TEST CASE

Authentication Module

Register API Test Cases

TC ID	Scenario	Input	Expected Output
REG_001	Register with all valid fields	Valid name, email, phoneNumber, employeeCode, strong password	201 Created with user object, accessToken, refreshToken
REG_002	Register with only phoneNumber	Valid phoneNumber, name, password	201 User created
REG_003	Register with only employeCode	employeCode, name, password	201 User created
REG_004	Register with only email	email, name, password	201 User created
REG_006	Missing identifiers	No email, phone, employeCode	400 Validation error
REG_007	Missing name	Only identifiers + password	400 Name required
REG_008	Missing password	name + identifiers	400 Password required
REG_009	Weak password	Password < 6 chars	400 Invalid password

Login API Test Cases

TC ID	Scenario	Input	Expected Output
LOG_001	Login using employeCode	identifier=EMP001, correct password	200 Success with tokens
LOG_002	Login using phoneNumber	identifier=9876543210, correct password	200 Success
LOG_005	Wrong password	Valid identifier, wrong password	401 Invalid credentials
LOG_006	Non-existing user	Identifier not found	404 User not found
LOG_007	Missing identifier	Only password sent	400 Validation error

Profile API Test Cases

TC ID	Scenario	Input	Expected Output
PROF_001	Valid token	Bearer validToken	200 User profile returned
PROF_003	Missing token	No Authorization header	401 Unauthorized
PROF_004	Invalid token	Bearer abc123	401 Unauthorized

Refresh Token Test Cases

TC ID	Scenario	Input	Expected Output
REF_001	Valid refresh token	refreshToken	200 New access token issued
REF_004	Missing refresh token	Empty body	400 Validation error
REF_005	Invalid refresh token	Wrong signature	401 Unauthorized

Logout Test Cases

TC ID	Scenario	Input	Expected Output
LOGOUT_001	Valid logout	Bearer validToken	200 Logout successful
LOGOUT_003	Missing token	No auth header	401 Unauthorized
LOGOUT_004	Invalid token	Bearer invalid	401 Unauthorized

Authentication - Advanced Negative & Security

TC ID	Scenario	Input	Expected Result
AUTH_NEG_001	Empty JSON body	{}	400 Bad Request
AUTH_NEG_002	Whitespace-only fields	' '	400 Validation error
AUTH_NEG_003	Email as identifier (not allowed)	identifier='test@mail.com'	401 Invalid credentials
AUTH_NEG_004	Password with special unicode	weird chars	400 or 401
AUTH_NEG_005	Extremely long identifier (>200 chars)	'a'*200	400
AUTH_SEC_001	Expired access token	Expired JWT	401 Token expired
AUTH_SEC_002	Tampered signature	Modify JWT payload	401 Invalid signature
AUTH_SEC_003	Use refresh token as access token	refreshToken in header	401 Unauthorized
AUTH_SEC_004	SQL injection attempt	identifier="' OR 1=1 --"	401 sanitized
AUTH_SEC_005	Brute-force login	multiple wrong attempts	429 Too many requests (if implemented)

Authentication - Edge & DB

TC ID	Scenario	Input	Expected Result
AUTH_EDGE_001	Identifier numeric but too long	20+ digit phone	400 invalid phone
AUTH_EDGE_002	User deleted but token valid	Token for deleted user	404 or 401
AUTH_EDGE_003	Refresh token rotation reuse	Use old token after refresh	401 reuse invalid

AUTH_DB_001	Duplicate email registration	Existing email	409 conflict
AUTH_DB_002	Soft-deleted user tries login	User in DB but inactive	403 Forbidden
AUTH_DB_003	Refresh token not stored in DB	Refresh endpoint	401 Unauthorized

