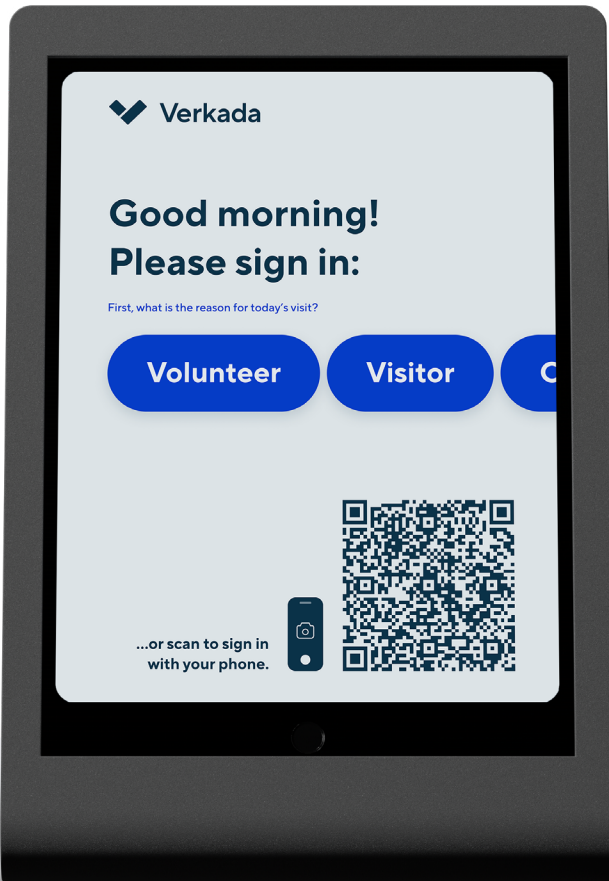


Dispositifs de sécurité Verkada Guest

Un niveau de sécurité supplémentaire pour les établissements scolaires



Présentation

Verkada Guest est un système de gestion des visiteurs qui offre à ces derniers une expérience fluide de leur arrivée à leur départ, tout en renforçant la sécurité du bâtiment.

Basées sur la plateforme Verkada Command, les intégrations natives de vidéosurveillance et de contrôle d'accès de Guest permettent aux administrateurs de visionner les vidéos de l'activité des visiteurs et de déverrouiller à distance les portes pour certains invités. L'impression de badges avec code couleur permet aux employés d'identifier les visiteurs d'un simple coup d'œil.

Pour les établissements scolaires et les organismes dédiés à la jeunesse qui souhaitent mieux surveiller leurs campus et leurs sites, Guest propose une fonctionnalité facultative de vérification des antécédents. Dans Guest, les administrateurs peuvent activer des contrôles supplémentaires qui comparent les antécédents des visiteurs aux registres des délinquants sexuels et aux bases de données criminelles, informant ainsi le personnel des personnes pouvant présenter un risque pour les enfants, les étudiants et le personnel. La vérification électronique des antécédents des visiteurs via Verkada Guest permet aux établissements scolaires et autres organisations de recueillir davantage d'informations afin de mieux contrôler l'accès à leurs sites.

