



# Incident tracking with Remedy

Andrew Cormack

JANET-CERT

[Andrew.Cormack@ukerna.ac.uk](mailto:Andrew.Cormack@ukerna.ac.uk)



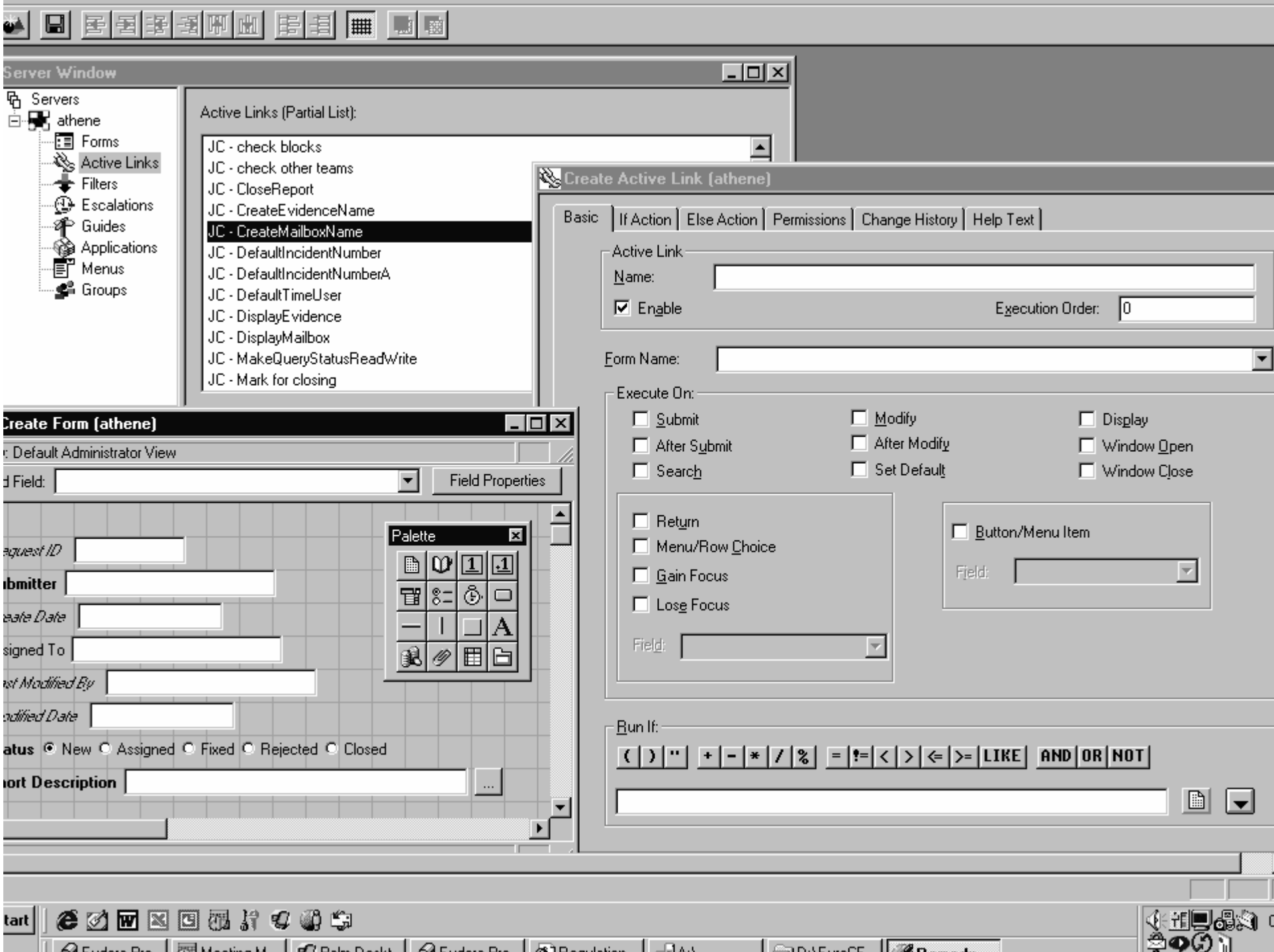
# Remedy AR Server is a toolkit

Building blocks for tracking systems

Remedy sell systems built on it

- Helpdesk
- Inventory
- Etc.

