



CITADELTEAM

Communication Transversale Sécurisée



Use Case

ERCOM
Cyber Solutions by Thales

Communication Transversale Sécurisée avec Citadel Team

La communication transversale sécurisée permet aux équipes de différents métiers (Ressources Humaines, Direction, Informatique, Production, Juridique, etc.), ainsi qu'aux collaborateurs répartis à l'international, d'échanger des informations sensibles en toute confiance. Elle assure également la diffusion d'informations fiables auprès de l'ensemble des collaborateurs. En garantissant la confidentialité, l'intégrité et la traçabilité des échanges, cette approche favorise une collaboration plus efficace, tout en protégeant les données stratégiques de l'entreprise. Dans un contexte où les risques de fuite d'informations, de malentendus ou de silos organisationnels sont croissants, sécuriser et fluidifier les échanges devient un enjeu essentiel de performance et de gouvernance.



Qui est concerné ?

- Tous les employés
- Les managers et responsables d'équipes
- Les équipes projet et métiers transverses
- Les départements supports
(RH, IT, Communication, Finance...)



Les objectifs :

- Permettre la communication transversale sécurisée entre l'ensemble des employés
- Faciliter la collaboration au quotidien tout en respectant des exigences élevées de confidentialité
- Centraliser et protéger les échanges sensibles

Nous vous garantissons une confidentialité et une étanchéité totale de vos échanges !

a) Facilité d'accès & inscription sécurisée

Les membres accèdent rapidement et facilement à Citadel Team via leur smartphone, leur tablette ou leur ordinateur avec leurs adresses email professionnelles.

b) Groupes de discussion sans limite de membres

Pouvant réunir l'ensemble des collaborateurs concernés au sein de larges communautés de travail. Ces salons publics facilitent le partage d'informations à l'échelle de l'entreprise, avec la possibilité de restreindre les droits d'écriture pour garantir une communication descendante claire et maîtrisée.

c) Contrôle sécurisé des accès aux salons

Les membres peuvent configurer différents types de salons avec des règles d'accès adaptées à leurs besoins, afin de garantir la sécurité des échanges. Les salons restreints sont réservés exclusivement aux membres de votre infrastructure, empêchant ainsi tout utilisateur externe de les rejoindre. Cette gestion fine des permissions permet de protéger les informations sensibles tout en assurant une collaboration sécurisée et maîtrisée.

d) Diffusion automatisée via des bots

Il est possible d'automatiser l'envoi d'alertes, de notifications et d'informations métiers, grâce à des bots capables de diffuser des messages ciblés, en temps réel dans les salons appropriés.

e) Messagerie, appels chiffrés de bout en bout

Les échanges (textes, fichiers, appels...) sont chiffrés de bout en bout.

f) Échange sécurisé en audio et visioconférence avec partage d'écran

La solution permet de participer à des conférences audio et vidéo, ou d'en organiser, depuis n'importe quel endroit, de présenter vos contenus et de collaborer en temps réel, grâce au partage d'écran intégré.

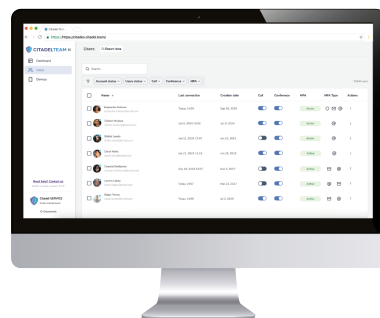


Gestion fine des utilisateurs :

Afin de garantir l'entière confidentialité et une totale étanchéité entre nos clients, chaque entreprise bénéficie d'une infrastructure dédiée, opérée par Thales et hébergée en France.

Cette approche vous offre une maîtrise totale de votre environnement. L'infrastructure est entièrement configurable afin de répondre aux exigences spécifiques de votre organisation, notamment en matière de politiques de sécurité, de gestion des identités et de contrôle des accès utilisateurs.

Depuis la console d'administration, vous pilotez l'ensemble de votre flotte d'entreprise ainsi que les droits d'accès associés, en toute simplicité. En cas d'incident ou de risque identifié, vous avez la capacité d'intervenir à distance sur les terminaux, de révoquer des accès ou de suspendre un compte de manière immédiate, garantissant ainsi la continuité et l'intégrité des opérations.



Les fonctionnalités clés :



- Groupes de discussion sans limite de membres
- Notification ciblées (@nom) et réactions (émojis)
- Diffusion automatisée via des bots
- Chat et partage de fichiers dans des salons chiffrés
- Partage d'écran sécurisé
- Multi-terminaux et navigateurs
- Chiffrement de bout en bout*

*messagerie, appels



Les bénéfices apportés :

- Communication transverse fluide et instantanée
- Sécurité & confidentialité garantie
- Facilité d'usage & adoption rapide
- Synchronisation des terminaux mobiles & PC
- Déploiement simplifié : disponible en SaaS sur un environnement SecNumCloud 3.2 ou Cloud Public