USERAUTHGUARD

CASE STUDY

Union City Public Schools

How one New Jersey district manages 17,000 Chromebooks with a team that used to drown in spreadsheets

17,000	17,000+	75%	2 hrs
STUDENTS	CHROMEBOOKS	LESS DEVICE LOSS	SETUP TIME

The Challenge

Union City Public Schools is one of the largest 1:1 Chromebook districts in New Jersey, serving 17,000 students across multiple buildings in Bergen County. Every student gets a Chromebook. Every Chromebook needs to be tracked, assigned, maintained, and eventually collected.

Before UserAuthGuard, the IT team relied on a patchwork of Google Sheets, Google Admin Console, and manual processes. Tracking which student had which device required cross-referencing multiple systems. When a device went missing, there was no quick way to identify who was responsible.

The Google Admin Console showed devices in organizational units, but there was no enforcement — devices could be moved between OUs without IT knowing, breaking filtering policies and creating security gaps.

> "UserAuthGuard saves our IT team countless hours every week. The Google Admin Console automation alone has been transformative for managing 17,000 devices. This should be mandatory for every school."
>
> **Alex Castillo, Union City Public Schools**

The Solution

Union City deployed UserAuthGuard across the entire district in under two hours. The platform connected to their Google Admin Console via the official API, importing all 17,000+ Chromebook records instantly. No manual data entry. No migration project.

The IT team immediately gained a single source of truth for device assignments. Every Chromebook is assigned to a specific student with a complete audit trail — who had it, when they got it, when they returned it, and what condition it was in.

1:1 Device Assignment
Every device tracked to a student with full history

OU Locking
Devices locked to assigned organizational units

Repair Queue
Full repair workflow from intake to return

Loaner Management
Automated loaner assignment during repairs

Google Admin Automation
Real-time sync with Google Workspace

Compliance Reports
FERPA-compliant reporting and AUE tracking

Implementation Timeline

1. **Google Admin Connection**
   Connected UserAuthGuard to Google Workspace via OAuth. All 17,000+ device records imported automatically. Completed in under 30 minutes.

2. **Device Assignment Import**
   Imported existing student-device assignment data via CSV bulk upload. Matched serial numbers to student records across all buildings.

3. **OU Policy Configuration**
   Set up OU locking rules to prevent unauthorized device movement. Configured per-school and per-grade organizational units.

4. **Repair Center Launch**
   Configured repair queue with custom workflow stages, technician assignments, and parts inventory.

The Results

Within the first semester, Union City saw dramatic improvements across every metric they tracked.

Device loss dropped 75% because students know every device is tracked to them personally. When a Chromebook goes missing, the IT team can instantly identify who had it last.

IT tickets dropped 60% because common issues were handled automatically or through self-service. Teachers could check repair status without emailing IT.

75%	60%	95%	2 hrs
Reduction in device loss	Fewer IT support tickets	Teacher satisfaction rate	Total setup time

Ready to see similar results?

Start free with up to 100 devices. Setup takes under 2 hours.

userauthguard.com/signup | **Book a Demo**