SarvDrik

SarvDrik User Guide

Installing the Hub on Windows or Linux, rolling out Operators and Endpoints, controlling who can reach what, working on remote machines, managing patches, software and configuration, and running the fleet day to day.

APPLIES TO

Hub · Operator · Endpoint 2.4.0

PRODUCT

SarvDrik — Remote and endpoint management

UPDATED

October 2026

01

How SarvDrik works

SarvDrik is remote control and fleet management that you install on your own infrastructure. Every session is routed through a server you run.

There are three components.

HUB

The server

Every agent connects to it. It holds user accounts, roles and access grants, routes every session, and serves the admin dashboard.

OPERATOR

The console

An agent installed on the machine a support person works from. They use it through a browser tab on that same machine.

ENDPOINT

A managed machine

An agent installed on every machine you want to reach. It runs as a background service and needs no attention.



The operator's browser only talks to `localhost`. Both agents make outbound connections to the Hub, so no inbound port needs to be opened on any Operator or Endpoint machine.

The Hub decides who can reach what

Access is set centrally, by an administrator, in the Hub. Each user account carries a **role**, which decides what they may do, and **grants**, which decide which machines they may do it on. When an operator opens a session the Hub checks both, once, before the session starts. Nobody at the Endpoint is prompted, and the Endpoint takes no part in the decision. Section 9 covers this in full.

02

Planning your deployment

Three decisions before you install: where the Hub goes, whether an Operator shares its machine, and what the network has to allow.

Where the Hub goes

REQUIREMENT	DETAIL
Always on	Agents reconnect on their own when the Hub comes back, but no session can start while it is down.

REQUIREMENT	DETAIL
Stable address	A fixed IP or DNS name. It is written into every install command and into the Hub's certificate.
Reachable	Every Operator and Endpoint must be able to connect to it on TCP `8484`.
Operating system	64-bit Windows. (Endpoints and Operators run on Windows and Linux.)
Database	PostgreSQL, bundled and configured automatically by the installer.

Hub and Operator on the same server

You can install an Operator on the Hub machine itself, so a single server is both the Hub and the console your support staff work from. **This is the recommended layout for fleets of fewer than 15 Endpoints.**

- One machine to install, patch and back up instead of two.
- Operator-to-Hub traffic stays on the same machine.
- It suits a small fleet, such as a trial or a first rollout.

What to know before choosing it:

- The Operator takes one Endpoint seat, like any other machine; the License page also shows how many of the seats are Operators.
- The console is served on `localhost:8486` of the server. On Windows, people use it from the server's desktop (for example over Remote Desktop). On a headless Linux server, they reach it through an SSH tunnel — see section 8.
- An Endpoint cannot also be installed on that machine. See the next rule.

Beyond 15 Endpoints, keep the Hub on a dedicated machine and install Operators on your support staff's own computers, so relaying many concurrent sessions is not competing with interactive use of the same server.

One agent role per machine

> **A MACHINE IS AN OPERATOR OR AN ENDPOINT — NEVER BOTH**
>
> Machine identity is derived from hardware, so the two agent roles would collide at the Hub. The agent enforces this with a machine-wide lock: if an Endpoint is running, an Operator installed on the same

machine registers its service but exits immediately at startup. To convert a machine, uninstall one role before installing the other. The Hub itself does not count — it can share a machine with either.

Network

PORT	FROM → TO	PURPOSE
8484	Every agent → Hub	Agent connection, TLS-encrypted. The only port agents need.
8485	Admin's browser → Hub	Admin dashboard (HTTPS). Loopback-only until first-run setup is complete.
8486	Browser → Operator machine (same machine by default)	The Operator console, on the Operator machine. Only reachable from that machine unless an administrator opens it to the network, over TLS (section 10). Endpoints serve no page.

03

Your product line: SarvDrik

SarvDrik is both products on the same Hub: everything in Netra (remote management) and everything in Drishti (endpoint management). One Hub installer serves every SarvDrik product line: your licence names the line, and the Hub shows only what that line includes.

What SarvDrik includes

FEATURE
IN EVERY PRODUCT LINE
Hub, admin dashboard and Endpoint agent, on Windows and Linux
Machine inventory — OS, IP, version — and online / offline status
Machine groups, aliases and notes
Kill switch / machine disable
Bulk actions on the Machines page — update, message

FEATURE
Messages to the people at the machines, and the tray on every machine
User accounts and the built-in roles; what each role may do can be changed
Machine policies and connection rules per group
Multi-factor sign-in — authenticator app or email code
Audit log — search, export, webhook and syslog forwarding
Alert channels — browser notification, email, webhook
Jobs page — run an action on a machine or a group, with retry for offline machines [1]
Reports page [2]
TLS encryption on all connections; encrypted local database (AES-256)
REMOTE MANAGEMENT (NETRA)
Operator agent and console; Operator commands on the Deploy page
Screen, keyboard and mouse; shared Screen Share; lock-screen capture (Windows)
File transfer, terminal and clipboard sync
Per-user machine grants and Access policies
Sessions page — active and recent sessions
Metrics and live charts — CPU, RAM, disk, network
Monitoring checks per group, and alert rules on metrics
Process manager, service manager, event log viewer, network insights
Security posture scan
Remote restart and shutdown; diagnostics bundle
Scheduled tasks
Scripts and playbooks
Session recording

FEATURE
ENDPOINT MANAGEMENT (DRISHTI)
Software inventory and change history; hardware inventory
Assets — asset records, Assets page, software licences, outdated versions
OS patch management — Windows Update, apt — and maintenance windows
Software deployment and removal — MSI, EXE, apt (Catalogue)
Configuration baselines
Automation rules and auto-healing
Compliance page — compliance policies assigned to groups and machines; device policy, USB and device inventory and blocking; OS events; sign-in anomalies; file integrity; firewall rules and machine isolation; disk encryption and recovery keys; local administrator passwords; hardening score; unmanaged devices; administrators and certificates; the secret vault; flagged software report and blocking
Regulation packs on the Reports page

1. What a job can run: updates, restarts, shutdowns, diagnostics, scripts, packages, baselines and patch batches.
2. The Reports page lists the reports whose data your licence includes: every report, and the five regulation packs.

What you see in the Hub

The admin menu shows only the pages your licence includes, and the Operator console shows only the tools it includes:

Dashboard, Machines, Groups, **Monitoring**, **Alerts** (the channels, on the Monitoring page), **Assets**, Users, Roles, **Sessions**, **Tasks**, **Automation**, Jobs, Messages, Deploy, **Scripts**, **Catalogue**, **Patches**, **Baselines**, Reports, Audit Log, **Recordings**, **Compliance**, License, Security

The **Alerts** channels sit on the Monitoring page; flagged-software alerts and the licence-ending notices use them.

When something is not there

- A feature that belongs to **another product line** is not shown and does not respond. The Hub answers a request for it as it would for an address or request that does not exist.
- A feature of **your own line** that your licence does not include answers *Not within the current licence*.

Licences issued before product lines

A licence issued before product lines keeps working as issued, including its Operators.

Endpoints and Operators

A licence is for a number of Endpoints. The License page shows how many are in use and how many of them are Operators: an Operator takes an Endpoint seat and has no separate limit. Once the Endpoint limit is reached the Hub refuses further enrolments.

The trial

The SarvDrik trial lasts 30 days: **up to 10 Endpoints and every SarvDrik feature**. It is started with a trial key that arrives with the download link (section 4), one key per email address and product, activated online on the Hub. It is a real deployment — what you set up carries over when you install a licence. When the 30 days end, licensed features stop and new machines cannot enrol until a licence is installed.

A Hub that was already running its earlier built-in 30-day trial keeps running it. A new Hub needs a trial key or a licence to finish first-run setup.

04

Getting SarvDrik

Installers and licences come from the SarvDrik portal at sarvdrik.in.

Download the trial

No account is needed for the trial. Each product line has its own: 30 days, up to 10 Endpoints, every feature of that line (section 3).

