Access Control and Tracking

User Guide

Fresh USA, Inc.
English US
Version 2.7
November 24 2026

Learn to connect readers, register tags, manage zone access and manual movements, review reports, take access payments and run mobile inventory. Screenshots follow Original DEMO; Working uses your own authorized data and configured devices.

Note Software and documentation are supplied AS IS and AS AVAILABLE under the accepted Fresh USA EULA. Contact Fresh USA for customizations, integrations or additional functionality.

Support fresh@fresh222.com
Sales and licensing order@fresh222.com
+1 (312) 312-9608
www.fresh222.com | software.fresh222.com

Contents

01 Your workspace and Original Demo 3

02 Install and sign in 4

03 Activate the computer license 5

04 Prepare reader connections 6

05 Configure and reconnect readers 7

06 Create zones and assign checkpoints 8

07 Register people vehicles and assets 9

08 Search and edit a record 10

09 Set validity access and tag protection 11

10 Use Dashboard for manual movement 12

11 Review activity save reports and print 13

12 Configure time tracking and notifications 14

13 Issue return and protect equipment 15

14 Respond to alarms and connection notices 16

15 Connect Square once 17

16 Set rates and take an access payment 18

17 Reconcile cancel and refund payments 19

18 Run category based mobile inventory 20

19 Manage categories fields and data exchange 21

20 Back up troubleshoot and contact support 22

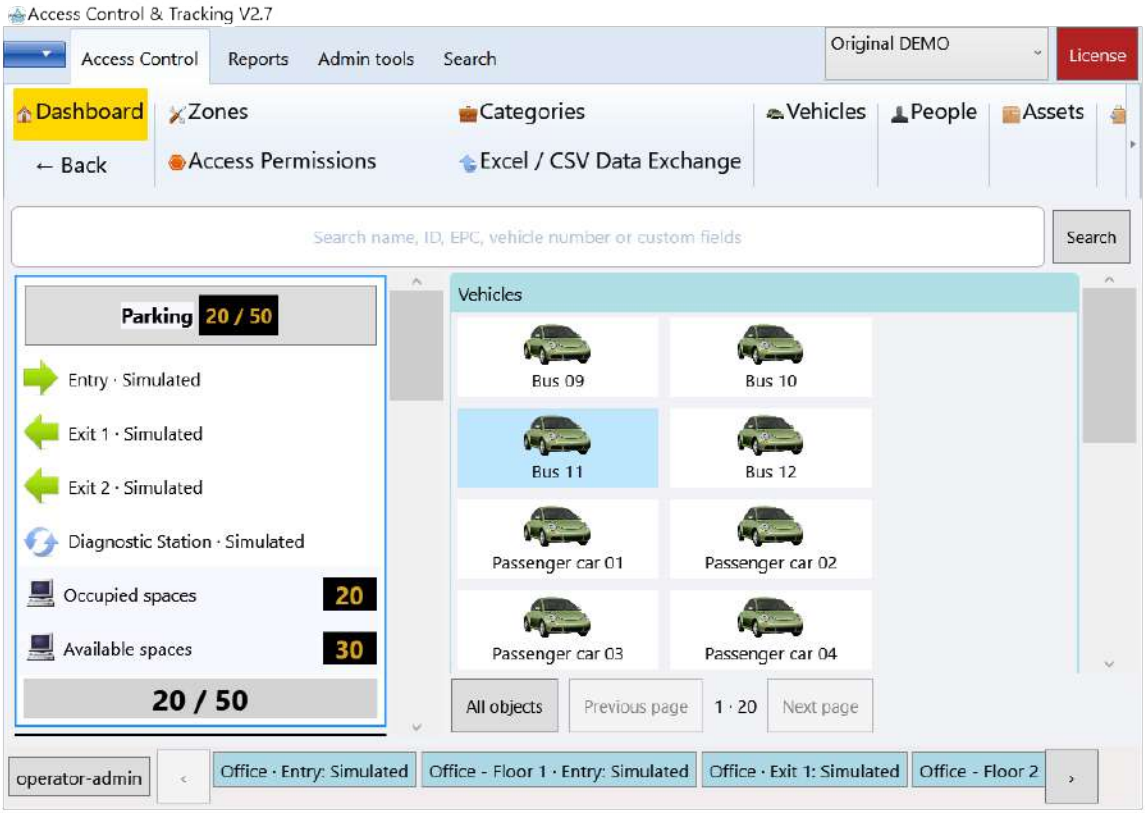
Use the chapter links in Word. Original DEMO is a separate practice workspace with fictional records. Screens can vary with your language, permissions, license, package and saved configuration.

1 Your workspace and Original Demo

Fresh USA Access Control & Tracking manages tagged people, vehicles and assets, their access, movements, time and operational history. This guide follows Original DEMO so you can learn with sample records before configuring your own Working database.

Payment terminals from other manufacturers may be integrated subject to compatibility and commissioning. Square is the example in this guide. Contact Fresh USA about connecting another POS system or terminal.

DEMO and Working are separate workspaces. DEMO uses sample events and virtual readers; it does not charge a Square account or operate a physical relay. Working uses your database, permissions, licensed devices and configured hardware.



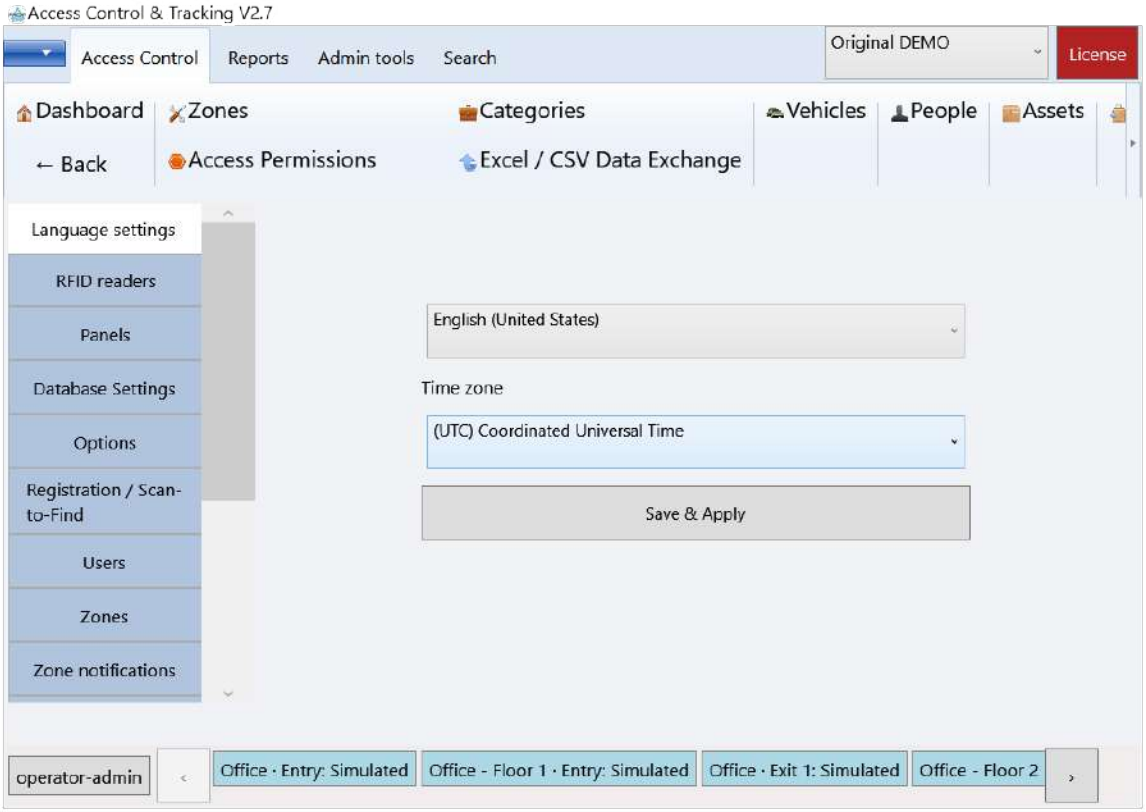
Original DEMO opens with zones on the left and the selected zone's objects on the right.

1. Choose Original DEMO in the scenario selector at the upper right, or in Admin tools > Settings > DEMO. Both selectors show the same choice.
2. Select a zone on the left to see its objects. Use All objects to browse beyond one zone.
3. Use the ribbon for categories and reports. Dashboard returns to the overview; Back returns to the preceding view.

Note Reset this DEMO creates a fresh sample workspace and preserves its previous database. Switching scenarios does not merge their records into Working.

2 Install and sign in

Use the installer supplied by Fresh USA for your licensed version of Access Control & Tracking. Close the application before updating. Keep your existing installation folder and database unless Fresh USA has supplied a separate migration plan.



Settings keeps device, database, user and operational configuration together.

1. Run the setup EXE, approve the Windows prompt, read the license agreement and accept it if you agree.

2. If SQL Server is already configured for this installation, choose the existing-server option. Do not install another database engine merely because you are updating the application.

3. For a new standalone site, follow the local SQL option included in your package. Review any Microsoft prerequisite terms shown by setup. On LAN installations, use the SQL server and secure connection details supplied by your administrator.

