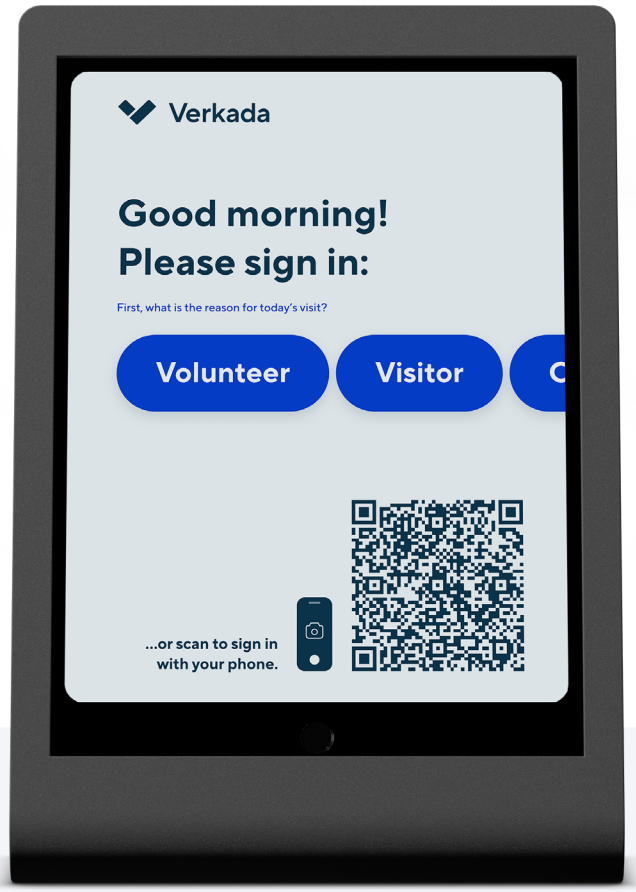
Verkada Guest Security Screens

An Additional Layer of Security for Schools



Overview

Verkada Guest is a visitor management system that provides guests with a seamless experience from arrival to departure, while also strengthening building security.

Built on the Verkada Command platform, Guest's native video security and access control integrations allow admins to review video of visitor activity and remotely unlock doors for specific guests. Color-coded badge printing allows employees to easily identify guests at a glance.

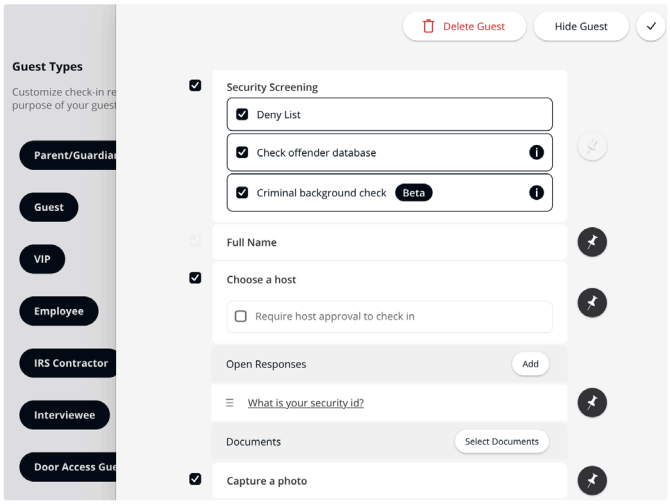
For schools and youth organizations that wish to have greater oversight of their campuses and sites, Guest offers an optional Security Screen feature. Within Guest, administrators can enable additional screenings that compare visitors against sex offender registries and criminal databases, alerting staff to those who may pose a risk to children, students and staff. Electronically screening visitors through Verkada Guest allows schools and other organizations to gather more information to better control access to their sites.

How it works

Screen Visitors Instantly

Easy to implement

The security screen feature is easy to set up and use. In Command, the Guest Administrator or Guest Site Manager simply selects the “Security Screen” checkbox on a specific Guest Type (e.g. "Visitor", "Parent", etc.) upon setup. That way, some guests can be prompted for security screens and not others. Admins can choose to have that visitor type checked against sex offender registries, criminal databases, or both. They can also choose whether to add flagged individuals to an auto-deny list if they try to check in again at some point in the future.

