

FTK REMOTE MOBILE DISCOVERY USER GUIDE

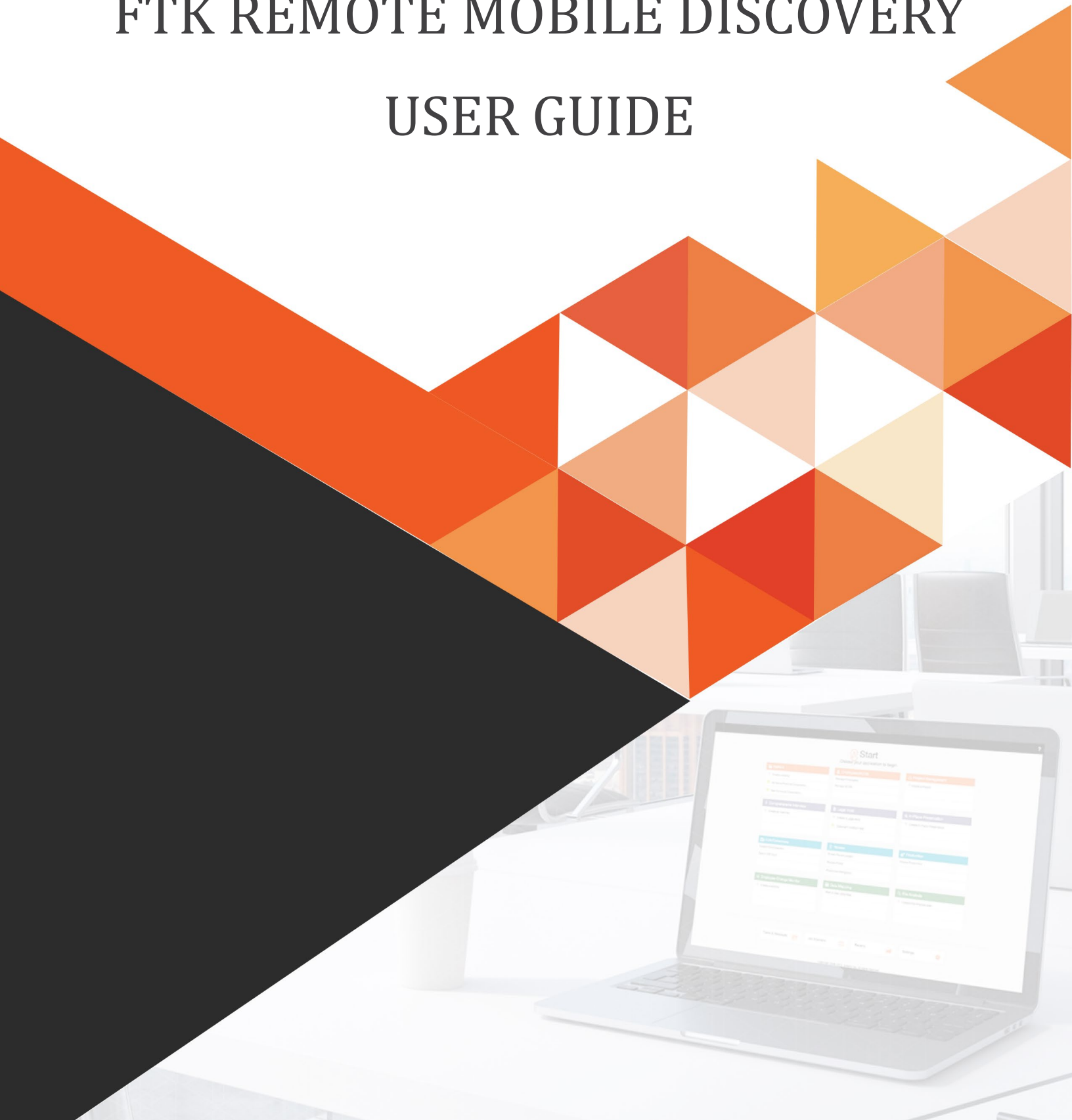


Table of Contents

ABOUT EXTERRO	2
REMOTE MOBILE DISCOVERY	3
CREATING MOBILE COLLECTION (VIA FTK CENTRAL)	4
<i>Custodian/Computer</i>	8
<i>Associated Mobiles</i>	11
<i>Collection Configuration</i>	15
<i>Review Collection</i>	28
VIEWING MOBILE COLLECTION.....	29
<i>Collection Details</i>	29
<i>Collection Logs</i>	32

About Exterro

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 Data Risk Management 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.

Remote Mobile Discovery

Exterro introduces Remote Mobile Discovery (RMD)-an advanced, efficient, and innovative solution for seamless mobile data collection in forensic investigations.

With RMD, you can:

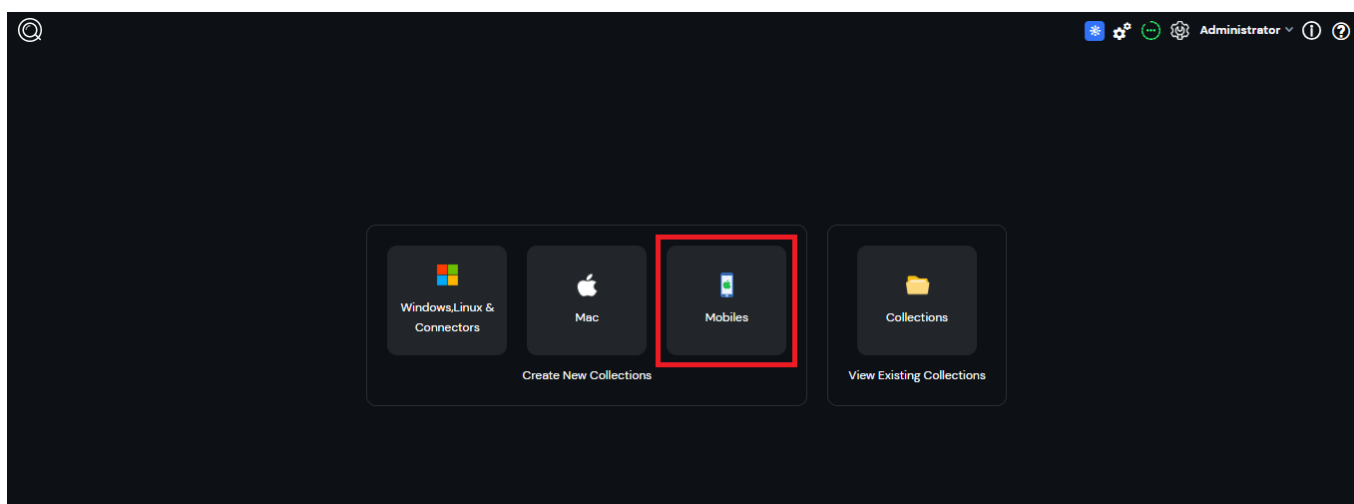
- Remotely connect to mobile devices associated with custodians or computers.
- Collect comprehensive data or focus on specific applications as per investigative needs.
- Ensure secure and forensically sound acquisition of mobile data without physical access to the device. (a user would still be required to consent to a collection by providing their passcode during a collection).

Designed for efficiency, accuracy, and compliance, RMD streamlines mobile forensic workflows, empowering investigators with fast, reliable, and remote data collection capabilities.