1. **Request a link**
   On the *Trial* page (or at the end of a product page), choose SarvDrik and fill in the trial form with your name, organisation and email. There is one trial key per email address and product.

2. **Open the email**
   A download link and your trial key arrive from `no-reply@sarvdrik.in`. The download page shows the key too. The link works **once** and expires after **14 days**. Requesting a new link cancels the previous one.

3 **Download the installer**

The link offers the Hub installer for Windows (`.exe`), saved as `SarvDrik-Hub-<version>-x64-<Line>.exe` , for example `SarvDrik-Hub-2.4.0-x64-SarvDrik.exe` , so trials of two lines can be told apart. The Linux Hub packages (`.deb` , `.rpm`) offered with 1.0.2 are no longer provided.

4 **Activate the key**

Enter the trial key in the Hub's first-run setup, or later on the License page. Trial keys are activated online (section 7).

Create an account

1 **Register**

Go to *Register* and enter your name, email and a password. You are signed in straight away.

2 **Confirm your email**

Click the button in the confirmation email. Your next sign-in is refused until you do. If it does not arrive, use *Resend confirmation email* on the sign-in page.

Forgotten password: use *Forgot password*. Reset links work once.

Get a licence

A licence is for one product line (SarvDrik), a number of Endpoints and a number of years.

1 **Order or contact SarvDrik**

With an account created, open the product page, choose *Buy now*, and pick the number of Endpoints and years. Or open *Contact* on sarvdrik.in and say which product and how many machines the licence should cover.

2 **Collect the licence**

The licence is issued to your account. Open *Your account*, then *Open licenses*. Each licence is a card with its product, its key (with a Copy button), its Endpoints and its expiry date. The Hub installer for that product is on the same card, saved as `SarvDrik-Hub-<version>-x64-<Product>.exe` , next to the activation options. All installers are the same program: the licence decides what the Hub offers.

Keep the licence key — you enter it in the Hub to activate (section 7).

05

WINDOWS Installing the Hub

A single installer sets up everything the Hub needs on a clean 64-bit Windows machine, with no other prerequisites.

Install

1. **Run the installer**
   Run `SarvDrik-Hub-2.4.0-x64.exe` (a trial download carries the line in its name, such as `SarvDrik-Hub-2.4.0-x64-SarvDrik.exe`) and approve the administrator prompt. If Windows shows *Windows protected your PC*, choose *More info → Run anyway* (see the note below).

2. **Choose a folder**
   The default is `C:\Program Files\SarvDrik Hub`.

3. **Finish**
   Leave *Open SarvDrik Hub setup in a browser* ticked. First-run setup opens on this machine (section 6).

What the installer does

- Installs and initialises a **bundled PostgreSQL** database, listening on loopback only on a non-default port, with a password generated at install time.
- Writes `config.yaml` and restricts it to SYSTEM and Administrators, because it contains the database password.
- Registers the `SD-Hub` Windows service, starts it, and sets it to start automatically and restart itself after a crash.
- Adds two inbound firewall rules: *SarvDrik Hub - agent channel* (TCP 8484) and *SarvDrik Hub - admin dashboard* (TCP 8485).
- Locks the `data` folder to SYSTEM and Administrators. The Hub's certificate authority key and signing keys are created there on first start.

Unattended install

From an elevated prompt:

```
Unblock-File .\SarvDrik-Hub-2.4.0-x64.exe
.\SarvDrik-Hub-2.4.0-x64.exe /S
```

The `/S` switch is case-sensitive. Run `Unblock-File` first on a copy downloaded from sarvdrik.in: without it, Windows waits for a SmartScreen confirmation that an unattended install never shows, and the install does not start. First-run setup still has to be completed on the machine afterwards.

WINDOWS SMARTSCREEN

The installer is not code-signed, so Windows SmartScreen shows *Windows protected your PC* when you run a copy downloaded from sarvdrik.in. Check the file first: its SHA-256 must match the one on your account page (`Get-FileHash .\SarvDrik-Hub-2.4.0-x64.exe`). Then choose *More info* → *Run anyway*.

SET THE ADDRESS AGENTS WILL USE — BEFORE SETUP

The generated `config.yaml` does not know your network address. If it is not set, the Hub guesses when it builds install commands, and the guess is `localhost` when the dashboard was opened on the Hub machine itself — which is exactly what happens after install. Add `advertised_host` under `server:` in `C:\Program Files\SarvDrik Hub\config.yaml` (edit it as an administrator), then restart the service:

```
server:
  host: 0.0.0.0
  port: 8484
  advertised_host: 192.168.1.10     # the IP or DNS name agents should use
  tls_enabled: true
```

```
Restart-Service SD-Hub
```

DOWNGRADES ARE BLOCKED

If a newer Hub is already installed, the installer stops with "A newer version of SarvDrik Hub is already installed". Uninstall the newer version first if you really intend to go back.

Uninstall

Use *Settings* → *Apps* → *SarvDrik Hub* → *Uninstall*. The uninstaller asks *Keep my data* (the default) or *Remove everything*; a silent uninstall (`/S`) keeps the data, and `/S /PURGE` removes it. Either way it removes:

- the `SD-Hub` service and both firewall rules
- the Hub program and the bundled PostgreSQL program files

- the agent installers the Hub hands out

When you keep your data, it deliberately **leaves** the following, so that reinstalling brings back the same Hub with all enrolled machines still trusting it. When you run the installer on a machine that still has an earlier Hub's data, it offers *Keep and use it* (the default) or *Install fresh*; *Install fresh* moves the old data to folders named `*.orphaned-<date>`, never deleting it, and a silent install takes `/FRESH` for the same. Over kept data the setup wizard skips the administrator step, and the earlier administrator signs in.

- `data\` — certificate authority, signing keys, the vault key (`vault.key`) and Hub identity
- `pgdata\` — the database: machines, users, grants and audit history
- `config.yaml`

Delete those by hand only if you are permanently decommissioning the Hub.

06

First-run setup

A new Hub has no certificate yet. First-run setup creates one and switches the dashboard over to HTTPS. Until it is done, agents cannot enrol.

Where to open it

Setup is served at `http://localhost:8485/setup` and is bound to loopback only, so nothing typed into it crosses the network. Trying the Hub's network address from another machine before setup is complete gets a message pointing back to that URL. This is intentional.

HUB ON	HOW TO REACH SETUP
WINDOWS	The installer opens it for you. Otherwise, open `http://localhost:8485/setup` on the Hub machine, directly or over Remote Desktop.

The wizard

1 **Create the administrator account**

Choose the username and password for the Hub's first administrator. The Hub ships with no default account, so this is the only way in once setup finishes.

2 **How will machines reach this Hub?**

Enter the address or addresses agents will use — the same value as `advertised_host`. These go into the certificate, so an agent connecting by any other name will not trust the Hub.

3 **Where does the certificate come from?**

Generate one for me

Enter your organisation name. The Hub creates its own certificate authority and issues itself a certificate. The install commands in Deploy add that authority to each machine's trust store automatically. This suits most deployments, including networks with no internet access.

I have my own CA

The Hub produces a certificate signing request. Have your CA sign it, then paste back the signed certificate and your CA's certificate (both PEM). Use this when policy requires every internal certificate to chain to your own root.

4 **Outgoing email (optional)**

The mail server the Hub uses for login codes and MFA notices. *Test connection* checks the saved settings. Skip it if you don't have the details to hand; it is also under Settings later.

5 **License**

A Hub needs a licence or a trial key to take machines. Enter the key from your trial or order email, or install a licence file (section 7 explains both ways). The step shows the limits of what is installed and the days left, and *Continue* stays off until a licence is active.

I have a license key

Enter the key (a trial key or a licence key) and select *Activate*. The Hub fetches its licence and binds it to this machine. Needs internet access. Not offered on a Hub built without online licensing.

Install a license file

Download this Hub's activation request, upload it in your SarvDrik account under the licence's *Activate*, then choose the licence file you get back and select *Install*.

