DeskGate

TECHNICAL HELP & OPERATIONS REFERENCE

25 essential views.
One operating model.

A portrait technical guide to administration, workforce intelligence, protection, remote support, audit, inventory, deployment, and system operations.

DESIGNED FOR QUICK TECHNICAL LOOKUP

Purpose + signals + controls + safe operating steps

01 / OPERATING MODEL

From trusted scope to action

Every screen belongs to the same tenant-aware operating loop.

1

Identity

Authenticated corporation and administrator

2

Scope

Groups, users, stations, and assignments

3

Evidence

Activity, work, support, audit, and inventory signals

4

Action

Policies, alerts, support, reports, and deployment

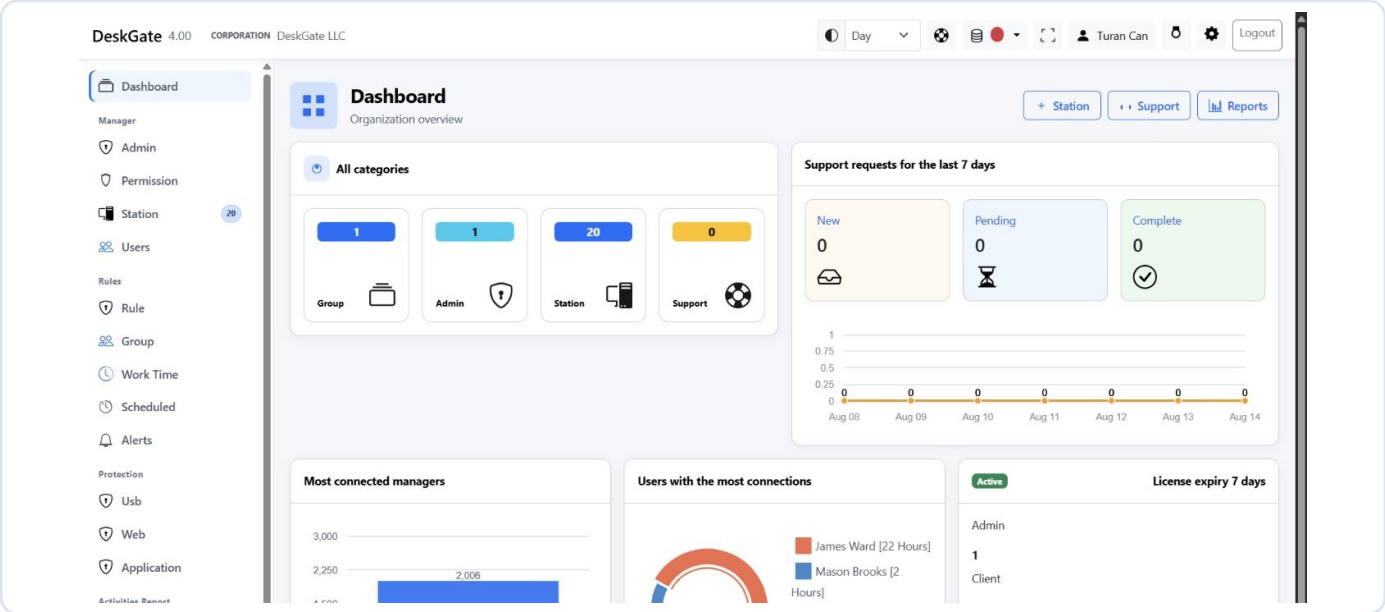
NON-NEGOTIABLE TENANT SAFETY

All reads, updates, deletes, exports, bulk actions, and relationship assignments must be restricted with the authenticated server-side corporation scope. A client-supplied identifier is never sufficient authorization.

02 / DASHBOARD

Dashboard

Organization health and first-line operational triage.



PURPOSE

Review current system health.

DATA / SIGNAL

Station, support, license, storage, and connection summaries.

KEY CONTROLS

Quick actions, category cards, charts, license panel.

OPERATING STEPS

1. Confirm totals.
2. Scan exceptions.
3. Open the relevant module.

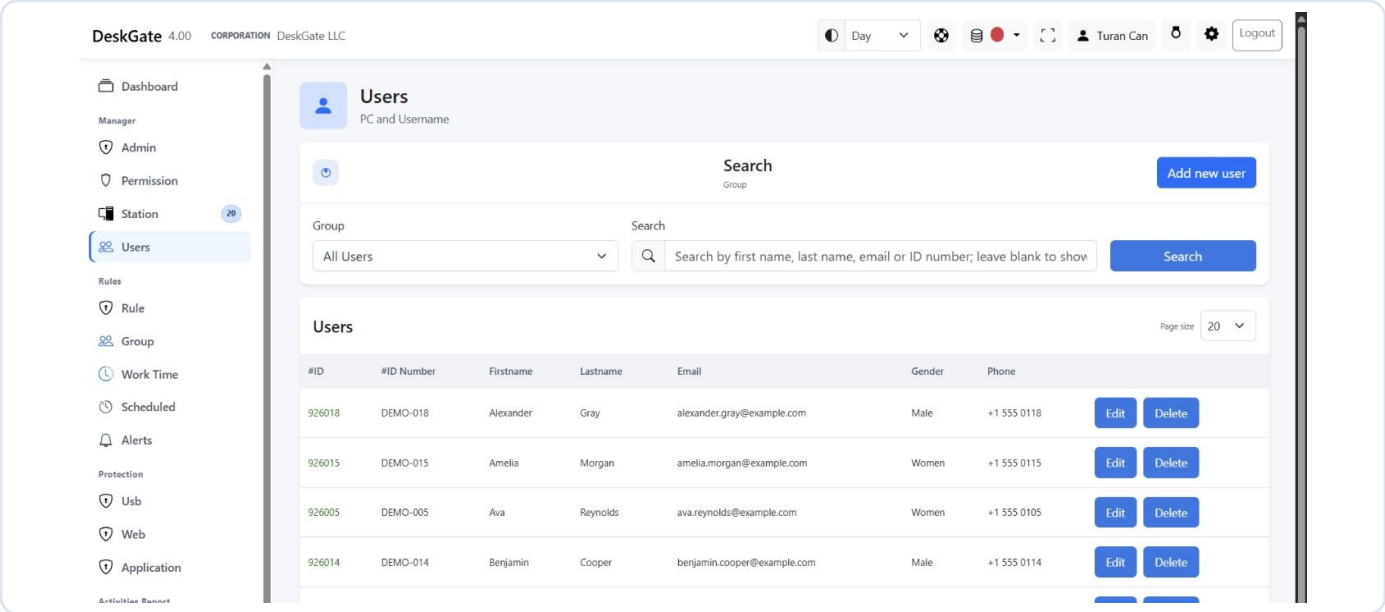
TECHNICAL NOTE

Dashboard indicators guide investigation; they are not standalone performance judgments.

03 / USERS

Employee directory

Maintain employee identity and endpoint relationships.



PURPOSE

Manage employee profiles.

DATA / SIGNAL

Employee identity linked to computer and Windows account.

KEY CONTROLS

Group filter, search, create, edit, page size.

OPERATING STEPS

1. Filter scope.
2. Verify identity.
3. Update permitted fields.
4. Save and recheck.

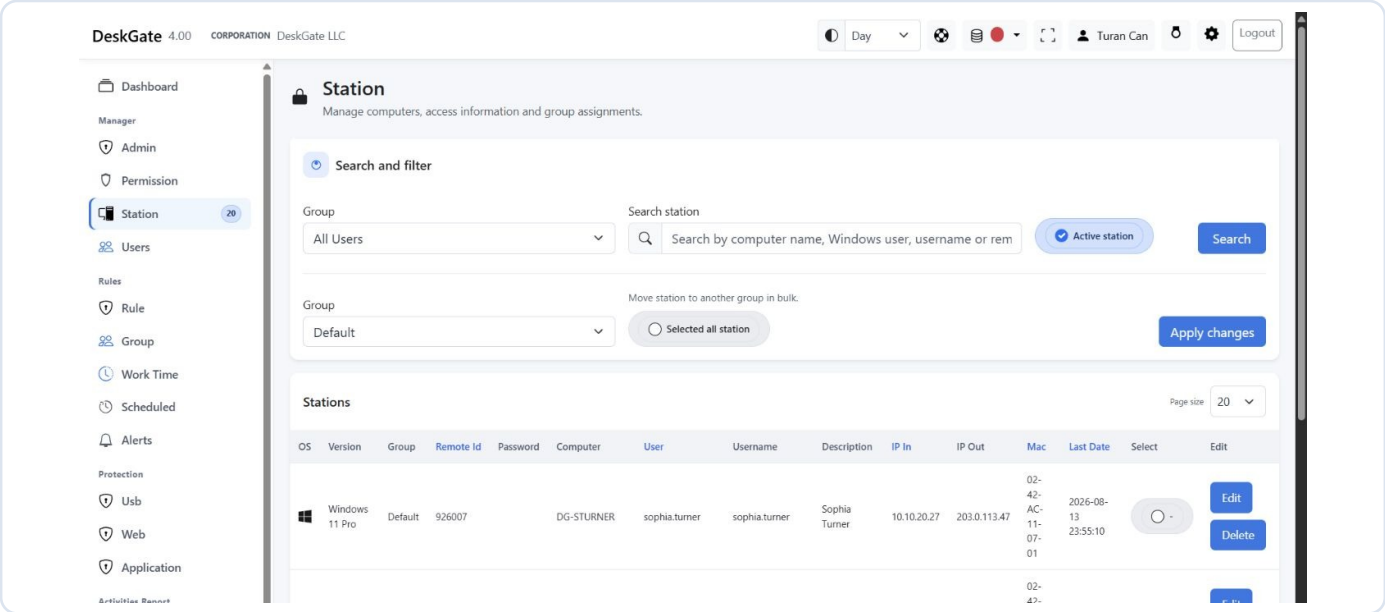
TECHNICAL NOTE

Ownership comes from the authenticated corporation, never from a submitted form value.

