DESK PORTAL

User Guide

A multi-tenant PSA ticket portal — for clients, technicians, managers, and administrators.

Version 0.1.0

This guide covers everyday use of the portal: raising and following tickets, the productivity dashboards, and administering PSA connections and field mappings.

1. Getting started

Signing in

Open the portal and choose **Continue with SSO**. Authentication is handled by your organization's identity provider — you'll be returned to the dashboard once signed in. Your name and a **Sign out** option appear at the top right.

Finding your way around

The left sidebar is your main navigation. On a phone it collapses into a scrollable bar at the top. A light/dark theme toggle sits at the top right.

- **Tickets** — raise and follow your support requests.
- **Productivity** — technician & team performance (staff).
- **PSA Connections, Field Mapping, Integration Health, Background Jobs, Audit Log** — administration.

2. Raising & following tickets

Create a ticket

Go to **Tickets** → **New ticket**. Give it a short title, choose a priority, and describe the issue. On submit, the ticket is created in your provider's system (the PSA) and appears in your list.

Track progress

- The **ticket list** shows status, priority, queue and when each was raised.
- Open a ticket to see its **public conversation** and add a reply.
- **Attach files** from the ticket detail — they are scanned for malware; executables are blocked; 25 MB max. Only clean files can be downloaded.
- **Notifications** lists recent activity on your tickets.

> Internal notes your support team writes are never shown in the portal — you only ever see public replies.

3. Productivity dashboards (staff)

The **Productivity** page shows technician and team metrics: assigned, resolved, open and overdue tickets, SLA compliance, average resolution time, and time worked. A configurable **productivity score** combines several signals into a single number, with a breakdown per component. Use **Export CSV** to download the team view.

> Productivity scores are operational indicators only and must not be used as the sole basis for employee performance decisions. The score only counts signals that are actually measured, and reports how much of the model that covers.

4. Administration

PSA Connections

Connect Autotask and ConnectWise tenants under **PSA Connections**.

- **Add connection** — name it, choose the provider, enter the API endpoint and credentials. Credentials are stored in a secure secret vault, never in the database and never shown again.
- **Edit** — change settings; leave the credential fields blank to keep the existing keys, or enter new ones to rotate.
- **Test** — runs a live check against the PSA and updates the connection's health status.
- **Boards** — discovers the connection's service boards/queues, statuses, priorities and categories live.

Rotating PSA credentials

If an API key is ever exposed, rotate it promptly. The portal is built so this needs no redeploy and no code or config changes:

- In your PSA, revoke the exposed key and generate a new one. In **ConnectWise Manage** this is **System** → **Members** → **API Members**: open the member, delete the old key pair on the **API Keys** tab, then create a new pair. The new private key is shown only once — copy it immediately.
- In the portal, open **PSA Connections** → **Edit** for that connection and enter the new credentials. Sensitive fields are masked and are never pre-filled, so type the new key(s) and save.
- Leaving a credential field blank keeps the current value; only the fields you fill are overwritten in the secret vault.
- Click **Test** to confirm the new key works, then check **Integration Health**.

> Never paste API keys into chat, tickets, email, code, or config files. The portal only accepts credentials through the masked fields on this screen, which write straight to the secret vault — treat any key that has been shared anywhere else as compromised and rotate it.

Field Mapping

Under **Field Mapping**, translate the portal's neutral values to each PSA's real values — this is how the portal and your PSA agree on what a status, priority, queue or category means.

- Pick a **connection** and a **field** (Status, Priority, Queue/Board, Category).
- For status and priority, map each portal value to a discovered PSA value.
- For queues and categories, add a mapping by naming a portal value and picking the PSA value.
- Each save is stored as a new **version** and recorded in the audit log, so changes can be reviewed.

Monitoring & audit

- **Integration Health** — per-connection status, pending jobs, dead-lettered jobs and failed events.
- **Background Jobs** — monitor sync jobs and **reprocess** any that dead-lettered.
- **Audit Log** — an immutable record of administrative and security events (connection changes, mapping updates, tests, job reprocessing).

5. Security & your data

- Each organization's data is fully isolated — you only ever see your own.

- PSA credentials live only in the secret vault; they are never returned to the browser or written to logs or the audit trail.
- Access is governed by role-based permissions (client user, client administrator, technician, manager, administrator, auditor).
- Attachments are validated and malware-scanned; downloads use short-lived, signed links.

6. Getting help

If a page shows a “sign in” or empty state where you expect data, your session may have expired — sign in again. For anything else, contact your MSP administrator, who can review the audit log and integration health to diagnose issues.