
Installation profiles

A security posture chosen at installation,
enforced and defended by the pool itself

Explanatory dossier for the IT department

Cellule-PRO, version 0.2.157 (image v1.0-rc92gj)

Key point

“Air gap by default. Opening up to the outside is your IT department’s decision, never ours.”

The installation profile turns this sentence into concrete rules. You choose it once, in the first-boot wizard; the pool applies it, passes it on to the other pools of your cluster, refuses the pools that do not share it, and entrusts neither its workers nor your data to a pool that departs from it.

Contents

1	Why installation profiles	2
2	The four profiles	2
2.1	Locks and proposed values	2
2.2	What profile A locks	3
3	Which profile to choose, and in what framework	3
3.1	The decision guide in four questions	3
3.2	Examples by sector	4
3.3	What each profile changes for employees	4
3.4	The regulatory framework	5
3.5	One organisation, several needs	5
3.6	Changing your profile over time	5
3.7	Frequently asked questions	5
4	Choosing the profile at installation	6
4.1	In the first-boot wizard	6
4.2	A pool joining an existing cluster	6
4.3	Changing the profile afterwards	6
5	One profile for the whole cluster	7
6	Joining the cluster: admission	7
6.1	How the pool knows the other one's profile	7
6.2	Admission rules	7
6.3	The exception	8
7	Working with the other pools: "Only work with pools of the same profile"	8
7.1	Three states for each member	8
7.2	What the pool no longer entrusts to a set-aside member	8
7.3	The safeguards	9
7.4	What you see	9
7.5	The setting	9
8	What the pool does by itself, and what it does not do	10
9	What you see in the Supervision	10
10	Step-by-step scenarios	10
10.1	A single site in full air gap	10
10.2	Adding a second site to the cluster	11
10.3	A pool hardened its profile without the others	11
10.4	A pool not yet updated	11
11	The settings at a glance	11
12	Known limitations and next steps	11
13	Glossary	12

1 Why installation profiles

A company that installs Cellule-PRO does not have the same needs depending on its line of business. A research department classified “defence secret” wants nothing, ever, to leave the building. A law firm wants the same confidentiality, but accepts that its IT department occasionally opens access to an external API. A branch network or a transport company needs its drivers to call and write from the road.

Without a profile, several dozen options would have to be set one by one, and the slightest mistake would open a door. The installation profile groups these choices into **a single decision**, made at first boot, readable by everyone (“this cluster is in full air gap”) and **defended by the pool itself**: its most important rules are no longer mere settings, they are locks.

Three principles guide this whole dossier:

1. **The choice belongs to your IT department.** The pool chooses none for you; the wizard requires an explicit choice.
2. **Hardening is easy, relaxing is hard.** Moving to a stricter profile takes one click and spreads by itself; going back requires the approval of two administrators.
3. **A cluster only brings together pools with the same profile.** A pool only admits, backs up and informs pools that share its posture.

2 The four profiles

Profile	For whom	In practice
A. Full air gap	Defence secrets, confidential health data, sensitive R&D.	Nothing ever leaves: no external API, no access from outside, every device approved by two administrators. Everything is locked .
B. On-site company (recommended)	Law firms, SMEs, industry.	Nothing leaves by default; the external API stays possible if your IT department decides so. Off-site access through your VPN.
C. Multi-site and mobility	Branch networks, transport, field teams.	Calls and messaging from outside for enrolled devices; phones sent to the most available pool.
D. Demonstration	Trial, trade fair, proof of concept.	Never real data. Not intended for production.

2.1 Locks and proposed values

Each profile acts in two different ways:

Locks apply no matter what: whatever value is stored in the database, received from another pool or imported, the pool applies the locked value. Only profile A has them.

Proposed values are set only once, at installation, on the settings you have not touched yet. You remain free to change them afterwards in the Advanced settings.

