Vound

# Intella Investigator™ Release Notes

**Intella™**

***evidence made visible***

Vound
email investigation and eDiscovery software

Covering versions 2.6 to 2.7.2

# Contact

To learn more about Intella Investigator™, please contact us using the contact information below, or contact an Intella Channel Partner.

## Vound


### Office Phone
+1 888-291-7201

### Email
sales@vound-software.com

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


### Sales Contacts
http://www.vound-software.com/partners

We will be pleased to provide additional information concerning Intella and schedule a demonstration at your convenience.

To become an Intella reseller, please contact us!

For user and technical support please visit our website:
http://www.vound-software.com.

The information in these Release Notes is subject to change without notice. Every effort has been made to ensure that the information in this document is accurate. Vound is not responsible for printing or clerical errors.

VOUND PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED AND SHALL NOT BE LIABLE FOR TECHNICAL OR EDITORIAL ERRORS OR OMISSIONS CONTAINED HEREIN; NOR FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES RESULTING FROM THE FURNISHING, PERFORMANCE, OR USE OF THIS MATERIAL.

Other company and product names mentioned herein are trademarks of their respective companies. It is the responsibility of the user to comply with all applicable copyright laws.

Mention of third-party products is for informational purposes only and constitutes neither an endorsement nor a recommendation. Vound assumes no responsibility with regard to the performance or use of these products. Under the copyright laws, this document may not be copied, in whole or in part, without the written consent of Vound.

Your rights to the software are governed by the accompanying software license agreement. The Vound logo is a trademark of Vound. Use of the Vound logo for commercial purposes without the prior written consent of Vound may constitute trademark infringement and unfair competition in violation of federal and state laws.

# Contents

# Intella Investigator 2.7.2

## Highlights

- **Intella Assist** improvements: **prompt optimizations**, support for **IBM WatsonX**.
- Improved searching for **emojis** and **acronyms**.
- Added full disk image support to **IntellaCmd**.
- Added a function to **export all words** from a set of items.

## Case Management

- Resolved an issue with cases sometimes staying listed as active in the Diagnostics Report, despite no user activity or background tasks taking place in the case anymore.

## Authorization

- Resolved an issue with the protection layer against CSRF (Cross Site Request Forgery) attacks inadvertently logging out users.

## Indexing – General

- Resolved an issue with missing Raw Data properties in the XMP section of a PDF document.

## Indexing – Disk images

- When validating and indexing AFF4 disk images, sub-folders will no longer be scanned. Only the current folder will now be scanned for disk image parts. This improves the time needed to validate disk images when there is a deep folder structure present in the local file system holding the disk image files.
- Improved stability when indexing ISO and DMG disk images.

## Indexing – Email

- Resolved an issue where emails inside OLK15 files were not identified as Top-Level Parents.

## Indexing – Chat messages

- Resolved an issue with indexing the SubstrateHolds folder in a MS Teams PST file.
- Resolved an issue with messages from RSMF archives not indexing properly when multiple messages in the archive have the exact same timestamp.
- Improved the performance of indexing messages from a Slack export, when that export contains a large amount of edited or deleted messages.

## Indexing – Cloud sources

- Updates to the Gmail and Microsoft 365 sources, reflecting server-side changes made by these vendors.
- Improved indexing and rendering of tables in iCloud Notes items.
- Resolved an issue with the selection of Google services not working properly.

## Indexing – Load files

- Resolved an issue where switching to the "Image preview" tab during load file source creation resulted in the user being redirected to the Cases list.

## IntellaCmd

- Added support for indexing disk images. These could already be indexed as files in a Folder source, but now the full set of disk image source options is supported. For example, disk image validation, volume shadow copy options, file carving, etc. can now be controlled on the command-line.
- Resolved an issue with the -indexChatMessages (-icm) option not working properly.
- Resolved an issue with a password list not being imported into the keystore.
- Resolved an issue with the case's temp folder setting not being picked up.
- Resolved an issue with a case template's optimization folder setting not being picked up.

## Intella Assist

- Added support for models shared on the IBM WatsonX platform. Currently supported models are:
    - granite-13b-chat-v2
    - mixtral-8x7b-instruct-v01
    - llama-3-8b-instruct
    - llama-3-70b-instruct

    - llama-3-1-8b-instruct
    - llama-3-1-70b-instruct
- Prompts generated by Intella Assist in the Previewer will now only include and submit those item parts (text, headers and/or raw data) needed to answer the user's question. This reduces API costs due to less tokens being generated, and speeds up processing of the prompt. Furthermore, it reduces the chance of context limits to be reached, especially for smaller models.
- Added a (hidden) option to re-enable the Intella Assist facet when a model is used that is not part of OpenAI's family of gpt-4 models.

## Searching

- Added support for searching for emojis. Previously this was only possible via regular expression search. Now, emojis can be directly entered in the Search field too. For this type of search to work, re-indexing of existing cases made with 2.7.1 or older is required.
- Improved searching for acronyms, such as "U.S. Bank".
- Resolved an issue where Saved Searches involving Content Analysis facet categories produced no results. Existing Saved Searches for this type of query should be discarded and re-created; they cannot be automatically fixed.
- Improved the loading process of several facets after the case was awakened from Standby mode.
- Resolved an issue with the "OCR candidates" case task querying for JPEG files instead of PNG files, or vice versa, when only one of these options was selected.

## Results

- Resolved an issue with table sorting producing incorrect results when the table sort order is toggled repetitively and quickly.
- Resolved an issue where table cells showing email senders/recipients would only show the contact's name but not the email address.

