

FreeSRA Installation Runbook

Version 0.2 · 2026-10-14 · Audience: the operator installing a FreeSRA gateway and its first site connector.

This runbook is a step-by-step procedure. Each step says what to do, what you should see, and what to check before moving on. Reference material (architecture, ports, licences) is in the `docs/` folder of the repository.

1. Before you start

1.1 What you will build

Node	Where	What it does
Gateway	Off-prem (cloud VM or DMZ)	Public entry point: web portal, identity provider, overlay controller, session broker, file airlock, management console
Site connector	On-prem, inside the plant or data-centre network	Dials out to the gateway and publishes local assets; nothing is opened inbound
Clients	Users' devices	A browser; optionally the Ziti Desktop Edge client for native tools

1.2 Requirements checklist

Gateway host:

- ☐ Linux VM with a **public IPv4 address** (or a DMZ host with ports forwarded to it)
- ☐ **DNS A record** for the gateway name (for example `gw.example.com`) pointing at that address, already propagated
- ☐ 2 vCPU, 4 GB RAM, 40 GB disk minimum (8 GB RAM if you enable ClamAV and CrowdSec)
- ☐ Either the FreeSRA appliance image **or** a Linux OS with Docker Engine 24+ and Compose v2 (or Podman 4.4+ with Compose v2)
- ☐ Inbound allowed from the Internet on **tcp/443, tcp/1280, tcp/3022** (plus tcp/80 for certificate issuance)
- ☐ Inbound allowed from your admin network on **tcp/22 and tcp/8443**
- ☐ Outbound allowed to the Internet (container images, certificate authority)

Site connector host:

- ☐ Linux host or the FreeSRA site appliance image on the plant network, 1 vCPU, 1 GB RAM
- ☐ **Outbound only** to the gateway name on tcp/443, tcp/1280, tcp/3022, plus DNS and NTP
- ☐ Layer-3 reachability from the connector to the assets you will publish (PLCs, HMIs, servers)
- ☐ No inbound rule needed

Information to have at hand:

- ☐ Gateway public name (FQDN)
- ☐ An email address for certificate notices (ACME)
- ☐ Name and email of the first administrator
- ☐ WAN interface name of the gateway (for example `eth0`); management interface name if there is one
- ☐ CIDRs of your admin networks (who may reach SSH and the console directly)
- ☐ For each site: the plant subnets that contain assets to publish

1.3 Decide your options

Option	Default	When to change it
ClamAV scanning in the airlock	off (YARA, file-type and hash policy are always on)	You want signature antivirus and accept pulling a GPL-2.0 engine from upstream

Option	Default	When to change it
Public SFTP (tcp/2022)	off (WebDAV/HTTPS and overlay SFTP only)	Users must use SFTP clients from outside the overlay
Keystroke recording	off	Compliance requires it; inform users
Let's Encrypt staging CA	off	First rehearsal on a throwaway host, to avoid rate limits

2. Install the gateway

Choose **2A** (appliance image), **2B** (existing container host) or **2C** (CLI only). All three end at step 3.

2A. Appliance image

- 1 Deploy the `freesra-gateway` image: `qcow2` for KVM/Proxmox, `vmdk` for VMware, `VHD` for Hyper-V/Azure, AMI for AWS, or boot the ISO on bare metal (`images/README.md` describes the build).
- 2 Give the VM its network. On first boot the console (VM screen or serial) prints:

```
FreeSRA gateway: open https://<ip>:8443/setup
Setup token: xxxxxxxxxxxxxxxxx
```

The same token is in `/var/lib/freesra/gateway/console/recovery-token` on the host.

- 3 Continue with step 3.

Unattended variant: seed `/etc/freesra/gateway.env` with `FREESRA_FQDN`, `ACME_EMAIL` and `FREESRA_ADMIN_EMAIL` through `cloud-init write_files` or the `kickstart %post` section; first boot then installs without the wizard and you skip to step 4.

2B. Existing container host (Docker or Podman)

- 1 Clone the repository and start the console:

```
git clone https://github.com/pascalseguin/FreeSRA.git
cd FreeSRA
bin/freesra bootstrap
```

Podman users first export `DOCKER_SOCKET=/run/podman/podman.sock` and `FREESRA_COMPOSE="podman compose"`. The console image is built locally unless `FREESRA_CONSOLE_IMAGE` points to a registry.

- 2 Expected output ends with:

```
FreeSRA Console is running in setup mode.
Open   https://<this host>:8443/setup
Token  xxxxxxxxxxxxxxxxx
```

- 3 Continue with step 3. After the wizard, apply the host firewall once (the console only renders it on non-appliance hosts):

```
sudo bin/freesra firewall apply --role gateway --wan eth0 --admin-cidrs 203.0.113.0/24
```

2C. CLI only (automation)

```
bin/freesra init --fqdn gw.example.com --email ops@example.com --admin-email ops@example.com --yes
bin/freesra up
sudo bin/freesra firewall apply --role gateway --wan eth0 --admin-cidrs 203.0.113.0/24
```

Skip to step 4.

