Incident tracking with Remedy

Andrew Cormack

JANET-CERT

Andrew.Cormack@ukerna.ac.uk

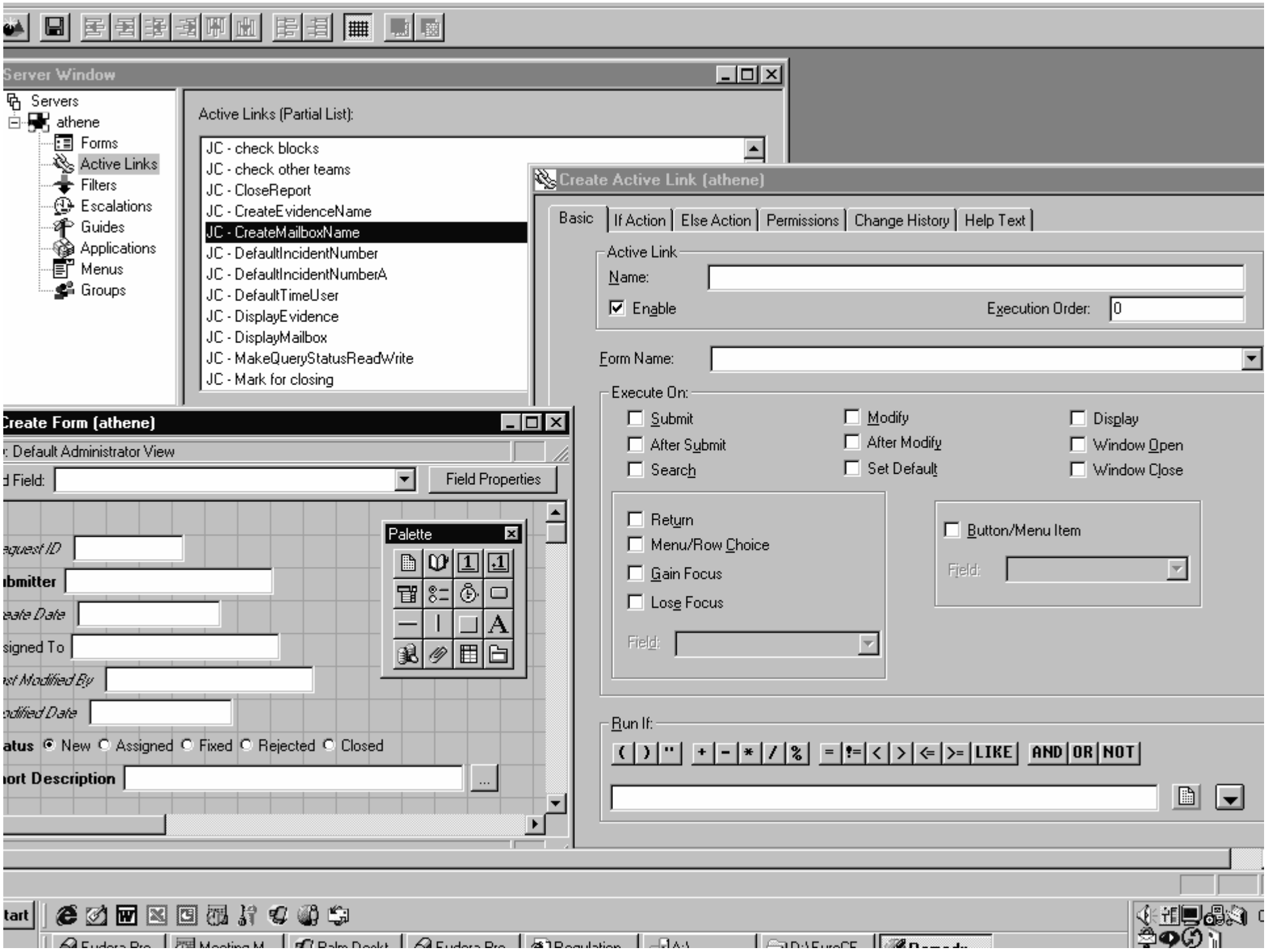
Remedy AR Server is a toolkit

Building blocks for tracking systems

Remedy sell systems built on it

- Helpdesk
- Inventory
- Etc.

We built our own…


Server Window
Servers
athene
Forms
Active Links
Filters
Escalations
Guides
Applications
Menus
Groups
Active Links (Partial List):
JC - check blocks
JC - check other teams
JC - CloseReport
JC - CreateEvidenceName
JC - CreateMailboxName
JC - DefaultIncidentNumber
JC - DefaultIncidentNumberA
JC - DefaultTimeUser
JC - DisplayEvidence
JC - DisplayMailbox
JC - MakeQueryStatusReadWrite
JC - Mark for closing
Create Active Link (athene)
Basic
If Action
Else Action
Permissions
Change History
Help Text
Active Link
Name:
Enable
Execution Order:
0
Form Name:
Execute On:
Submit
After Submit
Search
Modify
After Modify
Set Default
Display
Window Open
Window Close
Return
Menu/Row Choice
Gain Focus
Lose Focus
Field:
Button/Menu Item
Field:
Run If:
( ) " + - * / % = != < > <= >= LIKE AND OR NOT
Create Form (athene)
Default Administrator View
Field:
Field Properties
Palette
bmitter
signed To
atus
New
Assigned
Fixed
Rejected
Closed
ort Description
tart

Required functions

Record incident details

Record actions

Monitor progress of incidents

Generate reports

- For internal use (e.g. idle incidents)
- For external use (e.g. SLA reporting)

