Synapse-Conectiv

SERVICE LEVEL GOVERNANCE

User Guide

How to use Synapse-Conectiv day to day — the Governance Dashboard, SLA tracking, service reviews, CSAT, CSI, custom service SLAs, Cyber Security Services, executive reporting, and the Customer Portal.

ROLES COVERED	FEATURE AREAS	EDITION
4	10	v1.3

Contents

Welcome to Synapse-Conectiv

Synapse-Conectiv is a **Service Level Management & Governance** platform for Service Delivery Managers, built around ITIL v4's Service Level Management and Service Relationship Management practices. It sits above the service desk rather than replacing it — Synapse-Conectiv is deliberately **not** a ticketing system. Instead, it is the single place where an SDM, a client's stakeholders, and (optionally) the client's own end customers can see whether a service is meeting its commitments, review it together on a regular cadence, and track the improvement work that keeps it on track.

Everything in the app is organised around a **Client Account** — the contractual relationship with a customer. A client account carries SLA targets, a run of monthly SLA actuals, a calendar of service reviews, CSAT/NPS survey data, a Continual Service Improvement (CSI) register, and — optionally — Cyber Security Services and any number of individually named **Services**, each with its own bespoke SLAs.

What this guide covers

- Every feature area, with a description of what you'll see and step-by-step instructions for the things you'll actually do.
- Which of the four roles can do what — both as a single reference table and as inline “Applies to” badges on every section.
- The Customer Portal, for anyone who has been given a tenanted, read-only login.
- A glossary of the ITIL and product terms used throughout (SLA, OLA, MTTR, MTTD, CSAT, NPS, CSI and more).

> Looking for how to configure a client account, manage users, or provision Customer Portal access? That's covered in the companion **Administrator Guide** — this guide focuses on day-to-day use.

Roles at a Glance

Every account has exactly one role, assigned by an Administrator. Coloured badges like these appear throughout this guide, and throughout the app itself, to show who a feature is for.

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	—

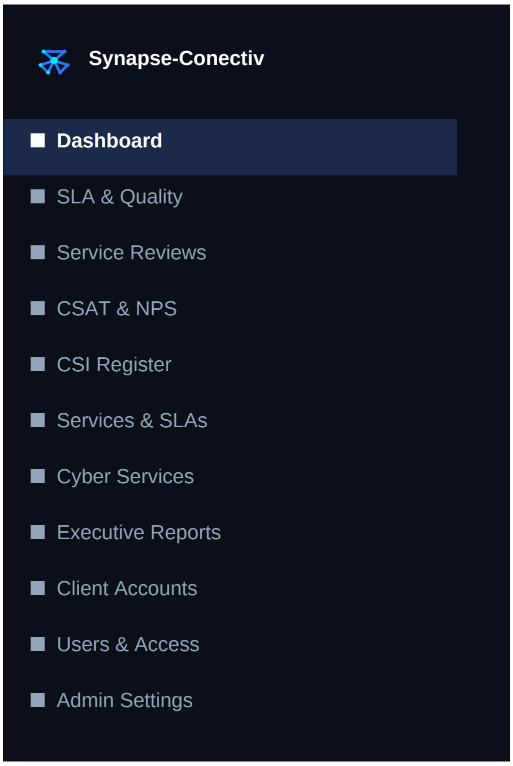
Area	Admin	SDM	Client Stakeholder	Portal
Services & Custom SLAs	Full	Full	Read-only	Own service only
Cyber Security Services (if enabled)	Full	Full	Read-only	—
Executive Reports (PDF)	Full	Full	Read-only	—
Client Accounts — create / delete	Full	—	—	—
Client Accounts — edit (SLA targets, Cyber, CSAT schedule)	Full	Full	—	—
Customer Portal toggle (per service)	Full	Full	—	—
Users & Access	Full	—	—	—
Admin Settings (currency)	Full	—	—	—

“Full” means create, edit and delete. “Read-only” means the identical data, with every edit control hidden. A Customer Portal account's row is almost entirely dashes — by design, it only ever sees one thing: its own service.

