



## Development of PixAlert Auditor 4.1

This document introduces some recent modifications to PixAlert's Auditor software. This is intended as a detailed, but user-focused description.

**Key:** (I) Image focused feature (CD) Critical Data focused feature (G) General feature

## Recent Development History

Some key new features that PixAlert have recently incorporated in the Auditor software are as follows.

- Reviewers can white list critical data result patterns from within the reviewing GUI (CD)
- Scan administrators can 'set to pending' disconnected targets to force them to resume (G)
- Auditor can automatically repopulate rescan targets from active directory and file shares (G)
- Scan administrators can target IBM DB2 databases. (CD)
- Auditor scanner can handle text from PDF files created with new Adobe Acrobat 9.0 (CD)
- Auditor can get critical data results from Auditor Remote Agent (CD)
- Auditor Remote Agent can be installed to remote machines so that they can be scanned even while off the network. (G)
- Reports showing timescale can now work off MONTH created/sent fields, not just year (G)
- Reviewers can clear out the image black list (I)

## Auditor 4.1 release

The following new features are being fully incorporated into the upcoming Auditor 4.1 software.

- Reports can include the ACLs of results found in scans. (G)
- Text can be extracted from images using the state-of-the-art *Tesseract OCR* engine (CD)
- Known images of any type can be discovered. (I)
- Last Accessed dates can optionally be left alone in all files scanned. (G)
- More comprehensive and user-friendly critical data reviewing facilities (CD)

Some cosmetic changes to Auditor will be implemented as part of the new version. There are 2 textual labelling modifications to be made:

- System tray icon for the 2 Auditor windows. (G)
- New severities and descriptions for critical data (CD)
  - Include default descriptions for UKNI, SSN, etc. results.
  - Use numbers of pattern hits in descriptions

- Default max. file size will go from 10mb ->100mb (G)

Two major new features incorporated into Auditor 4.1 include:

- Automatic Classification Policies (CD)
- Automatic Reporting (G)

Each of these has a new menu item and dialog for configuring the setup of each feature.

### Automatic Classification Policies

This feature is designed to automate the reviewing process for critical data results. As there is a lot more information about results available in the reviewing of critical data, and it is a task more suited to be done procedurally than image review, this feature has been implemented to automate the amount of reviewing that needs to be done for critical data results.

Each scan has a set of 'policies', and there is also a default set of policies that will be assigned to newly created scans.

Each policy has a set of rules, and an action to be carried out once the rules all hit.



The automatic classification feature is intended to automatically move critical data results into obvious categories automatically. EG If a file is found with over 1000 credit card numbers, it should automatically be reported regardless of whether the file has been encountered and reported before.

This feature will not mean that all critical data reviewing will be made unnecessary, as false positives will still need to be removed from reports.

Access the Automatic reviewing settings through the Auditor menu 'Review->Auto Review Policies'

### Automatic Reporting

This feature will allow a selection of reports to be automatically generated on scan completion, and either dropped in a file share location, or emailed to an address.

The reports that can be auto-generated, for both image and critical data results, are as follows:

- Audit summary report
- Email Audit summary report
- Description summary report
- Full details report

The reports can contain aliased user and location information if necessary, and they can be password protected before being emailed / exported.

Access the Automatic reporting settings through the Auditor menu 'Reports->Auto Export Reports'