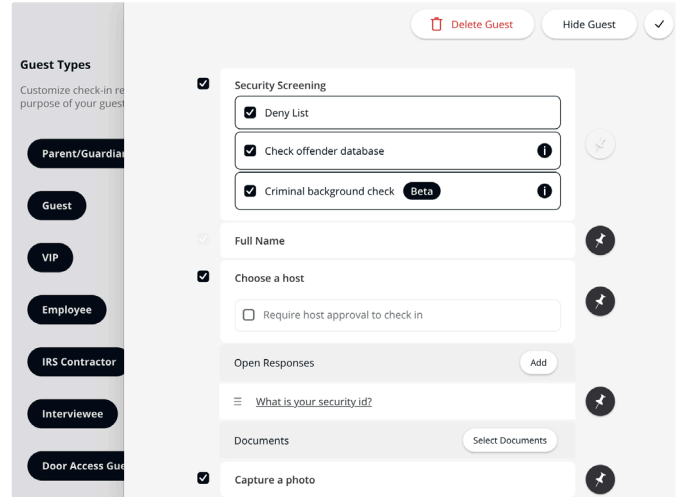


Fonctionnement

Vérification instantanée des antécédents des visiteurs

Facile à mettre en œuvre

Le contrôle de sécurité est une fonctionnalité facile à configurer et à utiliser. Dans Command, l'administrateur Guest ou le gestionnaire de site Guest sélectionne simplement la case à cocher « Contrôle de sécurité » sur un type de visiteur précis (par exemple, « Visiteur », « Parent », etc.) lors de la configuration. De cette manière, certains visiteurs peuvent se voir contrôlés et d'autres non. Les administrateurs peuvent choisir de vérifier les antécédents de ce type de visiteur par rapport aux registres des délinquants sexuels, aux bases de données criminelles ou aux deux. Ils peuvent également choisir d'ajouter des personnes signalées à une liste d'exclusion automatique afin de leur refuser toute nouvelle tentative d'enregistrement à l'avenir.



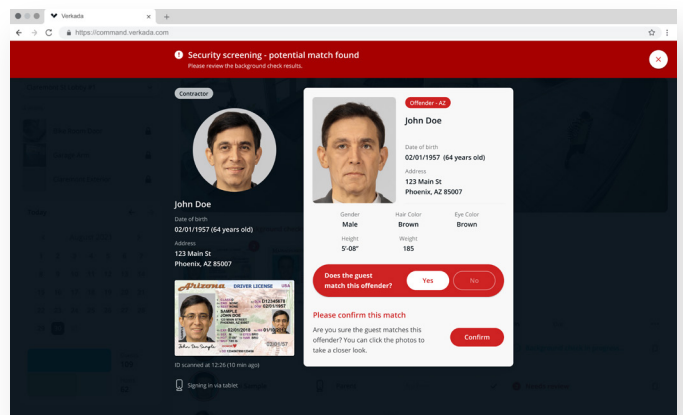
Vérification instantanée des antécédents des visiteurs

Lors de l'enregistrement, les visiteurs sont invités à donner explicitement leur consentement à la numérisation de leur pièce d'identité avec photo. Une fois le consentement donné, le visiteur prend simplement une photo de son permis de conduire ou de sa carte d'identité officielle. Le nom complet et la date de naissance du visiteur sont extraits et envoyés à un fournisseur de bases de données tiers pour effectuer une recherche dans tous les registres des délinquants sexuels des États-Unis, ainsi que dans diverses bases de données criminelles. En quelques secondes, Guest partage les résultats et, en fonction de ces derniers, permet au personnel de la réception d'imprimer un badge ou d'examiner une éventuelle correspondance.



Validation des correspondances potentielles

Pour les visiteurs pour lesquels une correspondance potentielle est reçue, l'interface Guest affiche la photo d'enregistrement et les informations du permis de conduire du visiteur par rapport aux informations reçues. Le personnel de la réception doit confirmer s'il existe bien une correspondance.





