JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

COURSE BROCHURE

# Advanced Maximo Administration and Access Security Course

14 – 25 February 2027
Amman

**jupiterprime.uk**

info@jupiterprime.uk

Registered in the United Kingdom and Saudi Arabia

# Advanced Maximo Administration and Access Security Course

**Ref:** 244_7683 **Date:** 14 – 25 February 2027 **Location:** Amman **Fees:** 6000 GBP

Maximo Administration and Access Security is a 2-week advanced training course for Maximo administrators, asset managers and maintenance system leads who configure IBM Maximo and decide who can see, approve and change asset records, and it ends with a secured Maximo workflow and access model. Maintenance systems now hold the keys to plant shutdowns, spare-part spending and contractor access, so loose permissions create both fraud and safety exposure. Jupiter Prime Training runs this course for the people who administer that system.

## Why Maximo Administration and Access Security Matters Now

Three pressures meet in Maximo today: the move to the Maximo Application Suite and cloud hosting, which changes how users, roles and integrations are managed; contractors and mobile technicians who need limited, time-bound access to work orders in the field; and auditors who now treat the asset management system as part of the security estate, asking for segregation of duties on purchasing and approvals. Well-administered systems give planners clean data and auditors clear trails; poorly controlled ones invite duplicate purchases, unauthorised work and gaps during incidents. Access design in the course follows the access control themes of ISO/IEC 27001:2022.

## Who Gains Most from Maximo Administration and Access Security

- Maximo administrators who build security groups, start centres and application access
- Asset managers who own asset hierarchies, criticality data and lifecycle decisions
- Maintenance system leads who configure work order, preventive maintenance and job plan processes
- Inventory and stores supervisors who control item masters, reorder rules and issues
- Integration specialists who connect Maximo to finance, HR and operational systems

An asset management office that sends its Maximo administrator with planning and stores leads together gains most, because access rules only hold when every module owner agrees them.

## Maximo Administration and Access Security Capabilities

Participants leave able to configure Maximo processes that run efficiently while keeping each user to exactly the access their role needs.

- Design security groups and application authorisations around job roles — system owners and auditors
- Specify segregation of duties for requisition, purchase and approval steps — finance and procurement
- Build workflow processes with escalations and approval limits — maintenance planners and supervisors
- Apply preventive maintenance, job plan and inventory configuration that keeps data reliable — asset managers
- Test integration and API access for least privilege and logging — IT security and integration owners
- Communicate asset performance and access exceptions through Maximo reports — operations leadership

## Key Maximo Administration and Access Security Terms

- Security group — A Maximo collection of application, site and data permissions assigned to users who share a role.
- Start centre — The configurable home screen that shows a Maximo user their work queues, key indicators and shortcuts.
- Workflow process — A designed sequence of nodes, approvals and actions that routes records such as work orders through defined steps.
- Escalation — A scheduled rule that checks records against conditions and triggers actions or notifications when deadlines or limits are breached.
- Segregation of duties — Splitting conflicting tasks, such as raising and approving a purchase, between different users to reduce fraud and error.
- Asset hierarchy — The parent-child structure of locations and assets that organises maintenance history, costs and criticality.

## Maximo Administration and Access Security Day by Day

## Day 1: Maximo in the Enterprise Security Picture

- Maximo Application Suite Architecture — Hosting and Administration Choices
- Asset Management System Threats — Fraud, Sabotage and Data Loss
- ISO/IEC 27001:2022 Access Control Themes — Expectations for Business Applications
- Current Access Baseline Extraction — Who Holds Which Rights Today
- Organisation, Site and Set Structure — Data Boundaries Across Plants

## Day 2: Users, Security Groups and Authentication

- User Lifecycle Administration — Joiner, Mover and Leaver Handling
- Security Group Design Patterns — Independent Versus Combined Groups
- Application and Signature Option Authorisation — Function-Level Control
- Single Sign-On and Directory Synchronisation — Central Identity Source
- Password, Session and Login Tracking Settings — Account Abuse Detection

## Day 3: Data Restrictions and Segregation of Duties

- Data Restrictions and Conditional Expressions — Record-Level Visibility
- Site and Storeroom Authorisation — Location-Based Access Limits
- Approval Limits and Tolerances — Financial Authority by Role
- Conflict Matrix for Purchasing Roles — Separating Request and Approval
- Contractor and Vendor User Profiles — Time-Bound External Access

