GUIDE DE DÉMARRAGE RAPIDE

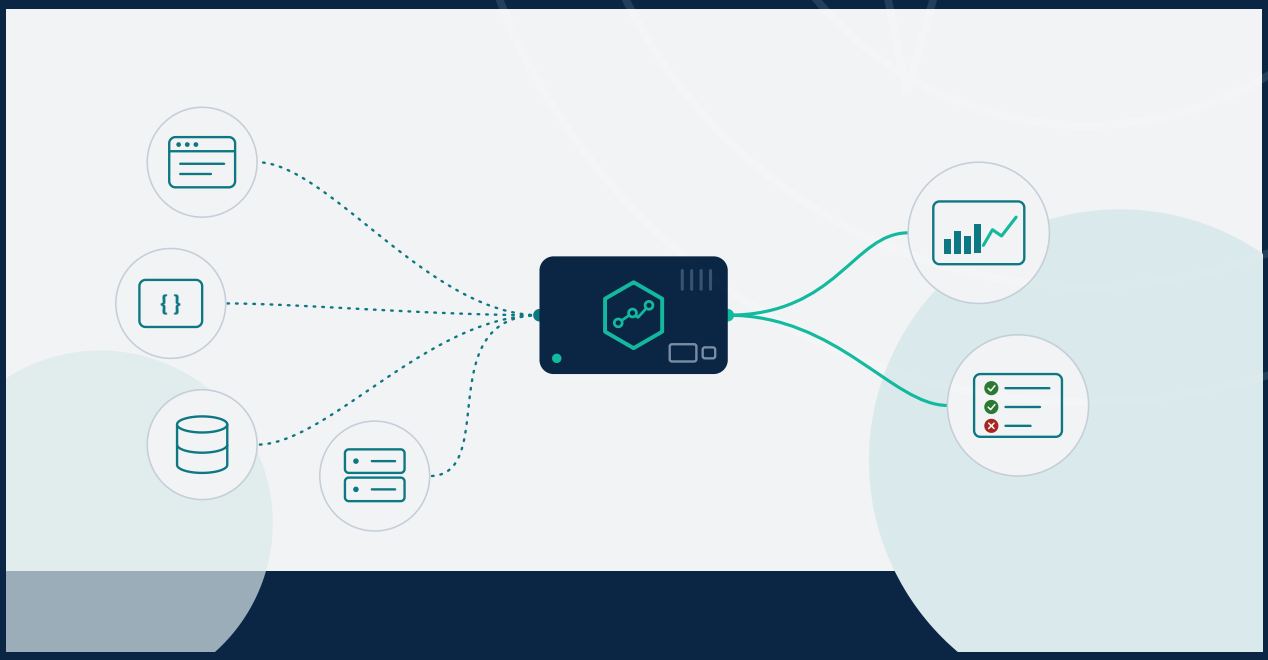
SYNOVEX

Guide de démarrage rapide

Matériel : Raspberry Pi 5

Éditions : Essential, Professional, Enterprise

Public : Techniciens d'installation, administrateurs et nouveaux clients



SYNOVEX — SIREN 884 713 009

Table des matières

Informations sur le document 3

Chapitre 1 — Avant de commencer 7
- 1.1 Contenu du colis 7
- 1.2 Matériel à réunir 8
- 1.3 Précautions de manipulation 9

Chapitre 2 — Installer la sonde 11
- 2.1 Installer le refroidissement 11
- 2.2 Installer la carte dans le boîtier 12
- 2.3 Insérer la microSD 13
- 2.4 Connexion Ethernet 14
- 2.5 Branchement de l'alimentation et démarrage 14
- 2.6 Voyant d'état 15
- 2.7 Liste de vérification de fin d'installation physique 16

Chapitre 3 — Mettre en service la sonde 17
- 3.1 Mise en service par l'assistant web (méthode B) 17

Chapitre 4 — Vérifier la sonde et créer un premier contrôle 24
- 4.1 Consulter l'état depuis l'interface d'administration 24
- 4.2 Vérifier la vivacité avec /health 24
- 4.3 Créer le contrôle depuis l'interface d'administration 24
- 4.4 Vérifier la remontée des résultats 25

Chapitre 5 — En cas de difficulté 26
- 5.1 Erreurs fréquentes lors de l'installation 26

Chapitre 6 — Documentation et assistance 27
- 6.1 Assistance et contacts 27

SYNOVEX

Guide de démarrage rapide

Sonde de supervision applicative autonome pour Raspberry Pi 5

Information	Valeur
Document	Guide de démarrage rapide — identifiant SYN-DOC-01
Révision documentaire	B
Public	Techniciens d'installation, administrateurs et nouveaux clients
Produit	SYNOVEX
Matériel pris en charge	Raspberry Pi 5
Éditions couvertes	SYNOVEX Essential, SYNOVEX Professional, SYNOVEX Enterprise
Éditeur	SYNOVEX — SIREN 884 713 009
Documentation en ligne	`https://docs-synovex.incitypark.fr` (après l'annonce de sa mise en service)
Langue	Français

Mentions légales

Éditeur

Cette documentation est éditée par SYNOVEX, SIREN 884 713 009. SYNOVEX est aussi le nom commercial de la gamme de sondes de supervision décrite.

Propriété intellectuelle et diffusion

© SYNOVEX. Tous droits réservés. Les textes, schémas, illustrations et exemples de cette documentation sont protégés par le droit d'auteur.

Cette documentation est réservée aux clients titulaires d'un droit d'utilisation du produit SYNOVEX. Le client peut la reproduire et la diffuser à l'intérieur de son organisation, et la communiquer aux prestataires qui interviennent pour son compte, pour les seuls besoins de l'installation, de l'exploitation et de la maintenance de ses sondes. Toute autre reproduction, diffusion ou mise à disposition, totale ou partielle, requiert l'accord écrit préalable de SYNOVEX.

Les fichiers d'exemple fournis avec la documentation (scénarios, règles d'alerte, tableau de bord, schémas JSON) peuvent être copiés et adaptés par le client pour l'exploitation de ses sondes.

Limitation de responsabilité

Les informations de cette documentation peuvent être modifiées sans préavis. L'éditeur s'efforce d'en assurer l'exactitude, mais ne peut être tenu responsable des erreurs ou omissions, ni des conséquences de l'utilisation des exemples fournis. Les exemples de configuration et de scénarios sont **fictifs** et doivent être adaptés à votre environnement, puis validés, avant tout usage. Cette documentation ne constitue pas un engagement contractuel : les engagements de l'éditeur, notamment de garantie, de support et de maintenance, résultent exclusivement de votre contrat.

Marques

SYNOVEX est un nom commercial de l'éditeur. Raspberry Pi est une marque de Raspberry Pi Ltd. Orange Pi est une marque de Shenzhen Xunlong Software Co., Ltd. Google Chrome est une marque de Google LLC ; Chromium et Puppeteer sont des projets open source de Google LLC. Java, OpenJDK, Oracle et MySQL sont des marques d'Oracle et/ou de ses filiales. Node.js est une marque de l'OpenJS Foundation. Prometheus et OpenTelemetry sont des marques de The Linux Foundation. Grafana est une marque de Grafana Labs. Datadog est une marque de Datadog, Inc. Dynatrace est une marque de Dynatrace LLC. Nagios est une marque de Nagios Enterprises, LLC. Centreon est une marque de Centreon. Microsoft et SQL Server sont des marques du groupe Microsoft. PostgreSQL est une marque de PostgreSQL Community Association of Canada. MariaDB est une marque de MariaDB plc. Les autres noms de produits et de sociétés cités peuvent être des marques de leurs propriétaires respectifs. Leur mention dans cette documentation n'implique aucun partenariat ni aucune approbation.

Logiciels tiers

La sonde intègre des logiciels libres et des composants tiers, distribués selon leurs propres licences. Les principaux composants et leurs licences sont listés au § 11.1 de la référence technique et API ; l'inventaire complet des composants accompagne chaque version du logiciel.

Matériel et fin de vie

Le Raspberry Pi 5 et ses accessoires officiels sont fabriqués par Raspberry Pi Ltd, qui en publie les déclarations de conformité. Avec l'offre microSD préconfigurée, le matériel est choisi et assemblé par vos soins. Avec l'offre boîtier complet, les informations de conformité applicables figurent dans les documents joints au produit. En fin de vie, la sonde relève de la collecte des déchets d'équipements électriques et électroniques : ne la jetez pas avec les déchets ordinaires et confiez-la à une filière de collecte agréée, après avoir effacé ses données (§ 8.13 du guide d'installation et d'administration).

À propos de ce guide

SYNOVEX est une sonde autonome de supervision réseau, applicative et métier. Installée à l'endroit dont vous voulez connaître le point de vue (réseau de vos utilisateurs, centre de données, site distant, réseau d'un client ou d'un partenaire), elle exécute à intervalles réguliers des contrôles qui reproduisent ce que vivent les utilisateurs et les applications, et met les résultats à disposition de vos équipes et de vos outils de supervision. Elle repose sur un Raspberry Pi 5 et sur une carte microSD fournie préconfigurée.

