



# DESK LAUNCH CODES

Browser routing - authentication is required for every protected view



## OPEN SCANNER DESK

Start here. Scan the operator badge, then Continue.

<https://tus1-scanner-desk.pages.dev/>



## CHECKOUT

Operator verifies access; scan borrower badge and scanner asset.

<https://tus1-scanner-desk.pages.dev/?desk=checkout>



## RETURN

Scan assigned borrower badge and scanner asset; confirm return.

<https://tus1-scanner-desk.pages.dev/?desk=return>



## HISTORY

Review recorded checkout / return events after sign-in.

<https://tus1-scanner-desk.pages.dev/?desk=history>



## AVAILABILITY

Show registered scanners available for checkout.

<https://tus1-scanner-desk.pages.dev/?desk=availability>



# WHAT TO SCAN, WHERE

Current supported browser workflow - no automatic FC Menu takeover

## 1. POWER ON / OPEN THE DESK

Open the website in a permitted browser, or select an approved Scanner Desk shortcut in FC Menu once site IT has configured one. Power-on auto-launch is not configured. A reader that types barcode text will not necessarily open a QR URL.

## 2. VERIFY THE OPERATOR

The L3+ desk operator scans their issued badge into Operator ID and presses Continue. An existing authenticated account is checked against an active verified TUS1 L3+ profile. A new session requires individual desk-account sign-in.

## 3. CHECK OUT EQUIPMENT

Focus Borrowing Associate Badge and scan the L1/L2 borrower badge. Focus Scanner Asset ID and scan the Code 39 label. Select the assigned line / area; enter the real station and work function. Press Confirm checkout and wait for cloud confirmation.

## 4. LOOK UP AN ASSET

A URL-capable QR reader opens the asset lookup link. After verified sign-in, the dashboard filters for that scanner. The URL never grants access or confirms a transaction. A keyboard-wedge reader should scan the linear asset barcode into the Scanner Asset ID field instead.

## 5. RETURN TO THE DESK

Select Return. Scan the assigned borrower badge and asset barcode. Press Confirm return. Wait for cloud confirmation, then put the device in its charging slot. The return log retains the original line, station and work function.

Readiness: zero verified operator profiles and zero registered scanners were confirmed at the last setup check. This pack creates labels only; it does not enroll devices or approve employees.



# DATA THAT CAN BE TRUSTED

Accountability first. Activity and attendance require their own evidence.

## SCANNER HEADCOUNT

Unique borrower badge IDs with outstanding scanner checkouts. It is not building staffing, physical presence, or clock-in status.

## CHECKED OUT

The desk recorded an assignment which has not been returned. It does not establish current device usage.

## LAST ACTIVITY

Unknown until scanner telemetry is connected. Show the telemetry source and timestamp when an authorized integration exists; never substitute checkout time.

## ATTENDANCE UNKNOWN

No verified attendance source is connected. Do not infer clock-in or clock-out from a barcode scan, an assignment or scanner silence.

## LINE / STATION / WORK FUNCTION

Entered by the verified desk operator at checkout. A verified roster and station system could supply those fields later; no roster is connected now.

## LABEL REGISTRATION

Assign one draft ID to one physical device. Record its manufacturer serial in the CSV and register it in the protected inventory. Do not re-use IDs, cover manufacturer labels, or treat a draft ID as proof the device exists.

Device behavior source: Zebra DataWedge Keystroke Output documentation (relevant only if the actual handheld uses DataWedge).  
<https://techdocs.zebra.com/datawedge/14-3/guide/output/keystroke/>



# DESIGNED TOWARD 2046

A proposed evolution - future capabilities are not deployed

## NOW: DURABLE IDENTITY

Keep a permanent asset ID independent of employee, line and station. Use printable Code 39 for existing keyboard-wedge readers and protected QR links for browser-capable devices. No employee information or credentials go in a barcode.

## NEXT: APPROVED DEVICE LAUNCHER

Use the actual FC Menu / device-management system to offer Checkout, Return and Asset Lookup. Configure the scanner input profile per app so a scan lands in the intended field. This requires the real handheld model, FC Menu details and site IT configuration.

## NEXT: RELIABLE SHARED OPERATIONS

Register real assets, bind verified operator identities, reconcile the desk at shift handoff, and add missing/damaged/service workflows. Add time-stamped telemetry and attendance only through approved sources. Separate identity, custody, activity and attendance in the data model.

## LATER: SMART CHARGING DOCKS

A dock could report device ID, battery, health and physical return. A dock signal would be return evidence; it should not silently claim a person is clocked out. Keep a manual reconciliation path when devices or network fail.

## LONG TERM: OPTIONAL NFC / RFID

Add secure tag readers or device certificates without replacing the permanent printed ID. Location and predictive maintenance could be useful, but each signal needs provenance, freshness and an approved purpose. Keep auditable confirmations and a human recovery path.

## FAILURE RULE

A beep is not a saved checkout. Never show success before server confirmation. Future offline capture must show Pending and reconcile conflicts; offline confirmed checkouts are not implemented today.