

IDent/3000 Summary

(c) Paul Taffel (PTC), 2001-2010
last update 2010-04-07

IDent/3000 allows MPE sites to significantly enhance their ability to monitor and control access to restricted data, and to create highly secure audit logs. IDent is tailored to the particular needs of companies faced with becoming compliant with PCI (Payment Card Industry) standards; it was designed with significant input from Ecometry users, and implements several unique features never before available on the HP3000.

IDent's features are tightly integrated, but may be divided into the following major areas:

- User Keystroke Logging.

Everything that any user types anywhere can be recorded, and retained for later audit. The audit trail includes whatever prompt was displayed (to simplify interpreting the audit file), a timestamp, all user input, and annotations if the user attempted to access any restricted files, or if they changed their MPE capabilities using a capability boosting program (like Vesoft's 'GOD' utility).

- TurboIMAGE Database Password Management.

TurboIMAGE password security can be configured by rules that allow database access to be defined independently of which password a user (or program) supplies. Rules are defined externally to databases, and allow TurboIMAGE passwords to be changed as often as required, without requiring any changes to the application programs that open the databases. This allows applications to continue working when TurboIMAGE passwords are changed, even if application passwords are hard-coded and the program source is unavailable.

- TurboIMAGE Dataset Access Security and Logging.

Both read and/or write access to particular datasets can be closely controlled, and all accesses can be logged. This feature may be used to closely control and monitor access to datasets containing Credit Card information. Accesses are logged in the same file used for User Keystroke logging, and can show the full audit trail of commands issued by users who gain (or attempt to gain) access to restricted datasets.

- File Access Security and Logging.

Access to particular files (or filesets) can be closely controlled, and all file accesses can be logged. This feature may be used to closely control and monitor access to files that contain restricted information. Accesses are logged in the same file used for User Keystroke logging, and can show the full audit trail of commands issued by users who gain (or attempt to gain) access to restricted data.

- Critical File Purge Protection.

Individual files (or filesets) can be protected against being purged or erased by any user, including users with SM or PM capability. This feature is intended to protect IDent audit files from tampering, and to provide an audit trail of any attempts to delete or modify the files, but may also be used to protect log files used by other products. Protection extends to attempts to purge files by any means (including, for example, PURGE, PURGELINK, PURGEGROUP, PURGEACCT, RESTORE, etc.). Purge attempts are logged to the same file used for User Keystroke logging, and can show the full audit trail of commands issued by users who attempt to purge critical files.

- Detecting Modifications to User-Defined 'Critical' System Files.

Critical files may be periodically scanned for modifications. IDent does not rely on timestamps to detect if files have been modified, but instead uses a cryptographically-secure hashing algorithm ('Whirlpool') to calculate a 512-bit message digest (or checksum) for every monitored file. These checksums are stored in a protected location, and can be used by IDent to automatically flag if a monitored file has been added, modified, or deleted. The checksum database can be stored remotely for additional security.

IDent is implemented using a number of features that further enhance implementing enhanced security:

- Central Configuration File with Simple and Flexible Rule Syntax.

IDent uses a powerful and flexible syntax designed to simplify setting up access control rules. IDent's rule-driven features allow rules to be defined that restrict access as a function of many different attributes, including the user's logon (job/session name, LDev number, IP address), the program's environment (program name, the UDC and/or command file used to access the program, and the program's STDIN file name), and advanced attributes such as the names of ancestor processes, and even the names of other files opened by the program. Rule syntax allows lists of authorized Users and Programs to be centrally defined and referred to by synonyms in other rules, simplifying complex configuration needs.

- Ability to Protect Against Attack by SM Capability Users.

IDent protection rules potentially apply to all Users, and the product can be configured to provide substantial protection against unauthorized access by any user, including users with SM capability.

- Flexible Violation Logging.

Access attempts (whether allowed or blocked) can be logged to the same file used to hold each User's keystroke audit trail, and can also be copied to the System Console, to a dedicated Security Monitor Session, and even displayed on the User's own terminal.

- Remote Log File Storage.

The audit files created by IDent may be automatically copied to a remote system (using FTP), as soon as the job or session they refer to logs off. The audit files may also be renamed and archived on the HP3000 system, in a protected location. Audit log files can be automatically discarded if they do not contain evidence of an attempt to access restricted information.

- Simple Installation and Removal.

IDent can be enabled or disabled by typing a single command; all configuration commands and access rules are defined in a single ASCII file, and no changes are required to any Jobs, UDCs, Command Files, or Application programs to take full advantage of all the security enhancements that it implements. When IDent is disabled, systems revert immediately to their state prior to enabling IDent, with no lasting effects.

For more information, or to obtain demonstration software, please contact the author:

Paul Taffel
ptaffel@io.com

424 442 9003