SOUTHGATE TERMINAL

Port Operations Security Documentation

Authentication Failure Response SOP

Document Information

Document Type: Standard Operating Procedure Intended Users: Technical Team, IT Security, System Administrators Usage Context: During authentication failures, credential compromise, or service account issues Related Scenarios: Service account failures (svc_gantry), password lockouts, authentication system compromise

---

Purpose

This SOP provides systematic procedures for responding to authentication failures, including service account lockouts, credential compromise, and authentication system malfunctions that could indicate security incidents.

When to Use This SOP

- Service account authentication failures (e.g., svc_gantry user)
- Multiple failed login attempts indicating potential brute force attacks
- Authentication system malfunctions or unusual patterns
- Suspected credential compromise or unauthorized access attempts
- Password rotation issues during operational incidents

Authentication Failure Classification

Level 1: Standard Authentication Issues

Characteristics: - Single user account lockout - Routine password expiration - Minor authentication service delays - Isolated login failures

Response Authority: IT Support Team Timeline: Address within 30 minutes Escalation: None required unless pattern emerges

Level 2: Service Account Failures

Characteristics: - Critical service account failures (svc_gantry, svc_crane, etc.) - Multiple service account lockouts - Authentication failures affecting operations - Service account credential rotation issues

Response Authority: Senior Technical Team Timeline: Address within 15 minutes Escalation: Operations Team immediate notification

Level 3: Suspected Security Incidents

Characteristics: - Multiple failed attempts from external sources - Authentication failures from unusual locations - Credential stuffing or brute force attack patterns - Evidence of compromised credentials

Response Authority: IT Security Team Timeline: Address within 5 minutes Escalation: Incident Coordinator and Legal Team immediate notification

Level 4: Authentication System Compromise

Characteristics: - Authentication system failure or compromise - Evidence of unauthorized access to authentication database - Multiple account compromises - Authentication bypass attempts

Response Authority: IT Security + External Security Consultant Timeline: Immediate response required Escalation: Executive Team and External Security immediate notification

---

Service Account Authentication Failure Response

Immediate Assessment (0-5 minutes)

Service Account Impact Analysis When svc_gantry or other critical service accounts fail:

1. Operational Impact Assessment:

☐ Affected Systems: Identify all systems using the service account
☐ Operational Impact: Assess impact on current operations
☐ Alternative Access: Check if alternative access methods available
☐ Service Dependencies: Identify dependent services and applications

2. Failure Pattern Analysis:

☐ Error Messages: Review specific authentication error messages
☐ Time Pattern: Check when authentication failures started
☐ Frequency: Determine how often failures are occurring
☐ System Correlation: Check if correlated with other system issues

Immediate Containment Actions

☐ Stop Automated Retries: Prevent account lockout from automated retry attempts

- ☐ Switch to Manual: Switch affected systems to manual operation if safe
- ☐ Log Preservation: Preserve authentication logs for analysis
- ☐ Impact Mitigation: Implement workarounds to maintain operations

Service Account Recovery Process (5-15 minutes)

Account Status Verification

1. Account Health Check:

- ☐ Account Status: Check if account is locked, disabled, or expired
- ☐ Password Status: Verify password expiration and complexity requirements
- ☐ Permission Verification: Confirm account still has required permissions
- ☐ Group Membership: Verify service account group memberships intact

2. System Integration Check:

- ☐ Authentication Server: Verify authentication server responding normally
- ☐ Network Connectivity: Check network connectivity to authentication services
- ☐ Service Configuration: Verify service configuration hasn't changed
- ☐ Certificate Validity: Check any certificates used for authentication

Recovery Actions

1. Account Unlock/Reset:

- ☐ Unlock Account: Unlock service account if locked
- ☐ Password Reset: Reset password using secure procedure if necessary
- ☐ Permission Restoration: Restore any missing permissions
- ☐ Group Membership: Restore service account to required groups