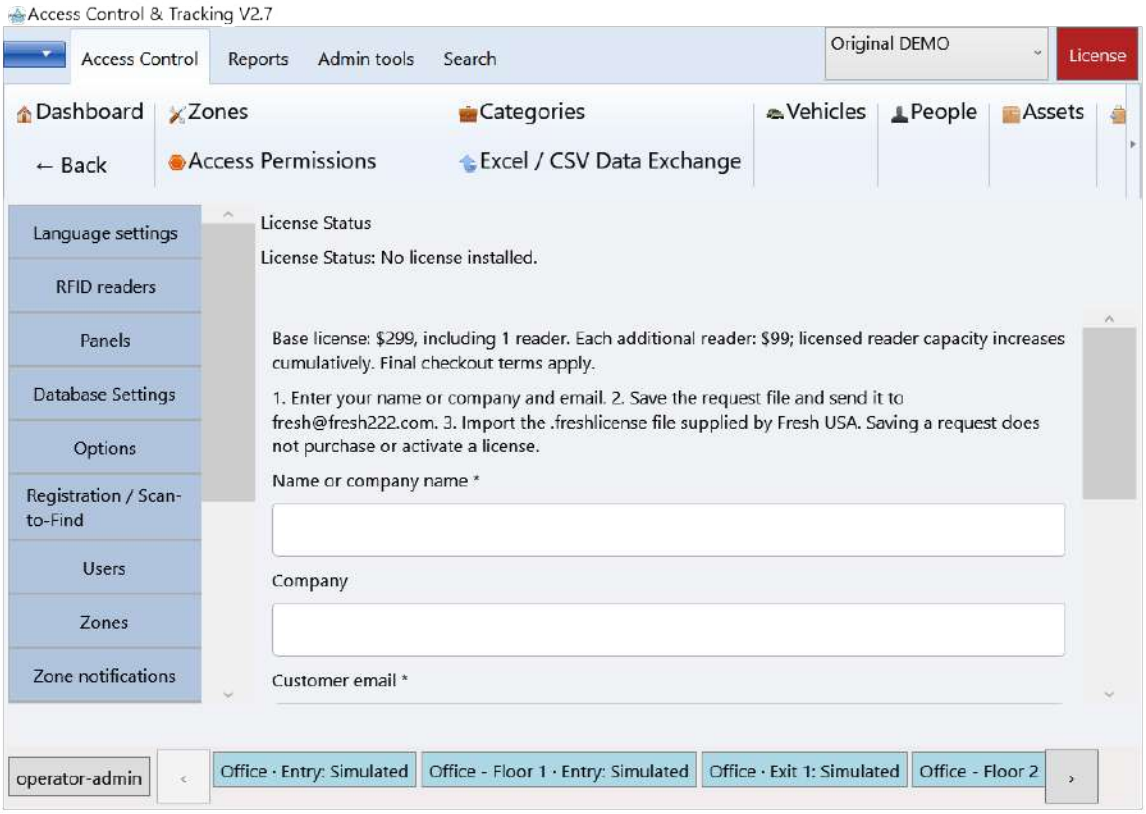
4. Launch Access Control & Tracking and sign in with your assigned account. If Continue with Windows is supplied in an authorized hardware-test package, use it only for that package's existing local workspace.

5. Confirm that you opened the intended Working or DEMO workspace. Set your language and display time zone in Settings, then Save & Apply.

Note An update should preserve records, events, settings and licenses. Keep a verified backup before updating. Do not delete a database or create a replacement account to work around a sign-in error.

3 Activate the computer license

A license request identifies the product and computer; saving it does not itself activate a license. Access Control & Tracking uses Fresh USA's signed license-file workflow. A Smart Control license is a different product entitlement.



The license page provides the request and import actions for ordinary customer packages.

1. Open the license page from the license control at the upper right or from Settings > License.

2. Enter your customer name and email. Enter your company if applicable.

3. Click Save license request file. Choose a folder you can find again, such as Documents, and save the .freshrequest file. Check the confirmation for the full saved path.

4. Send the request to Fresh USA at fresh@fresh222.com, including your order reference and required number of readers. Keep private signing keys and passwords on the issuer's computer.

5. When Fresh USA returns your .freshlicense file, click Import Offline License and select it. Review the resulting license status and allowed reader count.

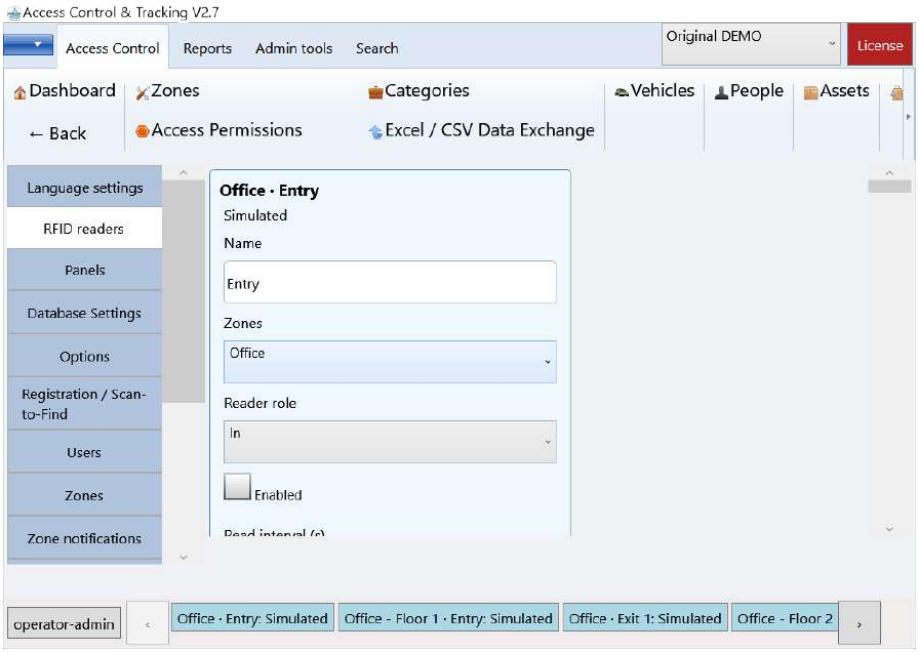
6. For more readers, request the required new total for the same computer. Import the updated signed license supplied by Fresh USA.

Note Customer packages and hardware-test packages have different license displays. Online code activation is shown only when the publisher has configured it. For a purchase or entitlement question, contact order@fresh222.com.

4 Prepare reader connections

Prepare network readers before adding them to the application. Give each TCP/IP reader its own IP address and, for a simple site plan, a distinct TCP port. Enter those exact device settings in Access Control & Tracking. Fresh USA provides a separate reader network-configuration utility free of charge; ask Fresh USA for the correct utility for your hardware.

A powered reader or a lit router LED does not establish an application connection. The saved profile, reachable network endpoint, compatible driver and exclusive use of the device must all be correct.



Reader settings show saved profiles. In Original DEMO these are virtual checkpoints.

Example device	Connection example	Purpose
F-02	USB / COM 3	Registration and lookup
F-920	192.168.1.190 : 6000	Assigned access or security point
F-950	192.168.1.195 : 6005	Assigned monitoring or access point

1. Keep the PC and readers on the intended LAN. Verify each reader's IP, port and model with your site plan.

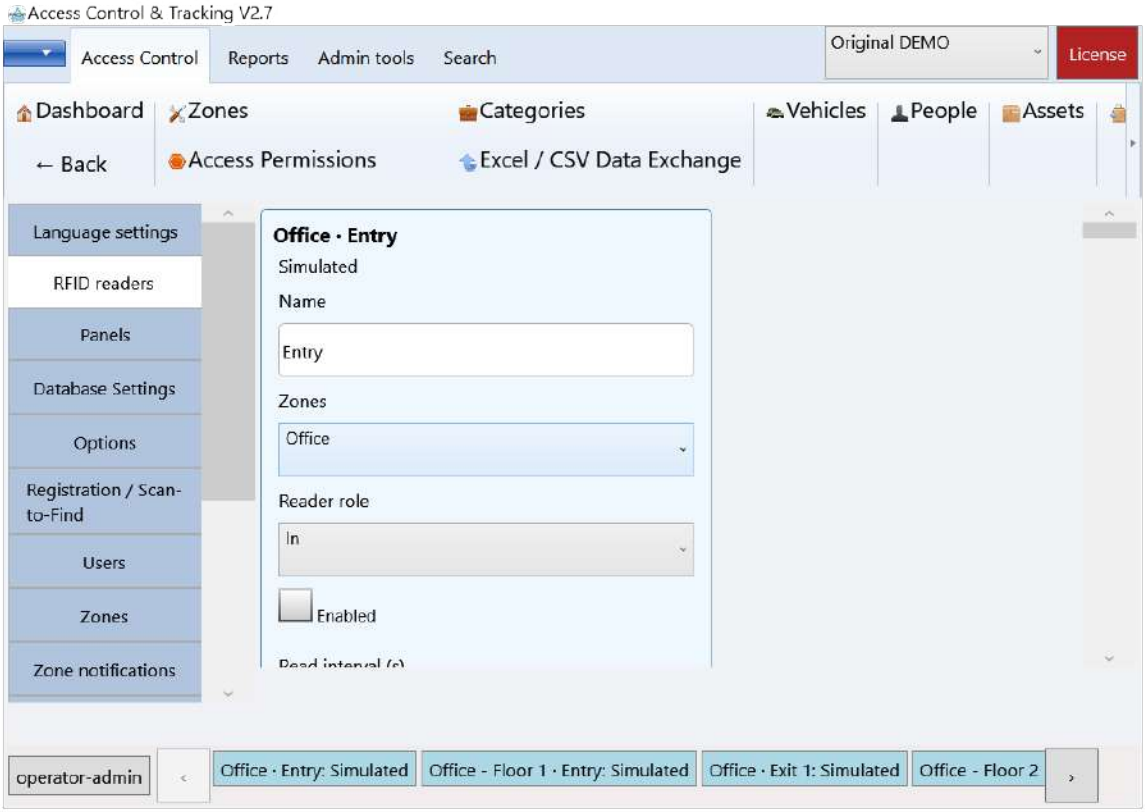
2. For USB/COM, use Windows Device Manager to identify the current port number. Install the approved driver from your supplied package when required.

3. Close other RFID programs that could own the same TCP endpoint or COM port. Add each reader in Settings > RFID readers and save it before assigning a zone.

Note Addresses above are examples, not settings to copy blindly. The router address is not a reader address. No baud-rate entry is required in the normal interface.

