Série SIGMA Lite

Guide rapide de l'utilisateur



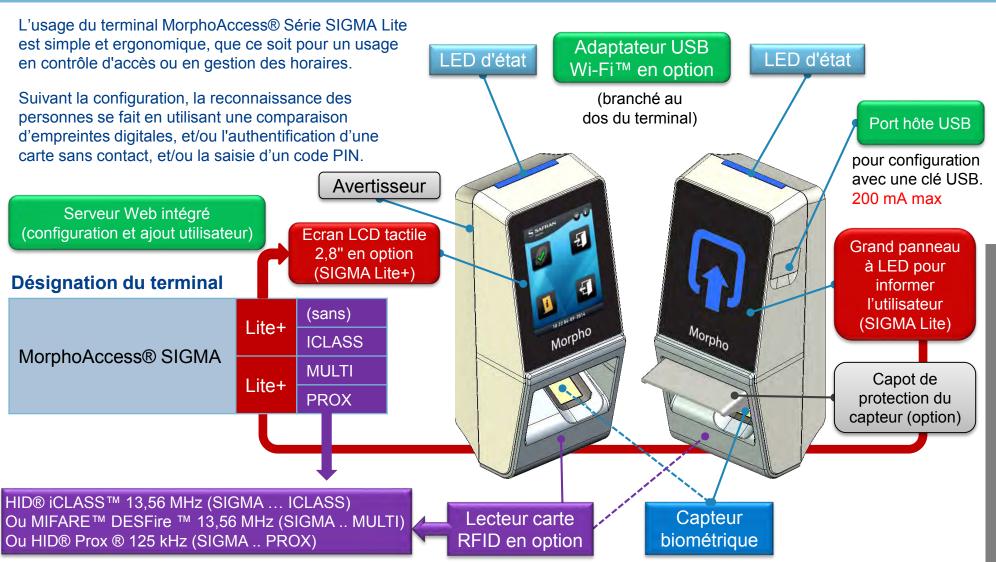




Table des matières

| Couleur | Etape | Contenu |
|---------|--------|---------------------------------|
| | Une | Présentation générale |
| | Deux | Câblage |
| | Trois | Communication |
| | Quatre | ACP ou SDAC |
| | Cinq | Administration |
| | Six | Logiciel |
| | Sept | Inscription |
| | Huit | Fonctions disponibles en option |

Présentation générale du produit



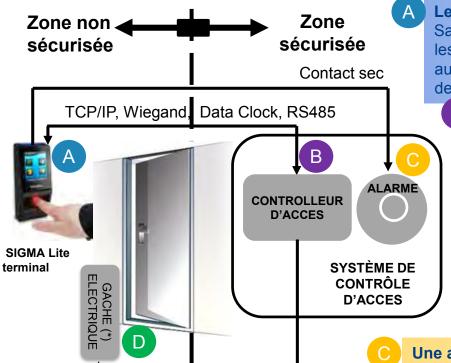
SIGMA Lite: contenu de l'emballage



3

Installation du terminal SIGMA Lite

Pour sécuriser un accès, Morpho recommande d'installer le terminal série SIGMA Lite dans un système de contrôle d'accès type comprenant les composants décrits ci-dessous.



Contact sec

Le terminal Série SIGMA Lite

Sa fonction consiste à traiter la demande d'accès de l'utilisateur. Il contrôle les droits d'accès par identification biométrique (avec une base), ou par authentification biométrique, et/ou par authentification d'une carte RFID (et de son contenu), et/ou vérification d'un code PIN.

Un contrôleur d'accès centralisé (produit tiers)

Le terminal est en interface avec un contrôleur d'accès (via un protocole TCP/IP, Wiegand, Data Clock ou RS485):

- → Après une demande d'accès, le terminal MorphoAccess® envoie le résultat des droits d'accès de l'utilisateur au Contrôleur d'accès (ce message contient au moins l'Identifiant de l'utilisateur)
- → Le Contrôleur d'accès effectue des contrôles supplémentaires et renvoie la décision finale (accès accordé/refusé) au terminal MorphoAccess[®] (qui affiche le résultat à l'intention de l'utilisateur) et au contrôleur de porte qui ouvre la porte (si l'accès a été accordé).

Une alarme (produit tiers)

Le terminal MorphoAccess® envoie un message au Contrôleur d'accès pour activer l'Alarme dès qu'une action malveillante comme une tentative d'intrusion ou d'arrachement du mur est détectée

Un verrou électrique de porte ou un dispositif équivalent (produit tiers)

Le Contrôleur d'accès envoie une commande pour activer le verrou si l'accès est accordé (c'est-à-dire l'identifiant de l'utilisateur est répertorié dans la liste des utilisateur autorisés). Le contrôle du verrou (ou de la gâche) est réalisé par un contact sec.