Ce guide accompagne la carte microSD ou le boîtier complet. Il vous conduit, étape par étape, de l'ouverture du colis au premier résultat de supervision :

1. vérifier le contenu du colis et réunir le matériel (chapitre 1) ;
2. installer la sonde et la raccorder au réseau et à l'alimentation (chapitre 2) ;
3. la mettre en service avec l'assistant web (chapitre 3) ;
4. vérifier son état de santé et créer un premier contrôle HTTP (chapitre 4) ;
5. résoudre les difficultés les plus courantes (chapitre 5).

Ce guide décrit la mise en service par l'assistant web, adaptée à une installation unitaire sur un réseau doté d'un serveur DHCP. Pour un réseau sans DHCP, un port soumis à l'authentification 802.1X ou un déploiement en série, utilisez la mise en service par fichier de provisionnement (méthode A), décrite au § 4.3 du guide d'installation et d'administration.

La bibliothèque documentaire SYNOVEX

La documentation SYNOVEX se compose d'un manuel technique complet et de six guides spécialisés. Tous sont produits à partir des mêmes sources : un passage repris dans plusieurs documents y est rigoureusement identique.

Document	Identifiant	Public
Manuel technique complet	SYN-DOC-00	Tous publics : référence intégrale
Guide de démarrage rapide	SYN-DOC-01	Techniciens d'installation, nouveaux clients
Guide d'installation et d'administration	SYN-DOC-02	Administrateurs système et réseau, équipes de sécurité
Guide d'utilisation et de supervision	SYN-DOC-03	Équipes d'exploitation et de supervision
Guide de développement des scénarios	SYN-DOC-04	Développeurs, intégrateurs, équipes de qualité
Guide d'intégration et d'observabilité	SYN-DOC-05	Architectes, DevOps, SRE
Référence technique et API	SYN-DOC-06	Intégrateurs avancés, architectes, développeurs

Renvois. Dans un guide, un renvoi sans autre mention désigne une section, un chapitre ou une figure du même guide, avec la numérotation de ce guide. Lorsque le sujet est traité dans un autre guide, le renvoi nomme ce guide, par exemple « § 6.3 du guide d'installation et d'administration ». La numérotation est alors celle du guide cité. Chaque

guide se lit ainsi sans le manuel technique complet, qui réunit l'intégralité de la documentation sous sa propre numérotation.

Services en ligne. L'ensemble de la bibliothèque est également publié sur `https://docs-synovex.incitypark.fr`, avec une recherche et une navigation par profil. Ce site, le portail de support et le service de distribution des mises à jour de l'éditeur sont accessibles après l'annonce de leur mise en service. Avant cette annonce, ou si l'un de ces services ne répond pas, utilisez le canal de contact prévu par votre contrat. Les adresses citées dans ce guide s'entendent sous cette réserve.

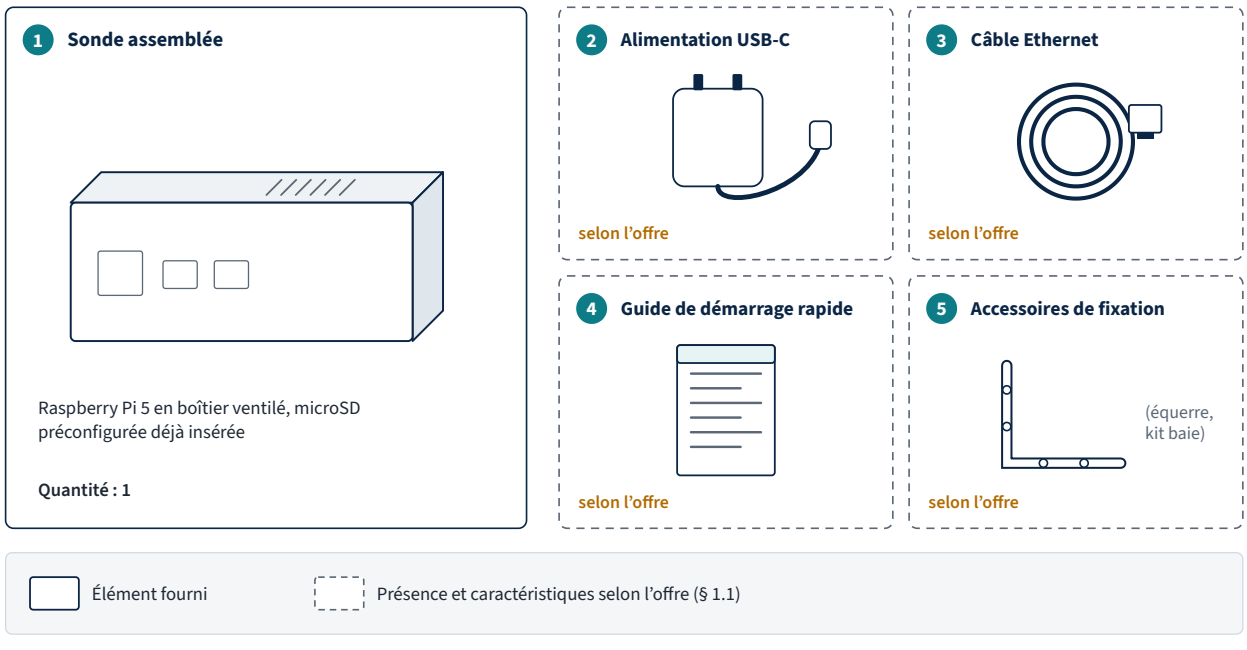
Chapitre 1 — Avant de commencer

Avant de commencer, vérifiez le contenu du colis, réunissez le matériel nécessaire et prenez connaissance des précautions de manipulation. Si vous avez reçu le **boîtier complet**, le Raspberry Pi 5 est déjà assemblé, avec sa carte microSD : seul le premier point vous concerne, puis passez directement au raccordement Ethernet (chapitre 2).

1.1 Contenu du colis

Offre boîtier complet.

Élément	Quantité	Vérifié
Sonde assemblée (Raspberry Pi 5 en boîtier ventilé, microSD préconfigurée insérée)	1	[ ]
Alimentation USB-C	Selon la liste de colisage de votre commande ; à défaut, voir § 2.2 du guide d'installation et d'administration	[ ]
Câble Ethernet	Selon la liste de colisage de votre commande ; à défaut, à fournir par vous (§ 2.5.1 du guide d'installation et d'administration)	[ ]
Guide de démarrage rapide	Selon la liste de colisage de votre commande	[ ]
Accessoires de fixation (équerre, kit baie)	Selon la liste de colisage de votre commande	[ ]



Représentation schématique, non à l'échelle

Figure 1-1 — Contenu du colis de l'offre boîtier complet

Offre microSD préconfigurée (§ 3.4 du guide d'installation et d'administration). Le colis contient les éléments suivants ; tout autre élément est fourni par vos soins (§ 1.2).

Élément	Quantité	Vérifié
Carte microSD contenant le système et le logiciel de la sonde, portant son numéro de série (§ 3.3.3 du guide d'installation et d'administration)	1	[ ]
Encart d'identification : édition acquise, numéro de série du produit et code d'installation (§ 3.3.3 du guide d'installation et d'administration)	1	[ ]

En cas d'élément manquant ou endommagé, contactez le support avant toute installation (coordonnées au chapitre 6).

> **Information** — Dans l'offre boîtier complet, la microSD est déjà insérée. Il n'est pas nécessaire d'ouvrir le boîtier. Si vous souhaitez utiliser un fichier de provisionnement (§ 4.3 du guide d'installation et d'administration), retirez la microSD selon les indications jointes au boîtier livré ou, à défaut, communiquées par le support ; ne forcez jamais sur le lecteur.

1.2 Matériel à réunir

Objectif : disposer de tous les éléments nécessaires avant de commencer l'assemblage.

Le tableau suivant liste le matériel que vous devez fournir. Les exigences détaillées figurent au chapitre 2 du guide d'installation et d'administration.

Élément	Exigence	Remarque
Raspberry Pi 5	RAM selon l'édition (§ 3.3.2 du guide d'installation et d'administration)	Modèle 5 exclusivement
Alimentation	Alimentation officielle Raspberry Pi 27 W USB-C (5,1 V, 5 A) recommandée	Une alimentation 5 V / 3 A fonctionne, mais limite le courant disponible sur les ports USB ; c'est un comportement documenté du Raspberry Pi 5
Refroidissement	Refroidisseur actif officiel (*Active Cooler*) ou boîtier équipé d'un ventilateur	**Obligatoire pour l'édition Enterprise**, recommandé pour les autres
Boîtier	Boîtier compatible Raspberry Pi 5, ventilé, laissant accès au lecteur microSD, au port Ethernet et au port USB-C	Le boîtier officiel Raspberry Pi 5 intègre un ventilateur
Câble Ethernet	Catégorie 5e minimum, longueur adaptée	Câble droit standard
microSD préconfigurée	Fournie	Ne pas la remplacer par une autre carte
Facultatif	Écran HDMI + câble micro-HDMI vers HDMI	Pour lire le code d'installation et l'empreinte du certificat à l'écran (§ 3.1.3)
Facultatif	Carte M.2 HAT+ officielle de Raspberry Pi et SSD NVMe M.2 2230 ou 2242 pris en charge	Volume de données complémentaire, surtout utile pour l'édition Enterprise (§ 2.3.3 du guide d'installation et d'administration). Exige l'alimentation officielle de 27 W

Élément	Exigence	Remarque
Facultatif	Pile officielle de l'horloge temps réel (RTC) du Raspberry Pi 5	Recommandée si le port réseau est protégé par 802.1X : elle conserve l'heure hors tension, nécessaire à la vérification des certificats avant tout accès NTP (§ 2.5.1, § 5.2.6 du guide d'installation et d'administration)

✓ **Conseil** — Le boîtier officiel Raspberry Pi 5 et le refroidisseur actif officiel ne s'utilisent généralement pas ensemble, le boîtier disposant de son propre ventilateur. Suivez la notice du fabricant de votre boîtier pour savoir quel refroidissement installer. Si vous installez la carte M.2 HAT+ et un SSD (§ 3.4.6 du guide d'installation et d'administration), le boîtier officiel n'est utilisable que **sans son couvercle ni son ventilateur** : le refroidissement est alors assuré par le refroidisseur actif officiel, installé en premier.