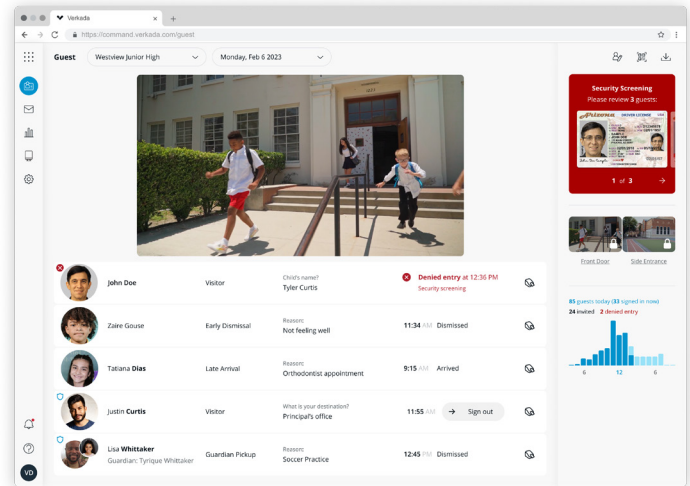
Fonctionnement

Vérification instantanée des antécédents des visiteurs

Entrée refusée aux visiteurs indésirables

En cas de correspondance confirmée, l'interface Guest affiche un message personnalisé à l'intention du visiteur dont l'entrée a été refusée et enregistre le fait que le visiteur s'est vu refuser l'entrée en raison d'une correspondance confirmée. En fonction des protocoles de sécurité des organisations, le personnel de la réception peut ignorer l'entrée refusée et autoriser l'invité à pénétrer dans les locaux. Les visiteurs qui ne passent pas le contrôle de sécurité peuvent être ajoutés à une liste d'exclusion automatique, qui informera immédiatement les administrateurs s'ils essaient de s'enregistrer à nouveau à l'avenir.

Si la photo ou les caractéristiques d'identification du registre des délinquants sexuels ou de la base de données criminelle ne correspondent manifestement pas au visiteur, le personnel de la réception peut confirmer qu'il n'y a pas de correspondance. L'interface Guest imprime ensuite un badge pour le visiteur et l'enregistrement se poursuit normalement. Les visiteurs qui passent le contrôle de sécurité peuvent être ajoutés à une liste d'approbation automatique afin de ne pas avoir à reproduire le processus la prochaine fois. Une fois scannée et examinée par le personnel de la réception, la pièce d'identité d'une personne peut être épinglée à son profil, afin qu'elle n'ait pas à sortir son portefeuille lors de son prochain enregistrement.





Contrôles de sécurité stricts

Préservation de la confidentialité des données

Pour la comparaison des données par rapport aux registres des délinquants sexuels et aux bases de données criminelles des États-Unis :

- Les visiteurs sont invités à donner leur consentement au début du processus de vérification.
- Seuls le nom complet et la date de naissance du visiteur sont extraits de la pièce d'identité via l'API et transmis à un fournisseur de base de données tiers (Checkr) pour effectuer une recherche dans tous les registres des délinquants sexuels des États-Unis.
- Aucune image n'est utilisée à partir des caméras Verkada ou du kiosque Verkada Guest pour effectuer des recherches biométriques dans la base de données tierce.
- Les résultats de la recherche ne sont pas communiqués à d'autres tiers ou à d'autres clients.
- Toutes les communications avec le système sont entièrement chiffrées, au repos comme en mouvement.
- Checkr supprime les informations utilisées pour effectuer la recherche une fois terminée ; les données ne sont pas conservées pendant plus de 24 heures.

Pour les données capturées après l'enregistrement :

- Lorsqu'un contrôle de sécurité n'aboutit à aucune correspondance, Verkada supprime immédiatement les données personnelles utilisées pour effectuer le contrôle, notamment l'image du permis de conduire et la date de naissance.
- En cas de correspondance vérifiée et confirmée par le personnel, les données pertinentes (nom, date de naissance, numérisation de la pièce d'identité) sont conservées dans le système Verkada Guest pendant un maximum de 90 jours, en fonction des paramètres définis par l'administrateur d'organisation du client lors de la configuration. Pour l'immense majorité des visiteurs dont les informations ne correspondent pas, leur nom, leur date de naissance et leur pièce d'identité scannée sont immédiatement supprimés de nos banques de données. Les données ne figurent chez Checkr qu'au maximum 24 heures, période après laquelle elles sont supprimées de leur système.

Pour en savoir plus sur les pratiques de Verkada en matière de confidentialité, consultez la page <https://www.verkada.com/fr/privacy/>.

Pour en savoir plus sur Checkr, le service utilisé par Verkada pour vérifier les antécédents des délinquants sexuels et des criminels, consultez leur site Web [checkr.com](https://www.checkr.com).



Questions fréquentes supplémentaires

Comment fonctionne le dispositif de sécurité ?