2. Service Restoration:

- ☐ Credential Update: Update credentials in affected services
- ☐ Service Restart: Restart services using the service account
- ☐ Functionality Test: Test service account functionality
- ☐ Monitoring: Enhanced monitoring of service account for 24 hours

Authentication Failure Investigation

Root Cause Analysis

1. Technical Investigation:

- ☐ Log Analysis: Detailed analysis of authentication and system logs
- ☐ Configuration Review: Review authentication system configuration changes
- ☐ Network Analysis: Check for network issues affecting authentication

☐ Timing Correlation: Correlate timing with other system events

2. Security Assessment:

☐ Unauthorized Access: Check for evidence of unauthorized access attempts
☐ Credential Compromise: Assess if credentials may be compromised
☐ Attack Patterns: Look for patterns indicating security attacks
☐ External Threats: Check for external threats or suspicious activity

---

User Authentication Failure Response

Multiple Failed Login Attempts

Brute Force Attack Detection Indicators: - Multiple rapid login attempts from same source - Login attempts using common passwords - Attempts against multiple user accounts - Unusual geographic locations for attempts

Immediate Response: 1. Source Analysis: - [ ] IP Address Investigation: Investigate source IP addresses - [ ] Geographic Analysis: Check geographic location of attempts - [ ] Pattern Recognition: Identify attack patterns and methods - [ ] Threat Intelligence: Cross-reference with known threat indicators

2. Defensive Actions:

☐ IP Blocking: Block suspicious IP addresses
☐ Account Protection: Lock accounts under attack if necessary
☐ Rate Limiting: Implement enhanced rate limiting
☐ Monitoring Enhancement: Increase authentication monitoring

User Account Lockout Response

1. Legitimate User Support:

☐ User Verification: Verify identity of locked-out user
☐ Account Unlock: Unlock account using secure procedures
☐ Password Reset: Assist with password reset if needed
☐ Security Briefing: Brief user on security awareness

2. Security Assessment:

☐ Compromise Check: Check if user credentials compromised
☐ Recent Activity: Review user's recent authentication activity
☐ Device Verification: Verify user's devices and locations
☐ Security Recommendations: Provide security recommendations to user

---

Authentication System Failure Response

System-Wide Authentication Issues

Authentication Service Failure

1. Service Status Assessment:

☐ Service Health: Check authentication service health and status
☐ Database Connectivity: Verify database connectivity and performance
☐ Network Connectivity: Check network connectivity to authentication servers
☐ Resource Utilization: Monitor CPU, memory, and disk utilization

2. Service Recovery:

☐ Service Restart: Restart authentication services if necessary
☐ Database Recovery: Recover authentication database if corrupted
☐ Configuration Restore: Restore authentication service configuration
☐ Performance Optimization: Optimize performance if resource-constrained

Alternative Authentication Procedures

1. Emergency Access Procedures:

☐ Emergency Accounts: Activate emergency administrative accounts
☐ Manual Verification: Implement manual identity verification procedures
☐ Temporary Access: Provide temporary access to critical personnel
☐ Documentation: Document all emergency access granted

2. Operational Continuity:

☐ Critical Systems: Maintain access to critical operational systems
☐ Safety Systems: Ensure safety systems remain accessible
☐ Communication Systems: Maintain access to communication systems
☐ Emergency Procedures: Implement emergency authentication procedures

---

Credential Compromise Response

Suspected Credential Compromise

Immediate Containment

1. Account Securing:

☐ Account Lockout: Immediately lock suspected compromised accounts
☐ Password Reset: Force password reset for compromised accounts
☐ Session Termination: Terminate all active sessions for compromised accounts

☐ Access Revocation: Revoke any special access or permissions

2. Impact Assessment:

☐ Data Access: Assess what data the compromised account could access
☐ System Access: Determine what systems were accessible
☐ Time Period: Establish timeframe of potential unauthorized access
☐ Activity Review: Review all activity by compromised account

