

SecurITPosture

Customer guide

Install on Azure

The same for Microsoft Azure.

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

Before you start	3
What is inside the appliance	3
Size	4
Install	4
FAQ	5
What does the appliance send out?	5
Does the appliance need the Azure agent?	5
Do boot diagnostics keep the first password?	5
Can I put a load balancer in front of the appliance?	5
How large can uploads be?	6
Troubleshooting	6
An integration cannot connect	6
The disk upload or the disk creation fails	6
The virtual machine boots with a smaller disk than expected	6
Users cannot reach the site	6
The virtual machine starts but never answers	7
Every change in the product is refused	7

Draft, pending the appliance build. The appliance image, its import steps, and the first start setup are specified but not built yet. Steps marked draft will change once the image is built and tested.

SecurITPosture is delivered as one virtual machine image (an OVA file). The same image runs on AWS, Azure, VMware, and Microsoft Hyper-V. This page covers Azure. As of 2026-10-15, only the AWS install is being proven; nothing on this page has been run on Azure yet.

A Vesta deployment engineer installs the appliance with you, at your site and in your environment. This page tells you what to prepare and what happens during the install.

Before you start

Prepare these before the Vesta engineer arrives:

- ☐ An Azure subscription, resource group, and virtual network where the appliance will run.
- ☐ A subnet for the appliance, and a static private IP address for it.
- ☐ A network security group that allows inbound HTTPS (port 443) from your users, and inbound SSH (port 22) from your administrators only.
- ☐ Someone with rights to create a managed disk and a virtual machine in that resource group, available during the install.
- ☐ The virtual machine size you will use (see Size below).
- ☐ The host name your users will type in the browser, and a DNS record for it pointing at the appliance's private IP address.
- ☐ Your own TLS certificate and key for that host name, issued by your certificate authority.
- ☐ Who will be the first administrator inside the product. They will set a password and enrol MFA at first start.
- ☐ Who will hold the operating system account, and their SSH public key. First start installs the key; SSH accepts no password.
- ☐ If the appliance will read an AWS account, the connection it will use. Outside AWS this is IAM Roles Anywhere or, as a last resort, an access key. See [Connect AWS with IAM Roles Anywhere](#).
- ☐ A safe place, outside the appliance, for a recovery copy of the field encryption key.

What is inside the appliance

- Ubuntu 24.04 LTS Server.
- The SecurITPosture application.
- A PostgreSQL 17 database. Your data stays inside the virtual machine.
- Apache in front of the application, serving HTTPS. The current build still uses Caddy; Apache replaces it before release.
- A small open source AI model that runs inside the virtual machine. Nothing it reads leaves the virtual machine. The model ships as its own signed file beside the image and is not in the image yet.

Size

The size below is provisional. Vesta measures the appliance under a realistic load and will publish a minimum and a recommended size with each release. Until then, use:

- Without AI: 4 virtual CPUs, 8 GiB of memory, 100 GB of disk.
- With the AI model on (the default): 8 virtual CPUs and 16 GiB of memory, with the same disk.

The appliance picks the larger AI model when the virtual machine has 16 GiB of memory or more, and the smaller one otherwise; an administrator can switch later. The AI model runs without a graphics card. If the virtual machine size includes a supported GPU, the appliance uses it. A GPU is never required.

Install

Draft, pending the appliance build. Azure runs virtual machines from a fixed size VHD. The release is planned to include one; until it does, your engineer converts the OVA's disk.

1. Download the image and its checksum file from the Vesta support site, and verify it. See [Getting updates](#).
2. Your engineer prepares a fixed size VHD from the image, aligned to 1 MiB, as Azure requires.
3. Your engineer creates an empty managed disk sized for the VHD, uploads the VHD into it, and closes the upload.
4. Create a virtual machine from that managed disk as a specialized Linux disk, at the size you chose, in the network and security group you prepared, with the static private IP address and boot diagnostics on.
5. Start the virtual machine. The appliance makes its own secrets on the first boot: the database passwords, the session secret, and the field encryption key. They are readable by the root user only. Vesta never holds them.
6. First start asks for the network settings: the IP address, netmask, gateway, and DNS servers, or DHCP.
7. First start asks for the host name.
8. First start creates the product's first administrator, who sets a password and enrolls MFA.
9. First start takes the operating system account's SSH public key from a small disk labelled SPSETUP holding it as `ssh_authorized_key.pub`, which your Vesta engineer attaches before the first start. The prompt for it is on the virtual machine's first screen, which this platform's serial console does not show, so without that disk first start waits and the product does not start; a prompt on the serial console is planned. The disk may also carry `os_password.sha512`, a SHA-512 crypt hash of the account's password; without it, the password is asked on the first screen. The account `spadmin` accepts an `ssh-rsa` key of 3072 bits or more, or an `ecdsa-sha2-nistp256` or `nistp384` key; an `ssh-ed25519` key is accepted but stops working if FIPS mode (Ubuntu Pro) is turned on later. A key that does not qualify is refused with the reason, and first start asks again. First start then asks twice for a password for `spadmin`, at least 15 characters, used only for `sudo` and for signing in on the console to recover the virtual machine. SSH accepts the key and never a password, and never root.