We built our own...





# 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

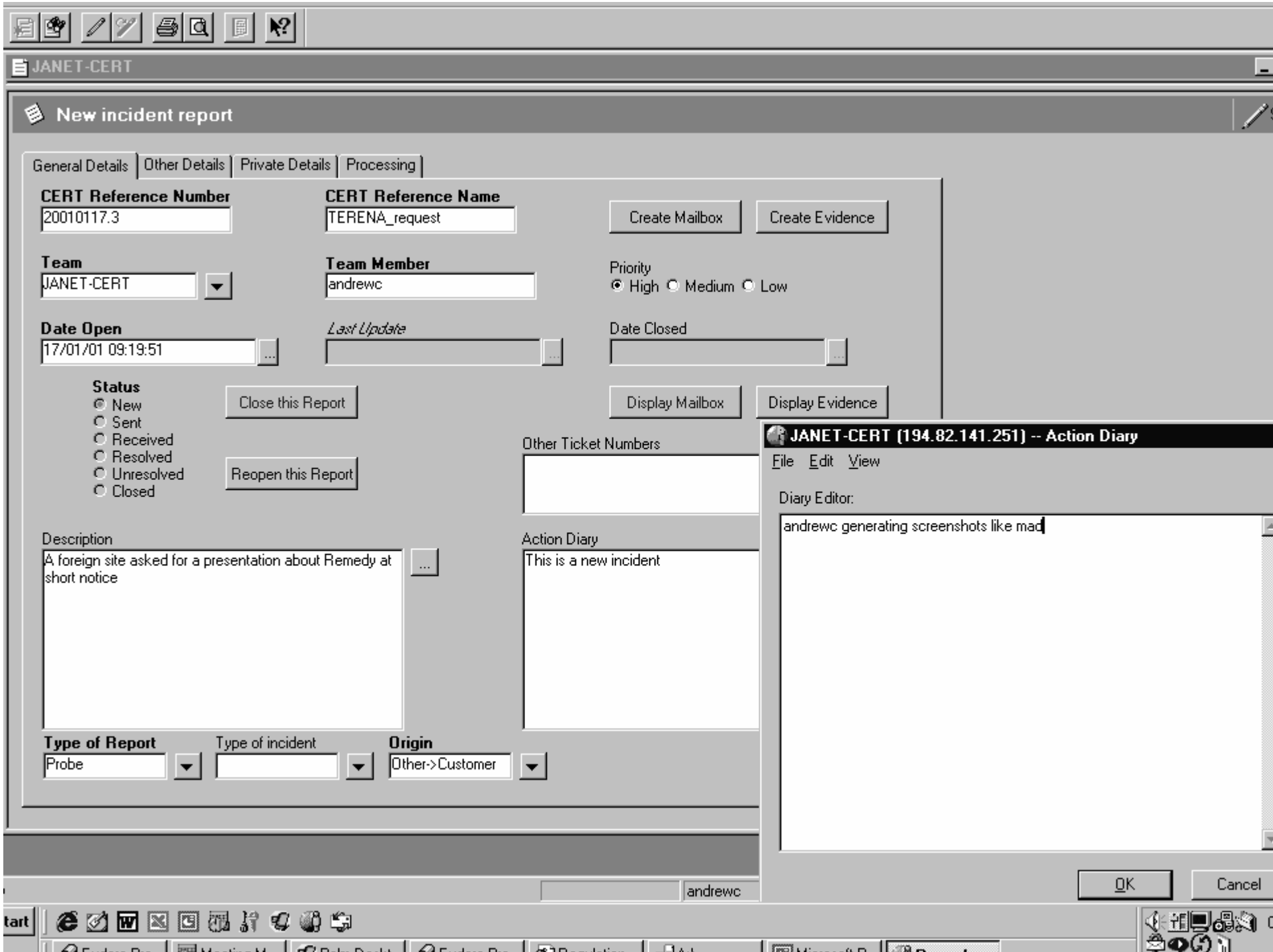
Remedy is a database application

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





# 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