3. Run the setup wizard

- 1 Open `https://<gateway-ip>:8443/setup`. The certificate is self-signed at this point; accept the warning.

- 2 Enter the setup token.
- 3 Fill in the four sections:
 - **Public identity:** the FQDN and the ACME email.
 - **First administrator:** username, email, optional temporary password (generated if empty).
 - **Network and firewall:** WAN interface, management interface (optional), admin networks.
 - **Options:** ClamAV, public SFTP, keystroke recording.
- 4 Click **Install FreeSRA**. The log page shows image pulls, database initialisation, identity-provider import and overlay bootstrap. First run takes 3 to 10 minutes depending on bandwidth.
- 5 **Check:** the status badge turns `ok` and the **Continue** button appears. If it turns `failed`, read the last lines of the log; section 9 lists the usual causes. The wizard can be re-run after fixing the cause.
- 6 The "FreeSRA is up" page lists the user portal, the console addresses and the first administrator's temporary password. Copy the password now.

4. First sign-in and hardening

- 1 Open `https://<fqdn>/`. **Check:** the page loads with a valid certificate (no browser warning). If you see a warning, certificate issuance has not completed; see section 9.
- 2 Click **Remote desktops**, sign in as the first administrator, set a new password, enroll an authenticator app (TOTP). Both are mandatory.
- 3 Open the console at `https://<gateway-ip>:8443/` from an admin network and sign in with single sign-on. **Check:** the dashboard shows the identity provider and the overlay controller as reachable, and every service as running.
- 4 On the **Firewall** page confirm the status reads `applied`. On appliances this happens automatically; on container hosts run the `firewall apply` command from step 2B.
- 5 Install the Ziti Desktop Edge client on your workstation (Windows, macOS, Linux, iOS or Android, from openziti.io), add the network `https://<fqdn>:1280` and sign in with your FreeSRA account. **Check:** the console is now also reachable at `https://admin.freesra.ziti/`.
- 6 Optional: on the **Devices** page download the break-glass identity token `freesra-admin.jwt` and store it offline; it grants overlay admin access without the identity provider.

5. Add a site

- 1 Console → **Sites** → enter a short name (`plant1`) → **Create site and bundle**. The job log shows the private router being registered.
- 2 Download the bundle (`freesra-site-plant1.tar.gz`). It contains a single-use enrollment token and a per-site policy token; treat it like a credential.
- 3 On the connector host inside the plant network:

```
tar xzf freesra-site-plant1.tar.gz && cd connector
./connector.sh up
sudo ./connector.sh firewall --lan eth0 --ot-subnets 10.10.1.0/24
```

`--ot-subnets` lists every subnet that contains assets you will publish; add `--mgmt-cidrs` for the network that may SSH to the connector.

Site appliance variant: copy the bundle's `.env` to `/etc/freesra/site.env` and `state/site.jwt` to `/var/lib/freesra/site/site.jwt`, set `FREESRA_OT_SUBNETS` and `FREESRA_LAN_IF` in the env file, then `systemctl start freesra-firstboot`.

- 4 **Check:** `./connector.sh status` shows the router container healthy; within a minute the console's **Sites** page shows the connector as online and a "last config pull" timestamp.

6. Publish targets

- 1 Console → **Targets** → choose the site, name (hmi1), host or IP, protocol and port, allowed groups.
 - For a PLC with read-only access, choose protocol `modbus` and tick **Read-only Modbus**; the connector's ot-proxy enforces it.
 - For RDP hosts with self-signed certificates tick **ignore the server certificate**.
- 2 **Check**: the job completes with ok; the target appears in the list; for RDP/VNC/SSH/Telnet it also appears under **Browser**.
- 3 Open `https://<fqdn>/guacamole/` as a member of an allowed group and start the connection. **Check**: the session opens and, afterwards, appears under **Sessions** with a recording file.
- 4 For native tools, from a workstation with the Ziti client signed in: connect to `hmi1.plant1.freesra:<port>`. **Check**: the connection succeeds only for identities in the allowed groups.

7. Users

- 1 Console → **Users** → **Invite a user**: username, email, groups. A temporary password is shown once; give it to the user through a separate channel.
- 2 The user signs in at `https://<fqdn>/`, changes the password and enrolls an authenticator.
- 3 For SFTP or WebDAV the user opens **My account**, creates an app password or adds an SSH key, then connects to `https://<fqdn>/dav/` or `sftp -P 2022 <user>@<fqdn>` (SFTP over the overlay, or publicly if enabled).
- 4 Directory integration (LDAP, Active Directory, SAML): **Users** → **Open the full identity console** → *Identity providers* or *User federation*. Map directory groups onto `ot-engineers`, `it-operators`, `vendors` and `freesra-admins`.

