Synapse-Conectiv
SERVICE LEVEL GOVERNANCE

# Administrator Guide

The administrator supplement to the Synapse-Conectiv User Guide — client account configuration, CSAT scheduling, user access, Customer Portal provisioning, Cyber Services administration, and system-wide settings.

| SCOPE | SECTIONS | EDITION |
| --- | --- | --- |
| **Admin & SDM** | **8** | **v1.3** |

# Contents

# About This Guide

This is the administrator supplement to the Synapse-Conectiv **User Guide** — it does not repeat the walkthrough of Dashboard, SLA, Reviews, CSAT, CSI, Services, Cyber Services and Executive Reports; that lives in the User Guide, and applies to Administrators exactly as it does to SDMs and Client Stakeholders. What follows here is the set of tasks that are Administrator- (or in a few cases, Administrator- and SDM-) only: provisioning client accounts, managing users and access, configuring CSAT collection schedules, granting Customer Portal access, and system-wide settings.

> New to the app? Read the User Guide's *Getting Started* and *Navigating the App* sections first — they cover signing in, MFA, and the general layout that Administrators use just like everyone else.

# Roles at a Glance

*Administrators have full access to everything in Synapse-Conectiv — every area in the User Guide, plus everything in this one. The other three roles are scoped down from that full picture in different ways.*

**ADMINISTRATOR**
Full control: client accounts, user access, system-wide settings, and every governance area.

**SDM**
Runs day-to-day governance for every client account — data entry, reviews, CSAT scheduling, service SLAs.

**CLIENT STAKEHOLDER**
Read-only view of their own client account across every governance area.

**PORTAL**
Read-only view of exactly one service, on a stripped-down page with no other navigation.

# Permission Matrix

*What each role can see and do, area by area.*

| Area | Admin | SDM | Client Stakeholder | Portal |
|---|---|---|---|---|
| Governance Dashboard | Full | Full | Read-only | — |
| SLA & Service Quality | Full | Full | Read-only | — |
| Service Reviews & Actions | Full | Full | Read-only | — |
| CSAT & NPS Tracker | Full | Full | Read-only | — |
| CSI Register | Full | Full | Read-only | — |
| Services & Custom SLAs | Full | Full | Read-only | Own service only |
| Cyber Security Services (if enabled) | Full | Full | Read-only | — |
| Executive Reports (PDF) | Full | Full | Read-only | — |
| Client Accounts — create / delete | Full | — | — | — |
| Client Accounts — edit (SLA targets, Cyber, CSAT schedule) | Full | Full | — | — |
| Customer Portal toggle (per service) | Full | Full | — | — |
| Users & Access | Full | — | — | — |

| Area | Admin | SDM | Client Stakeholder | Portal |
|---|---|---|---|---|
| Admin Settings (currency) | Full | — | — | — |

> **Why can SDMs edit Client Accounts?** Service Delivery Managers own the operational relationship — SLA targets, Cyber Services, and CSAT scheduling are day-to-day governance decisions, not account-provisioning ones. Only Administrators can create a new client account or remove one, since that affects billing and access at a company level.

# Administrator Responsibilities

In practice, an Administrator's job in Synapse-Conectiv breaks down into five areas. Each is covered in its own section of this guide.

| Responsibility | Where | Who else can help |
| --- | --- | --- |
| Provision and retire client accounts | Client Accounts | No one — Admin only |
| Configure SLA targets, Cyber toggle, CSAT schedule | Client Accounts | SDM can also edit |
| Create, edit, deactivate and delete users | Users & Access | No one — Admin only |
| Provision Customer Portal logins | Services & SLAs + Users & Access | SDM sets the portal toggle; only Admin creates the login |
| Set the system-wide currency | Admin Settings | No one — Admin only |