(*) ou équivalent

Processus de contrôle d'accès type



Sur demande d'accès, le terminal vérifie les droits d'accès de l'utilisateur à l'aide d'un contrôle biométrique. Si le résultat du contrôle est réussi (utilisateur reconnu), un message est envoyé au Contrôleur d'accès central pour d'autres contrôles sur les droits d'accès.

Si l'utilisateur est autorisé à accéder à la zone protégée, le contrôleur d'accès central renvoie un message « accès accordé » au terminal et une commande « d'ouverture » au contrôleur de porte.

Accès accordé







Les gabarits d'empreinte digitale de l'utilisateur doivent être stockées dans la base de données du terminal ou dans sa carte sans contact afin de permettre le contrôle biométrique.



SIGMA Lite : modes de contrôle d'accès disponibles

Le terminal peut être configuré selon l'un des modes décrits dans le tableau ci-dessous

| | Identification | Authentification | Multi facteur | Serveur proxy |
|---|--|---|--|---|
| Application de contrôle d'accès | Application exécutée sur le terminal au démarrage. | Application exécutée sur le terminal au démarrage. | Application exécutée sur le terminal au démarrage. | Application distante qui pilote le terminal via le réseau |
| Evénement déclencheur de la demande d'accès | | L'utilisateur place sa carte sans contact devant le lecteur. (*) | L'utilisateur pose son doigt sur le capteur ou présente sa carte devant le terminal | Les événements déclencheurs sont choisi par l'application à distance |
| Contrôle biométrique (si activé) | L'empreinte digitale capturée est comparée à toutes les empreintes digitales de la base de données. | L'empreinte digitale capturée est comparée à l'empreinte digitale de référence de l'utilisateur. (**) | Celui de l'identification ou de l'authentification, suivant l'événement déclencheur | Choisi par l'application distance |
| Décision d'afficher un signal de résultat à l'intention de l'utilisateur | Par application autonome d'identification | Par application autonome d'authentification | Par application autonome exécutée | Par application distante |

^(*) ou l'utilisateur entre son Identifiant sur le clavier, ou le terminal reçoit une trame Wiegand transmis par un dispositif externe

^(**) stockée sur la carte sans contact ou dans l'enregistrement de l'utilisateur dans la base de données locale du terminal, sous forme de gabarit (ensemble de vecteurs) et non d'une image d'empreinte

Environnements de déploiement

| Température de fonctionnement | -10° à + 55° C (14° à 131° F) |
|------------------------------------|--|
| Humidité tolérée en fonctionnement | 10 % < HR < 80 % (sans condensation) |
| Température de stockage | -25° à + 70° C (-13° à 158° F) |
| Humidité tolérée pour le stockage | 5 % < HR < 95 % |
| Code IP | Classe IP65, après fixation de la porte arrière avec les 4 vis |

Précautions générales

- Ne pas exposer le terminal à des températures extrêmes.
- Lorsque l'environnement est très sec, éviter toute moquette synthétique à proximité du terminal, afin de réduire le risque de décharge électrostatique indésirable.

Zones contenant des combustibles

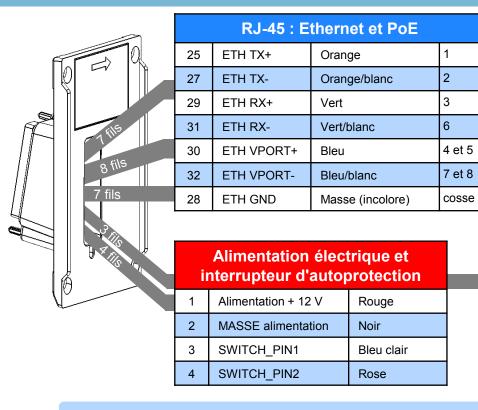
Ne pas installer le terminal près de postes d'essence ou d'autres installations contenant des gaz ou des matières inflammables ou combustibles. Le terminal n'est pas conçu avec une sécurité intrinsèque.

Le terminal doit être installé dans des conditions d'éclairage contrôlées

- Eviter d'exposer le capteur biométrique à un éclairage clignotant
- Eviter toute exposition directe du capteur biométrique à la lumière du soleil ou un éclairage UV.

