FTK CENTRAL 7.6 – RELEASE NOTES

September 2022
Table of Contents

Overview ......................................................................................................................................................................... 3
1  New Features & Enhancements ........................................................................................................................................... 4
2  Resolved Issues ............................................................................................................................................................ 20
3  Known Issues ............................................................................................................................................................... 22
Contact Exterro ........................................................................................................................................................... 24
Overview

Exterro was founded with the simple vision that applying the concepts of process optimization and data science to how companies manage digital information and respond to litigation would drive more successful outcomes at a lower cost. We remain committed to this vision today. We deliver a fully integrated Legal GRC platform that enables our clients to address their privacy, regulatory, compliance, digital forensics, and litigation risks more effectively and at lower costs. We provide software solutions that help some of the world’s largest organizations, law enforcement and government agencies work smarter, more efficiently, and support the Rule of Law.
1 New Features & Enhancements

- FTK Central now supports automated workflows with FTK Connect.

  - Automated workflows have been introduced within FTK Central. FTK Connect (licensed add-on) allows users to automate key functionality within FTK while allowing users to set an automatic workflow stop (on error):
    - **Case Creation** - Create cases automatically when utilizing the Watch Folder trigger.
    - **Evidence Processing** - Automatically process evidence such as forensic images and loose files when a user has uploaded them to a given directory, while utilizing default and custom processing profiles.
    - **Agent Collections** - Run filtered/full-disk/memory acquisitions using pre-created collection templates.
    - **Exporting** - Filter files for export by utilizing custom filters, search and tag, tags, extensions, natives & AD1 images, load files and portable cases.
    - **Search and Tagging** - Utilizing keyword lists, users can automate the labelling of files and folders.
2 FTK Central now supports live previewing and collection of off-network agents. (*ER-4168*)

- Live Preview allows users to view data on an agent before committing to a collection job. Users have the freedom to navigate across system directories and select multiple files/folders for collection even if they are located on off-network agents; furthermore, adding the capability of logical acquisitions using the Live Preview interface.

- Windows Agents can now have indexing enabled. This option can be toggled within the Live Preview page. (*ER-4131*)
3 FTK Central now supports processing of Mobile Evidence.

- FTK now supports processing of native extractions (logical, physical or file system images) from mobile devices from tools such as GrayKey, Cellebrite, XRY and Oxygen.
  - Exterro is now a Grayshift Technology Alliances Partner; allowing FTK to accurately import and parse iOS and Android extractions created by GrayKey.

<table>
<thead>
<tr>
<th>Operating System</th>
<th>File Type Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>Android 7.0 – 12.0</td>
<td>Physical Images, Full File System Images, Android Backups</td>
</tr>
<tr>
<td></td>
<td>(ADB – Unencrypted/Encrypted), UFD/UFDx.</td>
</tr>
<tr>
<td>iOS 12 – 14 (Partial support for iOS 15)</td>
<td>Full File System Images</td>
</tr>
</tbody>
</table>

- Supported Chat Application Parsing:
  - Android Messages (Android)  
  - Discord (iOS)  
  - Facebook Messenger (Android, iOS)  
  - Google Chat (Android, iOS)  
  - [Formerly known as Google Hangouts]  
  - IMOPlus (Android)  
  - Instagram (Android, iOS)  
  - Slack (Android, iOS)  
  - Snapchat (Android, iOS)  
  - Telegram (Android, iOS)  
  - Threema (Android, iOS)  
  - WhatsApp (Android, iOS)  
  - iOS Messages (iOS)  
  - KakaoTalk (Android)  
  - Kik (Android, iOS)  
  - Line (Android, iOS)  
  - Signal (Android, iOS)  
  - Skype (Android, iOS)  
  - Tinder (Android)  
  - Twitter (Android, iOS)  
  - Viber (Android, iOS)  
  - WeChat (Android)
FTK Central now supports PostgreSQL, multiple MSSQL database instances and MSSQL AlwaysOn:

- **FTK Central now supports PostgreSQL databases.** *(ER-4110)*
  PostgreSQL support has been added to FTK Central. Users are no longer limited to using MSSQL databases with FTK Central. FTK Central supports PostgreSQL out of the box with no limitation to functionality.

- **FTK Central now supports PostgreSQL databases hosted in Linux environments.**
  PostgreSQL instances can now be run on Linux environments. Support is only available for environments running FTK Suite 7.6 and above.