Advanced Authentication API Test Cases

TC ID	Scenario	Input	Expected Result
AUTH_NEG_001	Empty JSON body	{}	400 Bad Request
AUTH_NEG_002	Whitespace-only fields	' '	400 Validation error
AUTH_NEG_003	Email as identifier (not allowed)	identifier='test@mail.com'	401 Invalid credentials
AUTH_NEG_004	Password with special unicode	weird chars	400 or 401
AUTH_NEG_005	Extremely long identifier (>200 chars)	'a'*200	400
AUTH_SEC_001	Expired access token	Expired JWT	401 Token expired
AUTH_SEC_002	Tampered signature	Modify JWT payload	401 Invalid signature
AUTH_SEC_003	Use refresh token as access token	refreshToken in header	401 Unauthorized
AUTH_SEC_004	SQL injection attempt	identifier="' OR 1=1 --"	401 sanitized
AUTH_SEC_005	Brute-force login	multiple wrong attempts	429 Too many requests (if implemented)

Lead Module

Notes: Use clean test DB, create test users, recommended phone numbers: 9000000001-3. For file uploads use small dummy files. Tokens via /auth/login.

Lead CRUD - Create / Read / Update / Delete

TC ID	Scenario	Type	Steps / Input	Expected Result / Notes
LEAD_CRUD_001	Create Lead - valid payload	Positive	POST /leads with {name, phone_number, address, source, service_type, sales_executive(optional)}	201 Created, data with unique id
LEAD_CRUD_002	Create Lead - missing	Negative	POST missing name/phone/address/source/service_type	400 Bad Request listing missing fields

	required fields			
LEAD_CRUD_003	Create Lead - invalid service_type	Negative	service_type='INVALID'	400 Invalid service_type (SME,BROADBAND,LEASEDLINE)
LEAD_CRUD_004	Create Lead - duplicate phone_number	Negative	phone_number already exists	409 Conflict
LEAD_CRUD_005	Update Lead - valid	Positive	PUT /leads with id and updated fields	200 OK, lead updated
LEAD_CRUD_006	Update Lead - non-existing id	Negative	PUT with non-existent id	404 Lead not found
LEAD_CRUD_007	Get All Leads - default pagination	Positive	GET /leads?page=1&limit=10	200 OK, leads array + pagination
LEAD_CRUD_008	Get All Leads - search filters	Positive	GET /leads?search=abc&service_type=SME&status=OPEN	200 OK, filtered leads
LEAD_CRUD_009	Get Lead by unique ID - valid	Positive	GET /leads/unique/:unique_id	200 OK, lead with nested details
LEAD_CRUD_010	Get Lead by unique ID - not found	Negative	GET /leads/unique/invalid-id	404 Lead not found

Lead Status Management

TC ID	Scenario	Type	Steps / Input	Expected Result / Notes
LEAD_STATUS_001	Update Lead Status - valid enum	Positive	PUT /leads/status/:unique_id with {status:'QUALIFIED'}	200 OK, status updated
LEAD_STATUS_002	Update Lead Status - missing status	Negative	PUT with empty body	400 Status required

LEAD_STATUS_003	Update Lead Status - invalid enum	Negative	status='INVALID'	400 Invalid status
LEAD_STATUS_004	Update Lead Status - lead not found	Negative	nonexistent-id	404 Lead not found
LEAD_STATUS_005	Update Lead Status - unauthenticated	Negative	No JWT	401 Authentication required

Customer Details

TC ID	Scenario	Type	Steps / Input	Expected Result / Notes
CUST_001	Create Customer Details - valid	Positive	POST /leads/:unique_id/customer-details with first_name etc. (auth required)	201 Created, lead status updated
CUST_002	Create Customer Details - missing unique_id	Negative	POST without unique_id in URL	400 Unique ID required
CUST_003	Create Customer Details - missing first_name	Negative	POST without first_name	400 First name required
CUST_004	Create Customer Details - lead not found	Negative	unknown unique_id	404 Lead not found
CUST_005	Update Customer Details - update existing record	Positive	POST with id to update	200 Updated successfully
CUST_006	Get Customer Details by Lead ID - valid	Positive	GET /leads/:unique_id/customer-details	200 OK with customer details
CUST_007	Get Customer Details by Lead ID - not found	Negative	GET /leads/invalid/customer-details	404 Not found