Etape deux : câblage

Présentation générale du câblage



| RJ-45 | |
|-------|--|
|-------|--|



| Wiegand | | | |
|---------|----|-----------------|-------------|
| | 13 | WIEGAND_IN0 | Vert/rouge |
| | 15 | WIEGAND_IN1 | Blanc/rouge |
| | 14 | WIEGAND_OUT0 | Vert |
| | 16 | WIEGAND_OUT1 | Blanc |
| | 17 | WIEGAND_LEDOUT1 | Bleu |
| | 18 | WIEGAND_LEDOUT2 | Bleu/rouge |
| | 20 | WIEGAND_GND | Noir/rouge |

Entrée Wiegand et sortie

| RS-485, Entrée et sortie GP | | | |
|-----------------------------|-----------|--------------|--|
| 5 | RS485_A | Bleu | |
| 7 | RS485_B | Bleu/rouge | |
| 6 | RS485_GND | Noir/rouge | |
| 9 | GPI_0 | Orange | |
| 10 | GPI_1 | Orange/rouge | |
| 11 | GPO_0 | Jaune | |
| 12 | GPO_1 | Jaune/rouge | |
| 8 | GPIO_GND | Noir/rouge | |

| Relais interne | | | |
|----------------|-----------|--------|--|
| 19 | RELAY_NO | Jaune | |
| 21 | RELAY_NC | Orange | |
| 22 | RELAY_COM | Gris | |

Toutes les connexions du terminal sont de type SELV (Très Basse Tension de Sécurité électrique).

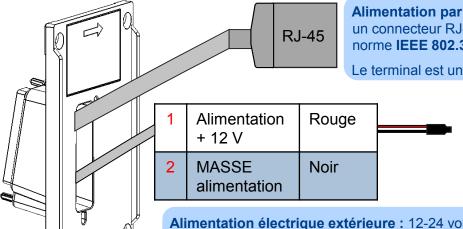


L'alimentation fournie par la source électrique doit être coupée avant de débuter l'installation.

Avant de procéder, s'assurer que la personne en charge de l'installation et des connexions est reliée correctement à la terre afin d'empêcher d'éventuelles décharges électriques (ESD).

Conservation de la Date/Heure du terminal : les réglages volatiles (comme la date/l'heure) du terminal sont protégés contre les pannes électriques au moyen d'un composant dédié pendant au moins 24 heures (à 25 °C) sans alimentation extérieure.

Câblage d'alimentation



Alimentation par Ethernet (POE, Power Over Ethernet): l'alimentation peut être fournie via un connecteur RJ-45 à l'aide d'un injecteur POE (PSE, Power Sourcing Equipment) conforme à la norme IEEE 802.3af ou IEEE802.3at type 1.

Le terminal est un équipement de Classe 0 (15.4W).

Spécifications de l'injecteur PoE

➤ Sortie de tension : 48 VCC

Courant de sortie : 0,32 A

> Alimentation: 15,36 W

Alimentation électrique extérieure: 12-24 volts (régulée et filtrée), 1 A min à 12 V, conforme à la norme CEE/EEC EN60950. Une alimentation électrique de 12 volts conforme à la norme Wiegand du SIA est également adéquate. En cas de partage d'alimentation entre plusieurs terminaux, chaque terminal doit recevoir 1 A (par exemple, deux terminaux nécessitent une alimentation de 12 VCC, 2 A).

Un système de sécurisation de l'alimentation par batterie ou une alimentation sans coupure (UPS, Uninterrupted Power Supply) avec une protection intégrée contre les surtensions sont recommandés.

Morpho recommande un câble de jauge AWG20 pour l'alimentation 12 V.

La tension mesurée sur le connecteur du bornier du terminal doit être égale à 12 V-24 V (-15 %/+10 %).

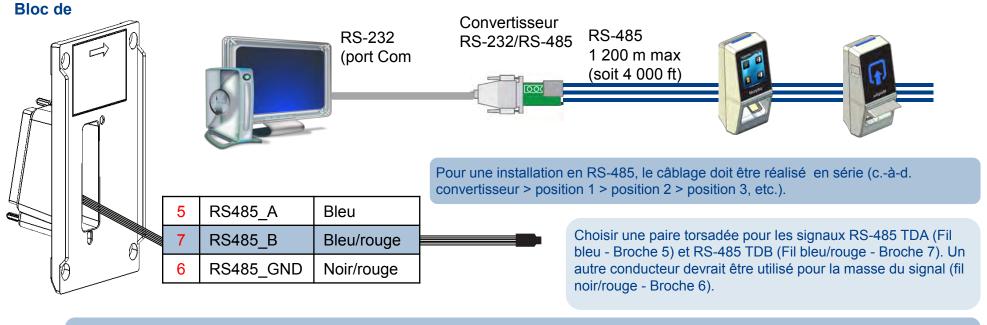
Le tableau à droite indique la chute de tension maximale entre la source d'alimentation et le terminal en fonction de la longueur du câble.

| | alibre AWG | Diamètre (mm) | | Chute de tensio maximale (V) | |
|-----|---------------|------------------|-------|---------------------------------|--------|
| Avv | AVVG | (11111) | à 1 m | à 5 m | à 10 m |
| | 20 | 0,81 | 0,03 | 0,17 | 0,33 |
| | 22 | 0,64 | 0,05 | 0,26 | 0,53 |
| | 24 | 0,51 | 0,08 | 0,42 | 0,84 |



ATTENTION : une alimentation insuffisante peut entraîner une corruption de la mémoire et des données ; de même une surtension peut endommager le matériel. Ces deux anomalies annulent la garantie

Communication RS-485



Utiliser un câble CAT-5 UTP (ou de qualité supérieure) (blindé de préférence) avec une impédance caractéristique de 120 ohms. Utiliser un câble de jauge AWG 24 minimum.