6 **Finish**

The Hub switches to HTTPS on its network address. From now on the dashboard is at `https://<hub-address>:8485`.

CHOOSE THE CERTIFICATE ONCE

Every agent that enrols trusts this certificate authority. Replacing it later means re-establishing trust on every enrolled machine. If you want a different, publicly trusted certificate for the browser dashboard

only, set `web_tls_cert_file` and `web_tls_key_file` in `config.yaml` — that changes the dashboard without affecting agents.

First sign-in

Sign in with the administrator account you created in the wizard's first step. There is no default account on any installation.

> ONE ACCOUNT PER PERSON
>
> Create a named account for each administrator under **Users**. The audit log records who did what, which is only useful if people are not sharing one account.

07

Activating your licence

Activation is done on the **License** page of the Hub dashboard, or during first-run setup (the same two ways). A trial key is activated the same way as a licence key.

The page shows the current licence status (on a trial, how many days are left), who it is issued to, the product line, the key, *Endpoint* seats in use against the limit (and *Operators*), when it ends, and what it is bound to. If a licence can't be used, the status says why. The licence decides the product line, and with it the pages the Hub shows (section 3).

Online activation

Enter your licence key under *Update online* and select *Update license*. The Hub fetches a signed licence and binds it to this machine.

If the page has no *Update online* section, this Hub can't activate online; use offline activation.

Offline activation

For Hubs without internet access, or without online activation:

1. **Download the activation request**

Under *Install a license* (or *Update offline* when online activation is available), select *Download activation request*. It identifies this Hub machine.

2. **Send it to SarvDrik**

   You receive a signed `license.lic` bound to this machine.

3. **Upload it**

   Choose the file under *Signed license file* and select *Install*.

> LICENCES ARE BOUND TO THE HUB MACHINE
>
> A licence activated on one Hub machine is not valid on another. If you move the Hub to new hardware, the licence has to be activated again for the new machine.

When seats run out

Once the Endpoint limit is reached, the Hub refuses further enrolments of any kind, Operators included, and the Deploy page stops offering new tokens until a seat is free. Check the License page before a large rollout, and see *Adding Endpoints or extending a licence* below.

When a licence nears its end

- A banner on every page of the Hub dashboard, and in each Operator console, shows when the licence ends and how many days are left.
- Notices go to the alert channels you pick on the License page 30, 7 and 1 days before the end.
- A paid licence has a 14-day grace period after its end date, so work carries on while a renewal is installed. A trial stops on its last day.
- A new licence takes effect as soon as it is installed: the banner and the features in every console follow within seconds.

Adding Endpoints or extending a licence

A running product-line licence can be changed without waiting for its end date. On the licence's card under *Your licenses* on sarvdrik.in, choose:

- **Add Endpoints**: enter how many to add. The new total applies for the rest of the current term and the end date does not move.
- **Extend**: enter 1 to 60 months to add. The Endpoints stay the same and the end date moves out.

The page shows the new total and the amount before you place the order. When the order is paid, the licence is replaced by a new one for the same holder, product line and Hub, and the card shows the earlier version under it. Activate the new key on the Hub's License page (or let the Hub take it over online); the earlier key stops being accepted. The buttons are not offered on a trial or on a licence issued before product lines.

08

Rolling out agents

Endpoints and Operators install the same way: create a deployment token, then run one command on each machine. The machine enrols itself.

Create a deployment token

1 **Open Deploy**

In the Hub dashboard, open **Deploy** and create a token with a descriptive name. Choose what it installs (Endpoints, Operators, or either) and how long it stays valid (7 days unless you choose otherwise).

2 **Copy the commands straight away**

The install commands for what the token allows appear, for Windows and Linux.

> A TOKEN IS SHOWN EXACTLY ONCE
>
> The Hub does not store the token in a form it can show again. Picking an existing token from the list later cannot produce a working command. If you lose it, create a new token.

Install an Endpoint

WINDOWS **elevated PowerShell**

```
irm "https://<hub-address>:8485/install/windows" -Headers @{Authorization="Bearer <token>"} | iex
```

- Installs to `C:\Program Files\SarvDrik RMM` and registers the `SD-Endpoint` service, running as LocalSystem.

- Adds the Hub's certificate authority to the machine's trusted root store.

LINUX **bash, with sudo**

```
curl -H "Authorization: Bearer <token>" "https://<hub-address>:8485/install/linux" | sudo bash
```

- Installs to `/opt/sarvdrik-rmm` and registers a systemd service, `SD-Endpoint.service`, running as root and restarting automatically.
- Adds the Hub's certificate authority to the system trust store.
- Loads the `uinput` kernel module, and configures it to load at boot, for keyboard and mouse control.

Always paste the commands exactly as the Deploy page shows them — it adds whatever connection options your Hub's certificate needs on first contact.

Install an Operator

Use the Operator commands from the same page. They differ only by `?component=operator` at the end of the URL.

	WINDOWS	LINUX
Install location	`C:\Program Files\SarvDrik RMM Operator`	`/opt/sarvdrik-rmm-operator`
Service	`SD-Operator`	`SD-Operator.service`
Counted as	One Endpoint seat (the License page also lists it under Operators, which have no separate limit)	

Installing the Operator on the Hub machine

For the single-server layout from section 2, run the Operator command on the Hub machine itself. Nothing else changes.

- WINDOWS People sign in to the server's desktop and open `http://localhost:8486`.
- LINUX From a workstation, forward both the console and the dashboard in one connection:

```
ssh -L 8486:localhost:8486 -L 8485:localhost:8485 you@hub-address
# console:   http://localhost:8486
# dashboard: https://localhost:8485
```

If port 8486 is already in use on the workstation, pick another local port, for example `-L 18486:localhost:8486`, and browse to `http://localhost:18486`.

Before rolling out widely

WINDOWS CTRL+ALT+DEL NEEDS A POLICY VALUE

Windows blocks services from sending Ctrl+Alt+Del unless this policy is set. Without it the viewer's Ctrl+Alt+Del button silently does nothing — and that button is how an operator gets past a lock or login screen. The installer does not set it. Apply it across the fleet with Group Policy, or per machine:

```
Set-ItemProperty `
  -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" `
  -Name "SoftwareSASGeneration" -Value 1 -Type DWord
```

LINUX DESKTOP SESSION AND CLIPBOARD TOOL

- Screen capture and input need a graphical desktop session on the machine.
- Clipboard sync needs `xclip` on X11 or `wl-clipboard` on Wayland. The installer warns if neither is present; install the one matching the desktop.
- The installer needs `bash`, `curl` and `systemd`.

Confirm the rollout

Open **Machines** in the Hub. Newly enrolled machines show the *Unmanaged* badge. Review each one and select *Acknowledge* to move it into the active fleet. Then give people access to it (section 9) — until then, no operator can reach it.

Removing an agent

From the Hub: **Machines** → the machine's row → *Actions*. Removing the software cannot be undone; the machine then moves to the *Removed* view and its licence seat is freed.

THE MACHINE IS	USE	WHAT HAPPENS
Online	*Uninstall…*	The agent removes itself at once and goes offline for good.
Offline	*Uninstall when it connects…*	The uninstall is queued and the row shows *Uninstall pending*. It runs the next time the machine connects, even if the

THE MACHINE IS	USE	WHAT HAPPENS
		licence is full. Until then the machine keeps its seat. *Cancel pending uninstall* withdraws it.
Gone for good (decommissioned, failed, stolen)	*Retire…*	Frees the seat without the machine's help. Offered only while it is offline. If it ever comes back it takes a seat again, unless an uninstall is pending, in which case it is removed on arrival.

On the machine itself, with a current deployment token:

```
# Windows, elevated PowerShell (add ?component=operator for an Operator)
$Uninstall = $true; irm "https://<hub-address>:8485/install/windows" -Headers @{Authorization="Bearer <to

# Linux (add ?component=operator for an Operator)
curl -H "Authorization: Bearer <token>" "https://<hub-address>:8485/install/linux" | sudo bash -s -- --un
```

Before removing anything, the script tells the Hub the machine is being uninstalled (it prints *Hub notified*), so the Hub moves it to *Removed* and frees its seat. If the Hub can't be reached the uninstall still completes; retire the machine from the Hub afterwards to free the seat. Uninstalling also removes the Hub's certificate authority from the machine's trust store.

