

Intella 2.4.1 Release Notes

Released: **February 1, 2021**

Highlights

- Added a top-level **Sources tab**, adding the ability to (re)index individual sources.
- Added support for **Microsoft Teams**.
- Notable improvements for processing **BitLocker images and NSF files**.
- Indexing and case merging/exporting **performance improvements**.

Sources

- Added a new top-level Sources tab. The new tab allows certain operations to be performed on specific sources, whereas previously this could only be done on the case in its entirety:
 - The ability to index specific sources.
 - The ability to re-index specific sources.
 - The ability to scan specific sources for new evidence files.
- Other notable elements in the new Sources tab:
 - Buttons for adding and removing sources, as well as creating an Exceptions Report.
 - Sources with critical issues, such as missing evidence files or major indexing errors, are emphasized.
 - Details panel now shows dates when source has been added, last indexed, as well as a result of the last crawling status.
- The Sources menu and the Source Editor dialog have been removed, as their functionalities are now handled by the new Sources tab.
- Resolved a performance issue when initializing the file browser in the Specify File Or Folder sheet of the New Source wizard.
- The branches in the "File type settings" tree are now sorted alphabetically where appropriate.

Indexing - General

- Added several optimizations to the post-processing phases of the indexing operation. These relate to the steps taken immediately after crawling of the evidence files, when

several databases are constructed from the crawl results. The optimizations improve the time needed for indexing evidence files. The optimizations also benefit case merging/exporting, as that operation predominately consists of the tasks performed in these phases.

- Added support for indexing Microsoft Teams data, in particular (but not limited to) chat messages. Teams data from PST files and Office 365 sources are both supported.
- Several improvements for the processing of BitLocker disk images:
 - Added support for BitLocker volumes with clear keys. These are keys stored in unencrypted and unprotected form in the BitLocker volume.
 - Added support for BitLocker volumes with multiple recovery keys. Earlier, only the first encountered recovery key was used to validate and index the disk.
 - Improved error reporting when the disk cannot be decrypted.
 - Resolved an issue with disk images of non-encrypted drives incorrectly being classified as an encrypted BitLocker disk.
- Several improvements for the processing of Notes NSF files:
 - Added support for HCL Notes 11.
 - Added support for decrypting individually encrypted emails in a non-encrypted NSF file.
 - Indexing stability improvements. Access to the NSF file through Notes now takes place in a dedicated process. This way, any Notes crashes can now be recovered from more reliably and cannot result in case corruptions anymore.



Phone Enquiries
+1 (888) 291-7201

Postal Address
10643 N Frank Lloyd Wright Blvd, Suite
101, Scottsdale, AZ 85259 U.S.A.

Email sales@vound-software.com

Sales Contacts
www.vound-software.com/partners

- Resolved an issue with files in a folder being skipped when that folder also contains a Sametime dump.
- All references to “IBM Notes” in the user interface and documentation have been renamed to “HCL/IBM Notes”, to reflect the new owner of this product.
- Added recovery of deleted mails from MS Outlook 2013 OST files.
- Added file type detection for AppleSingle and AppleDouble files.
- Added support for loose instant messages and DeviceConnectivity items in Cellebrite dumps.
- Added an “Advanced Indexing” tab to the Preferences window. This tab allows the user to specify the sections in a Cellebrite extraction dump that the user wants to skip indexing. Future versions will add other advanced indexing options that are currently only available through (generally undocumented) commandline options.
- Several extraction improvements as a result from software library upgrades.
- Resolved a stability issue when indexing E01 disk images made with the Tableau TD3 Forensic Imager.
- Stability improvements for indexing APFS disk images contained in AFF4 containers.
- Resolved a memory usage issue introduced in the 2.4 release when indexing exceptionally large text files (e.g., log files in the hundreds of MBs).
- Resolved a concurrency issue with the processing of prefetch (.pf) files.
- Resolved a stability issue where data integrity issues within certain parts of a Slack archive caused other items to be omitted as well.
- Resolved an issue with truncated text errors being shown as source level errors rather than item level errors.

