Intella 2.2.1 Release Notes

Highlights

- Added a **Welcome** tab.
- Improvements supporting the **large-scale redaction** of items, such as **queuing** items for redaction based on their keyword hits, **pre-generating redaction PDFs** to speed up the Redaction tab's loading time, redacting entire **page ranges**, and the automatic **redaction of duplicates**.
- Reorganized the **right-click menus** in the Table and other components.
- Several **facets load faster**.
- Many **indexing** and **OCR** improvements.

General

- A Welcome tab is now shown in all cases. This tab shows an overview of what is new in this Intella release, points the user to the various documentation, support, and training options, and offers hyperlinks to e.g. add a new evidence source or open the Dongle Manager.
- Various improvements to how the events.log file stores information and how the Restore Annotations functionality can use it to recover data when the case becomes corrupt, e.g. due to a power outage or disk failure.
- Improvements to the default window size and positioning.
- Reorganized the contents of the General tab in the Preferences window.
- Added a "Release Notes" item to the Help menu.
- Resolved a fatal error that would result in Intella not shutting down properly.
- Resolved a rendering error when the first tab in the main window is the default tab in a case.

Licensing

- The requirement to have at least 100 days of remaining Maintenance Agreement coverage has been reduced to 60 days.
- The version update notification now indicates when a license upgrade is required to run the new version. Dongle users will see "Dongle upgrade required". Intella P.I. users will see "License upgrade required".

Indexing – General

- Resolved an issue with the Remove button in the Passwords tab of the Key Store window not working properly.
- Updates for processing Apple Mail files and EMLX files.
- Added support for indexing loose S/MIME encrypted messages (usually .p7m files).
- Many improvements to the indexing of archives.
- Updates for indexing the most recent Cellebrite UFED XML exports and UFDR reports.
- Images in OpenOffice/OpenDocument files are now extracted.
- Improved parsing of email senders and receivers in cellphone extracts that contain both the contact name and the email address.

- Improved the extraction of email senders and receivers from PST/MSG/TNEF items. Instead of Active Directory addresses (X.500 Distinguished Names), regular contact names and email addresses will now be shown.
- Updates for indexing various browser artifacts such as download histories, typed URLs, and bookmarks.
- Improvements to the processing of date attributes:
  - Unrealistic dates are suppressed, e.g. dates before or at 1-1-1970 00:00:00 GMT, or at 1-1-1980.
  - Two-digit years in Date headers are corrected to a date in the range 1950 – 2049.
- Improved handling of emails with a non-standard MIME multipart hierarchy.
- Added the ability to index L01 files that contain folders with illegal characters in their name.
- Resolved an issue with missing files when indexing a MacOS disk image.
- Resolved some indexing issues with MS Exchange EDB files.
- Resolved suppressed indexing errors when processing registry artifacts.
- Resolved unnecessary copying of disk images to a temporary file.
- Email items that lack a body and all header fields relevant for message hash calculation are no longer seen as duplicates.
- Various logging improvements.

Indexing – Load Files

- Reintroduced the "Use the following column and value to identify emails" field. This was removed in an earlier version.
- Performance improvements when importing a large number of custodians.
- Added the ability to map data to the Conversation Index column.
- Added the ability to import hierarchical tags.
- Resolved an issue with rotated PDFs not importing correctly.

OCR

- Resolved memory issues that could occur when OCR-ing very large files.
- Various improvements to OCR-ing problematic files due to an upgraded OCR library.
- When using ABBYY Recognition Server, version 4 is now the default version.

Searching

- Performance improvements for opening branches in the Email Address, Chat Account and Phone Number facets. In one test, loading and displaying the From branch in the Email Address facet went from 4 minutes to 5 seconds.
- The Email Address and Chat Account facets are now case-insensitive. For example, two occurrences of the same address but with different casing will now be shown as a single entry in the Email Address facet.

Results

- The growing right-click menu in the Table, List and Thumbnail views has been reorganized to be easier to handle and allow for future expansion. This menu is now also used in the Timeline, Cluster Map, Geolocation view and Searches list.