09

Who can reach what

Everything about access is set in the Hub. An operator can open a session on a machine only when their account has been granted that machine, and they can only use the tools their role allows.

For any operator to work on any machine, three things must be in place:

1 · CONSOLE

Operator Login Access

Which Operator machines this person may sign in on.

2 · MACHINES

Endpoint Connection Access

Which Endpoints this person may reach — granted per machine, or through a group.

3 · TOOLS

Role

Which features they may use on those machines: screen, control, files, terminal, and so on.

Create a user and grant access

1. **Create the account**
   In **Users**, select *Create User* and enter a username, password and role.

2. **Grant a console**
   Select *Manage Access* on the user. Under *Operator Login Access*, choose an Operator machine and select *Grant Login*.

3. **Grant machines**
   Under *Endpoint Connection Access*, choose an Endpoint and select *Grant Access*. Repeat for each machine, or use a group instead (below).

Both grants are needed. With machine grants but no console grant, the person cannot sign in anywhere. With a console grant but no machine grants, they sign in to an empty list.

Also on the user row: *Change Role*, *Change Password*, and *Deactivate / Reactivate*. Deactivating an account is the fastest way to remove all of someone's access at once. Any grant can be removed with *Revoke*.

Removing someone's access to a machine ends only that session: their console shows a *Not allowed* notice, closes the machine's page and keeps everything else open. Nobody else is disconnected. A role change reaches the person's console within seconds.

Groups

In **Groups**, create a group — "Warehouse", "Finance" — add machines to it, and assign users. This is easier to keep correct than granting machines one by one, especially as the fleet grows.

Roles

A role decides exactly which features its users can use. There are seven fixed roles; you can change what each of them may do, on every line. Changes are pushed immediately to every connected Operator console whose signed-in user holds that role. The `admin` role is locked and cannot be edited.

Built-in roles

PERMISSION	ADMIN	OPERATOR	POWER USER	USER	SUPPORT	VIEWER	AUDITOR
ENDPOINT ACCESS							
View Screen	✓	✓	✓	✓	✓	✓	—
Control Screen (keyboard, mouse)	✓	✓	✓	✓	—	—	—
File Manager	✓	✓	✓	✓	—	—	—
Terminal / Commands	✓	✓	—	—	—	—	—
Clipboard Sync	✓	✓	✓	✓	—	—	—
MONITORING AND DIAGNOSTICS							
System Monitor	✓	✓	✓	—	✓	✓	✓
Alert Rules	✓	✓	✓	—	—	—	✓
Event Log Viewer	✓	✓	✓	—	✓	✓	✓
Network Insights	✓	✓	✓	—	—	—	—
Security Posture	✓	✓	—	—	—	—	—
ADMINISTRATION							
Manage Users (needed to sign in to the Hub dashboard)	✓	—	—	—	—	—	—

Process Manager and Service Manager are allowed by the *Terminal / Commands* permission, since they can stop programs and services.

> WHO CAN SIGN IN TO THE HUB DASHBOARD

> The dashboard only accepts roles that have the **Manage Users** permission. Out of the box that is only **Admin** — every other built-in role is for Operator console use. To give someone else dashboard access, assign them Admin, or a custom role that includes Manage Users.

Policies

For finer control, two kinds of policy can be attached: a Machine Policy and an Access Policy. Both are plain forms; every setting is checked when you save, and a setting the Hub cannot read refuses rather than allows.

Machine Policy and connection rules

Decide whether a machine may connect to the Hub at all. Set them for one machine under **Machines** → *Details* → *Policy*, or for every member of a group under **Groups** → *Manage Group* → *Connection rules*.

SETTING	EFFECT
Minimum agent version	Machines with an older agent are refused until they update. Picked from the versions your fleet reports.
Allowed networks	Machines connecting from outside these address ranges are refused. *This machine's network* fills in the current one.
Connect hours	Days and times, in a time zone you choose, when the machine may be connected. Outside them it is disconnected from the Hub: no sessions, patching, inventory or alerts. To limit only when people may open sessions, use the access window below instead.

A machine must meet its own policy and the rules of every group it is in; the strictest setting wins. When a machine is refused, the reason names the rule, for example *(rule of group Lab)*. The *Policy* tab lists the group rules that also apply. Changes take effect at once.

Device policy for one machine

Machines → *Details* → *Policy* also holds *Device policy for this machine*: the same editor as the group's, overriding the groups the machine is in for the classes and devices it names, allowing or denying them. Everything it does not name stays as the groups say. A Deny on a vendor and product blocks that one model on that machine. Each rule can *Deny: block*, *Deny: report only* or *Allow*; the group's *Enforce* switch is the master, and with it off nothing is disabled. A USB device with a video interface counts as *Camera* on Linux as on Windows.

Access Policy

Applies to one user's grant on one machine. Open it from **Users** → *Manage Access* → the machine's *Policy* button.

- **Access window**: days and times, in a time zone you choose (or the Hub's), when that person may open sessions on that machine.
- **Recent sign-in**: the person must have signed in within the last 15 minutes.

Multi-factor sign-in

A second step at sign-in, on the Hub dashboard and on the Operator console: a 6-digit code from an authenticator app (Google Authenticator, Authy, 1Password and similar), or a code sent by email. Email codes need the Hub's mail server (section 6, or **Security** in the dashboard).

A code is asked for only where a policy requires it:

- **Administrators**: *Admins must use MFA* on the **Security** page, on by default.
- **Everyone else**: *Require MFA* on a group (**Groups** → *Manage Group*) covers the people who reach that group's machines. The group shows an *MFA required* badge.
- **Setting it up.** Someone who must use MFA and has not set it up is shown the QR code (or offered an email code) at their next sign-in, on the Hub dashboard and on the Operator console. On the dashboard they can choose *Later* and are asked again at their next sign-in. Setting up an authenticator shows a set of one-time recovery codes: keep them somewhere safe. **My Account** shows each method's state.
- **Not required**: no code is asked, and a method set up earlier is kept for when a policy needs it again.
- **Lost device.** Users cannot switch MFA off themselves. An administrator resets it from **Users**, and the user sets it up again at their next sign-in. An administrator with no other administrator to help uses the Hub's `recover` command on the Hub machine (section 14).

10

The Operator console

What a support person does day to day. Everything happens in a browser tab on the Operator machine.

Sign in

On the Operator machine, open `http://localhost:8486` and sign in with your Hub account. Accounts are created by an administrator — the *Create account* link only tells you to contact them.

If sign-in is refused, your account probably lacks *Operator Login Access* for this particular machine, or has been deactivated.

- **One person at a time.** While someone is signed in to a console, a sign-in from another browser is refused with their name and since when. It frees up when they sign out, or after 30 minutes with no console page open.
- **One tab at a time.** Opening the console in a second tab moves your work there; the first tab pauses with *Use this tab instead* to take it back.
- **Reloading** the page keeps your session. Closing the console ends your sessions after a minute.
- **Dark mode**: the switch in the header.

Using the console from another computer

By default the console answers only on the Operator machine itself. An administrator can open it to the local network on the Hub: **Machines** → the Operator's *Details* → *Settings* → *Console access*: *Local network* (or for every Operator, with *Operator console* at the top of Machines). People then open `https://<operator-address>:8486` and sign in as usual.

- It only ever opens over TLS, with a certificate the Hub issues. Without one, or when the Hub uses your own certificate authority (which it can't issue from), the console stays on the Operator machine, and *Settings* says so.
- The Hub is the only place this is set; there is no override on the Operator machine.
- *Settings* shows what the Operator actually reported: this machine only, or open to the network. A change reaches a connected Operator within seconds.
- The Operator installer already allows TCP 8486 through the machine's firewall. If it reported it couldn't, open that port by hand.