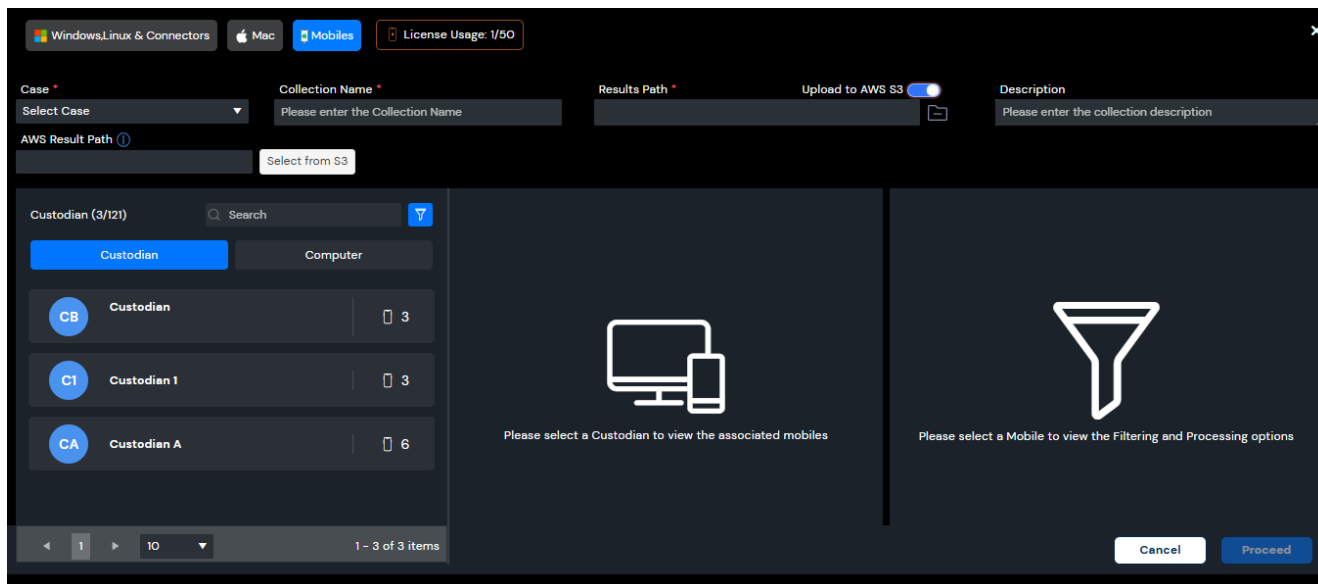
Creating Mobile Collection (Via FTK Central)

To create a Mobile Collection from the FTK Central application:

1. Login to the FTK Central application.
2. Select **Collections**.
3. Select **Mobiles**.

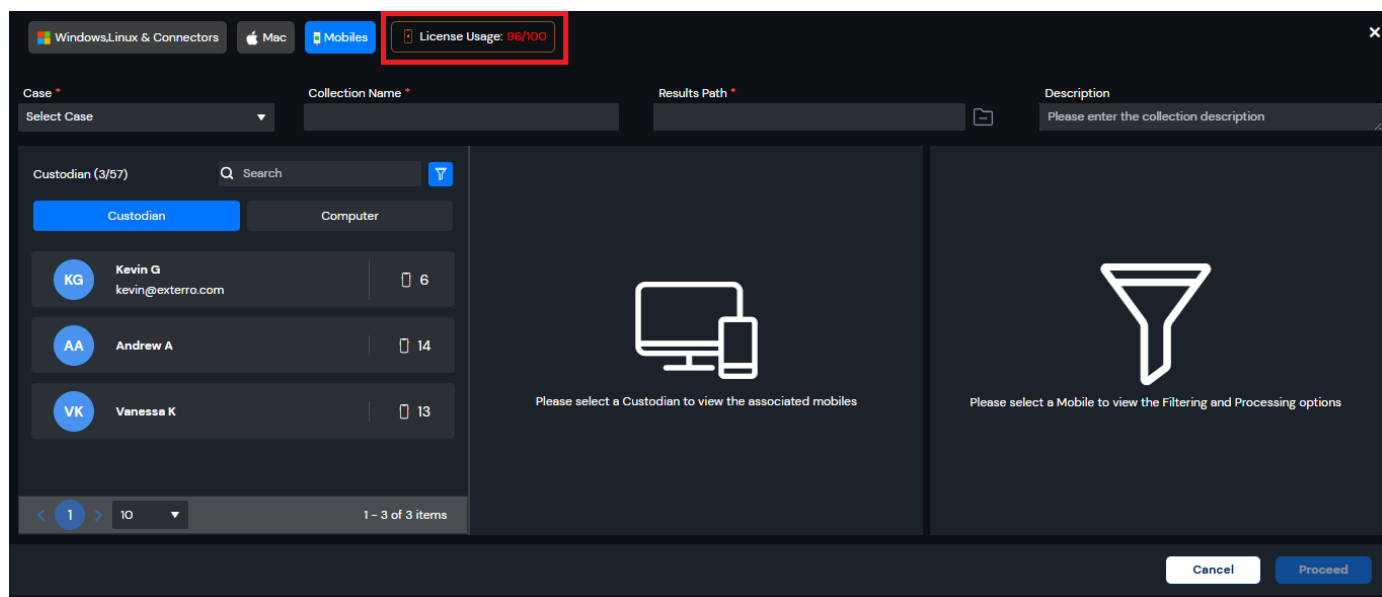


- The Mobiles Collection creation page is displayed:





Note: The **License Usage** field in the top of the page displays the total number of unique mobile devices allowed for collection against the number of mobile devices for which the collection is in-progress or completed.

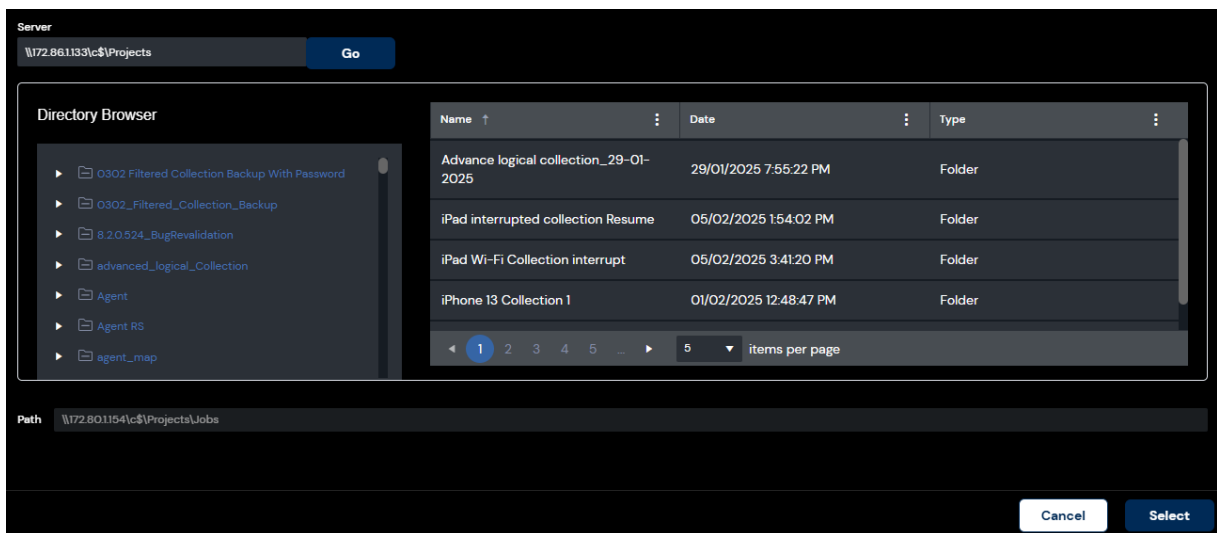


4. Provide the following details:

- **Case** – Select the case from the drop-down.
- **Collection Name** – Provide the collection name.

Note: The location for **Results Path** will be automatically populated based on the case selected in which the collected files will be stored. However, you can change the path if required. To do so,

- i. Click **Folder**  against the Results Path field.
 - The below page is displayed.



- ii. Enter the **Server Path**.
- iii. Click **Go** to view the directories available on the server.
- iv. Select the folder to be where the results are to be saved.
- v. Click **Select**.