1.3 Précautions de manipulation

Le Raspberry Pi 5 est une carte électronique nue. Comme tout équipement de ce type, il est sensible aux décharges électrostatiques, aux contraintes mécaniques et à l'humidité.

! **Avertissement** — Ne manipulez jamais la carte, la microSD ou les accessoires lorsque l'alimentation est branchée. Débranchez toujours le câble d'alimentation USB-C avant toute intervention à l'intérieur du boîtier.

1.3.1 Protection contre les décharges électrostatiques

Une décharge électrostatique (ESD, *ElectroStatic Discharge*) est le transfert brutal de charges électriques accumulées sur le corps humain vers un composant électronique. Elle est souvent imperceptible pour l'opérateur, mais peut endommager durablement un composant.

Appliquez les règles suivantes :

1. Travaillez sur une surface non conductrice et dégagée (table en bois ou tapis antistatique). Évitez la moquette et les vêtements en laine ou en fibres synthétiques.
2. Avant de saisir la carte, touchez une partie métallique reliée à la terre (châssis d'une baie raccordée à la terre, par exemple) ou portez un bracelet antistatique relié à la terre.
3. Tenez la carte **par ses bords**. Ne touchez ni les composants, ni les broches du connecteur GPIO, ni les contacts dorés de la microSD.
4. Conservez la carte dans son sachet antistatique d'origine jusqu'au moment de l'assemblage.

1.3.2 Précautions mécaniques

- N'exercez aucune pression sur les composants lors de la pose du refroidisseur ou de la fermeture du boîtier.
- N'insérez ni ne retirez la microSD en forçant : elle n'entre que dans un seul sens (voir § 2.3).
- Ne pliez pas les nappes ou câbles fins (câble du ventilateur notamment) à angle vif.
- Ne posez pas d'objet sur la sonde une fois installée : la circulation d'air doit rester libre.

1.3.3 Précautions liées à l'environnement

- N'installez pas la sonde dans un lieu humide, poussiéreux ou exposé aux projections de liquide.
- Ne l'exposez pas au rayonnement direct du soleil ni à proximité d'une source de chaleur.

- Respectez la plage de température ambiante de fonctionnement indiquée par Raspberry Pi Ltd dans la fiche produit du Raspberry Pi 5 (§ 2.8 du guide d'installation et d'administration).
- Laissez le matériel s'acclimater environ une heure s'il a été transporté par temps froid, afin d'éviter toute condensation lors de la mise sous tension.

Chapitre 2 — Installer la sonde

Les étapes suivantes concernent l'assemblage d'un Raspberry Pi 5 avec la carte microSD fournie. Si vous avez reçu le boîtier complet, passez directement au raccordement Ethernet, puis au branchement de l'alimentation. Le montage facultatif d'un SSD NVMe est décrit au guide d'installation et d'administration (SYN-DOC-02).

2.1 Installer le refroidissement

Objectif : assurer une dissipation thermique suffisante pour un fonctionnement permanent.

Prérequis : carte hors tension et hors de son sachet ; précautions ESD appliquées (§ 1.3.1).

Étapes (refroidisseur actif officiel) :

1. Posez la carte sur une surface plane, face supérieure visible.
2. Retirez les films de protection des pastilles thermiques situées sous le refroidisseur.
3. Positionnez le refroidisseur au-dessus de la carte en alignant ses deux tiges de fixation sur les deux trous de montage prévus à cet effet.
4. Enfoncez les tiges de fixation en appuyant **sur les tiges elles-mêmes**, et non sur le corps du refroidisseur, jusqu'au clic.
5. Branchez le câble du ventilateur sur le connecteur marqué « FAN », en respectant le détrompeur.
6. Vérifiez que le câble ne touche pas les pales du ventilateur.

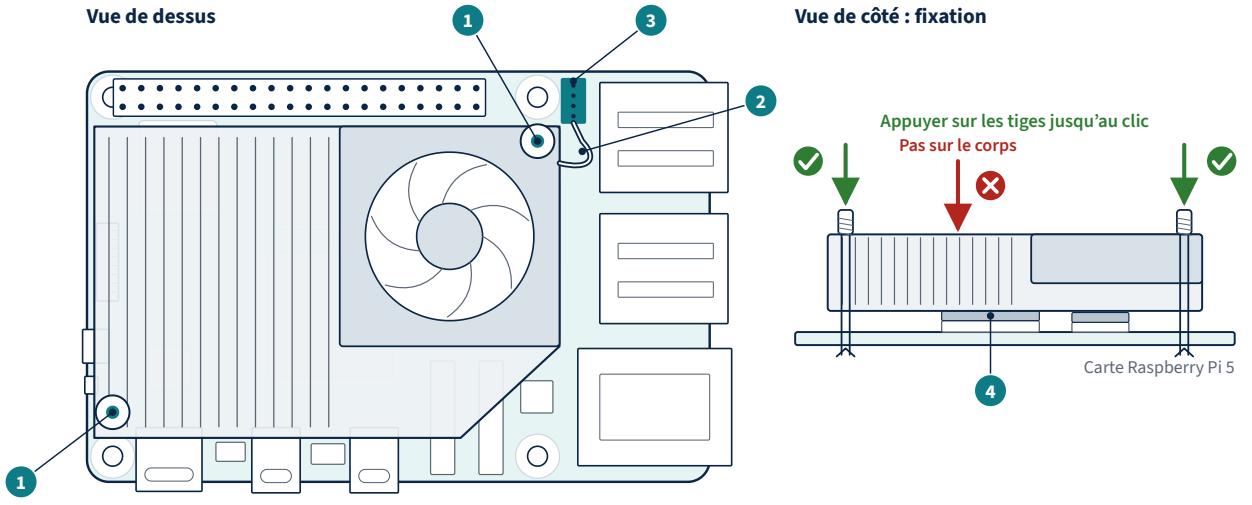


Figure 2-1 — Pose du refroidisseur actif officiel : alignement des tiges de fixation et branchement sur le connecteur FAN

Résultat attendu : le refroidisseur est fermement maintenu, sans jeu ; le câble est branché.

Vérification : la mise en rotation du ventilateur sera observée au premier démarrage. Le ventilateur peut ne pas tourner en permanence : sa vitesse est pilotée selon la température.

Avec un boîtier ventilé : suivez la notice du fabricant ; raccordez son ventilateur au connecteur « FAN » s'il est prévu pour cela.

> **Attention** — Un refroidisseur ne se repose pas : les pastilles thermiques perdent leur efficacité une fois décollées. Ne retirez le refroidisseur qu'en cas de nécessité.

2.2 Installer la carte dans le boîtier

Objectif : protéger la carte et faciliter son installation.

Prérequis : refroidissement installé (§ 2.1) ; si vous avez retenu l'option SSD, carte M.2 HAT+ et SSD déjà montés (§ 3.4.6 du guide d'installation et d'administration).

Étapes :

1. Ouvrez le boîtier selon la notice du fabricant. Suivez aussi ses éventuelles instructions propres au refroidissement (dissipateur fourni avec le boîtier, par exemple), sans les cumuler avec le refroidisseur actif officiel si la notice l'exclut.
2. Placez la carte dans le fond du boîtier en alignant les ports avec les ouvertures correspondantes.
3. Fixez la carte si le boîtier le prévoit (vis ou ergots), sans serrage excessif.
4. Si le boîtier est équipé d'un ventilateur, raccordez-le au connecteur « FAN ».
5. **Ne refermez pas encore le boîtier** s'il masque le lecteur microSD : certains boîtiers exigent l'insertion de la carte avant fermeture. Dans ce cas, réalisez d'abord le § 2.3.
6. Refermez le boîtier.