GIS Status Change

TC ID	Scenario	Type	Steps / Input	Expected Result / Notes
GIS_001	GIS Status Change - create FEASIBLE record	Positive	POST /leads/gis/status with {lead_id, status:'FEASIBLE', distance, optical_type}	201 Created, lead status updated to QUALIFIED
GIS_002	GIS Status Change - invalid status	Negative	invalid status	400 Invalid status
GIS_003	GIS Status Change - missing lead_id	Negative	no lead_id	400 Lead ID required
GIS_004	GIS Status Change - invalid distance	Negative	distance='abc' or negative	400 Distance must be positive number
GIS_005	GIS Status Change - unauthenticated	Negative	no auth header	401 Authentication required

KYC Submission

TC ID	Scenario	Type	Steps / Input	Expected Result / Notes
KYC_001	Submit KYC - valid files and fields	Positive	POST /leads/:unique_id/kyc with FormData (id_document,address_proof,signature,terms_accepted=true)	201 Created, lead status KYC_UPDATED
KYC_002	Submit KYC - missing files	Negative	missing id_document or address_proof or signature	400 File required
KYC_003	Submit KYC - terms not accepted	Negative	terms_accepted=false	400 Terms must be accepted
KYC_004	Submit KYC - lead not found	Negative	unknown unique_id	404 Lead not found

KYC_005	Submit KYC - update existing KYC	Positive	POST with id present to update	200 Updated successfully

Lead Security, Edge & DB Tests

TC ID	Scenario	Type	Steps / Input	Expected Result / Notes
SEC_001	Access protected endpoint without JWT	Security	Call protected endpoint without Authorization	401 Authentication required
SEC_002	Use expired JWT	Security	Call with expired token	401 Token expired
SEC_003	Role based access - invalid role	Security	Attempt EM user creation with unauthorized role	404 Role not found or 403 Forbidden
SEC_004	SQL Injection - phone_number field	Security	phone_number="' OR 1=1 --"	400 or sanitized
SEC_005	Attempt update another user's lead	Security	User A token updates User B lead	403/401 depending on rules
EDGE_001	Very long text fields	Edge	>=5000 chars	400 or handled gracefully
EDGE_002	Simultaneous duplicate create requests	Edge	Two concurrent POST with same phone	One 201, one 409
EDGE_003	Pagination with high page number	Edge	page=9999	200 OK with empty array
DB_001	DB Unique constraint - phone_number	DB	Duplicate create	409 Conflict
DB_002	Soft delete impact	DB	Delete executive then create lead assigned to them	404 or business rule
DB_003	Referential integrity - moduleIds mapping	DB	moduleIds contain invalid ids	404 Some modules not found

Lead Workflows

TC ID	Scenario	Type	Steps	Expected Result / Notes

WF_001	Create Lead -> Share Customer Link -> Submit KYC -> Verify status	Workflow	1.Create lead 2.Send customer link 3.Submit KYC 4.Get lead	Status transitions to KYC_UPDATED
WF_002	Create Lead -> GIS FEASIBLE -> Verify QUALIFIED	Workflow	1.Create lead 2.POST gisStatusChange FEASIBLE 3.Get lead	Lead status QUALIFIED

Inventory Management Module

Asset Operations (CRUD)

TC ID	Scenario	Type	Steps / Input	Expected Result
AST_001	Add Asset - Valid New Asset	Positive	POST /inventory/assets with unique name, company_id, asset_type_id, batchQty, thresholdLevel	201 Created, stockQty = batchQty
AST_002	Add Asset - Existing Asset (Update Stock)	Positive	POST with existing name; batchQty increments	200 Updated, stockQty increased
AST_003	Add Asset - Missing mandatory fields	Negative	POST missing name/company_id/asset_type_id	400 Validation error
AST_004	Add Asset - Negative batchQty	Negative	batchQty < 0	400 batchQty must be positive
AST_005	Get All Assets - default pagination	Positive	GET /inventory/assets?page=1&limit=10	200 list with metadata
AST_006	Get Asset By ID - valid	Positive	GET /inventory/assets/:id	200 asset returned
AST_007	Get Asset By ID - invalid id	Negative	GET /inventory/assets/unknown_id	404 Asset not found
AST_008	Update Asset - valid	Positive	PUT /inventory/assets/:id with valid updates	200 Updated; stockQty adjusted
AST_009	Update Asset - totalOut > stockQty	Negative	totalOut > stockQty	400 totalOut exceeds available stock