Finding your machines

Overview

Your machines at a glance.

Agent Info

This console's own details: its ID, hostname, agent version, Hub address and connection status. The first place to look if nothing is connecting.

Connections

Every machine the Hub has granted you, with a green dot when online. Select a machine to open its dashboard, or expand it for shortcuts to Screen Share, File Manager and Terminal.

There is no way to add a machine from the console. If a machine you need is missing, ask an administrator to grant it.

A machine's dashboard

The header shows the machine's details and these actions:

- **When online:** *Refresh Info*, *Permissions* (a read-only view of what your role allows), *Activity*, and *Leave Session*.
- **When offline:** *Reconnect*, and *Wake Machine* — sends a Wake-on-LAN packet, shown when the machine's network card address is known.

Below the header, each tool is a tile:

TILE	WHAT IT DOES	ROLE PERMISSION
Screen Share	Live view and control of the remote desktop	View Screen
Screenshot	Captures the remote screen	View Screen
File Manager	Browse, upload and download files	File Manager
Terminal	Interactive shell on the remote machine	Terminal / Commands
System Monitor	Live CPU, RAM, disk and network	System Monitor
Process Manager	View and end running processes	Terminal / Commands
Service Manager	Start, stop and restart services	Terminal / Commands
Alert Rules	Threshold alerts on this machine's metrics	Alert Rules
Event Log Viewer	Read system logs live	Event Log Viewer
Network Insights	Connections, open ports, ping, traceroute	Network Insights
Security Posture	Firewall, SSH keys, updates and antivirus status	Security Posture

Only the tools your licence includes are shown.

When a tile is greyed out

Hover over it. The reason is one of:

- **Access revoked by administrator** — your grant to this machine was removed.
- **Machine is offline** — the Endpoint is not connected to the Hub.
- **Not available on this machine** (or a more specific message) — the Endpoint's own health check reported that capability as broken.
- **Your role does not permit this feature** — ask an administrator to change your role.

Screen Share

Select *Start Screen Share*. Your mouse and keyboard act on the remote machine. The bar above the picture:

CONTROL	PURPOSE
Start / Stop	Start or stop the picture.
Fit / 1:1	Fit the remote screen to the window, or show it at its real size.
Full screen	Fill your display with the remote screen.
Control	Switch keyboard and mouse control on or off; off watches only.
Keyboard lock	Send shortcuts like Alt+Tab to the remote machine instead of your own browser.
Ctrl+Alt+Del	Reach the lock or login screen. On Windows, needs the policy value from section 8.
Clipboard	Send your clipboard to the remote machine, or fetch the remote one.
Screenshot	Save the current frame to your machine.

On a machine with more than one monitor, choose the display from the bar.

If the stream reports the machine is **busy**, another operator is connected and that machine allows one operator at a time (section 11).

File Manager

Laid out like Windows File Explorer: a navigation pane with the machine's drives and folders, the current folder beside it, an address bar, and Back, Forward, Up one level and Refresh. Show the folder as *Details* or *Large icons*. Create folders, rename, delete, upload from your machine and download to it. Large transfers

are sent in chunks with progress shown, and can be cancelled while they run. Sizes are shown in KB, as Explorer does.

To keep system files safe, the File Manager does not list or change system areas. On Linux those are the system folders (`/etc` , `/usr` , `/var` and the rest) and anything directly under `/` ; the drive list shows each home folder and the real partitions. On Windows they are the Windows folder and any hidden folder. A change in one of them is refused, and the notice says why.

Terminal

A full interactive shell — PowerShell on Windows, bash on Linux — with real terminal emulation, so editors and other interactive programs work normally. No SSH client is needed. On both systems you sign in with an account on the machine and its password, and the shell opens as that account (on Linux the password is checked by the system itself and the shell is a login shell, not root). Five wrong passwords lock the sign-in for that account for five minutes. Accounts that come from a directory service and second-factor sign-ins are not covered on Linux.

Monitoring and diagnostics tools

System Monitor

Live charts of CPU, memory, disks and network.

Process Manager

Running processes, filterable by name, user or PID, with the option to end one.

Service Manager

Services, filterable by name, with start, stop and restart.

Event Log Viewer

On Windows: Application, Security and System logs. On Linux: journald, syslog, auth.log and kern.log. Choose how many lines to fetch and whether to follow new entries.

Network Insights

Active connections and listening ports, plus ping and traceroute from the remote machine.

Security Posture

Firewall state, SSH keys, pending updates and antivirus status.

Alert Rules

Raise an alert when CPU %, RAM %, disk % (fullest volume), or network receive/send rate crosses a threshold. Deliver it as a browser notification, by email (SMTP) or to a webhook (HTTP POST).

Which of these you see depends on your licence (section 3) and your role.

11

On an Endpoint

The Endpoint agent runs in the background. The person using that machine does not need to do anything, and is not asked to approve connections.

Whether an operator can connect is decided entirely by the Hub (section 9). Someone who wants to know who can reach their machine should ask the administrator — it is not controlled from the machine.

The Endpoint has no local web page, and apart from its tray icon (below) no window of its own; it is managed entirely from the Hub and reached through the Operator console. To see a machine's state, use its row in the Hub's **Machines** page (section 12): status, agent version, last seen, and *Details* for its software, devices, hardware and health.

More than one operator at a time

What happens when a second operator opens a session on an Endpoint that already has one:

SETTING	SECOND OPERATOR
Exclusive (default)	Is told the machine is busy.
View-only	Watches the same screen; only the first operator controls it.
Multi	Shares the same screen, and both can work on it.

The setting is on the Hub: at the top of **Machines** (*Second operator on an Endpoint*), and for one machine under *Details* → *Settings*. A change reaches a connected machine within seconds.

The tray

Each Endpoint shows a SarvDrik icon in the system tray of the signed-in user: whether it is connected to the Hub, who is connected to the machine and since when, whether the session is recorded, and the last few actions. Messages from your administrators appear through it and stay listed in its menu (Messages, section 12). On Linux the tray needs the GNOME AppIndicator extension, installed and enabled.

12

Running the fleet

The rest of the Hub dashboard, at `https://<hub-address>:8485`. The menu lists only the pages your licence includes (section 3).

Dashboard

Summary statistics for the fleet, refreshed each time you open the page.

Machines

Every machine the Hub knows, in **Operators** and **Endpoints** sections, sorted by name so the list stays put between refreshes. Columns: status, name or alias, enrolment, hostname, OS, client version (the agent's version, as last reported), IP address, last seen, *Enabled* and actions.

VIEW	SHOWS
Fleet	Every machine still managed. The default.
Unmanaged	Machines waiting for *Acknowledge*.
Not seen	Machines offline for at least the number of days set in *Flag machines not seen for* (3 to 90, default 7). A flag only: they stay managed and keep their seats.
Removed	Uninstalled, retired and replaced (re-imaged) machines, kept for history. They are left out of every other list and count in the console.

The status dot is green when the machine is connected, grey when it is not, and black once it is removed. Hover over it for the words. For an offline machine the tooltip also says why, when the machine reported it as it stopped (*Stopped on the machine*, *Machine shut down*, *Restarting after an update*), and when it was last seen. Plain *Offline* means it simply dropped off: network, power or a crash.

Above the list, *Defaults for every machine* sets what an Endpoint does when a second operator connects (Exclusive, View-only or Multi, section 11) and whether Operator consoles are open to the network (this machine only unless changed). A machine's own *Settings* tab overrides either. Changes reach connected machines within seconds.

The same row has *Agents look for a new version*: *Only at start or on Push update* (the default), or every 6, 12 or 24 hours. With an interval set, each agent checks on its own and installs a newer release the way it does

at start-up; the checks are spread a little, so a fleet does not call the Hub at the same moment. It applies to every machine, with no setting per machine, and the Audit Log records the change.