## Previewer

- Improved HEIF image support.
- Resolved an issue where links to the previous and next conversation items in the Previewer could not be rendered for some items.
- Resolved an issue with previewing calendar items in compound cases.

## Exporting – PDF

- Improved rendering of the JPEG2000 (.jpx) image format.

- Resolved an issue with some emails with very wide inline pictures rendering incorrectly in the generated PDF.

## Exporting – PST

- Resolved a rare issue where exporting emails to a PST with the “Keep location structure” turned on would produce a "The folder with same name already exists" error.

## Exporting – Relativity

- Updates to the functionality for exporting to Relativity(One) instances, ensuring that it supports recent Relativity versions.
- Resolved a harmless “NotSerializableException” error when exporting to Relativity.

## Exporting – Words

- Added a background task for exporting all words used in a set of items to a text file, e.g. for use in a password cracking tool. For each word, the field name (corresponding with the options in the Search options panel) and document frequency are optionally listed.

## Retiring functionalities

**Intella Viewer** – In a future release, Intella Viewer’s ability to connect to a case shared by Intella Connect or Intella Investigator will be removed. Intella Connect and Intella Investigator will be able to deliver those functionalities entirely via the browser.

## Upgrade notes

Intella Investigator versions can be installed side-by-side. There is no requirement to uninstall old versions when installing an Intella Investigator version.

**Case versions 2.6.x and 2.7** – Intella Investigator 2.7.2 can open cases made with versions 2.6.x and 2.7.x. No case conversion is needed.

Due to a change in the underlying databases, results in the Image Categories and Detected Objects branches of the Image Analysis facet that were made with version 2.6 will not be visible when the case is opened with version 2.6.1 and later. This analysis will have to be repeated with a more recent version.

The 2.7.2 release resolves an issue for Saved Searches containing Content Analysis results. These searches would always yield no results. Existing Saved Searches containing Content Analysis queries should be discarded and re-created; they cannot be automatically fixed.

**Case versions 2.1.x to 2.5.x** – Intella Investigator 2.7.2 can open cases made with Intella 2.1.x to 2.5.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 original 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 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 2.0.x or older are not supported.

To open cases made with the 1.9.x and 2.0.x versions, please use Intella 2.5.1. This is the last version to support the 1.9.x and 2.0.x versions.

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

**Memory settings** – The 2.7 version changed how case memory settings are stored. Prior to version 2.7, these settings were stored in both the case.xml and case.prefs files, for historical reasons. This is now only stored in the case.prefs file. Consequently, if the 2.7(.x) version is used to alter the memory settings of a case made with an older version, the memory setting changes may not be picked up by older versions.

**Microsoft SharePoint** – Version 2.7.2 no longer supports local, on-premises SharePoint servers. Version 2.7 was the last version supporting this source type.

Cloud-based SharePoint instances are not affected by this change, as they can be retrieved using the M365 source type. Existing cases with local SharePoint sources can still be opened.

**Software versions** – Vound will provide technical support for one major past version. For this release that will mean the 2.6.x range of products. Vound always recommends that users upgrade to the latest version.

# Intella Investigator 2.7.1

## Highlights

- Intella Assist enhancements: support for **GPT-4o**, **OpenAI API-compatible models**, **local models** and **search suggestions**.
- Added support for **file carving**; recovering deleted items from unallocated space in disk images.
- Improvements to the handling of **privileged items**.
- Added support for acquiring data from **Google Meet**.
- Added support for indexing **MS Visio VSDX** files.
- Added functionality for **repairing broken cases**.

## General

- Major updates to the user interface libraries and frameworks, bringing a faster, more responsive and future-proof user interface.
- Tested that the applications work correctly and efficiently when using the IPv6 protocol.
- Improved the name of the Desktop shortcut to the check-service.bat executable, which is placed when installing the application as a Windows service. The old shortcut name could result in users expecting this shortcut to start the service.

## Licensing

- Introducing two new editions: Intella Investigator Medium and Intella Investigator Large. Investigator Medium allows up to 5 active cases with up to 10 concurrently active users. Investigator Large allows up to 10 active cases with up to 20 concurrently active users.

## Authentication

- Simplified the process of adding a standard Active Directory instance as an LDAP provider, where the user only needs to provide the user accounts location and a group membership.
- Performance improvements in the loading of user data from an LDAP server.

## Authorization

- Enhancements to the exporting and downloading of items that are subject to the "Cannot see items tagged with …" permission. A common use case of this permission is to suppress privileged items from a review. It may happen that a reviewer tries to export or download items that have child items that are hidden by this permission. For example, a user may attempt to download an email that contains a hidden attachment. When this occurs, the export or download is now blocked, as the native form of the parent item would reveal the restricted child item(s). The user gets to see a dialog explaining that the operation is blocked.
- Starting with this release, the default administrator account will now receive the "Can configure servers in Intella Grid" permission by default. This does not affect existing installations.

## Case Management

- Resolved an issue with the admin user not being able to remove cases in a very old case format.
- Resolved an "Error while loading activities" error message in a case details' Activity tab when there was no previous user activity.

## Intella Assist

- The GPT-4o ("omni") model is now the default OpenAI model.
- Added support for using any model that uses the OpenAI API. Besides alternative hosted LLMs, this also opens the door to using locally hosted LLMs.
- The Intella Assist facet has been extended with a Suggestions component, listing examples of searches that can be done with Intella Assist.