- Enable the **Upload to AWS S3** toggle if you want to store the collected data into the AWS S3 cloud storage. Upon enabling this option, the **AWS Result Path** field will be displayed to select the required AWS S3 storage location.



Note: The Upload to AWS S3 toggle will be displayed only when the **AWS S3 Path for Collection** option is enabled in the **FTK Central Settings > System Management > Case Defaults**.

- **Description** – Provide a description of the collection that will be displayed in the details page.

Custodian/Computer

This section displays the list of custodians and computers added in the application along with the mobiles associated to it.

Custodian:

Custodian (3/57)

Q Search

Custodian

Computer

KG

Kevin G
kevin@exterro.com

6

AA

Andrew A

14

VK

Vanessa K

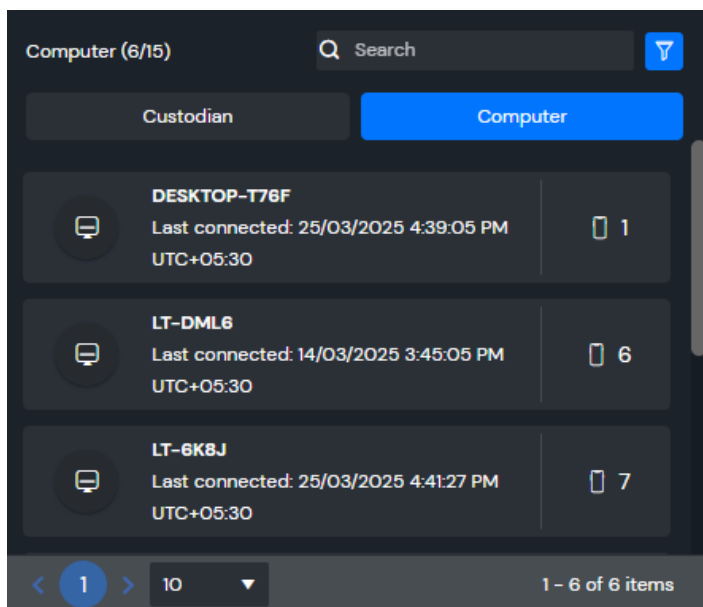
13

< 1 >

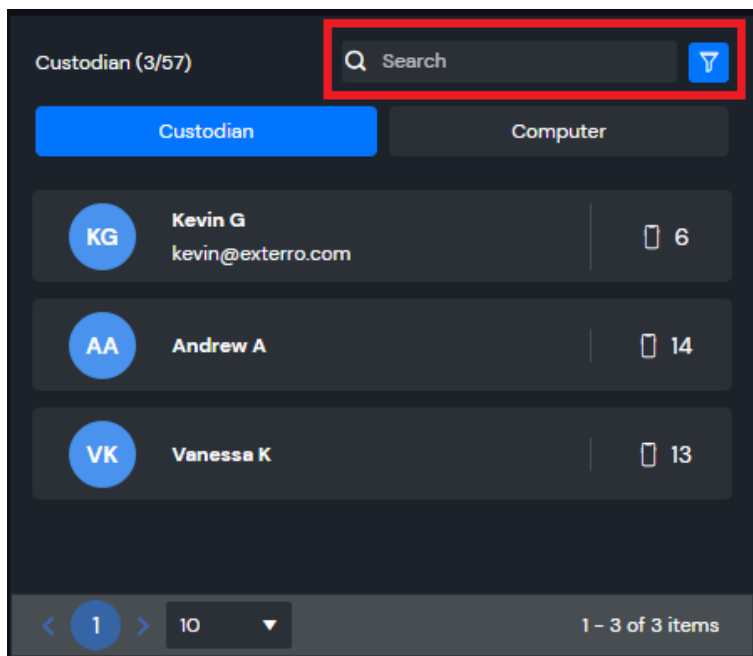
10 ▼

1 – 3 of 3 items

Computer:



You can use the search bar to search for computers, custodians, or mobile device names.



You can also click on  and select any of the below options to filter the custodians and computers:

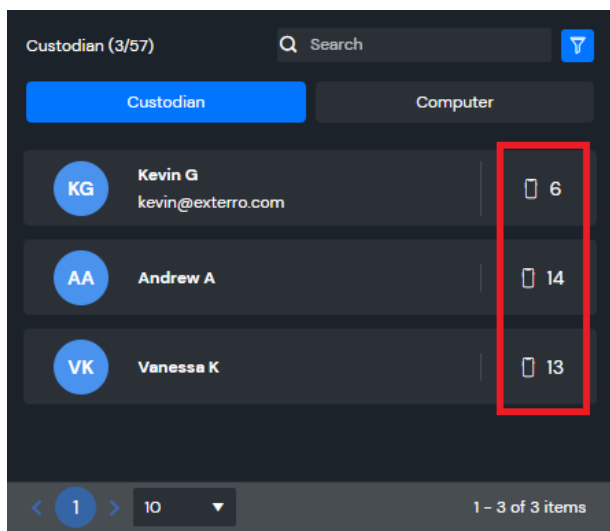
- **Recently Contacted** – Agents that have checked-in during the last auto provision.
- **Not Recently Contacted** – Agents that have not checked-in during the last auto provision.
- **Mobile Device Associated** –To filter only the custodians or computers that are associated with mobile phones.

Notes:



- Auto provision is the synchronization between site server and application databases. This synchronization is controlled based on the configuration made for the **autoprovisioninterval** property in the config file. Refer to the app config guide for more details.
- By default, the **Mobile Device Associated** filter is applied to display only the custodians and computers associated with mobile devices. However, you can disable this filter to view all the custodians and computers.

The number of mobile devices associated with the custodian or computer will be displayed against it.



5. Select the **Custodian** or **Computer** section and click on the required entity to view all the associated mobiles and its details.

Associated Mobiles

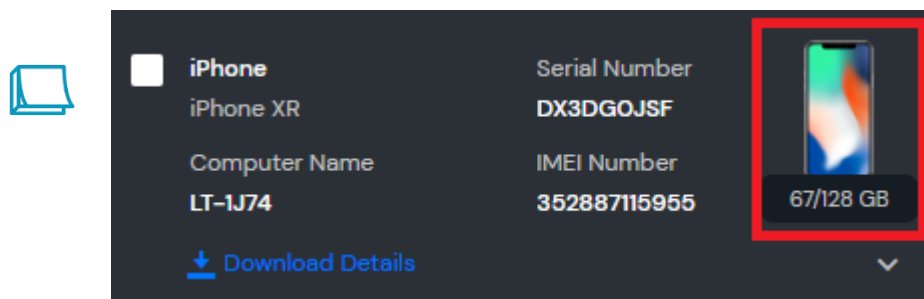
This section displays all the mobiles associated with the selected custodian or computer along with its basic details such as mobile device name, model number, serial number, etc. You can click on the expand icon  to view additional information about the mobile device.