# Client Accounts — Full Configuration Reference

APPLIES TO **ADMINISTRATOR** · **SDM**

Every client account's contract details, SLA targets, Cyber Services configuration and CSAT collection schedule live in one edit form, reached from **Client Accounts** in the sidebar. Here's what every field does:

| Field | Who sets it | Notes |
|---|---|---|
| Name | Admin only | Must be unique across the system; shown everywhere the client is referenced. |
| Industry | Admin / SDM | Free text — used for context only, no behaviour depends on it. |
| Contract Reference | Admin / SDM | Your internal contract or agreement number. |
| Account Tier | Admin / SDM | Platinum / Gold / Silver — descriptive only, doesn't change functionality. |
| SDM Owner | Admin / SDM | Free text name of the assigned Service Delivery Manager. |
| Contract Start / End | Admin / SDM | Informational dates shown on the account and in reports. |
| SLA Targets | Admin / SDM | Availability %, MTTR (hrs), FCR % — drive the status colour on the SLA view and Dashboard. |
| Cyber Services toggle | Admin / SDM | Switches the whole Cyber Security Services module on or off for this client. |
| Cyber MTTD / MTTR targets | Admin / SDM | Only relevant once Cyber Services is enabled. |
| CSAT Due Schedule | Admin / SDM | Drives the CSAT Due status shown internally and on the Customer Portal — see next section. |

## Creating and retiring client accounts

APPLIES TO **ADMINISTRATOR**

1. Select **New Client** from Client Accounts and fill in the required fields — name, industry, contract reference, SDM owner, and the contract dates. SLA targets default to sensible values (99.9% availability, 4-hour MTTR, 80% FCR) and can be adjusted immediately or later.
2. Save. The new account appears in the client selector for every Admin and SDM straight away, with no historical data — SLA, review, CSAT, CSI and service records all start from zero.
3. To retire an account, open it and select **Delete**. This is irreversible and removes every record tied to that client — SLA history, reviews, CSAT responses, the CSI register, Cyber Services data, and every service and its SLAs.

> Deleting a client account cascades to everything underneath it, including any Customer Portal or Client Stakeholder logins tenanted to it. There's no confirmation beyond the initial prompt — make sure it's the right account before confirming.

# CSAT Due Scheduling — Deep Dive

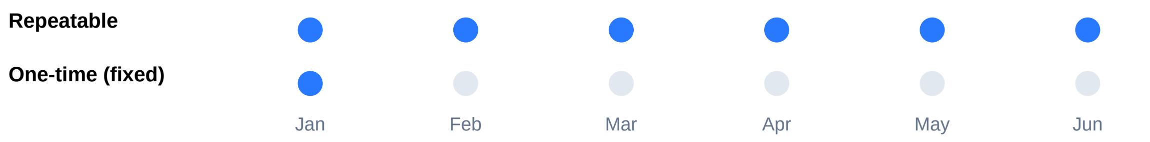
APPLIES TO **ADMINISTRATOR** · **SDM**

Rather than picking a specific date by hand every month, an Administrator or SDM chooses a recurring rule, and the app works out the actual date each time it's needed:

| Rule | Resolves to |
|---|---|
| First working day of month | The first Monday–Friday of the month. |
| 2nd week of month | The first working day on or after the 8th. |
| 3rd week of month | The first working day on or after the 15th. |
| 4th week of month | The first working day on or after the 22nd. |
| Last working day of month | The last Monday–Friday of the month. |

## Repeatable vs. one-time

The **Repeat automatically each month** checkbox controls whether the rule keeps applying indefinitely, or only produces a single due date:




Tick the box and the rule re-applies every month on its own — the due date shown is always worked out fresh against today's month, so there's nothing to reset. Leave it unticked and the date is calculated **once**, at the moment you save, and stays pinned there — even as months pass — until you come back and change the rule, or the repeatable flag, again.

> Saving unrelated changes to a client account — updating the contract end date, say — does **not** reshuffle a pinned one-time due date. Only actually changing the rule or the repeatable flag triggers a recalculation.

## Reading the CSAT Due status

The same three-state logic appears in three places: the Client Accounts table, the internal CSAT & NPS view, and the Customer Portal pill.

| CSAT DUE 22 Jul | CSAT DUE 15 Jul | CSAT DUE 01 Jul |
|---|---|---|
| **Not due yet.** Today is before the scheduled date. | **Due.** The scheduled date has arrived, within 7 days. | **Overdue.** More than 7 days past due — pulses red in the live app. |

> Clearing the schedule back to “Not configured” removes the CSAT Due indicator everywhere — the internal badge and the Customer Portal pill both disappear until it's set again.