AST_010	Delete Asset - valid	Positive	DELETE /inventory/assets/:id	200 Soft delete isActive=false
AST_011	Delete Asset - not found	Negative	DELETE invalid id	404 Asset not found

Company Operations

TC ID	Scenario	Type	Steps / Input	Expected Result
CMP_001	Get All Companies	Positive	GET /inventory/companies	200 list
CMP_002	Add Company - valid	Positive	POST /inventory/companies with unique name	201 Created
CMP_003	Add Company - duplicate name	Negative	POST with existing name	409 Company exists
CMP_004	Add Company - missing name	Negative	POST without name	400 Validation error

Asset Type Operations

TC ID	Scenario	Type	Steps / Input	Expected Result
ATYPE_001	Get All Asset Types	Positive	GET /inventory/asset-types	200 list
ATYPE_002	Add Asset Type - valid	Positive	POST /inventory/asset-types	201 Created
ATYPE_003	Add Asset Type - duplicate	Negative	POST with existing name	409 Asset type exists

Inventory Dashboard & Alerts

TC ID	Scenario	Type	Steps / Input	Expected Result
DASH_001	Get Dashboard Summary	Positive	GET /inventory/dashboard-summary	200 summary counts
DASH_002	Low Stock Alerts	Positive	GET /inventory/low-stock-alerts	200 assets <= thresholdLevel

Inventory Security & DB

TC ID	Scenario	Type	Steps / Input	Expected Result
SEC_001	Missing JWT	Security	Call endpoint without Authorization	401 Unauthorized
SEC_002	Invalid JWT	Security	Malformed token	401 Invalid token

SEC_003	Expired JWT	Security	Expired token	401 Token expired
DB_001	Foreign Key - company_id must exist	DB	POST asset with non-existing company_id	404 Company not found
DB_002	Foreign Key - asset_type_id must exist	DB	POST asset with invalid asset_type_id	404 Asset type not found
DB_003	Unique Asset Name + Company + Type	DB	Duplicate asset for same company & type	409 Duplicate asset

Inventory Edge Cases & Workflow

TC ID	Scenario	Type	Steps / Input	Expected Result
EDGE_001	Huge batchQty	Edge	batchQty=99999999	200/400 depending backend
EDGE_002	Zero batchQty	Edge	batchQty=0	400 batchQty must be positive
EDGE_003	Search with special characters	Edge	search='@#$%'	200 filtered or empty
WF_001	Create Asset → Update Asset → Dashboard alerts	Workflow	1.POST asset 2.PUT update 3.GET dashboard	StockQty updated; alert reflects

User Management Module

TC ID	Scenario	Type	Steps / Input	Expected Result
USR_GET_001	Fetch all users with valid token	Positive	GET /users?page=1&limit=10 with admin JWT	200 list + pagination
USR_GET_002	Search users by name	Positive	GET /users?search=john	200 filtered list
USR_GET_003	Missing JWT	Negative	GET /users without Authorization	401 Unauthorized
USR_GET_004	Non-admin fetch all users	Security	GET /users with regular user token	403 Forbidden
USR_ID_001	Get user by valid ID	Positive	GET /users/:id with valid token	200 user object
USR_ID_002	Get user by invalid ID	Negative	GET /users/99999	404 User not found

