



Sophia : Une application en ligne protégée par un réseau hautement sécurisé

Puisqu'il s'agit d'une application en ligne, la plateforme Sophia ne nécessite aucune installation locale sur l'ordinateur de nos clients, ce qui garantit une plus grande confidentialité et une meilleure efficacité.

De plus, nous avons veillé à ce que les deux méthodes de connexion possibles aux machines à café contournent les réseaux internet publics et, par conséquent, ne puissent pas compromettre le serveur ou les données de nos clients.



Connexion cellulaire

- La **carte SIM** à l'intérieur du modem* de la machine se connecte au **PA** de la tour cellulaire la plus proche par notre connexion privée. Notre réseau cellulaire ne passe pas par l'internet public, ce qui offre une plus grande fiabilité, une plus grande vitesse, des temps de latence moins importants et une plus grande sécurité que les connexions internet habituelles.
- Il est impossible d'accéder à la machine à café ou aux données privées du client par le biais d'un réseau externe.
- Cette solution permet au nuage d'apparaître comme un autre point de terminaison sur le réseau **MPLS VPN** d'Evoca Amérique du Nord, pour le rendre accessible à chaque machine et éviter d'envoyer des données sur l'internet public.
- Les avantages de cette approche incluent :
 - Performances supérieures du réseau, avec une latence réduite de 50 %.
 - Jusqu'à 3 fois plus disponible.
 - Sécurité de niveau entreprise, qui évite d'acheminer le trafic sur l'internet public.
 - Les données provenant de la machine sont **cryptées** à chaque fois qu'elles doivent être transférées vers le serveur.
 - Les informations relatives aux utilisateurs sont **cryptées** dans la base de données (**hachage à sens unique**).



Connexion Wi-Fi

- Les machines qui se connectent par Wi-Fi le font de la même manière qu'un ordinateur portable ou un téléphone mobile.
- La machine à café utilise un protocole **TCP/IP** pour se connecter au routeur. Pour obtenir une adresse IP, le **DHCP** de la machine est réglé sur l'**allocation dynamique**. Pour des raisons de sécurité, il est impossible de modifier ce paramètre.
- Une fois la connexion Internet établie, la machine envoie un signal au serveur d'Evoca Amérique du Nord pour indiquer qu'elle est en ligne. Il envoie alors un accusé de réception à la machine pour confirmer que le lien entre eux est établi. Toutes les 5 minutes, un nouvel accusé de réception est envoyé pour valider la connexion.
- Lorsqu'un utilisateur fait une demande à Sophia sur l'application en ligne, le serveur demande à la machine à café de lui fournir les données du fichier demandé (par exemple : une recette).
- La machine à café convertit ensuite le fichier en une chaîne de caractères et l'envoie au serveur.
- Sophia reconvertit finalement cette chaîne de caractères en données consultables



Que votre machine soit connectée au réseau cellulaire ou Wi-Fi, ces fonctions de sécurité garantissent que nous ne pourrions pas accéder à votre serveur ou à vos données.

Petit glossaire terminologique

Communication réseau

PA - Point d'accès réseau

Imaginez que chaque tour de téléphonie cellulaire dispose de deux portes. L'une d'entre elles est utilisée pour accéder à l'internet public, l'autre s'ouvre sur un tunnel privé (VPN).

Evoca Amérique du Nord a son propre point d'accès/porte.

Chaque machine à café a la clé pour passer par la porte d'Evoca Amérique du Nord, mais seulement cette porte.

DHCP - Protocole de configuration dynamique des hôtes (français)

Il s'agit d'un protocole de gestion de réseau qui définit automatiquement les paramètres de configuration. En principe, il permet aux machines de se connecter au réseau cellulaire en leur attribuant des adresses IP temporaires.

Allocation dynamique

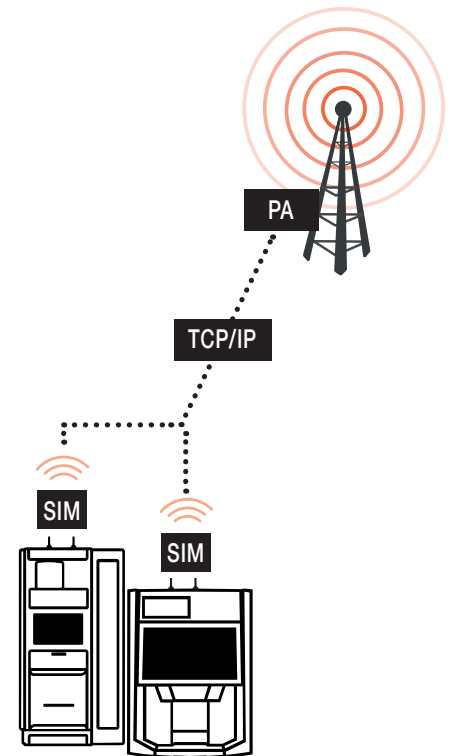
Cette méthode d'attribution DHCP attribue une adresse IP temporaire. Lorsque votre machine doit se connecter au réseau, une adresse IP lui est attribuée pour une période limitée afin de garantir la confidentialité des données.

Carte SIM - Module d'identification de l'abonné (français)

Une carte SIM est utilisée par le modem pour obtenir l'autorisation de se connecter à une tour cellulaire. Elle doit être activée pour pouvoir transmettre des données sur un réseau.

TCP/IP - Protocole de contrôle de transmission / Protocole internet (français)

Protocole de communication utilisé par la machine à café pour transférer des données avec le serveur.



Sécurité

Cryptage

Processus de codage d'un message ou d'une information de manière à ce que seules les parties autorisées puissent y accéder et que les personnes qui ne le sont pas ne puissent pas le faire. Le codage n'empêche pas en soi les interférences, mais refuse le contenu intelligible à un intercepteur potentiel.

Hachage à sens unique

Fonction de chiffrement cryptographique dont le renversement est quasiment impossible.

MPLS VPN - Commutation multiprotocole par étiquette par réseau privé virtuel (français)

Tunnel privé entre 2 points, créant un réseau privé.

Dans notre cas, nous avons un tunnel VPN entre les fournisseurs de réseaux cellulaires et notre serveur.

Sur notre réseau, chaque machine dispose d'un chemin VPN menant à notre serveur. Elles exécutent un petit logiciel qui ouvre le tunnel, toutes les communications passant exclusivement par celui-ci.