04 / STATIONS

Endpoint administration

Review connected computers, status, identity, network, and last activity.



PURPOSE

Manage trusted endpoints.

DATA / SIGNAL

Station identity, group relationship, Windows account, IP, MAC, last date.

KEY CONTROLS

Status filter, group, search, edit, list state.

OPERATING STEPS

1. Find endpoint.
2. Confirm group and owner.
3. Review status.
4. Apply scoped changes.

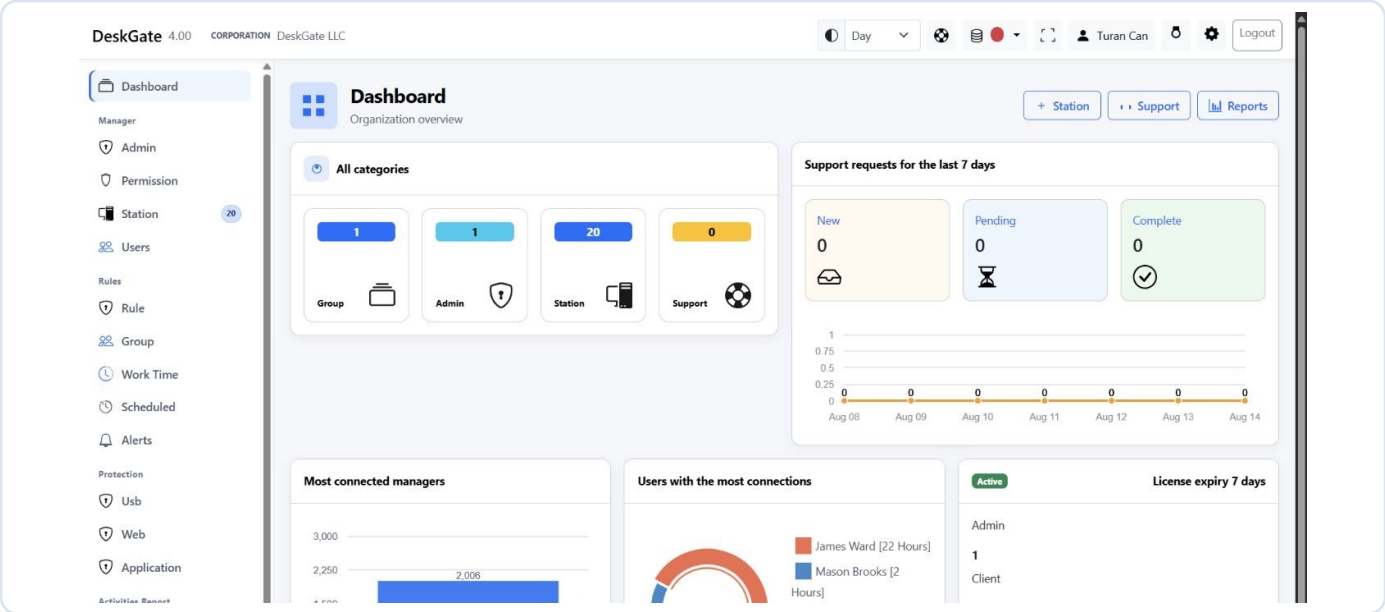
TECHNICAL NOTE

Validate both station and destination group before reassignment.

05 / ADMINISTRATION

Administrators & permissions

Apply least privilege to administrative access.



PURPOSE

Control administrative access.

DATA / SIGNAL

Administrator identity, allowed groups, feature permissions, active state.

KEY CONTROLS

Administrator list, permissions, groups, activation controls.

OPERATING STEPS

1. Verify role need.
2. Select minimum permissions.
3. Restrict groups.
4. Review regularly.

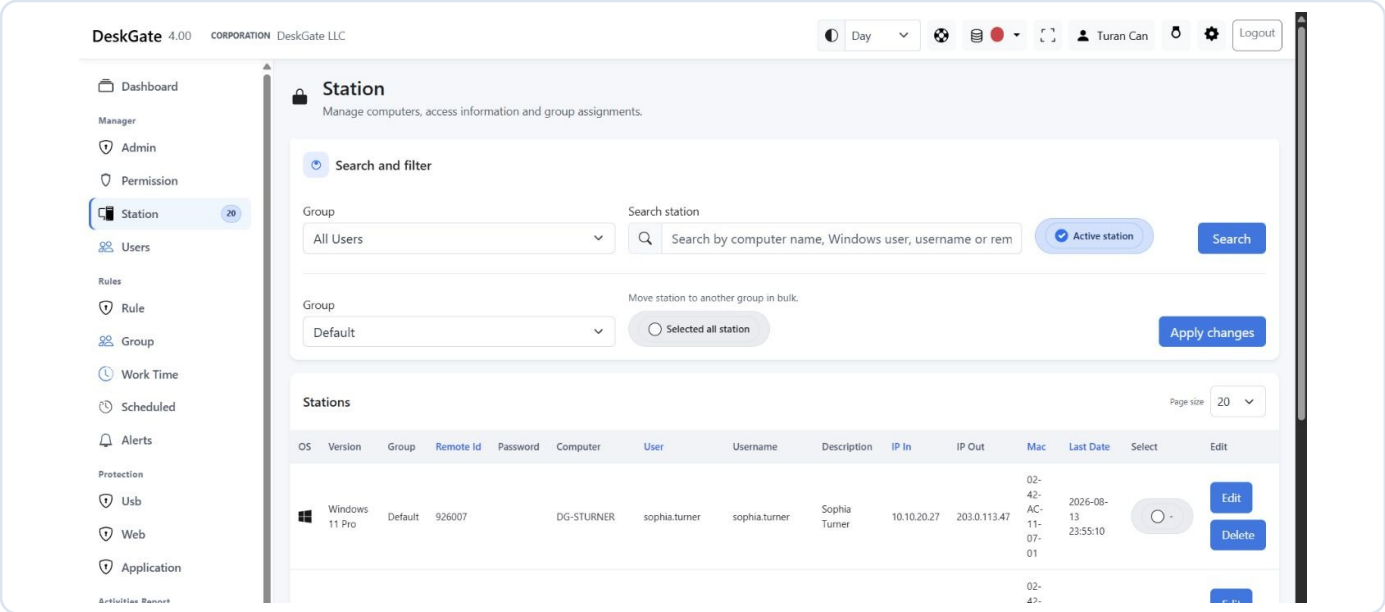
TECHNICAL NOTE

Do not reuse credentials. Disable unused accounts and retain an auditable access history.

06 / GROUPS

Groups & assignment

Organize users and computers into manageable policy scopes.



PURPOSE

Create operational scopes.

DATA / SIGNAL

Group definitions and endpoint relationships.

KEY CONTROLS

Create group, rule association, station assignment.

