



YOUR PRODUCT. YOUR GUIDE.

Software User Guide

Access, configure, complete tasks, and get help

5 PAGES / FILLABLE FIELDS / COMPLIANCE REVIEW



Make this document yours

Product / system name

Name used on the product or release

Model / version / configuration

Exact models and versions covered

Document ID and revision

Controlled reference and revision number

Issue date and market

Date, language and countries covered

Responsible manufacturer / organization

Your organization's legal name and address

Author and support contact

Document owner, support email / phone / URL

Inside this template

- 02 Product, release, and audience
- 03 Access and configure the workspace
- 04 Complete common workflows and manage data
- 05 Software compliance, security, and release review

Authoring draft: fill the labeled fields, replace bracketed prompts, and add verified procedures and diagrams. Complete product and market review before release. This template does not certify a product.

DOCUMENT THE SOFTWARE VERSION

Product, release, and audience

Software behavior changes by release, platform, account role, and region. State the supported combination so users do not follow a path from a different build.

Document identity**Responsible organization and contact**

[Legal organization], [address], [support email / URL / phone]

Software identity

[Product name], [release or build], [platforms / editions]

Document control

[Document ID], [revision], [issue date], [language]

Audience and markets

[User roles and prerequisites], [countries or regions]

Purpose and supported environment

Describe the problem the software supports and which user roles may perform each task. List operating systems, browsers, devices, network needs, integrations, and account types only from the current support matrix. Explain how to find the version number and where release notes identify changed behavior.

Before following a workflow

- ☐ Confirm the software version and platform shown in this guide.
- ☐ Sign in with an account role that permits the task.
- ☐ Check organization settings and required integrations.
- ☐ Use test data when learning a consequential workflow.
- ☐ Keep credentials and recovery methods private.

Template status

Manual Tools by Manuals+ publishes this authoring template at <https://manual.tools>. It is not verified software documentation. The responsible organization must validate screenshots, permissions, data handling, and version-specific behavior.

SET UP A SAFE, USABLE ACCOUNT

Access and configure the workspace

Explain access in terms of a user's actual role and deployment. Separate administrator actions from individual preferences and describe expected confirmation states.

Initial access

1. Open the approved application address or install source for this release.
2. Authenticate using the organization's supported sign-in method.
3. Complete required verification or recovery setup through the approved flow.
4. Choose only the workspace, role, and permissions intended for your work.
5. Confirm the home screen, organization, and software version are correct.

Roles and permissions

Describe role names in plain language and connect each role to the actions it can perform. Tell users how to request missing access and who approves it. If an administrator changes membership, integrations, or retention settings, refer to the controlled admin guide rather than asking ordinary users to change them.

Environment record

Setting	Where to verify	Release-specific value
Application version	[Menu / command]	[Verified]
Supported platform	[Support matrix]	[Verified]
Account role	[Profile / admin view]	[Verified]
Help route	[In-product link]	[Verified]

Access issue

Never ask a user to disclose a password, one-time code, private key, or recovery phrase to support. Describe the approved account recovery path and escalation contact.

TASKS AND EXPECTED RESULTS

Complete common workflows and manage data

Use screenshots and labels that match the shipped interface. For consequential operations, make the review, confirmation, and undo or recovery behavior explicit.

Workflow: [task name]

1. Open [screen or menu] and check that the correct workspace is selected.
2. Enter or select the required information, noting any format or permission rule.
3. Review the summary, recipient, scope, and effect before confirming.
4. Select [action] and verify the stated completion result or status.
5. If the result is wrong, follow the documented correction path before repeating.

Data and connected services

Explain what information users enter, import, export, or share through the workflow. Describe available retention, deletion, export, or consent controls only as implemented in this release. Name connected services and explain where their separate permissions or terms apply. Link to the approved privacy notice.

User data practices

- ☐ Use only the data needed for the task and permitted by the organization.
- ☐ Review recipients and sharing scope before sending or exporting.
- ☐ Protect downloaded files and remove local copies according to policy.
- ☐ Report unexpected access, disclosure, or data loss through [incident route].

Release-specific workflow details

Roles allowed to complete task

[Role names and permission source]

Data categories and retention

[Verified categories, controls, policy link]

Recovery or undo behavior

[Available action and documented limits]

VERIFY OBLIGATIONS FOR THIS SOFTWARE

Software compliance, security, and release review

Software risks and obligations depend on function, deployment, users, data, and markets. Record the applicable requirements and evidence, and route the guide for qualified review.

User-facing notices and limits

Include current security and privacy guidance, supported-version limits, accessibility instructions, and warnings for workflows with financial, health, safety, or irreversible effects where relevant. Identify when a user must stop and contact an administrator or support. Keep statements consistent with actual controls and the approved product notices.

Product-specific compliance author prompts

- ☐ Identify which privacy, security, accessibility, consumer, sector, export, and language requirements apply by deployment and market.
- ☐ Insert verified notices, retention or consent controls, accessibility guidance, and supported-version policy references.
- ☐ Record threat reviews, privacy assessments, accessibility tests, security testing, and release evidence by ID.
- ☐ Route claims and the final guide to appropriate security, privacy, accessibility, legal, and product reviewers.

Organization and review record**Responsible organization and support contact**

[Legal name, address, support email / URL / phone]

Applicable markets and release revision

[Markets, software versions, document ID, revision / date]

Evidence and notices

[Assessment / test / notice IDs and revisions]

Review sign-off

[Reviewer name, role, date, decision, approval record]

Publication decision

This Manual Tools by Manuals+ template at <https://manual.tools> does not establish software security, legal compliance, or accessibility conformance. Publish only after the responsible organization verifies the released system and approves its evidence-backed statements.

Official reference starting points - applicability must be determined for your product and market.

W3C: Web Content Accessibility Guidelines 2.2
European Commission: GDPR applicability