# Users & Access — Full Role Reference

APPLIES TO **ADMINISTRATOR**

Only Administrators create, edit or delete user accounts, from **Users & Access**. Four roles are available when creating a user:

| Role | Required fields | Scope |
|---|---|---|
| Administrator | Username, name, email, password | Everything |
| Service Delivery Manager | Username, name, email, password | Every client account, governance data only |
| Client Stakeholder | ...plus a Client Organisation | One client account, read-only |
| Customer Portal User | ...plus a portal-enabled Service | One service, read-only |

### Account status and MFA

Editing an existing user exposes two extra controls not present when creating one: a **Status** switch (Active / Disabled) that blocks sign-in without deleting the account or its history, and a **Reset MFA enrolment** option that clears a lost or compromised authenticator's registration so the user is prompted to set it up again on next login.

### Creating each type of user

1. Select **New User** from Users & Access.
2. Choose a role. For Client Stakeholder, a Client Organisation picker appears — every existing client account is selectable. For Customer Portal User, a Service picker appears instead, listing only services that currently have their portal toggle switched on (see the next section if the service you want isn't listed).
3. Set a username and password, then save. The new account can sign in immediately.

> You cannot delete your own Administrator account, and there's always at least one Administrator in the system as a result — if you need to hand off, create the replacement Admin first.

# Customer Portal Provisioning

APPLIES TO **ADMINISTRATOR** · **SDM**

Customer Portal access requires two separate actions by design — a service-level switch that makes the portal *available*, and a user account that's actually granted access to it. Neither one alone is enough.

## The two-key model

| 1. Enable the toggle | → | 2. Create the login | → | 3. Customer signs in |
|---|---|---|---|---|
| Services & SLAs — SDM or Admin | | Users & Access — Admin only | | Sees only that one service |

Step 1 alone changes nothing for any customer — it just makes the service eligible to appear in the service picker when an Administrator creates a Portal User in step 2. Nobody gets access until both steps are complete.

## Full walkthrough

1. Open **Services & SLAs** for the client, open the service, and switch on **Enable Customer Portal**.
2. Go to **Users & Access** → **New User** and set the role to **Customer Portal User**.
3. In the service picker, select the service from step 1 — only portal-enabled services are listed, so it's impossible to tenant a login to a service that isn't ready.
4. Set a username and password. That login will only ever see this one service — never the wider client account, never any other service on it.
5. Verify by signing in as the new user (or asking the customer to) — they should land directly on the service's read-only page with no sidebar.

> **The toggle is a live switch, not a one-time grant.** If the portal is later switched off for that service, every login tenanted to it is locked out immediately — even a session that's already signed in — until it's switched back on. Nothing is deleted; access simply pauses.

# Cyber Services Administration

APPLIES TO **ADMINISTRATOR** · **SDM**

Cyber Security Services is a client-level toggle, set from the same Client Accounts edit form as everything else. Switching it on immediately unlocks the Cyber Services nav item and dashboard sections for that client, for every role that can see the client at all (Admin, SDM, and — read-only — Client Stakeholder).

### What you're configuring

- The on/off toggle itself.
- An **MTTD target** in minutes — how quickly incidents should be detected.
- An **MTTR target** in minutes — how quickly they should be responded to once detected.

Both targets drive the status colour shown on the Cyber Services dashboard and in the executive report, the same way SLA targets drive the SLA view's status colours.

> Switching Cyber Services off does not delete anything. Every recorded month, every logged incident, stays in the database — the module is simply hidden again until it's switched back on, at which point the full history reappears exactly as it was.

# Admin Settings & Currency

APPLIES TO **ADMINISTRATOR**

A single system-wide setting, deliberately kept simple: the currency symbol used wherever the app displays money — CSI estimated and realized value, on screen and in the executive report PDF.

| | | |
|---|---|---|
| ● £ GBP | ● € EUR | ● $ USD |

Choose one from **Admin Settings** and save — the change applies immediately, everywhere, for every user and every client account. There is no per-client override; it's one currency for the whole system.