Basic details:

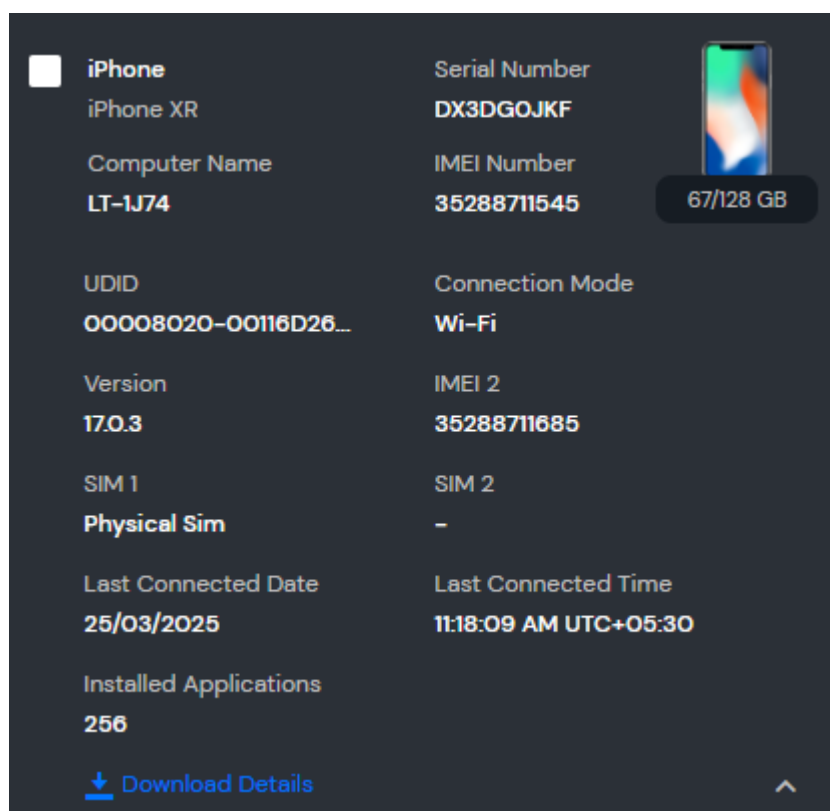
Associated Mobiles (0/6)

iPhone iPhone XR Custodian Name - Download Details	Serial Number DX3SKXKF IMEI Number 35288959045	 68/128 GB 
iPhone iPhone 14 Custodian Name - Download Details	Serial Number NGHFGP7 IMEI Number 35839341704	 91/128 GB 

Note: The volume displayed against the mobile device image indicates the available storage within the device's total storage.



Additional details:





Note: You can click on the **Download Details** button to download and view the following details of the corresponding mobile device along with the list of all applications installed on the mobile device:

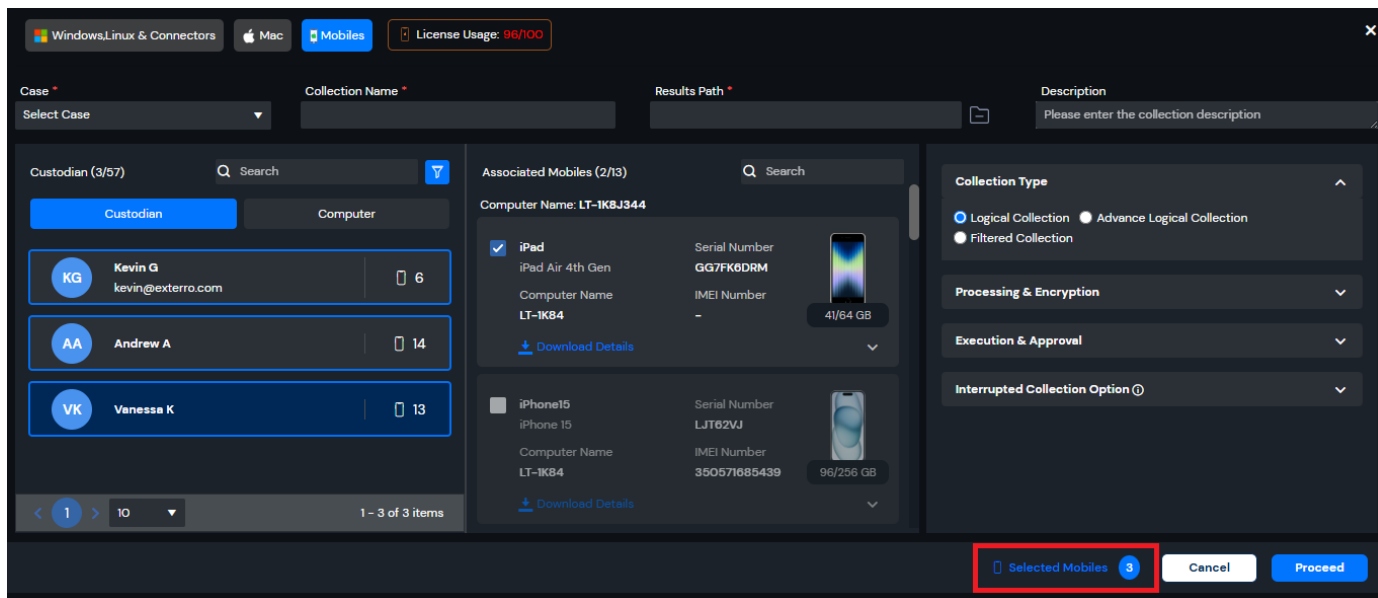
- Mobile Name
- Serial Number
- IMEI 2
- Last Connected Date & Time
- Connection Mode
- FirmwareVersion
- LastiTunesBackupDate
- Version
- UDID
- SIM 1
- Connected Computer
- Installed Application (Count)
- HardwareModel
- BackupEncryptionEnabled
- Storage
- IMEI 1
- SIM 2
- Associated Custodian
- EthernetAddress
- TimeZone

6. Check any one mobile from which the data needs to be collected.



Warning: You can select only one mobile per agent in the collection.

The **Selected Mobiles** option displays the total number of mobile devices selected for the collection. You can click on that count to view all the selected mobile devices and the associated custodians/computers.



Collection Configuration

This section displays all the configurations to filter and collect the targeted data from the mobile device.

The screenshot shows a dark-themed configuration panel with the following sections:

- Collection Type** (with an expand/collapse arrow):
 - ☒ Logical Collection
 - ☐ Advance Logical Collection
 - ☐ Filtered Collection
- Processing & Encryption** (with a collapse arrow)
- Execution & Approval** (with a collapse arrow)
- Interrupted Collection Option ⓘ** (with a collapse arrow)

Collection Type

This close-up shows the **Collection Type** section with three radio button options:

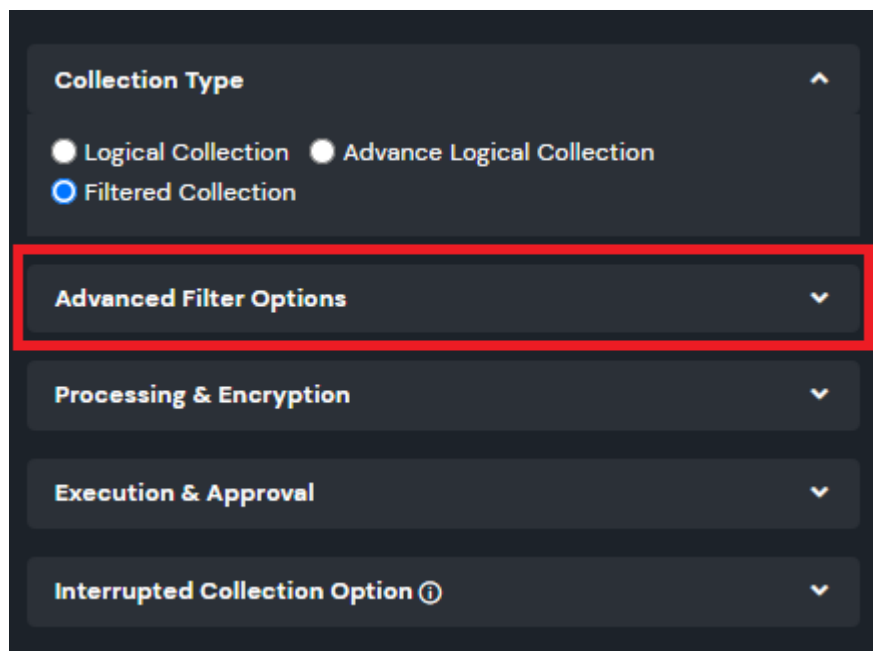
- ☒ Logical Collection
- ☐ Advance Logical Collection
- ☐ Filtered Collection

7. Select any one of the below **Collection Type** options:

- **Logical Collection** - To collect the entire backup of the mobile device.
- **Advance Logical Collection** – To collect the entire backup of mobile, AFC Service Data, and Lockdown Service.
- **Filtered Collection** – To collect data specific to the selected applications. Upon selecting this option, an additional section - [Advanced Filter Options](#) will be displayed, where you can configure all the filters for the collection.