Bulk actions: tick machines (or every one shown), then *Push update*, *Send message* or *Restart* them together. The bar says how many are ticked and how many of those are offline; offline machines are skipped for updates and restarts, and a message waits for them.

The **Enabled** switch is the kill switch. A disabled machine is refused by the Hub whatever credentials it presents — for a lost laptop, a suspected compromise, or a departure. Switch it back on at any time.

ROW ACTION	WHAT IT DOES
Acknowledge	Moves an unmanaged machine into the active fleet.
Details	Opens the machine's panel: *Notes* (a recognisable alias and notes other administrators see), *Software*, *Devices*, *Hardware*, *Asset* (the machine's asset record), *Health* (which capabilities work: screen capture, input, clipboard, terminal, file management), *Settings* (for an Endpoint, what happens when a second operator connects, section 11; for an Operator, whether its console is open to the network, section 10), *Policy* (Machine Policy, section 9) and *Checks* (the monitoring checks that apply to the machine).
Push update [1]	Tells the agent to check for a newer version now; the row then shows how it ended.
Restart / Shut down [1]	Restarts or powers off the machine's operating system immediately.
Diagnostics bundle [1]	Downloads a support bundle: system information, recent logs and running processes.
Uninstall…	Removes SarvDrik from the machine. On an offline machine it is queued until the machine next connects, and can be cancelled until then. See Removing an agent.
Retire…	For an offline machine that is gone for good: frees its seat and moves it to *Removed*.

[1] Offered only while the machine is online.

Sessions

Every session in progress and recently ended, with the operator, the machine, the start time, the traffic per session and what was done in it, from the audit trail. A session ends when the operator leaves it or closes the console, or when you remove their access (section 9).

Monitoring

Checks that run on the machines of a group and report to the Hub: a service running, a process running, free disk space, CPU use, memory use, a port listening, or a library script (exit 0, 1 or 2 for OK, warning or critical). Add them under **Groups** → *Manage Group* → *Checks*; each has warning and critical levels and how often it runs. The **Monitoring** page shows every check's state across the fleet, and a machine's *Checks* tab its own. A machine that stops reporting shows *unknown*. A check can alert by email or webhook on critical, warning, unknown and back to OK, and an automation rule can act when a check keeps failing.

Assets

Every machine with its hardware and asset record: asset tag, owner, location, purchase, warranty and replace-by dates, and status (in use, in stock, in repair, retired). Edit a record from the machine's *Details*. Filter by search, location, status, OS, owner, warranty, age and replace-by, save views, and export CSV. The page also lists software changes across the fleet for the last 7, 30 or 90 days, software installed on a past date, and **software licences**: seats bought against seats in use, with over-use and expiry highlighted. A flagged-software rule can cover only versions below a minimum, to find outdated installs. A note under each machine's operating system says whether it is still supported (support ended, extended updates only, ending soon), and an *OS support* filter and the CSV carry the same; a system the Hub has no dates for reads *Unknown*, never *Supported*.

Messages

One-way messages to the people at the machines: to one machine, a group or the whole fleet. They pop up through the tray (section 11) and stay listed in its menu. A message for a machine that is offline waits for it, for 1 to 30 days. The page shows, per machine, whether each message was delivered and read.

Reports

The reports on offer follow the licence (section 3).

Nine reports, as PDF or CSV, for the whole fleet, a group or one machine, over the dates you choose: compliance summary, patch compliance, user access review, endpoint security posture, device control, configuration baselines, asset inventory, remote session activity and the activity log. Five **regulation packs** map each requirement of CERT-In directions (2022), the RBI cyber security framework, SEBI CSCRF, the DPDP Act and Rules, and ISO/IEC 27001:2022 Annex A to the evidence SarvDrik holds. Status words are *Good*, *Review* and *Priority* (packs: *Evidence available*, *Partly supported*, *Review suggested*, *Outside scope*), and recommendations are suggestions. A report is evidence for your own review, not a certification. Reports can also be scheduled by email.

Groups

Machines are grouped automatically by operating system (Windows, Linux — Debian/Ubuntu, Linux — RPM, macOS, Other), and you can add your own with + *New Group*. Groups are what you grant users access to (section 9) and what jobs, patch batches and policies target. *Manage Group* holds the group's members and users, its device policy, monitoring checks, *Connection rules* (section 9), *Record Sessions* and *Require MFA*.

Jobs

The actions on offer follow the line (section 3).

Run an action now against one machine, or fan it out to every member of a group: self-update, restart, shut down, a diagnostics bundle, a registered package, script, playbook or baseline. A machine that is offline is retried automatically with backoff instead of skipped; after five tries it shows *Not delivered: the machine did not connect before the retries ran out*. Click a job to see each machine's result and, for a failed one, why (for example a script's exit code and error). *Retry* runs it again for just the ones that failed. Batches from Patches, Catalogue and Baselines appear here as well, rolled up per batch.

Catalogue

The software you have approved for deployment. + *Register Package* adds an apt package on Linux (leave the version blank for the latest in the machine's repositories), or an MSI or EXE on Windows (upload the file, or paste the vendor's download link). A registered package becomes a job action: deploy it to one machine from **Jobs**, or to a whole group with *Deploy to group*, which creates one job per package. Removal works the same way. Each result is confirmed against the machine's actual installed state.

Patches

Pending operating-system updates found on each machine: Windows Update on Windows, apt on Linux. *By machine* lists each machine's pending patches; *By group (batch)* merges a group's patches into one checklist showing how many members need each one, and the batch targets only those. Nothing installs unless you pick it here.

- **Maintenance windows** per group set when patch and deployment jobs may run; a reboot a patch needs is deferred into the window.
- **Exceptions** keep a patch you have rolled back from being offered again, until you remove the exception.

Baselines

Named sets of operating-system settings: Windows registry values, or Linux systemd units that must be enabled, disabled, running or stopped. Registering a baseline changes nothing; apply it to a machine from **Jobs**, or to a group with *Deploy to group*. Each machine then checks itself for drift and reports it in the *Compliance* list on this page. Drift is reported, never reverted automatically: re-apply the baseline when you want the setting back.

Scripts

PowerShell scripts for Windows and bash scripts for Linux, written by an administrator and registered here. + *Create Playbook* chains scripts into ordered steps that stop at the first failure. Registering one never runs it: run it from **Jobs**. *Recent Runs* keeps the output, result and exit code of every run, with secrets redacted.

Compliance

The fleet's compliance in one place, in six tabs. Everything here is for administrators, and each setting reaches the machines within a few minutes.

TAB	WHAT IT IS FOR
Overview	How many machines are compliant, how many machines each kind of policy reaches, and the device policy table with each violation.
Policies	Make and edit compliance policies.
Assignments	Choose a machine to see which policies reach it and which one applies; see the machines no policy reaches.
Findings	What the machines have reported, one table per kind, with a filter to show one kind.
Actions	Things that act on a named machine now: isolate and release, start encrypting, and the secret vault.
Settings	The OS event policy, where notices go, and the unexpected-restart notice.

Compliance policies

A compliance policy is a named set of controls: file integrity, firewall, local administrator password, disk encryption, hardening score and unmanaged devices. Make it once on the *Policies* tab, choose which controls it holds, and tick the groups and machines it applies to. A group or a machine can have several policies. When more than one reaches a machine, the Hub combines them: lists (watched files, firewall rules, baselines, network ranges) are joined; for a setting that can have only one value (the local

administrator account, disk encryption) the policy assigned to the machine itself wins, then the one with the lower order number beside it, then the group, then the older policy.

Pick *Windows only* or *Linux only* to keep a policy from reaching machines of the other system; the default, *Any*, applies to both. A policy is checked when you save it, with the same rules the old per-group forms used. A policy that is still assigned cannot be deleted by accident: the Hub lists where it is assigned and asks you to remove it first. Policies that groups or machines had before this version appear automatically, named for the control and the group or machine, and keep working.

On the *Assignments* tab, choose a machine to see, for each control, the policies that reach it, which one applies where only one can, and the result the machine receives. Below it, *Not covered* lists the machines no policy reaches for each control.

