IBIS®

INTEGRATED BALLISTICS IDENTIFICATION SYSTEM

Administration Guide

IBIS Products

FORENSIC TECHNOLOGY

IBIS Products

Administration Guide

Forensic Technology

IBIS® Products Administration Guide
Document No.: AGD35-EN001, Version 3.0

Trademarks

Forensic Technology WAI Inc.
5757 Cavendish Boulevard, Suite 200
Cote St. Luc, Quebec, Canada H4W 2W8

Telephone: +1 514-489-4247 Canada/USA Toll free +1-888-984-4247
Fax: +1 514-485-9336

E-mail: info@contactft.com
Web site: www.forensictechnology.com

Contents

CHAPTER 1

Welcome to IBIS

This section covers the following topics:

Introduction

This guide is intended for administrators who work with **IBIS®** workstations or servers in an IT maintenance capacity. The information provided in this guide includes all the IBIS products that are currently supported, except for **IBIS®** Heritage™.

The guide is not associated with any specific version of the following products: **IBIS®** TRAX-3D™, **IBIS®** Correlation Server, or **IBIS®** Infrastructure. It includes the following topics:

- Product descriptions
- User accounts
- Backup procedures
- Maintenance procedures

Note: For information about IBIS Heritage, see the IBIS Heritage documentation which includes an Administration Guide and a User Guide.

Administrative Privileges

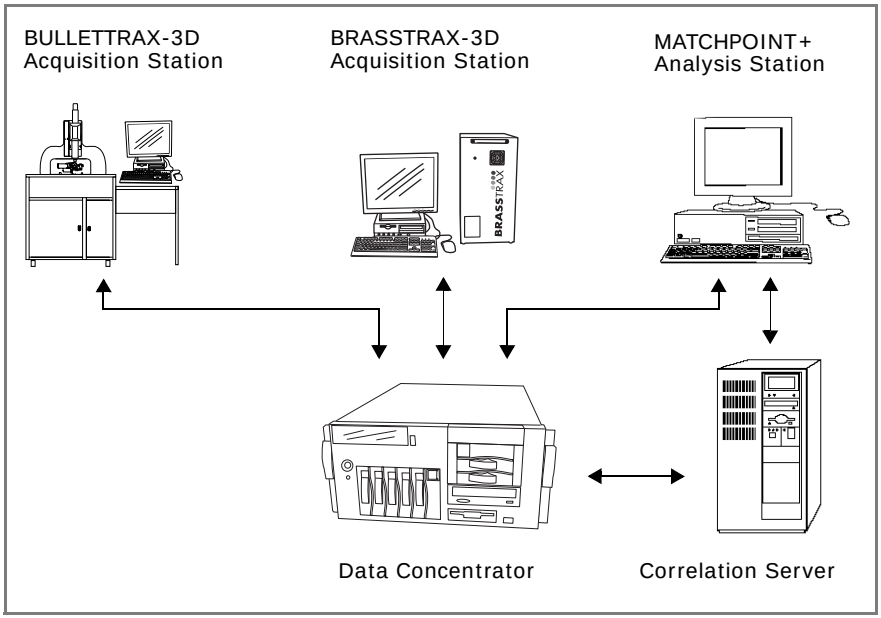
Administrators can manage IBIS TRAX-3D applications in local and network configurations. To manage user accounts on your IBIS network, you must have account operator or domain administration privileges.

For security reasons, only Forensic Technology personnel can assign administrative account privileges that allow users to perform the tasks and activities described in this guide. For more information, see Contact Technical Support (page 17).

Product Descriptions

The IBIS TRAX-3D product family consists of **IBIS®** BRASSTRAX-3D™, **IBIS®** BULLETTRAX-3D™, **IBIS®** MATCHPOINT+™, and **IBIS®** Data Concentrator.

An IBIS TRAX-3D system consists of a Data Concentrator, a MATCHPOINT+ Analysis Station, one or more BRASSTRAX-3D and/or BULLETTRAX-3D Acquisition Stations, and a Correlation Server.



Acquisition Stations

The BRASSTRAX-3D Acquisition Station is a cartridge case evidence imaging station that captures cartridge case images and information. BRASSTRAX-3D provides fully automated acquisition of breech face and firing pin marks and manual capture of ejector marks. If the appropriate features are activated, full headstamp images and 3D images of breech face marks can be acquired.