Advanced Filter Options

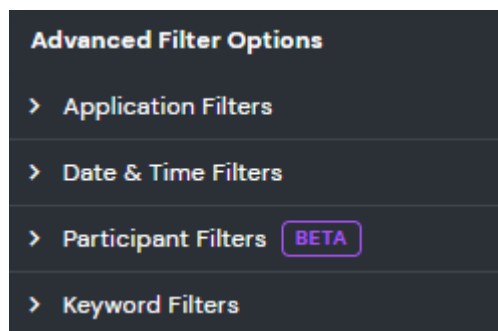
This section will be displayed only when the **Filtered Collection** option is selected for the **Collection Type** field.



The screenshot shows a dark-themed interface with a 'Collection Type' dropdown menu. It contains three radio button options: 'Logical Collection', 'Advance Logical Collection', and 'Filtered Collection' (which is selected). Below this menu is a list of other settings, each with a dropdown arrow. The 'Advanced Filter Options' item is highlighted with a red rectangular border. The other items are 'Processing & Encryption', 'Execution & Approval', and 'Interrupted Collection Option' (which includes an information icon).

This section consists of the following filtering options:

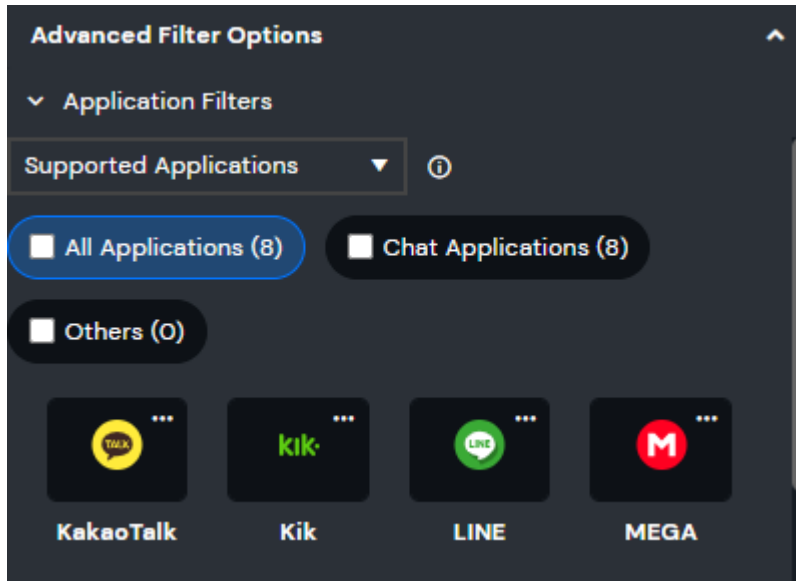
- Application Filters
- Date & Time Filters
- Participant Filters
- Keyword Filters



The screenshot shows the expanded 'Advanced Filter Options' menu. It lists four categories, each with a right-pointing chevron icon: 'Application Filters', 'Date & Time Filters', 'Participant Filters' (which has a purple 'BETA' badge next to it), and 'Keyword Filters'.

Application Filters

You can use this section to filter the data based on the applications present in the mobile device.



Select any one of the below options from the dropdown menu:

- **Supported applications-** Displays the applications installed in the selected mobile devices that are supported by the FTK Central application, which can be selected for collection.
- **Installed applications** – Displays all the applications that are installed in the selected mobile devices including the ones that are not supported by FTK Central. For the not supported applications, you can view them but not select them for collection.



Note: By default, the **Supported applications** option is selected for this field.

You can click on the following filtering options to filter and view the corresponding mobile applications in the device:

- All Applications
- Chat Applications
- Others

Moreover, you can click on the checkboxes against the filtering options to select the corresponding filtered applications.

You can click on the **Additional Details**  icon against the applications to view all the mobile devices (selected in the **Associated Mobiles** section) that have the applications installed on them.

Date & Time Filters

You can collect data within a specific time period by setting the From, To, and weekday filters in this section.

The screenshot shows the 'Date & Time Filters' section. It has a dropdown arrow on the left. Below the title, there are two input fields: 'From Date & Time' and 'To Date & Time'. Each field contains a placeholder 'day/month/year hou...' and a calendar icon. To the right of the 'To' field is a circular refresh icon. Below these fields is a 'Custom Calendar' section with seven circular buttons labeled S, M, T, W, T, F, and S, representing the days of the week.

Click on the **Refresh Dates**  button if you want to reset the date and time filters.

Participant Filters

This filter allows you to add participants and specifically filter all the conversations held between the participant and custodian.

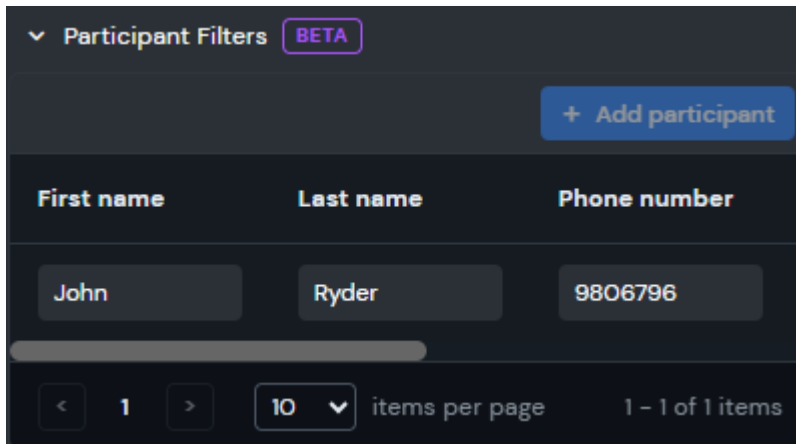
The screenshot shows the 'Participant Filters' section. It has a dropdown arrow on the left and a 'BETA' label in a purple box. On the right side, there is a blue button with a plus sign and the text '+ Add participant'. Below this is a table with three columns: 'First name', 'Last name', and 'Phone number'. The table is currently empty, and at the bottom right, it says 'No records found'.

To add the participants, click on the Add Participant button and fill in the following details:

- **First Name** – Participant's first name.
- **Last Name** – Participant's last name.
- **Phone Number** – Participant's phone number.
- **Email Address** – Participant's email address.

- **Direction** – The conversational direction between the custodian and participant (From, to, or Both).

Upon providing all the details, scroll horizontally to the end and click on **Save**  (in the **Actions** column) to add the participant.



Participant Filters **BETA**

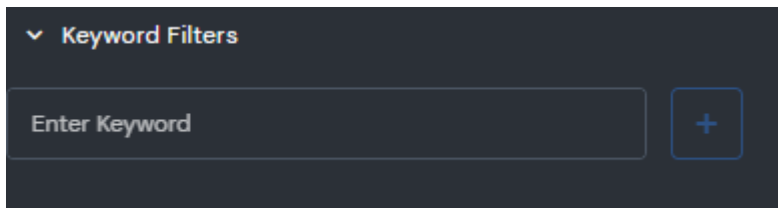
+ Add participant

First name	Last name	Phone number
John	Ryder	9806796

< 1 > 10 items per page 1 – 1 of 1 items

Keyword Filters

You can collect all files containing a specific set of keywords in the mobile device by configuring the list of required keywords in this section. You can add the required keyword in the text field and press **Enter** or click on the **Add Keyword**  button to add it. You can perform this step repeatedly to add multiple keywords.



