ACCOUNT & AUTHENTICATION TROUBLESHOOTING GUIDE
Version 1.9 | Last Updated: January 2025

==========
SECTION 1: PASSWORD RESET ISSUES
==========

SYMPTOMS:
- Cannot reset password via self-service portal
- Password reset email not received
- "Invalid reset link" or "Link expired" errors
- Password reset fails after entering new password
- Account locked after multiple reset attempts

ROOT CAUSES:
1. Email delivery delays or spam filtering
2. Expired or invalid reset token
3. Account locked due to security policies
4. Password doesn't meet complexity requirements
5. Email address not verified or incorrect

TROUBLESHOOTING STEPS:

Step 1: Check Email Delivery
- Check spam/junk folder for reset email
- Verify email address is correct in account
- Wait 5–10 minutes for email delivery
- Check email server status if corporate email
- Try alternative email address if available

Step 2: Verify Reset Link Validity
- Click reset link immediately (tokens expire quickly)
- Ensure link wasn't partially copied (check full URL)
- Try requesting new reset link if current expired
- Clear browser cache and cookies
- Try reset link in different browser

Step 3: Check Password Requirements
- Review password complexity requirements:
  * Minimum length (usually 8–12 characters)
  * Uppercase letters required
  * Lowercase letters required
  * Numbers required
  * Special characters required
  * Cannot match previous passwords
- Ensure new password meets all requirements
- Try different password that meets criteria

Step 4: Unlock Account
- Wait for automatic unlock (usually 15–30 minutes)
- Contact IT support to manually unlock account
- Verify account status in user management portal

- Check if account is disabled or suspended
- Review account lockout policy settings

Step 5: Alternative Reset Methods
- Use security questions if configured
- Contact IT helpdesk for manual reset
- Use mobile app for password reset if available
- Verify identity through support channels
- Complete account recovery process

AUTOMATED RESOLUTION:
- Script: reset-password.ps1
- Command: Reset-UserPassword -Username "user@company.com" -Method Email
- Verification: Test-UserAccountStatus

==========
SECTION 2: MULTI-FACTOR AUTHENTICATION (MFA) PROBLEMS
==========

SYMPTOMS:
- MFA code not received
- "Invalid MFA code" errors
- Authenticator app not working
- Backup codes not accepted
- MFA device lost or stolen

ROOT CAUSES:
1. Time synchronization issues
2. Incorrect MFA code entry
3. Authenticator app not properly configured
4. SMS delivery delays
5. Device time zone mismatch

TROUBLESHOOTING STEPS:

Step 1: Verify Time Synchronization
- Check device system time is correct
- Ensure time zone is set correctly
- Sync device time with internet time server
- Restart authenticator app after time sync
- Verify authenticator app time matches system time

Step 2: Check Code Entry
- Enter code immediately after generation (codes expire quickly)
- Verify no extra spaces before/after code
- Check if code is 6 or 8 digits as required
- Try next code if current one expired
- Wait for new code generation if needed

Step 3: Reconfigure Authenticator App
- Remove account from authenticator app

- Re-add account using QR code or setup key
- Verify account name matches in app
- Test code generation after reconfiguration
- Save backup codes in secure location

Step 4: Use Backup Codes
- Locate backup codes (saved during MFA setup)
- Enter backup code when prompted
- Use each backup code only once
- Generate new backup codes after using one
- Store backup codes securely

Step 5: Disable and Re-enable MFA
- Contact IT support to temporarily disable MFA
- Set up MFA again with new device
- Scan QR code or enter setup key
- Verify MFA works before closing support ticket
- Update MFA device in account settings

AUTOMATED RESOLUTION:
- Script: reset-mfa.ps1
- Command: Reset-MFADevice -Username "user@company.com"
- Verification: Test-MFAStatus

==
SECTION 3: SINGLE SIGN-ON (SSO) FAILURES
==

SYMPTOMS:
- SSO login redirects to error page
- "SSO authentication failed" message
- Infinite redirect loop
- Cannot access applications via SSO
- SSO works on some apps but not others

ROOT CAUSES:
1. SSO provider service outage
2. Incorrect SSO configuration
3. Browser cookie/session issues
4. Application not properly configured for SSO
5. Certificate or token validation failures

TROUBLESHOOTING STEPS:

Step 1: Check SSO Provider Status
- Visit SSO provider status page
- Check for service outages or maintenance
- Review SSO provider system status
- Wait for service restoration if outage
- Contact SSO administrator if persistent

Step 2: Clear Browser Data

- Clear cookies and cache for SSO domain
- Clear session storage
- Clear browser cache completely
- Close all browser windows
- Restart browser and retry SSO login