5 Configure and reconnect readers

Configure each physical device once with its actual model and transport. Use clear names such as Parking Out or Office In. The footer shows reader names and their current On/Off connection state. A saved Enabled setting and an actual connection are different things.



Each saved reader has its own connection and operational settings.

1. In Working, open Settings > RFID readers and add or edit the reader. Select its supported model and TCP/IP or COM/USB connection.

2. For TCP/IP, enter the actual IP and TCP port. For COM, use the Windows port number shown for the connected device.

3. Use Save & Connect or Save & Apply as shown. Confirm a live connected status. Read power when you need to inspect the supported transmit-power value; change power only according to your commissioning plan.

4. Configure the reader's sound and relay options where supported. Pulse and delay define how a permitted relay command runs; they do not establish a zone assignment.

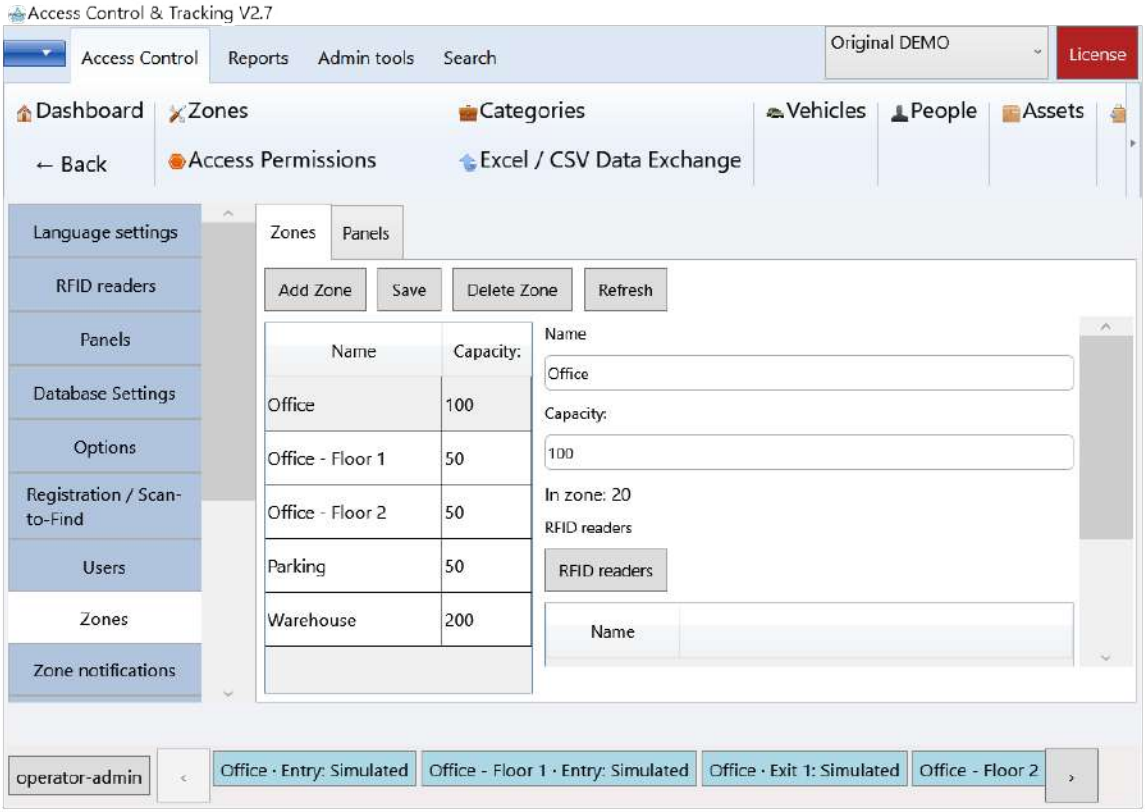
5. Use Repeat connection-loss reminder every minute to turn repeated reminders on or off for that reader. This preference does not disable connection recovery.

6. Keep the desired profiles enabled. Authorized readers reconnect after application restart or a temporary connection loss; investigate a persistent Off state before using a gate.

Note Reader capability depends on its SDK and model. An unassigned reader can be connected and explicitly selected for registration; it does not generate zone movements or operate an access relay.

6 Create zones and assign checkpoints

A zone represents a parking area, office, warehouse or another monitored location. Assign saved readers to explicit directions so counts and movement history reflect your physical layout. A read by itself does not prove which direction an object moved.



Zones and their assigned checkpoints are managed separately from saved reader profiles.

1. Open Settings > Zones and select the Zones view. Add a zone or select an existing one. Set its name, time zone and capacity when required.

2. Select the zone, then Add reader or Assign reader. Choose a saved free reader by name. A profile already assigned elsewhere must be unassigned from that zone before reuse.

3. Choose In for entry, Out for exit, Event for observation, or ALERT for an anti-theft point. Save the assignment.

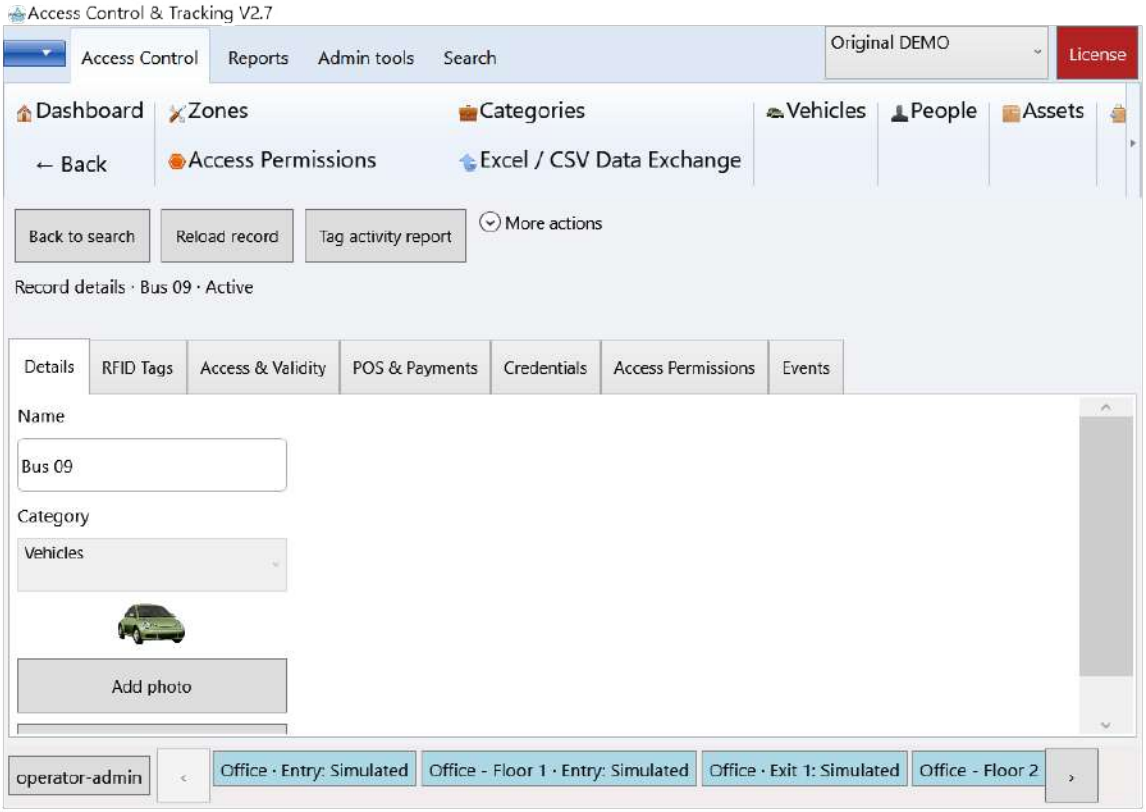
4. For a manual transfer between two zones, provide an Out reader in the source zone and an In reader at the destination. Enable their supported relays and configure the correct pulse/delay.

5. Confirm the zone's readers and counts on Dashboard. Test one direction at a time before relying on the occupancy figures.

Note Unassign reader removes only the zone assignment and preserves the device profile. An observation or anti-theft reader is not a substitute for a commissioned In or Out checkpoint.

7 Register people vehicles and assets

Use one universal record for each person, vehicle or asset. Optional photographs and descriptive fields help operators recognize objects, but a photograph is not required to register or use a record. Category names and custom fields can be adapted to your site.



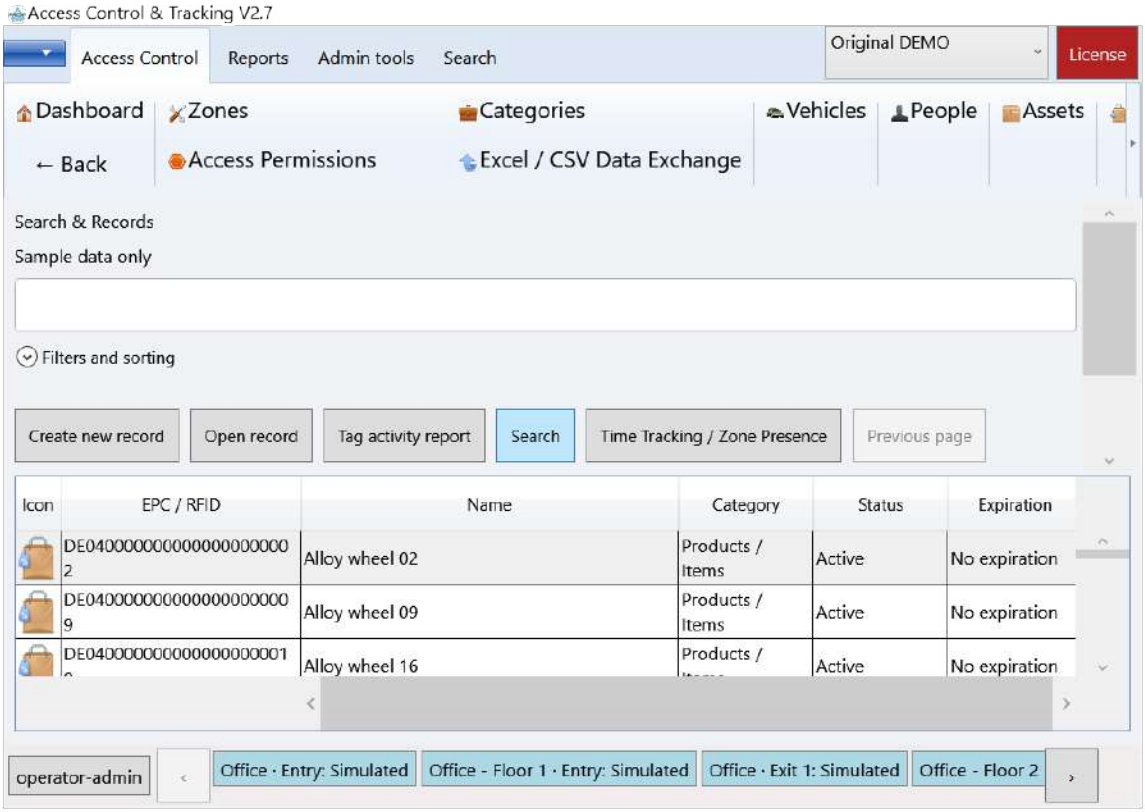
The record card keeps the category, identity, optional photograph and RFID sections together.

