FULL BROCHURE

Bring your Paxton Net2 Access Control System to the Next Level with Integration and Automation with **Auxilium Software**

AUXILIUM

OVERVIEW

Auxilium Software provides internally hosted applications that automate user management, ID Card production, and access-control synchronisation through direct integration with Paxton Net2.

Our design principle is to let Paxton Net2 perform its intended role – a proven access-control platform – while **Auxilium Software** extends its capability with automation, workflow logic, and structured data integration.

Paxton manages door control, permissions, and event logging; Auxilium manages data movement, user onboarding, reporting, and process control.

The system links organisational data sources such as HR systems, MIS, SQL databases, or API data feeds directly with Net2.

Users, tokens, and access levels are created, updated, or revoked automatically, keeping all connected systems synchronised.

Each deployment is hosted within the client's chosen environment – on-premises or private cloud – using standard browsers for access and role-based security.

PAXTON NET2 INTEGRATION

Integration uses the Paxton Net2 API, enabling two-way, real-time data exchange between Auxilium services and Net2.

Supported functions include:

- Automatic creation, update, and removal of users from HR/MIS feeds.
- Assignment of departments, access levels, and time zones by role or site.
- Population of Net2 fields such as Employee Number, Start/End Dates, Vehicle Registration, Notes, etc.
- Automatic disabling of leavers detected in upstream data feeds.
- Synchronisation across multiple Net2 servers for large or distributed estates.

Each user is given a unique identifier mapped directly to the Net2 User ID.

If the Auxilium layer is temporarily offline, Net2 continues functioning independently; data is resynchronised automatically once connectivity resumes.

Fig 2.1 – Net2 Integration Data Flow

ID CARD PRODUCTION

The ID Card Production System provides end-to-end control of badge issuance linked directly to Net2.

It operates via a secure internal web interface. Workflow:

1. New staff detected in data feeds appear in a pending list.
2. The system emails a secure link to each user.
3. User completes a web form (department, job title, photo upload).
4. Photo is automatically checked for lighting, background, and size.
5. Optional document/likeness verification (§ 4).
6. Security reviews, approves, or rejects submission.
7. Approved record enters the "Ready for Print" queue.

Printers are network-connected and require no host PCs. Cards can be printed at any authorised location.

When printed, the user's details, photo, and token information are written into Paxton Net2 through the API, activating the credential immediately.

Fig 3.1 – ID Card Workflow

TEMPORARY BADGE SYSTEM

If a user forgets their ID card, a temporary pass can be issued from reception or the security desk. When the operator searches for the user by name, the system displays the individual's photograph on screen for identity confirmation before the pass is released.

The temporary pass:

- Is re-usable stock that can be reassigned after return.
- Grants the same access levels as the user's standard card.
- Automatically blocks the original card until the temporary one is returned.
- Remains active for one day only to discourage retention.

When the user returns the pass, the operator re-enables the original card with a single action. All issues and returns are time-stamped and logged for audit.

This ensures users can continue working safely even if a card is misplaced, while maintaining full safeguarding and accountability within Paxton Net2.

Fig 3.2 – Temporary Badge Issue and Return Screens

IDENTITY AND DOCUMENT VERIFICATION

Users may be asked to upload a government-issued photo ID (passport or driving licence) alongside their portrait.

The verification module:

- Confirms the ID document is authentic and legible.
- Performs facial comparison between the document image and user photo.
- Checks exposure, alignment, and background quality.

All processing is handled through an embedded facial-comparison and document-analysis API. Verification results appear in the Security Dashboard for review.

Temporary data is deleted automatically after verification according to site retention policy.

Fig 4.1 – Document Verification and Approval Interface

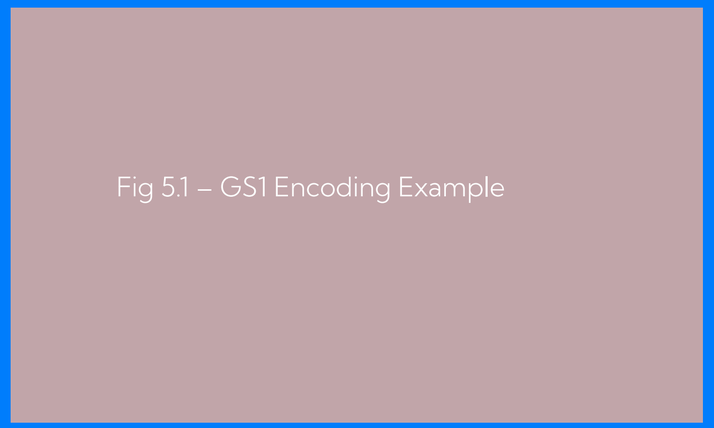
GS1 COMPLIANCE AND DATA STANDARDS

Auxilium Software supports full GS1 UK compliance for staff-ID and barcode structures.

Cards can include Global Service Relation Numbers (GSRNs) and other Application Identifiers (AIs) such as (8017), (8019), and (98).

