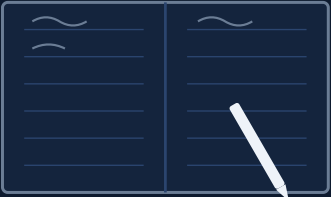


COMPLETE VISITOR MANAGEMENT

Complete visitor management from Knight Watch. Works with your existing access control.

Invitations, a self-service kiosk that runs the NDA, safety video and photo in the visitor's own hands, screening, host alerts, and a pass on their phone or a card from the pool — supplied, installed and supported by Knight Watch.

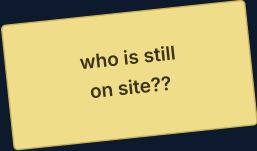
TODAY



the sign-in book at reception



last week's visitor cards, still live



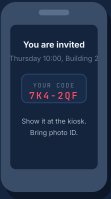
who is still on site??

VISITORS TODAY

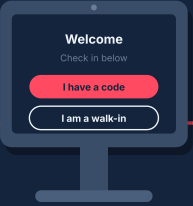


nobody told the host

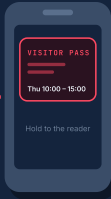
WITH KNIGHT WATCH



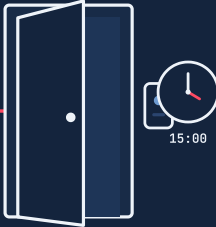
Invited, with a code



Checks in at the kiosk



Pass on their phone



Door opens — off at 15:00

One invitation. One kiosk. A pass that switches itself off.
The host is told the moment they arrive. Nobody has to remember to cancel anything.

Invite. Screen. Badge. Nothing to switch off after.

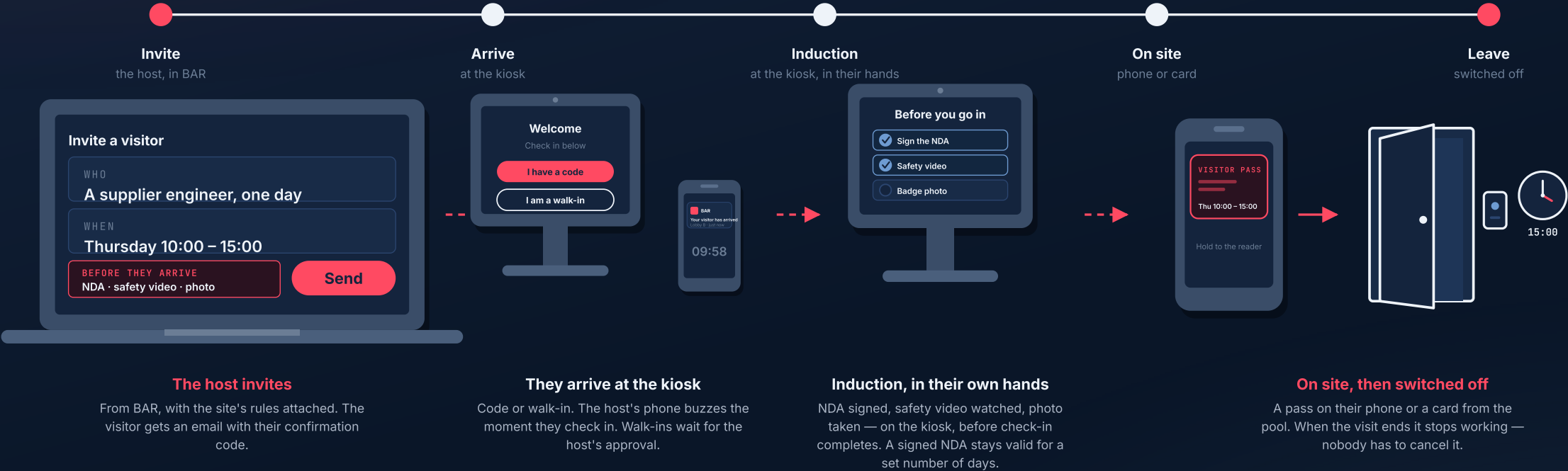
The host sends one invitation; the visitor checks in and completes induction at the kiosk; the pass or card stops working when the visit ends — and every step is written down.

ONE VISIT, START TO FINISH

The host sends one invitation. **BAR** does the rest.

Screening on registration, a reminder an hour before, the kiosk, induction in the visitor's own hands, the host alert, the pass and its expiry.

ONE VISIT, START TO FINISH – YOUR SITE SETS THE TIMES



The host does one thing: send the invitation.

Screening, reminders, the kiosk, the host alert, the pass and its expiry are BAR's job — and every step is written down.