The BULLETTRAX-3D Acquisition Station is a bullet evidence imaging station that captures bullet images and information. Operators can acquire 2D digital images and create 3D topographic models of the surface of a bullet.

The Acquisition Stations copy this information to the Data Concentrator. A built-in function is responsible for automatically copying exhibit information and images from the Acquisition Station to the Data Concentrator at predefined times.

Data is backed up at the end of each working day, after all the data on the Acquisition Stations has been synchronized with the Data Concentrator.

Both Acquisition Stations run on Microsoft® Windows® and are fully networkable using TCP/IP protocols.

IBIS MATCHPOINT+ Analysis Station

MATCHPOINT+ is a desktop Analysis Station that is connected to a Data Concentrator or Correlation Server via a Local Area Network (LAN). MATCHPOINT+ generates correlation requests and displays the ranked results. Firearm Examiners use MATCHPOINT+ to analyze correlation scores, visually compare potential matches, and record hits.

IBIS Data Concentrator

The Data Concentrator is a server that provides permanent data storage for signatures and acquired cartridge case and bullet images and information.

Electronic Signatures

The Data Concentrator generates electronic signatures, which are mathematical representations of a region of interest, from acquired bullet and cartridge case images. These signatures are sent to the Correlation Server for comparison with signatures that are already in the IBIS database.

Image Compression

The Data Concentrator generates compressed images using the raw image data of the given exhibit when the exhibit data is received. The Data Concentrator then provides the Correlation Server with the generated compressed images for data storage in the server database after the image is compressed.

Correlation Requests

After the exhibit's electronic signatures are generated, the Data Concentrator automatically generates a correlation request for the following event types: Assault with a Deadly Weapon, Homicide, Test Fire Returned, Unknown, and Other.

The correlation request uses the information about the exhibit to distinguish a sample in the IBIS database.

Note: Although the Data Concentrator stores data that has been copied from the Acquisition Stations, it does not own the data it receives. The Acquisition Stations remain the owners of the data. Therefore, if data needs to be modified, it can only be modified on the Acquisition Station that created it.

The Data Concentrator is connected to an uninterruptible power supply (UPS) so that in the event of a power failure, the UPS provides sufficient power to allow enough time to properly shut down the system and preserve the information on the Data Concentrator. In addition, the Data Concentrator provides backup and recovery. A backup device is provided to make incremental copies and to keep an image of the entire hard drive information.

IBIS Correlation Server

The Correlation Server polls the Data Concentrator at regular intervals and uploads any new signatures for comparison with the signatures that are already in the IBIS TRAX-3D system.

The principal functions of the Correlation Server are to:

- Receive and manage the unique digital signatures that are generated by the Data Concentrator
- Mathematically compare signatures, which enables operators to rapidly search through hundreds or thousands of exhibits
- Rank pairs of signatures according to their similarity

Domain Controller

The domain controller is part of the domain services included in the IBIS Infrastructure. Combined with a set of tools and services, it simplifies the administration of IBIS installations that have many workstations. Depending on a client's requirement, it can be configured as a dedicated server or the Data Concentrator can be promoted to a domain controller. The principal functions of the domain controller are:

- Centralized user management
- Improved security
  - Customized password policies
  - Replication of centralized changes throughout the network
- Routine collection and backup of event logs

Note: To meet requirements for additional security, some IBIS networks are configured to use a master domain controller.

Types of Platforms

A number of hardware platforms with different storage capacities are available for Data Concentrators and Correlation Servers.

For perspective, one terabyte of storage capacity can store from 100,000 to 220,000 exhibits on a Data Concentrator, or ten times more (compressed images) on a Correlation Server.

Note: If the Data Concentrator is promoted as a domain controller, the affect on data storage is insignificant.