10. Save the recovery copy of the field encryption key in your safe place. Stored files and integration secrets are encrypted with it, so a backup cannot be read without it. Vesta does not hold a copy.
11. A self signed certificate is created so first start always finishes. Install your own certificate for the host name.
12. Sign in as the first administrator and create user accounts. See the Administrator guide.
13. Harden the operating system to your own baseline. Vesta does not apply STIG hardening to the appliance; your organization hardens the operating system.
14. Decide how you will back up the appliance. Azure snapshots of the virtual machine's disk are the simplest choice. The product also has its own backup. See the Administrator guide.

Steps 6 to 9 are decided but not built yet. Until first start is built, the first boot takes its address from DHCP and prints a generated password for the product's first administrator once on the console. The first sign in must change it. Open the product by its IP address until then, because the site answers for that address only.

FAQ

What does the appliance send out?

By default, nothing. Every feature that would fetch from the internet is off; the CISA known exploited vulnerabilities catalog is imported as a file in Settings. The appliance never checks for updates and never downloads anything. The AI model runs inside the virtual machine. Integrations (AWS, Tenable, Jira, Microsoft Entra ID) are off until an administrator connects them; once connected, the appliance talks only to that integration's endpoints, on port 443, and only from the application: an AWS connection reaches the AWS endpoints of the regions you chose, Tenable and Jira reach the host you entered, and Microsoft Entra ID reaches its sign in and Graph hosts. While any integration is connected the appliance also asks its own DNS servers for those names, at a limited rate. Removing the integration closes its endpoints. Addresses on your private networks stay closed unless your administrator allows the range (see the troubleshooting entry below), and Tenable and Jira must answer on port 443. Vesta support has no standing access and no connection into the appliance. See Support.

Does the appliance need the Azure agent?

No provisioning agent is needed, because the virtual machine is created from a specialized disk that already holds the operating system. The appliance turns cloud-init off after it is built, so Azure does not install an SSH key or user you name when you create the virtual machine. First start installs the operating system account's SSH key instead.

Do boot diagnostics keep the first password?

They can. Boot diagnostics keep what the console shows, and today's first boot prints the first administrator's password there. That is why the first sign in must change it. First start, when built, sets the password instead of printing one.

Can I put a load balancer in front of the appliance?

Tell your Vesta engineer first. The application trusts exactly one proxy in front of it (`TRUSTED_PROXY_HOPS=1`), and a load balancer adds a second hop.

How large can uploads be?

Files up to 1 GB. The appliance allows 30 minutes per upload, enough for 1 GB at about 5 Mbit/s. Scan files are limited to 100 MB each.

Troubleshooting

An integration cannot connect

The appliance opens an integration's endpoints only while the integration is connected, and logs every address it opens, closes, or refuses.

What to check: sign in over SSH as `spadmin` and run `journalctl -t sp-egress --since today`. A line naming a private address means the range is not allowed: add it, as narrow as you can (ideally one address as a `/32`), to `/etc/security/egress-private.allow` with `sudo`, owned by `root` and writable only by `root`. A Tenable or Jira address on a port other than 443 is refused.

What to send Vesta: the `sp-egress` lines from the journal, the integration's type, and the exact message the product showed.

The disk upload or the disk creation fails

Azure accepts only a fixed size VHD whose size is a whole number of MiB, and the upload size must be the VHD's full size including its 512 byte footer.

What to check: the file is a fixed size VHD, not dynamic and not the OVA's VMDK; its size is a whole number of MiB plus the 512 byte footer; the managed disk was created with that exact upload size; the upload access was closed before you created the virtual machine.

What to send Vesta: the VHD's exact size in bytes, the managed disk's size, and the error Azure showed.

The virtual machine boots with a smaller disk than expected

What to check: the managed disk is at least 100 GB. On its first boot the appliance grows its root file system into the whole disk; if that fails, the boot log says the root file system keeps its size.

What to send Vesta: the managed disk's size and the lines from boot diagnostics that start `[firstboot]`, with any password line removed.

Users cannot reach the site

What to check: the network security group on the subnet or the network interface allows inbound 443 from the users' network, at a higher priority than any deny rule; the DNS record points at the virtual machine's private IP address; the users open the address the site answers for (the IP address until first start sets the host name).

What to send Vesta: the effective security rules for the network interface, the virtual machine's private IP address, and what the browser shows.

The virtual machine starts but never answers

What to check: the boot diagnostics serial log for lines starting [firstboot]. If the size has accelerated networking, the extra network interface it adds also takes DHCP; that is expected and harmless.

What to send Vesta: the serial log with any password line removed, the virtual machine size, and the time you started it.

Every change in the product is refused

What to check: the browser's address is the one the site was set up for. The application compares the browser's origin with the site's own host name and refuses every change when they differ. If you changed the web server settings, keep ProxyPreserveHost On.

What to send Vesta: the address in the browser, the address you set at first start, and the version shown in Settings, then About.