

ISIS Aspects™

ISIS has developed intelligent asset Management Software, Aspects™. Aspects™ is a Microsoft Windows application operating under Windows 95, 98 and NT; full Client/Server (SQL7) will soon be available.

In the last three years, manufacturers of “active” tagging hardware (battery-operated tags) have made significant advances in the performance, size and cost of tags. Aspects is versatile and easy-to-use software that harnesses these advances, allowing businesses to reap benefits in asset security, audit and deployment.

Aspects™ integrates with the best radio frequency identification (RFID) tags available. The system tracks and protects both mobile and static assets. From laptops and desktop equipment, to mission critical communications and trading systems, Aspects™ offers businesses complete control.

A typical installation incorporates sensors located at all exits to a building and throughout monitored areas. Aspects™ passively records all tagged asset movement throughout the enterprise and alarms when security breaches occur.

The system benefits businesses by protecting not only the static asset itself, but also its internal components and most importantly its data. Organisations depend on business critical systems, often housed in IT suites - the system protects cabinets from being opened without authority and the equipment they contain from being disturbed. IT assets are becoming smaller, more mobile and easier to conceal. Aspects™ alarms when portable assets leave the building without authorisation.

Since tags communicate with sensors at user definable intervals, Aspects™ offers businesses the capability of tracking assets in real-time. Some tags are read/write capable and maybe pre-programmed with information such as maintenance requirements, lease expiry, capital cost for depreciation and system configuration (available Q1 2000). Aspects™ delivers cost efficiencies by automating these time-consuming processes.

The system software can be integrated with non-proprietary security systems such as building Access Control and in particular CCTV to deliver video evidence of unauthorised security breaches.

The ISIS logo is displayed in a large, bold, sans-serif font. It is positioned on the left side of the page, partially overlapping a large, light blue abstract graphic that resembles a stylized eye or a curved shape. The background of the entire page is white, and the blue graphic extends from the bottom left towards the right edge.

System Security



Figure 1

Multi-user access to the programme is password protected (see Figure 1).

All windows in the program are "point & click", making management of the system at all authorisation levels very user friendly.

Communication between the software and the network of reader sensors in a building is constantly monitored and displayed on a ribbon at the bottom of the main window, along with any tag battery low warnings, the system user and system date and time.

ISIS

Asset Security

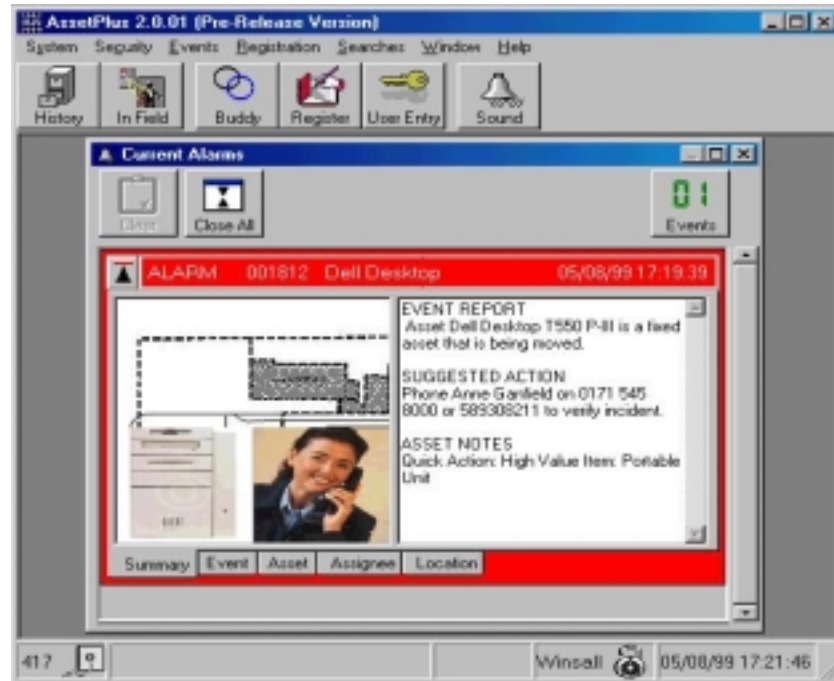


Figure 2

Figure 2 is the Aspects™ Main window. All other windows are child windows of this screen. The Current Alarms window is permanently displayed and takes priority over all other windows when in alarm.