1. In Working, open Settings > Registration / Scan-to-Find and select a compatible configured reader. Turn this registration session On.
2. Present one tag. For an existing EPC, open the matching record and review its status. For an unknown EPC, choose to create a record or explicitly assign the tag to an existing record.
3. Choose the correct category and enter a recognizable name or reference. Complete the fields your organization requires. Review the EPC before saving.
4. Save the record or tag assignment. Check that the expected name and EPC appear in search.
5. When registration is finished, turn the registration session Off. A reader selected for registration is reserved for that task and is not simultaneously a zone-monitoring device.

Note Scanning for a match is read-only. Creating, replacing, disabling or unlinking a tag requires an explicit permitted action. Keep previous EPC history; do not create a duplicate record for an existing identity.

8 Search and edit a record

Search from Dashboard or a category list using a full or partial name, EPC, external reference or a supported custom-field value. Results are filtered and paged by SQL, so use a narrower search when the application asks you to refine it. DEMO searches also recognize translated sample names.



Search and Records provides filters, record actions and paged results.

1. Open the category or use Dashboard search. Enter the term and click Search, or press Enter where supported.

2. Expand Filters and sorting to choose category, record status, RFID-tag presence or validity. Use Previous page and Next page for more results.

3. Select a row and click Open record. The card contains Details, RFID tags, permissions, history and other permitted sections.

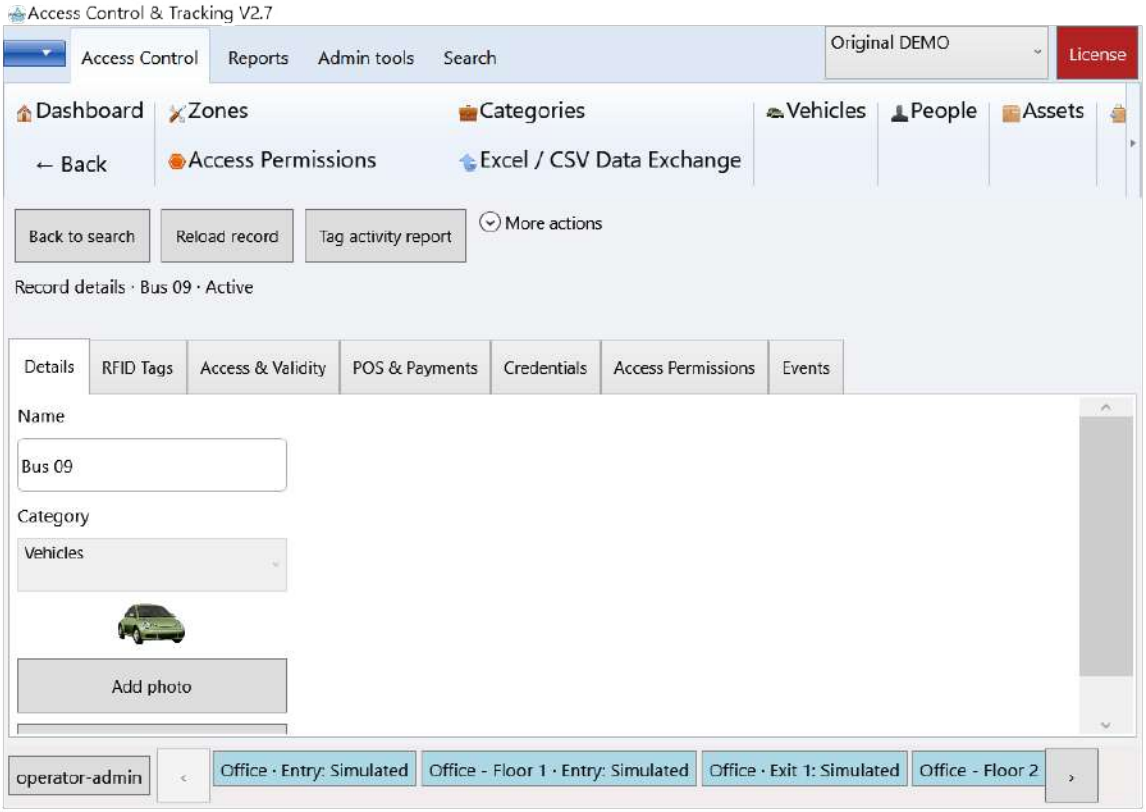
4. Review or edit the appropriate fields and Save. Use More actions for less common operations; Back returns to the preceding page.

5. If another workstation changed the record, reload and compare before saving again. Keep any unsaved input you need; do not overwrite a conflict blindly.

Note Double-click a result row to open Tag activity report when your account has report access. Open record opens the editable card. The catalog's Icon column is a category icon; the card can display an optional individual photo.

9 Set validity access and tag protection

Record validity, zone access and anti-theft protection are separate settings. A valid record does not automatically allow every restricted zone; a zone permission is not a payment receipt. A registered tag and its protected status should be reviewed independently.



The record card separates its details, RFID identities and operational permissions.

1. Open the record and review its active state and validity dates. No start date means no lower date boundary; it does not remove time limits or payment requirements.

2. Open Access permissions and allow only the required zones and periods. Apply the organization's explicit rules and check for denials or expired permissions.

3. In RFID tags, confirm the correct EPCs and the primary identity. Use the available actions to assign, replace, enable, disable or unlink a tag when authorized.

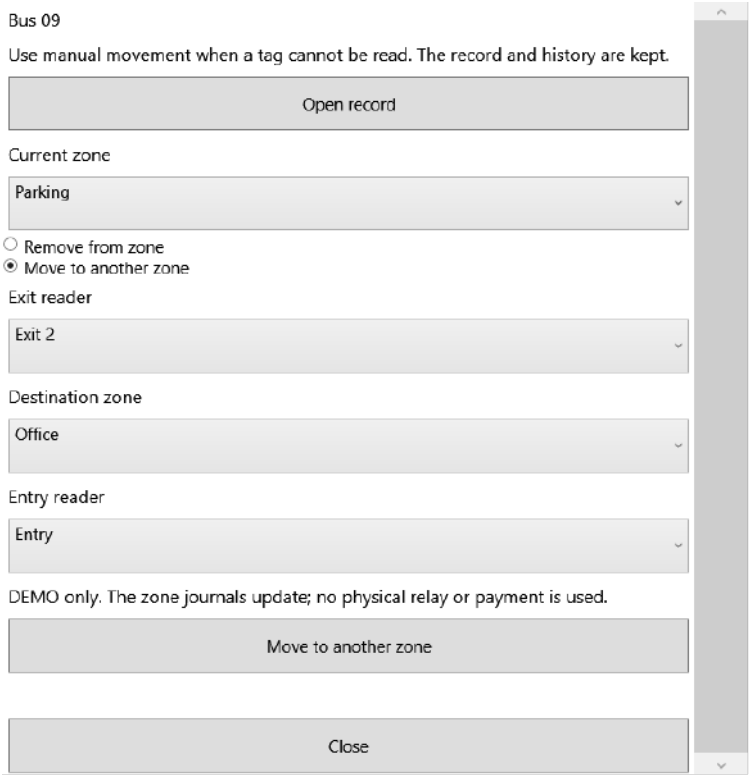
4. For anti-theft monitoring, review the tag's Protected setting and any approved issue/removal authorization. Keep protection enabled for items that must not leave without permission.

5. Save the intended changes and review the record history. Replacing an unreadable tag should keep the same object identity and previous events.

Note Manual movement is an explicit operator action. It does not repair a damaged tag, rewrite an EPC, switch off every protection rule or prove that a required charge was paid.

10 Use Dashboard for manual movement

Use this procedure when the person, vehicle or asset is physically at the passage but its tag cannot be read. Check the object's identity and actual location before confirming. The operation changes the recorded zone state and keeps the record and its history.



Object actions provides explicit zone and checkpoint choices, with automatic relay commands in Working.

1. On Dashboard, select the current zone. Click the person's picture, vehicle icon or other object tile to open Object actions.

2. To clear its presence in that zone, choose Remove from zone. To transfer it, choose Move to another zone and select the destination.

3. Review the Exit reader. A single matching Out reader is selected automatically; if several doors are available, select the actual one. For a transfer, also review the destination's In reader.