## Indexing – General

- Added support for indexing MS Visio VSDX files.
- Removed support for indexing local, on-prem SharePoint sources. Cloud-based SharePoint instances are not affected by this change, as they can be retrieved using the M365 source type.
- Added logging of the used indexing options.
- Resolved an issue with the "Enable unsupported version" option in Intella Node's IBM/HCL Notes settings still not allowing for an unsupported version to be used.
- Resolved Intella Node failing to show an error when the geolocation database could not be validated.
- Resolved Intella Node failing to revalidate source and Node server settings when re-indexing a case.

- Resolved an issue with users not being able to use an entire drive as an evidence path in a source.
- Improved indexing performance when processing emails and chat conversations with very large numbers of recipients.

## Indexing – Disk images

- Added support for file carving: the process of recovering deleted items from the unallocated space in a disk image. This requires the PhotoRec utility, which can be downloaded automatically. Currently, E01 and DD images are supported. Carving runs in parallel with regular indexing, to optimize speed. File carving requires the use of the Disk Image source; disk images that are indexed as part of a "File or Folder" source will not be carved.
- Improved checksum validation of AFF4 images. For AFF4 physical images, checksum validation is an optional step during disk image validation when using the Disk Image source type. For AFF4-L logical images, failed checksums are reported as exceptions in the Features facet and in the Exceptions report.
- Resolved an issue with disk images containing NTFS file systems that were decrypted by AXIOM. Incorrect NTFS data structures would cause some folders to be regarded as corrupted and subsequently skipped.
- Resolved an issue with incorrect (garbled) partition names on ext4 and FAT16 file systems.

## Indexing – Cellphones

- Resolved an issue where chat messages with identical content could mistakenly be responsive to certain keyword queries.
- Resolved an issue with interrupted crawl processes when indexing very large (> 100 GB) UFDR files.
- Improved memory usage when indexing Cellebrite reports with a large number of chat messages.

## Indexing – Cloud sources

- Extended the Google source with support for Google Meet.
- Improved indexing and rendering of tables in iCloud Notes items.
- Resolved an issue with Find my Phone artifacts in iCloud sources.

## IntellaCmd

- Added an option to rebuild the indices in a case. This operation regenerates the secondary indices that are derived from the data gathered during crawling. This

can be used to repair cases that fail to open or that show other forms of erratic behavior, especially in cases where no backup is available. As a precaution, users are still advised to run this operation on a copy of the broken case.

## Log Viewer

- Various minor usability improvements.

## Results

- Resolved an issue with the Mime Type column not rendering the item MIME types properly.
- Improved handling of items with alternative, less commonly used MIME types.

## Previewer

- Resolved an issue with the Previewer not showing an item when that item has no MIME type associated with it.

## Tagging

- Commas in tag names are no longer allowed, unless when properly escaped. This prevents issues in other subsystems that process tag data.

## OCR

- The default time-out of OCR workers of the embedded OCR engine has been changed from 30 minutes to 2 hours. The previous time-out value caused too many documents to fail unnecessarily.
- Added a cap on the number of OCR workers for stability reasons.

## Exporting – PDF

- Resolved an issue with certain calendar items failing to export.
- Resolved an issue with annotations such as comments in a PDF getting lost when exporting the item to a PDF.
- Resolved an issue with incorrect positioning of headers and footers in landscape-oriented PDF documents.
- Resolved an issue where Intella did not add a numbered suffix to a file name (e.g., “document(1).pdf”) when exporting multiple items with the same file name or subject to PDF.
- Resolved an issue with certain characters not rendering properly in the generated PDF, whereas they would render fine in the Previewer.

## Exporting – Load files

- The PDF-related improvements listed above also apply to the exporting of load files using the PDF or TIFF file formats.
- Resolved an issue where the "Also include PDF versions of images" setting was ignored when exporting to a load file. The default “Images” folder was used instead.

## Retiring functionalities

**Intella Viewer** – In a future release, Intella Viewer’s ability to connect to a case shared by Intella Connect or Intella Investigator will be removed. Intella Connect and Intella Investigator will be able to deliver those functionalities entirely via the browser.

## Upgrade notes

Intella Investigator versions can be installed side-by-side. There is no requirement to uninstall old versions when installing an Intella Investigator version.

**Case versions 2.6.x and 2.7** – Intella Investigator 2.7.1 can open cases made with versions 2.6.x and 2.7. No case conversion is needed.

Due to a change in the underlying databases, results in the Image Categories and Detected Objects branches of the Image Analysis facet that were made with version 2.6 will not be visible when the case is opened with version 2.6.1 and later. This analysis will have to be repeated with the more recent version used.

**Case versions 2.1.x to 2.5.x** – Intella Investigator 2.7.1 can open cases made with Intella 2.1.x to 2.5.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 original 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 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 2.0.x or older are not supported.

To open cases made with the 1.9.x and 2.0.x versions, please use Intella 2.5.1. This is the last version to support the 1.9.x and 2.0.x versions.

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

**Memory settings** – The 2.7 version changes how case memory settings are stored. Prior to version 2.7, these settings were stored in both the case.xml and case.prefs files, for historical reasons. This is now only stored in the case.prefs file. Consequently, if the 2.7(.1) version is used to alter the memory settings of a case made with an older version, the memory setting changes may not be picked up by older versions.

**Microsoft SharePoint** – Version 2.7.1 no longer supports local, on-premises SharePoint servers. Version 2.7 was the last version supporting this source type.

Cloud-based SharePoint instances are not affected by this change, as they can be retrieved using the M365 source type. Existing cases with local SharePoint sources can still be opened.

**Software versions** – Vound will provide technical support for one major past version. For this release that will mean the 2.6.x range of products. Vound always recommends that users upgrade to the latest version.

