failed/cancelled work that the interface allows.
6. For completed row failures, prepare a corrected new file containing the intended unresolved rows. Reconcile created, updated, skipped and failed counts before another import.

Expected result

The import has a reviewed preview or a reconciled execution outcome, with committed records and failed rows clearly distinguished.

Important considerations

- Background jobs cap at 10,000 rows and 50 columns; the upload byte limit defaults to 10 MiB. Legacy synchronous imports retain a 1,000-row limit.
- XLSX formulas, error cells, macros, external links and unsafe archive content are rejected. Store dates as ISO date text.
- Mapping becomes immutable after execution starts. Cancellation waits for the active bounded batch and stops later batches.
- A repeated upload of the same source can return the existing job; this prevents accidental recreation.

Troubleshooting

- Ready preview cannot confirm: refresh after mapping changes and review the current validation result.
- Some rows imported before cancellation: reconcile the execution counts; cancellation is not rollback.
- Repeated data errors: fix the source and upload a corrected file rather than retrying unchanged failed rows.

Related knowledge base articles: Background processing and durable jobs; API validation and safe concurrency; Private files and generated document storage; Prepare a safe support case.

Troubleshoot attachment upload and download

Zbix CRM 1.2.0 | Source reviewed | Reviewed 28 October 2026

Attachment access depends on both the attachment action and visibility of its parent CRM record. New files enter a pending scan state. A download can remain blocked even though its filename appears in the record. File format validation and malware scan evidence are separate checks; an unavailable scanner is not a clean result.

Use this procedure for rejected uploads, quarantined files and missing downloads while preserving original evidence.

Before you begin

- Access to the parent record and appropriate attachment permissions.
- The original file, its type and size, without exposing its confidential contents in a ticket.

Procedure

1. Open the parent record and its Attachments tab. Confirm that the record itself is accessible to the affected user.
2. For upload failures, compare the file type and size with the supported types and installed limit. Use a simple filename of at most 200 characters.
3. Review the displayed scan state. Pending requires worker progress; unavailable or error requires scanner/service diagnosis; infected files must remain quarantined.
4. Ask the administrator to inspect System Health and scan diagnostics when processing does not advance. Verify storage availability as well as worker activity.
5. After an authorized scan or storage repair, refresh the attachment and try the normal download action. Do not retrieve private file bytes through an exposed server directory.

6. Escalate persistent failures with the parent module, attachment name/type/size, scan state, time and safe error.

Expected result

The cause is identified as permission, content/size validation, scan evidence or storage integrity, with the original file preserved.

Important considerations

- PDF, DOCX, XLSX, PNG, JPG/JPEG, TXT and CSV are allowlisted, subject to content checks. Renaming an unsupported file does not make it valid.
- Production release requires matching clean evidence and actual content. A local compatibility allowance is not a general production bypass.
- Pending, infected and error states do not become downloadable merely because an administrator can view the record.
- Deletion is a recorded operation with later retention cleanup; use the supported control instead of removing storage objects manually.

Troubleshooting

- Download returns not found: check both record visibility and attachment permission before assuming the bytes are absent.
- Scanner unavailable: resolve the configured scanning service and reprocess through the supported operation.
- Checksum/evidence mismatch: preserve the artifact and escalate for integrity review.

Related knowledge base articles: Private files and generated document storage; Authorization and permission evaluation; Read System Health and verify service readiness; Prepare a safe support case.