Identifiers can differentiate permanent staff, agency staff, and contractors while remaining compatible with GS1-aligned scanners and document-tracking systems.

The platform automatically constructs compliant GS1 strings from HR or MIS data, ensuring interoperability across healthcare and enterprise environments.



DUAL-FREQUENCY ID CARDS

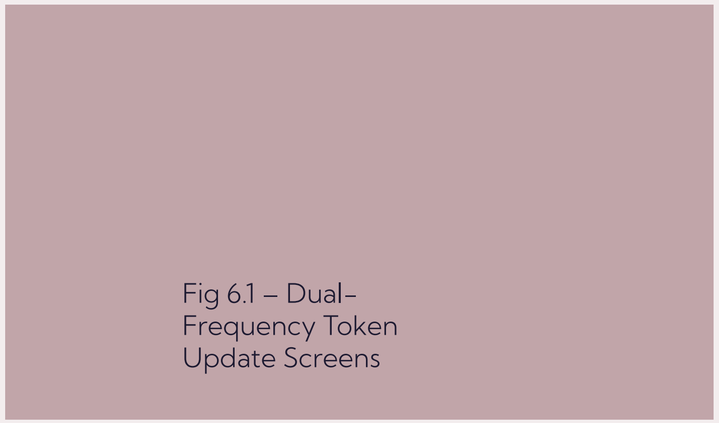
Auxilium systems support dual-frequency ID cards combining 13.56 MHz (MiFare/Smart) and 125 kHz (Paxton Prox) on one card.

Both credentials are encoded in a single print operation with no operator change or extra step.

When issued, token data from both frequencies is captured and written into Paxton Net2 via API. This allows mixed-reader environments – legacy 125 kHz and modern 13.56 MHz – to function seamlessly using one credential.

Multiple Net2 instances can receive the same token pair simultaneously.

Benefits include reduced card stock, simpler migration to newer technologies, and consistent credential management across sites.



VISITOR AND CONTRACTOR MANAGEMENT

Visitor and contractor handling uses the same database model as permanent users, providing consistent monitoring and reporting within Paxton Net2.

Visitors, contractors, and temporary staff can be registered in advance via a secure web form or entered on arrival by reception or security.

Details such as name, company, contact information, vehicle registration, and visit purpose are captured within the local database.

Documentation and Site-Compliance Verification

The system allows supporting documentation to be uploaded to confirm an individual's authority or readiness to work on site. Examples include:

- Proof of qualification, certification, or permit (e.g. CSCS card, insurance document).
- Signed induction forms or competence records.
- Digital sign-off for acceptance of site terms and conditions, including:
  - Acknowledgement of health-and-safety policy.
  - Confirmation of viewing a mandatory induction or fire-safety video.
  - Agreement to PPE, lone-working, or evacuation rules.

Uploaded items are linked to the person's record and stored only for the defined validity period.

Access credentials are not issued until all required uploads and declarations are complete, ensuring compliance before entry.

Badge and Access Control

- Temporary access levels and expiry dates applied automatically.
- Passes printable on thermal or full-colour printers.
- Credentials automatically disabled in Paxton Net2 at expiry.
- Unreturned passes automatically blocked after a defined period.

All actions – creation, document upload, approval, printing, activation, and deactivation – are logged and time-stamped.

This ensures only verified and compliant individuals gain access while maintaining a complete audit trail of visitor, contractor, and temporary-staff activity.

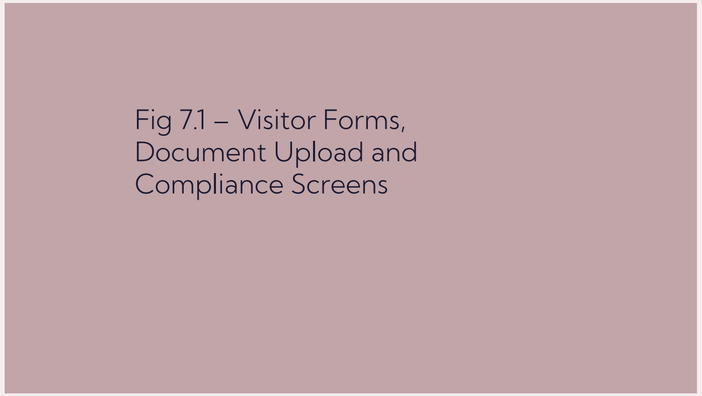


Fig 7.1 – Visitor Forms, Document Upload and Compliance Screens

REPORTING AND NOTIFICATIONS

Auxilium extends Paxton Net2 reporting with integrated SQL queries and a web-based dashboard. Example Reports:

- Active users by department or site.
- Contractors / visitors currently on site.
- Cards expired or unused within a defined period.
- Access attempts outside authorised hours.
- Doors held open, forced, or alarmed.
- Event frequency by area for compliance review.
- Door Health Status
- Access attempts with no authorisation.

Reports can be exported (CSV/Excel) or emailed on schedule.

Real-time alerts notify operators of invalid access, alarms, or flagged user arrivals.

