NOMAD SMALL BUSINESS SUITE

Service Desk Pro - Manager Role Guide

A role-specific guide for managing the complete support operation without settings, role, licensing, billing, financial quote or permanent-deletion access.

Edition: 1.1.3
Audience: Service Desk Managers and operational supervisors

Contents

This guide is based on the verified product package and is written as an operational reference. Use the online version for navigation and this PDF for offline access.

1. Role purpose and access boundary

The Service Desk Manager controls day-to-day service delivery across all tickets, customers and resources while configuration, roles, billing and destructive actions remain with authorised administrators.

Who should receive this access

Assign this role to the person accountable for queue quality, assignment, customer communication, workload and operational reporting. It is deliberately narrower than Service Desk Administrator and should be the normal highest role for an operations manager who does not administer the platform.

What this role can see

- All tickets and ticket histories
- All customers and operational customer data
- All resources, capacity and workload
- Internal notes, customer-visible and staff ticket files
- Quote-required indicators and quote status without financial creation controls
- Operational analytics and report exports

What this role can do

- Create, edit, assign, escalate, reopen and close tickets
- Reply to customers and add internal notes
- Upload files, log time and capture sign-off
- Manage customer records
- Maintain operational resource records and capacity
- Use Ticket AI and export operational reports

What this role cannot do

- Create financial quotes or use billing controls
- View or edit rates and billable financial values
- Change Service Desk settings, AI resources or integrations
- Create users, assign roles or change WordPress user links
- Synchronise HR users
- Permanently delete tickets or access licensing

2. Sign-in, navigation and account setup

Start with the correct named account and confirm that the visible workspace matches the assigned access.

First sign-in

1. Sign in with the named Manager account.
2. Confirm landing on Support Desk > Dashboard.
3. Confirm Dashboard, Tickets, Add Ticket, Customers, Resources and Analytics are available.
4. Confirm Billing, Users & Roles, Settings, AI Settings and Licence are absent.
5. Open a controlled ticket and test assignment, reply, file, time, sign-off and AI.
6. Confirm a financial quote or deletion action is unavailable.

Navigation

Area	Availability or purpose
Dashboard	All-ticket operational overview
Tickets / Add Ticket	Full operational ticket management
Customers	View and manage
Resources	Operational details, capacity and availability; no user links or rates
Analytics	Operational measures and export
Billing / Users / Settings / Licence	Not available

Account and resource relationship

A Manager receives an active staff resource profile and can be assigned to tickets. The role can manage resource operations but cannot change linked WordPress users, roles, HR-user synchronisation, rates or billing information.

3. Daily operating routine

Use a consistent routine so ownership, communication and audit records remain current.

Start of day or session

- Validate urgent and high-impact tickets
- Assign new and unassigned work
- Review customer replies on Waiting tickets
- Check resource workload and onsite commitments
- Review failed file or communication events

During the day

- Maintain priority, ownership and lifecycle status
- Review public reply and internal handover quality
- Resolve assignment conflicts
- Verify time and sign-off records
- Escalate configuration or financial work to the correct owner

End of day or session

- Hand over urgent unresolved work
- Review long-running Pending and newly answered Waiting tickets
- Confirm onsite outcomes and sign-off
- Review incomplete time records
- Record platform or access issues for the Administrator

4. Primary workflow

Manage the complete operational queue without crossing into configuration or commercial creation.

Manager queue procedure

1. Review impact, customer and duplicate status.
2. Assign the support owner and primary/additional resources.
3. Confirm the first useful customer response.
4. Monitor progress, blockers and customer requests.
5. Review files, internal evidence and time quality.
6. Approve operational resolution or reopen incomplete work.
7. Confirm sign-off and next-action status.
8. Escalate quote creation, billing, deletion or settings work to the authorised role.

Decision and quality rules

- Use priority for impact, not convenience
- Pending must have an active or scheduled support action
- Waiting on Customer requires a clear public request
- Operational quote status may be reviewed but financial quote creation is restricted
- Do not ask an Administrator to bypass a role restriction; hand over the restricted task

5. Communication, notes and records

Create records that another authorised person can understand without relying on memory or a separate email.

Record standards

Record	Required content
Triage note	Impact, priority rationale, assignment and next action
Customer reply	Confirmed state, action, owner and required customer response
Internal handover	Evidence, work completed, blocker, risk and new owner
Resource update	Capacity/availability change and operational reason
Resolution review	Completion evidence, sign-off and reopen/close decision

Visibility rules

Content	This role's access or responsibility
All tickets	Visible and operationally manageable
Internal notes/staff files	Visible
Customer/resource operational records	Visible and manageable
Rates/billing/financial quote PDFs	Hidden or unavailable
Settings/users/licence	Unavailable

Information protection

- Use customer data only for service delivery
- Confirm file visibility and notification recipients
- Keep management reasoning internal when it is not customer-appropriate
- Do not request credentials in tickets
- Mask sensitive evidence in exported reports

6. Handover and escalation

Escalate work with enough verified context for the next authorised role to act safely.

Escalate when

- Settings, users, roles or WordPress user links must change
- Billing, rate or financial quote action is required
- Permanent deletion is requested
- A cross-customer access or file incident is suspected
- Plugin, licence, hosting or database administration is required

Handover procedure

1. Record the operational outcome and affected ticket/customer.
2. State the restricted action required.
3. Provide evidence without credentials.
4. Name the responsible Administrator, finance or site owner.
5. Record any deadline and customer expectation.
6. Verify the authorised owner accepted the handover.

Escalation evidence

- Ticket and customer
- Current assignment/status/priority
- Exact action and timestamp
- Relevant non-secret file or mail ID
- Expected result and operational impact

7. Access problems and recovery

Identify expected restrictions before treating them as faults.

Access troubleshooting

Problem	Check or action
Billing menu missing	Expected Manager restriction
Cannot create quote	Expected; hand financial creation to Administrator/finance owner
Cannot change linked user	Expected; only Service Desk Administrator can change links/roles
Cannot open Settings or Licence	Expected role boundary
Cannot delete ticket	Expected; permanent deletion is Administrator-only

Do not bypass the role model

- Do not request direct per-user capabilities
- Do not use another person's Administrator account
- Do not store rates in internal notes to work around hidden financial fields
- Do not repeatedly submit a restricted action
- Do not export more customer information than the review requires

8. Quick reference and review

Use this checklist during onboarding, supervision and periodic access review.

Role checklist

- Service Desk Manager role
- Active staff resource
- All-ticket operational scope
- Expected six menus
- No financial/configuration/destructive access
- Permitted and prohibited tests passed
- Escalation owners documented

Periodic review

1. Review current Manager accounts.
2. Confirm their operational responsibility.
3. Sample assignments, replies, time and resource changes.
4. Check that no direct capabilities or broader WordPress role were added.
5. Retest hidden menus and financial restrictions after updates.

Related master documentation

- Service Desk Pro Detailed User Guide
- Service Desk Pro Administrator Role Guide
- Dispatcher and Technician Role Guides
- Customer / Requester Portal Guide