OPERATING STEPS

1. Define purpose.
2. Create group.
3. Attach rule.
4. Assign tenant-owned endpoints.

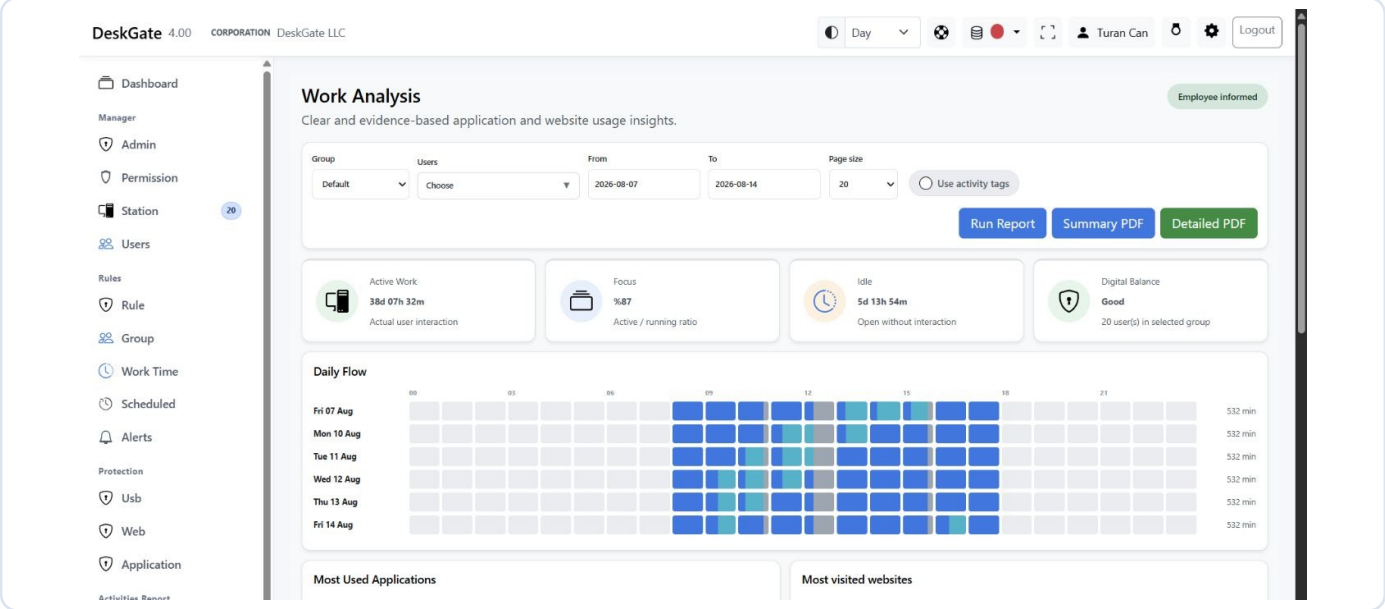
TECHNICAL NOTE

Validate every selected endpoint and rule inside the same corporation.

07 / WORK TIME

Work-time definitions

Define expected work windows without changing connection behavior.



PURPOSE

Set reporting and rule time context.

DATA / SIGNAL

Weekly day definitions and daily start/end windows.

KEY CONTROLS

Work-time profile, day rows, start/end, active state.

OPERATING STEPS

1. Create profile.
2. Configure each day.
3. Validate overnight cases.
4. Assign through rules.

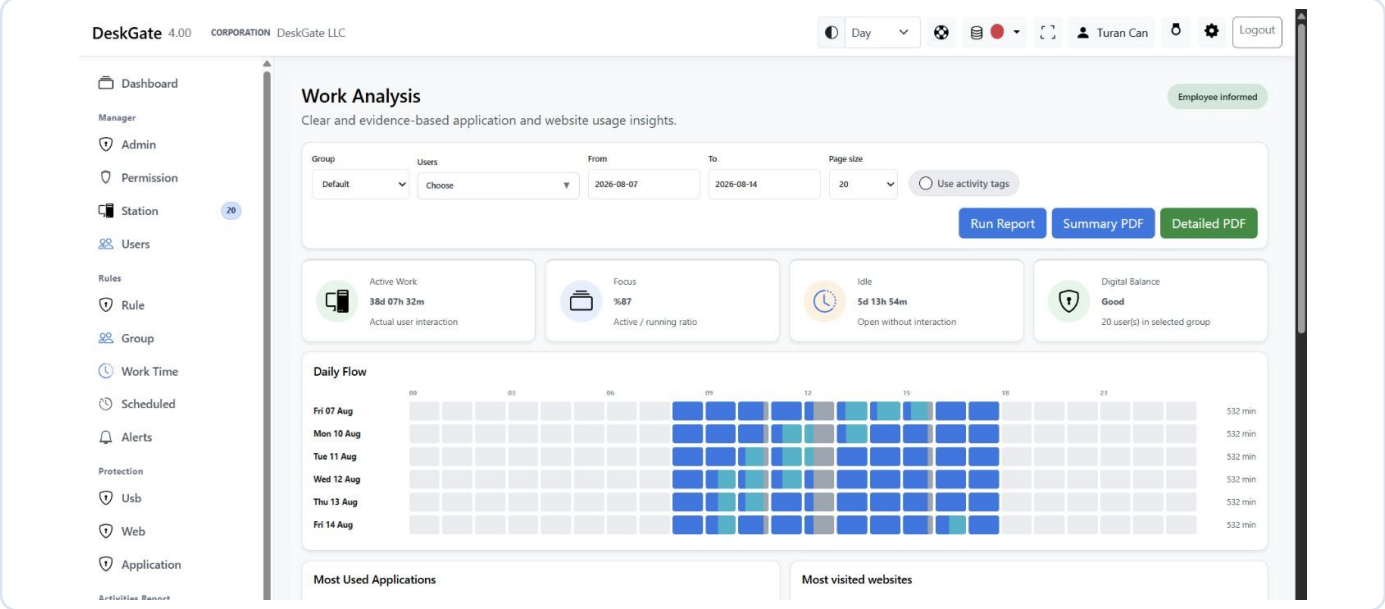
TECHNICAL NOTE

Work-time context affects interpretation and alerts; it must not silently alter socket sequencing.

08 / APPLICATION POLICY

Application controls

Define application allow, block, and monitoring behavior.



PURPOSE

Control application usage by policy.

DATA / SIGNAL

Application definitions, executable identity, list entries, group rule.

KEY CONTROLS

Policy status, executable, hash/name, work-time binding.

OPERATING STEPS

1. Identify application.
2. Choose behavior.
3. Attach to rule.
4. Validate endpoint scope.

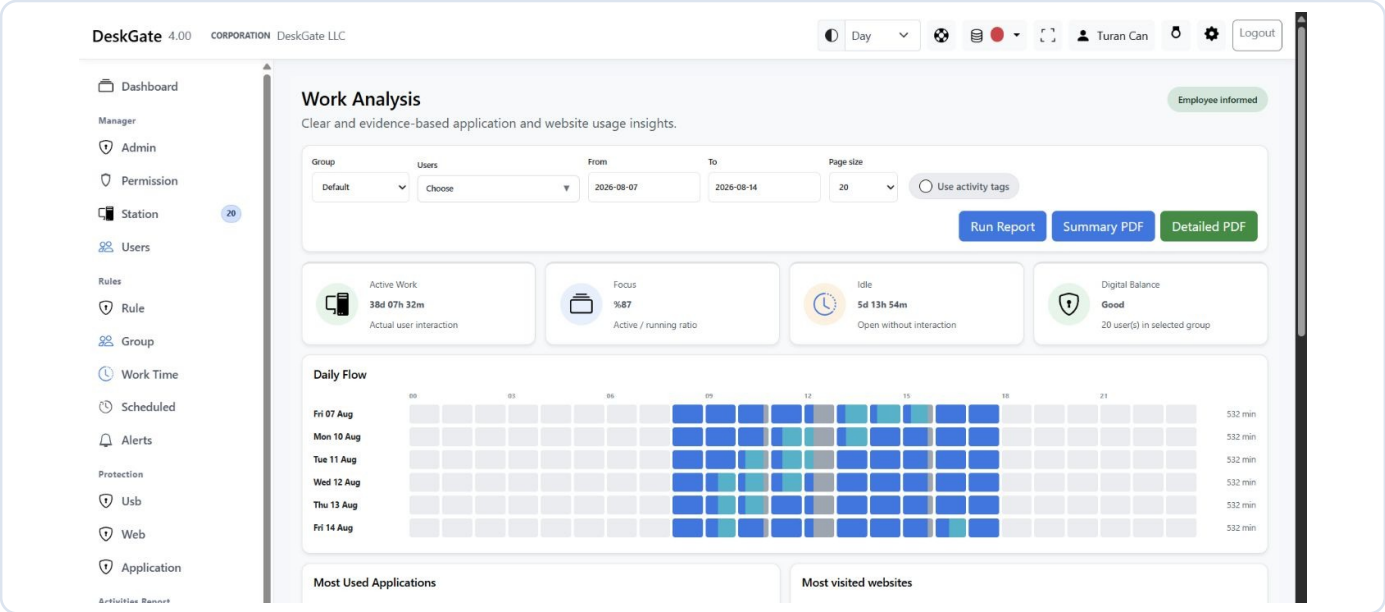
TECHNICAL NOTE

Use stable executable identity and review false positives before enforcement.

09 / WEB POLICY

Web controls

Manage website rules and inspect web usage context.



PURPOSE

Control website access by policy.

DATA / SIGNAL

Web definitions, URL entries, group rules, work-time context.

KEY CONTROLS

Domain/URL list, status, rule assignment, schedule.