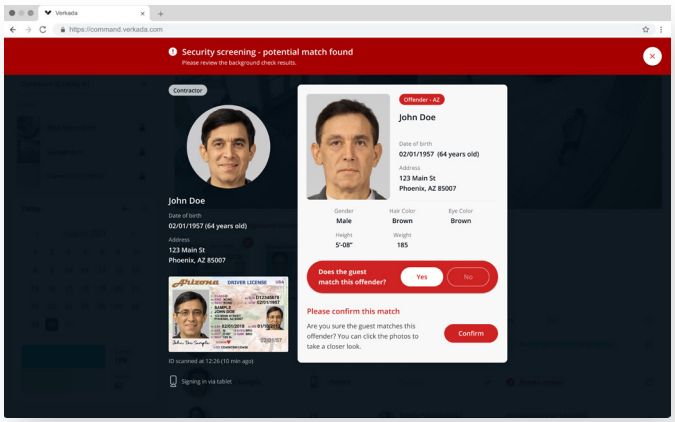


Screen visitors instantly

Upon check-in, visitors are asked to explicitly provide their consent to scan their photo ID. Once consent has been given, a visitor simply takes a photo of their US state issued driver's license or ID card. The visitor's full name and date of birth are extracted and sent to a third party database provider to search all state and local US sex offender registries and various criminal databases for matching records. Within seconds, Guest will share the results and – depending on the results – allow the front desk personnel to either print a badge or review a potential match.

Validate potential matches

For visitors where a potential match is received, the Guest interface will display the visitor’s check-in photo and driver’s license information compared to the information received. The front desk personnel must confirm whether there is a positive match.



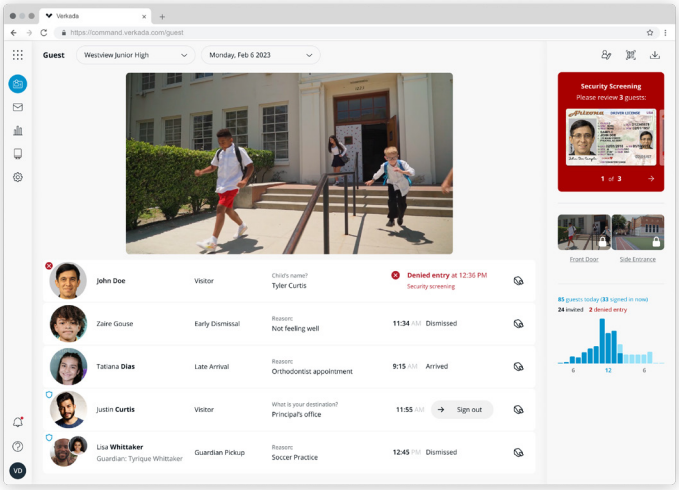
How it works

Screen Visitors Instantly

Deny entry to unwanted visitors

For confirmed matches, the Guest interface will display a custom message to the denied visitor and log that the visitor was denied entry due to a confirmed match. Based on the safety protocols of the organizations, the front desk personnel may override the denied entry and allow the guest to enter the premises. Visitors who do not pass a security screen may be added to an auto-deny list, which will immediately alert administrators if they try to check-in again at some point in the future.

If the picture or identifying characteristics from the sex offender registry or criminal database are clearly not the same person as the visitor, the front desk personnel can validate there is no match. The Guest interface will then print a visitor badge and the check-in will continue as normal. Guests who pass a security screen can be added to an auto-approve list so they will not need to repeat the process next time. Once scanned and reviewed by front desk staff, an individual's ID can be pinned to their profile so that next time they check-in they don't need to pull out their wallet.



Strict security screen controls

Maintain Data Privacy

For data scanned against local and state-level US sex offender registries and criminal databases:

- Visitors are asked to provide affirmative consent at the start of the screening process.
- Only the visitor's full name and date of birth are extracted from the ID via API to a third party database provider (Checkr) to search state and local sex offender registries for matching records.
- No imagery is used from Verkada Cameras or the Verkada Guest kiosk to do biometrics searches within the third party database.
- The results of the search are not shared with any other third parties or across customers.
- All communications to the system are fully encrypted when it transit and rest.
- Checkr deletes the information used to conduct the search once completed; data is not retained for more than 24 hours.

