iSecurity

DATASHEET

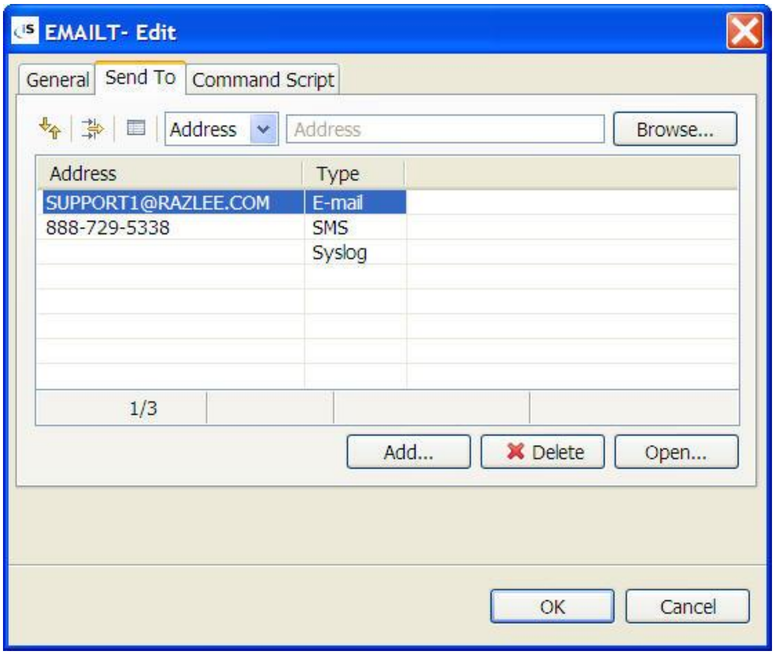
# Action™

## Overview

Action is a powerful IBM i security enhancing solution that intercepts security breaches and other events in real-time and immediately takes appropriate informative and corrective action. Actions may include sending alert messages to key personnel and/or running command scripts or programs that take corrective steps.

Action alerts can be sent as Syslog messages to any SIEM system, SMS, SNMP, e-mail, MSGQ or Twitter messages.

Raz-Lee's Syslog capabilities are "RSA Certified" for enVision, providing an RSA-support integration between the RSA enVision and iSecurity



| Address | Type |
|---|---|
| SUPPORT1@RAZLEE.COM | E-mail |
| 888-729-5338 | SMS |
| | Syslog |

1/3

Send alert messages to security personnel via Syslog, SMS, pager, email, SNMP etc.

## The Action Solution

In today's business environment, it is not enough to discover and report on a security problem after it occurs. Traditional audit software provides useful historical data after the fact but often lacks state-of-the-art functionality to provide relevant managers with alerts and enable corrective specific corrective actions.

Action provides a comprehensive, easy-to-use solution. For example, if a user attempts to copy a critical file, Action can send an SMS message to the security officer's mobile phone and automatically sign off and disable the offending user. Scripts can even initiate actions that execute if an appropriate response does not occur within a specified period of time!

Action real-time detection continuously monitors the system for a wide variety of security and other system events, including:

- Events detected by **Audit** real-time auditing
- Transactions detected by **Firewall** network security rules
- Viruses detected by **Anti-Virus**, suspicious data changes by AP-Journal and more
- Active job status and checking for jobs that are not active
- Current system and memory pool status

## Working with Action

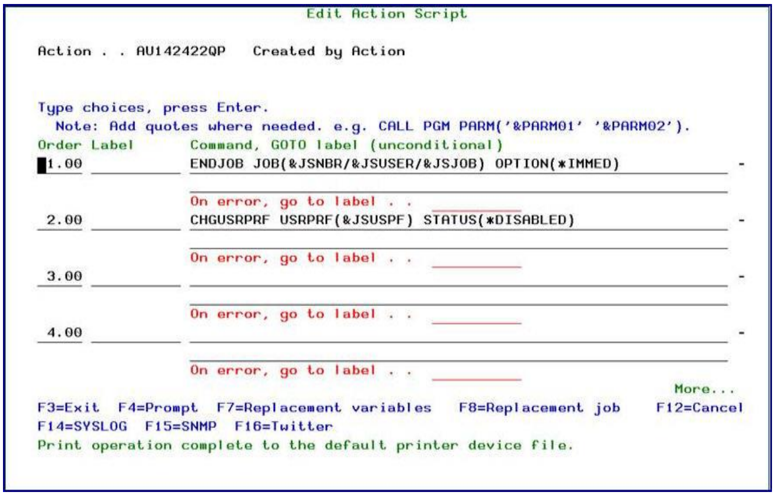
It is extremely easy to define rules and actions with the Action Rule Wizard feature. Rules trigger actions and alerts based on one or more parameters associated with a particular event.  Examples of selection parameters include user, date, time, job, workstation, library, object name, IP address, command, job name, etc.

Rule criteria use many different boolean operators such as: equal/not equal, greater than /less than, like/not like, "contained in list", "starts with", etc., and even Group/Item. For example "NE ALLUSERS/MANAGER" would filter events which were initiated by a non-manager! No other security alert/action system offers such power and flexibility.

Action includes additional security features such as automatic disabling of inactive users, restricting user access during planned absences and control over creating and running programs that use adopted authority.

# Key Features

- Alert messages sent via Syslog, SNMP, e-mail, SMS, MSGQ or Twitter
- Automatically takes corrective actions by running command scripts or programs
- Rule Wizard makes definition process simple for non-technical users
- Rules can use many different selection criteria
- Built-in command script interpreter with replacement variable support
- Responds to events detected by Audit, Firewall, AP-Journal, Anti-Virus, Authority on Demand, etc.
- Responds to current system status parameters and active jobs
- Restrict user access during vacations, holidays and other planned absences
- Automatically disables inactive user profiles
- Tight control over authority adoption



```
                              Edit Action Script

 Action . . AU142422QP   Created by Action


 Type choices, press Enter.
   Note: Add quotes where needed. e.g. CALL PGM PARM('&PARM01' '&PARM02').
 Order Label       Command, GOTO label (unconditional)
  1.00 ________    ENDJOB JOB(&JSNBR/&JSUSER/&JSJOB) OPTION(*IMMED)            -

                   On error, go to label . .  _________
  2.00 ________    CHGUSRPRF USRPRF(&JSUSPF) STATUS(*DISABLED)                 -

                   On error, go to label . .  _________
  3.00 ________                                                                -

                   On error, go to label . .  _________
  4.00 ________                                                                -

                   On error, go to label . .  _________
                                                                        More...
 F3=Exit  F4=Prompt  F7=Replacement variables  F8=Replacement job   F12=Cancel
 F14=SYSLOG  F15=SNMP  F16=Twitter
 Print operation complete to the default printer device file.
```

**Activate a CL command**

End the Job immediately and Disable the User Profile
Replacement variables beginning with &JS
are automatically generated

## Benefits

- Specially designed for use by non-technical users such as auditors, managers and administrators
- Alerts keep security officers and administrators informed about security breaches in real-time
- Automatic corrective actions minimize damage from security breaches and prevent recurrence
- You determine exactly what will happen, when it will happen, and under what conditions
- User access control features ensure that authorized users have access to the system only at appropriate times
- Adopted authority control prevents users from bypassing system security
- Superior human engineering ensures security implementation quickly, efficiently, and without requiring expensive security consultants