Keyword Filters

Enter Keyword +

Processing & Encryption

8. Check the **Auto Process Collection** option and select the processing profile from the drop-down to automatically process the collected data.
9. Select the required Distributed Processing Manager (DPM) from the **Processing Manager** field to process the collection.
10. Check the **Enable Encryption** option and provide the iTunes backup passwords of all the selected mobile devices to create an encrypted collection.

Notes:

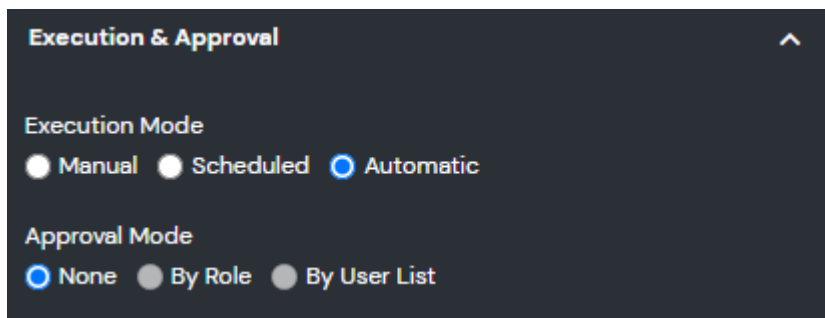


- If an encrypted collection has already been created for the device, the password will be automatically populated. You can update the password by replacing the existing one or reset the password by clicking on the **Reset Password**  icon and enter a new password.
- The time taken for the backup completion via Wi-Fi is longer when compared to wired connection.



Tip: You are recommended to use encrypted backups for better security and to include additional data, such as account passwords, call history, etc.

Execution & Approval



Execution & Approval

Execution Mode

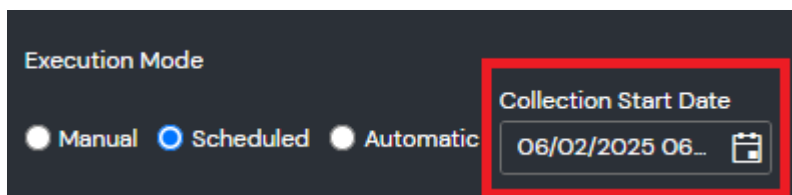
☐ Manual ☐ Scheduled ☒ Automatic

Approval Mode

☒ None ☐ By Role ☐ By User List

11. Select any one of the following **Execution Modes**:

- **Manual** - To manually initiate the collection process.
- **Scheduled** - To schedule the collection on the specified date and time. You configure it to be a recurring collection for a specified number of times using the following steps:
 - i. Upon enabling the Scheduled option, the **Collection Start Date** field is displayed. Click on the  icon against it.



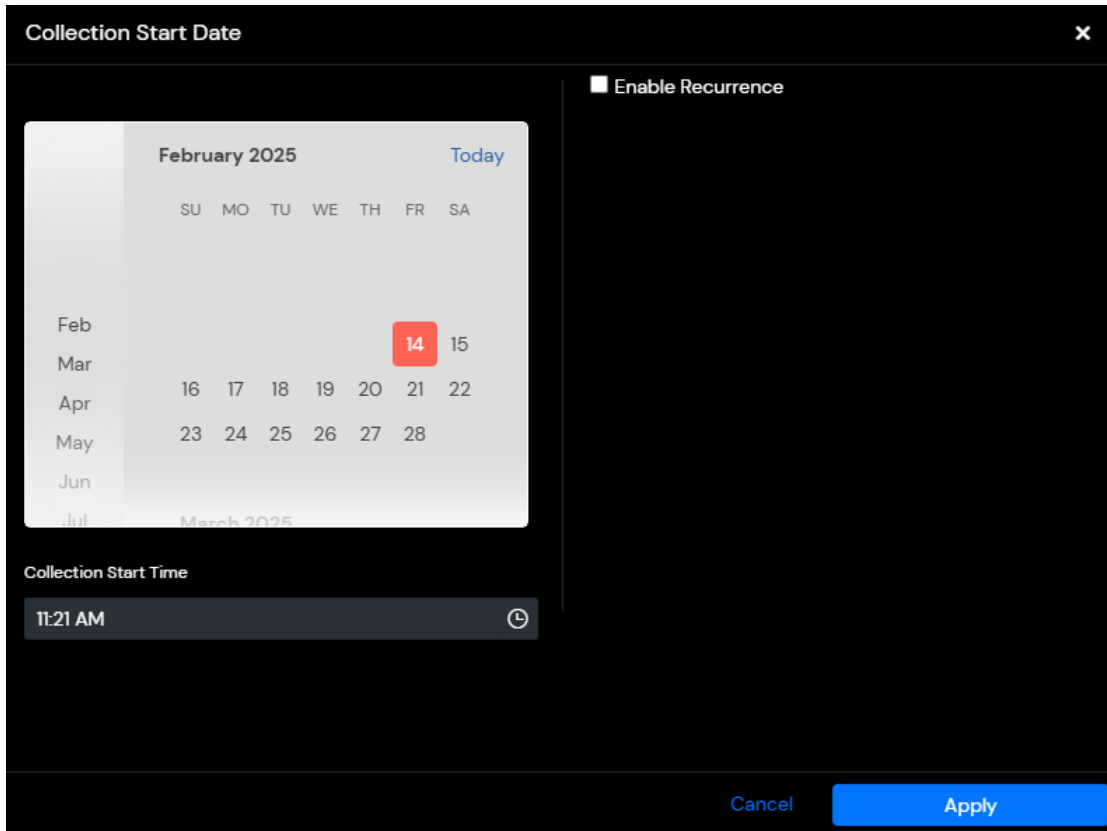
Execution Mode

☐ Manual ☒ Scheduled ☐ Automatic

Collection Start Date

06/02/2025 06... 

- ii. The **Collection Start Date** pop-up is displayed.



Collection Start Date [X]

February 2025 Today

SU MO TU WE TH FR SA

Feb 14 15

Mar 16 17 18 19 20 21 22

Apr 23 24 25 26 27 28

May

Jun

Jul

Collection Start Time

11:21 AM [Clock Icon]

☐ Enable Recurrence

Cancel Apply

- iii. Select the date from the calendar and **Collection Start Time** to schedule the collection.

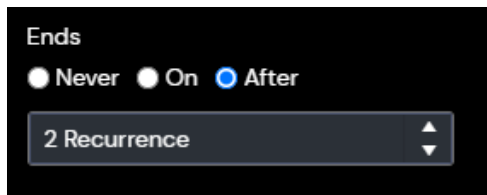


Note: If you want the collection to be processed just once on the scheduled date and time, click the **Apply** button after performing the above step. If you want it to be a recurring collection that should be performed for a specified number of times, proceed to follow the below steps as well.

- iv. Check the **Enable Recurrence** option to create a recurring collection.

- v. Select the time interval in the **Repeat Every** field during when the collection should recur.
- vi. Select the days in the **Repeat On** field when the action should be repeated.
- vii. Configure the Ends field to set when the recurring collection should end:
- **Never** – The recurring collection should continue indefinitely.
 - **On** – Set a date when the recurring collection should end.

- **After** – Set number of recurrences after which the recurring collection should end.



Ends

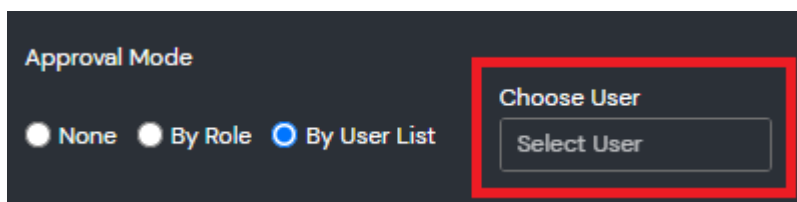
☐ Never ☐ On ☒ After

2 Recurrence

- **Automatic** – To automatically initiate the collection process immediately after creating it.