OPERATING STEPS

1. Normalize domain.
2. Select behavior.
3. Bind to rule.
4. Test expected access.

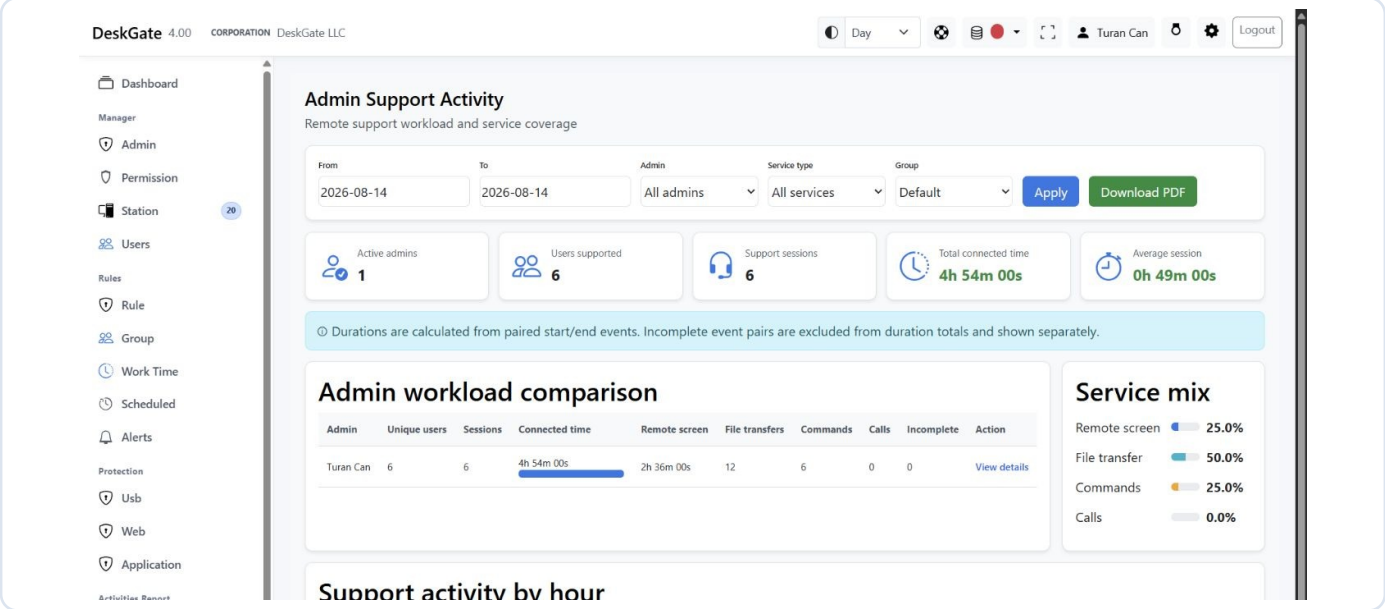
TECHNICAL NOTE

Avoid overly broad patterns. Validate URL scope and tenant ownership before updates.

10 / USB POLICY

USB & removable media

Control removable media while preserving event evidence.



PURPOSE

Manage USB device behavior.

DATA / SIGNAL

USB policy, serial/drive entries, file-operation events.

KEY CONTROLS

Allow/block list, serial, drive, notification, group rule.

OPERATING STEPS

1. Define policy.
2. Add trusted devices.
3. Assign group.
4. Review USB events.

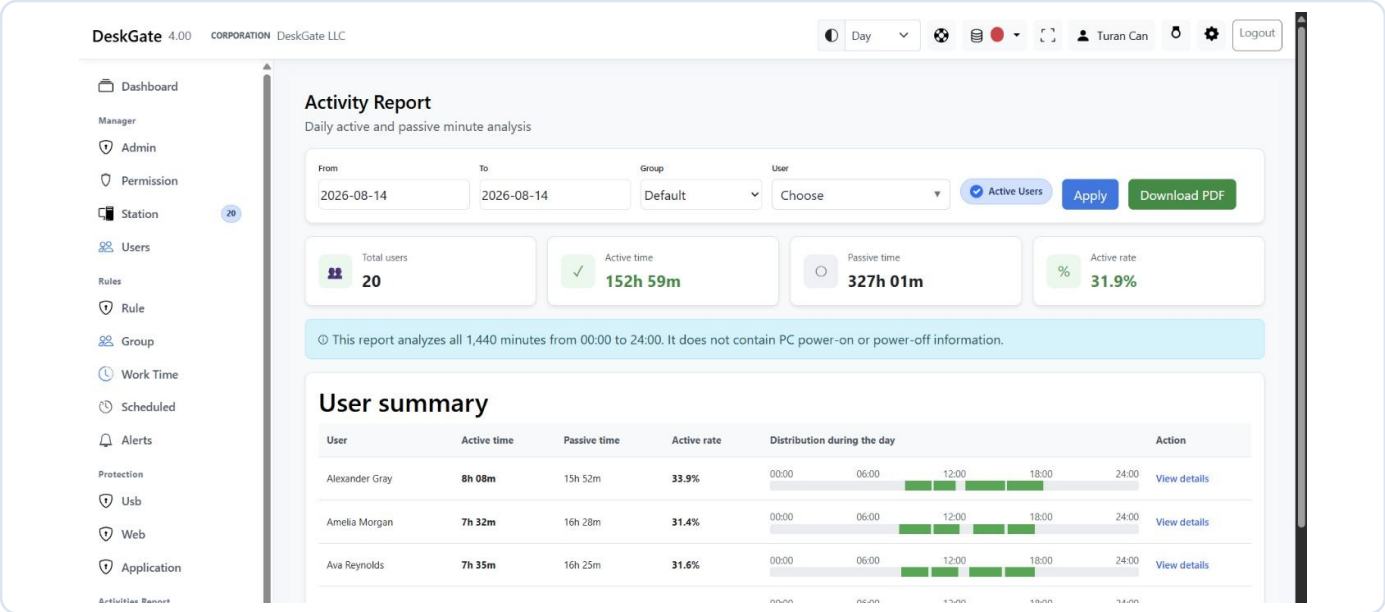
TECHNICAL NOTE

Source and destination paths may contain sensitive data. Restrict access and exports.

11 / ACTIVITY

Daily activity report

Analyze active and passive minutes with daily timelines.



PURPOSE

Review daily interaction patterns.

DATA / SIGNAL

One 1,440-minute activity map per employee and day.

KEY CONTROLS

Date range, group, user selection, active users, PDF.

OPERATING STEPS

1. Set scope.
2. Run report.
3. Compare balance.
4. Open detail or export.

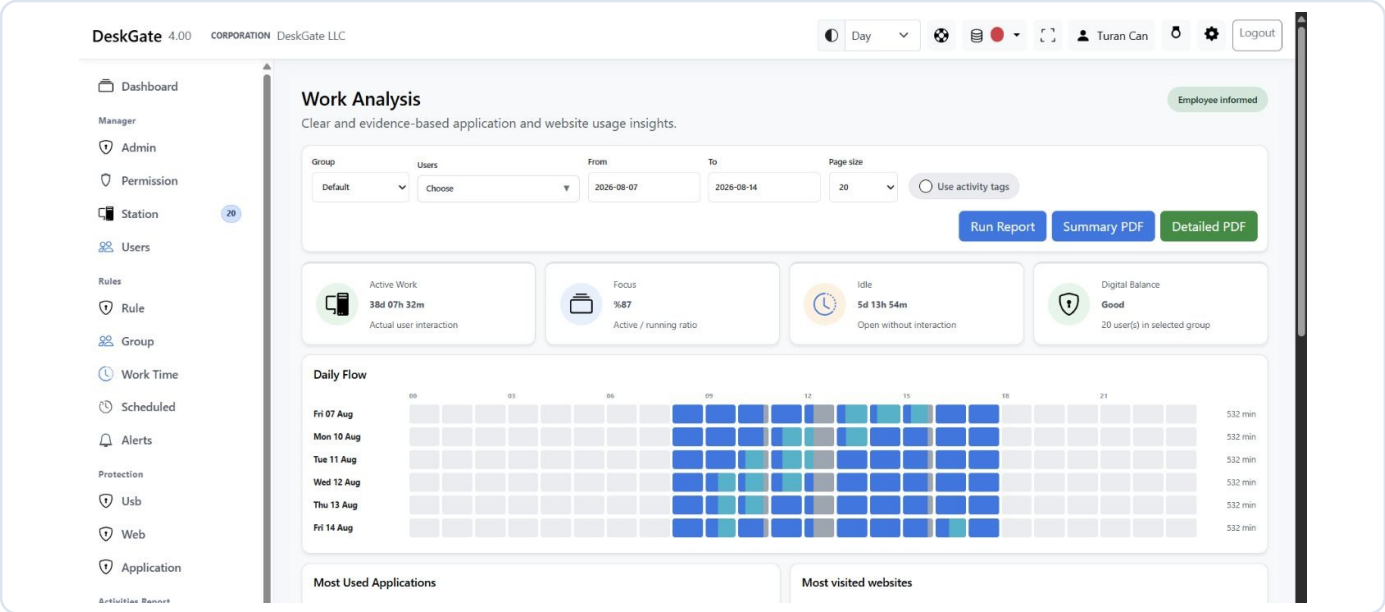
TECHNICAL NOTE

The minute map does not itself prove power-on or power-off time.

12 / WORK ANALYSIS

Work Analysis

Compare focus, idle time, applications, websites, and daily flow.



PURPOSE

Turn raw activity into operational insight.

DATA / SIGNAL

Application/web intervals, activity maps, keyboard and USB summaries.

KEY CONTROLS

Scope, date range, activity tags, summary PDF, detailed PDF.