What a policy can hold

- **File integrity**: watch folders and files you name, or the named sets of system sign-in files and of places programs start from. The first pass records each file's name, size, time and SHA-256; later passes list files added, changed or removed in *Findings*, with the machine. Tick *Tell me when many user files change at once* (50 files by default) to be told of a mass change, which names the most common file types. *Accept as normal* on a machine records a new baseline. Scans run on a schedule, so a file changed and put back between two scans is missed; a watch holds up to 20,000 files, and files over 256 MB are not hashed.
- **Firewall**: rules for Windows Defender Firewall and Linux nftables, edited as a table (name, direction, action, protocol, ports, addresses, on or off), with presets: block inbound except management, web server, block outbound mail. The rules that keep a machine connected to the Hub are always written first, a rule that would cut the Hub off is refused, and an agent that cannot reach the Hub after applying takes the rules back by itself. Only rules made here are ever changed. *Findings* shows each machine's state: in line, drifted, rolled back or failed.
- **Local administrator password**: each machine sets its own random password for one local administrator account and hands it to the Hub, which keeps it sealed in the vault. Choose the account (blank means *Administrator* on Windows and *sdbreak* on Linux), its length, how often it changes, and whether it changes after it has been read. On Windows the account must already exist. Machines under Windows LAPS and domain controllers are left alone. A machine that cannot reach the Hub changes nothing, so it cannot be locked out by a password the Hub never received.
- **Disk encryption**: whether each machine's system disk is encrypted (BitLocker on Windows; the root device on Linux), and BitLocker recovery keys kept in the vault. Encryption can be started from *Actions* on Windows machines you name; the machine stores a key with the Hub first and encrypts only afterwards. A machine without a TPM says why it cannot. On Linux the state is read only.
- **Hardening score**: choose the configuration baselines (from the Baselines page) a machine is measured by. Each machine reads its own settings, changing nothing, and the page shows a percentage with the

settings that differ. A baseline for the other operating system is skipped. A fall of 10 points is announced.

- **Unmanaged devices**: machines you choose look at the network ranges you approve and list devices that have no agent (printers, cameras, phones, unenrolled laptops). Each machine scans only the subnets it is directly attached to, by address resolution, at a limited rate and without credentials. A range the machine is not on is refused with the reason. Each new device is announced once; mark it *Known* with a label, or *Ignored*, to stop that.

Findings

- **Device policy status**: which machines have a device policy (set per group, in *Manage Group → Device Policy*, or for one machine under its *Policy* tab), and which are compliant, with each violation. A policy can block a device class (for example USB storage, or on Windows cameras and webcams) when it is attached. With *Enforce* off for the group, a violation is only reported here and nothing is disabled; hubs, keyboards, mice and network adapters are never disabled.
- **Sign-in anomalies**: machines report sign-ins (failed, at the keyboard, remote, privileged) and the Hub looks across all of them every minute for what one machine cannot see: a burst of failures (10 in 5 minutes); one address trying 5 accounts in 10 minutes; one account failing on 3 machines in 15 minutes; a successful sign-in right after 5 failures for the same account; one account on 3 machines at once; and a new source address for an account after the first weeks of learning. Each finding is announced once; *Seen* and *Not a problem* close one. Needs the Authentication events switched on in the OS event policy (see Settings). Accounts and addresses are kept for 35 days, never passwords.
- **File integrity**: the changes the watches found, and the machines being watched.
- **Firewall**: each machine's state, and what is applied.
- **Unmanaged devices**: the devices found, with first and last seen, the machine that saw them, and their status (new, known, ignored, or has an agent).
- **Hardening score**: a percentage per machine and the settings that differ.
- **Disk encryption**: each machine's state and whether the Hub holds its key. *Unknown* means the agent has not reported it.
- **Administrators**: who holds administrator rights on each machine (the local Administrators group on Windows; uid 0, the sudo, wheel and admin groups and sudoers rules on Linux), with a note where something is worth a look, such as a password that never expires or sudo without a password. Agents report every few hours, and a notice goes out when someone is added or removed or gains passwordless sudo.
- **Certificates**: certificates that serve or authenticate something (the Windows machine's personal store; certificate files of web, mail and proxy servers on Linux; private keys are never read), soonest end first, with an *Ending within* filter. Notices go out 30, 14, 7 and 1 days before the end and when it ends; *Ignore* a certificate, with a note, to stop its notices.

- **Flagged software**: name patterns you flag (every change is audited), and the machines that have matching software installed. A flag marked *Block* also ends the program on machines in groups that switch blocking on, with an alert; blocked programs are listed here and in the machine's *Software* tab. Flagged software can be removed from ticked machines as a job batch.

Actions

- **Isolate a machine**: cuts a machine off from everything except the Hub, to contain it while keeping it manageable. Choose the machine, give a reason (required), choose how long (1 hour, 4 hours, 24 hours or until released) and confirm. It holds across a restart and lifts by itself at the time chosen; *Release* on the machine's row lifts it at once. The Hub's own machine cannot be isolated.
- **Start encrypting**: tick the Windows machines to encrypt with BitLocker (see Disk encryption above).
- **Secret vault**: a sealed place on the Hub for the secrets that open machines (local administrator passwords, disk recovery keys). Each secret has its own key, wrapped by the Hub's master key, so a database copy or backup holds nothing readable. A secret is read with a reason of at least five characters, is shown once, and is limited to 20 reads an hour per person. Every read is listed with who read it and why, and is written to the Audit Log (the reason, never the value). Old versions are kept for 7 days. **Keep a copy of the file `data\vault.key` on the Hub, apart from the database**: it protects the vault and new session recordings, and a Hub that loses it cannot read its sealed secrets. The card then reads *Locked*.

Settings

- **OS Event Policy**: which operating-system events machines watch for, by category, and how much of it reaches the Hub. *Devices*: attach and removal, enable and disable, Bluetooth pairing. *Security posture*: firewall (each profile), antivirus, disk encryption and local administrators changing. *Authentication*: failed sign-ins, lockouts, local accounts created or deleted, remote sign-ins. *Filesystem*: removable drives mounted and removed, and files written to them (count and size only, never names or content). New categories start off. Device policy is enforced on the machine either way.
- **Where notices go**: for each kind of finding (sign-in anomalies, file integrity, firewall, unmanaged devices, hardening score, disk encryption, administrators, certificates, unexpected restarts), pick the alert channels you have already set up (email or webhook). Each finding is announced once, and nothing is sent until a channel is chosen.
- **Unexpected restarts**: when an agent starts without a clean stop recorded (a crash, a power cut, the process ended from outside), the Audit Log records it and a notice goes to the chosen channel, at most once a day per machine. A normal restart sends none.

Recordings

Turn on *Record Sessions* for a group (**Groups** → *Manage Group*) and every session on its machines is recorded by the Hub. Play recordings back here; playback shows a watermark with the viewer's name and

the time. Viewing them needs the *View Session Recordings* permission, separate from viewing a screen live. Recordings are stored encrypted on the Hub, each with its own key, and a recording stops growing at 2 GB; playback and export are unchanged, and recordings made before this version still play. Keep a copy of the file `data\vault.key` on the Hub, apart from the database, because it protects them: a Hub that loses it cannot play its new recordings. Recordings are kept until you set a retention period on this page (0 = keep them all).

Security

The Hub's mail server (SMTP) for MFA codes and notices, with *Test connection*, and the *Admins must use MFA* switch (on by default). MFA for everyone else is required per group (section 9). *Sign out after inactivity* is *Never* by default; choose 30 minutes, 1, 2, 4 or 8 hours and an open admin page with no keyboard, mouse, touch or scroll for that long signs out, and a browser left closed for that long asks for a sign-in. Only an administrator can change it, and the change is audited.

Audit Log

A permanent record of significant events: enrolments, sign-ins that succeeded or failed, access granted, revoked and denied, role and policy changes, sessions started and terminated, features opened, files transferred, Ctrl+Alt+Del sent, machines stopping and starting, and more. Every remote action names the user who did it. Entries are written in plain words. Connections that close without signing in (for example a port scan) are recorded once per address per hour, and the next entry for that address counts the rest.