2.2 What profile A locks

Locked rule	Effect
External API (Claude, ChatGPT...)	Turned off: key refused, ignored, connector stopped. The key is never erased, only made unusable.
Access from outside (calls, mail, files, uploads, remote installations)	Closed.
Confidential jobs	Reserved for the trusted servers you have designated.
Workers	Pairing mandatory, encrypted link mandatory.
CelluleBot devices	Every device approved by an administrator; enrolment requires a <i>second</i> administrator; no standalone use.
Supervision	Employee names hidden.
Inference confidentiality	Strict mode.
Cluster pools	The pool only works with pools of the same profile (section 7).

3 Which profile to choose, and in what framework

The profile is not a technical setting: it is the translation, into rules enforced by the software, of a decision by your management and your IT department about what is allowed to leave the company, and from where people can work. It is therefore chosen on the basis of your obligations and your way of working, not on the basis of the machine.

3.1 The decision guide in four questions

1. **Is this a trial, a demonstration, a trade fair?** With no real data at all: profile **D**. In every other case, never use D.
2. **Do you handle information whose leak would be serious and over which the law, a contract or a security clearance requires full control** (classified or clearance-restricted information, critical industrial secrets, confidential health data, investigations)? Profile **A**.
3. **Do your employees need CelluleBot outside the company** (calls and messaging while travelling, drivers, technicians, branches without a VPN)? Profile **C**.
4. **Otherwise:** your teams work on site, or remotely through the company VPN. Profile **B**, the recommended choice for most organisations.

Key point

When in doubt, choose **the strictest** profile your activity can bear. Hardening later takes one click; relaxing requires the approval of two administrators. Starting strict costs nothing; starting too open can cost a leak.

3.2 Examples by sector

Organisation	Profile	Why
Defence, cleared subcontractors, sensitive laboratories	A	Nothing must be able to leave, even through an administrator's mistake; two people for any sensitive decision.
Healthcare institutions, clinical research	A or B	A for the departments that handle patient records; B for administration if the external API may one day serve non-sensitive uses.
Law firms, notaries, chartered accountants	B	Professional secrecy: nothing leaves by default, but the IT department keeps the option of occasionally opening an external API for general uses.
Industry, engineering firms, SMEs	B	Know-how protected on site; remote work through the VPN.
Transport, logistics, field teams	C	Drivers and technicians call and write from the road; knowledge bases and mail stay on site.
Branch networks, franchises, multi-site local authorities	C	Several sites and mobile employees; each phone is sent to the most available pool.
60-day trial, proof of concept, trade fair	D	Evaluation without real data; never put any company document in it.

3.3 What each profile changes for employees

Capability	A	B	C	D
Use AI on site (questions, documents, debates)	yes	yes	yes	yes
An external AI API for general questions	never	on the IT department's decision	on the IT department's decision	on decision
Calls and messaging from outside	never	no (VPN)	yes	no
Send files in messaging off site	never	no	yes	no
Upload to knowledge bases off site	never	no	no	no
Mail from outside	never	no	no	no
Phone sent to the most available pool	no	no	yes	no
New device approved by	2 admins	1 admin	1 admin	optional

“never” = locked by the profile; “no” / “yes” = value proposed at installation, which can be changed afterwards in the Advanced settings.

3.4 The regulatory framework

The profile helps you meet your obligations; it does not replace them, and it is not a certification. Your security officer and your data protection officer remain the judges of the configuration chosen.

- **GDPR:** data minimisation and location. Profiles A and B keep all processing inside the company by default; any opening to an external API is a recorded decision of the IT department.
- **Professional secrecy** (lawyers, healthcare, chartered accountants): nothing leaves without an explicit decision; in A, nothing can leave at all.
- **Sensitive or classified information:** profile A cuts off every outbound flow and requires two administrators; the accreditation of your system remains your responsibility and that of your authority.
- **Health data hosting:** Cellule-PRO is software installed on your premises; it is your infrastructure that hosts the data, and it is your infrastructure that falls under your hosting obligations.
- **NIS2** and information system security: locked profiles, the profile log, and the Supervision’s findings and alerts help demonstrate control over the configuration.

3.5 One organisation, several needs

A cluster has only **one** profile: all its pools share the same posture. If one department must be in full air gap (research, legal department) while the rest of the company needs mobility, install **two separate clusters**: one in A for the sensitive department, one in C for the rest. They will not be linked together, and that is intended: nothing can flow from cluster A to cluster C.