# Intella Investigator 2.7

## Highlights

- Added **Intella Assist**, an AI-powered assistant based on OpenAI's ChatGPT that helps with formulating search queries and reviewing results.
- Redesigned **Source** and **Export** wizards.
- Added an **integrated log viewer**.
- **Identity improvements**, such as mass importing and exporting of identity data.
- Added the ability to directly export items to an on-premises **Relativity** or **RelativityOne** instance.
- Added exporting to the **AFF4-L logical image** format.
- A variety of indexing improvements related to **chat messages**, e.g. support for **Google Chat**.
- Added support for **EDRM MIH hashes**.
- Added **source filters**, letting one filter items based on file name or size.
- **2 to 5 times faster exporting** to PDF and load file formats.

## Intella Assist

- An AI-powered assistant called Intella Assist has been added. Based on ChatGPT, this assistant lets the user enter and refine queries using natural language, across a range of facets. Examples of searches:
    - "Give me all JPEG images larger than 1 MB"
    - "Search for invoices, using both English and Spanish words related to invoicing"
    - "Find all emails sent by john.doe@gmail.com between January 15, 2019 and September 1, 2019"
- Intella Assist is also integrated in the Previewer, where users can inspect and analyze items using natural language instructions. Examples of instructions:
    - "Summarize this document"
    - "Translate this document"
    - "Do the SMTP headers of this email show any signs of data tampering?"
    - "Who are the key persons named in this document?"
    - "What personally identifiable information does this document contain?"
    - "Where there any negative sentiments expressed in this conversation?"

- To use this functionality, the server admin needs to specify a provider and an API key for that provider. Currently supported providers are OpenAI and Azure OpenAI. Furthermore, reviewers need a role with the "Can use Intella Assist" permission.
- Admins should take note of several critically important caveats.
    - Using Intella Assist involves submitting parts of evidence data (text and metadata) to external services. The sensitivity and confidentiality of the data may make this undesirable or even illegal.
    - All prompts sent to ChatGPT are logged and available for auditing.
    - This functionality is experimental. The provided results may be incorrect and incomplete. Asking the same query again may not yield the same results.
    - Processing of the data by these services is subject to billing. All processing costs are for the owner of the API key.
    - End users will be shown warning dialogs expressing these risks. Nevertheless, they need to be educated in the proper handling of sensitive evidence data and the assessment of ChatGPT-generated results.
- Integration of this functionality in the Intella desktop application is planned for a future release. Contact Vound Support to be notified when an early access version becomes available.

## General

- The memory requirements for all server-based products have been adjusted.
- Resolved an issue with the main branding logo (the Connect logo or the organization-specified logo) linking to the case dashboard rather than the user dashboard.

## Installer

- When installing a product as a Windows service, an explicit dependency of the product's service on the Sentinel LDK License Manager service is now registered in Windows. This prevents the server application from launching before the license manager is running, which could cause licensing errors.
- Resolved an issue with the Node desktop shortcut not being added when using the Custom profile during installation.
- The Investigator installer now also places an IntellaNode.l4j.ini file when Intella Node is installed.
- Resolved blurry desktop and taskbar icons when using high-resolution screens and display scaling.

- Resolved an issue with applications not uninstalling when uninstalled from Windows' Programs and Features / Apps and Features settings panel.
- Removed the "(x64)" suffix from all new firewall rules.

## Licensing

- Resolved an issue where Intella Node would no longer fall back on an Intella Professional license.

## Security

- Added prevention against click-jacking attacks.

## Authentication

- Added automatic forced logouts of inactive sessions.
- When 2FA is made mandatory on the server level, a QR code would immediately be shown upon login if the user did not have 2FA set up. This QR code is now shown on demand, for security reasons.
- Resolved an issue with some accounts unable to login when a lockout policy is defined.

## Admin UI

- Added Investigator Grid functionality. This allows multiple Investigator servers to work together and offer a single point of entry to all users. This simplifies case management in larger organizations, as users do not need to be aware which Investigator server is hosting a case.
- An integrated log viewer has been added. This allows the admin to:
    - Get quick access to the logs from the Admin UI. Inspect and download them without needing file system-level access to the servers.
    - Search the logs.
    - Get educated about the existence and locations of the server, case and Node logs.
- Usability improvements to the Scan Logs functionality.
- The "Processing" permission group has been renamed to "Analysis".

## Case management

- The Add Source user interface has been redesigned from scratch.
    - Improved overview of the overall process, remaining steps, and separation between mandatory and optional parameters.

    - Better usage of the available screen space.
    - Many subtle UI improvements.
- Compound cases can now be converted in an automated manner. It no longer requires manual editing of configuration files.
- Resolved an issue with importing compound cases not importing their sub-cases. This resulted in errors when attempting to share the compound case.
- Resolved an issue with cases being considered “active” for too long and counting towards the active cases limit, while users had already stopped working on those cases.
- Editing of a case’s sources no longer requires the user to click “Finish source management”.
- Resolved an issue with cases not being sorted properly on the Last Shared Date.
- Resolved an issue with a case failing to be shared due to the use of a large list of sources, each with a very long MD5 hash list in them.
- When importing a case to the cases list, a check is done to see if a case with that ID (listed inside the case.xml file) already exists. When such a case is present, the user is asked whether the imported case should replace the existing case with the same ID, or whether it should be imported with a newly generated case ID.
- Improved the default memory settings for new cases on machines with 512 GB or more RAM.