- **FTK Central now supports multiple MSSQL database instances.** *(ER-4168)*
  Cases can be distributed (round-robin – even distribution) to multiple MSSQL database instances. FTK Central requires one master database to store application dependent databases, tables and stored procedures while utilizing multiple databases for case data. Users have the ability to deactivate databases when they require it.

  *Note:* Refer to the [Multi-Database Setup](#) article.

- **FTK Central now supports AlwaysOn MSSQL database instances.** *(FTKC-8838)*
  Environments utilizing a MSSQL database (including multiple case databases), now support AlwaysOn configurations. Users can utilize this feature to allow high availability and disaster recovery.

  *Note:* Refer to the [MSSQL AlwaysOn Configuration](#) article.
5 FTK Agents have been enhanced:

- **Windows Agent installations now have additional parameters for firewall rules.** *(ER-7222)*
  
  Additional MSIEXEC parameters have been added to allow customization of the name of the firewall rule required; or remove the firewall rule entirely. These parameters are optional.

  *Note: Refer to the* Installing the Windows Enterprise Agent *article.*

- **The name of collection jobs are the names assigned as the evidence within a case.** *(FTKC-3065)*

  FTK Central allows users to create collections and automatically name the collected evidence using the provided collection name.

- **Site Server Log Accessibility (ER-6676)**

  Site Server logs can now be configured to automatically be stored in a specific location. The log file itself will only contain information related to a specific job and not all existing jobs.

  *Note: Refer to the* Site Server Log Accessibility *article.*
6  FTK Central now supports integration with Palo Alto: Cortex XSOAR for playbook functionality. *(ER-3804)*

- Users can now integrate FTK Central with Cortex XSOAR, a security orchestration automation and response (SOAR) platform to create automated workflows. With this new integration capability, users can build an automated workflow for adding evidence from endpoints, processing evidence and using filters to export native files. This integration allows seamless workflow creation with FTK Connect.

7  FTK Central Authentication methods have been enhanced:

- **Federated Identity: SAML Authentication *(FTKC-7962):***
  
  FTK Central now allows users to utilize SAML providers for user authentication. Users can configure SAML to redirect users away from the default login screen which is shown for local/active directory authentication methods, to the SAML login form. SAML 2.0 compatible IDP’s are supported.

  *Note: Refer to the SAML Configuration guide.*

- **Dual-Authentication *(FTKC-7962):***
  
  Environments utilizing Active Directory/SAML user authentication allows users to access the application using local user credentials. This is limited to FTK Central only.
FTK Central Connectors have been enhanced:

- **Microsoft GCC High Collections (ER-3981):**
  Organizations within the Defense Industrial Base, DoD contracts and Federal agencies can now collect from Microsoft GCC High cloud environments.

- **Microsoft Graph API Filters (ER-7021):**
  Users can now collect data from Recoverable Deletes, Purges, Versions and Archive MailBoxes when collecting from Microsoft Graph API data sources.

FTK Central Exporting has been enhanced:

- **General UI Updates (FTKC-12004) (FTKC-5341):**
The export wizard now allows:
  - View, copy and delete previous exports/production sets.
  - Create new exports based on previous export parameters.
  - Export parameters can be saved as a template for use in automated workflows within FTK Connect.
  - Greater control over file names with the ability to select any case field as the exported object’s name.

*Note: The ability to copy from a previous export does not support exports/productions created in previous versions of FTK Central.*
10 FTK Central Processing/Evidence Options have been enhanced:

- **Managing Custom Carvers (FTKC-12553):**
  Users can now manage custom carvers within the Processing Options UI.

![Carving Options](image)

- **Updated Expansion Options (FTKC-12997):**
  The expansion options available previously have been refined. Obsolete options have been removed and mobile options have been consolidated within the new Exterro Mobile Parser.

- **Index Refinement Options (FTKC-5921):**
  Users now have the ability to select index refinement Inclusion/Exclusion options based on the Status/Type and/or Date/Size of files.
• **Upload Multiple Graphics to an associated Evidence File. *(FTKC-12997):**
Users can now upload multiple graphics in relation to an evidence file being ingested. This option is available during and after any evidence is added to a case.

• **Custom Case Properties *(FTKC-7231):**
Administrators can create 'Custom Case Properties' which can be utilised to select specific property tags during case creation. Users can select a text field or create a custom picklist.
• **Managing Custom Processing Profiles (FTKC-6951):**

FTK Central now allows users to create and delete processing profiles. If any changes have been made to an existing profile during creation of a custom processing profile, these options can be discarded.

