

Nemo Connect

Fiche Sécurité

1. Aucune donnée stockée

Aucune donnée issue de votre messagerie ou du PIM n'est stockée sur les architectures Nemo Connect, l'ensemble de vos données est en sécurité derrière votre pare-feu. Nemo Connect permet la synchronisation des données entre utilisateurs nomades authentifiés et votre serveur de messagerie d'entreprise pendant de courtes sessions de synchronisation.

Aucune donnée n'est en transfert ou stockée sur nos serveurs, ou sur des infrastructures dépendantes de nos services. Les informations d'authentification ne sont jamais stockées sur nos serveurs.

Le service Nemo Connect effectue 2 niveaux d'authentification d'utilisateur pour chaque session. L'authentification de second niveau auprès du serveur de messagerie de l'entreprise requiert que les informations soient fournies par l'utilisateur du terminal mobile. Le service Nemo Connect n'y a pas accès et ne les stocke pas sur ses serveurs.

Aucun mot de passe n'est stocké en clair sur les terminaux mobiles. Chaque utilisateur s'authentifie par une combinaison unique d'informations. Si les administrateurs choisissent de permettre à l'utilisateur de stocker leurs informations d'authentification sur leurs terminaux (dans le cas du push notamment), ces informations sont stockées via un format de chiffrement fort.

2. Sécurité éprouvée

Nemo Connect vous garantit les meilleures technologies existantes pour la protection des données :

- Pare-feu Clavister
- Chiffrement fort des données (échange de clés 1024-bit RSA et chiffrement 128-bit AES)
- Authentification sur 2 niveaux, d'abord sur notre plateforme, puis avec la source d'authentification de l'entreprise.