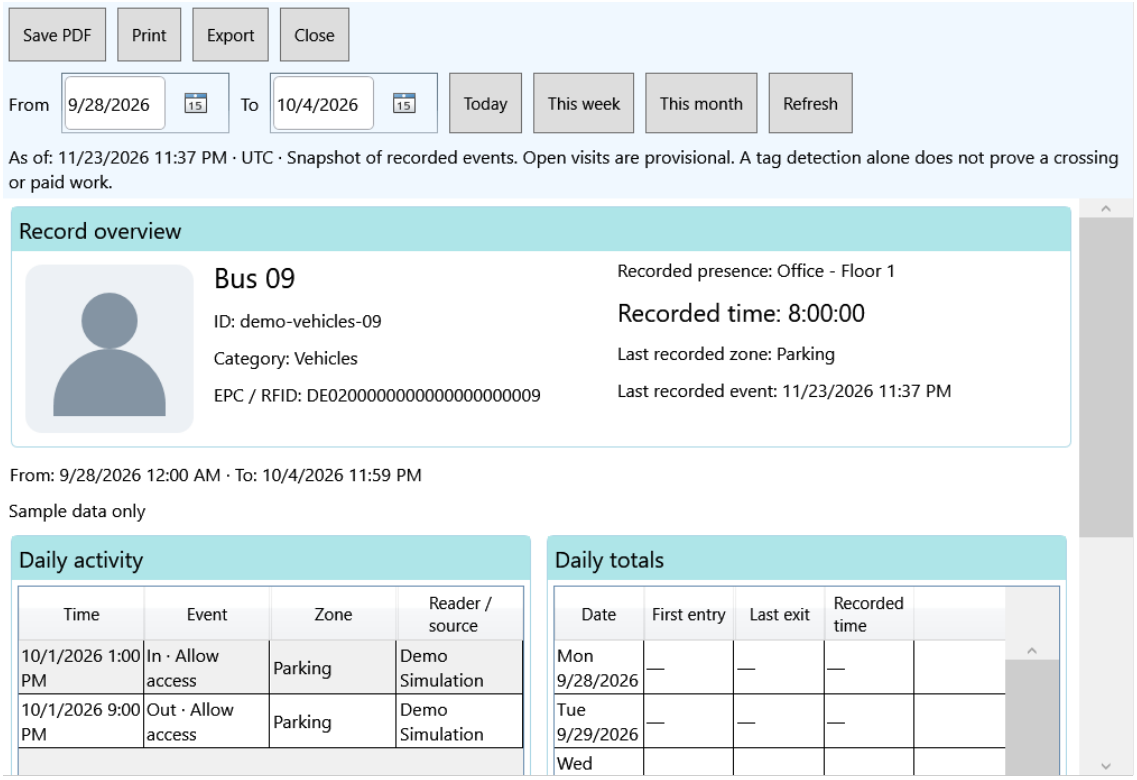
4. In Working, keep the selected readers online with Relay enabled. Click the movement action and confirm the source and destination. The configured source Out pulse and, for a transfer, destination In pulse run automatically.

5. Read the completion message, close the action window and check Dashboard and the object's event history.

Note If the movement is recorded but a relay command is not confirmed, check the doorway and reader status. Do not repeat the movement or charge the customer again. DEMO updates its journals without physical relay commands.

11 Review activity save reports and print

The activity report is available for people, vehicles and assets. It reports recorded evidence; missing reads, incomplete visits and unconfirmed direction must not be treated as certain physical attendance or theft.



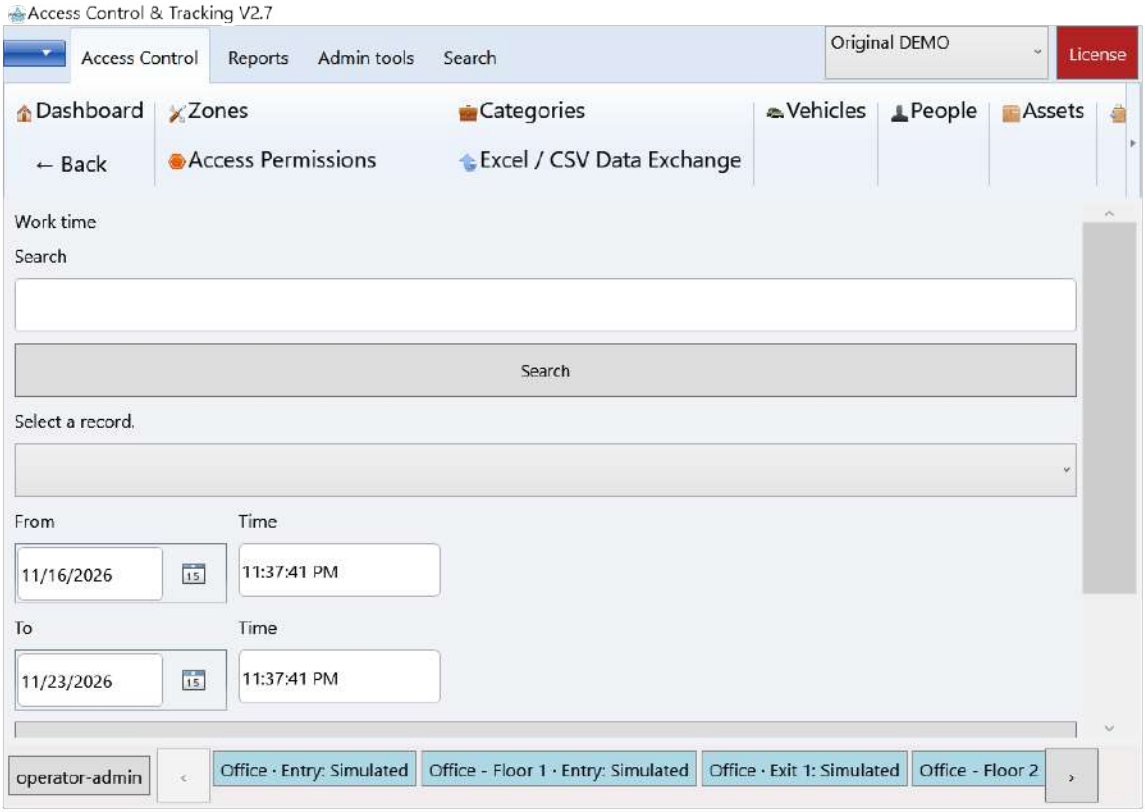
Tag activity report combines identity, presence, daily events and the selected reporting period.

1. Find the record in a category list and double-click its row, or select it and click Tag activity report. You can also open the report from its card.
2. Choose the period or a date preset. Review arrival, departure, last detection, zone totals, daily events and the period summary where available.
3. Check the event source and outcome. Operator corrections, simulated events, observations and access decisions have different meanings.
4. Click Save PDF and choose a folder and file name. Wait for confirmation, then open the saved file to verify it.
5. Use Print or the available print preview, select the correct printer and paper size, and review the page layout before printing.

Note Reports require Reports.Read. A report is a snapshot of the selected range and display time zone. Keep original records and use explicit corrections for missing exits rather than editing historical timestamps outside the application.

12 Configure time tracking and notifications

Time tracking uses recorded zone visits and the configured work schedule. Presence duration and scheduled working time are different measures. Breaks, missing exits and overlapping evidence can affect the result and may require review.



Work time uses a selected object and reporting range; schedules and breaks are separate settings.

1. In Settings, open the work-schedule section. Select the person or applicable category, the time zone and the work zones.

2. Set the start/end of each relevant day's shift and any break periods. Check each weekday and save the schedule.

3. Open Work time from the ribbon or record actions. Select the person, set From and To, then Calculate.

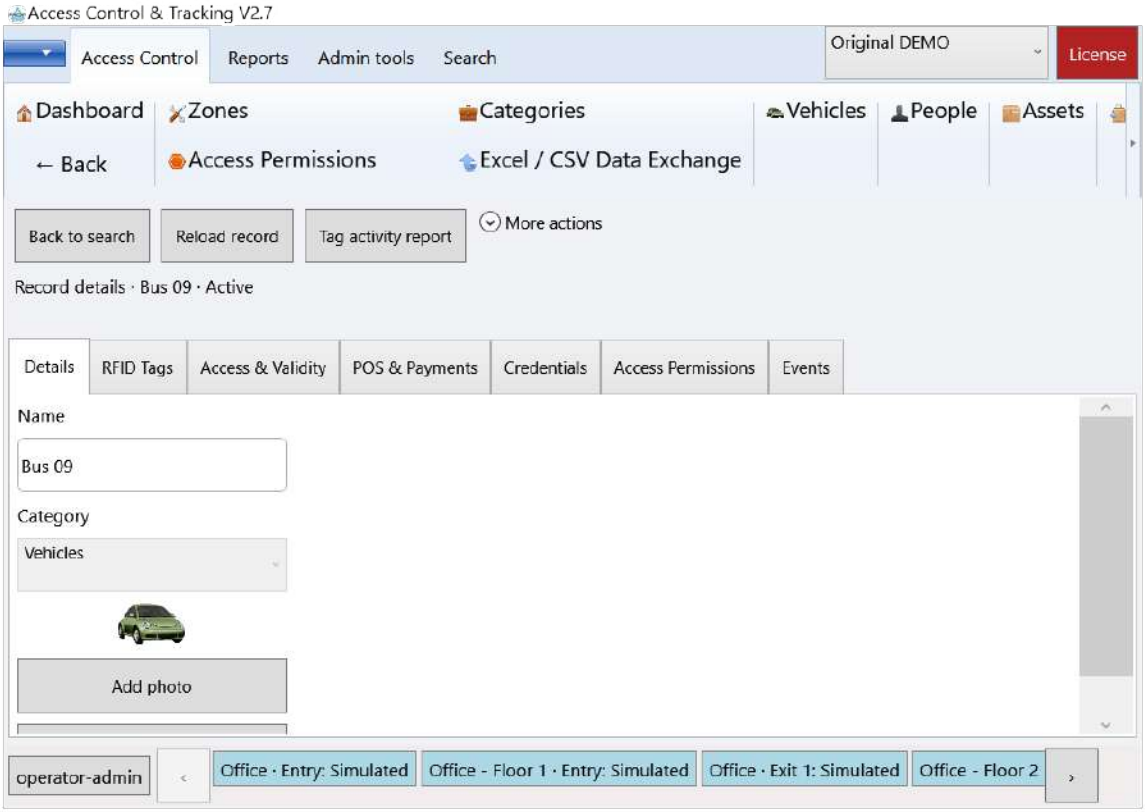
4. Review Zone presence and Work time. If the application flags incomplete evidence, inspect the activity report before using the total.

