

SecurITPosture

Customer guide

Install on VMware

The same for VMware vSphere.

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 include VMware Tools?	5
Can I change the network adapter type?	5
Can I put a load balancer in front of the appliance?	5
How large can uploads be?	5
Troubleshooting	6
An integration cannot connect	6
The OVA will not import	6
The virtual machine has no network	6
The clock is wrong, or times in the audit log are off	6
The virtual machine starts but never answers	6
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 VMware. As of 2026-10-15, only the AWS install is being proven; the OVA has not been imported into VMware 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:

- ☐ A vSphere cluster or ESXi host, and a datastore with room for a 100 GB disk.
- ☐ A port group on the network where users will reach the appliance.
- ☐ A static IP address for the virtual machine, with its netmask, gateway, and DNS servers.
- ☐ Firewall rules that allow inbound HTTPS (port 443) from your users, and inbound SSH (port 22) from your administrators only.
- ☐ Someone with rights to deploy an OVF template and open the virtual machine's console, 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 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.
- ☐ Your own time servers (NTP), and the host's clock set correctly. Audit timestamps depend on the time.
- ☐ 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 OVA 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. This is the OVA's default hardware.
- 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 host passes a supported GPU to the virtual machine, the appliance uses it. A GPU is never required.

Install

Draft, pending the appliance build. The OVA is an OVF 1.0 package with a stream optimized VMDK disk, which VMware imports directly. The import has not been tested on a released image yet.

1. Download the OVA and its checksum file from the Vesta support site, and verify it. See [Getting updates](#).
2. In the vSphere Client, choose Deploy OVF Template and select the OVA file.
3. Choose the name, folder, host or cluster, datastore, and port group.
4. Set the virtual CPUs and memory to the size you chose before the first power on.
5. Power on the virtual machine and open its console. 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 asks on the console for the operating system account's SSH public key, on one line. Paste it with the console's Type text feature, or type it, press Enter, check the fingerprint shown, and type yes. Your Vesta engineer can instead attach a small ISO labelled SPSETUP holding the key as `ssh_authorized_key.pub`. 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. VMware snapshots or your existing virtual machine backup tool 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 include VMware Tools?

Not in the current build. The image does not install open-vm-tools, so the vSphere Client may report VMware Tools as not installed.

Can I change the network adapter type?

The OVA declares an E1000 adapter and an LSI Logic disk controller. Keep them for now: they are the types the image is built and tested for, and another type has not been tested.

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/securitposture/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 OVA will not import

What to check: the checksum matched before import; you chose the OVA file itself, not a folder; the host supports virtual hardware version 13 or later. The OVA carries its build manifest as an extra file; whether every VMware version accepts it is confirmed at the first import, and if one refuses it, Vesta ships it beside the OVA instead.

What to send Vesta: the exact error from the vSphere Client, the vSphere and ESXi versions, and the OVA's file name and checksum.

The virtual machine has no network

What to check: the adapter is connected at power on and on the right port group; the adapter type is still E1000; the port group's VLAN reaches your gateway. Until first start is built, the appliance takes its address from DHCP, so the network needs a DHCP server or a reservation.

What to send Vesta: the adapter type and port group, and a photo or copy of the console.

The clock is wrong, or times in the audit log are off

The appliance turns off Ubuntu's own network time service, because nothing may leave the virtual machine unless you allow it. It does not include VMware Tools, so the host does not set its clock. Setting a time source is not built yet: first start is planned to open your own time servers.

What to check: the ESXi host's clock and its NTP settings; the time the console shows.

What to send Vesta: the host's time, the appliance's time, and your time servers' addresses.

The virtual machine starts but never answers

What to check: the console for lines starting `[firstboot]`; the firewall rules for 443; that the virtual machine was not powered off during its first boot. A first boot that stopped part way starts again from nothing on the next boot.

What to send Vesta: a copy of the console with any password line removed, the size you set, and the time you powered it on.

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.