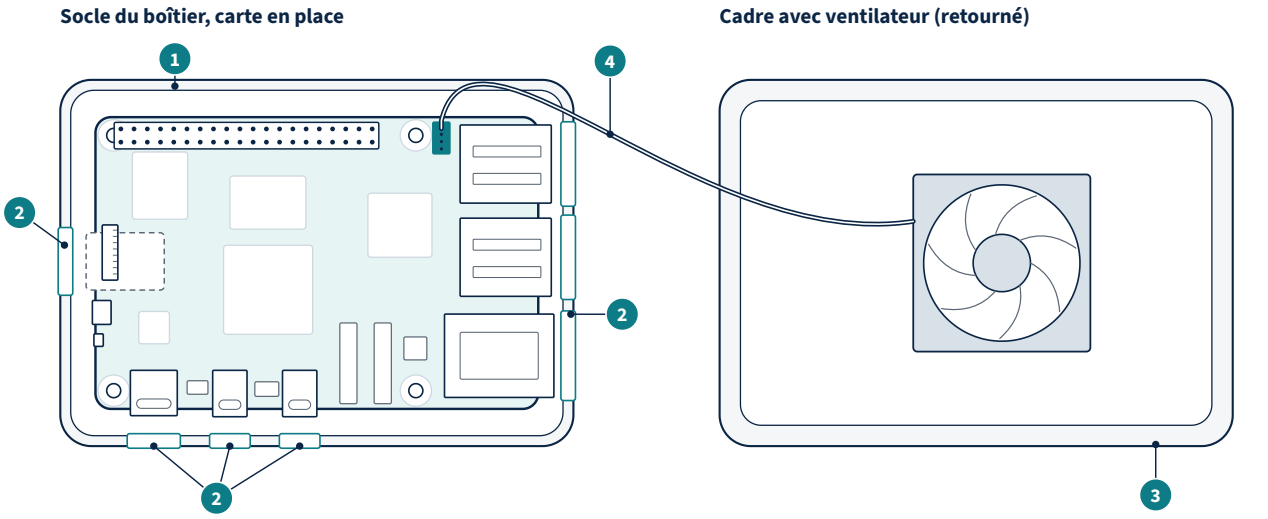


Figure 2-2 — Carte installée dans le boîtier officiel Raspberry Pi 5 : alignement des ports et raccordement du ventilateur

Résultat attendu : la carte est maintenue ; le port USB-C, le port Ethernet et le lecteur microSD restent accessibles.

2.3 Insérer la microSD

Objectif : installer le support contenant le système de la sonde.

Prérequis : carte **hors tension** ; microSD préparée si vous utilisez la méthode A (§ 4.3 du guide d'installation et d'administration).

Étapes :

1. Repérez le lecteur microSD sur la **face inférieure** de la carte, sur le petit côté opposé aux ports Ethernet et USB (figure 3-2 du guide d'installation et d'administration).
2. Tenez la microSD par ses bords, **contacts dorés tournés vers la carte électronique** : lorsque vous regardez la face inférieure de la carte retournée, c'est l'étiquette de la microSD qui est visible.
3. Faites glisser la microSD dans le lecteur, sans forcer, jusqu'à ce qu'elle soit entièrement insérée. Le lecteur du Raspberry Pi 5 n'a pas de mécanisme à ressort : la carte est maintenue par friction.
4. Vérifiez que la carte ne dépasse que légèrement du bord de la carte électronique ou de l'ouverture du boîtier.

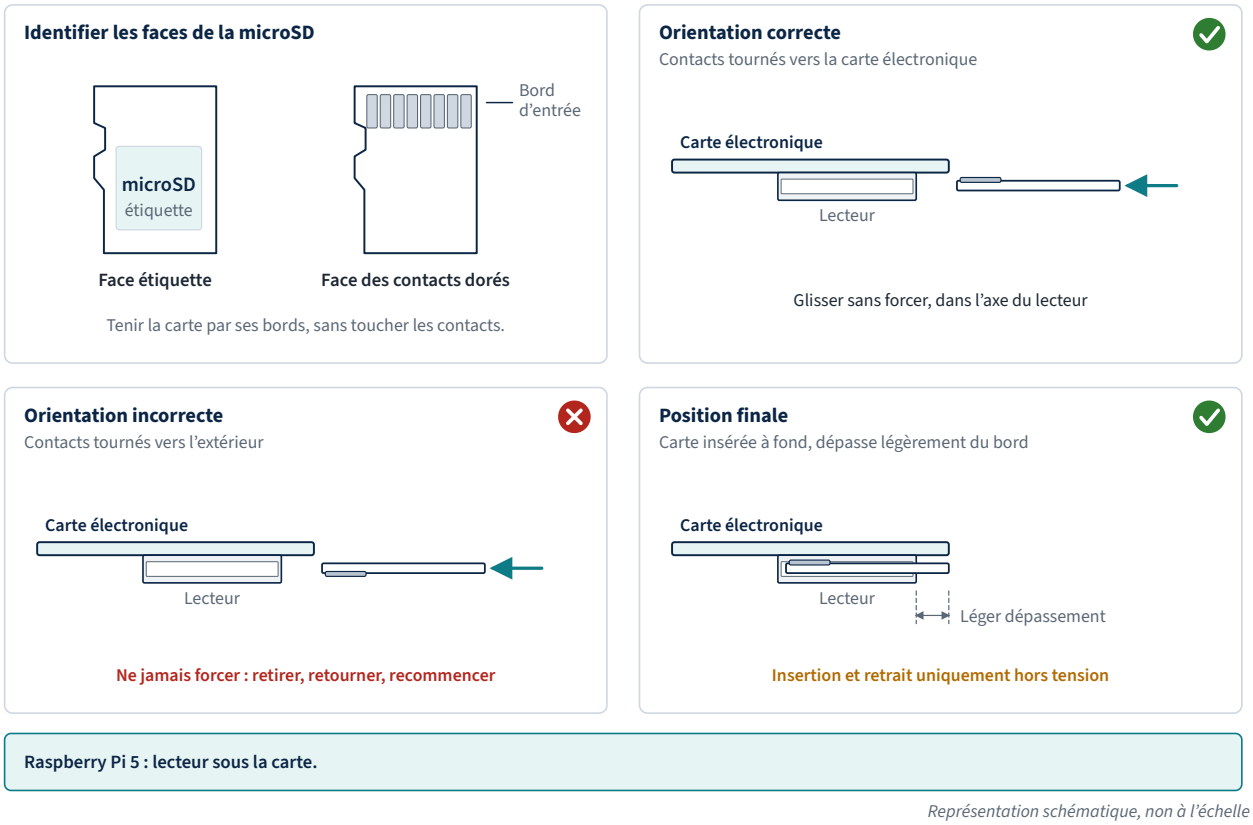


Figure 2-3 — Insertion de la microSD : orientation correcte (contacts vers la carte) et position finale

Résultat attendu : la microSD est insérée à fond et ne bouge pas lorsqu'on effleure son bord.

En cas de problème : si la carte n'entre pas, retirez-la, vérifiez son orientation et recommencez. Ne forcez jamais.

> **Attention** — N'insérez et ne retirez jamais la microSD lorsque la sonde est alimentée. Un retrait à chaud peut corrompre le système de fichiers et rendre la sonde inutilisable.

2.4 Connexion Ethernet

Objectif : raccorder la sonde au réseau choisi pour son implantation (§ 2.5.2 du guide d'installation et d'administration).

Prérequis :

- port de commutateur ou prise murale active, sur le réseau prévu (VLAN de supervision, par exemple, voir § 5.10 du guide d'installation et d'administration) ;
- si le port est protégé par le contrôle d'accès 802.1X, la sonde s'authentifie par certificat (EAP-TLS). Deux possibilités, à arrêter avec l'équipe réseau (§ 2.5.1 et § 5.2.6 du guide d'installation et d'administration) : le fichier PKCS#12 de la sonde et le certificat de l'AC du serveur RADIUS ont été déposés sur la microSD avec le fichier de provisionnement (§ 3.4.2 du guide d'installation et d'administration), ou le port est provisoirement non contrôlé ou autorisé par adresse MAC (MAB) pour la mise en service, 802.1X étant activé ensuite ;
- si la sonde doit obtenir une adresse par DHCP, un serveur DHCP doit être actif sur ce réseau ; sinon, une configuration statique doit être fournie par le fichier de provisionnement (§ 4.3 du guide d'installation et d'administration).

Étapes :

1. Branchez une extrémité du câble Ethernet sur le port RJ45 de la sonde, jusqu'au clic du loquet.
2. Branchez l'autre extrémité sur le port du commutateur ou la prise murale.
3. Ne branchez pas encore l'alimentation.

Résultat attendu : le câble est verrouillé aux deux extrémités.

Vérification : les voyants du port Ethernet de la sonde et du commutateur s'allumeront après la mise sous tension (§ 3.9.2 du guide d'installation et d'administration).

> **Information** — La sonde fonctionne exclusivement en Ethernet. Le Wi-Fi et le Bluetooth intégrés au Raspberry Pi 5 sont désactivés dans le système de la sonde, par une surcouche de l'arbre des périphériques (*device tree overlay*).

> **Évolution prévue** — La prise en charge du Wi-Fi est envisagée dans une version ultérieure.

2.5 Branchement de l'alimentation et démarrage

Objectif : mettre la sonde sous tension dans de bonnes conditions.

Prérequis : microSD insérée ; boîtier fermé ; câble Ethernet branché ; méthode de mise en service choisie (chapitre 3).

Étapes :

1. Branchez l'alimentation sur la prise secteur (de préférence secourue).
2. Branchez le connecteur USB-C sur le port d'alimentation de la sonde. **L'alimentation doit être branchée en dernier.**
3. La sonde démarre automatiquement dès qu'elle est alimentée. Il n'est normalement pas nécessaire d'appuyer sur le bouton d'alimentation.
4. Ne débranchez pas la sonde pendant le premier démarrage, qui comporte des opérations d'initialisation (extension du système de fichiers, génération des clés de sécurité). Sa durée est indiquée au § 4.2 du guide d'installation et d'administration.

Résultat attendu : le voyant d'état s'allume, puis traduit l'activité du système (§ 2.6).

