JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

COURSE BROCHURE

Contact Centre Platform Technical Administration Training Course

jupiterprime.uk

info@jupiterprime.uk

Registered in the United Kingdom and Saudi Arabia

Contact Centre Platform Technical Administration Training Course

Contact Centre Platform Technical Administration is a 1-week training course for contact centre engineers, platform administrators and telephony support staff who configure and secure cloud contact centre tenants, producing a platform configuration and access baseline. As customer conversations move to cloud tenants that blend voice, chat and messaging, a single misrouted queue or over-privileged account can disrupt service and expose customer records. Jupiter Prime Training delivers this course on contact centre platform technical administration.

Why Contact Centre Platform Technical Administration Matters Now

Three shifts are changing the administrator's role: on-premises switches giving way to multi-tenant cloud platforms, customer journeys spanning voice, web chat and messaging apps, and security teams treating the contact centre as a target for social engineering and account takeover. A well-administered tenant keeps wait times predictable, isolates agent privileges and leaves a clean audit trail; a poorly administered one leaks call recordings and fails during peak demand. The course anchors access and logging practice in ISO/IEC 27001:2022, the international standard for information security management systems, and in the NIST Cybersecurity Framework 2.0 NIST CSF 2.0.

Who Gains Most from Contact Centre Platform Technical Administration

- Engineers who build routing strategies, queues and skills-based distribution rules
- Administrators who provision agent accounts, roles and permission sets
- Telephony specialists who maintain trunks, numbers and IVR call flows
- Integration staff who connect CRM, workforce and ticketing systems through APIs
- Support analysts who monitor platform health and resolve agent-reported faults

A tenant operations group combining telephony, identity and integration specialists gains most through one shared change routine.

Contact Centre Platform Technical Administration Capabilities

Participants leave able to configure a tenant end to end.

- Design routing strategies that balance skills, priority and service level targets — customer experience owners
- Build IVR call flows with self-service branches and safe fallbacks — operations leads
- Specify role-based permission sets following least privilege — information security officers
- Configure secure integrations using OAuth clients and scoped API credentials — CRM and IT owners
- Apply audit logging and alerting to administrative changes — internal auditors
- Test fault isolation across network, softphone and carrier layers — service desk escalation

Key Contact Centre Platform Technical Administration Terms

- Tenant — an isolated customer instance on a shared cloud contact centre platform, holding its own users, numbers and configuration.
- Skills-based routing — distributing each interaction to the available agent whose recorded skills and proficiency best match its needs.
- IVR call flow — the scripted sequence of prompts, menus and data lookups a caller passes through before reaching an agent.
- Permission set — a named bundle of rights assigned to a role, controlling which configuration objects a user may view or change.
- Wrap-up code — a label an agent applies after an interaction, recording its outcome for reporting and quality checks.
- Audit trail — the time-stamped record of who changed which configuration object, from where and with what result.

Contact Centre Platform Technical Administration Day by Day

Day 1: Tenant Architecture and Security Context

- Cloud Tenant Architecture — Shared Responsibility Between Platform Provider and Customer
- Organisation Structure and Divisions — Segregating Business Units Inside One Tenant
- Numbers, Trunks and Carrier Connections — Inbound Capacity and Resilience Choices
- Threats to Contact Centres — Social Engineering, Toll Fraud and Account Takeover
- ISO/IEC 27001:2022 Access Principles — Framing Administrative Privilege Decisions

Day 2: Routing, Queues and Call Flows

- Queue Configuration — Service Level Targets, Overflow and Callback Options
- Skills-Based Routing Rules — Matching Interactions to Agent Proficiency
- IVR Call Flow Design — Menus, Data Dips and Safe Fallback Paths
- Schedules and Emergency Groups — Out-of-Hours and Disaster Routing Behaviour
- Digital Channel Routing — Web Chat, Email and Messaging in One Queue Model

Day 3: Identity, Roles and Permissions

- Single Sign-On and Identity Provider Federation — Removing Local Passwords
- Role and Permission Set Design — Least Privilege for Agents and Supervisors
- Administrative Access Reviews — Detecting Dormant and Excessive Accounts
- Call Recording and Data Retention Settings — Protecting Customer Conversations
- Payment Interaction Handling — Pausing Recording During Card Capture

Day 4: Integrations, Monitoring and Troubleshooting

- OAuth Clients and Scoped API Credentials — Securing CRM and Ticketing Connectors
- Audit Log Queries — Tracing Who Changed Routing or Permissions
- Real-Time Dashboards and Alerts — Spotting Queue Breaches and Outages Early
- Voice Quality Diagnostics — Jitter, Packet Loss and Softphone Faults
- Change Release Routine — Testing Configuration Before Production Promotion

Day 5: Practising the Platform Configuration and Access Baseline

- Retail Bank Scenario — Rebuilding Routing for a Card Fraud Hotline
- Utility Provider Scenario — Outage Surge Handling With Callback Queues
- Permission Audit Exercise — Remediating Over-Privileged Supervisor Roles
- Incident Simulation — Diagnosing a Failed Integration During Peak Demand
- Platform Configuration and Access Baseline — Documented Settings, Roles and Log Checks

Applying Contact Centre Platform Technical Administration After the Course

- Export current roles and permission sets, compare them with the least-privilege model from the course and remove excess rights.
- Set up saved audit log queries and alerts for routing, IVR and permission changes, and share a weekly change digest with security.

Contact Centre Platform Technical Administration Questions FAQ

What is contact centre platform technical administration and why does it matter now?

It is the configuration and secure upkeep of a cloud contact centre tenant. It matters now because voice and digital channels share one platform, so errors affect service and customer data at once.

Which roles gain most from contact centre platform technical administration?

Contact centre engineers, platform administrators and telephony support staff gain most.

How does contact centre platform technical administration differ from a contact centre operations course?

This subject covers the technical settings behind the service. An operations course focuses on staffing, coaching and performance metrics, whereas here you configure routing, identities, integrations and logging inside the tenant.

What do you bring back from contact centre platform technical administration?

You bring back a platform configuration and access baseline for your tenant. It records routing and IVR settings, approved roles and the log checks that confirm changes stay controlled.

Contact Centre Platform Technical Administration: The Way Forward

The platform configuration and access baseline first informs which permission sets are trimmed in the next access review. Administrators use it to approve changes, security officers use it to verify controls, and support analysts use it when tracing faults. After its first use, revisit routing assumptions against real queue statistics.