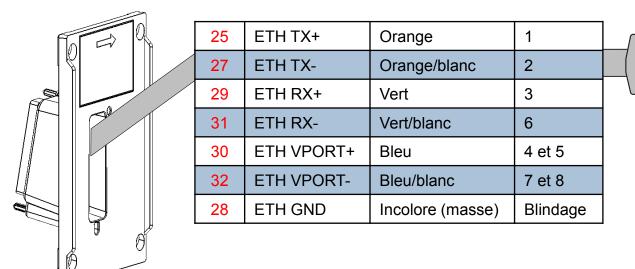
Choisir un convertisseur RS-232/RS-485 supportant le passage du mode émission à réception (et vice versa) par l'état "idle".

IMPORTANT:



- > Jusqu'a 31 dispositifs peuvent être installés au maximum sur une même ligne RS485.
- La longueur de câble totale maximale ne doit pas dépasser 1 200 m (soit 4 000 ft).
- Le câble doit être dédié à cette installation uniquement et non utilisé à d'autres fins.

LAN Ethernet et WLAN (sans fil)

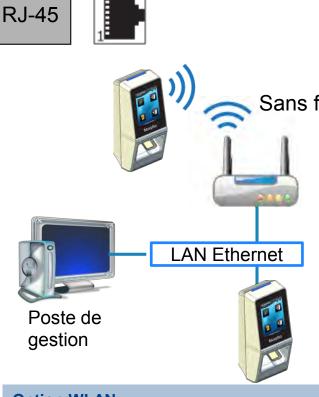


Utiliser un câble blindé de catégorie 5 (120 ohms) ou de qualité supérieure. Il est fortement recommandé d'insérer un répéteur tous les 90 m.

Le mode DHCP est activé par défaut sur les terminaux MorphoAccess® SIGMA Lite (réglage usine).

Connexion Ethernet sur le bornier

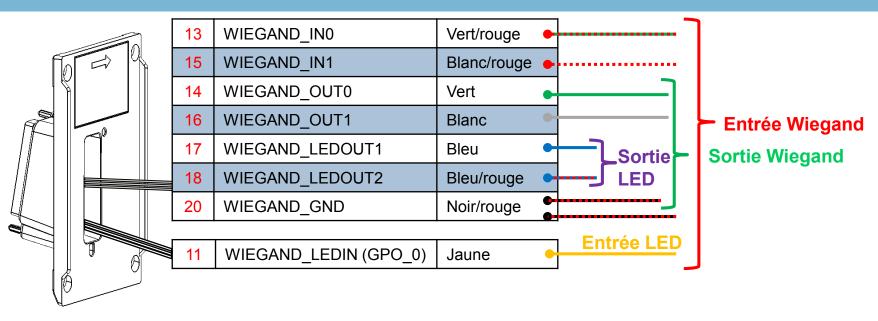
- → Une très grande vigilance est recommandée lors de la connexion du câble Ethernet sur le bornier car une connexion de mauvaise qualité peut dégrader considérablement la sensibilité du signal Ethernet.
- → Brancher Rx+ et Rx- avec les deux fils d'une même paire torsadée (et faire de même pour Tx+/Tx- avec les deux fils d'une autre paire torsadée).



Option WLAN

Les adaptateurs sans fil Morpho prennent en charge les normes 802.11b et 802.11g. WEP Open, WPA et WPA2 sont supportés.

Communication Wiegand



Un câble à trois conducteurs (blindé de préférence) est nécessaire pour Data 0, Data 1 et WGND.

Utiliser un câble de jauge 18-22 AWG selon la configuration d'interconnexion entre le terminal et le Panneau de contrôle d'accès (ACP, Access Control Panel).

- ➤ Brancher **WIEGAND_OUT0** (Fil vert Broche 14) avec Data 0 de l'ACP,
- > Brancher WIEGAND OUT1 (Fil blanc Broche 16) avec Data 1 de l'ACP,
- > Brancher WIEGAND GND (fils noir/rouge Broche 20) avec la borne commune du lecteur de l'ACP (0 VCC).

Pour un câble de jauge 18 AWG, la distance de câble maximale est de 150 m (500 feet); pour une jauge de 20 AWG, la distance maximale est de 90 m (300 feet); pour une jauge de 22 AWG, la distance maximale est 60 m (200 feet).

Toutes les sorties du contrôleur devront être de type à collecteur ouvert ou 5 V+/-5 %

Communication Wiegand (suite)

Important

Par défaut, le port de sortie Wiegand n'est pas activé. La sortie Wiegand doit être configurée avant d'effectuer la connexion à l'ACP.

