

SecurITPosture

Customer guide

Administrator guide

Users and roles, AI settings, support access, backups, updates, and integrations.

Version 0.1.0

Generated 2026-10-16

Draft: steps are specified but not final.

Vesta Cyber Solutions. Made from the same source as the guide on the web, so the two always match.

Contents

Users and roles	3
AI settings	3
Support access	4
Backups and restore	4
Applying a signed update	5
Turning integrations on	5
Other settings	5

This guide is for the system administrator of a SecurITPosture install. The system administrator manages users, settings, and the platform. By design, the system administrator does not perform assessment or approval work.

Users and roles

Open Settings, then User accounts. Only a system administrator can manage users.

1. Choose Create user. Enter the person's name and username, and choose a role.
2. The product sets a temporary password, shown once. Hand it to the person through a channel your organization approves.
3. At first sign in, the person must replace the temporary password before they can open any page.
4. From the same page you can change a role, deactivate an account, unlock a locked account, and end a person's sessions. Changes take effect at once and are recorded in the audit log.

The roles:

- Customer user: works inside your workspace. Views, creates, and updates records, uploads documents, and edits worksheets.
- Compliance analyst: day to day compliance work. Evidence, documentation, findings and remediation, AI drafts, reports, and worksheets. Connects integrations.
- Assessor: independent review. Records evidence reviews, test results, and findings, and maintains the SAP, SAR, and RET. Does not administer the platform.
- System administrator: users, roles, settings, and platform health. Does not assess or approve.
- Executive: dashboards, reports, metrics, and summaries. Does not do day to day work.
- Approving official: accepts or rejects AI drafts. Should not approve what they created.

Signing and exporting an authorization package is not tied to a role. Only the person you name as the system's accountable official may sign, after confirming the attestation in the product. A system administrator names the official, never themselves and never another administrator, and an administrator never signs.

Settings, Roles and permissions lists every capability per role, from the same rules the server checks.

Two step sign in, by password plus an emailed code, is decided and not built yet.

AI settings

Open Settings, then AI assistance. Only a system administrator can change these settings, and every change is recorded in the audit log.

- AI on or off. In the appliance, AI is on by default for a new workspace, because the model runs inside the virtual machine and nothing leaves it. You can switch it off at any time. Switching it off always works.
- Review threshold. Drafts with confidence below the threshold are marked low confidence for the final review. The default is 0.80 (80 percent). You can set it between 0.50 and 0.99.

- Requester and approver must differ. When on, a person cannot accept an AI draft they requested or edited. On by default. When off, such a decision is allowed and marked self decided in the audit log.
- AI disclosure page. When on, generated provider documents include one page that lists each AI assisted section and who accepted it. On by default. The package metadata records AI assistance whatever this setting says.

See [Working with the AI](#) for what the AI drafts and how people review it.

Support access

Open Settings, then Support access. Only a system administrator can use it. See [Support](#) for what Vesta support can and cannot do.

1. Create a support account for the engineer Vesta names on your case: their name and a username. The product shows a temporary password once. The account cannot sign in yet.
2. Grant support: choose the account, enter the case reference, choose when it starts (now, or up to 14 days ahead) and how long it lasts (1, 2, 4, or 8 hours). The scope is read only.
3. While the grant is live, every administrator sees a notice naming the engineer and the time left.
4. Revoke the grant at any time. The engineer's sessions end at their next request. A grant also ends by itself when its time is up.

Grants cannot overlap for the same account, and a revocation cannot be undone. Every grant, revocation, and action by the engineer is in the audit log, marked as support.

Backups and restore

Draft, pending the appliance build. The commands below are from the container install. Inside the appliance they may be run differently.

Choose how you back up. The simplest choice is your platform's snapshots of the virtual machine (AWS, Azure, VMware, or Hyper-V). The product also has its own backup, which copies the database and every stored file into one archive with a manifest of SHA-256 hashes.

Keep the field encryption key safe and separate. Stored files and integration secrets are encrypted with it. A backup cannot be read without the same key, and Vesta does not hold a copy.

To back up with the product's tool:

1. Run `docker compose --env-file .env.docker --profile tools run --rm tools npm run backup`.
2. The last line names the archive and its manifest hash.
3. Copy the archive off the machine to encrypted storage. It holds your data.

To restore:

1. Take a backup of the current state first. A restore replaces the current data.

2. Put the archive in the backups folder.
3. Run `docker compose --env-file .env.docker --profile tools run --rm tools npm run restore -- /backups/<archive>.tar.gz`.
4. The restore checks every entry first. If anything is missing, extra, or changed, it prints "refused, nothing was changed" and stops.
5. Otherwise it replaces the database and stored files and writes a restore event to the audit log.
6. Restart the application.

Applying a signed update

Draft, pending the appliance build. How an update file is imported into the appliance is not built yet.

Updates are never automatic. The appliance never checks for or downloads updates. You choose when to apply one.

1. Download the update file from the Vesta support site and verify it. See [Getting updates](#).
2. Take a backup or a snapshot first.
3. Read the release notes. If the release changes the AI model, the notes say so.
4. Apply the update with the written instructions that come with the release.
5. After the update, open Settings, then About, to confirm the version.

Turning integrations on

Integrations are off until someone connects them. A compliance analyst or a system administrator can connect them; every role can see the integration pages.

1. Open Integrations and choose AWS, Tenable, Jira, or Microsoft Entra ID.
2. Follow the setup on that page. For AWS, see Instance role, IAM Roles Anywhere, or Access key.
3. The product validates the connection before it marks it connected.
4. Once connected, the appliance talks only to the endpoints you configured. Removing an integration keeps its audit history.

Other settings

- Known exploited vulnerabilities: import the CISA catalog as a file. The appliance does not fetch it.
- Organization: export everything your organization owns, or delete it with the audit trail kept.
- Audit log: every sign in, change, refusal, and export, with who, when, and from where.
- About: the version and build, where the product runs, the licence, and how to reach support.