OPERATING STEPS

1. Select scope.
2. Run report.
3. Review flow and mix.
4. Investigate anomalies.

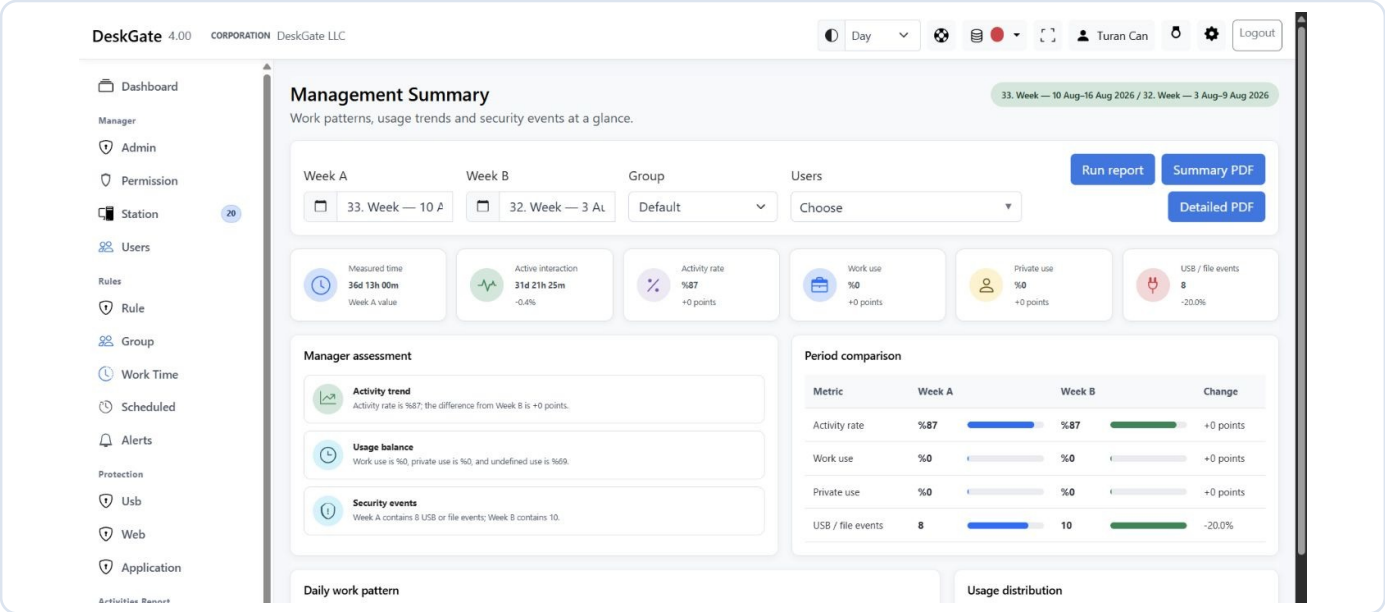
TECHNICAL NOTE

Aggregates require context. Validate detail before employment or security decisions.

13 / MANAGEMENT

Management summary

Present concise KPIs for leadership review.



PURPOSE

Summarize team-level operating signals.

DATA / SIGNAL

Coverage, active work, focus, category distribution, trends.

KEY CONTROLS

Period, group/users, KPI cards, export.

OPERATING STEPS

1. Verify coverage.
2. Read trends.
3. Compare groups.
4. Share with context.

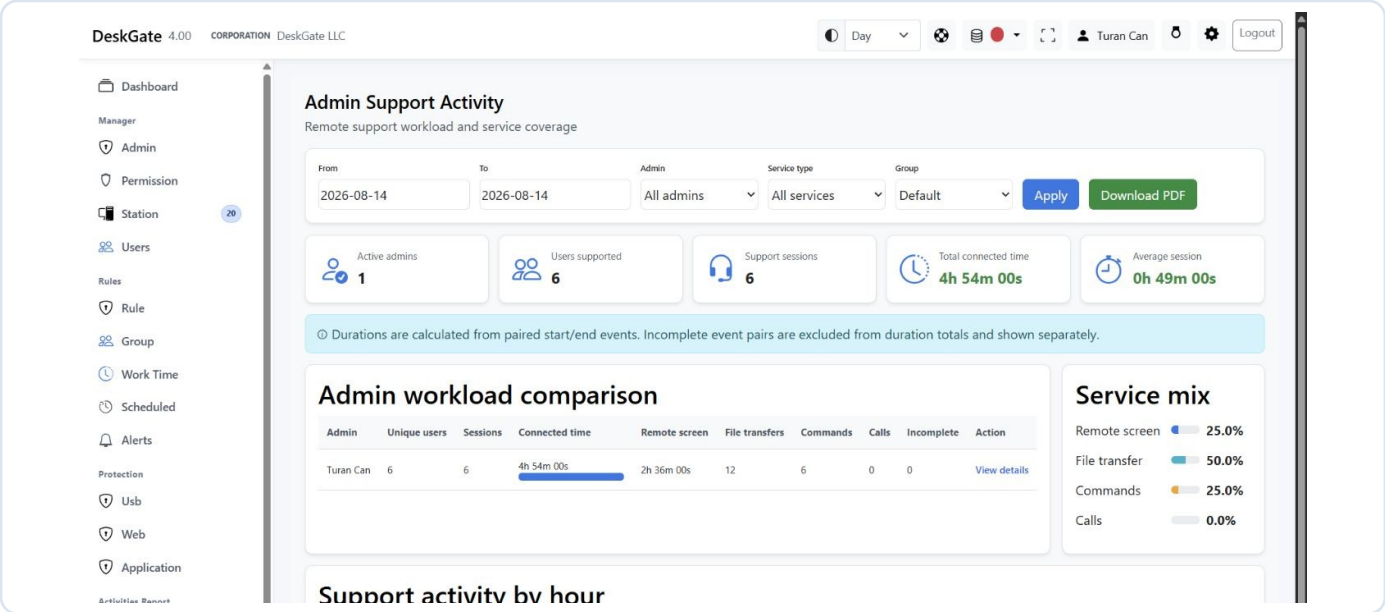
TECHNICAL NOTE

A management summary is decision support, not an automated employee score.

14 / REMOTE SUPPORT

Support activity

Audit connections, remote screen, file transfer, commands, and calls.



PURPOSE

Measure remote support delivery.

DATA / SIGNAL

Paired support events and durations by administrator and employee.

KEY CONTROLS

Date, administrator, service type, group, details, PDF.

OPERATING STEPS

1. Filter scope.
2. Review workload.
3. Inspect service mix.
4. Check event pairs.

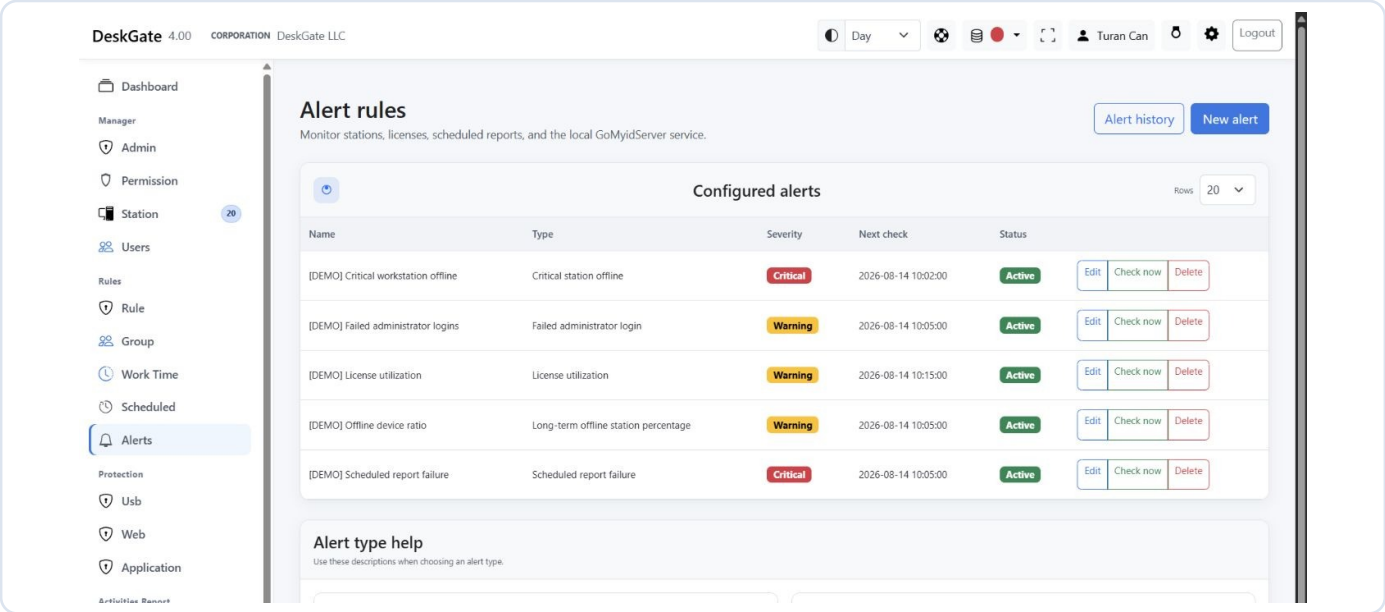
TECHNICAL NOTE

Incomplete start/end pairs are excluded from duration totals and shown separately.

