NOMAD SMALL BUSINESS SUITE

Service Desk Pro - Reporting Viewer Role Guide

A read-only guide for dashboards, ticket history, operational analytics and exports, including masking and the actions deliberately unavailable to this role.

Edition: 1.1.3
Audience: Management viewers, auditors and 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 Reporting Viewer reviews service performance without changing operational records. It can see all tickets in a privacy-reduced view and use operational analytics and exports, but it cannot communicate, edit, assign, upload, record work or administer the desk.

Who should receive this access

Assign this role to an authorised manager, auditor or supervisor who needs operational evidence but no write access. Confirm that all-ticket reporting is necessary before assigning it, even though sensitive fields are masked or hidden.

What this role can see

- Read-only ticket dashboards and all-ticket history
- Ticket volumes, trends and lifecycle status
- Operational workload and performance measures
- Closed-ticket history
- Operational analytics and report exports
- Customer-visible ticket content
- Customer identity/contact in a masked form where the view applies privacy controls

What this role can do

- Filter and review the all-ticket list
- Open read-only ticket records
- Review dashboard and analytics measures
- Export operational reports available to the role
- Raise a correction request with the operational owner
- Use reports for the approved management or audit purpose

What this role cannot do

- Create or edit tickets
- Reply to customers or add internal notes
- Assign or reassign resources
- Change status, priority or category fields
- Upload or download staff-only files
- View internal notes or staff-only ticket attachments
- View financial quote PDFs, rates, billing or financial controls
- Use time, sign-off or Ticket AI actions
- Manage customers, resources, settings, users, roles, integrations, licensing or deletion

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 Reporting Viewer account.
2. Confirm landing on Support Desk > Dashboard.
3. Confirm Tickets and Analytics are available in read-only form.
4. Confirm Add Ticket, Customers, Resources, Billing, Users & Roles, Settings, AI and Licence are absent.
5. Open a controlled ticket and verify customer contact is masked and internal notes/staff files are hidden.
6. Attempt an edit, reply, upload and status change; each must be denied.

Navigation

Area	Availability or purpose
Dashboard	Read-only operational overview
Tickets	All-ticket read-only review with privacy controls
Analytics	Operational measures and export
Add Ticket / Customers / Resources	Not available
Billing / financial quotes	Not available
Users / Settings / AI / Licence	Not available

Account and resource relationship

A Reporting Viewer is not an assignable staff resource. Creating or changing a user to this role does not create a resource and deactivates an existing linked resource so the account cannot receive technician assignments.

3. Daily operating routine

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

Start of day or session

- Confirm the reporting period and approved purpose
- Check dashboard freshness and filters
- Identify missing or unusual records for follow-up
- Confirm exports are stored only in the approved location

During the day

- Use consistent filters and date ranges
- Distinguish current workload from closed history
- Record the source report and generation time
- Raise data-quality issues without editing records
- Avoid unnecessary export of customer-level detail

End of day or session

- Close local report files not required for retention
- Record material findings and their source
- Assign correction requests to an operational owner
- Confirm no report was sent to an unauthorised recipient
- Sign out of shared devices

4. Primary workflow

Produce a traceable operational review without changing source tickets.

Reporting review procedure

1. Define the question, period, population and authorised audience.
2. Open Dashboard or Analytics and apply the documented filters.
3. Validate totals against a controlled ticket sample.
4. Review lifecycle, workload or performance measures in context.
5. Export only when the audience and storage location are approved.
6. Record report name, filters and generation time.
7. Raise source-data corrections with the Manager or Administrator.
8. Retain or dispose of the report under the organisation's policy.

Decision and quality rules

- Read-only access does not remove confidentiality obligations
- Use the minimum customer detail necessary
- Do not interpret a masked field as missing source data
- Reports reflect the data recorded at generation time
- Raise corrections through the ticket owner; do not request write access for routine reporting
- Operational analytics are not automatically a contractual SLA or financial statement

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
Report request	Question, period, population, requester and approved audience
Filter record	Date range, status, customer/resource scope and exclusions
Finding	Measure, source, comparison and material limitation
Correction request	Ticket/record, observed inconsistency, expected owner and due date
Export log	Filename, generation time, recipient/storage and retention decision

Visibility rules

Content	This role's access or responsibility
All tickets	Read-only
Customer contact	Masked where the reporting ticket view applies masking
Internal notes and staff files	Hidden
Customer-visible ticket content	Visible for authorised review
Financial quote PDFs, rates and billing	Hidden/unavailable
Settings, credentials and users	Unavailable

Information protection

- Export only the fields required for the approved purpose
- Store reports in an access-controlled location
- Do not attempt to reverse masked data
- Do not share raw ticket exports through unapproved channels
- Remove local copies according to retention policy
- Escalate any apparent cross-customer exposure immediately

6. Handover and escalation

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

Escalate when

- A source record appears inaccurate or incomplete
- A report exposes more customer detail than expected
- Internal or financial information appears unexpectedly
- A measure cannot be reconciled to ticket data
- A new report or field requires configuration
- An auditor requires evidence outside the role's approved scope

Handover procedure

1. Record the report and exact filters.
2. Identify the affected ticket, measure or field.
3. Describe the discrepancy without altering source data.
4. Attach only an appropriately protected extract.
5. Name the Manager, Administrator or data owner required.
6. Confirm the correction and report-rerun owner.

Escalation evidence

- Report/dashboard name
- Date range and filters
- Generation timestamp
- Ticket IDs from a controlled sample
- Expected and observed totals
- Approved audience and storage location

7. Access problems and recovery

Identify expected restrictions before treating them as faults.

Access troubleshooting

Problem	Check or action
Customer details are masked	Expected privacy control
Internal notes or staff files are missing	Expected Reporting Viewer restriction
Cannot edit, reply or change status	Expected read-only boundary
Export is empty	Check filters, reporting period and ticket population
Totals differ	Record filters and sample records; ask the Manager to review source data
Menu redirects	The page is outside the viewer's approved capability

Do not bypass the role model

- Do not request direct edit capabilities for reporting convenience
- Do not reuse another role's account
- Do not alter URLs to reach hidden content
- Do not combine exports with unrelated data to identify masked people
- Do not publish raw ticket exports

8. Quick reference and review

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

Role checklist

- Named Reporting Viewer account
- No active assignable resource
- Dashboard/Tickets/Analytics only
- All-ticket read-only scope
- Masking and hidden staff content confirmed
- Edit/action tests denied
- Export handling approved

Periodic review

1. Review current Reporting Viewer accounts and business purpose.
2. Confirm all-ticket access remains necessary.
3. Sample masking and hidden-content controls.
4. Review exports, recipients and retention.
5. Disable unnecessary accounts and repeat prohibited-action tests.

Related master documentation

- Service Desk Pro Detailed User Guide
- Service Desk Pro Implementation Guide
- Service Desk Manager Role Guide
- Customer / Requester Portal Guide