Investigation Process

1. Forensic Analysis:

☐ Log Collection: Collect all relevant authentication and access logs
☐ Timeline Construction: Build timeline of account activity
☐ Unauthorized Activity: Identify any unauthorized activities
☐ Data Exfiltration: Check for evidence of data exfiltration

2. Scope Assessment:

☐ Other Accounts: Check if other accounts may be compromised
☐ Lateral Movement: Look for evidence of lateral movement in network
☐ Persistent Access: Check for backdoors or persistent access mechanisms
☐ External Communications: Monitor for unauthorized external communications

---

Password and Credential Management

Emergency Password Rotation

Rotation Triggers

- Suspected credential compromise
- Departing personnel with high-level access
- Security incident involving authentication systems
- Scheduled emergency rotation exercises

Rotation Process

1. Planning Phase:

☐ Scope Definition: Define scope of password rotation
☐ Service Impact: Assess impact on services and operations
☐ Timeline Planning: Plan rotation timeline to minimize disruption
☐ Communication Plan: Plan communication to affected personnel

2. Execution Phase:

- ☐ Password Generation: Generate new secure passwords
- ☐ Service Coordination: Coordinate password changes with service owners
- ☐ Update Documentation: Update password documentation securely
- ☐ Testing Verification: Test new passwords and service functionality

Service Account Credential Management

Service Account Security

1. Access Control:

- ☐ Least Privilege: Ensure service accounts have minimum required privileges
- ☐ Regular Review: Regularly review service account permissions
- ☐ Usage Monitoring: Monitor service account usage patterns
- ☐ Automated Monitoring: Implement automated monitoring for unusual activity

2. Credential Protection:

- ☐ Secure Storage: Store service account credentials securely
- ☐ Encryption: Encrypt stored credentials and communications
- ☐ Access Logging: Log all access to service account credentials
- ☐ Regular Rotation: Implement regular credential rotation schedule

---

Monitoring and Alerting

Authentication Monitoring

Real-time Monitoring

- Failed Login Attempts: Monitor for excessive failed login attempts
- Unusual Login Patterns: Detect logins from unusual locations or times
- Service Account Activity: Monitor service account authentication patterns
- Privilege Escalation: Monitor for unauthorized privilege escalation attempts

Alert Thresholds

- Multiple Failures: 5 failed attempts within 15 minutes
- Geographic Anomalies: Logins from unusual geographic locations
- Time Anomalies: Logins outside normal business hours
- Service Account Failures: Any service account authentication failure

Log Collection and Analysis

Authentication Logs

1. Log Sources:

- Authentication server logs
- Application authentication logs
- Network device authentication logs
- Operating system authentication logs

2. Analysis Focus:

- Authentication success/failure patterns
- Source IP address analysis
- User account activity patterns
- Service account behavior analysis

Communication and Escalation

Internal Notification

Authentication Failure Notifications Level 2-3 Issues: - Operations Team: Immediate notification for service account failures - IT Security: Immediate notification for suspected security incidents - Incident Coordinator: Notification within 15 minutes for operational impact

Level 4 Issues: - Executive Team: Immediate notification - Legal Team: Immediate notification for potential compliance implications - External Security: Immediate engagement for system compromise

External Notification

Regulatory Notifications

- Data Breach: If authentication compromise leads to data access
- Financial Impact: If authentication issues affect financial systems
- Safety Impact: If authentication failures affect safety systems
- Compliance Violation: If authentication issues violate regulatory requirements

---

Success Criteria

- Rapid identification and resolution of authentication failures
- Effective protection against unauthorized access attempts
- Maintained operational continuity during authentication incidents
- Successful investigation and remediation of security incidents
- Improved authentication security posture through lessons learned

---

Related Documents

- Technical Containment Guide
- Access Control Summary
- Incident Reporting Guide (Technical)
- Legal Risk Escalation Flowchart
- Crisis Communications SOP