AML Alert Suppression System - Management Documentation

Executive Summary

The AML Alert Suppression System is an automated solution designed to reduce analyst workload by intelligently suppressing repetitive false positive alerts while maintaining compliance standards. The system has been enhanced with stricter criteria to ensure only truly repetitive cases are suppressed.

Business Logic & Criteria

Suppression Qualification Criteria (ALL 4 Must Be Met):

1. **Historical Pattern**: Entity must have at least 2 closed cases with closure dates

2. **False Positive Status**: The last 2 closed cases (by date) must both be marked as 'Closed FP'

3. **Manual Investigation**: Both cases must have been closed with reason 'manual_investigation'

4. **Recent Activity**: Both closure dates must be after February 14th, 2025 *(New Requirement)*

5. **Different Dates**: The two cases must have been closed on different dates

Suppression Period:

- **Duration**: 60 days from the most recent closure date

- **Scope**: All open cases for the qualifying entity are suppressed

- **New Cases**: Any new cases created during suppression period are automatically suppressed

---

Four Output Reports - Usage Guide

1. Suppression Lookup Table 📊

File: `suppression_lookup_YYYYMMDD_HHMMSS.xlsx/csv`

Purpose: Operational table for real-time suppression checking

When to Use:

- **Daily Operations**: Check which entities are currently under suppression

- **Case Creation**: Integrate with case workflow to prevent new case creation

- **Monitoring**: Track suppression expiry dates for planning

Key Fields:

- `alert_entity_id`: Entity under suppression

- `suppression_end_date`: When suppression expires

- `days_remaining`: Countdown to expiry
- `suppression_status`: Active/Expired

Business Application:

- **Analysts**: Skip working on suppressed entities
- **System Integration**: Automatic new case prevention
- **Planning**: Prepare for suppression expiry

---

2. Suppressed Cases Detail 📋

File: `suppressed_cases_YYYYMMDD_HHMMSS.xlsx/csv`

Purpose: Detailed audit trail of suppressed cases

When to Use:

- **Compliance Audits**: Demonstrate which specific cases were suppressed and why
- **Quality Assurance**: Review suppression decisions for accuracy
- **Reporting**: Provide detailed case-level suppression information

Key Fields:

- `case_id`: Specific case that was suppressed
- `suppression_reason`: Detailed reason for suppression
- `original_alert_count`: Number of alerts in the suppressed case
- `suppression_id`: Unique identifier for tracking

Business Application:

- **Auditors**: Verify suppression logic was applied correctly
- **Managers**: Review impact on individual cases
- **Compliance**: Demonstrate audit trail for regulatory review

---

3. Comprehensive Report 📈

File: `comprehensive_report_YYYYMMDD_HHMMSS.xlsx/csv`

Purpose: Complete business intelligence and impact analysis

When to Use:

- **Weekly/Monthly Reviews**: Assess overall suppression effectiveness

- **Management Reporting**: Present ROI and efficiency gains to leadership
- **Strategy Planning**: Identify patterns and optimization opportunities
- **Performance Metrics**: Track analyst productivity improvements

Key Fields:

- `alert_entity_id`: Entity being analyzed
- `total_cases_suppressed`: Count of cases suppressed
- `total_alerts_suppressed`: Count of individual alerts suppressed
- `suppressed_case_ids`: "1001,1002,1003" (comma-separated list)
- `suppressed_alert_ids`: "A001,A002,A003" (comma-separated list)
- `analyst_hours_saved`: Estimated time savings (2 hours per case)
- `false_positive_rate`: Historical FP percentage for the entity
- `days_remaining`: Time left in suppression period

Business Application:

- **Senior Management**: ROI demonstration and resource optimization
- **Operational Managers**: Workload planning and capacity management
- **Analytics Teams**: Performance trend analysis and forecasting
- **Budget Planning**: Quantify cost savings from reduced manual review

---

4. Updated Cases Data 🔄

File: `updated_cases_YYYYMMDD_HHMMSS.xlsx/csv`

Purpose: Complete dataset with suppression flags applied

When to Use:

- **Data Integration**: Update your main case management system
- **Historical Analysis**: Maintain complete record of all case statuses
- **System Synchronization**: Ensure all systems reflect suppression status
- **Backup & Recovery**: Comprehensive data snapshot

Key Fields:

- All original case data plus:
- `status`: Updated to show 'Suppressed' for affected cases
- `suppression_applied`: Boolean flag indicating suppression

Business Application:

- **System Administrators**: Update case management databases

- **Data Engineers**: Synchronize suppression status across systems

- **Analysts**: See complete picture of case portfolio

- **Archive Management**: Maintain historical suppression records

---

Business Impact Metrics

Efficiency Gains:

- **Time Savings**: 2 hours saved per suppressed case

- **Workload Reduction**: Automatic elimination of repetitive false positives

- **Focus Enhancement**: Analysts can concentrate on genuine suspicious activity

Quality Improvements:

- **Reduced Alert Fatigue**: Fewer irrelevant cases for review

- **Consistency**: Automated decision-making for repetitive patterns

- **Compliance**: Detailed audit trail for regulatory requirements

Risk Management:

- **Conservative Approach**: Strict criteria (4 conditions + Feb 14th requirement)

- **Override Capability**: Manual review flags for exceptional cases

- **Expiry Management**: Automatic suppression expiry prevents indefinite blocking

---

Recommended Usage Schedule

Daily Operations:

- **Morning**: Check Suppression Lookup for active suppressions

- **During Workflow**: Use Suppressed Cases Detail for case-specific queries

- **End of Day**: Monitor new suppressions from daily run

Weekly Management Review:

- **Primary**: Comprehensive Report for business metrics

- **Secondary**: Updated Cases Data for system synchronization

- **Focus Areas**: Hours saved, suppression effectiveness, upcoming expiries

Monthly Strategic Review:

- **Deep Dive**: All four reports for complete analysis
- **Metrics**: ROI calculation, trend analysis, process optimization
- **Planning**: Resource allocation, rule tuning, system improvements

Quarterly Compliance Review:

- **Audit Preparation**: Suppressed Cases Detail for regulatory review
- **Documentation**: Comprehensive Report for management presentation
- **Validation**: Updated Cases Data for system integrity checks

---

Success Metrics & KPIs

Operational Efficiency:

- **Cases Suppressed**: Target 10-15% of open cases (varies by organization)
- **Hours Saved**: 20-40 hours per week (depending on volume)
- **False Positive Reduction**: 5-10% improvement in FP rates

Quality Metrics:

- **Suppression Accuracy**: >95% of suppressed cases remain valid suppressions
- **Override Rate**: <5% of suppressions require manual override
- **Compliance**: 100% audit trail availability

Business Value:

- **Cost Savings**: $50-100K annually in analyst time (varies by organization)
- **Productivity**: 15-25% improvement in analyst case closure rates
- **Risk Reduction**: Improved focus on genuine suspicious activity

---

Implementation Recommendations

Phase 1 - Pilot (Weeks 1-2):

- Run system weekly with manager review of all four reports
- Validate suppression decisions against manual analysis
- Fine-tune criteria based on initial results

Phase 2 - Deployment (Weeks 3-4):

- Integrate Suppression Lookup with case creation workflow
- Automate daily system execution

- Establish weekly management reporting routine

Phase 3 - Optimization (Month 2+):

- Analyze trends from Comprehensive Reports
- Adjust suppression criteria based on performance data
- Expand to additional entity types or rule patterns

Success Factors:

1. **Regular Monitoring**: Weekly review of all reports
2. **Team Training**: Ensure analysts understand suppression logic
3. **Continuous Improvement**: Monthly analysis of effectiveness metrics
4. **Compliance Readiness**: Maintain detailed audit trails

This documentation provides the framework for maximizing business value from the AML Alert Suppression System while maintaining regulatory compliance and operational excellence.