![Save Processing Profile dialog](image)

• **Load File Ingestion: Create new fields (FTKC-1713):**

During and post case creation users are now able to create custom fields when ingesting load files. Users are no longer limited to using custom fields created prior to ingestion of load files.
11  FTK Central Searching has been enhanced:

- **Cancelling Search Jobs (FTKC-8131):**
  
  When a search job has been initiated, users can cancel ongoing search jobs on demand.

- **DocID Range Searching (FTKC-6792):**
  
  The following operators can be used in quick search or in the text search box to retrieve files within a DocID range:
  
  - GE (Greater than or Equal to)
  - LE (Less than or Equal to)
  - BETWEEN
  - GT (Greater Than)
  - LT (Less Than)

- **File List Column Visibility (FTKC-4829):**
  
  Users can now select specific columns to be displayed for an advanced search. The selected fields will be displayed once a search job has completed.
12 FTK Central Review/Viewer have been enhanced:

- **FTK Plus Viewer Integration (**FTKC-14022**):**
  FTK Central has been enhanced with a new Desktop Viewer. This will alleviate any issues when viewing videos not supported by HTML5. There will be no reliance on converting the video format prior to viewing them. When the Desktop Viewer is selected, users will be prompted to open the viewer in a new window. If the viewer has not been previously installed, then users will be prompted to install the required dependencies.
• **CAID/VIC: Pixelization of Graded Images (FTKC-12134):**

When images have been categorized by reviewers, users can toggle if these images should be obfuscated from both the thumbnail view and the primary viewer.

![Image of pixelization](image.png)

• **Videos: File Size Validation (FTKC-7547):**

When viewing video files within the viewer, users are no longer limited to a configured file size limit.

• **Metadata/Family/Email Conversation/Duplicates Tab (FTKC-12184):**
  - The Metadata tab has now been relocated within the viewer itself, users can toggle to view metadata related to the file selected.
  - The Family/Email Conversation/Duplicates tab have been added to the shortcuts bar and will appear collapsed by default. Users can toggle to view these tabs in a maximized popup view.
13  FTK Central Detailed Reports have been enhanced: *(FTKC-12184)*:

- **Configuring Columns:**
  Detailed reports now allow users to configure columns to be displayed within a report. Users can edit existing column sets as well as create templates for future use.

- **Embedding Objects:**
  Detailed reports now allow users to embed tagged objects within them. Users have full control of which file types should be embedded during report creation. Depending on the file type, users will see a full-size preview or a thumbnail.
FTK Central Filtering has been enhanced:

- **Inclusion/Exclusion Filtering (FTKC-4606):**
  Users can now utilize Inclusion/Exclusion filters within the filters panel. Clicking on a filter once will actively filter the file list, clicking twice will exclude the selected filter from the file list.

- **Configuring Default Quick Filters during Case Creation (FTKC-8703):**
  Quick filters can now be selected during case creation. These filters will be applied on a case level. Additionally, the ProductType configuration will dictate whether or not these quick filters are selected by default during case creation but will not limit users from toggling these quick filters during case creation.

  *Note: Refer to the Product Type article.*

- **Column Filtering Visibility (FTKC-10974):**
  When a filter is applied to a column within review it will now be displayed as an active filter chip. Users can remove these filters by clicking on these filter chips.
15 Other Enhancements:

- **Supported Artifacts**
  You can refer to the [Supported Artifacts](#) article to view the supported Artifacts for Windows, Mac, Android, and iOS operating systems.

- **Modifying Existing LitHolds (ER-141):**
  Existing LitHolds can now be modified by users. Notification emails will note any changes that may have been made within an existing LitHold.

- **Improved Error Reporting (FTKC-2014):**
  The job monitor now displays additional details associated to a job when errors have occurred. Additionally, any objects associated to a job will be labelled with their job ID within a folder named Error while in Review. Users can now view processing statuses and information using additional columns (HasProcessingError and ProcessErrorDescription) associated to a file during erroneous processing.

- **Assigning Users during Case Creation (FTKC-7548):**
  Users and user groups can now be assigned to a case when it’s being created.

- **Job Monitor Visibility (FTKC-6250):**
  The job monitor can now be opened within a separate window.