When an *unauthorised* event occurs an audible alarm sounds and immediately the Current Alarms window flashes graphics relating to the security breach, such as the owner of the asset, a visual of the asset itself and where the alarm is located. Aspects™ gives security controllers the tools necessary to prevent theft rather than belatedly searching for information long after the breach has passed.

Comprehensive data concerning the Asset, Assignee and Location are available by clicking on the relevant tab at the bottom of the window. The system manager can mandate a written record of what action was taken in the "Options" set-up before the software will allow security controllers to clear an alarm to the History log.

Typical alarms are:

- SAT Alarm - unauthorised movement of a static asset
- PAT Alarm - a portable asset is leaving the building without authorisation
- Tamper Alarm - when a tag is taken off an asset inside the building
- Reader Tamper - when the cover is removed from a reader sensor
- Reader Offline - when communication between a reader sensor and the software has been terminated
- CAB Alarm - when an IT cabinet is opened without authorisation

ISIS

The alarm flashes both the importance of the asset and the type of alarm. The system manager may pre-configure the colour code for each event and asset priority furnishing the security controller with visual recognition of the importance of that event.

When a security breach has been rectified the security controller clears the event to the History database which logs all authorised and unauthorised events in descending order.

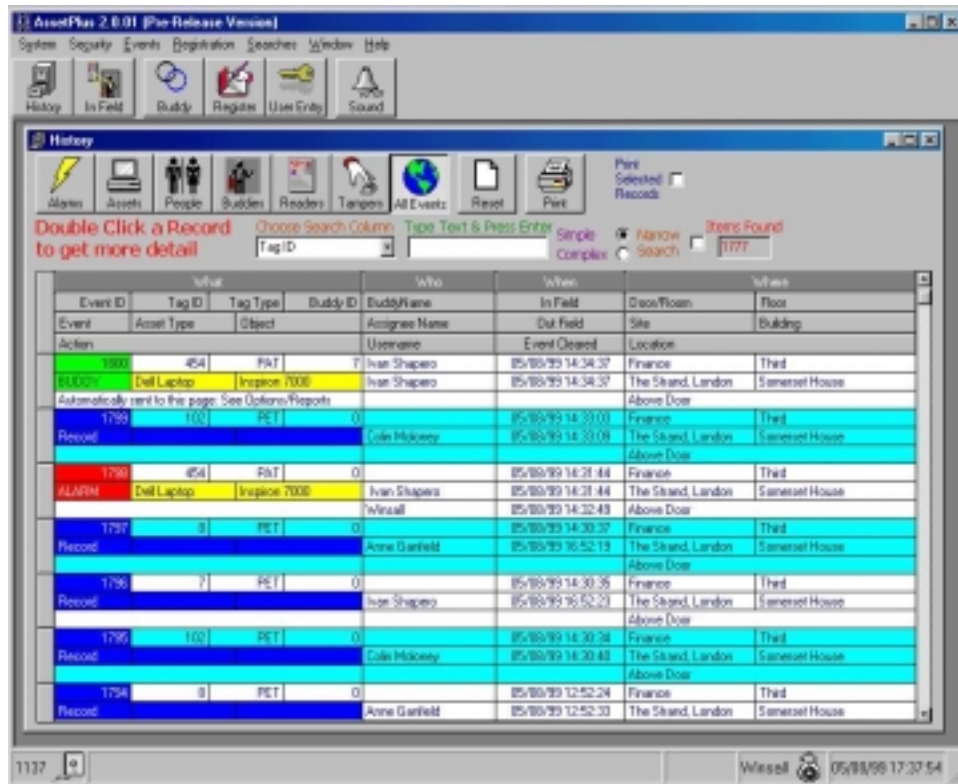


Figure 3

The History window (Figure 3) also unobtrusively records non-alarm events: personnel access and egress, and *authorised* removal of portable assets from the site - a process commonly called "buddying".

When an employee is authorised to take an asset out of the building the asset and personnel tag details are downloaded by the reader sensors to the Aspects™ software which then correlates the "buddy" transaction and silently records the event.

Event records in the History window are filtered using specific event icons at the top of the window. The system manager may also process a granular search using any combination of the data headings, for instance where an asset or person (or both) has been, within a certain timeframe, or through a certain door.

For More Information...

Please contact:

ISIS Limited
11 Kings Road
London
SW3 4RP

Tel : 020 7259 9212
Fax : 020 7259 9213
Email : info@isis.co.uk

Website : www.isis.co.uk

© Copyright 1999-2000 ISIS Limited. All rights reserved.



ISIS