3.6 Changing your profile over time

- **Towards stricter** ($D \rightarrow C \rightarrow B \rightarrow A$): one click in “Profile of this pool”, applied to the whole cluster within a few minutes.
- **Towards less strict** (for example $B \rightarrow C$ when your teams become mobile): this is a relaxation, which will require the approval of two administrators (procedure planned for a future version). Anticipate it when making the initial choice.
- **From D to a production profile:** an evaluation becomes a real installation by hardening its profile; remember to delete the trial data beforehand.

3.7 Frequently asked questions

Does the profile slow down the AI? No. It decides what can leave and where people work from; the computing power and the models are the same in all four profiles.

Can each pool have a different profile? No, and that is deliberate: a less strict pool would be the door through which the cluster’s data would leave. A pool with another profile does not get in, and a member that diverges is set aside.

What happens if an administrator makes a mistake? In A, the locks prevent them from opening anything at all. In the other profiles, every change is logged, and a relaxation will require two administrators.

A pool installed before profiles existed? It works as before as long as no profile is chosen; as soon as a pool of the cluster chooses one, the others adopt it by themselves.

4 Choosing the profile at installation

4.1 In the first-boot wizard

The Cellule-PRO image is delivered blank: no administrator, no profile. The “Security” step of the wizard presents the four profiles, each with the exact list of its locks, read from the pool’s own code. **No profile is preselected:** the wizard cannot finish without a choice.

Caution

Profile A requires **two administrators** from installation onwards (different addresses, checked by the server). This is the condition for no single person being able, later on, to enrol a device or relax the profile.

At the end of the wizard, the pool checks everything before writing anything, applies the profile *before* creating the accounts, then sets the proposed values on the free settings. Submitting the same step a second time has no effect; an attempt to lower the profile is refused.

4.2 A pool joining an existing cluster

When the wizard is used to add a pool to a cluster already in service, no profile is chosen: the cluster’s profile will apply. Until it has been received, the new pool puts itself **in the strictest posture** (air-gap locks) and reports it:

- “Profile of this pool” card: “waiting for the cluster’s profile”;
- Supervision and health status: finding “Pool X is waiting for the cluster’s installation profile”.

The profile arrives within a few minutes, through the signed transmission described in the next section; the wait then ends by itself. A restart during the wait does not end it: only a real profile does.

4.3 Changing the profile afterwards

In the Advanced settings, “Profile of this pool” card, an administrator can **harden** the profile (for example move from B to A), after entering their password again. The change is written to the profile log and sent immediately to the other pools.

Relaxing (from A to B, for example) is not possible from this screen: it is a decision that will require the approval of two administrators (procedure planned for a future version).

5 One profile for the whole cluster

A Cellule-PRO cluster brings together several pools (one per site, for example) linked by a signed federation (Ed25519). The profile is a property of the *cluster*, not only of one pool.

The pool handles it by itself

- Each pool republishes its profile, signed, every 5 minutes, and immediately after a change.
- A pool that receives a profile **stricter** than its own adopts it by itself and records it in its log (“profile received from pool X”).
- A **less strict** profile received is always refused: a pool cannot weaken the others.
- Two simultaneous choices on two pools converge towards the stricter one.

The setting `INSTALL_PROFILE_ACCEPT_FROM_PEERS` (“Accept the installation profile sent by the other pools”, on by default) lets a pool accept only the decisions of its own administrator. It is a choice specific to each pool, which no other pool can impose on it.

6 Joining the cluster: admission

Linking two pools (Federation, “Add a peer”) is not enough to make them *members* of the same cluster. The pool first checks the other one’s profile.

6.1 How the pool knows the other one’s profile

Never through a mere question without proof. Another pool’s profile is only taken into account if it arrives in a message **signed** by that pool:

- in the signed handshake that links the two pools;
- in a signed attestation, bound to the pool requesting it and to a unique random challenge, valid for two minutes (impossible to replay or divert);
- in a member’s signed republication.