5. Use Preview report to review or print the calculation. Configure zone notifications for permission expiry or excessive presence separately when needed.

Note No start date in a validity filter is not a work-schedule option. A missing exit should be corrected with an authorized, explained operational correction; do not assume the person remained present indefinitely.

13 Issue return and protect equipment

Issue/Return records who holds an asset. It is different from the object's zone and from authorization to take it off site. For example, a diagnostic device can be issued to a technician without automatically permitting removal through every protected exit.



Open the object's card, then More actions, for the issue and return workflow allowed to your account.

1. Find the asset and open its card. Choose Issue/Return from the permitted actions.

2. Search for and select the recipient. Review the asset, holder and any required terms or notes, then confirm the issue.

3. If the asset may leave a protected area, use the site's explicit removal/access authorization in addition to custody. Keep the permitted zones and protection policy consistent.

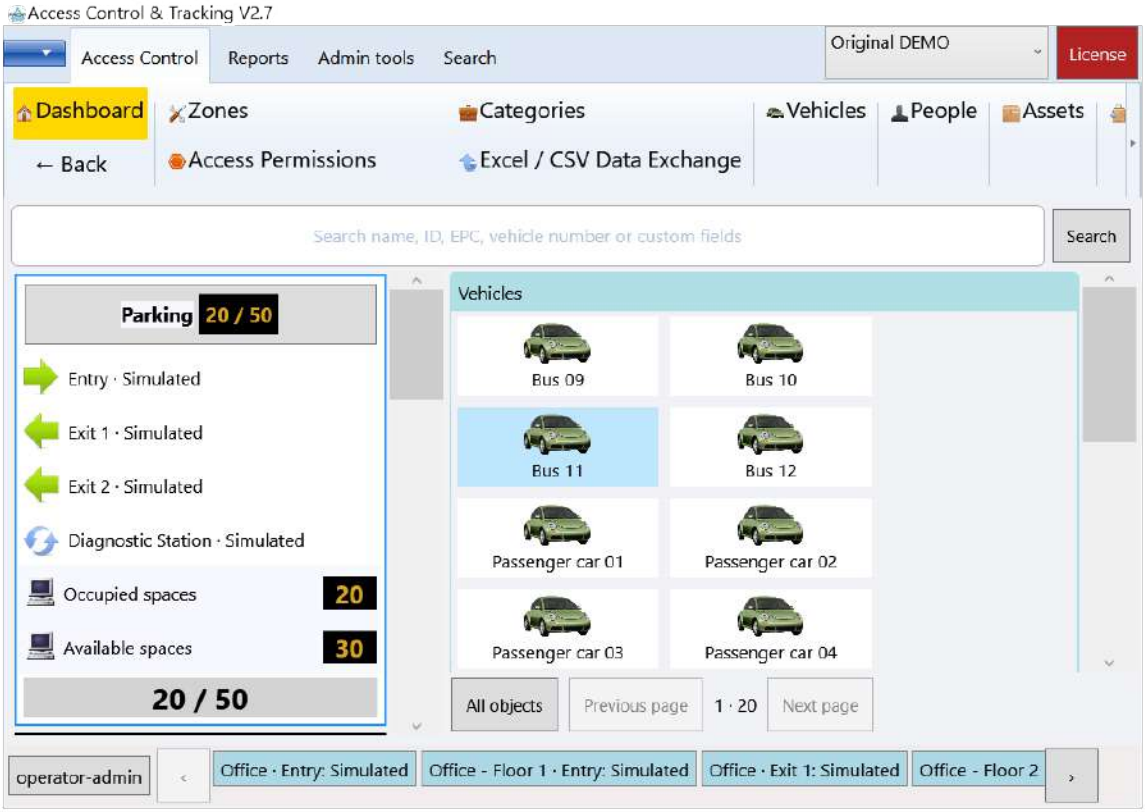
4. On return, select the open issue and confirm Return. Check that the holder/status and history reflect the return.

5. Use the activity report and inventory results together to distinguish an issued item, an authorized transfer and an item that was not detected.

Note An anti-theft event concerns the detected protected tag. Do not attribute it to a person unless the system has confirmed evidence linking that person and the item.

14 Respond to alarms and connection notices

Treat security alerts and reader connection warnings as different events. A protected-tag alert indicates a policy decision at that security point. A connection-loss warning indicates that a device is unavailable; it does not prove a theft or a physical movement.



Dashboard and the reader footer provide context before an operator acts on an alert.

1. Read the alert type, reader, time and any identified object. Check the physical location before taking action.

2. For an anti-theft alert, inspect the tag's protection, access/removal authorization and event history. Use the site's authorized acknowledgement or Stop ALERT action when appropriate.

3. For connection loss, check power, cable, network endpoint or COM number and device ownership by another program. Wait for automatic reconnect after the cause is corrected.

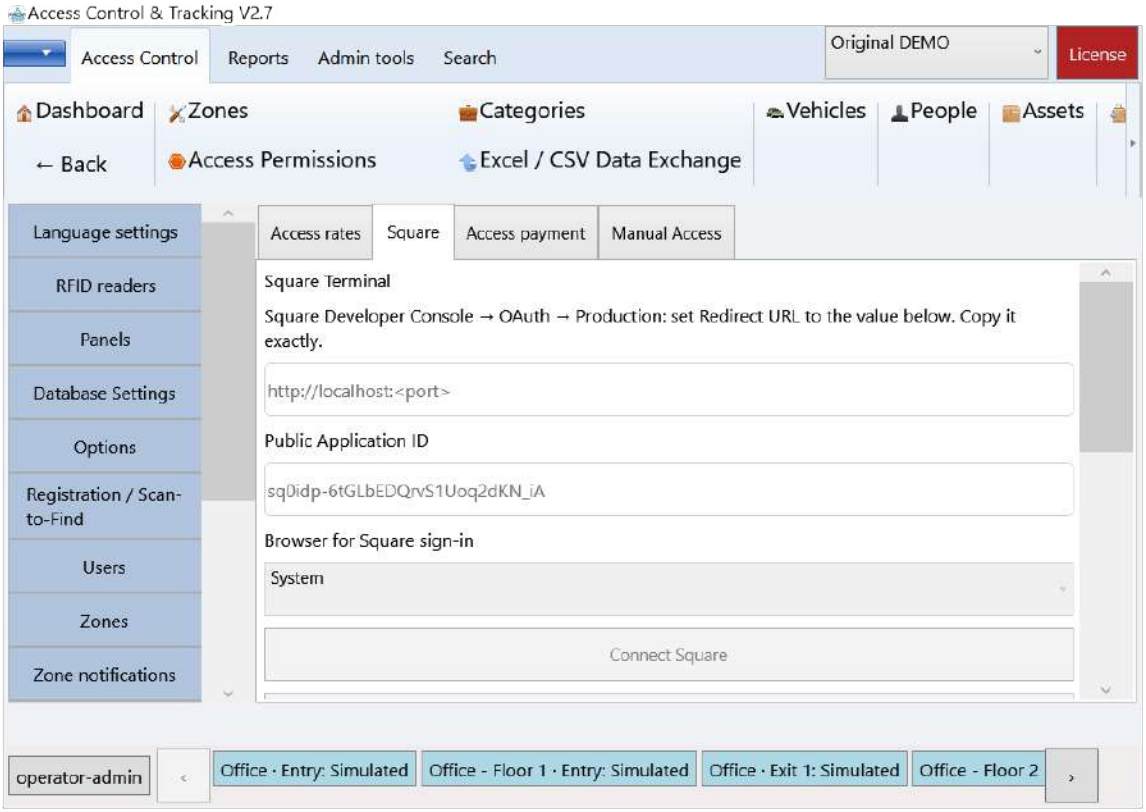
4. To silence repeated connection-loss reminders only, edit that reader and clear Repeat connection-loss reminder every minute. Keep the reader enabled if it should reconnect.

5. Record any required operational correction explicitly. Do not erase history to clear a notice.

Note Relay behavior depends on the reader's assigned role and enabled settings. A brief reader sound, an alert on screen and a physical contact change are separate observations.

15 Connect Square once

An administrator commissions Square in Working, using the merchant account, correct location and compatible Square Terminal. The application saves the confirmed setup. Routine reopening should not require pairing the terminal again; check the connection if authorization was revoked or the device changed.



Square setup is integrated under Payments. Its real actions are disabled in DEMO, while scrolling remains available.

1. Power on the terminal, connect it to the Internet and complete its required updates. Open Settings > Payments > Square in Access Control & Tracking.

2. Use the supplied Production Application ID. If Fresh USA asks you to configure your own developer application, set its Production OAuth Redirect URL to the exact value shown: http://localhost:<port>. Type <port> literally for this native PKCE setup. Do not enter or share an application secret in the client.

3. Choose System or Firefox for Square sign-in. Click Connect Square and approve the requested access on Square's official page.

4. Click Check connection / load locations and select the correct Square location. Click Get pairing code to generate its device code.