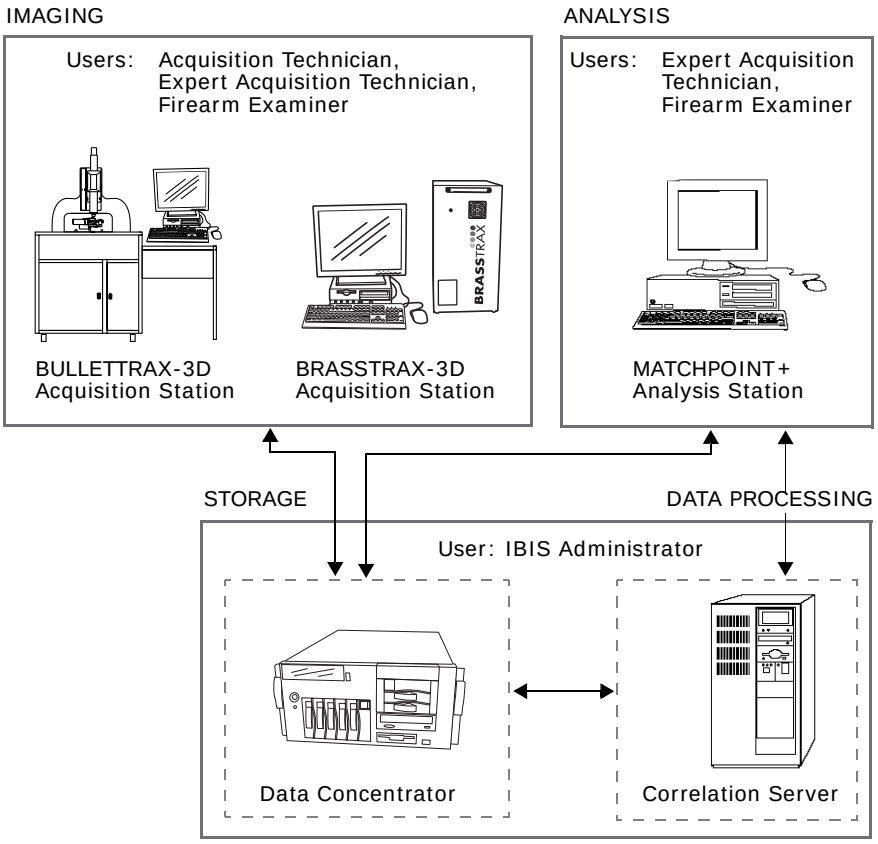
The backup and maintenance procedures apply to the platform that is configured for your facility. The following table describes the different platforms, models, their storage capacity, and backup.

Platform	Model	Capacity	Description
A	A1	275 GB	A hardware configuration that uses individual tapes for backups.
B	B1 B2	1 TB 3 TB	A hardware configuration that uses disk media for backups.
C	C1 C2 C3	3 TB 6 TB 9 TB	A hardware configuration that uses a tape library for backups.

For information about the backup procedure for each platform, see About Backups (page 25).

Workflow

Users acquire images of bullets and cartridge cases using BULLETTRAX-3D and BRASSTRAX-3D Acquisition Stations. These images are submitted to the Data Concentrator for compression and signature generation. The Correlation Server checks the Data Concentrator at regular intervals for newly submitted cases and uploads them to the IBIS database.



The system automatically generates correlation requests, or users submit manual correlation requests, to compare exhibits. Results are ranked according to similarity. Firearm Examiners can then use the MATCHPOINT+ MultiViewer and Side-by-Side Viewer to examine the most highly-ranked exhibit pairs. If a match between two images is found, a hit is declared, which indicates that the firearm linked to the exhibit was used at the site of a reported crime.

Note: The physical networking configuration of IBIS TRAX-3D can be adjusted according to specific needs.

IBIS TRAX-3D Configuration

IBIS TRAX-3D can be configured through a system of one or more Acquisition Stations and Analysis Stations. Each Acquisition Station stores exhibit information in flat files and regularly synchronizes this information with the Data Concentrator. For a configuration diagram, see Product Descriptions (page 10).

Acquisition Stations operate independently of one another. If one Acquisition Station fails, the other Acquisition Stations at the site will continue to function.

MATCHPOINT+ can assess all the data that Acquisition Stations have synchronized with the Data Concentrator. If an Acquisition Station fails, any data that has not yet been synchronized with the Data Concentrator will be lost.

Data from a failed Acquisition Station cannot be modified until a replacement is installed and the data is recovered from the Data Concentrator.

Contact Technical Support

For information about the minimum system requirements to run IBIS TRAX-3D applications, or for product support, contact Forensic Technology Support. You can contact us by phone, fax, or email.

	Europe, Africa, and Western Asia	**Americas, Oceania, and Asia (other than western)**
Toll free number	800 4247 4247	866 984 4247
Direct number	+353 1 690 9199	+1 727 826 7236
Fax	+353-1-457-1822	+1 727-826-7242
Email	fti.support@contactft.com	fti.support@contactft.com

Your Feedback

Forensic Technology is dedicated to continually improving the documentation products. Your comments are appreciated and will be used to improve our services. Please include the title of the document and the specific section that you are commenting on in all correspondence.