For data captured after sign–in:

- When a background screen has come back without a match, Verkada immediately expunges the personal data used to run the security screen, including driver's license image and DOB unless a customer has configured driver's license images to be saved. If a customer has configured driver's license images to be saved, then they may be retained for up to 90 days, based on settings defined by the customer's Organization Admin.
- In the event of a human verified and confirmed match, the matching data (name, date of birth, ID scan) are retained in the Verkada Guest system for up to 90 days, based on settings defined by the customer's Organization Admin. Data remains with our 3rd party providers for no more than 24 hours, after which it is expunged from their system.

To learn more about Verkada's privacy practices, please visit https://www.verkada.com/privacy/.

To learn more about Checkr, the service Verkada uses to provide sex offender and criminal background checks, please visit checkr.com.

Additional FAQs

How does the Security Screen feature work?

In Command, the Guest Administrator or Guest Site Manager selects the “Security Screen” checkbox on a specific Guest Type (e.g. "Visitor", "Parent", etc.). Admins can choose to have that visitor type checked against sex offender registries, criminal databases, or both. Visitors follow the prompts to check-in and, once they have consented, Guest will extract the visitor’s full name and DOB from their US driver license and search the state and local sex offender registries, as well as various criminal databases, for matching records. These searches are conducted through Checkr.

- **If no match is made: it then prints a visitor badge and check–in continues as normal**
- **If a potential match is received:**
  - The Guest interface will display the photo of the visitor next to the photo of the person on the sex offender registry or criminal database - The designated operator is required to validate whether there is a positive match
- **If a potential match is confirmed:**
  - An alert by email and/or text message will be sent to designated staff and the visitor can be denied entry
  - The Guest interface will also log that the visitor was denied entry due to a confirmed match
- **If a potential match is not confirmed:**
  - If the pictures or identifying characteristics are clearly not of the same person, an administrator can designate that there is no match
  - The Guest interface will then print a visitor badge and check-in can continue as normal

Does the security screen feature enable customers to satisfy legal obligations?

The security screen feature is intended to add an additional layer of security to a customer’s existing visitor management practices. It is not meant to address any particular legal requirements to which a customer may be subject.

Is Verkada performing the sex offender and criminal background scans?

No, Verkada has partnered with Checkr, a third party database provider to search sex offender registries and various criminal databases for matching records. Checkr aggregates records from local and state-level US registered sex offender registries, which includes Level 1, 2 and 3 offenders. For criminal background checks, Checkr will compare against US Department of Corrections records, fugitive records, FBI most wanted records and Interpol records.

What types of IDs will work with Guest’s security screen feature?

All U.S. state–issued driver’s license or ID cards can be automatically scanned to extract the visitor's name and birthdate. Alternatively, the receptionist or other personnel designated by the customer can type in the full name or date of birth of the visitor.

Is an ID card scan necessary each time a person comes into the building?

Verkada Guest allows the security screen feature to be optional for repeat guests. Both Guest Admins and Guest Site Managers can configure Guest to allow approved repeat visitors to avoid additional security screens on future visits by adding them to an auto-approve list. Visitors who are flagged and denied entry can similarly be added to an auto-deny list.

Must visitors give their consent before conducting the security screen?

Yes. Before a visitor shares a photo of their identification, the visitor must consent to having their information screened against a public database.

Additional FAQs

What information is Verkada extracting from drivers' licenses?

Verkada scans drivers' licenses to extract the visitor's full name, photo, address and date of birth. The data that is being sent to the third party database is only the full name and date of birth, which is the minimum information required to screen entrants. If there is a potential match, the third party database returns full name, date of birth, height, weight and address of the match so that the receptionist or other personnel can compare in real-time if the potential match is real.

Who has access to the data? What access do Verkada employees have to the data?

- An organization's employees can access the data based on their assigned roles and permissions within Guest. To learn more about the Guest user roles and permissions, review this article.
- Verkada Support employees can only access the data through explicit approval of the customer using the 'Enable Support Access' feature in order to help troubleshoot issues via Command. Other Verkada employees do not have access to any customer Guest data.

Is there an additional cost for the security screen feature?

No, there is no additional cost to enable and perform security screens.

