

REBEL SOFTWARE · RebelPSA

# GDAP / M365 Management Portal Guide

Connecting To, Monitoring & Managing Customer Microsoft 365 Tenants

|                   |                              |
|-------------------|------------------------------|
| Version           | 1.0                          |
| Date              | August 2026                  |
| Intended audience | Administrators & Technicians |

## Contents

1. About This Guide
2. The Two Planes: Insight & Control
3. Connecting to a Customer's Microsoft 365 Tenant
4. Insight: Security Posture
5. Insight: Service Health
6. Insight: Microsoft Updates
7. Control: User & License Lifecycle
8. What's Not Here Yet
9. Permissions
10. Common Workflows
11. Quick Reference & Glossary

## 1. About This Guide

This guide covers the Ops Center's Microsoft 365 capability — the first-wave foundation of what will eventually be a much broader operations platform. Today, that foundation covers how RebelPSA connects to a customer's Microsoft 365 tenant, three read-only Insight tracks (Security Posture, Service Health, Microsoft Updates), and a first set of write actions for managing users and licenses.

**Important.** *Ops Center is being built as a much larger platform — tenant compliance assessments, policy backup/restore, SaaS discovery, Copilot management, and automation workflows are all planned in detail, but none of that is built yet. This guide covers what's live today. Section 8 lists what's still ahead so you know what to expect later rather than assume it's already there.*

## 2. The Two Planes: Insight & Control

Everything in the Ops Center's Microsoft 365 capability is organized into two planes, and this split is both how it's presented to you and how it's built underneath:

- **Insight (read)** -- every read-and-alert surface. It shows you what's happening across your managed customer tenants — security posture, service health, upcoming Microsoft changes — without ever changing anything in the customer's environment.
- **Control (write)** -- every action surface. This is where a technician does something inside a customer's Microsoft 365 environment — resetting a password, assigning a license, disabling sign-in.

**Tip.** *The Insight plane's default display name is "Insight / Security Center," but your organization can rename it to fit your own service catalog — the underlying capability doesn't change, just the label.*

## 3. Connecting to a Customer's Microsoft 365 Tenant

RebelPSA uses two different connection methods, with a clear primary and a clear fallback.

### GDAP (Primary Method)

GDAP — Granular Delegated Admin Privileges, Microsoft's own partner-relationship model — is the primary way RebelPSA connects to your customers' Microsoft 365 tenants, and it's built specifically to scale across many customers at once rather than requiring a separate setup per client.

- One GDAP relationship covers your whole RebelPSA tenant. A single partner relationship, established once, fans out to every customer tenant that approves it — you don't set up a new connection for each individual client.

- Customers are discovered automatically through Microsoft, then matched to the correct company record in your CRM. If a customer can't be automatically matched, it lands in a technician review queue rather than being auto-created incorrectly.
- Once your organization's partner credential is established, individual technicians never need to separately authenticate to Microsoft — the system handles token exchange behind the scenes for each customer as needed.

**Important.** GDAP relationships are time-bound (up to two years, with optional auto-extend) and require customer approval, and the underlying partner credential has its own separate expiry risk. These are monitored with advance warnings, and a credential problem is surfaced distinctly from a single customer's pending approval, so if something needs attention, you'll know which of the two it is.

**Tip.** Known limitation: today's GDAP setup requests Global Administrator rather than a more tightly-scoped read-only role. It's sufficient for what's built so far but expect this to tighten in a future update. Also, the one-time credential setup currently requires an operator to sign in interactively and paste a token by hand, rather than a fully automated in-app flow.

## Direct Connection (Fallback)

For edge cases where a GDAP relationship isn't available or appropriate, a Direct connection — one dedicated app registration per client company — is available instead.

- A Direct connection is structurally isolated from any mailbox/calendar credentials for that same client, so applying a Conditional Access policy to M365 admin actions never affects mail or calendar sync.
- Each Direct connection is explicitly flagged read-only or write-capable, and the broader management permissions are only ever requested on connections flagged write-capable.

## 4. Insight: Security Posture

A per-client view of Microsoft 365 security health, built from Microsoft's own security signal sources:

| Surface                   | What It Shows                                                                                                                                                 |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Client Security Scorecard | Secure Score, open incidents, risky users, unprotected endpoints, and MFA adoption percentage, per client.                                                    |
| Risky Users Panel         | Users Microsoft's own identity protection has flagged as at-risk, with risk level and last sign-in — you can dismiss the flag or confirm compromise directly. |
| Risky Sign-Ins            | Individual sign-ins flagged as risky, with location, IP, and device detail; blocking the user hands off to the Control plane's block action.                  |

| Surface                    | What It Shows                                                                                                                                                         |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Unified Alerts Feed</b> | A single, normalized alert stream across every connected security signal source, filterable by client, provider, and severity, with open/investigating/closed states. |
| <b>Secure Score Trend</b>  | How a client's score has moved over time, with recommendation drill-down.                                                                                             |
| <b>Coverage Gaps</b>       | Devices reporting to no security vendor at all — a fast way to spot unprotected endpoints across your base.                                                           |
| <b>MFA Adoption</b>        | Per-client MFA enrollment rate, broken down by user.                                                                                                                  |

## 5. Insight: Service Health

A mirror of the Microsoft 365 Admin Center's own service health view — this track is purely operational, not a security signal, so a service degradation never feeds into the security alert model above.

| Status                     | Meaning                                                              |
|----------------------------|----------------------------------------------------------------------|
| <b>Normal Service</b>      | Operating normally.                                                  |
| <b>Service Degradation</b> | Minor issues that may affect some users.                             |
| <b>Restoring Service</b>   | A previous problem has been corrected and service is being restored. |
| <b>Out of Service</b>      | Certain features, or the entire service, may be unavailable.         |

Clicking an advisory badge opens a detail panel with the full advisory record — title, affected service, impact summary, advisory ID, affected feature groups, the latest message, and the complete message history, stored exactly as Microsoft published it.