USR_UPD_001	Update user name/email	Positive	PUT /users/:id {name,email}	200 Updated user
USR_UPD_002	Update with invalid email	Negative	PUT /users/:id {email:'abc'}	400 Invalid email
USR_UPD_003	Update user role invalid	Negative	PUT {role:'super-admin'}	400 Role must be user/admin
USR_UPD_004	Normal user updating another user	Security	PUT /users/:id with regular user token	403 Forbidden
USR_DEL_001	Delete user as admin	Positive	DELETE /users/:id with admin JWT	200 Deleted
USR_DEL_002	Delete non-existing user	Negative	DELETE /users/9999	404 User not found
USR_DEL_003	Non-admin tries to delete	Security	DELETE with regular token	403 Forbidden
SEC_001	Expired JWT	Security	Call /users/* with expired token	401 Token expired
SEC_002	Tampered JWT	Security	Modify token signature	401 Invalid token
DB_001	Email uniqueness check	DB	PUT /users/:id with email used by another	409 Email already exists
EDGE_001	Long name field	Edge	PUT /users/:id with name 500 chars	400 or truncated
EDGE_002	Pagination overflow	Edge	GET /users?page=9999	200 empty list
WF_001	Create → Assign role → Update → Delete	Workflow	1.Create 2.Update role 3.Update email 4.Delete	Smooth flow

Role Module Test Cases

TC ID	Scenario	Type	Steps / Input	Expected Result
ROLE_CR_001	Create role - valid data	Positive	POST /role {name:'Manager', description:'Manages teams'}	201 Created
ROLE_CR_002	Create role - missing name	Negative	POST {description:'test'}	400 Name required
ROLE_CR_003	Create role - duplicate	Negative	POST {name:'Manager'} twice	409 Role already exists
ROLE_CR_004	Create role - whitespace name	Negative	POST {name:' '}	400 Invalid name

ROLE_CR_005	Create role - long name	Edge	POST {name:'A'*300}	400 or truncated
ROLE_GET_001	Get all roles - normal	Positive	GET /role	200 list
ROLE_GET_002	Get roles when none exist	Positive	DB empty -> GET /role	200 []
ROLE_GET_003	Check fields returned	Functional	GET /role	Returns id,name,description,is_active
ROLE_SEC_001	Endpoint accessible without JWT	Security	GET /role without Authorization	200 Public endpoint
ROLE_SEC_002	POST without JWT	Security	POST /role without token	201 Created (public)
ROLE_SEC_003	Brute-force create roles	Security	Send 50 POST requests quickly	200 or rate-limit
ROLE_DB_001	Unique name constraint	DB	Insert duplicate names	409 Error
ROLE_DB_002	Null name check	DB	Insert null name	400
ROLE_EDGE_001	Special characters in role name	Edge	POST {name:'@@@###'}	200 or 400
ROLE_EDGE_002	Very long description	Edge	POST {description repeated}	200 or truncated
ROLE_WF_001	Create role → Assign to user → Verify	Workflow	1.Create role 2.Update user 3.GET /users/:id	Role assigned successfully

Module Management

TC ID	Scenario	Type	Steps / Input	Expected Result
MOD_CR_001	Create module with valid fields	Positive	{"name":"Attendance","description":"Handles attendance"}	201 Created

MOD_CR_002	Create module without name	Negative	{"description":"Test module"}	400 Name required
MOD_CR_003	Create duplicate module	Negative	POST twice {"name":"Inventory"}	400 Duplicate module name
MOD_CR_004	Create module with long name	Edge	{"name":"A"*300}	400 or truncated
MOD_CR_005	Create module with special characters	Edge	{"name":"@@@Module###"}	201 Created if allowed
MOD_GET_001	Fetch all modules	Positive	GET /module	200 list
MOD_GET_002	Empty module list	Positive	DB empty -> GET /module	200 []
MOD_GET_003	Verify fields returned	Functional	GET /module	Each object contains id,name,description, is_active
MOD_SEC_001	No JWT required (public)	Security	GET /module without token	200 OK
MOD_SEC_002	POST /module without JWT	Security	POST /module	201 Created
MOD_VAL_001	Whitespace-only name	Negative	{"name":" "}	400 Invalid name
MOD_DB_001	Unique constraint check	DB	POST {"name":"HR"} twice	400 Duplicate name
MOD_EDGE_001	Very long description	Edge	{"description":"text"*5000}	200 or truncated
MOD_WF_001	Create module → Fetch modules	Workflow	POST CRM then GET /module	CRM present in GET

	→ Verify presence			