Can anyone within the organization turn on this feature?

Only the Guest Admin and Guest Site Manager roles can configure Guest workflows, including enabling the security screen feature. To learn more about the Guest user roles and permissions, review this article.

Are security screens available outside of the United States?

Security screens are only available in the United States (including Washington D.C.) and Puerto Rico. For customers outside of these geographies, the security screen feature will not be present within the UI to enable.

To learn more about Guest visitor management, contact sales@verkada.com.

Guest
Tech Specs

Requirements

Hardware Requirements	• iPad (must run iOS14 or above) Label printer (Brother QL820-NWB, Brother QL1110-NWB, Epson C3500, or Epson C4000) iPad stand (optional, but recommend Lamicall iPad Stand A1 or Lamicall iPad Stand DT03)
Software Requirements	• Download the free Verkada Guest app on the App Store A valid Verkada Guest license per iPad

Ordering Information

The Workplace License and Workplace K-12 License include both Verkada Guest and Verkada Mailroom. The Workplace for Government License includes only Verkada Guest. Licenses can be purchased in 1, 3, 5, or 10 year increments.

Workplace License (New/Capacity Increase)

Model Number	Description	Cost per site (MSRP) USD
LIC-WP-1Y-CAP	1-Year Workplace License, Capacity Increase	$3,600
LIC-WP-3Y-CAP	3-Year Workplace License, Capacity Increase	$10,800
LIC-WP-5Y-CAP	5-Year Workplace License, Capacity Increase	$18,000
LIC-WP-10Y-CAP	10-Year Workplace License, Capacity Increase	$36,000
LIC-WP-1Y-CAP-K	1-Year Workplace K-12 License, Capacity Increase	$1,500
LIC-WP-3Y-CAP-K	3-Year Workplace K-12 License, Capacity Increase	$4,500
LIC-WP-5Y-CAP-K	5-Year Workplace K-12 License, Capacity Increase	$7,500
LIC-WP-10Y-CAP-K	10-Year Workplace K-12 License, Capacity Increase	$15,000
LIC-WP-1Y-CAP-G	1-Year Workplace License for Government, Capacity Increase	$5,400
LIC-WP-3Y-CAP-G	3-Year Workplace License for Government, Capacity Increase	$16,200
LIC-WP-5Y-CAP-G	5-Year Workplace License for Government, Capacity Increase	$27,000
LIC-WP-10Y-CAP-G	10-Year Workplace License for Government, Capacity Increase	$54,000

Get started

Verkada Workplace makes it easy to manage visitors and packages in a single dashboard. Visit verkada.com/workplace to start a free 30-day trial today, or contact sales@verkada.com to request more information.

Ordering Information

The Workplace License and Workplace K-12 License include both Verkada Guest and Verkada Mailroom. The Workplace for Government License includes only Verkada Guest. Licenses can be purchased in 1, 3, 5, or 10 year increments.

Workplace License (Renewal)

Model Number	**Description**	**Cost per site (MSRP)** USD
LIC-WP-1Y-CAP	1-Year Workplace License, Capacity Increase	$3,600
LIC-WP-3Y-CAP	3-Year Workplace License, Capacity Increase	$10,800
LIC-WP-5Y-CAP	5-Year Workplace License, Capacity Increase	$18,000
LIC-WP-10Y-CAP	10-Year Workplace License, Capacity Increase	$36,000
LIC-WP-1Y-CAP-K	1-Year Workplace K-12 License, Capacity Increase	$1,500
LIC-WP-3Y-CAP-K	3-Year Workplace K-12 License, Capacity Increase	$4,500
LIC-WP-5Y-CAP-K	5-Year Workplace K-12 License, Capacity Increase	$7,500
LIC-WP-10Y-CAP-K	10-Year Workplace K-12 License, Capacity Increase	$15,000
LIC-WP-1Y-CAP-G	1-Year Workplace License for Government, Capacity Increase	$5,400
LIC-WP-3Y-CAP-G	3-Year Workplace License for Government, Capacity Increase	$16,200
LIC-WP-5Y-CAP-G	5-Year Workplace License for Government, Capacity Increase	$27,000
LIC-WP-10Y-CAP-G	10-Year Workplace License for Government, Capacity Increase	$54,000