## 6. Insight: Microsoft Updates

A searchable feed of Microsoft 365 change communications — Message Center posts and Microsoft 365 Roadmap items — so you can stay ahead of feature changes, retirements, and rollouts before a customer is surprised by one.

- Each update shows its title, affected product(s), category (updated / retirement / new feature / plan-for-change), latest update date, and a short excerpt, with a full detail view available.
- Filter by product, category, and date, or free-text search across title and body.

## Per-Tenant Relevance Filter

By default, every tenant sees the same full Microsoft update feed — this keeps things simple and requires no extra computation. Your organization can optionally turn on a per-tenant relevance filter that narrows the feed to only what's relevant to a given client's licenses and services.

**Tip.** This filter is off by default and fully reversible — turning it off simply returns you to the shared full feed, with nothing lost.

## 7. Control: User & License Lifecycle

The first set of write actions available lets you manage the core user lifecycle directly inside RebelPSA, without needing to jump into the Microsoft 365 admin center separately:

| Action                  | What It Does                                                                                        |
|-------------------------|-----------------------------------------------------------------------------------------------------|
| List users              | See every user in a client tenant with their status, license, and last sign-in.                     |
| Reset password          | Reset a user's password, with an option to force a password change at next login.                   |
| Edit contact info       | Update phone, job title, display name, and department.                                              |
| Add user                | Create a new user, assigning a license at the same time.                                            |
| Delete user             | Soft-delete (recoverable, recycle-bin aware), with a required confirmation.                         |
| Block / unblock sign-in | Disable or re-enable a user's ability to sign in, with a required confirmation.                     |
| Assign / remove license | Add or remove license SKUs (Stock Keeping Units), with your tenant's available license count shown. |

**Important.** Delete, and block/unblock sign-in, both require an explicit confirmation step before they execute — these are treated as meaningfully destructive/impactful actions, not one-click undo-able ones.

## 8. What's Not Here Yet

The following are planned in detail but are not available to use today. If a customer or colleague asks about any of these, the honest answer is: planned, not yet built.

- Groups, distribution lists, and Enterprise App role assignment
- Shared mailboxes, aliases, forwarding, and convert-to-shared for offboarding

- Intune device actions (wipe, retire, sync, compliance state)
- Per-user MFA reset/re-enrollment and Conditional Access review from within RebelPSA
- Bulk actions applied across multiple client tenants at once
- Tenant Assessments against frameworks like CIS, Essential 8, NIS2, or CMMC, and branded assessment reports
- Copilot readiness scoring and ongoing Copilot management
- Policy backup, restore, and drift detection
- SaaS/Shadow-IT discovery
- Broader reporting/usage analytics and compliance-readiness auditing
- Automated alerts-to-workflow, approval routing, and flow agents

## 9. Permissions

| Permission Area                | Grants                                                                                                                                          |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Insight: Security</b>       | View the security dashboard/scorecards; view or manage the alerts feed; view risky users/sign-ins, or act on them (dismiss/confirm-compromise). |
| <b>Insight: Service Health</b> | View the service status grid and advisory detail.                                                                                               |
| <b>Insight: Updates</b>        | View the updates feed; manage the per-tenant relevance filter.                                                                                  |
| <b>Control: Users</b>          | View, edit, create, or delete users; reset passwords; block/unblock sign-in — each a distinct permission.                                       |
| <b>Control: Licenses</b>       | Assign and remove licenses.                                                                                                                     |
| <b>Control: Connections</b>    | Connect or disconnect client tenants; set a connection's read-only vs. write-capable flag.                                                      |

## 10. Common Workflows

### Checking a client's security standing before a call

- Open that client's Security Scorecard and note their Secure Score and MFA adoption rate.
- Check the Risky Users panel for anything flagged that needs a conversation.
- Check Coverage Gaps for any devices with no security vendor reporting at all.

### Resetting a user's password for a client

- Open that client's user list and find the user.

- Use Reset Password, choosing whether to force a change at next login.
- Confirm the action — this executes directly against the customer's Microsoft 365 tenant.

### Staying ahead of a Microsoft change that could affect clients

- Check the Microsoft Updates feed regularly or search it when you hear about a change secondhand.
- Read the detail view for affected products and whether action is required.
- Communicate proactively with any affected client before the change lands, since update-to-ticket automation isn't built yet.

## 11. Quick Reference & Glossary

| Term                               | Meaning                                                                                                                                                      |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>GDAP</b>                        | Granular Delegated Admin Privileges — Microsoft's partner-relationship model; RebelPSA's primary connection method to customer M365 (Microsoft 365) tenants. |
| <b>Direct Connection</b>           | A per-client-company app registration, used as a fallback when GDAP isn't available or appropriate.                                                          |
| <b>Insight Plane</b>               | The read-and-alert side of the Ops Center — security posture, service health, and updates.                                                                   |
| <b>Control Plane</b>               | The write/action side of the Ops Center — currently user and license lifecycle.                                                                              |
| <b>Secure Score</b>                | Microsoft's own composite security posture metric for a tenant, surfaced on the Client Security Scorecard.                                                   |
| <b>Per-Tenant Relevance Filter</b> | An opt-in setting that narrows the Updates feed to a client's actual licenses/services.                                                                      |
| <b>Write-Capable Connection</b>    | A connection (GDAP or Direct) explicitly flagged as allowed to perform write actions, not just read.                                                         |