Navigating the App

APPLIES TO **ADMINISTRATOR** · **SDM** · **CLIENT STAKEHOLDER**

Admin, SDM and Client Stakeholder accounts share the same layout: a dark sidebar on the left for navigation, and a light content area on the right. The sidebar lists only the areas your role can access — an SDM never sees “Users & Access”, for instance, because the nav item itself is hidden, not just the buttons inside it.



At the top of every page is the client selector. Admins and SDMs use it to switch between every client account in the system; a Client Stakeholder doesn't get a choice — the selector shows their own organisation's name and nothing else. Whichever client is selected stays selected as you move between areas, so switching to “SLA & Quality” after picking a client shows that same client's SLA history.

> Two nav items only appear when they're relevant: **Cyber Services** is hidden entirely for any client that doesn't have it enabled, and **Client Accounts** / **Users & Access** / **Admin Settings** are Administrator- (or Administrator+SDM-) only. There's no empty tab or placeholder for features you can't use — if you can't see it, it isn't relevant to your role.

Getting Started & Signing In

APPLIES TO **ADMINISTRATOR** · **SDM** · **CLIENT STAKEHOLDER** · **PORTAL**

Every account, regardless of role, signs in from the same screen. What happens immediately afterwards depends on your role — the full governance app for Admin, SDM and Client Stakeholder accounts, or the stripped-down Customer Portal for Portal accounts.

1. Go to the Synapse-Conectiv sign-in page and enter your username and password.
2. If your account has never set up two-factor authentication, you'll be offered a QR code to scan with an authenticator app — Google Authenticator, Authy, 1Password, or similar. You can activate it immediately by entering the 6-digit code it generates, or choose **Skip for Now** and set it up on a later login.
3. If MFA is already active on your account, you'll instead be asked for the current 6-digit code from your authenticator app.
4. You're in. Admin, SDM and Client Stakeholder accounts land on the Governance Dashboard; Customer Portal accounts land directly on their service's page.

Two-factor authentication

MFA in Synapse-Conectiv is TOTP-based — the same standard used by most authenticator apps, so any of them will work. It's optional per account, but recommended for every role, including Customer Portal logins.

> Lost your authenticator device? You can't self-recover MFA — it has to be reset by an Administrator from **Users & Access**, which clears the enrolment and lets you set it up again (or skip it) on your next login.

Governance Dashboard

APPLIES TO **ADMINISTRATOR** · **SDM** · **CLIENT STAKEHOLDER**

The Dashboard is the single-page overview for whichever client account is selected — the first thing you see after signing in, and the fastest way to answer “how is this account doing right now?”

What you'll see

AVAILABILITY

Target ≥ 99.9%

MTTR

2.6 hrs

Target ≤ 3 hrs

CSAT SCORE

4.4 / 5

14 responses recorded

NET PROMOTER SCORE

35.7

7 promoters · 2 detractors

- A KPI row for Availability, MTTR, CSAT and NPS, each with a status colour against target.
- A 12-month SLA trend chart (Availability and First Contact Resolution together).
- A distribution chart of the CSI register by stage.
- A list of upcoming service reviews, and the open action items nearest their due date.
- If the client has Cyber Security Services enabled, a second KPI row for Security Events, Incidents, MTTD and MTTR.

Switching between client accounts

Admins and SDMs use the client selector at the top of the page — every view you open afterwards reflects the newly selected client, including the Dashboard itself. Client Stakeholder and Customer Portal accounts don't have this control; they always see their own account.

SLA & Service Quality

APPLIES TO **ADMINISTRATOR** · **SDM** · **CLIENT STAKEHOLDER**

This is the client-wide SLA record — the four headline metrics that most contracts are written against, tracked month over month against the targets set on the client account.

