OpsAtlas
OPERATIONAL RUNBOOKS BY SMALLWOOD ENTERPRISES
Reliable cloud operations documentation

Password Reset and Account Unlock

IT Service Desk Runbook 01

IT Service Desk Runbooks

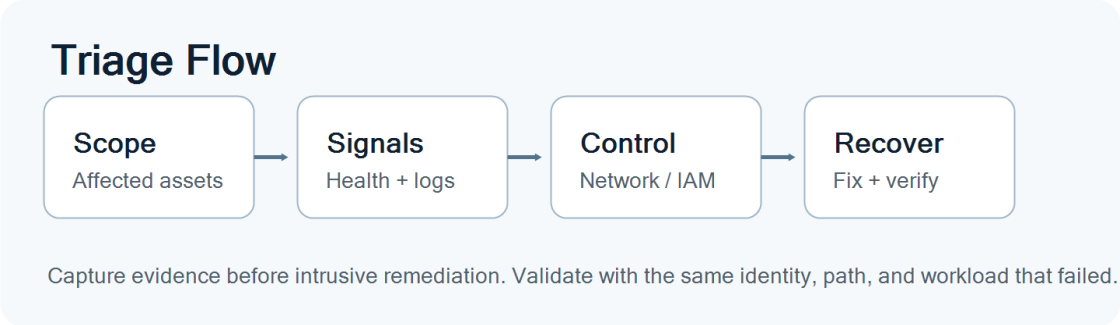
2026-05-29

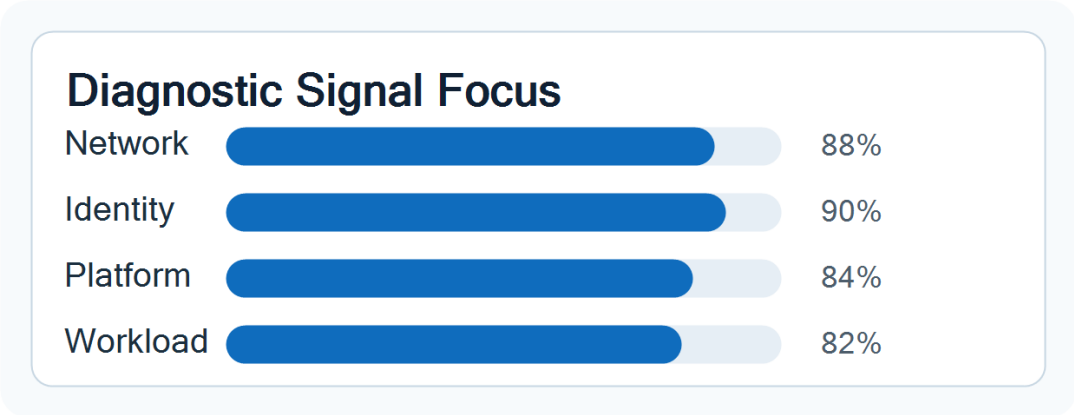
Table of Contents

Password Reset and Account Unlock

IT Service Desk Runbook 01
Audience: Tier 1 and Tier 2 service desk analysts, desktop support, MSP help desks, and IT operations leads
Severity guide: Sev 1 when a VIP, site, department, security-sensitive account, or business-critical workflow is blocked; Sev 2 when a single user or noncritical device has a workaround.
Incident objective: Restore user access while confirming identity, lockout source, MFA state, and whether the account is under attack.

> **Operator note:** Capture who is affected, when it started, exact error text, device/service identifiers, request IDs, screenshots, and before/after evidence. Prefer the smallest reversible change that restores service, then replace emergency access with a durable fix.





Common Symptoms

- User cannot sign in or reports account locked.
- Repeated prompts or invalid password errors appear across apps.
- Lockouts recur shortly after reset.

First 15 Minutes

- Verify caller identity using approved process.
- Check whether lockout is isolated or repeated across devices.
- Confirm recent password change, saved credentials, VPN/Wi-Fi mappings, and mobile email profiles.
- Review sign-in or security logs before repeated resets.
- Check MFA registration and conditional access prompts where applicable.

Command Starters

Replace placeholders before running. Use the approved admin context and record output in the ticket.

```
whoami /user

klist purge

cmdkey /list
```

```
Get-ADUser <user> -Properties LockedOut,PasswordLastSet,BadLogonCount
```

Decision Path

If you find...	Do this next
One-time forgotten password	Reset password and require change at next sign-in if policy requires.
Recurring lockout	Find stale credentials on phone, mapped drive, service, VPN, or scheduled task.
Suspicious sign-ins	Escalate security incident and preserve logs before reset.
MFA also blocked	Follow MFA reset/re-registration workflow.

Remediation Actions

- Reset password through the approved identity platform.
- Clear stale credentials from Credential Manager, mobile apps, VPN clients, and mapped drives.
- Unlock the account only after lockout source is understood.
- Escalate suspected compromise instead of repeatedly unlocking.

Validation Checklist

- User signs in successfully from a clean browser session.
- Lockout does not recur after 30 minutes.
- Ticket includes identity verification and lockout source notes.

Evidence to Attach

- User, device, service, tenant, location, IP/network, timestamps, and exact error text.
- Screenshots, logs, health/status evidence, message traces, policy results, or admin-center audit entries.
- Before/after configuration for identity, licensing, endpoint, network, mailbox, policy, or device changes.
- Approval record for any emergency permission, data restore, policy bypass, account unlock, deletion, rollback, or public exposure.

Customer-Facing Summary Template

What happened: `<brief customer-safe description>`
Impact: `<users/services/locations affected and time range>`
Root cause: `<confirmed root cause or current leading cause>`
Resolution: `<fix applied and validation completed>`
Prevention: `<monitoring, guardrail, training, policy, or knowledge-base follow-up>`

Reference Anchors

- Microsoft password reset help
- Windows troubleshooting