## Indexing – General

- Added support for generating EDRM Message Identification Hashes (MIH). This is a cross-platform and cross-vendor message hashing standard, making email hashes comparable and exchangeable between forensic and eDiscovery applications.
- Added a source option to skip storing the binary data of items larger than a specific size. This helps reduce the case folder size and the indexing time. By default, items larger than 250 MB are not stored in the case folder anymore.
- Add a source option for skipping items based on their file name. This can be used to suppress files based on a known file extension or on another fragment in their file name.
- Put a limit on the length of the stored and indexed raw data. This increases performance and improves stability, by reducing the risk of memory errors. An example is chat conversations spanning a long time range, where the bundled metadata of all included chat messages can result in very large data streams. When indexing metadata fields, only the first 1 MB of text will be indexed. Only the first 5 MB of raw data will be stored. Warnings are added to the case logs when data is truncated. Items that exceed a limit are marked as Exception items with the type “Truncated”.

- Resolved an issue with the temporary folder failing to be cleared.
- Resolved an issue with Hangul HWPX documents showing an incorrect file name.
- Resolved an issue with incorrect creation dates extracted from an Adobe Photoshop PSD file.
- Stability improvements in the post-processing stage.
- Stability improvements when processing lots of small files over a network connection.
- Stability improvements when indexing damaged EDB files. This affects MS Exchange email databases, Windows Mail databases, and non-email EDB files.
- Harmless warnings stating "End of data reached" when processing PNG images and MP4 videos are now suppressed.
- Resolved an issue with incorrect crawler memory settings being reported in the case logs.

## Indexing – Disk images

- Resolved an issue with processing of VHDX images created by the Kroll Artifact Parser and Extractor (KAPE).
- Resolved an issue with missing folders when processing Apple DMG images.
- Resolved an issue with processing Japanese folder names in FAT32 images.
- Stability improvements when indexing Apple DMG images.

## Indexing – Email

- Improvements to the processing of PST containers:
    - The Conversation ID column is now populated for emails from PST containers.
    - Resolved an issue with missing emails due to incorrect MIME structures. These emails were not represented as an item, nor was anything logged.
- Improvements to the processing of Apple Mail containers:
    - Added support for recent Apple Mail versions.
    - Resolved several cases of missing attachments.
    - Stability improvements.
- Resolved an issue with the parsing of email headers with duplicate recipient headers, e.g. multiple CC headers, rather than a single header with a list of addresses.

## Indexing – Chat messages

- The Google source has been extended with support for Google Chat.
- Improvements to the processing of Cellebrite UFDR and UFED XML reports:

    - Resolved an issue with chat messages not being indexed.
    - Resolved an issue with a UFDR file being incorrectly classified and processed as a Slack data dump.
- Improvements to the processing of RSMF files:
    - Added full support for the RSMF 2.0 standard.
    - Performance improvements. Next to the speed improvement, this also significantly reduces the chance of time-outs on very large RSMF containers.
- Improvements to the processing of MS Teams PST files:
    - Resolved an issue with conversations not being split properly by month or year.
    - Resolved an issue with inconsistent participant information between conversations and reply threads nested within that conversation.
    - Resolved an issue with start and end dates being reversed for some messages.
    - Stability improvements.
- Improvements to the processing of Slack data exports:
    - Improvements to the processing of the original and edited message timestamps.
    - Improvements to the processing of Slack participant usernames.
    - Stability improvements.

## Indexing – Load files

- Improved the load file integrity check that is performed when the user clicks on "Check for Errors". Additional item type checks are being performed.

## Indexing – Cloud sources

- The Google source has been extended with support for Google Chat.
- When selecting an S3 bucket or Google Drive to acquire, one can now indicate which folder(s) need to be acquired.
- Resolved several authorization errors when accessing Google sources.
- Stability improvements for SharePoint acquisitions.
- Improved error logging when indexing Dropbox sources.

## Indexing – Crawler scripts

- Resolved an issue with crawler scripts failing to modify items that lack an MD5 hash.
- Resolved an issue with the Visited URL and Size fields not being accessible for crawler scripts.

## IntellaCmd

- Added support for the -keyID argument. This lets one specify the dongle or SL key to use.
- Added a -replaceSourcePaths argument. This lets one do a substring replace of all evidence paths of all sources in a case.
- Improved the lookup process for alternative licenses.
    - Intella Node licenses are now always preferred over Intella Professional licenses.
    - When the first applicable license already has all its seats consumed, it will switch to an alternative license with available seats, rather than giving up.
    - Removed a false but misleading "Product license not found" error message. This was a byproduct of IntellaCmd simply trying out several alternative licenses.
- Improved memory usage of the case conversion process.
- Resolved an issue with Notes ID files not validating properly.
- Resolved an issue with case creation, where the main process memory setting of the specified case template was ignored.
- Resolved an issue where the system's temporary files folder was used, rather than the folder specified in the case settings. Also added some stability improvements related to the use of the temporary files folder.
- Resolved an issue with the -exportSourcesList operator failing to produce results when invoked on cases holding Slack data dumps.

## Full-text search

- Improvements to the searching of email addresses containing underscore characters.
- Improvements to the searching of acronyms.

## Facets

- The Item ID Lists facet's import functionality has been extended to also support the importing of URI lists. This facilitates the exchange of item lists between one case and another case exported from that first case. The item IDs will differ between those cases, but the URIs are constant and can be relied upon to find those items in the other case.
- The Features > Exported category now also reflects items that were exported to a (portable) case.
- Resolved an issue with custodian information not appearing in a case converted from an earlier version. This affected the custodian information in the converted

compound case itself, not the custodian information found in its converted sub-cases.

