

REBEL SOFTWARE · RebelPSA

Asset & Device Management Guide

Device Catalog, Maintenance & Work Orders

Version	1.0
Date	August 2026
Intended audience	Technicians & Administrators

Contents

- 1.** About This Guide
- 2.** Devices & Assets: Key Concepts
- 3.** The Device List
- 4.** Device Types & Groups
- 5.** The Device Detail Page
- 6.** QR Codes & Label Printing
- 7.** Preventive Maintenance Scheduling
- 8.** Work Orders
- 9.** Parts & Inventory
- 10.** Security & Compliance Tracking
- 11.** Documents & Reference Materials
- 12.** RMM Integration Cards
- 13.** Common Technician Workflows
- 14.** Quick Reference & Glossary

1. About This Guide

This guide covers RebelPSA's Asset & Device Management module. A catalog of every managed device and physical asset across your client base, plus the preventive maintenance, work order, parts, and security tracking built directly on top of it.

The module goes beyond a typical RMM (Remote Monitoring and Management) configuration-item list: it's built to handle real preventive maintenance workflows for anything your organization maintains — IT equipment, network gear, and non-IT physical assets like printers or HVAC units alike.

Tip. *The device catalog is the source of truth. Your RMM integrations (NinjaOne, Datto) feed data into a device's record — they don't replace it. A device's identity and history stay stable in RebelPSA even if the RMM agent on it changes or is reinstalled.*

2. Devices & Assets: Key Concepts

- **Device** -- any managed endpoint, server, or network appliance typically tracked via an RMM agent (exp. a workstation, server, or switch).
- **Asset** -- the broader category, including physical equipment that doesn't run an RMM agent at all (exp. a printer, projector, HVAC unit, or vehicle) but still needs scheduled maintenance and a service history.

Both live in the same catalog under a single profile model, distinguished by an Asset Type flag, so a technician's workflow (work orders, maintenance schedules, QR labels) works identically whether they're servicing a server or a rooftop HVAC unit.

A Device's Identity Never Changes

Every device gets a permanent internal identifier the moment it's added to the catalog. That identifier never changes, even if the device is renamed, re-imaged, transferred to a different client, or eventually decommissioned. Every work order, ticket, maintenance record, and integration data point stays permanently linked to that one identity.

- When renaming a device you will be prompted for a reason and the old name will stay in a permanent name history.
- The device's timeline groups history by name era, so you can see exactly what happened while it was called "DESKTOP-OLD01" versus after it became "WORKSTATION-MKT-01", while all on one continuous timeline.
- Device history is retained for years (7 by default, tenant-configurable up to 10) and decommissioned devices are archived, never hard-deleted, and remain fully searchable.

3. The Device List

The Device List is a sortable, filterable grid of every device and asset across every client, with columns for make, model, serial number, status, assigned company, and device type. Use it to find a specific device, or to see everything of a given type or status at once (for example, every server that's overdue for maintenance).

Status	Meaning
Active	Currently in service and being tracked.
Inactive	Temporarily out of service but not decommissioned.
Archived	Retired, but its full history remains queryable.
Decommissioned	Permanently retired from service.

Tip. Filter the list by company to see everything a specific client has on file, or by device group/type to review a whole category (for example, all network switches) at once.

4. Device Types & Groups

Device Types

A Device Type is a category — Workstation, Server, Switch, Printer, HVAC Unit, and so on. Each type can carry its own custom field template, so every new device of that type automatically inherits the right set of extra fields, and its own Document Center library link (see Section 11).

Device Groups

A Device Group is an organizational bucket you define (exp. "Workstations — Site A" or "Network Infrastructure.") Groups support up to three levels of parent-child hierarchy, and a device can belong to more than one group at the same time.

Group-level actions save time when you need to act on many devices at once:

- Assign a maintenance schedule to an entire group — every member device inherits it
- Attach a Document Center library to the whole group
- Bulk-update a field across every device in the group
- View a group-level health dashboard

5. The Device Detail Page

Opening a device brings up its detail page, organized into tabs:

Tab	What It Shows
Overview	Standard fields (make, model, year built, serial, service tag, MAC address, purchase date, warranty expiry, location, assigned user, assigned company) plus any custom fields defined for this device's type.
Timeline	A unified history of everything that's happened to this device: work orders, maintenance events, linked tickets, integration sync events, name changes, ownership transfers, and manual notes.
Work Orders	Every work order ever raised against this device, current and historical.
Maintenance	Active and upcoming preventive maintenance schedules for this specific device.
Parts	Parts consumed or reserved against this device's work orders.
Security	The device's security and compliance record — see Section 10.
Documents	The reference library attached to this device's type and groups — manuals, procedures, compliance checklists.

Tip. The Overview tab also shows a gallery of integration cards — one per connected integration (NinjaRMM, Datto, antivirus, backup, Microsoft 365) — each surfacing that tool's own data points for this device. These cards are read-only and refresh automatically on the integration's own sync cycle.

6. QR Codes & Label Printing

Every device gets a unique QR code the moment it's added to the catalog, encoding its permanent internal identifier. Print labels directly from a device's detail page, or in batch from the device list for a whole group of devices at once — your organization can configure the label size and which fields appear on it.

- Scanning a device's QR code from the mobile app opens straight to its detail page.
- If the device has an active work order, a "Start Work Order" shortcut appears immediately on the scan result. This can be useful for jumping straight into a job while standing in front of the equipment.

7. Preventive Maintenance Scheduling

A Maintenance Schedule defines a recurring service task, and can target a single device, an entire device group, or a whole device type at once.

Trigger Type	How It Fires
Time-based	Every N days, weeks, months, or years.
Usage-based	When a meter or counter reaches a configured threshold.
Condition-based	Triggered manually, or by an integration-reported alert.