6.2 Admission rules

Situation	Decision
Same profile on both sides	Admitted as a member.
Different profiles	Refused: the pool remains only “known”.
The other pool has just been installed and is waiting for the cluster’s profile	Admitted: it will adopt yours.
The other pool’s profile is unknown (older version, announcement older than 24 h)	Refused if your pool is in air gap; admitted otherwise.
Your own pool is waiting for its profile	It admits nobody for now.

Situation	Decision
No profile chosen (cluster installed before profiles existed)	Admitted, behaviour unchanged.

6.3 The exception

When a pool is refused, the “Add a peer” screen explains why (“Different installation profiles: this pool is A, the other is B”) and how to fix it (choose the same profile on both sides). If your IT department nevertheless decides to admit it, it ticks “I link this pool as a member anyway” then “Link anyway”.

Caution

The exception is only possible from the dashboard, by an identified administrator (never read-only, never through the API). It is **recorded under the administrator’s name before** the pool becomes a member: if the recording fails, the pool does not get in. A pool admitted by exception receives the cluster’s data.

7 Working with the other pools: “Only work with pools of the same profile”

Admission is decided only once. But a member may change afterwards: its administrator hardens its profile without yours following (automatic reception turned off), or it is no longer up to date. The pool never *demotes* a member by itself (that would be an easy way to disrupt a cluster); on the other hand, **it stops entrusting it with anything** as long as the profiles differ.

7.1 Three states for each member

State	Meaning
Compatible	Same profile, known through a signed message less than 24 h old; or admitted by exception; or no profile chosen on your pool.
Different	Profile known, recent and different from yours: the divergence is certain.
Unknown	Profile missing or too old (pool not up to date yet), or being adopted.

7.2 What the pool no longer entrusts to a set-aside member

What is protected	How
Inference jobs	A busy pool no longer passes work on to this member.
Searches in memory and documents	No question is sent to it; its own questions are refused (it obtains no excerpt from your pool).

What is protected	How
Workers and proxies	The member disappears from the standby list handed out at each connection; no move order targets it (an order already issued is closed, never retried); load balancing and proximity routing ignore it; a switchover forced by the administrator goes out with the up-to-date list.
Certificate fingerprints	The member's fingerprint is no longer handed to workers and phones: they can no longer connect to it, even if asked to.
CelluleBot devices	The member is no longer offered as the “best pool”.

7.3 The safeguards

Data stops immediately. As soon as a profile is different (or unknown in air gap), no job and no question leaves any more.

Switchovers wait ten minutes. Right after a profile change on your pool, the other pools have not yet received the new profile (replication every 5 minutes). During these ten minutes, standby lists and move orders stay unchanged: a normal hardening does not cut off the cluster's backup.

Certificates are only removed when it is certain. A member whose profile is merely *unknown* keeps its fingerprint: a fingerprint removed by mistake is much harder to give back to devices than an address.

When in doubt, closed. If the pool cannot read its own profile again (startup, database temporarily unreadable), it behaves as in air gap until the next read.

Nothing breaks. If no member is compatible any more, the workers simply stay on their pool.

7.4 What you see

In the Supervision and in the health status (“@Cellule, what is your health status?”):

Key point

Pool X is no longer used by this pool.

This pool no longer sends it standby workers or proxies, jobs or searches: its installation profile is different, or unknown (pool not up to date yet).

Advice: choose the same profile on both pools, or update the other pool. To use it anyway: link it again in “Federation” and tick “Link anyway”.

The finding is an error on a pool in air gap, a warning otherwise.

7.5 The setting

`INSTALL_PROFILE_PEER_GATING` — “Only work with pools of the same installation profile”. Specific to each pool, **on by default, always on in profile A**. Without a chosen profile, it has no effect. Turning it off (outside profile A) gives your pool back the use of all members, whatever their profile.

8 What the pool does by itself, and what it does not do

The pool handles it by itself

- Apply the profile's locks, at every startup, whatever the database contains.
- Put itself in the strictest posture while it waits for its cluster's profile, or if it cannot read its own again.
- Send its profile, signed, to the other pools; adopt a stricter profile received.
- Refuse entry to a pool with a different profile.
- Continuously sort the members it works with, and show it in the Supervision.