- The table row divider is now turned on by default. When the table is sorted on a column supported by this divider (e.g. a date-based column), it will render lines in the table that group the rows that have the same value in that column.
- The Location column that is populated through Content Analysis has been renamed to "Geographical Location". This prevents confusion with the Location column that represents the evidence location and prevents column name clashes in the CSV export.
- Added a "Batches" column to the Table and CSV export and to the Properties tab in the Previewer.
- Resolved a fatal error when creating a very large Timeline visualization.
- Resolved an issue with the Custodians facet not updating properly after deletion of a source.

Previewer

- The output of the Print Report button has been simplified to only show the item's native rendering, the most critical item metadata, and (optionally) the native rendering of its attachments.

Tagging

- Performance and stability improvements when using the -importTags command-line option.

Redaction

- Added an option to queue the current item for redaction, together with its currently highlighted keyword hits. This queue can then be processed batch-wise later, which creates their redaction PDFs and applies the redactions to these keywords.
  - This functionality makes it possible to quickly review keyword hits in the Contents and Preview tabs and postpone the generation of the redaction PDF generation. That generation can then be run when Intella is not in use, e.g. run overnight.
  - It is recommended to review the redaction PDFs and the added redactions in the Redaction tab after processing the queue.
  - This functionality is currently only available for local cases.
- Added a menu item for pre-generating redaction PDFs for a set of items. This can be used to speed up the initialization time of the Redaction tab.
  - The benefit of this option over the queue option described above is that the user is reviewing the redaction PDF, which may differ from the presentation shown in the Contents and Preview tab.
  - The downside is that redaction PDFs are generated for items that ultimately turn out not to need any redactions.
- Added an option to let any redactions be applied to all duplicates automatically.
- Added a button to redact full pages. One can either redact the current page or a range of pages.
- Added a menu item for removing all redactions of a set of items.
- Resolved an issue with export errors being added to the redaction PDF rather than the export report.

Exporting – General

- When exporting items from the Review tab, the sort order used in this tab is now used for ordering the export, rather than the sort order that is used in the Search tab.

Exporting – PST

- Improvements related to exporting to PST on Windows 10 or when using MS Outlook 2019.

Exporting – Load Files

- Added a checkbox titled "Opticon Page Count field contains number of pages of entire document". This checkbox controls the meaning of the last field in an Opticon file. When switched off, the field is interpreted as the number of pages of the current image file. When switched on, it becomes the number of pages in the entire document. This number should then only be listed for the first page.
- Added ALL_LOCATIONS and ALL_CUSTODIANS as custom field types.
- Reduced the verbosity of the date notation when using the "date only" format for a custom field.

Upgrade Notes

Intella 2.2.1 can directly open cases made with Intella 2.2 and 2.1.x.

When a case made with Intella 2.1 or older is opened, all Content Analysis results are automatically migrated to a new data storage format. This migration happens only once. The old store is retained and will still be used when using version 2.1 or older. New results will not be added to the old store though, and new results added to the old store will not be migrated. Cases made with 2.1.1 or later already use the new data store and are therefore not affected.

When items in cases made with 2.1.x are exported to a separate case, the registered case size of the target case will be incremented with the size of the original case. This may be problematic for users with licenses that have a case size limitation. To resolve the inflated case size, the source case needs to be re-indexed before exporting items from it.

Intella 2.2.1 can open cases made with Intella 1.9.x and 2.0.x, but these cases first require conversion before they can be opened. Case conversion will create a copy of the case in which all item data is converted, and all tags, comments and flags are imported. The existing case will not be altered in any way and can afterwards still be opened in the older Intella version. Access to the original evidence files is not required for case conversion.

Case conversion will not transfer the geolocation metadata extracted from emails when the "Determine geographic location of emails" option was used. Re-indexing of the converted case is required to restore such metadata.

Case conversion will require sufficient disk space. As a rule of thumb, please reserve twice the amount of the evidence size for your case folder.

Cases made with Intella 1.8.x or older are not supported.

Cases made with beta versions are not supported and should be recreated.