## Identities

- Added importing of identities. Using a CSV file, identity data like names, organizations, email address and other communication aliases, etc. can be imported. This allows data on known identities to be utilized in a case.
- Added exporting of defined identities to a CSV file.
- The identity suggestions algorithm no longer suggests identities that have already been defined by the user.
- Identities chosen by the user from the suggestions list are now immediately removed from that list.

## Results

- UI improvements in the selection of multiple items.
- UI improvements in the rounding of values such as byte counts.
- Quality improvements in thumbnail generation.
- Resolved an issue with the Hide Non-inclusive button not hiding all non-inclusive items in a compound case.

## Previewer

- Made the old behavior of how email properties are rendered in the Contents and Previewer tabs available again, after user feedback. Both old and new behavior are available, controlled by a preference.
- The rotation data in an image's EXIF data, if present, is now applied to the rendering of the image. This ensures that the image is rendering with the intended rotation.
- Added support for rendering SVG images.
- Added a checkbox controlling whether videos should automatically start playback when opened in the Previewer.
- Usability improvements in the rendering of items with a lot of tags.
- Resolved an issue with email bodies in HTML format not rendering properly.
- Resolved an issue with certain email SMTP headers failing to render in the Headers tab.
- Resolved text alignment issues in the Contents tab.
- Improved error messaging when the native view of an item fails to be produced.
- Resolved an issue with the Download button not working on OCR-ed items.
- Resolved an issue with full-page redactions not working.

- Resolved an issue with the “Previous conversation” and “Next conversation” links not working on some chat conversations.
- Resolved an issue with the native preview of spreadsheets not occupying all available space.
- Resolved an issue with special characters in an item’s location being rendered incorrectly in the breadcrumbs bar at the top of the Previewer.
- Resolved an issue with incorrect positioning of hit marks in the scrollbar’s area.
- Resolved an issue with the scrollbar inside the Previewer not resetting properly when navigating from item to item.
- Resolved an issue with flagging inconsistencies between messages in conversations and the underlying, nested items, due to internal parsing errors.
- Resolved an issue with the Previewer failing to render chat message attachments in a converted case.
- Resolved an issue with Slack-internal links not being followed properly when clicked in the Previewer.

## Preferences

- Various usability improvements.

## Exporting – General

- The Export user interface has been redesigned from scratch.
    - Improved overview of the overall process, remaining steps, and separation between mandatory and optional parameters.
    - Better usage of the available screen space.
    - Many subtle UI improvements.
- Added exporting to the AFF4-L image format. This is a logical image format, similar to L01.
- Exporting errors are now reported to an Errors.csv file, separate from the regular export report that covers the successfully exported items. Optionally, this file can be converted to PDF, RTF and/or HTML, depending on the chosen main report format.
- Improvements to the suggested name of a new export set.
- Resolved an issue with inline attachments in Notes rich text emails being reported twice when exporting to EML or PST format.

## Exporting – PDF

- Speed improvements through the increased use of multi-threading. The improvement in total duration typically ranges between 2 to 5 times faster than the 2.6.1 version.
- The “For every email include” header in the PDF rendering options screen has been renamed to “For every communication include”. This has been done because it applies to all communication types, not only emails.

## Exporting – Load files

- The PDF-related improvements listed above also apply to the exporting to load files.
- Resolved an issue with comments being exported from one case to another through load file overlays. All comments would be squashed together, rather than kept as separate comments.
- Resolved a memory issue when using the “Export native chat content as PDF” option in the load file options.

## Exporting – PST

- Resolved an issue with emails exported to a PST file lacking a Conversation Index field. This caused issues when attempting to perform email threading when the PST file was ingested in the Logikull platform.
- Resolved an issue with the automatic skipping of very large emails, done for stability and reliability reasons. An issue with the determination of the size of the email caused some emails to be skipped inadvertently.
- Resolved an issue with tasks with inconsistent timestamps failing to export to a PST.
- Resolved an issue with certain types of export errors not being reported in the export report.

## Exporting – Relativity

- Added the ability to directly export to an on-premises Relativity or RelativityOne instance.

## Exporting – Case

- Compound cases now also support exporting items to a separate case.
- Case exporting now supports exporting Image Analysis, Email Threading and Near-Duplicates item data.

- Resolved an issue with exporting decrypted items to a separate case. Decrypted items that could be opened in their native format in the original case, would fail to open in the case that it was exported to.
- Resolved an issue with Skin Tone Analysis results not carrying over to the target case.

## Intella Viewer

- Resolved items failing to render when opened in a Previewer, in a remote case shared by Intella Connect or Intella Investigator. In one case this affected MS Teams chat messages. In another case this affected tagged items in a compound case.

## Retiring functionalities

**Intella Viewer** – In a future release, Intella Viewer's ability to connect to a case shared by Intella Connect or Intella Investigator will be removed. Intella Connect and Intella Investigator will be able to deliver those functionalities entirely via the browser.

**Microsoft SharePoint** – The 2.7 version will be the last version to support local, on-premises SharePoint instances. Cloud-based SharePoint instances are not affected by this change, as they can be retrieved using the M365 source type.

## Upgrade notes

Intella versions can be installed side-by-side. There is no requirement to uninstall old versions when installing an Intella version.

**Case version 2.6.x** – Intella 2.7 can open cases made with Intella 2.6.x. No case conversion is needed.

Due to a change in the underlying databases, results in the Image Categories and Detected Objects branches of the Image Analysis facet that were made with version 2.6 will not be visible when the case is opened with version 2.6.1 and later. This analysis will have to be repeated with the more recent version used.

**Case versions 2.1.x to 2.5.x** – Intella 2.7 can open cases made with Intella versions 2.1.x to 2.5.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 original 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 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 2.0.x or older are not supported.