Dans Command, l'administrateur Guest ou le gestionnaire de site Guest sélectionne la case à cocher « Contrôle de sécurité » sur un type de visiteur précis (par exemple « Visiteur », « Parent », etc.). Les administrateurs peuvent choisir de vérifier les antécédents de ce type de visiteur par rapport aux registres des délinquants sexuels, aux bases de données criminelles ou aux deux. Le visiteur suit les instructions pour s'enregistrer et, une fois qu'il a donné son consentement, Guest extrait son nom complet et sa date de naissance de son permis de conduire américain et effectue une recherche dans les registres des délinquants sexuels des États-Unis, ainsi que dans diverses bases de données criminelles. Ces recherches sont effectuées via [Checkr](#).

- **Si aucune correspondance n'est trouvée : un badge est imprimé pour le visiteur et l'enregistrement se poursuit normalement.**
- **Si une correspondance potentielle est reçue :**
 - L'interface Guest affiche la photo du visiteur à côté de la photo de la personne figurant dans le registre des délinquants sexuels ou dans la base de données criminelle. - L'opérateur désigné est tenu de confirmer s'il existe une correspondance positive.
- **Si une correspondance potentielle est confirmée :**
 - Une alerte par e-mail et/ou par SMS est envoyée au personnel désigné et le visiteur peut se voir refuser l'entrée.
 - L'interface Guest enregistre également le fait que le visiteur s'est vu refuser l'entrée en raison d'une correspondance confirmée.
- **Si une correspondance potentielle n'est pas confirmée :**
 - Si les photos ou les caractéristiques d'identification ne correspondent manifestement pas à la personne, un administrateur peut déclarer qu'il n'y a aucune correspondance.
 - L'interface Guest imprime ensuite un badge pour le visiteur et l'enregistrement peut se poursuivre normalement.

Le dispositif de sécurité permet-il aux clients de satisfaire aux obligations légales ?

Le dispositif de sécurité est destiné à ajouter un niveau de sécurité supplémentaire aux pratiques existantes d'un client en matière de gestion des visiteurs. Il ne vise pas à répondre à des exigences légales particulières auxquelles un client peut être soumis.

Est-ce que Verkada effectue les vérifications des antécédents des délinquants sexuels et des criminels ?

Non, Verkada s'est associée à [Checkr](#), un fournisseur de bases de données tiers, pour effectuer des recherches dans les registres des délinquants sexuels et dans diverses bases de données criminelles. Checkr regroupe les dossiers provenant des registres des délinquants sexuels des États-Unis, qui incluent les délinquants des niveaux 1, 2 et 3. Pour la vérification des antécédents criminels, Checkr compare les données aux dossiers du US Department of Corrections, aux dossiers des fugitifs, aux dossiers des personnes les plus recherchées par le FBI et aux dossiers d'Interpol.

Quels types de pièces d'identité fonctionnent avec le dispositif de sécurité de Guest ?

Tous les permis de conduire ou cartes d'identité émis par les États-Unis. Les passeports et autres pièces d'identité ne sont pas acceptés. Pour le moment, le réceptionniste ou tout autre membre du personnel désigné par le client ne peut pas saisir le nom complet ou la date de naissance du visiteur.

Est-il nécessaire de procéder à la numérisation de la carte d'identité à chaque fois qu'une personne entre dans le bâtiment ?

Le dispositif de sécurité de Verkada Guest peut être facultatif pour les invités réguliers. Les administrateurs Guest et les gestionnaires de site Guest peuvent configurer Guest pour permettre aux visiteurs réguliers approuvés d'éviter les contrôles de sécurité supplémentaires lors de leurs futures visites en les ajoutant à une liste d'approbation automatique. De la même manière, les visiteurs qui sont signalés et à qui l'entrée est refusée peuvent être ajoutés à une liste d'exclusion automatique.

Les visiteurs doivent-ils donner leur consentement avant de passer le contrôle de sécurité ?

Oui. Avant qu'un visiteur ne partage une photo de sa pièce d'identité, il doit consentir à ce que ses informations soient comparées à celles d'une base de données publique.



