

CUSTOMER CASE STUDY

Standardising equipment access across hundreds of shared facilities

About Powerfleet

Powerfleet is a global leader in the artificial intelligence of things (AIoT) software-as-a-service (SaaS) mobile asset industry. With more than 30 years of experience, Powerfleet unifies business operations through the ingestion, harmonisation, and integration of data, irrespective of source, and delivers actionable insights to help companies save lives, time, and money. Powerfleet's ethos transcends our data ecosystem and commitment to innovation; our people-centric approach empowers our customers to realise impactful and sustained business improvement. The company is headquartered in New Jersey, United States, with offices around the globe.

REGIONS

United States, Canada and Mexico

BUSINESS & INDUSTRY

Contract logistics / Supply chain management, warehousing and distribution

OPERATIONAL FOOTPRINT

Hundreds of facilities and properties

WORKFORCE

30%+ annual equipment-operator turnover

SOLUTION DEPLOYED

Warehouse IoT Enhanced Access Control (EAC)

AIMS

Standardise equipment access, align authorisation with certifications and cost centres, and enforce equipment-specific proficiency requirement

RESULTS

Consistent equipment access across business lines | Access updates as certifications and cost centres change | Proficiency policies enforced consistently

Background

A large pure-play contract logistics provider operates hundreds of facilities and properties across the United States, Canada, and Mexico, specialising in outsourced supply chain management, warehousing, distribution, and reverse logistics.

Across the organisation, businesses spanning last-mile transportation, warehousing, and third-party logistics operate with different processes and systems.

Multiple business lines and cost centres frequently share the same facility, and sometimes the same floor space, creating a complex environment for managing equipment access consistently.



Challenge

Equipment access rules varied by business line, facility, and manager, while **annual equipment-operator turnover exceeded 30%**, making certification rosters and access rights difficult to keep current.

The challenge was compounded by a wide range of material handling equipment, each with different training and proficiency requirements.

The organisation needed equipment access to reflect the operator's business assignment, current qualifications, and the requirements of the specific equipment being used.



● The solution

Warehouse IoT Enhanced Access Control created a consistent workforce authorisation model by linking operator identity, organisational information, and qualification data to equipment access.



Operator- and cost-centre-based authorisation

Operator identity and cost-centre data are configured directly in Warehouse IoT, creating a single source of truth for who should have access to what. Equipment access can be automatically scoped to authorised departments, even when multiple business units share the same site.



Automated updates and offboarding

Operator competency and certification transcript data are ingested automatically each morning before the shift starts. Optional HRIS integration can also suspend manager and operator accounts as soon as an offboarding action is triggered and confirmed.



Certification and competency controls

Specific competencies and certifications can be assigned by operator and equipment type, including make, model, and year, so equipment access reflects current qualifications.



Equipment-specific proficiency

Minimum login and usage proficiency policies can be applied by operator and equipment type, make, model, and year, allowing proficiency requirements to be enforced consistently across sites.

The Results

Enhanced Access Control standardised equipment access across hundreds of facilities, multiple business lines, and shared floor space.

Operator identity, cost-centre, and qualification data now provide a consistent workforce authorisation model, with equipment access automatically updated as certifications and cost-centre assignments change.



Consistent access across shared operations

Equipment access is automatically scoped by business unit, even where multiple operations share the same floor space.



Access that keeps pace with workforce change

With annual operator turnover above 30%, EAC reduces the need to manually reconcile certification rosters and equipment access across business lines.



Equipment-specific proficiency at scale

Login and usage proficiency policies can be enforced by operator and by equipment type, make, model, and year – consistently across sites.

KEY PROOF POINTS

HUNDREDS OF FACILITIES



A consistent equipment access model across shared operations.

30%+ ANNUAL OPERATOR TURNOVER



Access updates as certifications and cost-centre assignments change.

EQUIPMENT-SPECIFIC POLICIES



Proficiency requirements enforced by operator and equipment type, make, model, and year.

Customer perspective



"We run multiple business lines – warehousing, transportation, reverse logistics – often out of the same four walls. Before EAC, keeping equipment access aligned with the right cost centre and the right certifications across all of that was a constant manual juggling act. Now access configures itself based on who people are and what they're certified for, no matter which business unit they're supporting that day."

— VP of Safety & Operations, Multi-Business Contract Logistics Provider



Conclusion

Warehouse IoT Enhanced Access Control gives this contract logistics provider a standardised workforce authorisation model across shared operations, keeping authorisation aligned with operator identity, cost-centre assignment, certification, and equipment-specific proficiency requirements.