> **Attention** — Ne coupez jamais l'alimentation d'une sonde en fonctionnement en débranchant le câble, sauf en dernier recours. Utilisez la procédure d'arrêt propre décrite au chapitre 8 du guide d'installation et d'administration. Une coupure brutale peut provoquer une perte des dernières données et, de manière répétée, une corruption de la microSD.

> **Information** — Si l'alimentation utilisée ne fournit pas le courant attendu par le Raspberry Pi 5 (alimentation 5 V / 3 A, par exemple), la carte peut fonctionner avec un courant USB limité. La sonde surveille les situations de sous-tension et les signale dans ses indicateurs de santé (chapitre 7 du guide d'utilisation et de supervision et chapitre 9 du guide d'installation et d'administration).

2.6 Voyant d'état

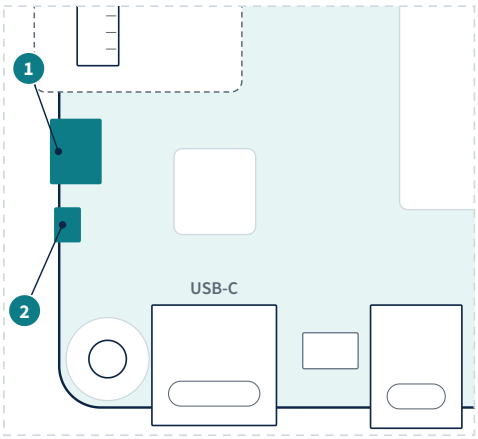
Le Raspberry Pi 5 dispose d'un voyant d'état unique, bicolore. D'après la documentation du fabricant, sa couleur indique l'état d'alimentation de la carte :

Observation	Signification (comportement général du Raspberry Pi 5)	Action
Aucun voyant allumé	Cause probable : la carte n'est pas alimentée (à recouper avec l'écran HDMI éventuel et les voyants Ethernet, encadré ci-dessous)	Vérifier l'alimentation, le câble et la prise (§ 5.1)
Rouge fixe	La carte est alimentée mais le système est arrêté ou en veille	Appuyer brièvement sur le bouton d'alimentation pour démarrer ; si la situation persiste, voir § 5.1
Vert, clignotant de façon irrégulière	Le système fonctionne ; le clignotement traduit l'activité de lecture et d'écriture	Situation normale
Clignotements répétitifs selon un motif régulier (séquences de flashs longs et courts)	Code d'erreur du chargeur d'amorçage, documenté par Raspberry Pi (par exemple, microSD illisible ou système introuvable)	Noter le motif, consulter la documentation Raspberry Pi et le chapitre 9 du guide d'installation et d'administration

La sonde ne définit aucune signalisation propre : le voyant ne présente que les comportements standard du Raspberry Pi 5 décrits ci-dessus. En particulier, il n'indique ni la fin de l'initialisation ni l'état de configuration de la sonde ; ces informations se vérifient sur l'écran HDMI éventuel ou par le réseau (chapitre 3).

> **Information** — Les couleurs et clignotements du voyant sont des **indices matériels** : leur comportement exact dépend du microprogramme (*firmware*) du Raspberry Pi 5, de sa configuration et de l'étape du démarrage. Un voyant vert actif signale une activité de lecture et d'écriture sur le support de stockage ; il ne confirme ni que le logiciel de la sonde fonctionne, ni qu'il est correctement configuré. Pour établir l'état de la sonde, recoupez toujours le voyant avec la console de l'écran HDMI éventuellement raccordé (adresse IP, empreinte du certificat, état de la mise en service) et, dès que la sonde est joignable, avec l'adresse `/health` (§ 4.2).

Gros plan (vue de dessus)



Indices matériels uniquement
Le voyant n'indique ni la fin de l'initialisation ni l'état de configuration de la sonde. Recoupez-le avec l'écran HDMI éventuel et l'adresse /health (§ 4.2).

Repères

1. Bouton d'alimentation : sonde arrêtée, un appui la démarre ; sonde en fonctionnement, un appui bref déclenche l'arrêt propre, un appui long force la coupure
2. Voyant d'état, unique et bicolore

Observation du voyant (comportement général du Raspberry Pi 5)

○	**Aucun voyant allumé** Cause probable : carte non alimentée
●	**Rouge fixe** Carte alimentée, système arrêté ou en veille
● ⟋	**Vert, clignotement irrégulier** Système en fonctionnement (activité de lecture et d'écriture)
▬ ▬ ▮ ▮	**Motif régulier de flashs longs et courts** Code d'erreur du chargeur d'amorçage (ex. microSD illisible)

Représentation schématique, non à l'échelle

Figure 2-4 — Emplacement du voyant d'état et du bouton d'alimentation du Raspberry Pi 5

2.7 Liste de vérification de fin d'installation physique

Point de contrôle	Vérifié
Matériel conforme à l'édition (RAM, refroidissement)	[ ]
Refroidissement installé et raccordé	[ ]
microSD insérée à fond, sonde hors tension lors de l'insertion	[ ]
Emplacement ventilé, sécurisé, alimentation secourue si possible	[ ]
Câble Ethernet verrouillé, voyants de liaison allumés	[ ]
Alimentation branchée en dernier	[ ]
Voyant d'état vert avec activité	[ ]
Adresse MAC et numéro de série relevés	[ ]
Si SSD prévu : carte M.2 HAT+ et SSD montés, nappe verrouillée, alimentation de 27 W utilisée (§ 3.4.6 du guide d'installation et d'administration)	[ ]

L'installation physique est terminée. Poursuivez avec la mise en service au chapitre 3.

Chapitre 3 — Mettre en service la sonde

La sonde a démarré. Vous allez maintenant la configurer depuis un navigateur web, avec l'assistant de mise en service : création du compte administrateur, réseau, heure et premiers paramètres.

3.1 Mise en service par l'assistant web (méthode B)

La méthode B, décrite dans cette section, consiste à configurer la sonde après son démarrage, dans un assistant web protégé par le code d'installation. La méthode A désigne l'autre parcours : le provisionnement par fichier, décrit au § 4.3 du guide d'installation et d'administration, où un fichier `provision.yaml` déposé sur la microSD configure la sonde dès son premier démarrage.

3.1.1 Prérequis

- Sonde installée et démarrée (chapitre 2), sans fichier de provisionnement.
- Serveur DHCP actif sur le réseau de la sonde.
- Port de commutateur sans authentification 802.1X, ou autorisé par adresse MAC (MAB, *MAC Authentication Bypass*) : l'assistant ne permet pas de fournir un identifiant 802.1X. Sur un port contrôlé, utilisez la méthode A, ou activez 802.1X après la mise en service (chapitre 5 du guide d'installation et d'administration).
- Poste d'administration sur un réseau autorisé à joindre la sonde en HTTPS (port TCP 443), équipé d'un navigateur récent.
- Accès au code d'installation (§ 3.1.3).
- Paramètres à saisir : nom d'hôte et site souhaités, serveurs DNS et NTP, proxy éventuel ; l'adresse IP définitive est obtenue par une réservation DHCP, et non saisie dans l'assistant.

3.1.2 Trouver l'adresse IP de la sonde

La sonde obtient son adresse du serveur DHCP. Plusieurs moyens permettent de la retrouver.

> **Avertissement** — N'utilisez pas d'outil de balayage réseau (*scan*) sans l'accord de votre équipe sécurité : ce type d'outil peut déclencher des alertes de détection d'intrusion.

Moyen	Procédure	Remarque
Table des baux DHCP	Rechercher, dans la console du serveur DHCP, le bail associé à l'**adresse MAC** de la sonde (étiquette du boîtier complet) ou au nom d'hôte `sva-XXXXXX`	Méthode la plus fiable
Réservation DHCP préalable	Créer avant le démarrage une réservation associant l'adresse MAC à une adresse choisie	Recommandé : l'adresse ne changera pas
Nom mDNS	Saisir `https://sva-XXXXXX.local/` dans le navigateur, `XXXXXX` correspondant aux six derniers caractères hexadécimaux de l'adresse MAC	Annonce mDNS active par défaut, désactivable dans la section `network` des paramètres. Fonctionne uniquement si le poste est sur le même segment réseau et si mDNS n'est pas filtré

Moyen	Procédure	Remarque
Écran HDMI	Brancher un écran sur un port micro-HDMI : la console locale affiche l'adresse IP, le nom mDNS, l'empreinte du certificat et, tant que la sonde n'est pas initialisée, le code d'installation	Utile en l'absence d'accès au serveur DHCP
Table des adresses MAC du commutateur, table ARP du routeur	Rechercher l'adresse MAC sur le port de raccordement, puis l'adresse IP associée	Nécessite l'équipe réseau

> **Information** — mDNS (*multicast DNS*) est un mécanisme de résolution de noms sans serveur, limité au réseau local. Les noms se terminent par `.local`. Il est souvent filtré entre VLAN.

3.1.3 Obtenir le code d'installation

Le code d'installation est un code propre à la carte, qui protège l'assistant : il est généré lors de la préparation de la carte et imprimé sur l'encart ou l'étiquette qui accompagne le produit. Il empêche qu'une autre personne présente sur le réseau ne s'approprie la sonde avant vous. Il devient invalide dès la fin de l'assistant.