15 / ALERT RULES

Alert rules

Configure detection for device, license, login, service, and report failures.



PURPOSE

Automate exception detection.

DATA / SIGNAL

Threshold, scope, severity, duration, interval, notification state.

KEY CONTROLS

New alert, history, check now, edit, status.

OPERATING STEPS

1. Choose type.
2. Define scope.
3. Set threshold.
4. Assign an owner.

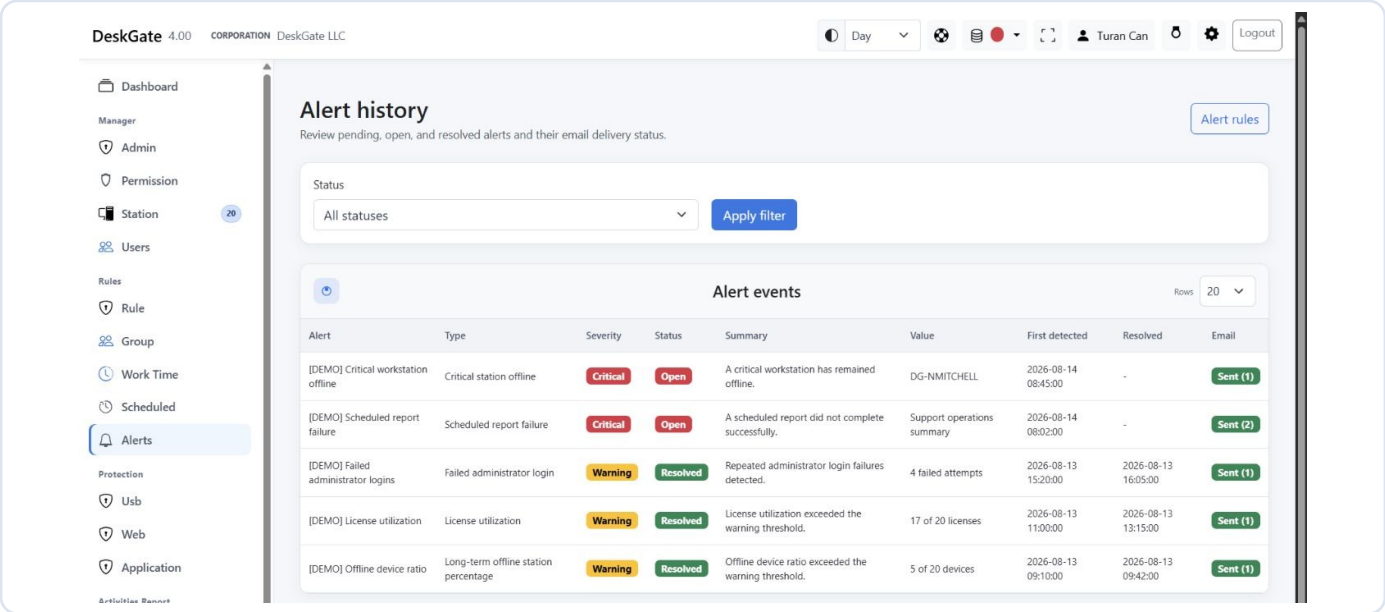
TECHNICAL NOTE

Every active alert needs a documented response expectation.

16 / ALERT HISTORY

Alert history

Review pending, open, resolved, and notified events.



PURPOSE

Preserve detection and recovery evidence.

DATA / SIGNAL

Actual value, threshold, detection, trigger, recovery, notification result.

KEY CONTROLS

Status filter, page size, event details.

OPERATING STEPS

1. Prioritize severity.
2. Read evidence.
3. Confirm response.
4. Verify recovery.

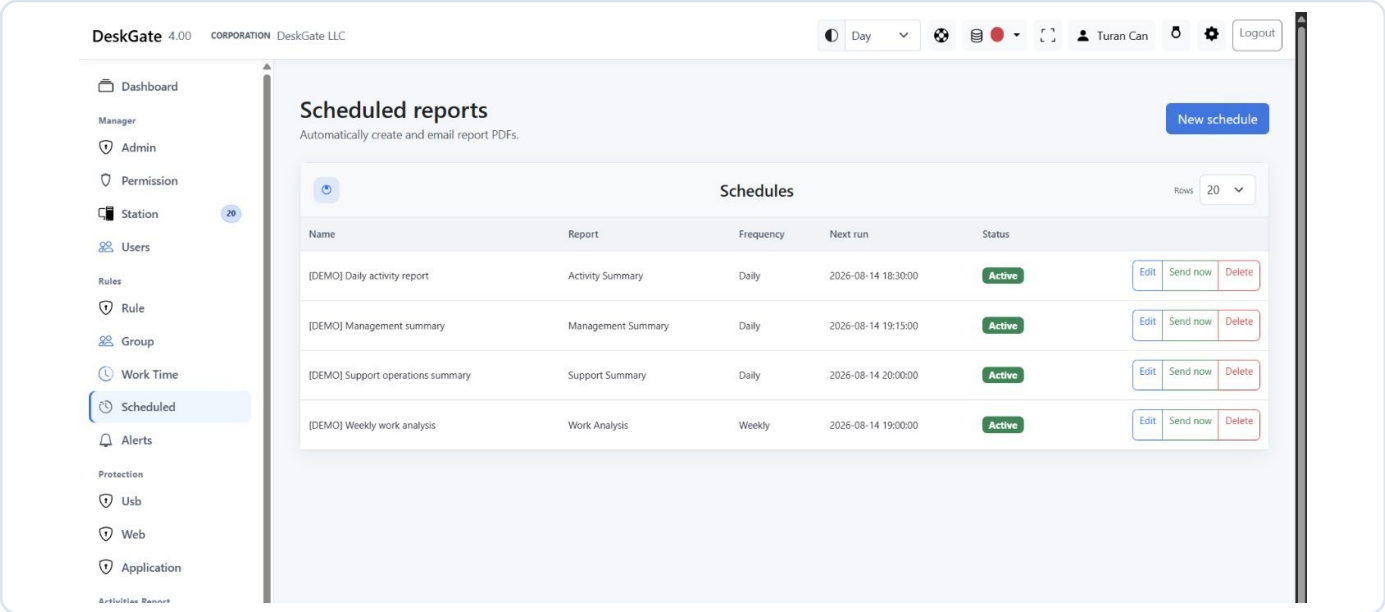
TECHNICAL NOTE

Do not delete useful history merely to clear an operational view.

17 / SCHEDULED REPORTS

Scheduled reports

Automate recurring report generation and delivery.



PURPOSE

Deliver repeatable PDFs.

DATA / SIGNAL

Report type, scope, cadence, next run, last result, error state.

KEY CONTROLS

New schedule, edit, send now, delete, active status.

OPERATING STEPS

1. Select report.
2. Define scope.
3. Test Send now.
4. Enable and monitor.

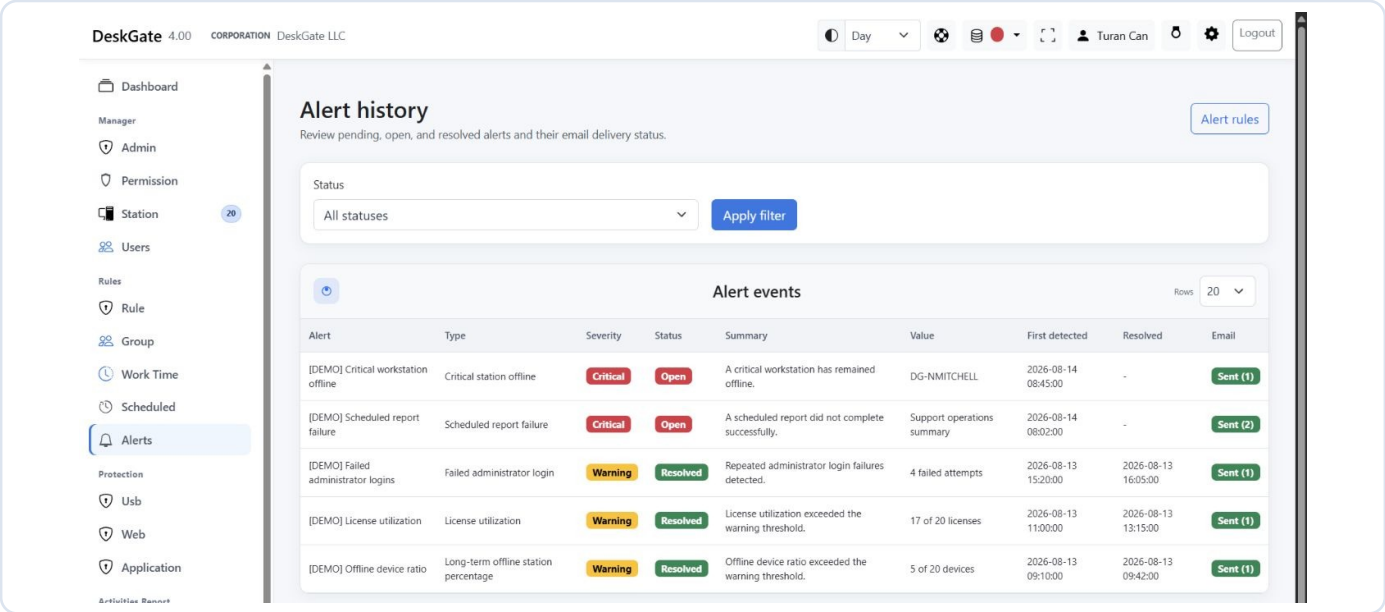
TECHNICAL NOTE

Validate one manual send and its audience before recurring delivery.

