Troubleshooting Checklist

Storeroom Leak Troubleshooting Checklist

A tech can see storerooms that are not theirs even if the data restriction looks correct. The restriction is usually isn't the problem. In Maximo a user's effective profile is the combination of all their security groups. The highest privilege prevails, and data restriction conditions OR together, so a broader group with no condition on the object is *OR-ing* right past your scope. Work this in order.

WHAT IS ACTUALLY HAPPENING

Your restriction works. Another security group is broader. Higher privileges prevail, conditions OR together, and any group that opens the object with no condition grants full access. Find that group.

Diagnose, in order

☐ 1 List every security group the user is in. That full set is the user's effective profile, and it is what actually decides what they can see.

☐ 2 For each group, mark which ones grant the inventory objects in question. Inventory, item availability and balances, issues and transfers, and receipts are the usual set, but the exact list varies by your applications and customizations.

☐ 3 Find any security group that opens those objects with no data restriction on them. That is the likely offender.

☐ 4 Check MAXEVERYONE, the everyone security group. It always combines, even when marked independent.

☐ 5 Confirm the scoped security group is the only path the user has to those objects. Intended supervisor or admin breadth is a separate case, not a leak.

☐ 6 Confirm the ownership attribute is populated, which for the truck-storeroom solve is the Inventory Owner set on each of the user's storerooms. A blank value is the opposite symptom, the user sees nothing.

☐ 7 Confirm the condition family covers every object and view the user can reach the data through, including views.

☐ 8 Retest as the actual user in Dev, not as an admin.

Fix it

Make the scoped security group the only path to those objects. Strip the objects out of the broad group, or take the user out of it if they do not need the rest of what it grants. Do not reach for the independent flag reflexively. It changes how site and application access combine and does not make a restriction win against a more permissive group.

Confirm

☐ The user now sees only their own storeroom across inventory, balances, issues, and receipts.

☐ The user can still do their job. The scoped security group still grants what they need.

☐ You verified by logging in as the user, not by reading the security group configuration.

THE OPPOSITE SYMPTOM

A user who suddenly sees nothing is usually a blank ownership field or no scoping security group at all. Different cause, different fix.

WHEN THIS CHECKLIST IS NOT ENOUGH

This checklist fixes the common broad-security group leak. If the broad-security group check comes up clean, the leak is

> *somewhere narrower: a missing object or view, a gap in the condition family, a custom object, lookup behavior, or a workflow or application path the restriction never covered. That is a full build review, not a quick fix.*

This checklist fixes the leak. Building per-user storeroom scoping correctly is covered in the article "Give Your Techs Access to Only Their Own Truck," and the Maximo Right-Sizing Playbook walks the full solve end to end.

Article link: https://brockindustries.io/articles/tech-storeroom-access-without-200-groups.html

Playbook link: https://amzn.to/4eGDkAf

Group combination behavior verified against IBM MAS security documentation, June 2026. Brock Industries.