Intella Connect 2.2.1 Release Notes

Highlights

- **Case templates** enable quick initialization of a new case.
- Items can now be **exported to a new case** or **copied to another case**.
- Added a **key store** for password and other credentials, to be used when indexing encrypted evidence items.
- Added a **Geolocation** view, showing the geographic locations of search results, e.g. based on GPS data and IP addresses.
- 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**.
- Several **facets load faster**.
- Added a **Show Family** search option.
- Many **indexing** and **OCR** improvements.

Installer

- On supported systems, the entered user credentials are verified when installing Intella Connect or Intella Node as a Windows service.

Licensing

- The requirement to have at least 100 days of remaining Maintenance Agreement coverage has been reduced to 60 days.

General

- Various LDAP-related improvements, increasing general robustness and making connection reuse and pooling configurable.
- 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.
- The About screen now shows the source code revision number.
- The Cases item in the systray's right-click menu has been renamed to "Admin Dashboard".
- Resolved an issue where clicking the Cases item in the systray icon's menu produced an error due to the use of SSL with a multi-subdomain certificate.

Case Management

- The settings of a case can now be stored in a case template. Such a template can be used to easily initialize the settings of a new case, e.g. to comply with organization policies or to optimize it for the nature of the investigation. Case templates can for example cover:
    - Settings in the Preferences window.
    - The default table column setup.
    - Saved Searches.
    - Task definitions.

    - Tags.
    - Keyword and MD5 hash lists.
    - Export templates.
    - Redaction profiles.
    - Coding layouts.
- One can now export items to a case. This can either be an existing case or a new case. Several configuration options are available for controlling what item information is included, e.g. tags, comments, custodians, OCR text, etc. Parents of exported items that are not in the export set themselves are represented as stubs in the destination case.
  The new export functionality supports several use cases:
    - Merging of two or more cases, so that indexing can be spread across multiple machines.
    - Adding data to an ongoing case while minimizing downtime. The new evidence is indexed in a separate case first, rather than by adding a source to the current case.
    - Exporting of selected items to a new case, e.g. to filter out privileged information or irrelevant items, or to divide the work among reviewers in such a way that each reviewer only has access to their own assigned items.
- The name and description of a case can now be changed.
- Various usability improvements in this part of the user interface.
- Resolved several issues where a shared case would not show properly in its tab when it was restored from standby state after not being used for a while. The user would keep seeing the "The case is being prepared" message indefinitely.
- Resolved an issue with case conversion not functioning when Intella Node was running on an Intella TEAM Manager or Intella Professional license.

Indexing – General

- A key store has been added for entering and managing passwords and other credentials. These credentials are used to decrypt any encrypted items encountered during indexing. Supported credentials are:
    - Passwords
    - IBM Notes ID files
    - X.509 certificates
    - PGP keys
- 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 downloaded files, 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

- Imported OCR packages can now be larger than 2 GB.
- 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

- Added a Show Family search option. This new operation effectively combines the Show Parents and Show Children operations into a one-click operation, by determining for the selected item(s) the top-level parents and all their nested items. This also relates to the Family Date field.
- Performance improvements in loading the Email Address, Chat Account and Phone Number facets. In one test, loading and displaying a 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.
- Added an Item Stubs category to the Features facet. Item stubs are inserted when items are exported to a new case, to represent parent items that are not in the export set.

Results

- A Geolocation results view has been added, showing the geolocation of items on a zoomable world map. Items are grouped in clusters that break down into smaller clusters when zooming in. Map tiles for the first few zoom levels are bundled with Intella Connect. For deeper zoom levels a connection with a tile server is required. Each cluster of items can be clicked, which lists the items in the Details view beneath the map. Geolocation data is obtained from:

    - Geographic coordinates stored in the EXIF data of digital camera photos.
    - Geographic coordinates stored in items extracted from cellphones.
    - Email sender locations, using a geolocation lookup of the sender's IP address.
- 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.

Previewer

- A geolocation tab has been added, showing the geolocation of the current item, if any. See above for a description of the information that this is based on.
- 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.
- Improvements to the native rendering of various document types.
- The "Redact" button has been removed. Instead, the Redaction tab is now always present.
- The "OCRed" tab has been renamed to "OCR".
- Various usability improvements.
- Resolved an error that occurred when previewing EMLX items.
- Resolved an issue with hit highlighting not clearing when switching to a different item.
- Resolved several issues with the rendering of email items that have many recipients.

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 Connect 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.
- Added a background task 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 background task 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.
- Various usability fixes.

Exporting – CSV

- Resolved an issue with the export to CSV not exporting Raw Data fields correctly.

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 Connect 2.2.1 can directly open cases made the 2.2 and 2.1.x versions of Intella and Intella Connect.

When a case made with Intella or Intella Connect 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 a 2.1.x version 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.

Cases made with the 1.9.x and 2.0.x versions of Intella and Intella Connect can be opened, but these cases first require conversion. 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.

Caveats concerning the case contents:

- 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.

- Multi-page TIFFs will be displayed in the converted case as if they were single-page TIFFs. Exporting and printing of the item report does reveal the other pages. Re-indexing of the converted case will make all pages displayable again.

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.