Indexing – Cloud Sources

- Updated the Dropbox source so that it works with the new “Scoped access” API. Note that Dropbox is retiring the old Dropbox API and Dropbox Business API. It is no longer possible to define new apps on Dropbox with these APIs. The online documentation in the Vound knowledge base has been updated accordingly.
- Several stability and usability improvements for indexing iCloud accounts.

Near-Duplicates

- Optimized the time needed to open a case containing near-duplicate detection results.
- Optimized the loading speed of the Near-Duplicates facet in remote cases.
- Documents consisting only of paragraphs marked as excluded are now skipped during near-duplicate detection. Earlier, they were all placed into the same near-duplicate group.

- The algorithm used in the Previewer’s Near-Duplicate tab for highlighting the differences between the current item and its master item has been made case-insensitive.

Searching

- Resolved a stability issue when evaluating Show Conversation queries.

Results

- Added a Table column and item property for the chat protocol of a message or conversation item. E.g. Skype, Slack, SMS, iMessage, ... The case needs to be (re)indexed with the 2.4.1 version for these values to appear.

Previewer

- Resolved an issue with the Contents, Headers and Raw Data tabs showing their content in a skewed manner when Windows display scaling was set to an uneven number, for example 125% or 175%.
- Resolved an issue with the Previewer not rendering properly when displaying certain types of emails with embedded images.
- Resolved an issue with certain Content Analysis entities failing to be highlighted in the Contents tab.

Tagging

- Added safe-guards to prevent reviewers from creating circular parent-child references in the tag model. These could lead to system instability.
- Resolved an issue with certain child tags disappearing in the Tags facet until the case was restarted, which would occur when a tag was given a different parent tag.

Redaction

- Resolved an issue with redactions being multiplied when the case is under heavy load.

Insight

- Resolved an issue with titles and subtitles of Insight panels failing to render Japanese values.
- The Insight tab now shows the link rather than the case folder of a remote case.

Exporting – PST

- Stability improvements for MS Outlook validation.

Exporting – Load Files

- Resolved an issue with certain load file configurations resulting in the Subject being rendered twice and the Attachments line being omitted.



Phone Enquiries
+1 (888) 291-7201

Postal Address
10643 N Frank Lloyd Wright Blvd, Suite
101, Scottsdale, AZ 85259 U.S.A.

Email sales@vound-software.com
Sales Contacts
www.vound-software.com/partners

www.vound-software.com



Upgrade Notes

Case versions 2.1.x to 2.4.x – Intella 2.4.1 can directly open cases made with Intella 2.4, 2.3.x, 2.2.x and 2.1.x.

Due to changes in data storage, Intella 2.4 is not able to open cases made with Intella 2.4.1.

When a case made with Intella 2.3.0 or older is opened in Intella 2.4.1, adding Custom ID tasks to the case in version 2.4.1 may render the case unopenable in that older version. Changes have been made in the 2.3.1 release to prevent such forward compatibility issues in future releases.

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.

In Intella 2.2.2, a new method for calculating message hashes was introduced. While this change is transparent, please be aware that message hashes will change when re-indexing a case that has been made with an older Intella version.

Case versions 1.9.x to 2.0.x – Intella 2.4.1 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.

Other case versions – Cases made with Intella 1.8.x or older are not supported. Cases made with beta versions are not supported and should be recreated.

Software versions – Vound will provide technical support for one major past version. For this release that will mean the 2.3.x range of products. Vound will always recommend that users upgrade to the latest version.

TEAM case sharing – one can now share maximally two cases simultaneously on a single TEAM Manager license. Please see Intella Connect for a solution to share larger amounts of cases.



Phone Enquiries
+1 (888) 291-7201

Postal Address
10643 N Frank Lloyd Wright Blvd, Suite
101, Scottsdale, AZ 85259 U.S.A.

Email sales@vound-software.com
Sales Contacts
www.vound-software.com/partners

www.vound-software.com

Vound
AMERICA • ASIA • EUROPE