Offre	Où trouver le code
Boîtier complet	Étiquette d'identification du boîtier (§ 3.5.3 du guide d'installation et d'administration)
microSD préconfigurée	Encart d'identification qui accompagne la carte (§ 3.3.3 du guide d'installation et d'administration)
Secours (les deux offres)	Écran branché en micro-HDMI au démarrage (console locale, avec l'empreinte du certificat), ou fichier `setup-code.txt` de la partition `SVA-BOOT`. Ce fichier contient aussi l'empreinte SHA-256 du certificat de la sonde, utile au § 3.1.4 ; il est réécrit à chaque démarrage avec l'empreinte courante (§ 4.2 du guide d'installation et d'administration)

Si vous ne disposez plus de l'encart ou de l'étiquette, lisez `setup-code.txt` sans écran :

1. Laissez la sonde terminer son premier démarrage (§ 4.2 du guide d'installation et d'administration).
2. Arrêtez-la proprement. Si l'interface n'est pas encore accessible, un appui bref sur le bouton d'alimentation déclenche l'arrêt propre (comportement standard de Raspberry Pi OS sur Raspberry Pi 5 ; un appui long force la coupure et doit être évité) ; attendez que le voyant passe au rouge fixe.
3. Débranchez l'alimentation, retirez la microSD et lisez le fichier `setup-code.txt` sur votre poste.
4. Réinsérez la microSD et redémarrez la sonde.

Le code d'installation reste valide d'un démarrage à l'autre tant que la sonde n'est pas initialisée : le code relevé reste donc valide après ce redémarrage. Il est invalidé à la fin de l'assistant, puis redevient valide après une réinitialisation usine (§ 8.10 du guide d'installation et d'administration). Il est aussi exigé, avec le code de récupération, par la procédure de récupération du compte administrateur (§ 3.1.6) : conservez l'encart ou l'étiquette pendant toute la vie du produit.

> **Avertissement** — Traitez le code d'installation comme un mot de passe. Toute personne qui le détient, et qui peut joindre la sonde sur le réseau, peut en prendre le contrôle tant que la mise en service n'est pas terminée. Effectuez la mise en service sans délai après le premier démarrage.

3.1.4 Se connecter et vérifier le certificat

La sonde présente un **certificat TLS autosigné**, généré à son premier démarrage. Un certificat autosigné n'est pas émis par une autorité de certification reconnue par votre navigateur : celui-ci affiche donc un avertissement de sécurité. Cet avertissement est attendu lors de la mise en service. Il ne doit cependant être accepté qu'après vérification de l'**empreinte** du certificat, qui garantit que vous êtes bien connecté à votre sonde et non à un équipement intercalé.

Cette section est la procédure de référence de la vérification d'empreinte, quel que soit le parcours de mise en service (méthode A ou B) et quel que soit l'outil utilisé ensuite (navigateur, `curl`, Prometheus, Nagios). Les autres sections de la documentation y renvoient.

Objectif : établir une connexion chiffrée et authentifiée avec la sonde.

Prérequis : l'empreinte SHA-256 courante du certificat, relevée par un canal indépendant du réseau (tableau ci-dessous).

Étapes :

1. Saisissez dans le navigateur `https://<adresse-ip-de-la-sonde>/` (exemple : `https://192.0.2.50/`).
2. Le navigateur signale que le certificat n'est pas reconnu. N'acceptez pas encore.
3. Affichez le détail du certificat (icône à gauche de la barre d'adresse, puis détail du certificat ; le libellé varie selon le navigateur). Relevez son **empreinte SHA-256**.
4. Comparez cette empreinte avec celle communiquée par la sonde par un canal indépendant du réseau : écran HDMI ou fichier `setup-code.txt` de la partition `SVA-BOOT` (§ 3.1.3). Seule cette comparaison hors réseau protège contre une interception : l'empreinte affichée ensuite par l'assistant ou par l'interface transite par la même connexion que celle que vous cherchez à vérifier.
5. Si les empreintes concordent, acceptez l'exception de sécurité pour cette adresse.
6. Si elles diffèrent, **interrompez la procédure** et contactez votre équipe sécurité : une interception de la connexion est possible.

> **Attention** — La vérification de l'empreinte est **obligatoire avant toute saisie d'identifiants** (code d'installation, compte administrateur) **et avant toute transmission d'un jeton d'API**. Elle se refait chaque fois que le certificat change (changement de nom ou d'adresse, renouvellement, réinitialisation usine), avec l'empreinte **courante** : une empreinte relevée avant un redémarrage ou un changement de certificat n'est plus une référence sûre.

Canal indépendant du réseau selon le parcours. L'empreinte courante est réécrite dans `setup-code.txt` à chaque démarrage et affichée sur la console HDMI (§ 4.2 du guide d'installation et d'administration).

Parcours	Canal indépendant du réseau disponible
Provisionnement sans écran (méthode A)	Fichier `setup-code.txt`, lu en retirant la microSD après le premier démarrage (§ 3.1.3)
Assistant web (méthode B)	Console de l'écran HDMI, ou fichier `setup-code.txt` (§ 3.1.3)
Certificat émis par l'AC de votre entreprise (§ 5.7.2 du guide d'installation et d'administration)	La chaîne de certification de votre entreprise, vérifiée par le navigateur ou par `curl` : aucune exception de sécurité n'est alors nécessaire
Après régénération ou renouvellement du certificat autosigné	Empreinte reçue par une connexion déjà vérifiée (§ 5.2.3 du guide d'installation et d'administration) ; à défaut, console HDMI ou fichier `setup-code.txt`

Vérification en ligne de commande. Pour interroger la sonde avec `curl` ou un outil de supervision **sans désactiver la vérification TLS**, ces outils ont besoin du certificat de la sonde au format PEM. Récupérez-le, soit en l'exportant depuis votre navigateur après la vérification ci-dessus, soit par l'adresse `GET /api/v1/system/certificate`, puis vérifiez son empreinte avant de l'enregistrer, par exemple sous le nom `sonde-paris-01.pem` :

```bash
# Récupérer le certificat puis afficher son empreinte SHA-256 pour la comparer à celle de setup-
    code.txt
curl --insecure --silent https://192.0.2.50/api/v1/system/certificate -o sonde-paris-01.pem
openssl x509 -in sonde-paris-01.pem -noout -fingerprint -sha256
```

L'option `--insecure` n'est admise ici que pour ce téléchargement unique, effectué sans jeton et suivi obligatoirement de la comparaison d'empreinte. Supprimez le fichier si les empreintes diffèrent. Une alternative consiste à afficher l'empreinte du certificat présenté par le serveur avec OpenSSL :

```bash
# Afficher l'empreinte SHA-256 du certificat présenté par la sonde
openssl s_client -connect 192.0.2.50:443 </dev/null 2>/dev/null \
  | openssl x509 -noout -fingerprint -sha256
```

L'empreinte affichée doit être identique à celle relevée par le canal indépendant du réseau.

> **Information** — Le certificat autosigné couvre, dans son extension *Subject Alternative Name*, le nom d'hôte, le nom mDNS et l'adresse IPv4 de la sonde, ainsi que son adresse IPv6 statique lorsqu'elle est configurée. Si l'un de ces éléments change et qu'aucun certificat importé n'est en place, la sonde régénère son certificat : le fichier PEM enregistré n'est plus valable. Récupérez-le et vérifiez-le de nouveau comme ci-dessus.

> **Conseil** — À l'issue de la mise en service, il est recommandé de remplacer le certificat autosigné par un certificat émis par l'autorité de certification interne de votre organisation. Les navigateurs et outils de votre parc le reconnaîtront alors sans exception de sécurité (§ 5.7 du guide d'installation et d'administration).

3.1.5 Parcourir l'assistant

L'assistant comporte les étapes suivantes, dans cet ordre. Les intitulés du tableau décrivent le contenu de chaque étape ; ils ne reproduisent pas nécessairement les libellés des écrans.

Étape	Contenu	Remarques
1. Code d'installation	Saisie du code (§ 3.1.3)	Après 5 saisies erronées, la saisie est bloquée pendant 15 minutes ; cette durée double à chaque nouvelle série d'échecs. Chaque échec est journalisé
2. Édition	Affichage de l'édition inscrite sur la carte (Essential, Professional, Enterprise) ; aucune saisie	Voir § 4.5 du guide d'installation et d'administration
3. Compte administrateur	Identifiant et mot de passe du premier administrateur	Mot de passe de 12 à 128 caractères, sans règle de composition ni expiration périodique
4. Réseau	Nom d'hôte, site, mode DHCP ou statique, adresse, passerelle, DNS ; activation facultative de l'IPv6 (désactivé par défaut), en mode SLAAC ou statique (adresse IPv6, passerelle IPv6)	Ne changez pas l'adresse IP dans l'assistant ; utilisez une réservation DHCP (§ 5.2.1 du guide d'installation et d'administration). Un changement d'adresse ou de nom d'hôte impose une réauthentification à la nouvelle adresse dans les 120 secondes (procédure après le tableau). L'IPv4 reste toujours actif ; les serveurs DNS peuvent être IPv4 ou IPv6

Étape	Contenu	Remarques
5. Heure	Serveurs NTP, fuseau horaire d'affichage	La sonde vérifie la synchronisation (§ 5.4 du guide d'installation et d'administration)
6. Proxy	Proxy sortant éventuel et exclusions	Facultatif
7. Certificat	Affichage de l'empreinte SHA-256 ; option d'import d'un certificat de votre AC	L'import peut être réalisé plus tard (§ 5.7 du guide d'installation et d'administration)
8. Destinations d'export	Configuration facultative d'une première destination (Prometheus, OTLP…)	Peut être reportée au chapitre 2 du guide d'intégration et d'observabilité
9. Mises à jour	Choix du mode de chaque canal (correctifs de sécurité : `automatic` ou `manual` ; versions fonctionnelles : `manual` ou `automatic`), politique des correctifs critiques, puis définition d'**au moins une fenêtre de maintenance** (jours, heure de début, durée), ou choix explicite du **mode manuel** (chaque activation est alors décidée par un administrateur) ; préavis et délai de drainage	**Aucune fenêtre n'est proposée par défaut** : l'étape ne peut être validée sans un choix explicite. Sans fenêtre, aucune mise à jour n'est activée automatiquement et l'état de santé `updates` reste en `WARNING` (chapitre 8 du guide d'installation et d'administration)
10. Récapitulatif	Relecture et validation	Le code d'installation est invalidé à la validation
11. Code de récupération	Affichage **unique** du code de récupération du compte administrateur	À enregistrer immédiatement dans le coffre-fort de l'organisation (§ 3.1.6) ; il ne pourra plus être affiché

Résultat attendu : la sonde affiche la page d'accueil de l'interface d'administration ; vous êtes connecté avec le compte administrateur créé.