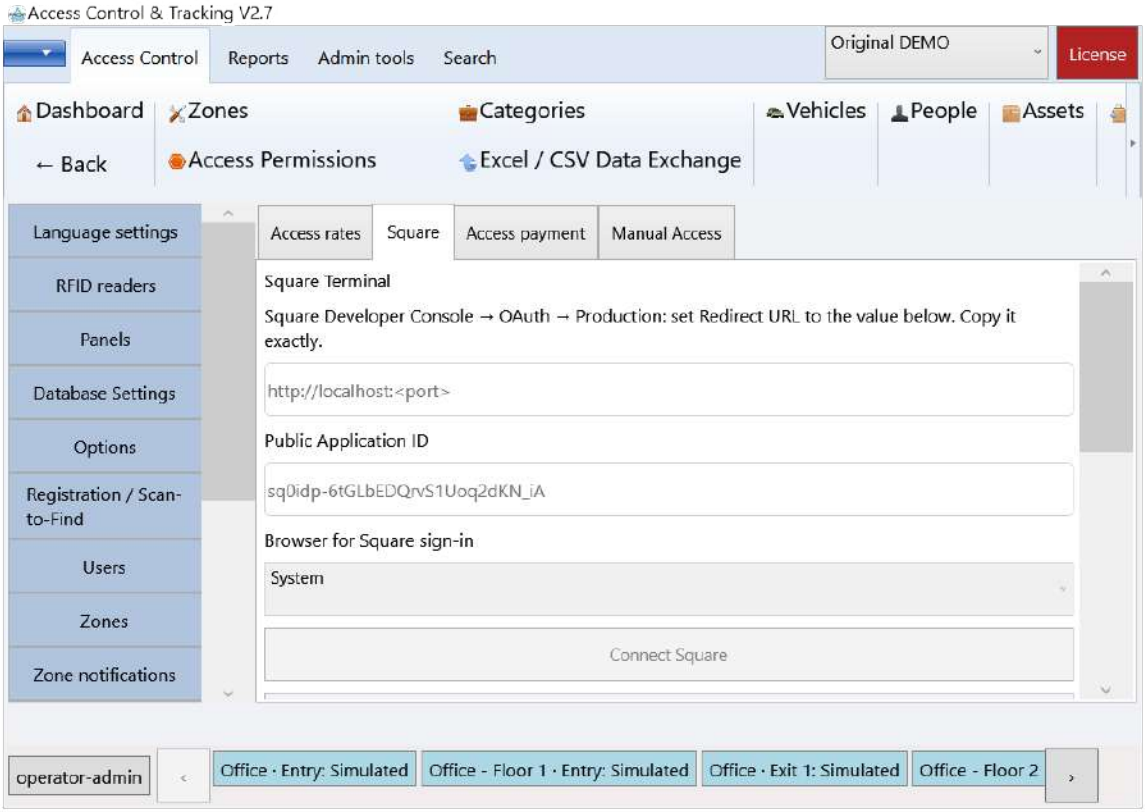
5. On the terminal's sign-in screen, choose the device-code option and enter the current code promptly. Return to the application and click Check pairing. Verify the confirmed Device ID.

6. Enable live payments only when you intend to accept real charges, then verify the saved setup.

Note Square is the example, not a promise that every POS device is interchangeable. Contact Fresh USA for other terminal integrations. Do not generate a new pairing code for an already paired terminal simply because the application restarted.

16 Set rates and take an access payment

Access rates can represent a one-time entry, prepaid entries, a timed entitlement or a stay charged at exit. A currency in the rate list does not mean your Square location can accept it; the terminal, merchant account and requested currency must be compatible.



Open Access rates beside Square in Payments to configure the zone and charging rules.

1. In Settings > Payments, open Access rates. Choose the zone and payment type, then set its amount and currency. Review credits, duration, time unit, free minutes, grace period and validity as applicable. Save & Apply.

2. Enable the intended paid-access rule for the zone and assign the appropriate In or Out reader. For pay-on-exit, use the matching commissioned exit with an enabled relay.

3. Open Access payment, select the record and relevant rate/visit, and Calculate / resume payment. Check the exact person/vehicle, amount, currency and time basis.

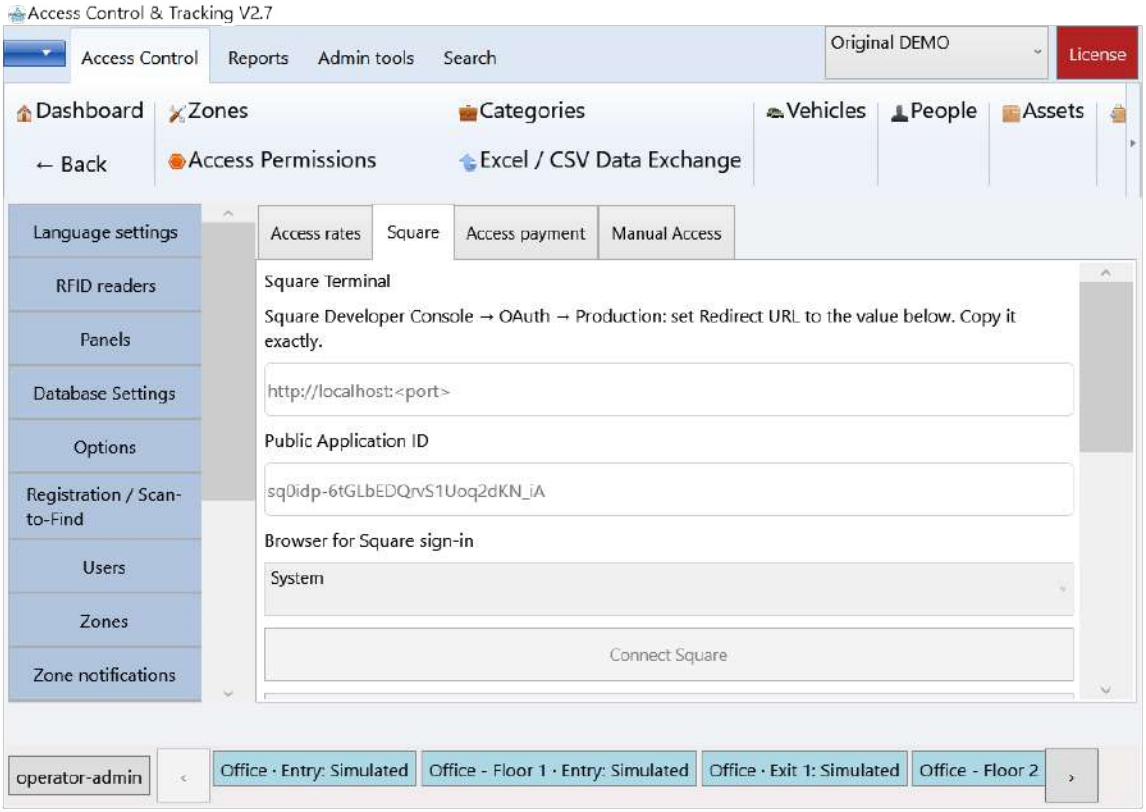
4. Confirm a real payment only when the customer agrees. Complete the transaction on the Square Terminal and wait for the application's confirmed result.

5. For an eligible completed exit payment, use the matching gate action if shown. The application checks payment and access policy before requesting its configured relay pulse.

Note A pending payment or a receipt request is not confirmed payment. If payment completed but the gate did not open, check the gate/reader and permissions. Do not charge again to resolve a relay error.

17 Reconcile cancel and refund payments

Payment reconciliation resolves an existing order with Square. A confirmed refund is a separate operation with its own permission and audit trail. Removing a zone presence or changing a rate does not automatically refund a payment.



Open Access payment beside Square to work with the selected record and its payment.

1. If a result is pending or the connection was interrupted, reopen the existing record/order and use Calculate / resume payment or the reconciliation action shown.

2. Compare the application's saved order, Square result and terminal receipt. Avoid creating a second charge while the first result is uncertain.

3. Use cancellation for a payment that is still eligible to cancel. Cancellation is not the same as refunding a completed charge.

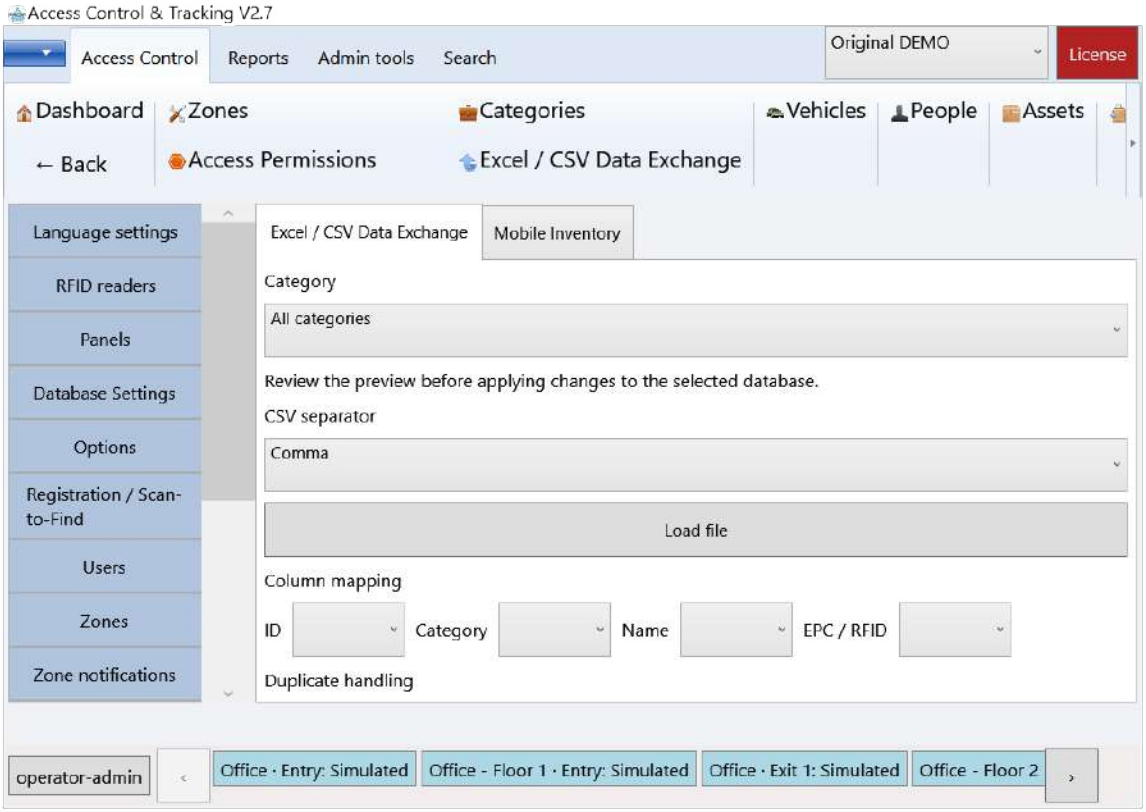
4. For a refund, open the completed payment's permitted refund action, check the record, original payment, amount and currency, and confirm once.

