Central Command User Guide

Malachor MSP Compliance Platform

Version: 1.0.0 **Last Updated:** December 30, 2025

Table of Contents

Getting Started

Accessing Central Command

Central Command is accessed via web browser at your organization's designated URL (e.g., `http://your-server:3000`).

Login

1. Navigate to the Central Command URL
2. Enter your credentials:
    - **Username:** Your assigned username
    - **Password:** Your assigned password
3. Click "Sign In"

Default Administrator Account:

- Username: `admin`
- Password: `admin`

> ***Important:*** *Change the default password immediately after first login.*

Dashboard Layout

The interface consists of:

- **Sidebar** (left): Navigation menu and client list
- **Header** (top): Page title, search, refresh, and user info
- **Main Content** (center): Current page content

Dashboard Overview

The Dashboard provides a real-time overview of your MSP fleet health and compliance status.

Key Metrics

Metric	Description
Total Clients	Number of active client sites
Avg Compliance	Average HIPAA compliance score across all clients
Incidents (24h)	Number of compliance incidents in the last 24 hours
L1 Resolution	Percentage of incidents resolved automatically (L1)

Health Scoring

Health scores are calculated using:

- **Connectivity (40%):** Check-in freshness, healing success, order execution
- **Compliance (60%):** Patching, antivirus, backup, logging, firewall, encryption

Status Thresholds:

- **Healthy (Green):** 80-100%
- **Warning (Orange):** 40-79%
- **Critical (Red):** 0-39%

Fleet Overview

Displays all client sites as cards showing:

- Client name and appliance count
- Overall health gauge
- Recent incident count

Click any client card to view detailed information.

Recent Incidents

Shows the latest compliance incidents with:

- Timestamp
- Client/Host information
- Check type (Patch, AV, Backup, etc.)
- Resolution level (L1, L2, L3)
- Status (Active/Resolved)

Fleet Management

Client List

The sidebar displays all clients with health status indicators:

- **Green dot:** Healthy
- **Orange dot:** Warning
- **Red dot:** Critical

Click a client name to navigate to their detail page.

Client Detail Page

Shows comprehensive information for a single client:

- Appliance inventory with individual health scores
- Compliance breakdown by check type
- Recent incidents for this client
- Historical trends

Runbook Library

Runbooks are automated remediation playbooks that resolve compliance issues.

Viewing Runbooks

Navigate to **Runbooks** in the sidebar to see all available runbooks.

Runbook Information

Each runbook card displays:

- **ID:** Unique identifier (e.g., RB-WIN-PATCH-001)
- **Name:** Descriptive name
- **Level:** L1 (Deterministic) or L2 (LLM-assisted)
- **HIPAA Controls:** Mapped compliance requirements
- **Execution Stats:** Count, success rate, average time
- **Disruptive Flag:** Whether execution may cause service interruption

Filtering Runbooks

Use the filter controls to:

- Search by name, ID, or HIPAA control
- Filter by resolution level (All, L1, L2, L3)

Runbook Details

Click any runbook card to see:

- Full description
- Execution steps with timeouts
- Configuration parameters
- Recent execution history

Audit Logs

Audit logs track all user actions for accountability and compliance.

Accessing Audit Logs

Navigate to **Audit Logs** in the sidebar (Admin only).

Log Information

Each log entry includes:

- **Timestamp:** When the action occurred

- **User:** Who performed the action
- **Action:** Type of action (LOGIN, VIEW, REFRESH, etc.)
- **Target:** What was affected
- **Details:** Additional context

Action Types

Action	Description
LOGIN	User signed into the system
LOGOUT	User signed out
VIEW	User viewed a page or resource
REFRESH	User manually refreshed data
CREATE	New resource created
UPDATE	Resource modified
DELETE	Resource removed
EXECUTE	Runbook or command executed

Filtering Logs

Use the filter controls to:

- Search by target or details
- Filter by action type
- Filter by user

Exporting Logs

Administrators can export logs to CSV:

1. Click "Export CSV" button
2. File downloads with timestamp in filename
3. Use for compliance audits or analysis

User Administration

User Roles

Role	Permissions
Admin	Full access including audit logs, user management
Operator	Standard access to dashboard, clients, runbooks

Signing Out

1. Click the logout icon (arrow) in the bottom-left sidebar
2. You will be returned to the login screen

Session Management

- Sessions persist across browser refreshes
- Sessions are stored locally in the browser
- Closing all browser windows does not automatically log you out

---

Keyboard Shortcuts

Shortcut	Action
`/`	Focus search box
`Esc`	Close modals/dialogs

Troubleshooting

Cannot Log In

1. Verify username and password are correct
2. Check caps lock is not enabled
3. Clear browser cache and try again
4. Contact administrator if issue persists

Data Not Loading

1. Check network connectivity
2. Click the refresh button in the header
3. Wait 30 seconds for auto-refresh
4. Contact administrator if issue persists

Slow Performance

1. Clear browser cache
2. Close unused browser tabs
3. Check network connection speed

Support

For technical support, contact your system administrator or refer to the internal IT helpdesk.

Document generated for Malachor MSP Compliance Platform Central Command Dashboard v1.0.0