Remarque

Lors de l'installation, l'administrateur du système sera invité à choisir un format de trame Wiegand préexistant ou à créer un format de trame personnalisé et à le charger dans le terminal avant sa première utilisation.

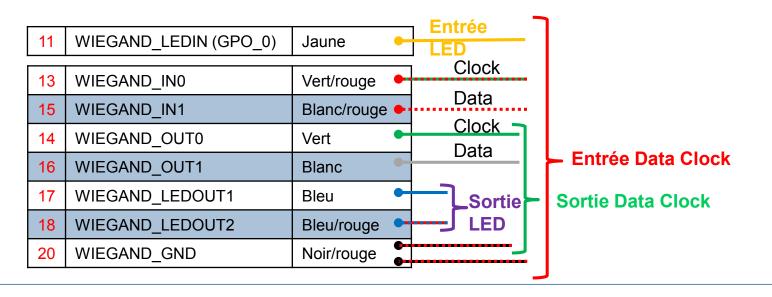
Data Clock

Le port Wiegand prend supporte également le protocole Clock & Data. Le câblage est décrit ci-dessous.

Exemple d'informations sur le format

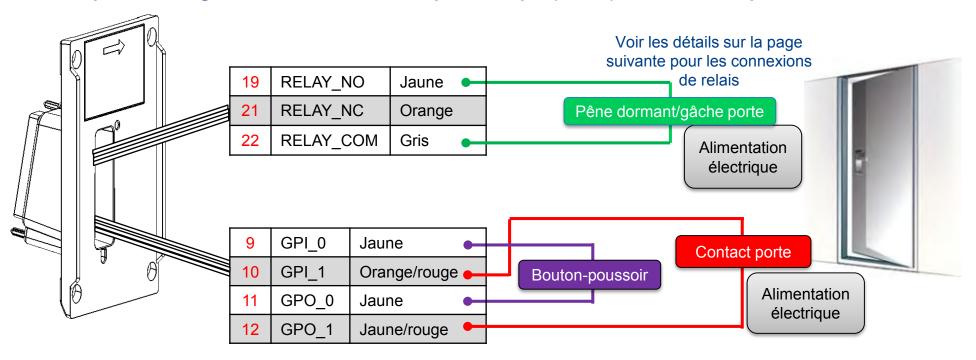
Type: 26 bits standard

- Plage de code site Alt et de code site Fail : 0 à 255
- Plage modèle de numéro ID : 1 à 65535
- Plage étendue de numéro ID : N/A
- Bit start ID : 9Longueur ID : 16
- Bit start de code site : 1
- Longueur de code site : 8
- Longueur de bit start : 0



Contrôle d'accès de porte unique (SDAC, Single Door Access Control)

Exemple de câblage de Contrôle d'accès de porte unique (SDAC) : avec bouton-poussoir



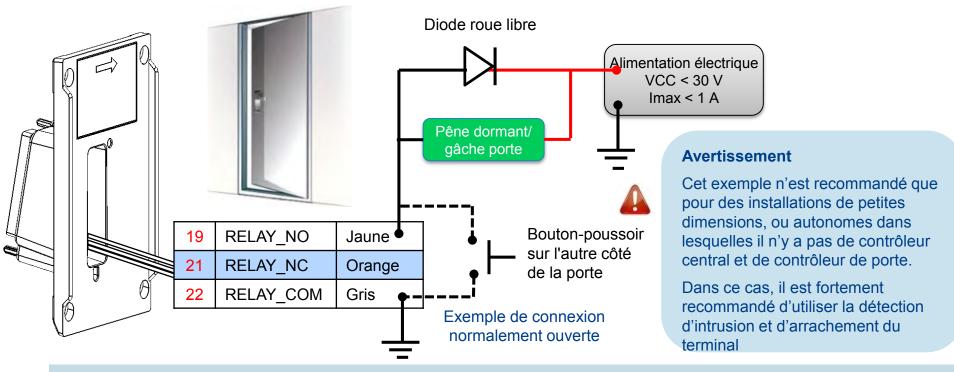


S'il n'y a pas de contact de porte, GPI1 (9) et GPO1 (11) doivent être connectés ensemble



L'alimentation fournie par la source électrique doit être coupée avant de débuter l'installation.

Câblage du relais interne



La gestion de la charge inductive nécessite une diode parallèle pour une durée de vie optimale des contacts.

Avertissement



- Le relais interne est limité à un courant maximal de 1 A à 30 V. Si le pêne dormant ou la gâche de la porte ponctionne plus de 1 A, le dispositif peut être endommagé. Si la charge du pêne dormant ou de la gâche de la porte dépasse 1 A, un relais externe doit être utilisé.
- Le relais interne a été conçu pour 100 000 cycles. Si un nombre supérieur de cycles est nécessaire, un relais externe piloté par GPO doit être utilisé.