To open cases made with the 1.9.x and 2.0.x versions, please use Intella 2.5.1. This is the last version to support the 1.9.x and 2.0.x versions.

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

**Memory settings** – The 2.7 version changes how case memory settings are stored. Prior to version 2.7, these settings were stored in both the case.xml and case.prefs files, for historical reasons. This is now only stored in the case.prefs file. Consequently, if the 2.7 version is used to alter the memory settings of a case made with an older version, the memory setting changes may not be picked up by older versions.

**Intella Node default port** – In version 2.6, the default port Intella Node runs on changed from 9999 to 10000. This was done to ensure that installing Node on the same server as Connect or Investigator will not result in port clashes. To change the port that Node runs on, one can specify the NodePort property. See the Administrator Manual for instructions.

**Software versions** – Vound will provide technical support for one major past version. For this release that will mean the 2.6.x range of products. Vound always recommends that users upgrade to the latest version.

# Intella Investigator 2.6.1

## Highlights

- Added support for acquiring and indexing **S3 buckets**.
- Added support for acquiring and indexing various **Google** services.
- Improved the presentation of **contacts, meetings, invites** and **phone calls**.
- Added an **Events view**, showing a timeline of events observed in the evidence data.
- Added a system for license add-ons, enabling larger amounts of active cases and reviewers.
- **Command-line support** has been extended with options for case conversion, custodians, type filters, various forms of exporting, and more.
- **Case conversion with IntellaCmd.exe no longer requires a license**, allowing the task of converting large amounts of cases to be spread across several machines.
- Added a **log management** page, for scanning and providing easy access to all logs on a server.
- **Authentication** enhancements for 2FA and SSO**.**

## General

- Added a log management page to the Admin environment. This functionality scans all logs present in a Connect/Investigator system: Investigator server logs, case logs and/or Node logs. The logs are checked against a list of common errors. Examples are errors related to file system permissions, disk space use, memory settings, etc. The user can download the logs from this page, removing the need to have file system-level access to various servers to obtain these logs.
- Windows Server 2022 is now listed as a supported OS.
- Resolved an issue with character encoding handling, which resulted in characters being displayed incorrectly.
- Resolved an issue with the temp folder setting sometimes not being used for certain tasks.
- Resolved an issue with file sizes being rounded incorrectly in several places.
- Various styling improvements.

## Security

- Resolved a cross-site scripting vulnerability in the Tags facet.

- Resolved a redirection vulnerability in the Login page.
- Several library updates triggered by vulnerability analysis.

## Licensing

- Added a modular licensing system for enabling more active cases and active reviewers on an Investigator server.

## Authentication

- Added the ability to enforce the use of 2FA upon all users.
- Added a validator and troubleshooter for SSO setups.

## Case management

- Suppressed a harmless error on case lock files when converting a case to the 2.6.x format.
- Resolved an error that occurred when importing certain case templates.
- Resolved several errors with case conversion failing to convert the geolocation database.

## Compound cases

- A compound case's Custodian facet now shows a unified list of all custodians present in its sub-cases.
- Compound cases can now be converted fully automatically. In the 2.6 version, several manual steps were required to convert the compound case and all its sub-cases.
- Several enhancements in command-line processing involving compound cases. See the "Command-line support" section for more information.
- Resolved an issue with saved searches containing tags not loading properly in a compound case.
- Resolved an issue with the duplicate counts and the results of the Show Duplicates operation being too high in compound cases, due to items not being deduplicated across sub-cases.

## Sources

- Resolved an issue where a source's type filter configuration defined in a Connect/Investigator source would show up inverted when viewed in the Intella desktop application.
- Added support for adding W4 cases made with W4 version 1.1.5.

- Resolved an issue with the “Analyze paragraphs” setting not allowing to be turned off.

## Indexing – General

- Resolved an issue with DestList entries in a jump list not being extracted properly.
- Resolved an issue with all sources being marked as having an error after re-indexing, when only a subset of sources failed to index.

## Indexing – Disk images

- The Select Folders sheet now shows volume labels when adding an APFS disk image. These were already extracted and shown in the Location facet; only the folder chooser was not showing them until now.
- Resolved an issue with missing volume labels when indexing ISO images.
- Resolved an issue with certain DMG images failing to process.
- Resolved an issue with certain APFS file systems failing to process.

## Indexing – Email

- Added detection of MS Outlook IRM-protected emails (.rpmsg files).
- Resolved stability issues when indexing EDB files.

## Indexing – Chat messages

- Resolved an issue with chat messages without a protocol that would fail to index.
- Resolved an issue with the chronological ordering of edited Slack messages.
- Resolved an issue with the Raw Data of certain chat messages lacking the full list of recipients.
- Resolved an issue with non-existing folders appearing in the Location facet when indexing a Slack Enterprise Grid export.

## Indexing – Cloud

- Added support for indexing Amazon AWS S3 buckets.
- Elevated the Gmail source to become a Google source. Currently supported Google (Workspace) services are Gmail, Drive, Calendar, Tasks and Contacts. Future versions will extend this to a broader set of Google services.
- Resolved an issue with iCloud sources producing cookie validation failures.
- The “Connect to iCloud” page now uses a masked password field, obscuring the entered password.

## Indexing – Crawler scripts

- Crawler scripts can now check whether an item passed to the script is a top-level item or a nested item. Examples of top-level items are the files in a file system folder and the emails in an Outlook PST file. Examples of nested items are images embedded in a document and files attached to an email. This family information allows for more fine-grained filtering of items, where the parent role is often crucial. For more information, see the GitHub page on crawler scripting: https://github.com/vound-software/intella-crawler-scripts.
- Resolved an issue when multiple sources with a crawler script were re-indexed. Re-indexing could give a fatal error when the second source was re-indexed.