# Security & Compliance Notes

APPLIES TO **ADMINISTRATOR**

### MFA policy

MFA is optional per account by design, so onboarding never blocks on it — a new user can always **Skip for Now** and set it up later. For accounts handling sensitive client data, enforcing MFA is a manual process today: check enrolment status in Users & Access (the MFA column shows Enabled / Skipped / Pending) and follow up directly with anyone who hasn't activated it.

### Session and access behaviour

- Sessions are JWT bearer tokens; there's no server-side session list to manage, but role and scope are re-checked on every request — not just at login.
- This is why a Customer Portal toggle-off takes effect immediately: the very next request from an already-signed-in session is re-evaluated against the current state of the service, not a cached permission from login time.
- Deactivating a user (Status: Disabled) blocks new logins but does not revoke an already-issued token until it expires — for immediate revocation of a specific compromised account, also reset its password.

### Before production use

This deployment defaults are meant for evaluation and internal use. Before exposing Synapse-Conectiv beyond that:

- Replace the JWT signing secret with a securely generated value from a proper secrets manager.
- Change every default password created during setup and encourage MFA enrolment for all accounts, especially Administrators.
- Terminate TLS in front of the application (or place it behind a reverse proxy that does).
- Restrict CORS to your actual frontend origin instead of allowing all origins.

# Glossary

**SLA (Service Level Agreement)**
A measurable commitment about service quality — e.g. 99.9% availability — agreed with a client.

**OLA (Operational Level Agreement)**
An internal commitment between teams that underpins an external SLA.

**MTTR (Mean Time to Resolution)**
Average time from an incident being raised to being fully resolved. (See also the distinct Cyber Services usage, “Mean Time to Respond”.)

**MTTD (Mean Time to Detect)**
Average time between a security incident occurring and being identified — Cyber Services only.

**CSAT (Customer Satisfaction)**
A 1–5 satisfaction score collected via survey and averaged over a period.

**NPS (Net Promoter Score)**
Percentage of promoters minus percentage of detractors from a 0–10 recommendation survey.

**CSI (Continual Service Improvement)**
An ITIL v4 practice for tracking ongoing improvement work through Proposed, Active, Completed and Benefits Realized stages.

**RBAC (Role-Based Access Control)**
The system that determines what each of the four Synapse-Conectiv roles can see and do.

**MFA (Multi-Factor Authentication)**
TOTP-based two-factor login security, optional per account, resettable by an Administrator.

**Tenanted (Customer Portal)**
Scoped to exactly one resource. A Customer Portal login is tenanted to a single service — it has no visibility of anything else.

**JWT (JSON Web Token)**
The bearer-token format used for session authentication; re-validated against current role and scope on every request.

# Appendix: Quick-Reference Permission Matrix

*Repeated here for convenience — identical to the matrix earlier in this guide.*

| Area | Admin | SDM | Client Stakeholder | Portal |
|---|---|---|---|---|
| Governance Dashboard | **Full** | **Full** | Read-only | — |
| SLA & Service Quality | **Full** | **Full** | Read-only | — |
| Service Reviews & Actions | **Full** | **Full** | Read-only | — |
| CSAT & NPS Tracker | **Full** | **Full** | Read-only | — |
| CSI Register | **Full** | **Full** | Read-only | — |
| Services & Custom SLAs | **Full** | **Full** | Read-only | Own service only |
| Cyber Security Services (if enabled) | **Full** | **Full** | Read-only | — |
| Executive Reports (PDF) | **Full** | **Full** | Read-only | — |
| Client Accounts — create / delete | **Full** | — | — | — |
| Client Accounts — edit (SLA targets, Cyber, CSAT schedule) | **Full** | **Full** | — | — |
| Customer Portal toggle (per service) | **Full** | **Full** | — | — |
| Users & Access | **Full** | — | — | — |
| Admin Settings (currency) | **Full** | — | — | — |