18 / SENSITIVE DATA

Sensitive file scan

Find configured sensitive patterns and review matched evidence.



PURPOSE

Support data-loss investigations.

DATA / SIGNAL

Scan definitions, matched files, findings, endpoint and user scope.

KEY CONTROLS

Definition list, station/user filter, status, findings.

OPERATING STEPS

1. Confirm authorization.
2. Narrow scope.
3. Review findings.
4. Document response.

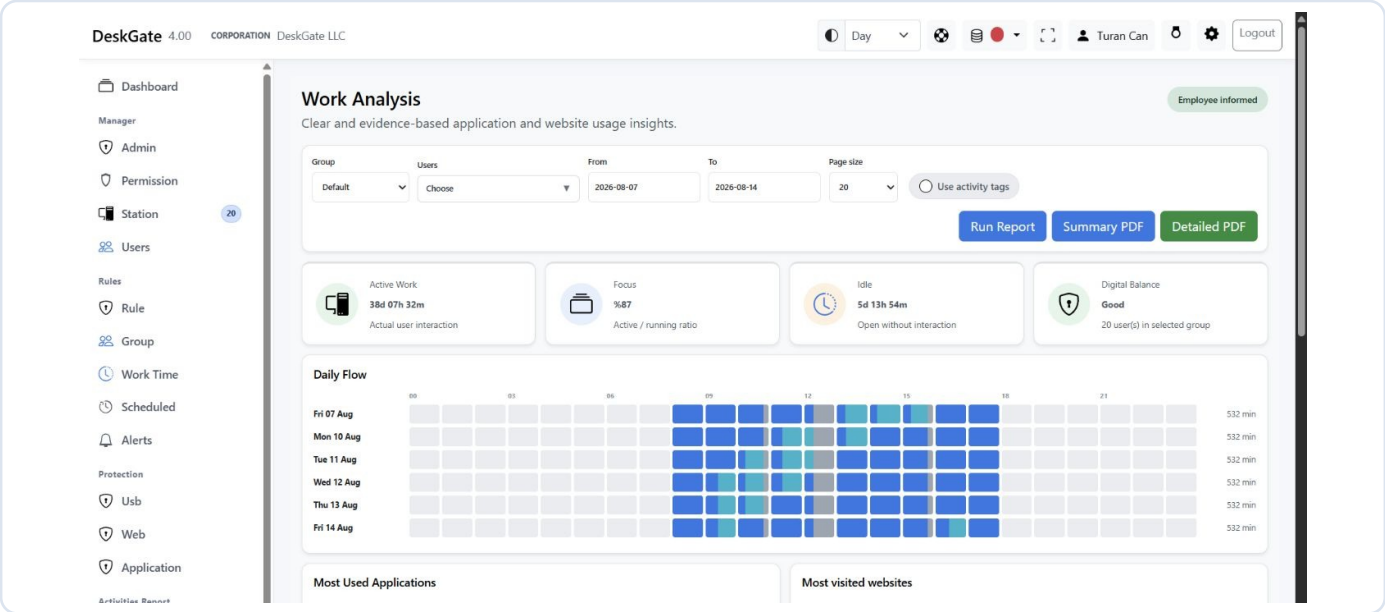
TECHNICAL NOTE

Apply purpose limitation, least privilege, and retention controls.

19 / KEYSTROKE AUDIT

Keystrokes

Investigate application-level keyboard evidence in restricted workflows.



PURPOSE

Support authorized audit investigations.

DATA / SIGNAL

Application, title, captured text, user, device, client date.

KEY CONTROLS

Date, group, users, application, page size, export.

OPERATING STEPS

1. Confirm legal purpose.
2. Narrow scope.
3. Review minimum evidence.
4. Record access.

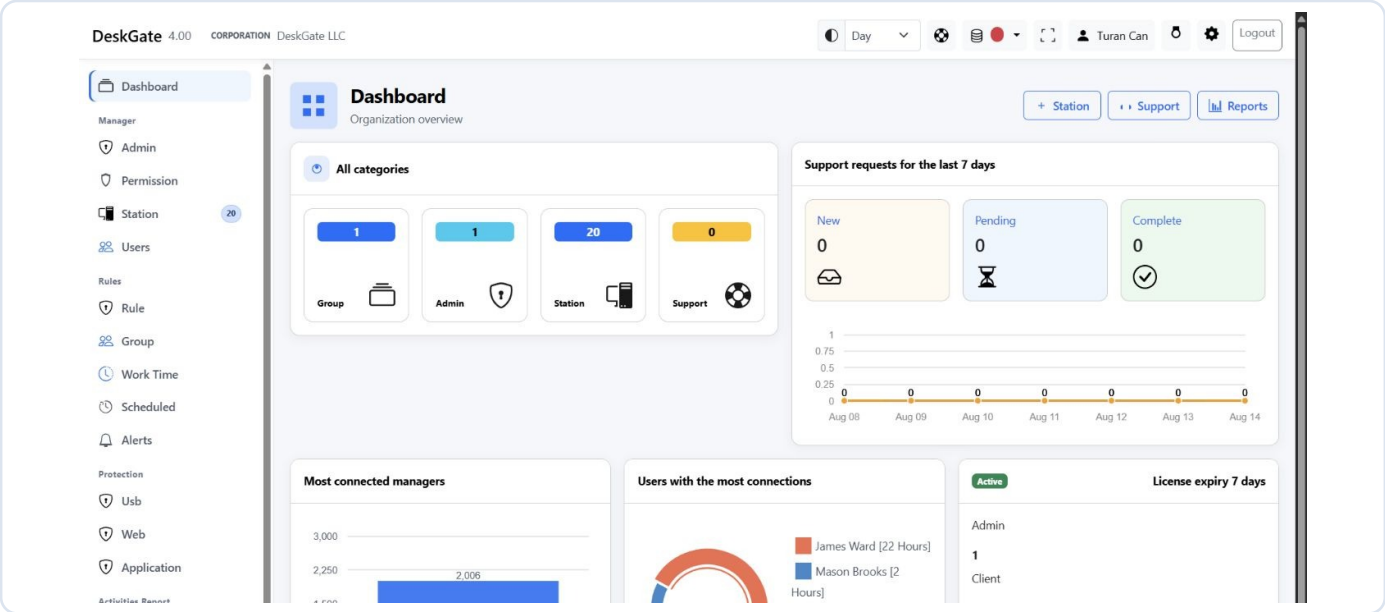
TECHNICAL NOTE

Keystroke data is highly sensitive. Access must be exceptional and auditable.

20 / SCREEN RECORDING

Screen records

Review and export authorized screen recordings.



PURPOSE

Support incident reconstruction.

DATA / SIGNAL

Recording metadata, station/user relationship, storage and playback.

KEY CONTROLS

Date, users, records, player, export.

OPERATING STEPS

1. Confirm authority.
2. Select exact record.
3. Review securely.
4. Export only when required.

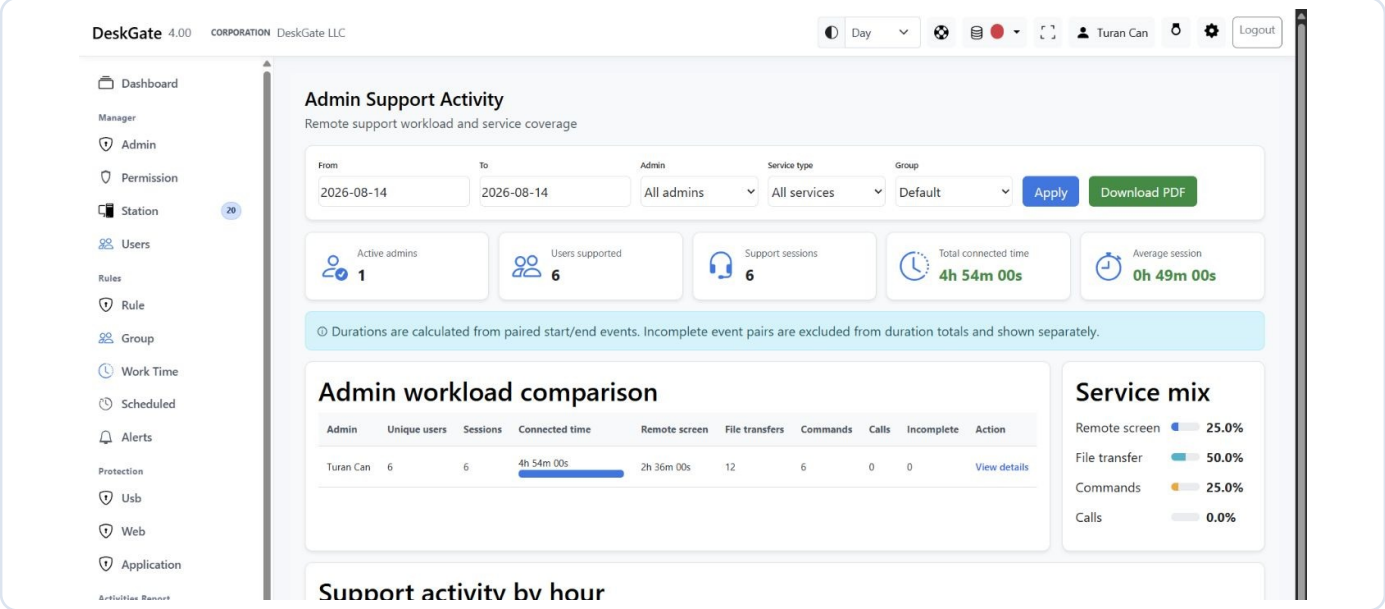
TECHNICAL NOTE

Protect recording storage and avoid unnecessary duplication.