5. Wait for the confirmed refund result and review its history. Resolve associated access credits or exit rights according to the site's existing policy; do not assume a refund proves a physical departure.

Note DEMO does not submit Square charges, cancellations or refunds. Receipt printing depends on the configured Square terminal and available print options. Keep payment secrets out of screenshots and support messages.

18 Run category based mobile inventory

Mobile inventory uses the category XML exchange format shared with Smart Control. It records planned and actual counts without manufacturing access events or changing zone presence. A mobile reader must use the compatible exchange application and file profile.



Choose the Mobile Inventory tab beside Excel / CSV Data Exchange for the category XML workflow.

1. Open Settings > Mobile inventory and select its Mobile inventory tab. Choose an authorized exchange folder and Save & Apply.

2. Choose the category to count. Select the current file profile or Legacy names only if your mobile application requires it.

3. Click Export inventory plan or Export catalogue. Keep the exported batch and category associated with that counting session.

4. Transfer/load the files using the compatible mobile application, perform the count, then return the result XML to the exchange folder.

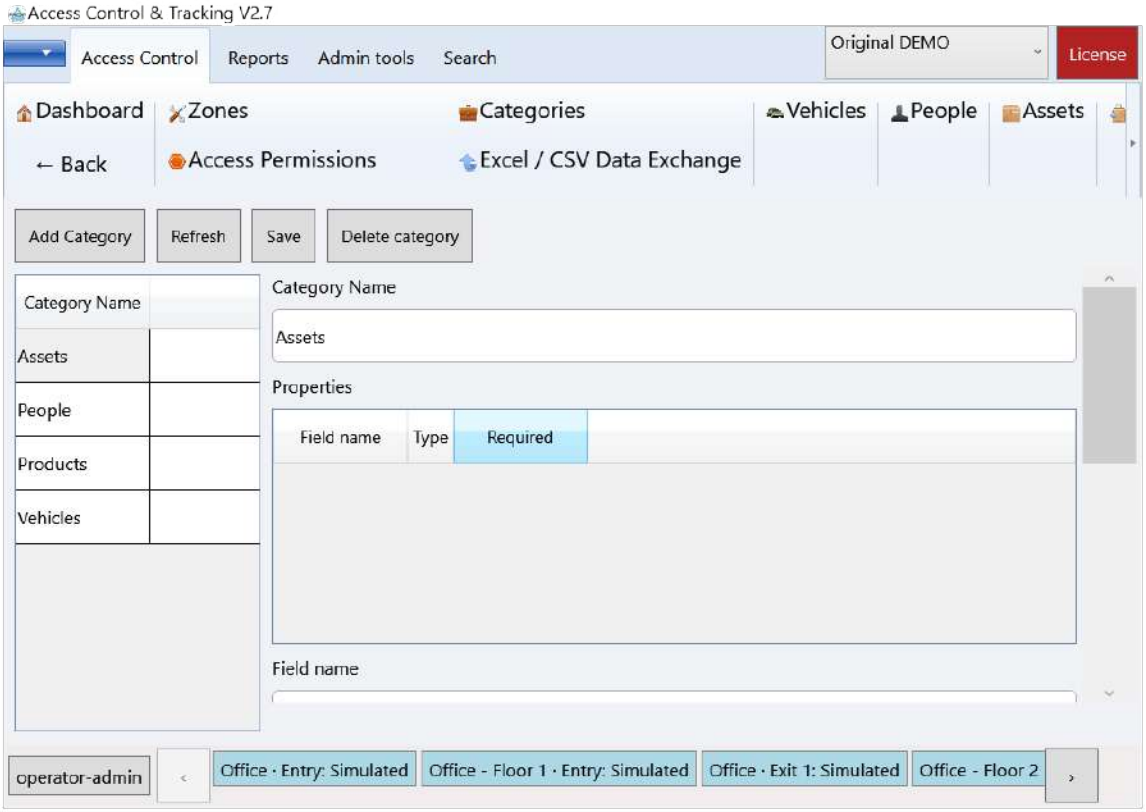
5. Select the original batch in Access Control & Tracking. Click Review handheld result, choose the returned XML and compare Plan and Fact before applying.

6. Click Apply import once after reviewing. Use View saved inventory result to reopen a result that was already accepted.

Note An expected but undetected item is an inventory difference, not proof of theft. Check issue/return records and authorized movements. Do not rename XML elements or mix results from different categories/batches.

19 Manage categories fields and data exchange

Working starts with the categories supplied for your package, typically Vehicles, People and Assets. Original DEMO also provides sample products. Custom categories use the same record, RFID and report model; they are not separate databases.



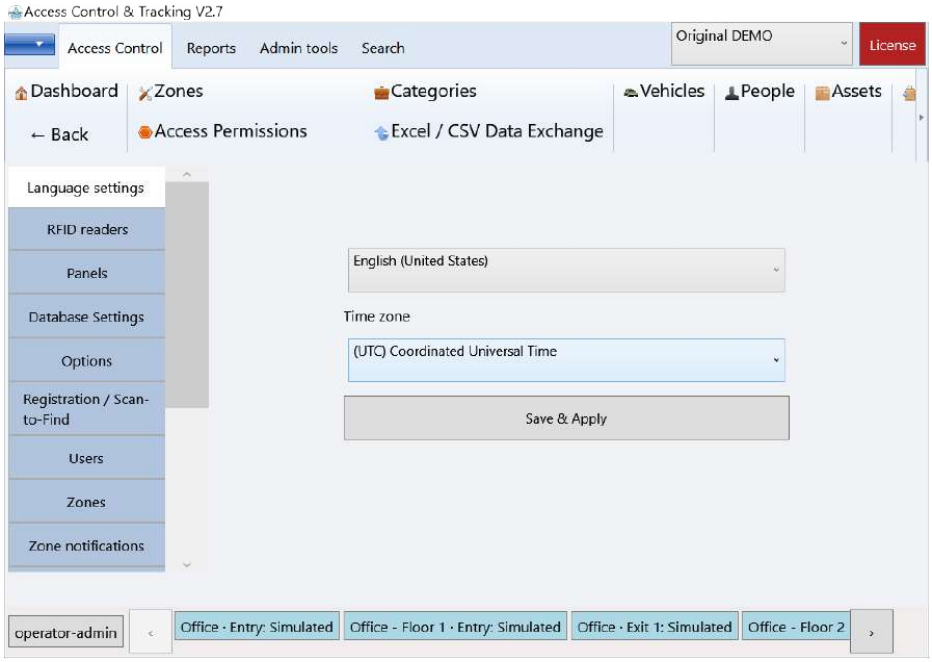
Category configuration lets the administrator adapt the universal record model to the site.

1. Open category administration when permitted. Create or select the category, choose its recognizable name/icon and define the fields your operators need.
2. Choose the displayed main field and optional image field deliberately. Required business fields should reflect your organization's needs; an optional photo should stay optional.
3. For CSV/XLSX exchange, open the existing Exchange function, select the category and file, review field mappings and duplicate handling, and inspect the preview before Apply.
4. Export only the categories/records permitted to your account. Keep EPC and stable identifiers intact when exchanging with another system.
5. For a new integration or an unsupported workflow, contact Fresh USA before altering SQL structures or reusing an unrelated category.

Note Do not create a second record simply to extend validity or replace a tag. Keep the object's ID and previous history. Software updates should not remove your custom categories or change existing data silently.

20 Back up troubleshoot and contact support

Keep current verified database backups and the installation/license files needed to restore your authorized system. A PDF report or exported spreadsheet is useful evidence, but it is not a full SQL backup. Ask your administrator to test restoration to a separate target.



Settings provides the connection and support context needed to diagnose a site issue.

1. Before an update, close the application and arrange a verified backup of the database and relevant protected configuration. Preserve the license and authorized computer identity.
2. If SQL connection is lost, check the configured server/service, PC/LAN availability and credentials. Recover the existing recognized workspace; do not delete it or silently replace it with a fresh database.
3. If a reader stays Off, check its power, unique endpoint/COM port, cable, profile and competing programs. Review diagnostics and the exact reader name.
4. If an action is unavailable, check your account's permissions and license. If a saved file seems missing, read the confirmation path and check that exact folder.
5. Send Fresh USA the product/version, concise steps, time of failure, relevant reader model/connection and a support package if requested. Exclude passwords, access tokens, private keys and unnecessary personal data.

Note The software and documentation are supplied AS IS and AS AVAILABLE, subject to the accepted Fresh USA EULA. For customizations, additional functions, integrations or assistance, contact Fresh USA. Phone +1 (312) 312-9608; support fresh@fresh222.com; sales/licensing order@fresh222.com. www.fresh222.com | software.fresh222.com

Square setup references

Square Terminal pairing and native OAuth redirect configuration. Verified November 24 2026.

Square Terminal pairing: https://developer.squareup.com/docs/terminal-api/pos-integration

Native OAuth redirect URL: https://developer.squareup.com/docs/oauth-api/create-urls-for-square-authorization