- **Custodian Fields (FTKC-1515):**
  A new ‘All Custodians’ field lists all the custodians in the case who had a duplicate/copy of the selected object. The primary custodian of the selected object can be found in the ‘DataSource’ field.

- **Agent Certificates (FCR-7903):**
  Agent certificate paths are now stored within the ADG database thereby protecting the confidentiality of the certificates from non-admin users.

- **FTK now allows users to migrate the AppDB to the ADG DB. (ER-4567)**

  **Note:** Users must utilise the 'Migrate Data' option within DBConfig to automate this process.

- A 'View Log' button has been added to DBConfig. This option will be available during upgrades and allows users to keep track of steps being made by the application during a DB upgrade. (FTKC-11198)
2 Resolved Issues

1. Resolved an issue where the coding changes were applied for all the files in the Review page instead of only the selected files when user performed the following steps: *(FTKC-13639)*
   - Filtered the files in the Review page
   - Enabled ‘Select all files’ options
   - Applied the coding changes via Coding panel

2. Resolved the following issue:
   - Upon renaming a radio button type custom field, the updated name was also reflected for some of the files for which the radio button custom field was not assigned. *(FTKC-12759)*

3. Resolved an issue where incorrect file count was displayed in the ‘Collection Progress’ pop-up for the collections performed for Group Custodians. *(FTKC-12887)*

4. Resolved an issue when performing an agent collection where a filter to include or exclude an exact file path was also filtering results containing the file path name. *(ER-8075)*

5. Resolved an issue where the job intended to process the ‘Auto Deploy Agents’ operation of a Collection failed. *(ER-6992)*

6. Resolved an issue where no information was present in Slack ‘Chat Conversation’ file downloaded from the Document Viewer. *(ER-1891)*

7. Resolved an issue where users were not able to import custodians with multiple subdomains using the ‘Import From AD’ option. *(FTKC-13136)*

8. Resolved an issue where files consisting of similar content were also filtered out upon enabling the ‘Remove Duplicates’ quick filter. *(FTKC-7324)*

9. Resolved an issue where the following file types were not supported in the viewer while using the FTK Central application in Mozilla Firefox browser. *(FTKC-3960)*
   - FLASH MP3
   - MP4
   - RIFF WAVE

10. Resolved an issue where the deleted Holds were displayed in the ‘LitHolds Responses’ and ‘IT Staff - Hold Notifications’ page. *(ER-5490)*

11. Resolved an issue where the approvers were not able to approve a LitHold via email link. *(FTKC-11658)*
12 Resolved an issue where the PST file (with attachments) extracted from a ZIP file was marked as a child file of the ZIP file. Now, the extracted PST file will be marked as the parent for its attachments (child files) **(FTKC-10975)**.

13 Resolved an issue where the files produced in TIFF image format using the Tabbed Production option were not displayed in the Viewer. **(FTKC-13223)**

14 Resolved an issue where HTML codes were displayed in the Microsoft Teams chat messages displayed in the Viewer. **(ER-7236)**

15 Resolved an issue where the generation of ‘Search Term Report’ for AD1 file types was being processed indefinitely. This issue occurred only upon performing the ‘Import’ operation while configuring the ‘Search Term Report’. **(FTKC-12678)**

16 Resolved an issue where the sorting of graphic files were reset when switched from Grid view to Thumbnail view. **(FTKC-6708)**

17 Resolved an issue where Slack collections would fail sporadically and/or would take longer than expected. **(FTKC-11220)**

18 Resolved an issue where the production version would not load tiff images within the Image view. **(FTKC-13223)**

19 Resolved an issue where FIPS enabled FTK environments could not connect to PostgreSQL. **(FCR-821)**

20 **Spring4Shell vulnerability** is not applicable to any Exterro product.

21 Resolved an issue where Video files would take significant time to convert to be viewable in the Image viewer. **(FTKC-14022)**

22 Internal Evidence Processing components have been updated to yield better performance for EXIF data recovery, video/picture thumbnail creation and encryption detection for BitLocker devices. **(FCR-7246)**

23 Resolved an issue where some graphic files would be categorized incorrectly. **(FCR-2855)**

24 Improvements have been made to UFDR processing. Users can expect a higher processing count in comparison to previous versions of FTK. **(FCR-7248)**

25 Resolved an issue where the entire dataset was processed irrespective of the File Types selected in Evidence Refinement. **(FTKC-14345)**

26 When the web service crashes while there is an ongoing site server job, the service will attempt to reconnect to those ongoing jobs and continue.