The four metrics

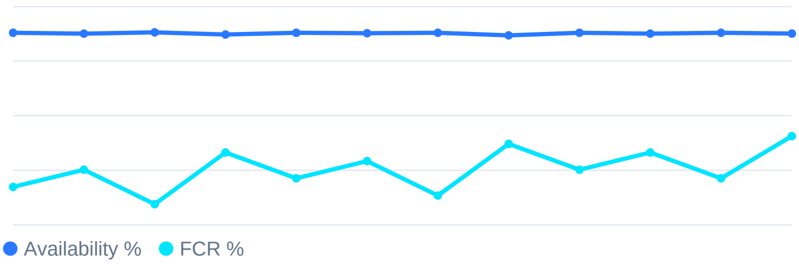
Metric	Meaning	Good direction
Availability	Percentage of time the service was up and usable during the period.	Higher
MTTR	Mean Time to Resolution — average time to fix an incident once raised.	Lower
First Contact Resolution (FCR)	Percentage of tickets resolved on first contact, no escalation.	Higher
OLA Compliance	Percentage of internal Operational Level Agreements met that period.	Higher

Reading the status colour

MET	AT RISK	BREACHED

Met means the latest month cleared its target outright. At Risk means it's close — within a small margin of the target — worth watching but not yet a problem. Breached means the target was missed by more than that margin, and is worth raising at the next service review.

Trend and incident volume



A 12-month line chart sits above a bar chart of incident volume, so a spike in breaches is easy to line up against a spike in raised incidents for the same month.

Recording a new month's SLA figures

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

1. Open **SLA & Quality** for the client and select **Record Month**.
2. Enter the period, Availability %, MTTR (hours), FCR % and OLA Compliance %, plus the total and breached incident counts for that month.
3. Save. The new month appears at the top of the register immediately and rolls into the trend chart and the Dashboard's KPI row.

> Each client account can only have one entry per calendar period — trying to record the same month twice is rejected, so historical figures can't be silently overwritten.

Service Review Manager

APPLIES TO **ADMINISTRATOR** · **SDM** · **CLIENT STAKEHOLDER**

Organises the recurring cadence of governance meetings ITIL v4 calls for — Weekly, Monthly and Quarterly service reviews — each with its own attendee list, summary, and Action Item Register.

Review status and action item priority

● SCHEDULED	● COMPLETED	● CANCELLED

● LOW	● MEDIUM	● HIGH	● CRITICAL

Action items move through a simple status workflow — **Open**, **In Progress**, **Completed**, or **Overdue** once the due date has passed without being closed. Admins and SDMs update the status from a dropdown directly in the action item table; there's no separate edit screen for a routine status change.

Scheduling a review and logging actions

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

1. Open **Service Reviews** for the client and select **New Review**.
2. Choose the type (Weekly / Monthly / Quarterly), set the date, and list attendees. Reviews can be created as **Scheduled** ahead of time and marked **Completed** afterwards with a summary.
3. Within a review, select **Add Action** to log a follow-up — description, owner, due date and priority.
4. As work progresses, update each action item's status directly from the register until it's marked Completed.

Client Stakeholders see the exact same review list and action item register, read-only — useful for confirming what was agreed at the last review without needing to ask.

CSAT & NPS Tracker

APPLIES TO **ADMINISTRATOR** · **SDM** · **CLIENT STAKEHOLDER**

Aggregates individual satisfaction survey responses into two headline scores and a qualitative feedback log.

How the scores are calculated

- **CSAT** is a straight average of every response's 1–5 satisfaction score for the selected period.
- **NPS** (Net Promoter Score) buckets each response by its 0–10 recommendation score: **promoters** (9–10), **passives** (7–8), and **detractors** (0–6). NPS is the percentage of promoters minus the percentage of detractors, giving a score from -100 to +100.