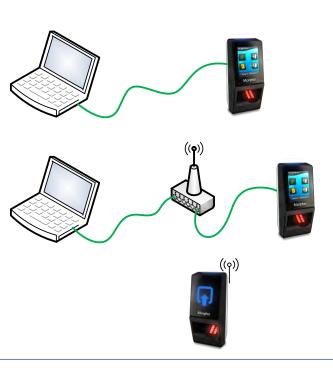
Première communication avec le terminal (1/2)

→ La première configuration nécessite une liaison réseau

Le terminal MorphoAccess® Série SIGMA Lite a été conçu de manière à pouvoir fonctionner en mode autonome, mais il faut au moins une connexion point à point entre un PC et le terminal pendant la première configuration. Cette connexion sera utilisée pour la gestion de la base de données, la maintenance du terminal, etc.

Méthodes de connexion du réseau

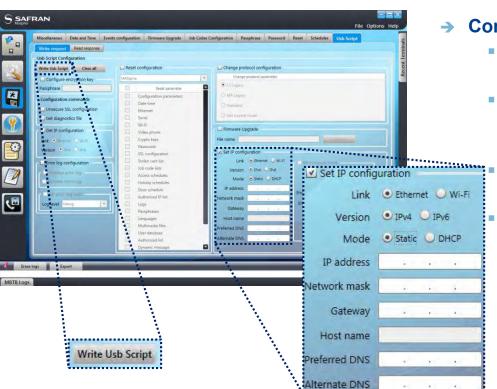
- Connexion point à point Ethernet
 - Cette méthode nécessite une configuration IP statique (sauf si un serveur DHCP est installé sur le PC)
- Connexion via un LAN (Local Area Network, réseau local)
 - En présence d'un serveur DHCP sur le réseau, les paramètres du réseau seront assignés automatiquement aux terminaux (contacter l'administrateur du réseau).
 - En l'absence de serveur DHCP, il faut configurer une IP statique sur chaque terminal et sur le PC.
- Utiliser MorphoBioToolBox pour configurer les paramètres du réseau (voir la page suivante)



Première communication avec le terminal (2/2)

> Remarque générale pour la configuration du réseau

- Pour un terminal est connecté à un réseau local sans serveur DHCP, veiller à configurer les paramètres suivants :
 - Le PC d'administration et tous les terminaux doivent avoir une adresse IP distincte (ex. : 192.168.0.1;
 192.168.0.2; etc.).
 - Le PC d'administration et tous les terminaux doivent avoir le même masque réseau (ex. : 255.255.255.0 si les 3 premiers octets de l'adresse IP sont identiques pour tous les terminaux et le PC).



→ Configuration à l'aide de MorphoBioToolbox

- Remplir l'adresse IP et le masque réseau en suivant les recommandations du paragraphe précédent.
- Même en l'absence d'utilisation, remplir les valeurs DSN préférées et Passerelle alternatives (avec 1.1.1.1 par exemple).
 - Cliquer sur le bouton « Write USB Script » puis les enregistrer sur une clé USB.
 - Brancher la clé USB sur le terminal à l'aide du câble d'adaptation.
 - Sur la version Lite, un bip aigu, suivi d'un panneau LED violet clignote et des bips aigus un panneau LED vert indique que la configuration est terminée
 - Sur la version Lite+, une image de prise USB suivie de 2 bips aigus indiquent que la configuration est terminée

Etape cinq: Administration

Administration via le serveur Web intégré au terminal

Le serveur Web intégré du terminal permet de configurer facilement le terminal et les utilisateurs via un navigateur Web sur un PC de bureau, un ordinateur portable, une tablette ou un smart phone.



La connexion au serveur Web intégré, via un LAN ou un WLAN, nécessite l'adresse IP et le mot de passe du terminal

Désactivez le serveur Web s'il n'est pas utilisé.



Administration via l'application MorphoBioToolBox

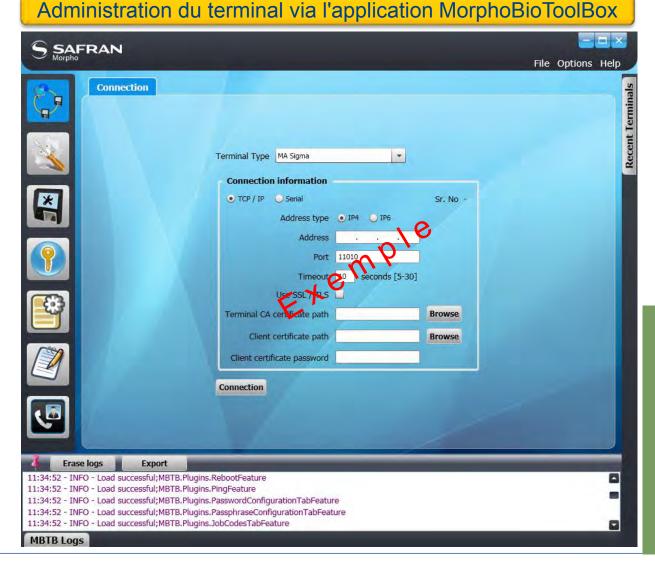
Il est également possible de configurer le terminal SIGMA Lite en utilisant une application dédiée : MorphoBioToolBox (pour Windows) Veuillez noter que cette application a un Guide de l'utilisateur intégré (Menu Aide).