> ! **Attention** — Ne changez pas l'adresse IP dans l'assistant ; utilisez une réservation DHCP (§ 5.2.1 du guide d'installation et d'administration). Si un changement d'adresse ou de nom d'hôte est indispensable à l'étape 4, vous devez vous réauthentifier à la nouvelle adresse dans les **120 secondes**, faute de quoi la sonde revient automatiquement à la configuration précédente : suivez la procédure ci-dessous.

Changement d'adresse ou de nom d'hôte à l'étape 4 (déconseillé). Après validation de l'étape 4, la sonde devient joignable à sa nouvelle adresse. La session d'administration est liée à l'adresse d'origine (cookie de session et protection contre la falsification de requêtes, CSRF) : à la nouvelle adresse, le navigateur ouvre une **nouvelle session**, et la confirmation n'est émise qu'après votre réauthentification. L'interface émet alors pour vous la confirmation `POST /api/v1/settings/network/confirm` décrite au § 5.2.3 du guide d'installation et d'administration. Procédez ainsi :

1. Dans les 120 secondes, ouvrez la nouvelle adresse. Pendant ce délai, la sonde présente encore l'**ancien certificat**, celui dont vous avez vérifié l'empreinte au § 3.1.4 : le navigateur affiche la **même empreinte**, que vous reconnaissez avant d'accepter l'exception pour cette adresse.
2. Authentifiez-vous de nouveau : la confirmation est alors émise.
3. Lorsque le nom d'hôte ou l'adresse change, le certificat autosigné est régénéré pour les inclure, et son empreinte change. Après la confirmation, l'assistant affiche l'empreinte SHA-256 du nouveau certificat, reçue par la connexion déjà vérifiée, qui en fait une source de confiance ; le nouveau certificat est mis en service 30 secondes plus tard. Relevez cette empreinte.
4. Après la bascule, comparez l'empreinte présentée par le navigateur à celle relevée à l'étape 3, avant d'accepter l'exception. Aucune vérification hors réseau n'est nécessaire dans ce délai.

Sans confirmation, la sonde revient d'elle-même à la configuration précédente au bout de 120 secondes. La nouvelle empreinte s'affiche aussi sur la console HDMI, figure dans le journal d'audit et est écrite dans le fichier `setup-code.txt` de la partition `SVA-BOOT` au plus tard au démarrage suivant ; jusqu'à ce démarrage, ce fichier peut donc encore contenir l'empreinte précédente. Si la politique de votre navigateur interdit l'exception de sécurité, si la réponse de confirmation est perdue ou si vous ne savez pas si la confirmation a été enregistrée, appliquez les recours du § 5.2.3 du guide d'installation et d'administration. Un certificat émis par l'AC de votre entreprise ne dispense de l'exception que s'il couvre le nom ou l'adresse que vous utilisez pour joindre la sonde après le changement (§ 5.7.2 du guide d'installation et d'administration).

3.1.6 Conserver le code de récupération du compte administrateur

Le **code de récupération** permet de redéfinir le mot de passe d'un compte administrateur si plus aucun administrateur ne peut se connecter, sans perdre la configuration de la sonde. Il comporte 24 caractères et est généré à la fin de la mise en service, quelle que soit la méthode :

- méthode B : il est affiché à la dernière étape de l'assistant (§ 3.1.5) ;
- méthode A : il est affiché à la première connexion à l'interface d'administration d'une sonde provisionnée.

La sonde ne conserve qu'une empreinte Argon2id de ce code (§ 4.3.4 du guide d'installation et d'administration) : elle ne peut donc plus jamais l'afficher. La procédure de récupération exige à la fois un accès physique à la carte microSD, le code d'installation imprimé (§ 3.1.3) et ce code de récupération. Elle est décrite au § 8.10 du guide d'installation et d'administration.

Objectif : conserver le code de récupération de façon sûre et durable.

Prérequis : accès en écriture au coffre-fort de mots de passe de votre organisation, ouvert sur le poste d'administration avant la fin de la mise en service.

Étapes :

1. Lorsque le code de récupération s'affiche, ne quittez pas l'écran.
2. Enregistrez le code dans le coffre-fort de votre organisation, dans une entrée qui identifie la sonde (nom d'hôte, numéro de série).
3. Relisez l'entrée enregistrée et comparez-la au code affiché, caractère par caractère.
4. Quittez l'écran seulement ensuite.

Résultat attendu : le code de récupération est enregistré dans le coffre-fort et nulle part ailleurs.

Vérification : l'entrée du coffre-fort contient un code de 24 caractères, rattaché à la bonne sonde.

Erreurs possibles :

Situation	Conséquence	Action
Écran fermé avant l'enregistrement du code	Le code ne peut plus être affiché	Un administrateur génère un nouveau code depuis l'interface ou par `POST /api/v1/system/recovery-code` (rôle `admin`, saisie de son mot de passe exigée) : le nouveau code s'affiche une seule fois et l'ancien est invalidé. Tant qu'aucun code n'est disponible, la perte du dernier compte administrateur n'est réparable que par une réinitialisation usine (§ 8.10 du guide d'installation et d'administration)
Code consommé par une récupération	Un nouveau code est affiché à l'issue de la récupération	Remplacer l'ancien code par le nouveau dans le coffre-fort

> **Avertissement** — Le code de récupération donne, avec le code d'installation et un accès physique à la carte, le contrôle d'un compte administrateur. Ne le conservez ni sur l'encart du produit, ni sur la sonde, ni dans un courriel. Ne le transmettez jamais au support de l'éditeur.

Chapitre 4 — Vérifier la sonde et créer un premier contrôle

Une fois la mise en service terminée, vérifiez l'état de la sonde, puis créez un premier contrôle depuis l'interface d'administration et contrôlez que ses résultats remontent. La création d'un contrôle par l'API, destinée à l'automatisation, est décrite au § 4.7.2 du guide d'installation et d'administration.

4.1 Consulter l'état depuis l'interface d'administration

La page d'accueil de l'interface présente l'état de santé de la sonde : version, édition, durée de fonctionnement, état des moteurs, utilisation des ressources, synchronisation horaire, état des destinations d'export.

Les mêmes informations sont disponibles par l'API, avec la ressource `GET /api/v1/system` (§ 4.6.3 du guide d'installation et d'administration).

4.2 Vérifier la vivacité avec `/health`

L'adresse `/health` répond sans authentification et indique uniquement si la sonde est en fonctionnement. Elle ne révèle aucune information sensible. Elle convient à une vérification rapide ou à une supervision de premier niveau.

La commande suivante utilise le fichier `sonde-paris-01.pem`, récupéré et vérifié selon le § 3.1.4 (vérification en ligne de commande) :

```bash
# Vérifier la vivacité de la sonde (exemple fictif)
# --cacert : fait confiance au certificat exporté de la sonde, et à lui seul
curl --cacert sonde-paris-01.pem https://192.0.2.50/health
```

Résultat attendu : un code HTTP `200`. La réponse est `{"status": "OK"}`.

> **Avertissement** — L'option `-k` (ou `--insecure`) de `curl` désactive toute vérification du certificat : elle expose vos jetons d'API à une interception. Ne l'utilisez pas, même pour un test ponctuel, en dehors du téléchargement initial du certificat décrit au § 3.1.4.

4.3 Créer le contrôle depuis l'interface d'administration

Étapes :

1. Ouvrez la gestion des contrôles et créez un contrôle de type **HTTP**.
2. Renseignez :
   - identifiant : `intranet-accueil` ;
   - nom : « Intranet : page d'accueil » ;
   - URL : `https://intranet.example.internal/` ;
   - fréquence : 5 minutes ;
   - délai maximal (*timeout*) : 10 secondes ;

- vérification : code de réponse égal à 200.

3. Enregistrez puis déclenchez une exécution immédiate.
4. Ouvrez le détail de l'exécution.

Le détail de l'exécution indique l'état du contrôle, sa durée et les phases de la requête. La même opération par l'API est décrite au § 4.7.2 du guide d'installation et d'administration.

4.4 Vérifier la remontée des résultats

Les résultats sont conservés **localement** par la sonde, qui fonctionne de manière autonome : aucune plateforme externe n'est nécessaire pour les consulter.