The CSAT Due status

If a Service Delivery Manager has configured a recurring survey collection schedule for this client (see the Administrator Guide), a status banner at the top of this view shows the next due date and its urgency — the identical logic that drives the pill shown on the Customer Portal, covered later in this guide.

NOT DUE	DUE	OVERDUE

Logging a survey response

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

1. Open **CSAT & NPS** for the client and select **Log Response**.
2. Enter the period, respondent name and role, the CSAT score (1–5), the NPS score (0–10), and an optional comment.
3. Save — the response feeds into the current average, the NPS calculation, and the qualitative feedback log immediately.

CSI Register

APPLIES TO **ADMINISTRATOR** · **SDM** · **CLIENT STAKEHOLDER**

Continual Service Improvement is one of ITIL v4's core practices: a running register of the improvement work a service is doing, tracked as a kanban board through four stages.

Proposed (2)	Active (4)	Completed (1)	Benefits Realized (1)
TECHNOLOGY **Automate Sev-1 notifications**	PEOPLE **Cross-train L1 support**	COST **Consolidate monitoring tools**	TECHNOLOGY **Proactive capacity alerting**

Categories

PROCESS	TECHNOLOGY	PEOPLE	COST

Every initiative carries an **estimated value** when it's proposed, and — once it reaches **Benefits Realized** — a **realized value** reflecting what was actually delivered. Both are shown in whichever currency an Administrator has set for the whole system.

Working the register

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

1. Select **New Initiative**, choose a category, and describe the improvement, its owner, and the expected benefit.
2. Drag a card to the next column as work progresses — Proposed → Active → Completed → Benefits Realized — or open it and change its status directly.
3. When an initiative reaches Benefits Realized, record its realized value so the register reflects the actual return.

Services & Custom SLAs

APPLIES TO **ADMINISTRATOR** · **SDM** · **CLIENT STAKEHOLDER** · **PORTAL**

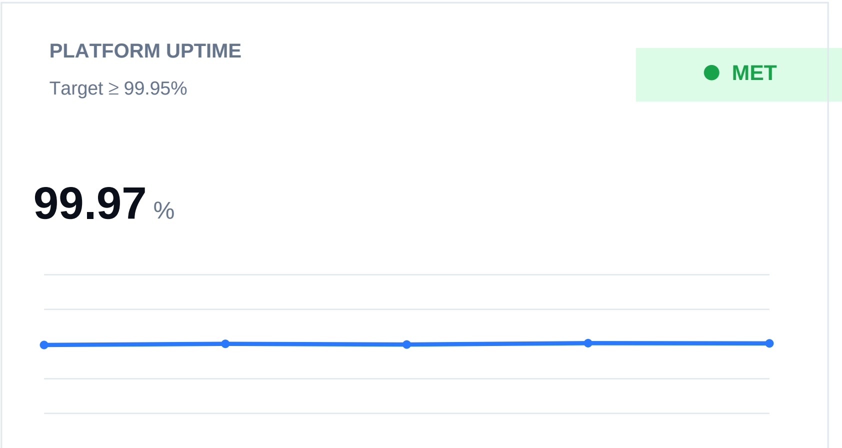
The client-wide SLA metrics cover the relationship as a whole, but most accounts are really several distinct services under one contract — a platform, a support desk, a monitoring function. **Services & Custom SLAs** lets you model that: any number of named services per client, each with its own bespoke SLAs.

Defining a custom SLA

A custom SLA has no fixed shape — you choose the name, the unit, the target value, and whether hitting the target means going **at least** that high or **at most** that low:

Comparison	Meaning	Example
At least (≥)	Higher is better.	Platform Uptime ≥ 99.95%
At most (≤)	Lower is better.	Checkout API Response Time ≤ 400ms

What an SLA card looks like



Creating a service and tracking its SLAs

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

1. Open **Services & SLAs** for the client and select **New Service**. Give it a name and description.
2. Open the service and select **New SLA** to define each metric you want to track — name, unit, target, and comparison direction.
3. Each month, select **Record Actual** on an SLA to log that period's value. The status (Met / At Risk / Breached) and trend chart update immediately.