- A schedule can carry an optional checklist template — an ordered set of confirmable steps, which can reference specific parts from the Parts Catalog.
- Configure an advance-notice window (exp. 7 days before due) and an escalation if the work order isn't completed within the grace period.
- Every completed PM (preventive maintenance) is logged permanently against the device. Overdue and upcoming maintenance surfaces both on the device's own detail page and on a tenant-wide PM dashboard.

Tip. *Scheduling maintenance for a whole Device Group generates an individual work order per device when the schedule activates — you get one clean, trackable job per device, not one combined job covering many devices.*

8. Work Orders

A work order is the maintenance-specific layer on top of a Help Desk ticket — every work order is backed by a real ticket, which carries the SLA (Service Level Agreement), time tracking, and billing, while the work order itself adds the checklist, parts, QR reference, and sign-off.

Creating a Work Order

- Automatically, when a maintenance schedule activates
- Ad-hoc, directly from a device's detail page
- By scanning a device's QR code from the mobile app
- By promoting an existing Help Desk ticket into a work order

Status Flow

Draft -> Assigned -> In Progress -> Pending Parts -> Completed -> Closed. Closing a work order, maps back to resolving its underlying ticket.

Printing & Sign-Off

- A work order can be printed as a formatted PDF including the device's QR code, job description, checklist steps, assigned technician, parts list, and signature blocks.
- An optional customer sign-off block can be configured per work order type; a technician can capture a signature directly in the mobile app, and the signed PDF is stored permanently with the work order.

9. Parts & Inventory

The Parts Catalog is your organization's list of spare parts and consumables — tracked by part number, manufacturer, on-hand quantity, reorder threshold, vendor, unit cost, and bin/shelf location.

- A work order can request a part directly from the catalog. If enough is on hand, it's reserved automatically.
- If there isn't enough on hand, a parts request is created and can escalate straight into a purchase order.
- Receiving a purchase order updates on-hand quantity automatically.
- Parts costs on a work order flow into the originating ticket's cost summary for billing.
- An inventory dashboard shows on-hand counts, anything below its reorder threshold, open purchase orders, and recent consumption by device type.

10. Security & Compliance Tracking

Every device carries its own security record, tracked alongside its maintenance history:

Field	Tracks
Antivirus	Product in use and current protection status.
Patch Compliance	Current / Behind / Critical.
MFA Enforcement	Whether multi-factor authentication is enforced on this device.
Disk Encryption	BitLocker, FileVault, or other, and its current status.
Vulnerability Scan	Date of the last scan and count of open CVEs (Common Vulnerabilities and Exposures).

Devices can also be tagged with a compliance framework label — HIPAA, PCI-DSS, SOC 2, NIST CSF — which drives filtered compliance views and reports across your whole client base.

- Antivirus and patch fields populate automatically from a connected NinjaRMM or Datto RMM integration where available; anything not covered by an integration can be maintained manually.

- A tenant-wide compliance dashboard shows devices by compliance status, patch posture, antivirus coverage, and encryption compliance and is filterable by client, device group, or compliance tag.

Tip. Every manual change to a device's security record is logged with who made it and when. Updates that come in automatically from an integration are clearly tagged as system-sourced, so you always know whether a value was verified by a person or reported by a tool.

11. Documents & Reference Materials

Any Device Type or Device Group can have one or more documents or knowledge base articles attached as a reference library — vendor manuals, maintenance procedures, compliance checklists. When a technician opens a device or its work order, the right library shows up automatically in the Documents panel, based on that device's type and group memberships.

Tip. Documents are never duplicated into the device module — the Document Center remains the single owner of the actual file. The device just holds a link, so updating the source document updates it everywhere it's referenced.

12. RMM Integration Cards

Where a device has a connected RMM or security integration (NinjaOne, Datto RMM, an antivirus tool, a backup tool, Microsoft 365), that integration's data appears as its own card on the device's Overview tab. Cards are read-only in RebelPSA and refresh on the integration's own sync schedule — think of them as a live window into what that tool reports, layered onto the device record that RebelPSA itself owns.

13. Common Technician Workflows

Arriving on-site for a scheduled maintenance visit

- Scan the device's QR code with the mobile app.
- Use the Start Work Order shortcut on the scan result.
- Work through the checklist step by step, pulling any needed parts from the catalog as you go.
- Capture a customer signature if sign-off is required, then close the work order.

Adding a brand-new device to the catalog

- Add the device and select its Device Type so it inherits the right custom field template.
- Fill in the standard fields (make, model, serial, assigned company, location).
- Assign it to any relevant Device Groups.
- Print a QR label for it if you'll need to scan it on future visits.

Investigating a device's history before a call

- Open the device's detail page and review the Timeline tab.
- Check the Security tab for any outstanding patch or antivirus concerns.
- Review past Work Orders for recurring issues before you diagnose a new one.

14. Quick Reference & Glossary

Term	Meaning
Device Profile	A device's permanent record — the root identity everything else links back to.
Device Type	A category (Workstation, Server, Printer, etc.) that can carry its own custom fields and document library.
Device Group	A tenant-defined organizational bucket, supporting up to three levels of hierarchy.
Work Order	A maintenance task instance, backed by a Help Desk ticket, with its own checklist, parts, and sign-off.
Maintenance Schedule	A recurring service task definition — time-based, usage-based, or condition-based.
Parts Catalog	Your organization's tracked inventory of spare parts and consumables.
Integration Card	A read-only summary of data from a connected RMM or security tool, shown on the device's Overview tab.
Compliance Tag	A framework label (HIPAA, PCI-DSS, SOC 2, NIST CSF) applied to a device to drive compliance reporting.