Vérification	Méthode	Résultat attendu
Historique local	Interface : historique du contrôle ; API : `GET /api/v1/runs?checkId=intranet-accueil`	Les exécutions planifiées apparaissent toutes les 5 minutes
Destination d'export (si configurée)	Interface : état des destinations ; API : `POST /api/v1/exporters/{id}/test`	Envoi de test réussi
Métriques Prometheus (si utilisé)	Collecte de `/metrics` par votre serveur Prometheus	La série de l'état du contrôle est présente (chapitre 2 du guide d'intégration et d'observabilité)

La configuration des destinations d'export (Prometheus, Grafana, Datadog, Dynatrace, Nagios/Centreon) est décrite au chapitre 2 du guide d'intégration et d'observabilité ; l'interprétation des résultats, au chapitre 7 du guide d'utilisation et de supervision.

> ✓ **Conseil** — Une fois le premier contrôle validé, révoquez (supprimez) les jetons `viewer` et `operator` créés pour ces vérifications, ou créez-les dès le départ avec une date d'expiration (`expiresAt`) (§ 6.5 du guide d'installation et d'administration).

Chapitre 5 — En cas de difficulté

5.1 Erreurs fréquentes lors de l'installation

Symptôme	Causes possibles	Vérifications et actions
Aucun voyant	Alimentation non branchée ou défectueuse ; prise sans courant	Tester la prise avec un autre appareil ; essayer une autre alimentation conforme
Voyant rouge fixe, pas de démarrage	Système arrêté ; alimentation insuffisante	Appui bref sur le bouton d'alimentation ; utiliser l'alimentation recommandée (§ 1.2)
Motif de clignotement répétitif	microSD absente, mal insérée, endommagée ou ne contenant pas l'image de la sonde	Mettre hors tension, réinsérer la microSD à fond ; vérifier qu'il s'agit bien de la carte fournie ; voir chapitre 9 du guide d'installation et d'administration
Voyant vert actif mais pas de voyant Ethernet	Câble non verrouillé ou défectueux ; port de commutateur inactif	Changer de câble ; tester un autre port ; vérifier la configuration du port avec l'équipe réseau
Ventilateur bruyant en permanence	Température élevée ; emplacement mal ventilé	Améliorer la ventilation ; vérifier l'absence de source de chaleur proche
La sonde redémarre de façon répétée	Alimentation insuffisante ; microSD défectueuse	Utiliser l'alimentation recommandée ; contacter le support si le problème persiste
Voyant de liaison Ethernet allumé, mais la sonde n'obtient pas d'adresse, sur un port protégé par 802.1X	Authentification 802.1X refusée, ou sonde sans identifiant client	Consulter l'état affiché sur l'écran HDMI éventuel et le journal du serveur RADIUS ; voir § 5.2.6 du guide d'installation et d'administration et chapitre 9 du guide d'installation et d'administration
Aucun démarrage, avec ou sans message sur l'écran HDMI, sur une carte autre qu'un Raspberry Pi 5	Modèle de carte non pris en charge (Raspberry Pi 4, Raspberry Pi 400, Compute Module, Orange Pi…)	Le système vérifie le modèle au tout début du démarrage, avant tout montage en écriture et avant l'extension de la partition ; s'il a pu démarrer, il s'arrête sans monter de partition en écriture et affiche un message sur l'écran HDMI. Si le microprogramme de la carte ne charge pas l'image, aucun composant de la sonde ne s'exécute et aucun message ne peut s'afficher. Dans les deux cas, le contrôle vise à préserver la microSD, sans que sa conservation puisse être garantie lorsque le microprogramme d'une autre carte a manipulé le support (§ 2.1.1 du guide d'installation et d'administration). Mettez hors tension et installez la carte dans un Raspberry Pi 5 (§ 2.1.1 du guide d'installation et d'administration).
La microSD a été « formatée » par un ordinateur	Acceptation d'une proposition de formatage du système d'exploitation du poste	Le formatage a effacé le système et le certificat d'édition, qui ne peut pas être réinscrit par vos soins : la carte doit être remplacée. Contactez le support avec le numéro de série du produit (§ 8.6.4 du guide d'installation et d'administration)

Le diagnostic détaillé de ces situations est traité au chapitre 9 du guide d'installation et d'administration.

Chapitre 6 — Documentation et assistance

Votre sonde est en service. Pour aller plus loin, consultez le guide qui correspond à votre rôle (page « La bibliothèque documentaire SYNOVEX », au début de ce guide) ou le manuel technique complet.

6.1 Assistance et contacts

Rubrique	Information
Service, adresse électronique, téléphone, horaires et langues du support	Indiqués dans votre contrat ; le portail de support (voir ce tableau) centralise les demandes dès sa mise en service
Site commercial	`https://synovex.incitypark.fr`
Portail de support	`https://support-synovex.incitypark.fr`, après l'annonce de sa mise en service (encadré ci-dessous)
Niveaux de service	Délais de prise en charge définis par votre contrat, par niveau de gravité (§ 6.1.1) et par édition
Garantie et remplacement de carte	Durée, conditions et procédure de retour selon vos conditions de vente ; procédure technique de remplacement : § 8.6.4 du guide d'installation et d'administration
Documentation en ligne et notes de version	`https://docs-synovex.incitypark.fr`, après l'annonce de sa mise en service (encadré ci-dessous)
Distribution des mises à jour	`https://updates-synovex.incitypark.fr` (utilisée par la sonde pour les mises à jour en ligne, après l'annonce de sa mise en service ; images signées)
Console de gestion centralisée	`https://fleet-synovex.incitypark.fr` : adresse réservée à la console centrale prévue ; non utilisée par la sonde
Signalement d'une vulnérabilité de sécurité	Canal dédié indiqué dans votre contrat, distinct des canaux ordinaires du support ; voir § 6.1.4
Service commercial (changement d'édition, reprise, remplacement de carte)	Coordonnées indiquées dans votre contrat ou votre bon de commande ; site commercial ci-dessus

> **Information** — Ces adresses constituent le plan de nommage officiel de l'éditeur ; les services correspondants sont mis en service progressivement. Une procédure qui s'appuie sur l'un de ces services (portail de support, documentation en ligne, téléchargement d'une image) ne s'applique qu'après l'annonce de sa mise en service par l'éditeur. Avant cette annonce, ou si un service ne répond pas, utilisez le canal de contact et de mise à disposition des images convenu dans votre contrat.

6.1.1 Niveaux de gravité proposés

Gravité	Définition	Exemple
1 — Bloquant	Sonde hors service, aucune supervision assurée	La sonde ne démarre plus
2 — Majeur	Fonction importante indisponible, sans contournement	Tous les scénarios navigateur en `UNKNOWN`

Gravité	Définition	Exemple
3 — Mineur	Fonction dégradée, contournement possible	Une destination d'export en erreur intermittente
4 — Demande	Question, demande d'information ou d'évolution	Conseil sur la conception d'un scénario

Les délais associés à chaque niveau sont définis par votre contrat.

6.1.2 Informations à préparer

Avant de contacter le support, rassemblez les informations listées au § 9.9 du guide d'installation et d'administration : version, édition, numéro de série ou adresse MAC, description et horodatage du symptôme, identifiants des exécutions, actions déjà tentées. Ne transmettez jamais de secret.

6.1.3 Ce que couvrent l'assistance et la maintenance

Service	Accès	Référence
Correctifs et avis de sécurité de la version acquise, pendant la période de support	Toute sonde, sans contrat	§ 8.4.6 du guide d'installation et d'administration
Garantie et remplacement d'une carte défectueuse, sans rachat de l'édition acquise	Toute sonde, selon les conditions de vente	§ 8.6.4 du guide d'installation et d'administration
Documentation et notes de version	Toute sonde	Ci-dessus
Nouvelles versions fonctionnelles	Sondes couvertes par un contrat de maintenance	§ 8.4.7 du guide d'installation et d'administration
Assistance technique (diagnostic, conseil de configuration)	Sondes couvertes par un contrat de maintenance	Ce chapitre
Prestations : mise en service sur site, écriture de scénarios, formation, développement spécifique	Sur devis	Service commercial

Les conditions applicables, et notamment les délais de prise en charge, sont celles de vos conditions de vente et, le cas échéant, de votre contrat de maintenance. Aucun délai n'est garanti par cette documentation.

6.1.4 Signaler une vulnérabilité de sécurité

Si vous découvrez une vulnérabilité dans la sonde ou dans son logiciel intégré, signalez-la par le canal dédié indiqué dans votre contrat (tableau ci-dessus, rubrique « Signalement d'une vulnérabilité de sécurité »), et non par les canaux ordinaires du support. Votre contrat indique également où consulter la politique de divulgation coordonnée de l'éditeur, qui précise le traitement des signalements, ainsi que la clé de chiffrement à utiliser pour transmettre un signalement confidentiel.

Indiquez :

- la version et l'édition de la sonde ;
- la description de la vulnérabilité et son impact ;
- les étapes de reproduction.

Testez uniquement sur des sondes que vous possédez ou que vous êtes autorisé à tester, sans accéder aux données d'autrui ni perturber un service.

L'éditeur publie des avis de sécurité pour les vulnérabilités corrigées. Les correctifs sont diffusés par le canal `security` (§ 8.4 du guide d'installation et d'administration).