12. Select the **Approval Mode** for the collection:

- **None** - No approvals required.
- **By Role** - To be approved by users with specific roles.
- **By User List** - To be approved by users selected from the **Choose User** field.



Approval Mode

☐ None ☐ By Role ☒ By User List

Choose User

Select User

Incremental Collection:



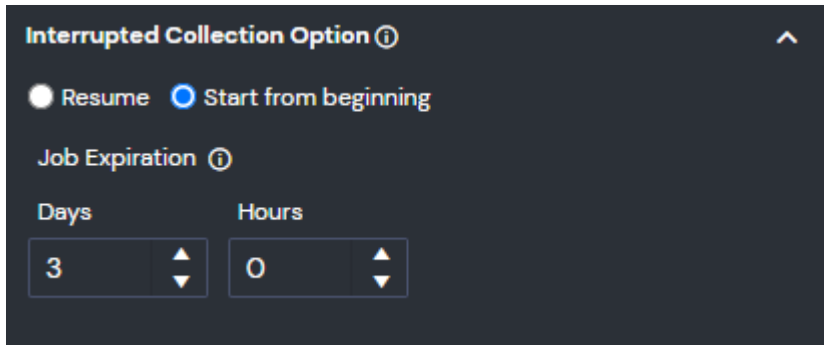
Note: This section is displayed only when the **Enable Recurrence** option is checked in the **Collection Start Date** pop-up .



13. Select any one of the following options for the **Incremental Collection** field:

- **Enable** – The collected data will be saved in the agent’s computer as a backup until the recurrence collection is concluded. If the data in the computer is deleted or moved, the collection will be initiated from the beginning.
- **Disable** – The collected data backup will be deleted as soon as a collection’s recurrence is completed.

Interrupted Collection Option



14. Select the action that should be taken in case of collection interruption:

- **Resume** - A backup will be created and maintained till the collection is resumed to start from where it was left off.
- **Start from beginning** - To start the collection from the beginning.



Tip: You are recommended to select the **Start from beginning** option to ensure the integrity and completeness of the data. Resuming the collection may result in missing some files which were not successfully collected prior to the interruption,

15. Set the **Job Expiration** duration.

16. Click **Proceed**.

Review Collection

Review Collection

Basic Details

Case	Collection Name	Collection Type
Tetra Org. Case	RMC - 001	logical
Result Path	Description	
\\organization\Projects\Jobs		
Encryption	Auto Process	
Enabled	Collection	
	Mobile Processing	

Execution

Execution	Collection Start Date	Collection Start Time
automatic		
Repeat On	Ends	Repeat Every
		null
Collection Option	Interrupted Collection	Job Expiration
-	Option	Days 3 Hours -
	Start From Beginning	

Selected Mobiles

DEV01

Last Connected: 29/01/2025 7:40:44 AM

Steph's iPhone

(iPhone 15 Pro)

Approval (none)

Custodians

No Custodians Selected

Applications

Cancel

Submit

17. Review and verify the configurations made to the collection.

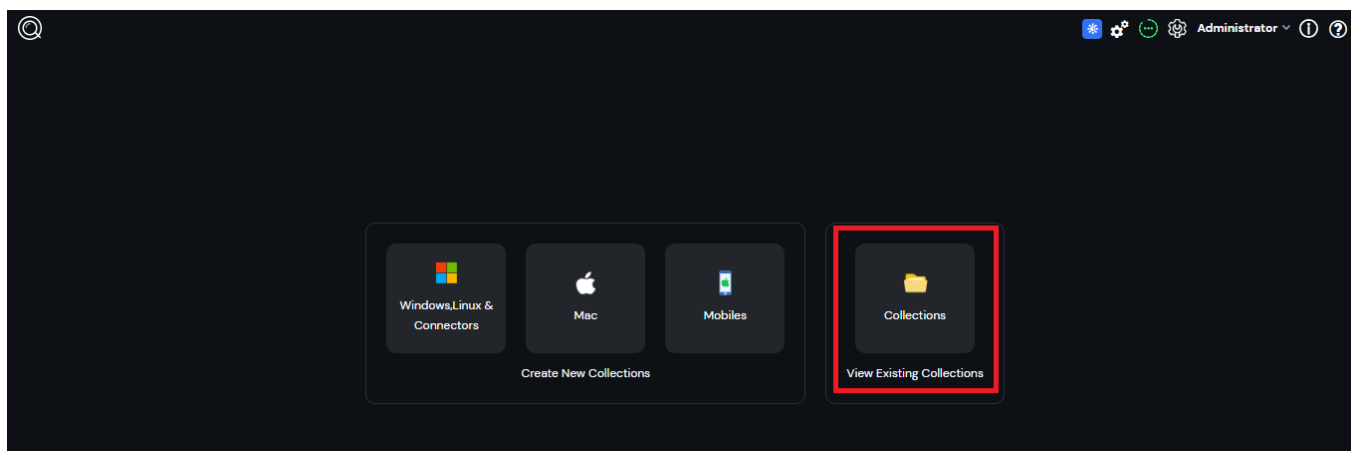
18. Click **Submit**.

Viewing Mobile Collection

Collection Details

To view the details of a Mobile Collection:

1. Login to the FTK Central application.
2. Select **Collections**.
3. Select **View Existing Collections**.



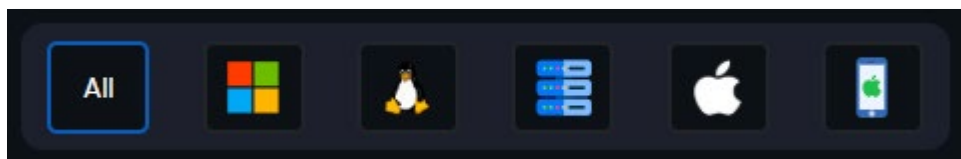
- The manage collections page is displayed.

The screenshot shows the 'Collections' page in the FTK Central application. The page has a dark theme and includes a search bar at the top right. Below the search bar, there are tabs for 'All', 'Pending', 'Not Started', 'Collecting', 'Completed', 'Cancelled', and 'Failed'. The 'All' tab is selected. Below the tabs, there is a table with the following columns: Collection Name, Case Name, Job Ty..., Collection Status, Processing Status, Approved, Target, Created, and Actions. The table lists several collections, including iPad collection, Colt 98 Collection, FC_Data_Backup, iPhone 15 Collection, Chat Applications - Collection, BMJ Collection, and iPhone 14 Collection. The bottom of the page shows a pagination bar with 'Page 1 Of 19' and '10 Items per page'.

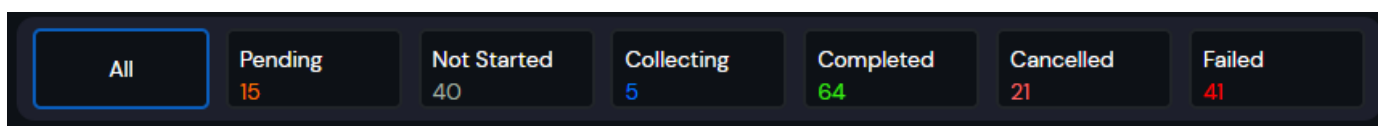
Collection Name	Case Name	Job Ty...	Collection Status	Processing Status	Approved	Target	Created	Actions
iPad collection	Tetra Org. Case	Mobile Collection	Collecting 0%	NotStarted 0%	Yes	1	07/02/2	...
Colt 98 Collection	Colt Case	Mobile Collection	Pending 0%	Pending 0%	No	1	07/02/2	...
FC_Data_Backup	FC Company Case	Mobile Collection	Completed 100%	Completed 100%	Yes	1	07/02/2	...
iPhone 15 Collection	Kevin Case	Mobile Collection	Completed 100%	Completed 100%	Yes	1	07/02/2	...
Chat Applications - Collection	NRG Case	Mobile Collection	Completed 100%	Completed 100%	Yes	1	07/02/2	...
BMJ Collection	AMT Case 002	Mobile Collection	Collecting 0%	NotStarted 0%	Yes	1	06/02/2	...
iPhone 14 Collection	Case 820.525	Mobile Collection	Pending 0%	Pending 0%	No	1	06/02/2	...

