Password Reset / Unlock

Category: Access/Account

Sub-Category: User Account

Group: Password Reset / Unlock

Step No.	Action	Description	Expected Outcome
1	Verify User Identity	- Confirm caller via **registered phone/email/employee ID**. - Enter the Code or click the link sent to your email to verify the request.	User identity verified successfully.
2	Guide Self-Service Reset	- Click on self-service reset portal. - Create a strong new password with a mix of letters, numbers, and symbols.	User resets password without admin intervention.
3	Check Account Status	- Validate if account is **locked, disabled, or expired**. - In AD (Active Directory): Go to Account tab → User must change password → Unlock Account checkbox. - In SAP: run SU01 transaction.	Root cause of issue identified.
4	Unlock	- In AD/Portal: Right-click →	User account

	Account	**Unlock Account**. - Save and confirm. - For SAP: in SU01, choose **Unlock** option.	unlocked.
5	Generate Temporary Password	- Create password following organisation security policy (length, complexity, history rules). - Example: 12+ characters, mix of upper/lower, numbers, symbols.	Temporary password generated.
6	Deliver Temporary Password Securely	- Send via encrypted email, one-time SMS. - Never share plaintext via chat/phone.	User receives temporary password securely.
7	Force Password Change	- In AD (Active Directory): check User must change password at next login. - In SAP: set initial password flag.	User forced to set new password on next login.
8	User Instruction	- Inform user: "Use temporary password to log in and create a new password." - Share **password rules**: no dictionary words, avoid reuse, min length, special chars.	User is aware and prepared to reset password.
9	Validate	- Ensure new password	Password

	Policy Compliance	complies with: → SAP security rules → AD/SSPR rules → Organizational password standards. - Reject weak passwords.	accepted and compliant.
10	Backend Validation	- If repeated failures occur, check: → Synchronization scripts → Password sync connectors → Security policies.	Config corrected, preventing recurring issue.
11	Close & Document	- Confirm with user that login is successful. - Document actions taken . - Tag ticket as Resolved – Password Reset / Unlock.	Ticket closed, resolution documented.

VIM Workflow & Approvals Issue

Category: Record To Report

Sub-Category: Financial Accounting

Group: VIM Workflow and Approvals.

Step No.	Action	Description	Expected Outcome
1	Verify User Authorization	- Check user's assigned catalogs/roles for invoice approvals. - Ensure role like `SAP_MM_BC_INV_WIAPPROVE_PC` is assigned for My Inbox. - Validate authorization objects in **SU53** if access denied.	User has proper authorization for VIM approval.
2	Retry Approval	- Ask user to retry approval in **VIM Workplace/My Inbox**. - If "No administrator found" or workflow error, **refresh org environment**. - Use **SBWP (SAP Business Workplace)** fallback if Fiori/My Inbox fails.	Approval retry successful, or fallback access enabled.

3	Validate Invoice Data	- Check invoice header completeness (vendor, company code, PO reference). - Ensure attachments are visible and accessible. - Re-open **PDF preview** to confirm readability.	Invoice data validated, PDF preview functional.
4	Inspect Workflow Configuration	- Review VIM flexible workflow settings (approval patterns, rules, agents, substitutions). - Check workflow log in **SWI1/SWI2_FREQ**.- Re-trigger workflow if required.	Workflow settings validated and approval path corrected.
5	Analyse Exception Rules	- Review exception cases: • **417** = Price variance • **271** = Name/City mismatch • **113** = Missing data- Align exceptions with **MM/PO configuration**.	Exception root cause identified and mapped to MM-FI setup.
6	Validate Duplicate Check	- Investigate duplicate postings via **duplicate check rules**. - Verify status of invoices flagged as duplicates. - Remove false positives if found.	Duplicate errors cleared or corrected.
7	Correct VIM Engine Config	- Inspect VIM engine configuration and integration	Engine issues resolved, DP

		points with S/4 workflow. - Apply relevant **SAP Notes/Support Packages**. - Adjust **DP document types** if mismatched.	processing stabilized.
8	Implement Enhancements	- Use **BAdIs** for workflow routing/custom logic. - Implement substitutions where agents are missing. - Rebuild workflow if structural defects exist.	Customized workflow enhancements implemented.
9	Confirm Resolution	- Re-test approval in My Inbox and Workplace. - Validate FI/MM postings. - Ensure workflow moves invoice to next stage.	Invoice approval error resolved.
10	Close & Document	- Attach workflow logs or error screenshots. - Close ticket under "Resolved – VIM Workflow Error".	Ticket documented and closed successfully.

SAP Access / Authorization Issue

Category: Access/Account

Sub-Category: User Account

Group: Access/Authorization to SAP Systems and Apps

Step No.	Action	Details / Sub-Steps	Expected Outcome
1	Validate User Access Request	- Confirm user details (Employee ID, Department, Role). - Validate request type: **standard, developer, or business role**. - Ensure proper approval via **GRC/ITSM workflow** if applicable.	User request validated with correct justification.
2	Check Role Assignment	- Run SU01 → Roles tab to review assigned roles/profiles. - Verify if standard access roles already include **SE38** or **RSUSR100N** authorization. - Check role validity dates.	User's assigned roles identified.
3	Assign Standard Roles	- If missing, assign pre-approved **standard roles** for transaction access. - Ensure changes align with **role catalog** and SoD compliance.	Standard roles assigned successfully.
4	Verify Access in SE38	- Have user retry SE38 → Run program **RSUSR100N**.	Access test confirms role

		- If denied, proceed with trace analysis.	sufficiency or indicates missing authorization.
5	Analyze Missing Authorizations	- Execute **STO1** or **SU53 (Authorization Check)** to capture missing objects. - Identify which authorization object is blocking access. - Note TCODEs like SE38, SPRO, LTMC, or custom objects.	Missing authorization objects identified.
6	Apply Custom Roles/Objects	- Modify or assign **custom role** in **PFCG** with required authorization objects. - Adjust **field values (Auth fields)** per business requirement. - Re-generate and transport roles.	User receives access with correct custom objects.
7	Review Security Policy	- Ensure assignment complies with **org security policies**. - Validate segregation of duties (SoD) using **SAP GRC Access Control**. - Escalate to security team if high-risk transaction.	Role assignment is compliant and risk-free.
8	Implement Workflow	- If recurring, configure **GRC Firefighter ID** or temporary	Automated approval

	Controls	elevated access workflow. - Use **IdM workflows** to streamline request/approval process.	workflow in place.
9	Re-Test & Confirm	- Confirm successful execution without authorization error.	User gains expected access.
10	Document & Close	-Document actions taken. - Mark resolution type as **Access/Authorization Provided**.	Ticket documented and closed successfully.