THE FEATURE LIST

Everything the front desk needs. **Nothing you have to replace.**

■ BEFORE THE VISIT

Invitation with a confirmation code

Group and event invites from a list

Visitor types, each with its own rules

Watchlist screening on registration

Host reminded an hour before arrival

■ AT THE KIOSK

Check in by code, or register as a walk-in

NDA and documents signed on screen

Safety video, quiz, declaration, form

Photo capture for the badge

Guest Wi-Fi on the done screen

Works offline, syncs when back

■ THE HOST

Microsoft Entra ID single sign-on

Told by email, text or Microsoft Teams

Told the moment the visitor arrives

Approves walk-ins

Extends a visit that runs over

Sees who is on site right now

■ THE CREDENTIAL

HID Mobile Access, by text at check-in

Apple Wallet or Google Wallet pass (KnightPass)

Pre-encoded pool card from Security Expert

Revoked at check-out

Overdue visitors expired every fifteen minutes

Use-limited cards caught when spent

■ AFTER, AND IN AN EMERGENCY

Check-out at the kiosk or by the host

Everyone on site via Everbridge, when connected

External screening provider, when connected

Every step in the audit record

Visit statistics per site and per event

Scheduled data retention

■ FOR IT

Your infrastructure, database and mail server

Kiosk locked to its site by device token

Address allow-list, lockout on failed attempts

Per-site branding, wording and languages

Security Expert today; others via KnightPass webhook

No visitor app to install

THE CREDENTIAL

Phone or card. **Either dies on time.**

Either

A PASS ON THEIR PHONE, OR A CARD FROM THE POOL

The visitor never handles a credential that outlives the visit. A phone pass carries its own active window and the wallet platform stops honouring it when the window closes. A pool card is assigned at check-in, released at check-out, and a job every fifteen minutes expires anyone still on the books past their departure time and switches their badge off.

- HID Mobile Access, issued from the check-in by text message
- KnightPass – Apple Wallet and Google Wallet, on the WaveLynx Wallet API
- A pre-encoded visitor card from the site's pool, back in the pool at check-out
- Check-out releases the pool card and revokes the mobile credential
- A job every fifteen minutes expires overdue visitors and switches their badge off
- A phone pass carries its own window; the wallet platform stops honouring it

KnightPass is the route running in production today; the other two are built and enabled per deployment.

HID MOBILE ACCESS

Issued at check-in, revoked at check-out. BAR creates the HID Origo user and credential, and the visitor receives their invitation code by text. Built and wired into the visitor flow; enabled per deployment once your own HID Origo tenant is configured. Not yet running in a production tenant.

KNIGHTPASS

A visitor pass with an active window, from five minutes to thirty days. Provisioned into Apple Wallet or Google Wallet through the WaveLynx Wallet API by a link sent as a QR code, email or text. Running in production today on Knight Watch's own AWS account.

THE POOL CARD

A real card, already encoded, that belongs to the site. At check-in BAR takes one from the Security Expert visitor pool and assigns it; at check-out the card goes back. Usage counts sync from the platform every five minutes, so a card limited to a number of uses is caught the moment it is spent.

YOUR ACCESS CONTROL

The experience is platform-agnostic. The last step is not. Invitation, screening, kiosk, host alerts and the pass itself do not care what you run. Writing the credential to a door does: BAR drives Schneider Electric EcoStruxure Security Expert today, and KnightPass pushes provision, suspend and delete to any platform through its webhook adapter. Anything else is a scoped driver, not a setting.

HOW YOU BUY IT

Where it fits, and how to start.

30 min

ONE VISITOR, INVITATION TO EXPIRED PASS, IN YOUR LOBBY

We walk one visitor from the host's invitation to the pass switching itself off — on your access control, with your NDA and your safety video — then scope the rest: which lobbies get a kiosk, which visitor types need what, and which credential your readers can take.

- Assessment: your lobbies, your visitor types and their requirements, your readers
- Pilot in one lobby, with Knight Watch supplying, installing and servicing the kiosk
- Rollout lobby by lobby; hosts sign in with Microsoft Entra ID, visitors never need an account
- Runs on infrastructure you control, with your own database and mail server
- Support coverage set in the agreement you sign

Status, plainly: KnightPass runs in production on Knight Watch's own AWS account; the visitor flow has been walked end to end against a live Security Expert system and the kiosk is built, not yet at a customer. No uptime figure or response-time promise appears in this material.

THE KIOSK

Knight Watch supplies, installs and services the kiosk. The software keeps working when the network does not — check-ins and sign-outs queue on the device and sync when it is back — and is branded, worded and languaged per facility. Each kiosk is locked to a facility with its own device token and address allow-list.

SCREENING AND ALERTS

Every registration is screened against your watchlist. An external screening provider can be connected where your policy requires one. Hosts are told by email, text or Microsoft Teams when a visitor registers, is an hour away, arrives, checks out or expires. Everbridge can be connected to reach everyone on site in an emergency.

WHO BUILDS IT

An integrator, not a software house. Knight Watch installs and services access control systems. The people who wrote the check-in know what a visitor card does at the panel — which is why the card comes from a pool the platform already trusts.



SEE IT ON YOUR OWN LOBBY

Book a thirty-minute demo. We will walk one visitor from invitation to expired pass — and tell you plainly what would have to be built for your access control.
knightwatch.net