> This is also where a service's **Customer Portal** access is switched on or off — see *Customer Portal Guide* later in this guide, and the Administrator Guide for how a portal login actually gets provisioned.

Cyber Security Services

APPLIES TO **ADMINISTRATOR** · **SDM** · **CLIENT STAKEHOLDER**

An optional module an Administrator or SDM can switch on for any client account. Once enabled, a dedicated dashboard tracks security event volume, confirmed incidents, and how quickly they're detected and responded to.

Events, Incidents, and two kinds of MTTR

Term	Meaning
Security Event	Any alert or signal surfaced by monitoring tooling — most need no follow-up.
Confirmed Incident	An event that turned out to be a genuine security issue requiring response.
MTTD	Mean Time to Detect — average time between an incident occurring and being identified.
MTTR (Cyber)	Mean Time to Respond — average time from detection to an initial response. Distinct from the service-desk MTTR on the main SLA view, which measures resolution, not first response.

Security Incident Register

● LOW	● MEDIUM	● HIGH	● CRITICAL
● OPEN	● CONTAINED	● RESOLVED	● CLOSED

Every incident is logged with a category (Phishing, Malware, Unauthorized Access, Data Exposure, Denial of Service, Insider Threat, Vulnerability Exploit), a severity, a status, and detection / response / resolution timestamps.

Recording cyber activity

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

1. Select **Record Month** to log that period's event count, confirmed incidents, critical incident count, MTTD and MTTR.
2. Select **Log Incident** to add an individual security incident to the register, with its category, severity, owner and timestamps.

Executive Reports

APPLIES TO **ADMINISTRATOR** · **SDM** · **CLIENT STAKEHOLDER**

Packages the current state of a client account into a single, print-ready summary — the document you'd actually hand to a stakeholder at a quarterly review.

What's included

- SLA snapshot for the latest period, against target.
- Service-level SLA summary — every custom SLA across every service, with its current status.
- Cyber Security snapshot and recent incidents, if the client has it enabled.
- Customer sentiment (CSAT / NPS) and the CSI register summary with realized value.
- The five most recent service reviews and every currently open action item.

Generating a report

1. Open **Executive Reports** for the client — the on-screen view renders immediately.
2. Select **Print** to use your browser's print dialogue directly against the on-screen layout, or **Download PDF** for a branded PDF generated server-side.

> The PDF is generated fresh every time from the live data — there's no caching or manual refresh step, so it always reflects exactly what's on screen at the moment you download it.

Customer Portal Guide

APPLIES TO **PORTAL**

If you've been given a Customer Portal login, you see exactly one page: your service's name and description, and a card for every SLA that applies to it — current value, target, status, and a trend chart. There's no sidebar, no client selector, and no navigation to anything else — nothing else is tenanted to your login.

The CSAT Due pill

If your Service Delivery Manager has scheduled a satisfaction survey cycle for your account, you'll see a pill in the top-left of the page, next to the Synapse-Conectiv logo. It always reads **CSAT Due** with the scheduled date — the colour alone tells you the urgency:

● 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.

If you don't see a pill at all, no survey cycle is currently scheduled for your account.

> If your page shows “Portal access is not currently available,” your Service Delivery Manager has temporarily switched off portal access for your service. Your login still exists — access returns automatically as soon as it's switched back on, with no need to sign in again.

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”, on the incident-response side.)

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

FCR (First Contact Resolution)
Percentage of support contacts resolved without escalation or a repeat contact.

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; ranges from -100 to +100.

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

KPI (Key Performance Indicator)
Any of the headline metrics — Availability, MTTR, CSAT, NPS and similar — used to judge service health at a glance.

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.

Kanban
A visual workflow board — used here for the CSI register — where work moves left to right through fixed stages as it progresses.

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, even other services on the same client account.