27 Agent collection results can now be stored on network locations by using redirected acquisitions. **(ER-6066)**

28 Resolved an issue where network share collections would not follow the original folder structure. **(ER-6145)**
3 Known Issues

1. Microsoft Teams collections when configured with GCC URLs will not finish without errors. *(ER-7299)*
2. Processing profiles created with mobile processing options prior to 7.6 does not function correctly when used. Users are advised to remove previously created custom processing profiles and create new profiles. *(FTKC-13436) (FTKC-13437)*
3. If a user would like to remove “Document Cluster Analysis” from a processing profile, “Cluster Analysis” must also be removed. *(FTKC-14223)*
4. When processing .DMG files (with loose files and a folder with files), FTK will process only the loose files but not the files within the folder. *(FTKC-8527)*
5. Windows Defender can cause decline in processing performance. *(FCR-8477)*
6. Empty folders are not displayed within the Live Preview tree view. However, when the collection is complete, the empty folder is viewable. *(ER-7092)*
7. When selecting the “Select All Custodians” option during LitHold creation/editing can cause the application UI to lockup. *(ER-5438)*
8. When viewing Google web graphics in the viewer, they are not displayed. *(FCR-2855)*
9. Incorrect search dates are shown within the generated search count report. This issue only exists when creating a search count report within FTK Connect. *(FTKCT-678)*
10. Forensic Images with incomplete file structures may be misidentified. Users must select an evidence category manually. *(FCR-10191)*
11. When a user manually selects loose files to perform OCR, Windows adds redundant thumbnail files to the thumbnail database while processing it. *(FCR-10051)*
12. When installing the Exterro AD Connectors service, it prompts users to select a Temp location. However, when a custom path is selected, the installer disregards the custom path and instead will use "EXTERROSERVICETEMPLOCATION" within the installers default Temp path. *(CRI-1621)*
13. Live Previews for agent connections can take 30 minutes on initial usage. If 30 minutes has lapsed the agent communication will be terminated. **Workaround:** Users can modify the 'AgentNotificationInterval' value within the ADG.WeblabSelfHost.exe.config file. This will dictate when a backend job will be initiated to poll the status of the public agent; when complete the UI will notify users when the agent is communicating. Alternatively, users can restart the agent service on the agent machine. *(ER-8042)*
14 RegEx searches need two options enabled in advanced search for it to work: ‘FTK Search’ and ‘Regex’. (FTKC-15217)

15 When filter panel is left open, the dynamic hit counts won’t update if a new search or filter is applied until the filter panel is refreshed. (FTKC-14994)

16 The ‘Labels’ field exports out the numeric value when the label field is used as a file name. Do not use the label field as a file name. (FTKC-1497)

17 The ability to copy from a previous export does not support exports/productions created in previous versions of FTK Central. (FTKC-15416)
Contact Exterro

If you have any questions, please refer to this document, or any other related materials provided to you by Exterro. For usage questions, please check with your organization’s internal application administrator. Alternatively, you may contact your Exterro Training Manager or other Exterro account contact directly.

For technical difficulties, support is available through support@exterro.com.

Contact:
Exterro, Inc.
4145 SW Watson Ave., Suite 400
Beaverton, OR 97005.
Telephone: 503-501-5100
Toll Free: 1-877-EXTERRO (1-877-398-3776)
Fax: 1-866-408-7310
General E-mail: info@exterro.com
Website: www.exterro.com

Information in this document is subject to change without notice. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Exterro, Inc. The trademarks, service marks, logos or other intellectual property rights of Exterro, Inc and others used in this documentation (“Trademarks”) are the property of Exterro, Inc and their respective owners. The furnishing of this document does not give you license to these patents, trademarks, copyrights or other intellectual property except as expressly provided in any written agreement from Exterro, Inc.

The United States export control laws and regulations, including the Export Administration Regulations of the U.S. Department of Commerce, and other applicable laws and regulations apply to this documentation which prohibits the export or re-export of content, products, services, and technology to certain countries and persons. You agree to comply with all export laws, regulations and restrictions of the United States and any foreign agency or authority and assume sole responsibility for any such unauthorized exportation.

You may not use this documentation if you are a competitor of Exterro, Inc, except with Exterro Inc’s prior written consent. In addition, you may not use the