21 / SUPPORT DESK

Support requests

Manage categories, requests, assignments, states, and outcomes.



PURPOSE

Operate the service desk workflow.

DATA / SIGNAL

Support group, request, user, station, administrator, status, timestamps.

KEY CONTROLS

New request, category, assignment, status, list, report.

OPERATING STEPS

1. Categorize.
2. Validate user/device.
3. Assign owner.
4. Close with outcome.

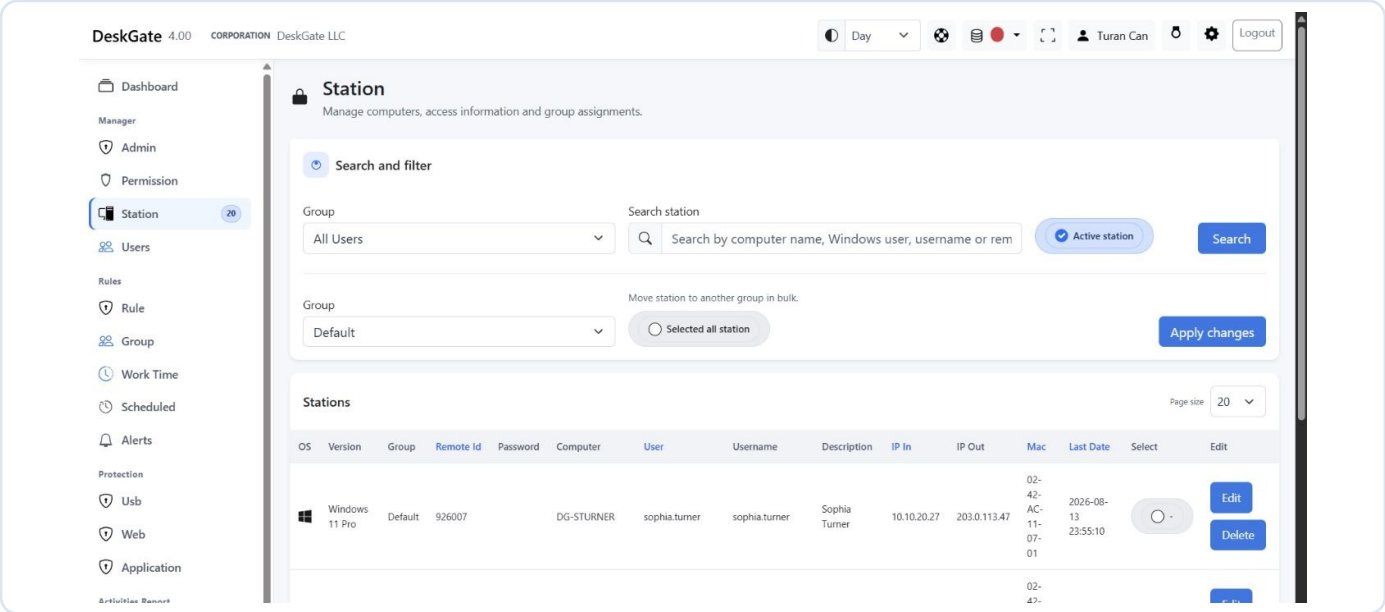
TECHNICAL NOTE

Repeat ownership validation immediately before every assignment or update.

22 / INVENTORY & DEPLOYMENT

Inventory, software & scripts

Track assets and execute controlled endpoint operations.



PURPOSE

Maintain assets and deployment actions.

DATA / SIGNAL

Inventory, devices, computers, install tasks, scripts, target stations.

KEY CONTROLS

Asset lists, device assignment, install package, script, target selection.

OPERATING STEPS

1. Verify targets.
2. Review payload.
3. Execute controlled action.
4. Audit result.

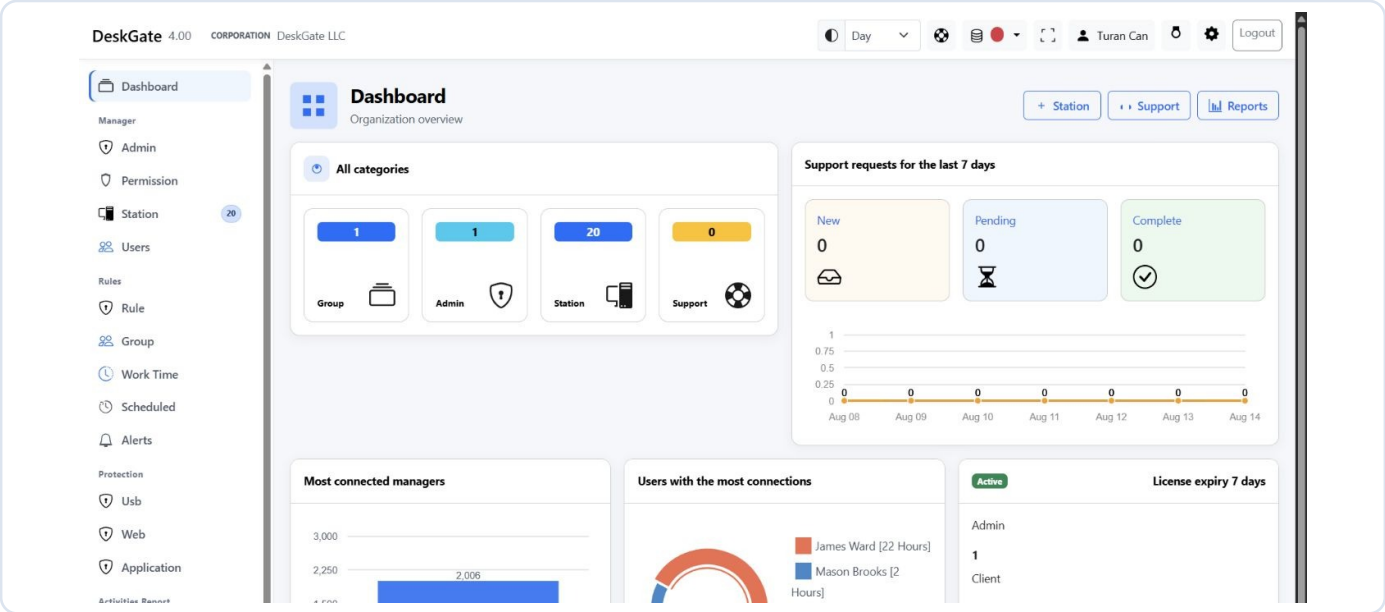
TECHNICAL NOTE

Bulk targets and command arguments remain untrusted until server-side validation.

23 / SYSTEM OPERATIONS

Logs, settings & corporation

Configure platform behavior and diagnose operational history.



PURPOSE

Administer the tenant and troubleshoot safely.

DATA / SIGNAL

Corporation, license, settings, setup, login logs, connection logs.

KEY CONTROLS

Theme, SMTP, license, setup links, log filters, system status.

OPERATING STEPS

1. Inspect logs.
2. Validate configuration.
3. Apply one scoped change.
4. Re-test behavior.

TECHNICAL NOTE

Do not expose passwords, encryption values, or user-specific cached database data.

24 / OPERATIONS CHECKLIST

Keep the platform decision-ready

A repeatable cadence for administrators, managers, and support owners.

DAILY	Dashboard health, open alerts, support exceptions, schedule failures.
WEEKLY	Work patterns, application mix, web mix, USB events, connection history.
MONTHLY	Administrator access, group assignments, policies, inventory, retention.
BEFORE EXPORT	Verify dates, tenant scope, selected users, detail limits, and audience.
BEFORE CHANGE	Validate ownership, dependencies, rollback path, and audit requirement.
ALWAYS	Use least privilege and explain monitoring context to employees.
NEXT ACTION	Choose one exception, verify the evidence, assign an owner, and close the loop.