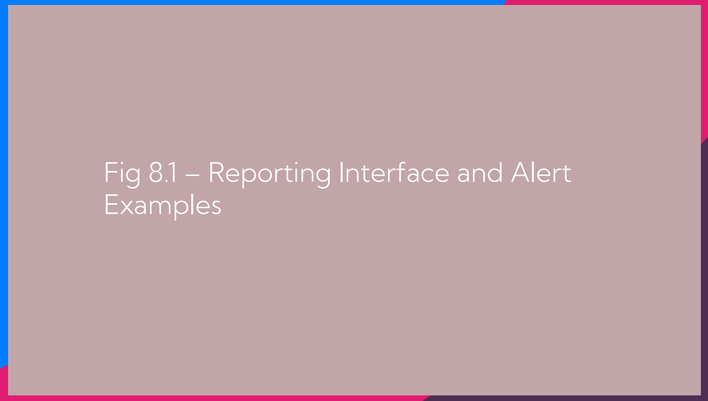


Fig 8.1 – Reporting Interface and Alert Examples

SYSTEM ARCHITECTURE

A standard installation includes:

- Web Application: Apache Tomcat service hosting the interface.
- Database: Microsoft SQL Server for user, event, and configuration data.
- Integration Service: Secure API link to Paxton Net2.

Peripheral Services: Network print and reader modules. Security Features:

- Role-based access (Administrator, Operator, Approver, Viewer).
- Optional Active Directory SSO.
- Encrypted inter-service communication.
- Comprehensive event logging for audit.

All modules operate within the organisation's controlled environment – on-premises or client-hosted cloud – and integrate with existing backup and monitoring policies.

Fig 9.1 – System Architecture Diagram

SCALABILITY AND MULTI-SITE OPERATION

For large or distributed organisations, the platform supports multi-server and multi-instance deployment.

Architecture Example:

- Multiple HR/MIS feeds imported into separate SQL databases.
- Each database linked to a dedicated Tomcat instance.
- Each Tomcat instance connected to one or more Paxton Net2 servers.

Through multi-server and multi-instance configuration, **Auxilium Software** can mask the 200 IP-node limitation of a single Paxton Net2 system.

By running several Net2 instances under one unified web interface, administrators can manage large estates without fragmenting data or workflows.

Many clients choose multiple Net2 instances for good housekeeping – for example, one site per instance – while maintaining a single integration layer and consolidated reporting.

Structured dataflows ensure that user additions, changes, and deletions replicate automatically to every relevant instance.

Fig 10.1 – Multi-Instance Topology

SUMMARY

Auxilium Software's integration platform combines automation, structured dataflow, and credential management with the reliability of Paxton Net2.

The system automates user lifecycle management, ID Card production (including temporary-badge control), dual-frequency encoding, GS1 identifier generation, visitor compliance, and detailed reporting – all within the client's chosen hosting environment.

Our approach ensures Paxton Net2 remains focused on access control, while Auxilium Software provides the automation and data intelligence around it.

The multi-server / multi-instance architecture removes the 200 IP-node limitation, enabling enterprise-scale estates to be managed from a single web interface.

Each Net2 instance retains its own database for resilience and audit separation, yet all are unified through shared dataflows, automated synchronisation, and centralised reporting.

The result is a scalable, maintainable, and auditable solution adaptable to any operational structure – from a single building to a nationwide network – without altering the core simplicity of the Paxton Net2 system.

DATA HANDLING AND PRIVACY

Auxilium Software systems are built around security, flexibility, and compliance.

All processing, storage, and communication follow the client's network policy and resilience plan.

Deployments may be on-premises, client-hosted private cloud, or hybrid, according to IT strategy and cyber-security posture.

Data Flow and Storage

- User data resides in the client-controlled SQL database (local or cloud).
- Inter-service communication is encrypted.
- Temporary image/document data is deleted after verification.
- Audit logs of all actions are retained per policy. Data Protection and Retention

Data Protection and Retention

- Operates under UK Data Protection Act and UK GDPR principles.
- Processes only information required for operation.
- Retention and purge schedules configurable per governance policy.
- Administrative access role-controlled with full audit trail.

Authentication and Access Control

- Supports Active Directory integration and SSO.
- Distinct roles for operator, administrator, and auditor.
- All actions time-stamped and stored in tamper-evident logs.

EXTERNAL CONNECTIVITY (OPTIONAL)

For web-based visitor registration or off-site submissions, a **DMZ gateway** can be deployed to temporally hold data before secure transfer into the internal or cloud system.

No continuous external exposure occurs.

Client Network Policy and Resilience

Each installation aligns with the client's hosting, redundancy, and recovery design.

Auxilium Software does not impose a network model; it integrates with the organisation's cyber-security framework to maintain reliability while supporting architectural flexibility.

Compliance and Governance

The data-handling framework supports NHS Digital, ISO 27001, and ISPS audit environments. Each deployment includes data-flow diagrams, retention schedules, and defined administrator responsibilities to ensure transparency and accountability from data creation through deletion.

auxilium.software
hello@auxilium.software