Information storage

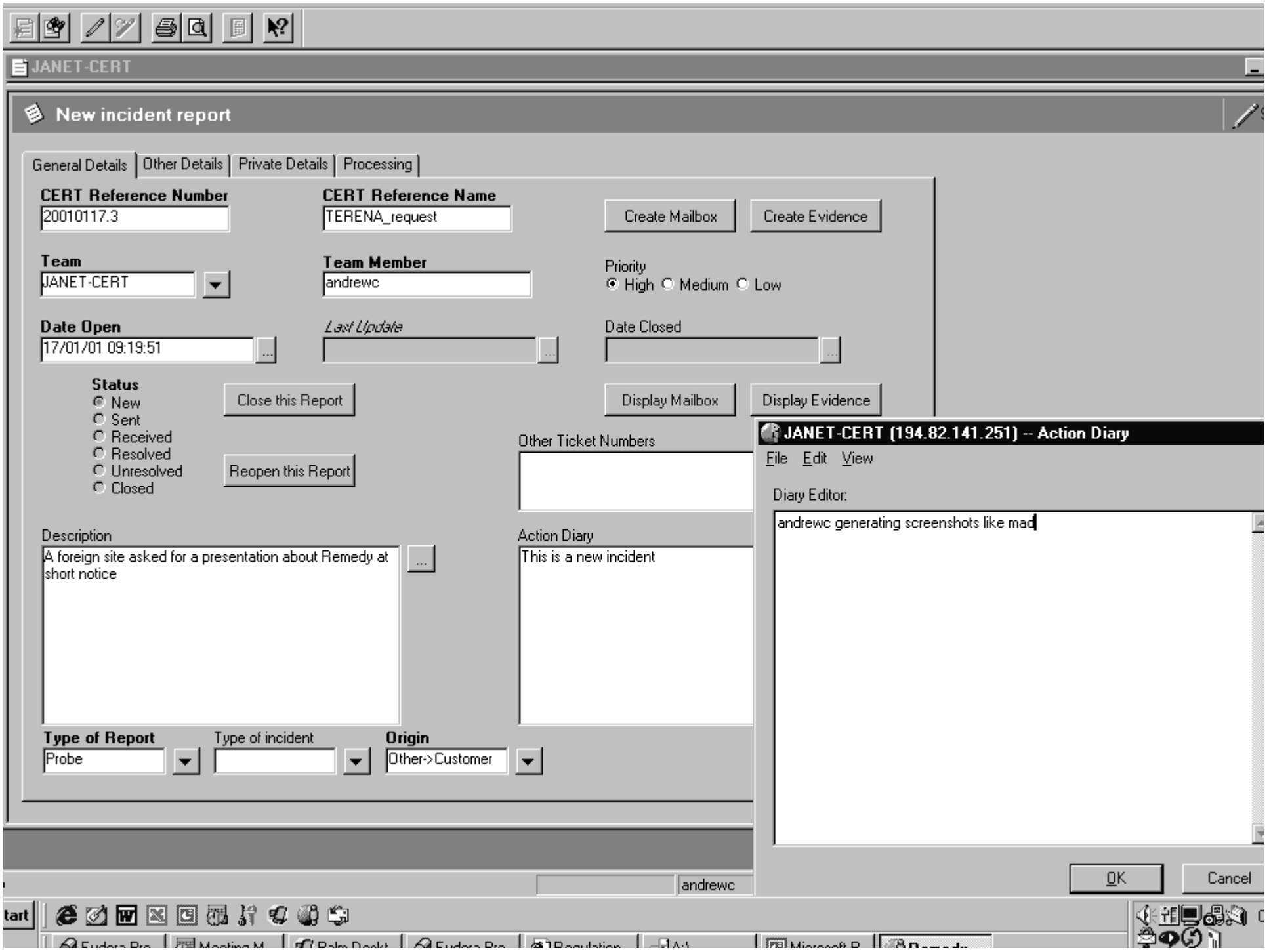
Remedy is a database application

We also store e-mails

- In mailboxes
- Linked by filename to Remedy database

DDE should allow e-mails to be sent from a form

- We’re still working on it…
- We can create/rename mailboxes already


JANET-CERT
New incident report
General Details
Other Details
Private Details
Processing
CERT Reference Number
20010117.3
CERT Reference Name
TERENA_request
Create Mailbox
Create Evidence
Team
JANET-CERT
Team Member
andrewc
Priority
High
Medium
Low
Date Open
17/01/01 09:19:51
Last Update
Date Closed
Status
New
Sent
Received
Resolved
Unresolved
Closed
Close this Report
Reopen this Report
Display Mailbox
Display Evidence
Other Ticket Numbers
Description
A foreign site asked for a presentation about Remedy at short notice
Action Diary
This is a new incident
Type of Report
Probe
Type of incident
Origin
Other->Customer
andrewc
JANET-CERT (194.82.141.251) -- Action Diary
File
Edit
View
Diary Editor:
andrewc generating screenshots like mad
OK
Cancel

Monitoring progress

Status field on Remedy form

Escalation (batch job) measures mailboxes

- Last e-mail date (& direction)

Daily reports for

- Idle incidents (no communication in N days)
- Active incidents (communication yesterday)

Delayed closure is another escalation

Reporting

Built-in facility is just about adequate

Use cron to run Remedy macro

- Perl script to tidy up report
- Can also buy commercial report writers!

Future developments

Better link to e-mail

More detailed status field

- Currently just open/closing/closed

Post-it notes

IODEF input/output