## Day 4: Work Management Configuration

- Work Order Status Model — Controlled Transitions and Accountability
- Job Plans and Safety Plans — Standard Work and Hazard Controls
- Labour, Crafts and Assignment Manager — Scheduling Workload Fairly
- Work Order Classifications and Failure Codes — Reliable Root Cause Data
- Mobile Technician Access — Field Work Without Excess Rights

## Day 5: Preventive Maintenance and Asset Data

- Preventive Maintenance Records and Frequencies — Time and Meter Triggers
- PM Hierarchies and Sequencing — Nested Maintenance Routines
- Asset and Location Hierarchy Design — Cost Roll-Up and Criticality
- Meters and Condition Monitoring — Triggering Work From Readings
- Asset Data Quality Rules — Validation Before Records Go Live

## Day 6: Inventory, Purchasing and Stores Control

- Item Master and Storeroom Configuration — Single Source for Parts
- Reorder Points and Economic Order Quantities — Stock Level Decisions
- Purchase Requisition to Receipt Flow — Three-Way Match Controls
- Rotating Items and Serialised Parts — Traceability of Critical Spares
- Inventory Adjustments and Cycle Counts — Detecting Shrinkage and Fraud

## Day 7: Workflow Design and Escalations

- Workflow Designer Nodes and Actions — Modelling Approval Routes
- Role-Based Assignments in Workflow — Dynamic Approver Selection
- Escalations and Notifications — Deadline and Limit Enforcement
- Automation Scripts Governance — Change Control for Custom Logic
- Workflow Testing and Version Control — Safe Promotion to Production

## Day 8: Integration and Interface Security

- Maximo Integration Framework Channels — Inbound and Outbound Flows
- REST and OSLC API Access — Service Account Least Privilege
- API Keys and Integration Credentials — Rotation and Storage Rules
- Interface Error Queues — Data Integrity Between Systems
- Utilities and Transport Integration Cases — Sector Lessons

## Day 9: Reporting, Audit Trails and Monitoring

- Electronic Audit and Attribute Tracking — Evidence of Who Changed What
- Key Performance Indicators and Start Centre Portlets — Operational Visibility
- Report Security and Scheduling — Controlled Distribution of Data
- Access Recertification Reports — Periodic Rights Reviews
- Logging and Alerting for Administrative Actions — Insider Misuse Detection

## Day 10: Practising the Secured Maximo Workflow and Access Model

- Role and Security Group Mapping for a Case Plant — Clean Access Design
- Purchasing and Work Order Workflow Build — Approvals and Escalations Applied
- Segregation of Duties Test Scenarios — Conflicts Detected and Resolved
- Integration and Audit Trail Verification — Evidence Ready for Auditors
- Secured Maximo Workflow and Access Model Completion — Groups, Rules and Approval Routes

## Applying Maximo Administration and Access Security After the Course

- Extract current security group memberships and run a segregation of duties check on purchasing and approval rights
- Enable electronic audit on high-risk objects such as purchase orders and item masters and review the first month of change history

## Maximo Administration and Access Security Questions FAQ

### What is Maximo administration and access security and why does it matter now?

Maximo administration and access security is the configuration of Maximo processes together with the users, groups and rules that control them. It matters now because migrations, mobile field work and audits put the asset management system inside the security estate.

### Which roles gain most from Maximo administration and access security training?

Maximo administrators, asset managers, maintenance system leads and stores supervisors gain most. You benefit if you build security groups, design workflows or answer auditors' questions about who approved work and purchases.

### How does Maximo administration and access security training differ from a Maximo end-user course?

It focuses on configuring and securing the system rather than using screens to raise work orders. You design security groups, workflows, escalations and integrations, while end-user courses cover day-to-day navigation and data entry.

## What do you bring back from Maximo administration and access security training?

You bring back a secured workflow and access model you can apply to your own Maximo environment. It includes role-based groups, segregation rules, approval routes and audit settings ready for review by system owners.

## Maximo Administration and Access Security: The Way Forward

The secured Maximo workflow and access model first informs how security groups are rebuilt and which approval limits change. Administrators implement it, asset and stores managers confirm its roles, and auditors test its segregation rules. After the first access recertification, revisit contractor profiles, since temporary rights tend to linger longer than any design intends.