8. Verification checklist

- ☐ `https://<fqdn>/` serves a valid certificate
- ☐ First administrator can sign in with password + authenticator
- ☐ Console dashboard: identity provider reachable, overlay reachable, all services running, firewall applied
- ☐ From the Internet, only `tcp/443`, `tcp/1280` and `tcp/3022` (and `tcp/80`) answer on the gateway; `tcp/8443` and `tcp/22` answer only from admin networks (test with `nmap` or `nc` from an outside host)
- ☐ Site connector shows `online` on the Sites page
- ☐ A browser session to a published target works and produces a recording
- ☐ A native-client connection to a published target works through the Ziti client
- ☐ An upload to the airlock appears in the user's files after a few seconds; the EICAR test file is quarantined and listed under **Airlock**
- ☐ A read-only Modbus target refuses a write (function code 16 returns an exception) and the event appears in the connector's ot-proxy log
- ☐ **System** → **Create backup now** completes and the archive can be downloaded

9. Troubleshooting

Symptom	Likely cause	Action
Wizard job fails while pulling images	No outbound Internet, or a registry blocked	Allow egress to <code>docker.io</code> , <code>quay.io</code> , <code>ghcr.io</code> ; re-run the wizard

Symptom	Likely cause	Action
Wizard job fails at "waiting for ziti-controller"	Host lacks resources or the controller port is busy	<code>freesra logs ziti-controller</code> ; check tcp/1280 is free
Browser warning on <code>https://<fqdn>/</code> after install	DNS not yet pointing at the host, or tcp/80 and tcp/443 not reachable from the Internet, or Let's Encrypt rate limit	Check <code>freesra logs caddy</code> ; fix DNS or firewall; use the staging CA for rehearsals
"Identity provider unreachable" on the dashboard	Keycloak still starting (first start takes minutes) or import failed	<code>freesra logs keycloak</code> ; the realm import log names the failing field
Console at :8443 not reachable	Host firewall admin networks do not include your source address	From the gateway shell: <code>sudo freesra firewall apply --role gateway --admin-cidrs <your-cidr></code>
Connector stays not registered or offline	Token already used or expired; gateway ports blocked outbound	Sites → re-issue token , redeploy the bundle; verify outbound tcp/1280 and tcp/3022
Connector online but target unreachable	Wrong asset IP, asset blocks the connector, or OT subnet missing from the connector firewall	From the connector host: <code>nc -vz <asset> <port></code> ; re-run <code>connector.sh firewall</code> with the right <code>--ot-subnets</code>
Modbus tool gets "illegal function"	Read-only policy working as intended	Use a target without read-only, or switch the listener to an allow-list under OT policies
Airlock upload never appears	Scanner blocked it, or the file is still being written	Airlock page shows the event; quarantined files list the reason
Locked out of the console (identity provider down)	—	Sign in with the recovery token from <code><state>/console/recovery-token</code> ; over SSH use <code>ssh -L 8443:127.0.0.1:8443 <gateway></code> then <code>https://localhost:8443/</code>

Useful commands on the gateway host:

```
bin/freesra status           # services and overlay routers
bin/freesra logs <service>   # caddy, keycloak, ziti-controller, console, airlock, guacamole, ...
bin/freesra backup           # databases, overlay state, TLS material, env file
bin/freesra ziti edge list services
```

10. Backup, update and rollback

- **Backup:** System → Create backup now (or `freesra backup`). Copy `<state>/backups/*` off the host. Recordings and the airlock volumes are separate; back them up with your volume tooling.
- **Update containers:** edit the version pins in the gateway env file, then `freesra up`. Pins are listed on the System page.
- **Update the appliance OS:** `sudo bootc upgrade` then reboot; `sudo bootc rollback` returns to the previous image.
- **Rotate the first administrator's temporary password:** forced at first login. Rotate `ZITI_ADMIN_PASSWORD`, `KEYCLOAK_ADMIN_PASSWORD` and database passwords from the env file once the system is stable; they are only used by the console and CLI.

Appendix A. Port reference

Port	Direction	Node	Purpose
tcp/443, udp/443	inbound from Internet	gateway	web portal, identity provider login, airlock, WebDAV
tcp/80	inbound from Internet	gateway	certificate issuance, redirect to https
tcp/1280	inbound from Internet	gateway	overlay controller (routers and clients)

Port	Direction	Node	Purpose
tcp/3022	inbound from Internet	gateway	overlay public router
tcp/8443	inbound from admin networks	gateway	FreeSRA Console (direct)
tcp/22	inbound from admin networks	gateway	SSH
tcp/2022	inbound (only if enabled)	gateway	public SFTP
tcp/443, 1280, 3022	outbound to gateway	site connector	policy pull, control channel, data path
udp/53, udp/123	outbound	site connector	DNS, NTP

Appendix B. Files and locations

Item	Container host	Appliance
FreeSRA tree	the git checkout	/usr/lib/freesra
Env file (secrets, pins)	deploy/gateway/.env	/etc/freesra/gateway.env
State (console db, tokens, bundles, backups)	deploy/gateway/state/	/var/lib/freesra/gateway/
Rendered firewall	/etc/freesra/nftables.conf	same
Recovery token	<state>/console/recovery-token	same