Section 9: Security & Administration in Maximo

Q1. How is security managed in Maximo?

Security in Maximo is role-based.

Users are assigned to Security Groups, and groups define:

- Application access (which apps they can use).
- Options/Controls (which actions they can perform).
- Data Restrictions (which records they can see/edit).
- Conditional UI (field-level security).

Q2. What is the difference between Users, Security Groups, and Roles?

Term	Purpose
User	An individual account (login ID).
Security Group	A set of permissions (application access, data restrictions). Users belong to groups.
Role	Can be linked to workflows/escalations (dynamic assignment of responsibility).

Example:

User = John

Group = "Planners" (can create/edit Work Orders)

Role = "Approver" (assigned in Workflow)

Q3. What are Data Restrictions in Maximo?

Data Restrictions limit what records users can read/update/delete.

Types:

1. Object Restriction - Applies to an object (e.g., Work Orders of a site).
2. Attribute Restriction - Hide or make read-only a specific attribute (field).
3. Condition - SQL-based condition for restriction (e.g., SITEID = 'EAST').

Example: A planner in Site A should not see Work Orders of Site B.

Q4. What is the difference between Application Security and Data Restrictions?

Application Security - Grants or denies access to entire applications (e.g., WO Tracking).

Section 9: Security & Administration in Maximo

Data Restrictions - Restrict records within the application (e.g., can only see own Site's Work Orders).

Q5. What is Start Center security?

Security Groups define which Start Center templates users can see.

You can create role-specific dashboards (Planners, Technicians, Managers).

Q6. How do you make a field read-only in Maximo?

There are two main ways:

1. Through Security - Data Restrictions

Create an Attribute restriction.

Example: Make STATUS field read-only for a group.

2. Through Automation Script (Attribute Launch Point):

```
mbo.setFieldFlag("STATUS", MboConstants.READONLY, True)
```

In interviews, highlight both methods.

Q7. What is the difference between Conditional Security and Data Restrictions?

Conditional Security - Used to control UI elements like buttons, fields, menus.

Example: Hide "Approve" button if WO status != "WAPPR".

Data Restrictions - Restrict data access in the database.

Example: User cannot even query Work Orders from another site.

Q8. How are licenses managed in Maximo?

Maximo supports different license types:

1. Authorized - Each user consumes one license.

2. Concurrent - License consumed when user logs in, freed after logout.

3. Limited - Restricted functionality (can only perform certain actions).

4. Express - Very limited (view only, no transactions).

License usage can be monitored via License Usage Monitor.

Section 9: Security & Administration in Maximo

Q9. What is the difference between MaxAdmin and MaxUser?

MAXADMIN - Superuser group, full control of system (all applications, configurations).

MAXUSER - Default group for end users (basic operations only).

Q10. What are Organization and Site level security?

Organization = Highest level, controls financial & data separation.

Site = Operational unit within an Organization.

Security can be restricted at Organization or Site level.

Example: User may only access Work Orders in Site = "Plant1".

Q11. How do you secure an Integration in Maximo?

Integration security is controlled by:

- External System definitions (enable/disable).
- Security Groups - Integration Controls.
- User Authentication (LDAP or Application Server).

Q12. Have you configured any security in your project? (Scenario Question)

Sample Answer:

"Yes. In my last project, I configured data restrictions to ensure that planners only had access to Work Orders from their own site.

I created an Attribute Restriction on the WORKORDER object, with the condition SITEID = :&SITEID&.

I also configured Conditional Security in Work Order Tracking so that the 'Approve' action was only visible if the user belonged to the Supervisor group.

This prevented unauthorized approvals and ensured compliance with audit policies."