Step 3: Try Different Browser
- Test SSO in different browser
- Verify SSO works in alternative browser
- If works, issue is browser-specific
- Update or reinstall problematic browser
- Check browser extensions blocking SSO

Step 4: Verify Application SSO Configuration
- Check application is SSO-enabled
- Verify application appears in SSO portal
- Review application SSO settings
- Contact application administrator
- Check application logs for SSO errors

Step 5: Check Network and Firewall
- Verify network connectivity to SSO provider
- Check firewall allows SSO traffic
- Test SSO from different network
- Review proxy settings if applicable
- Check for blocked SSO domains

AUTOMATED RESOLUTION:
- Script: test-sso-connection.ps1
- Command: Test-SSOConnection -Provider "Okta"
- Verification: Get-SSOStatus

==========
SECTION 4: ACCOUNT LOCKOUT ISSUES
==========

SYMPTOMS:
- "Account is locked" error message
- Cannot log in after multiple failed attempts
- Account automatically locks repeatedly
- Lockout occurs immediately after unlock
- "Too many failed login attempts" warning

ROOT CAUSES:
1. Incorrect password entered multiple times
2. Automated login attempts (bot/script)
3. Stored credentials with old password
4. Account lockout policy too restrictive
5. Malicious login attempts detected

TROUBLESHOOTING STEPS:

Step 1: Wait for Automatic Unlock
- Review lockout policy (usually 15-30 minutes)
- Wait for automatic unlock period
- Do not attempt login during lockout period
- Verify lockout duration with IT support
- Check account status after unlock period

Step 2: Clear Stored Credentials
Windows:
- Open Credential Manager
- Remove stored credentials for affected account
- Clear Windows Credential Manager
- Remove from "Stored User Names and Passwords"

macOS:
- Open Keychain Access
- Search for account credentials
- Delete old or incorrect credentials
- Clear keychain cache

Step 3: Verify Correct Password
- Confirm current password with user
- Check if password was recently changed
- Verify password meets complexity requirements
- Test password on different device
- Reset password if uncertain

Step 4: Check for Automated Attempts
- Review account login logs
- Identify source of failed attempts
- Check for automated scripts or bots
- Review security event logs
- Contact security team if suspicious activity

Step 5: Adjust Lockout Policy (IT Admin)
- Review current lockout threshold
- Consider increasing failed attempt limit
- Adjust lockout duration if appropriate
- Review lockout policy with security team
- Document policy changes

AUTOMATED RESOLUTION:
- Script: unlock-account.ps1
- Command: Unlock-UserAccount -Username "user@company.com"
- Verification: Get-UserAccountStatus

==========
SECTION 5: CERTIFICATE & TOKEN AUTHENTICATION ERRORS
==========

SYMPTOMS:
- "Certificate expired" or "Invalid certificate" errors

- Token validation failures
- "Certificate not trusted" warnings
- Authentication fails with valid credentials
- Certificate chain validation errors

ROOT CAUSES:
1. Expired client or server certificates
2. Certificate not installed correctly
3. Certificate authority (CA) not trusted
4. Token expired or invalid
5. Clock/time synchronization issues

TROUBLESHOOTING STEPS:

Step 1: Check Certificate Expiration
- Review certificate expiration date
- Verify certificate is still valid
- Check certificate validity period
- Renew certificate if expired
- Install updated certificate

Step 2: Verify Certificate Installation
- Check certificate is in correct store
- Verify certificate chain is complete
- Review certificate installation logs
- Reinstall certificate if needed
- Test certificate after reinstallation

Step 3: Trust Certificate Authority
- Verify CA certificate is in trusted store
- Install CA certificate if missing
- Update trusted root certificates
- Review CA certificate expiration
- Contact CA if certificate issues persist

Step 4: Check System Time
- Verify system date and time are correct
- Sync time with internet time server
- Check time zone settings
- Restart device after time correction
- Retry authentication after time sync

Step 5: Renew or Regenerate Token
- Request new authentication token
- Clear old token from cache
- Generate fresh token
- Verify token format and validity
- Test authentication with new token

AUTOMATED RESOLUTION:
- Script: renew-certificate.ps1
- Command: Renew-ClientCertificate -User "user@company.com"
- Verification: Test-CertificateValidity

==
ESCALATION CRITERIA
==

Escalate to Identity & Access Management (IAM) Team if:
- Multiple users affected simultaneously
- SSO provider outage or configuration issues
- Security breach or unauthorized access suspected
- Complex certificate or token issues
- Enterprise-wide authentication failures

Contact Information:
- IAM Team: iam@company.com
- Security Team: security@company.com
- Emergency: 1-800-ACCESS
- On-call IAM Engineer: Check IT portal

==
END OF DOCUMENT
==