4. You can filter the collections by clicking on any of the following filter options:

- **Collection Type Filters:**



- **Collection Status Filters:**



5. Click on the **Actions Menu** and select **Collection Details**.



Note: Alternatively, you can click on the **Collection Status** column value against the required collection to view its details.

Collection Details

logical_collection_2

826.37 MB
Total Collection Size

00:16:04
Elapsed Time

Logs

Reports

Targeted

Completed

Failed

Not Started

Collecting

Collection Status

Completed 100%

Processing Status

Completed

Mobile Name	Custodian N_	Computer N_	Created _	Start _	Collected Da_	Collection Status	Processing Stat
iPhone13	Kevin R	LT-6K84	26/03/2025 11:41:07 AM	26/03/2025 11:41:10 AM	826 MB	Completed 100%	Compl

1

Page 1 Of 1

10

Items per page

1 - 1 Of 1

The details of the corresponding collection will be displayed.

Collection Logs

You can click on the **Logs** button from the Collection details page to view the detailed Agent logs and comprehensive progress status of the Collection. You can select the required agent from the **Target** field to view the corresponding details.

Collection Details

logical_collection

iphone_logical_collection

826.27 MB

Total Collection Size

00:16:07

Elapsed Time

Logs

Reports

Targeted

Completed

Failed

Not Started

Collecting

Collection Status

Completed

100%

Processing Status

Completed

← Logs

Target

LT-6K8J344

Collection Status

Completed

100%

Processing Status

Completed

Start Date & Time

26 Mar 2025 1:33:16 PM

Last Log Update

26 Mar 2025 1:53:17 PM

Search...

UTC+05:30

Search...

Hits (0)

UTC -5:30

Download

Refresh

Fullscreen

Job Completed

26 Mar 1:49:36 PM

Collection Completed

26 Mar 1:49:27 PM

Evidence Job Created

26 Mar 1:49:27 PM

Collection InProgress

26 Mar 1:49:26 PM

Transfer Completed

26 Mar 1:49:26 PM

Apple Service Restarted Unlock Required

26 Mar 1:44:35 PM

2025-03-26 01:35:22 PM I [ModuleInvoker.cpp:647]: [23768] [module: netfs.exe] [thread: 19360] RMC-(Mobile Device Job Started) Mobile device backup job has started with taskid 099bbc97-5396-4278-aatl-a902d56c2105 device id : 00008110-000248960A69801E

2025-03-26 01:35:22 PM D [ModuleInvoker.cpp:644]: [23768] [module: netfs.exe] [thread: 19360] RMC:taskid 099bbc97-5396-4278-aatl-a902d56c2105 MobileDeviceBackupExecution received base path : C:\Program Files\AccessData\Agent\config\netfs.exe\00008110-000248960A69801E

2025-03-26 01:35:25 PM I [ModuleInvoker.cpp:647]: [23768] [module: netfs.exe] [thread: 19360] RMC-(Apple service restarted Unlock required) taskid 099bbc97-5396-4278-aatl-a902d56c2105 Accessory Connected unlock iPad/iPhone to access the accessories

2025-03-26 01:35:25 PM D [ModuleInvoker.cpp:644]: [23768] [module: netfs.exe] [thread: 19360] RMC:Getting list of connected mobile device taskid : 099bbc97-5396-4278-aatl-a902d56c2105

2025-03-26 01:35:37 PM D [ModuleInvoker.cpp:644]: [23768] [module: netfs.exe] [thread: 19360] RMC-(Mobile connected) deviceid 00008110-000248960A69801E is connected for taskid 099bbc97-5396-4278-aatl-a902d56c2105

2025-03-26 01:35:37 PM D [ModuleInvoker.cpp:644]: [23768] [module: netfs.exe] [thread: 19360] RMC-(Enable Encryption) Encryption already enabled for taskid 099bbc97-5396-4278-aatl-a902d56c2105 device id 00008110-000248960A69801E

2025-03-26 01:35:37 PM D [ModuleInvoker.cpp:644]: [23768] [module: netfs.exe] [thread: 19360] RMC-(Wifi) Mobile

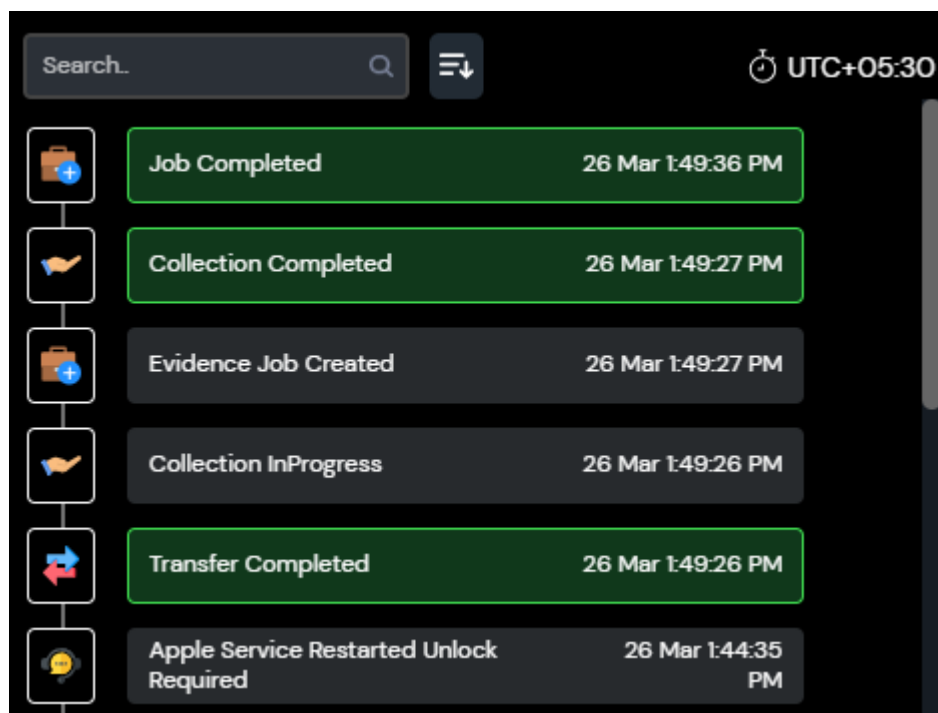
© Exterro, Inc. All rights reserved

www.exterro.com

Collection Progress:

You can view the Collection progress status from the left pane of the Logs section. You can use the search bar to search for the required status and sort the order of progress from job initiation to completion or vice versa by clicking of the **Sort**  icon.

The timezone displayed here in this pane is the default time zone set in the **Case Defaults** of FTK Central Settings.



Agent Logs:

The right pane of the **Logs** section displays the entire and detailed Agent logs. You can search for the required logs using the search bar. You can click on the following icons to perform the corresponding operations:

-  - Download the logs
-  - Refresh the logs
-  - Expand the pop-up to have a better view of the logs

The timezone displayed in this section is based on the Agent selected.



We'd love to hear from you

Our team will be happy to help you on any questions. Write to us!

support@exterro.com

© Exterro, Inc. All rights reserved