Amérique du Nord et du Sud :

Envoyer un e-mail à l'adresse cscenter@morpho.com avec votre nom, numéro de téléphone, numéro de série de votre MASIGMA, et comme objet « Please Send Link for MBTB ». Un lien permettant de télécharger le logiciel vous sera envoyé par e-mail.

Autres pays : veuillez contacter votre représentant commercial.





Logiciel permettant l'administration à distance du terminal

- → Les terminaux Série SIGMA Lite sont compatibles avec :
 - L'application MorphoManager (version 8.0.3 ou ultérieure)
- → Lorsque le mode Legacy Morpho est activé, le terminal est compatible avec :
 - MEMS (version 7.3.1 ou ultérieure),
 - Les limitations du mode Morpho Legacy sont décrites dans le document suivant :
 - Notes de version de MorphoAccess® Série SIGMA Limitations de Legacy Morpho
- → Lorsque le mode Legacy L1 est activé, le terminal est compatible avec :
 - SecureAdmin (version v4.1.20.0.1 ou ultérieure),
 - Les limitations du mode L1 Legacy sont décrites dans le document suivant :
 - Notes de version de MorphoAccess[®] Série SIGMA Limitations de Legacy L1

Principes de capture des empreintes digitales 1/3



aining num on

Région d'intérêt

Le capteur biométrique a été conçu pour capturer la zone la plus utile d'une empreinte digitale, ce qui correspond (en règle générale) au centre de l'extrémité du doigt comme indiqué sur la figure ci-dessus.

Doigts recommandés



Le capteur peut capturer les empreintes de n'importe quel doigt, mais nous recommandons :

- d'utiliser l'index en 1^{er} choix
- d'utiliser le majeur en 2nd choix
- d'utiliser l'annulaire comme autre 2nd choix (3^e choix)
- d'éviter l'auriculaire (données insuffisantes)
- d'éviter le pouce (meilleure précision, mais ergonomiquement plus difficile à utiliser)

Résolution des difficultés d'acquisition

Recommandations générales

- Retirer les bandes ou les rubans adhésifs de la zone des empreintes digitales
- Ne pas appuyer ou contracter le doigt afin d'éviter toute constriction des vaisseaux sanguins.

Image d'empreinte digitale trop sombre : le doigt est probablement trop humide et/ou trop sale

- > trop humide : se sécher le doigt
- > top sale : se nettoyer le doigt

Image d'empreintes digitale trop claire : le doigt est probablement trop froid et/ou trop sec

- > trop froid : se réchauffer le doigt
- trop sec : humidifier le doigt (par exemple avec une buvard humidifié) et/ou le réchauffer.

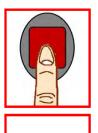
Pour une campagne de capture à grande échelle, contactez votre représentant Morpho afin de connaître nos offres de formation et de service

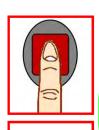
Principes de capture des empreintes digitales 2/3

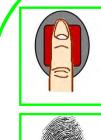


Position idéale du doigt

Hauteur du doigt









POSITION

Position incorrecte: ...



- Ne pas placer le bout du doigt en bas du capteur
- Ne pas placer le bout du doigt au milieu du capteur

Position correcte:

 Aligner le centre de la 1ère phalange avec le centre du capteur

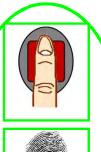
Angle du doigt













Position incorrecte : 🗥



- Ne pas incliner le doigt vers le bord droit ou gauche du capteur
- Position correcte :
 - Le doigt doit être parallèle aux bords du capteur

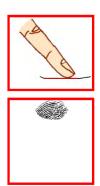
Principes de capture des empreintes digitales 3/3

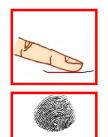


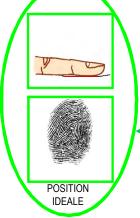
Position idéale du doigt



du doigt







Position incorrecte : 🗥



- Ne pas laisser le doigt en l'air
- Ne pas pencher le doigt vers l'avant ou vers l'arrière

Position correcte:

Le doigt doit être parallèle à la surface du capteur

Rotation du doigt









Position incorrecte :



Ne pas rouler le doigt

Position correcte:

 Le doigt doit être parallèle à la surface du capteur

Etape sept : principes de capture

Fondamentaux sur l'IHM de SIGMA Lite

Bleu continu



En attente d'une carte RFID ou de la pose d'un doigt

Vert continu



accordé Script USB terminé

avec succès

Accès

Rouge continu



Echec script USB

Accès

refusé

Jaune clignotant



Placer le doigt

Déplacer le doigt

Violet clignotant



Script USB en cours d'exécution

Eteint



Pas en attente de carte

Pas en attente de doigt (Base vide)

Etape sept : principes de capture

Fondamentaux sur l'IHM de SIGMA Lite+



En attente d'une carte **RFID** ou de la pose d'un doigt



accordé Script **USB** terminé



Echec script **USB**

refusé



doigt Déplacer





Clé USB détectée



Clé USB a retirer

Position de la carte sans contact – Entrée du code PIN

Position de la carte sans contact/



Placer la carte RFID devant le lecteur de cartes sans contact

L'authentification de l'utilisateur est déclenchée suite à la détection d'une carte utilisateur par le lecteur de carte sans contact (en option).

Le terminal lit les données de l'utilisateur mémorisées dans la carte (au moins l'ID de l'utilisateur) et débute le processus d'authentification suivant les réglages du terminal.

Entrer le code PIN (SIGMA Lite+)



Lorsque les réglages du terminal l'y invitent, l'utilisateur doit saisir son code PIN: une fois au cours du processus d'enrôlement, puis lors de chaque authentification (en plus ou à la place du contrôle biométrique).

L'utilisateur saisi son code PIN à l'aide d'un clavier numérique affiché sur l'écran tactile LCD (en option).

Etape sept: principes de capture

Position de la carte sans contact – Avertissement



Fonction de gestion des horaires (SIGMA Lite+ uniquement)

Les terminaux MorphoAccess[®] Série SIGMA Lite+ intègrent une fonction de gestion d'horaire (T&A : Time and Attendance) disponible en option.

A cet effet, le terminal ajoute des informations spécifiques à la gestion des horaires, à l'enregistrement créé pour chaque demande d'accès traitée. Ces enregistrements sont conservés dans un journal interne au terminal, et peuvent être envoyées au fur et à mesure à un système distant, ou bien lues par blocs par un même système.

Ces informations sont fournies par l'utilisateur via un écran spécifique affiché au cours du processus d'identification ou d'authentification.

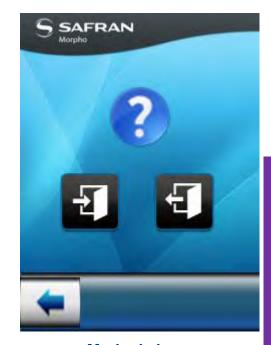
Cet écran spécifique contient 2 touches de fonction dédiées :

- > L'une permet de spécifier une entrée ou un début de tâche
- > L'autre permet de spécifier une sortie ou une fin de tâche

L'utilisateur doit appuyer sur l'une de ces touches pour fournir les informations de gestion des horaires au terminal.

En fonction des réglages du terminal, cet écran s'affiche avant ou après que l'utilisateur a placé le doigt sur le capteur ou sa carte devant le lecteur.

Cette fonction est uniquement disponible sur un terminal équipé d'écran LCD tactile.



Mode de base (exemple d'écran)

Recommandations

Mise en garde générale

→ Le fabricant ne peut être tenu responsable en cas de non-respect des recommandations suivantes ou d'utilisation incorrecte du terminal.

Précautions générales

- → Ne pas essayer de réparer le terminal SIGMA Lite par vous-même. Le fabricant ne peut pas être tenu responsable en cas de dommage/d'accident résultant de tentatives de réparation des composants. Toute intervention réalisée par un personnel non autorisé annulera la garantie.
- N'utiliser le terminal qu'avec ses accessoires d'origine. Des tentatives d'utilisation d'accessoires non approuvés avec le terminal annulera la garantie.

Terminaux non connectés au réseau

→ Pour les terminaux utilisés en mode autonome, il est fortement recommandé de sauvegarder régulièrement la base de données locale et systématiquement après des modifications significatives de cette base (ajout, suppression ou modification d'utilisateur).

Synchronisation de la date et de l'heure

- → Si utilisez le terminal SIGMA Lite pour des applications nécessitant une grande précision horaire, nous vous recommandons de synchroniser régulièrement l'heure du terminal avec l'horloge externe précise et fiable.
- → L'horloge interne du terminal à une précision de +/- 10 ppm à +25 °C (soit environ +/- 3 s par jour).
- → A des températures inférieures ou supérieures, l'écart peut être supérieur (de 7 s par jour dans le pire des cas).

Précautions pour le nettoyage

- → Un tissu sec devrait être utilisé pour nettoyer le terminal, notamment le capteur biométrique.
- L'emploi de liquides acides, d'alcool ou de matériaux abrasifs est interdit.