



Capture™

Overview

Capture is a green-screen tracking solution that automatically captures and saves user activity as displayed on System i (AS/400) screens.

Capture works invisibly in the background without adversely affecting system performance. Users may not even be aware that it is collecting their screen activity.

Capture's invaluable tracing capabilities allow organizations to conform with the compliance requirements that apply to industries such as banking, insurance, health care, and defense. Capture works both a stand-alone product and also as a module fully integrated into the iSecurity suite.

```
Modify Rule

Type choices, press Enter.

Sequence . . . . . 100.0
Description . . . . . Non-working hours

Selection criteria      Not Value      Only specified fields are checked.
IP Address . . . . .  _  1.1.1.1
Subnet mask . . . . .  _
Time group . . . . .  _  NIGHTSHIFT
Job (Terminal Id) . . . . .  _
User / Special Authority . . . . .  _
Subsystem . . . . .  _
Rule is valid until date . . . . .  _ time _

Process
Capture (copy screen) . Y
Log CL program commands. Y

F3=Exit  F4=Prompt  F8=Print  F12=Cancel

Modify data, or press Enter to confirm.
```

The Capture Solution

In today's increasingly complex business environment, effective and searchable audit trails are a key component of any organizational IT security program. Regulations require many organizations to maintain detailed transaction activity records and to retain these records for an extended period of time.

In addition, IT departments and technical support personnel need to monitor user activity in order to troubleshoot error conditions, track performance bottlenecks, and ensure compliance with organizational policies. This often requires detailed knowledge of not only what users are doing, but also, how they are doing it. Computer logs and audit reports, more often than not, do not provide enough forensic evidence for these purposes.

Capture solves this problem by complementing journals and reports with a visual audit trail of user activity. Capture shows exactly what users are doing and when they are doing it! Screen capture sessions are initiated as required and are retrievable using an intuitive process featuring flexible scrolling and a powerful free-text search engine for locating the captured data screens and logs.

Within each screen capture session, you can scroll through the screens sequentially or you can use the moveable Capture Menu to jump directly to a particular screen or search for screens containing a specific text string. The Capture Menu also provides commands for displaying the job log and the Audit log entries related to the particular screen and capture session. You can even access the DSPJOB command and print the screen directly from the Capture Menu.



The floating Capture menu serves as a convenient control panel for navigating through frames and for displaying job and audit history logs associated with the current capture session.

Key Features

- Provides three solutions in one product - a powerful auditing solution, a regulation compliance solution, and a help-desk troubleshooting solution
- Captures and retains all System i green-screen user activity screens according to predefined criteria such as IP address, user profile, job name, date/time
- Replays user session screens, as if looking over the user's shoulder
- Enables compliance with Sarbanes-Oxley, HIPAA, the California Privacy Act and other regulations
- Preserves job logs and CL Command logs for subsequent review, even after a session is finished
- Uses a simple rule definition process suitable for both IT professionals and non-technical users
- Archives captured screens offline to meet data retention requirements without consuming excessive disk resources
- Searches user sessions in a specific timeframe, in accordance with any screen content, for example, mortgage or patient number specified in the screen
- Easy navigation through captured sessions via moveable Capture Menu

Benefits

- Runs either in "silent-mode" or as a deterrent known to possible offenders
- Automatically triggers screen capturing according to a variety of pre-defined rules
- Searches screens for suspicious content using a powerful text search capability
- Saves hours of tedious work and costly phone calls in the event of an application-related problem
- Retrieves captured user screens easily via a user-friendly display
- Reduces operational risk and fraud
- Provides an invaluable troubleshooting aid for Help Desks and Technical Support departments
- Works as a stand-alone product yet fully integrates with other iSecurity modules
- Installs in minutes, non-invasive and is risk-free