## Command-line support

- IntellaCmd.exe is now also installed when installing Intella Investigator/Connect. Previously, this was only installed with Intella and Intella Node.
- IntellaCmd.exe will now revert to looking for a Connect or Investigator license, when a Node or Professional license cannot be found.
- Added support for case conversion to IntellaCmd. Previously this could only be done by Intella.exe or interactively.
- No license is needed to run IntellaCmd.exe for case conversion.
- Added support for creating a compound case.
- Added support for specifying a case template when creating a new case.
- Added the ability to set a crawling script in a source configuration.
- Added the ability to set the custodian when adding evidence items to a case.
- Added the ability to include or exclude a list of item types during indexing. Depending on the filtering mode used, all items with a MIME type on, or not on the list are skipped.
- Added the ability to install a hash list through a command-line call, and to specify its use as part of a source definition.
- Added the ability to add various forms of data in bulk: source paths, BitLocker recovery files, password lists, email certificates and Notes ID files.
- The "-importText" option can now also be used on a compound case.
- Added the ability to export items using an export template. This change allows all export types to be automated through command-line arguments.
- The events.log file, containing a record of all actions taken place in a case, can now be exported to a CSV file through command-line arguments.
- Added a "-listAllTimezones" argument, which list all timezones that can be used in Intella(Cmd).exe invocations.

- Added options for exporting the exception report and a separate “fatal errors” file. These reports reduce the chance of critical errors being overlooked.
- Resolved an issue with the “-exportSourceList” command not exporting all chat-related settings of a source.
- Resolved an issue with paths failing to work due to the presence of a backslash character at the end of a quoted string, which resulted in the backslash being interpreted as the start of a character escape sequence.

## Searching

- Improved the Image Analysis facet user interface and underlying database. Thresholds for image and object categories can now be altered directly inside the Image Analysis facet, instead of via the Preferences window. Changing the threshold immediately alters the facet counts, without requiring lengthy database updates.
- Resolved an issue with Boolean queries involving single term phrase queries with leading and trailing wildcards not producing adequate results.

## Results

- Added an Events view. This view shows the timestamps of results as a list of events sorted chronologically. Selecting an event will show the details of the item corresponding with that event in a preview panel.
- Resolved an issue with the Select All and Invert Selection buttons in the table’s right-click menu not working.
- Resolved an issue with the item counts in the facets and the Searches list not considering that certain items may be hidden due to the use of the “Cannot see items tagged with …” permission. While those items were not uncovered, the item counts shown in those places were incorrect.
- Resolved an issue with the table column widths being restored to their default widths when the table is updated.

## Analysis

- Image Analysis and Object Detection have been extended to support more image formats, e.g. iOS HEIC images. As a rule of thumb, when an image can be displayed in the application, it can now also be subjected to Image Analysis and Object Detection.
- The algorithm for suggesting Identities now ignores accounts named “admin” or “administrator”.

## Previewer

- Enhanced the presentation of items representing contacts, meetings, invites and phone calls. The Contents tab now shows the relevant properties of these items in an appropriately formatted list, making the information easier to review.
- Enhanced the rendering of images in the Previewer.
- Added a slider for the object detection threshold. This allows the user to control whether all detected objects are highlighted or only the highest scoring objects.
- Resolved an issue where hidden slides, speaker notes and comments of a PowerPoint file were not rendered, when viewed in the native rendering.

## Exporting – General

- Resolved an issue with export packages larger than 2 GB failing to download.

## Exporting – PDF

- The enhancements for rendering contacts, meetings, invites and phone calls listed in the Previewer section also apply to the PDF export of these items.
- Resolved an issue with some PDF items failing to export to PDF.
- Resolved an issue with some JPG images failing to export to PDF.
- Resolved an issue with chat messages and conversations failing to export when they include corrupt embedded images.
- Resolved an issue where hidden slides, speaker notes and comments of a PowerPoint were not rendered, when exported to native rendering.
- The “Prefer HTML over plain text” option for email exporting is now selected by default.

## Exporting – PST

- Resolved an issue with emails with LDAP-style addresses failing to export to PST.
- Resolved an issue with emails with tens of thousands of recipients failing to export.

## Exporting – Load file

- All PDF-related export changes apply to load files as well.

## Exporting – Report

- Resolved an issue with the Next button on the “Report – Title Page” sheet staying disabled.

## Export – Case

- Resolved an issue with tags that are not assigned to any items, but are present in the Tags facet, not being exported to the target case.

## Upgrade Notes

Intella Investigator versions can be installed side-by-side. There is no requirement to uninstall old versions when installing an Intella Investigator version.

**Case version 2.6** – Intella Investigator 2.6.1 can open cases made with the 2.6 version of Intella, Intella Connect and Intella Investigator. No case conversion is needed.

Due to a change in the underlying databases, results in the Image Categories and Detected Objects branches of the Image Analysis facet that were made with version 2.6 will not be visible when the case is opened with version 2.6.1. This analysis will have to be repeated with version 2.6.1.

**Case versions 2.1.x to 2.5.x** – Intella Investigator 2.6.1 can open cases made with versions 2.1.x to 2.5.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 original 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 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 version 2.0.x or older are not supported.

To open cases made with the 1.9.x and 2.0.x versions, please use version 2.5.1. This is the last version to support the 1.9.x and 2.0.x versions.

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 2.5.x range of products. Vound always recommends that users upgrade to the latest version.