- **Search** by event type, status, machine, user, session and date range.
- **Export** the filtered rows as CSV or JSON. Compliance reports are on the **Reports** page.
- **Forwarding** (⚙ *Forwarding*): mirror every event as it is written to a webhook URL or a syslog server, best-effort.
- By default the log is kept in full; nothing is deleted from it.

Tasks

Schedule an action on a machine.

ACTION	WHAT IT DOES
Self-update	Updates the agent to the current release.
Restart	Restarts the machine.
Shutdown	Shuts the machine down.

ACTION	WHAT IT DOES
Diagnostics bundle	Collects logs and state for troubleshooting.

Run it *Once* at a set time, or *Recurring* every N minutes. The list shows each task's next and last run.

Automation

Rules that act without anyone watching. Each rule has a trigger, a machine, an action (the same four as Tasks, or a script from the library, where your licence includes them), and a cooldown so it cannot fire repeatedly.

Machine offline for…

Fires when the machine has been unreachable for longer than the number of minutes you set.

Feature health check failed

Fires when screen capture, clipboard, file management, input injection or terminal stops working on the machine, even though it is still connected.

Check failing for…

Fires when one of the machine's monitoring checks has been failing for longer than the minutes you set.

Auto-healing presets fill in the common rules in one click: restart the machine if screen capture, clipboard, terminal or input injection fails, with a 60-minute cooldown. Adjust before saving. The *Last Fired* column shows when a rule last acted; one that fires often points to an underlying problem worth investigating.

13

Troubleshooting

A machine never appears in the Hub

CHECK	HOW
Is the agent running?	WINDOWS `sc query SD-Endpoint` LINUX `systemctl status SD-Endpoint` If it starts and stops at once, check for an Operator already installed on that machine.

CHECK	HOW
Is the Hub address right?	The install command must point at the Hub's network address, not `localhost`. If it does not, set `advertised_host`, restart the Hub, create a new token and reinstall.
Can it reach port 8484?	Outbound TCP from the machine to the Hub. On the Hub side: the installer opened it.
Seats and licence	Check the License page: enough Endpoint or Operator seats left, and the trial or licence not expired.

An operator's machine list is empty

The account has Operator Login Access but no Endpoint Connection Access. Grant machines in Users → Manage Access, or add the user to a group.

An operator cannot sign in to the console

- The account needs *Operator Login Access* for that specific Operator machine.
- The account may be deactivated.
- Check the Audit Log for failed sign-ins to see whether the attempt reached the Hub at all.

Someone cannot sign in to the Hub dashboard

Their role lacks the *Manage Users* permission. Of the built-in roles, only Admin has it.

An administrator is locked out

Another administrator can reset the password or MFA from **Users**. With no other administrator, use the Hub's `recover` command on the Hub machine (section 14).

A tile is greyed out

Hover over it for the reason — see section 10.

The setup page does not load from another computer

Correct behaviour. Setup is loopback-only until completed. Open it on the Hub machine, directly or over Remote Desktop (section 6).

Ctrl+Alt+Del does nothing

The `SoftwareSASGeneration` policy is not set on that Windows machine (section 8). Windows fails silently, so there is no error to find.

Black screen, or the stream will not start

- Open the machine's *Health* panel in Machines to see whether screen capture is reported as working.
- Windows: the agent must be running as its service (LocalSystem), not started by hand from a user session.
- Linux: a graphical desktop session must be running on the machine.

Clipboard sync does not work on Linux

Install `xclip` (X11) or `wl-clipboard` (Wayland) on the Endpoint.

"Busy" when starting a stream

Another operator is connected to that machine, which is set to one operator at a time (Exclusive). Wait or ask them to leave; an administrator can also set the machine to View-only or Multi (section 11).

A page or feature is missing, or answers "Not within the current licence"

The menu shows only what your licence includes. A feature of another product line is not shown at all; a feature of your own line that the licence does not include answers *Not within the current licence*. Check which line the licence names on the License page, and see section 3.

"Online licensing is not configured on this server"

Use offline activation (section 7).

Collecting information for support

Select *Diagnostics* for the affected machine in **Machines** and send the downloaded bundle with a description of the problem.

Reference

Components by platform

COMPONENT	PLATFORM	SERVICE	INSTALL LOCATION	CONFIGURATION
HUB				
Hub	Windows	`SD-Hub` created by the installer	`C:\Program Files\SarvDrik Hub`	`…\SarvDrik Hub\config.yaml` written by the installer
OPERATOR				
Operator	Windows	`SD-Operator`	`C:\Program Files\SarvDrik RMM Operator`	`config.yaml` in the install folder
Operator	Linux	`SD-Operator.service`	`/opt/sarvdrik-rmm-operator`	`config.yaml` in the install folder
ENDPOINT				
Endpoint	Windows	`SD-Endpoint`	`C:\Program Files\SarvDrik RMM`	`config.yaml` in the install folder
Endpoint	Linux	`SD-Endpoint.service`	`/opt/sarvdrik-rmm`	`config.yaml` in the install folder

Linux service names are case-sensitive: `SD-Endpoint`, not `sd-endpoint`.

Hub data and database

	WINDOWS HUB
Keys and identity	`C:\Program Files\SarvDrik Hub\data`
Database	Bundled PostgreSQL, data in `…\SarvDrik Hub\pgdata`
Log file	`…\SarvDrik Hub\server_runtime.log`
Firewall	Rules added by the installer

Service commands

```
# Windows — state and restart
sc query SD-Hub
sc query SD-Operator
sc query SD-Endpoint
Restart-Service SD-Hub

# Linux agents
sudo systemctl status SD-Endpoint      # or SD-Operator
journalctl -u SD-Endpoint -n 100 --no-pager
```

Admin recovery on the Hub machine

For an administrator who cannot sign in and has no other administrator to help. On the Hub machine, from an elevated PowerShell (*Run as administrator*):

```
& "C:\Program Files\SarvDrik Hub\SD-Hub.exe" recover
```

It lists the admin accounts and resets the chosen one's password, its MFA or both, re-enables the account and signs it out everywhere. It works with the Hub stopped. Every run is recorded in the Audit Log with the Windows account that ran it and exactly what changed, and is announced to the alert channels and the other administrators.

Back up

PLATFORM	BACK UP
Windows Hub	`data\`, `pgdata\` and `config.yaml` from the install folder, with the `SD-Hub` service stopped.

LOSING THE HUB'S DATA FOLDER STRANDS THE FLEET

Every enrolled agent trusts the certificate authority stored there. Without a backup, a rebuilt Hub has a new identity, and every machine must be re-enrolled.

Glossary

Hub

The server you run. Holds accounts, roles and grants, routes every session, serves the admin dashboard.

Operator

The agent on a support person's machine and the browser console it serves. Also the person using it.

Endpoint

The agent on a managed machine, and the machine itself.

Role

A set of feature permissions attached to a user account.

Operator Login Access

A grant allowing a user to sign in on a particular Operator machine.

Endpoint Connection Access

A grant allowing a user to reach a particular Endpoint, directly or through a group.

Machine Policy

Connection rules for one machine: hours, IP ranges, minimum agent version.

Access Policy

Rules on one user's grant to one machine, such as an access time window.

Deployment token

A secret embedded in install commands so machines can enrol themselves. Shown once.

Unmanaged

A machine that has enrolled but has not yet been acknowledged by an administrator.

Kill switch

The Enabled switch in Machines. A disabled machine is refused by the Hub.

Health check

The Endpoint's own report of which capabilities work on it.

Seat

One enrolled machine counted against your licence. An Operator takes an Endpoint seat; the License page also shows how many seats are Operators.

Product line

The product your licence is for. The licence names the line, and the Hub shows what that line includes.

First-run setup

The one-time, loopback-only wizard that gives a new Hub its certificate.