ORYELE DOCUMENTATION

Digital Workforce

Create, configure, and manage AI-powered workers that operate 24/7 inside your business processes.

This guide covers everything from creating your first digital worker to using pre-built templates, understanding worker lifecycle management, and accessing the complete audit history of every action a worker takes.

Creating a Digital Worker

A digital worker is an AI agent with a defined role, a set of permitted actions, and a structured escalation path. Unlike simple bots, Oryele workers understand context, handle exceptions, and know when to hand off to a human.

Step 1: Define the Worker Role

- Navigate to Digital Workforce > Workers and click New Worker.
- Enter a name that reflects the worker's function (e.g., Client Intake Coordinator).
- Select a department to organize the worker within your team structure.
- Write a plain-language role description the AI uses to understand its purpose.

Step 2: Set Responsibilities

- Choose the workflows this worker is permitted to execute.
- Select the communication channels the worker can use (email, SMS, voice).
- Specify which knowledge bases the worker can read.
- Define any tools or integrations the worker has access to (e.g., calendar, document storage).

Step 3: Configure Escalation Paths

- Define the conditions that trigger escalation to a human (e.g., client complaint, ambiguous request).
- Assign a primary escalation contact and a backup.
- Set a timeout threshold: how long the worker waits before automatically escalating.
- Choose whether escalation suspends the workflow or allows the worker to continue with limited actions.

Step 4: Test and Activate

- Use the built-in Sandbox mode to run test scenarios without affecting live data.
- Review the test activity log to confirm the worker behaves as expected.
- Toggle the worker to Active status when ready.
- Monitor the worker's first 10 live interactions from the Dashboard.

Key Concept	Each digital worker has an isolated permission scope. A worker assigned to client intake cannot read financial workflows unless explicitly granted access. Scope isolation is enforced at the platform level and cannot be overridden at runtime.

Worker Templates

Templates give you a pre-configured starting point for the most common professional services use cases. Each template includes a role definition, a set of default workflows, recommended escalation paths, and suggested communication scripts.

Template Name	Primary Function	Best For
Client Intake Coordinator	Collects new client information, sends welcome materials, and schedules kickoff calls	Accounting, consulting, legal firms
Scheduling Assistant	Manages meeting requests, calendar conflicts, and rescheduling communications	Any client-facing team
Document Follow-Up Agent	Tracks outstanding documents, sends reminders, and escalates overdue items	Tax, audit, and compliance teams
Onboarding Specialist	Guides new clients through a multi-step onboarding checklist	Wealth management, advisory
Renewal Reminder Agent	Monitors contract and engagement renewal dates and initiates outreach	Subscription and retainer businesses
Support Triage Worker	Categorizes inbound support requests and routes them to the right team	Operations and client services

Using a Template

- Go to Digital Workforce > Workers > New Worker > Start from Template.
- Browse or search the template library and click Preview to review defaults.
- Click Use Template to create a draft worker based on the template.
- Customize the name, escalation paths, and workflow assignments.
- Run Sandbox tests before activating.

Tip	Templates are living resources. Oryele adds new templates as professional services use cases evolve. Check the template library after each platform update for new options.

Audit Logs and Activity History

Every action a digital worker takes is logged automatically. Audit logs are immutable, timestamped, and available for export. They are designed to satisfy the requirements of professional services regulators and internal compliance programs.

What Gets Logged

- Every workflow step the worker executes, including conditions evaluated and branches taken.
- All communications sent or received on the worker's behalf (email, SMS, voice).
- Document accesses, reads, and writes performed during task execution.
- Escalations triggered, including the reason, timestamp, and target.
- Any configuration changes made to the worker by an administrator.
- Login and authentication events tied to the worker's service account.

Accessing Audit Logs

- Go to Governance > Audit Logs and filter by Worker, Date Range, or Event Type.
- Use the search bar to locate specific client names, workflow IDs, or message threads.
- Click any log entry to expand it and see the full event detail including payload snapshots.
- Use the Timeline view to trace a single client interaction end-to-end across multiple workers.

Exporting Records

- Click Export in the top-right corner of the Audit Logs view.
- Choose CSV for data analysis or PDF for formal documentation.
- Apply your current filters before exporting to scope the output.
- Large exports are processed asynchronously and delivered to your notification email.

Compliance Note	Audit logs cannot be modified or deleted by platform users, including Owners. If a record needs to be preserved for legal purposes, apply Legal Hold before the standard retention period expires. See the Security and Compliance guide for details.