Questions fréquentes supplémentaires

Quelles informations sont extraites des permis de conduire par Verkada ?

Verkada numérise les permis de conduire pour extraire le nom complet, la photo, l'adresse et la date de naissance du visiteur. Les données qui sont envoyées à la base de données tierce sont uniquement le nom complet et la date de naissance, qui constituent les informations minimales requises pour contrôler les personnes entrantes. S'il existe une correspondance potentielle, la base de données tierce renvoie le nom complet, la date de naissance, la taille, le poids et l'adresse de la personne concernée afin que la réceptionniste ou tout autre membre du personnel puisse vérifier en temps réel si la correspondance potentielle est avérée.

Qui a accès aux données ? Quel accès aux données les employés de Verkada ont-ils ?

- Les employés d'une organisation peuvent accéder aux données en fonction des rôles et autorisations qui leur sont attribués dans Guest.
Pour en savoir plus sur les rôles et autorisations des utilisateurs Guest, consultez cet article.
- Les employés du service d'assistance Verkada peuvent uniquement accéder aux données sur approbation explicite du client à l'aide de la fonctionnalité « Activer l'accès du service d'assistance » afin de résoudre les problèmes via Command. Les autres employés de Verkada n'ont accès à aucune donnée Guest des clients.

Y a-t-il des frais supplémentaires pour utiliser la fonctionnalité de contrôle de sécurité ?

Non, il n'y a aucuns frais supplémentaires pour activer et effectuer des contrôles de sécurité.

Toute personne issue de l'organisation peut-elle activer cette fonctionnalité ?

Seuls les rôles d'administrateur Guest et de gestionnaire de site Guest peuvent configurer les flux de travail Guest, dont l'activation du dispositif de sécurité. Pour en savoir plus sur les rôles et autorisations des utilisateurs Guest, consultez cet article.

Les contrôles de sécurité sont-ils disponibles en dehors des États-Unis ?

Les contrôles de sécurité sont uniquement disponibles aux États-Unis (y compris à Washington D.C.) et à Porto Rico. Pour les clients en dehors de ces zones géographiques, le dispositif de sécurité ne sera pas disponible dans l'interface utilisateur.

Existe-t-il une limite au nombre de contrôles de sécurité pouvant être analysés ?

Même si Guest propose un nombre illimité d'enregistrements de visiteurs par mois, les contrôles de sécurité sont limités à 1 000 par mois et par organisation cliente. Si vous avez besoin de contrôles de sécurité supplémentaires par mois, veuillez contacter votre représentant.

Pour en savoir plus sur la gestion des visiteurs dans Guest, veuillez nous contacter à l'adresse sales@verkada.com.



Guest

Spécifications techniques

Configuration matérielle et logicielle requise

Configuration matérielle requise

- iPad (avec iOS 14 minimum)
Imprimante d'étiquettes (Brother QL820-NWB, Brother QL1110-NWB, Epson C3500 ou Epson C4000)
Support pour iPad (facultatif, mais recommandé, support iPad Lamicall A1 ou support iPad Lamicall DT03)
-

Configuration logicielle requise

- Téléchargez l'application gratuite Verkada Guest depuis l'App Store
Une licence Verkada Guest valide par iPad
-



Informations relatives à la commande

Tarifs de Guest

Numéro de modèle	Description	Coût (prix de vente conseillé) en USD
LIC-VG-1Y	Licence Guest 1 an	3 600 USD
LIC-VG-3Y	Licence Guest 3 ans	10 800 USD
LIC-VG-5Y	Licence Guest 5 ans	18 000 USD
LIC-VG-10Y	Licence Guest 10 ans	36 000 USD
ACCX-TBL-1	Apple iPad, 10,2 po, Wi-Fi, 64 Go	329 USD
ACCX-PRT-1	Imprimante d'étiquettes Brother, QL-820NWB	249 USD
ACCX-TBL-STD-1	Support pour tablette Stouchi	39 USD