What it does **not** do, on purpose:

- **Relax a profile:** reserved for two administrators. Otherwise, a single compromised pool could weaken the whole cluster.
- **Force another pool:** it sets it aside and warns you, it does not change it.
- **Exclude a member from the cluster:** demotion remains a human decision.

9 What you see in the Supervision

Finding	What to do
Pool X is waiting for the cluster's installation profile	Normal for a few minutes after linking it. If it lasts: check the Federation, or choose the cluster's profile in "Profile of this pool".
Pool X does not have the same installation profile	The profile copies itself; if it stays different, check that the pool is linked and runs the same version.
Pool X adopted the installation profile received from pool Y	If your team did not decide this change, check the profile log and turn off automatic reception.
Pool X is no longer used by this pool	Same profile on both sides, update of the other pool, or exception ("Link anyway").

10 Step-by-step scenarios

10.1 A single site in full air gap

1. Start the image, open the wizard; at the "Security" step, choose **A**.
2. Enter two administrators (different addresses).
3. Finish: the external API and outside access are turned off and locked; devices require approval by two administrators.

10.2 Adding a second site to the cluster

1. Bring the new pool to the **same version** as the others.
2. In its wizard, choose “Join an existing cluster”: it goes into waiting, in the strict posture.
3. Link it from a pool of the cluster (“Add a peer”): it is admitted (it is waiting for the profile).
4. Within a few minutes, it receives the cluster’s profile; the “waiting” finding disappears.

10.3 A pool hardened its profile without the others

The Boston pool moves to A; the Chicago pool (automatic reception turned off) stays in B.

- As soon as it is republished, Chicago knows that Boston is in A: it immediately stops passing it jobs and searches.
- Since Chicago’s profile has not changed, no grace period applies: Boston immediately leaves the standby lists of Chicago’s workers, and its fingerprint is no longer handed to devices. (The ten-minute delay only applies right after a profile change of the pool itself.)
- Chicago’s Supervision shows “Pool Boston is no longer used by this pool”.
- Fix: turn automatic reception back on in Chicago (or choose A there); everything recovers by itself.

10.4 A pool not yet updated

A pool with a version older than 0.2.156 does not announce its profile: it is “unknown”. In air gap, it is set aside from jobs and backup, but keeps its fingerprint. Updating it is enough.

Caution

Bring all the pools of a cluster to the same version **before** choosing profile A: otherwise the older pools will be set aside until they are updated.

11 The settings at a glance

Setting	Default	Role
<code>INSTALL_PROFILE_ACCEPT_FROM_PEERS</code>	on	Adopt a stricter profile chosen on another pool.
<code>INSTALL_PROFILE_PEER_GATING</code>	on (locked in A)	Only work with pools of the same profile.

These two settings are specific to each pool: the “Align the cluster” repair never copies them.

12 Known limitations and next steps

- **Business data between divergent members.** Messages, memory, project documents and API keys are still copied to a member whose profile has become different. This will be fixed before any distribution to customers (batch P3b).

- **Relaxing a profile:** two-administrator procedure (batch P4).
- **Profile D:** “no real data” banner and blocking at the end of the evaluation, without erasure.
- **One-click repair:** “Put this pool back on the cluster’s profile” among the repairs offered by the Supervision.
- A member pool can still *harden* the others’ profile: this is intended (security can only go up), and every adoption is logged and visible.

13 Glossary

Cluster Set of linked Cellule-PRO pools, which share identities, common settings and backup.

Member Pool admitted into the cluster (trust level 2 or higher), as opposed to a pool that is only “known”.

Pool Cellule-PRO server of a site (Docker image).

Worker Workstation or server that runs the models for the pool.

Proxy Mobile relay that serves one or more engines and can switch from one pool to another.

Standby list Pools to which a worker or a proxy switches if its own goes down.

Fingerprint Identifier of a pool’s certificate; a device only connects to a known fingerprint.

Signed message Message accompanied by a verifiable Ed25519 signature: it can neither be forged nor attributed to another pool.

Exception An administrator’s explicit decision to admit a pool despite a different profile, recorded under their name.