Send your comments to: documentation@contactft.com.

CHAPTER 2

Managing User Accounts

This section covers the following topics:

User Accounts

Each individual who needs to use an IBIS application must be assigned a user account. A user account identifies who created or modified data within the application and includes a password to ensure that only authorized individuals have access to the system.

A user account also has a set of permissions associated with it that restricts the user to certain tasks within the IBIS application that are related to that user's group.

IBIS TRAX-3D User Groups

Users of IBIS TRAX-3D applications are organized into FTITRAX groups. There are three core groups and two specialty groups. A user group is defined by permissions to perform specific tasks. All the FTITRAX user groups and their related permissions are defined by Forensic Technology personnel.

Only one core group can be assigned to a user. A specialty group can be assigned alone, or assigned in addition to a core group to give a user additional permissions.

The following table lists the main permissions associated with each user group.

Core Groups	Permissions
FTITRAX Acquisition Technician	Manage cases and exhibits. Acquire breech face and centerfire firing pin cartridge case images using BRASSTRAX-3D. Acquire 2D and 3D images of pristine bullets using BULLETTRAX-3D. Modify, delete, and reacquire local images. Submit new cases. Analyze images in MATCHPOINT+.
FTITRAX Expert Acquisition Technician	Manage cases and exhibits. Acquire images using BRASSTRAX-3D and BULLETTRAX-3D. Modify, delete, and reacquire local images. Submit new cases. Analyze images, view correlation results, and create hits in MATCHPOINT+.
FTITRAX Examiner	Manage cases and exhibits. Acquire images using BRASSTRAX-3D and BULLETTRAX-3D. Modify and delete submitted cases and exhibits. Modify, delete, and reacquire local and submitted images. Submit new and modified cases. Force data synchronization. Analyze images, view correlation results, and create hits in MATCHPOINT+.

Specialty Groups	Permissions
FTITRAX Administrator	Set preference values for the system that override any individual user preference settings.
FTITRAX Report	Create and print reports in MATCHPOINT+.

User Account Management

IBIS TRAX-3D User Account Management is a tool to help you set up and manage accounts for all the users on your IBIS TRAX-3D network.

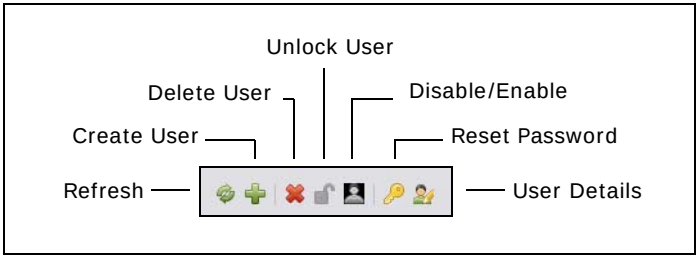
Depending on your configuration, the application may be installed on one or all of the workstations on your network. You must be an account operator to access the application. For more information, see Administrative Privileges (page 9).

A user account includes the user's real name, a user ID, and a password. When you set up a user account, you must also select a role for the user. A user role has a set of permissions that define what the user can and cannot do in a particular IBIS TRAX-3D application.

For a summary of the permissions associated with each user role, see IBIS TRAX-3D User Groups (page 21).

Note: If you have a Windows XP operating system that has been configured with local user accounts, you must manage user accounts from: **Control Panel** > **Administrative Tools** > **Computer Management** > **Local Users and Groups**.

The User Account Management toolbar contains the following commands:



Start IBIS TRAX-3D User Account Management

To start the application:

- Start the application in one of the following ways:
  - Double-click the IBIS TRAX-3D User Account Management icon on the desktop.
  - From the Windows **Start** menu, select **All Programs** > **Forensic Technology** > **IBIS TRAX-3D User Account Management**.

  If you are an authorized user, the IBIS TRAX-3D User Account Management window opens.

  The User folder in the left pane contains the user accounts on your network. The right pane displays the individual user accounts in the folder.

Create a User Account

To create a user account:

1. On the toolbar, click **Create User**.
2. On the **User Information** tab, complete the following:
   - First Name
   - Last Name
   - Display Name
   - User ID. The User ID must be unique in your IBIS TRAX-3D network.
   - Password
   - Confirm Password
3. Select the **User must change password at next logon** check box.
4. On the **IBIS TRAX-3D Settings** tab, complete the following:
   - Select a core role.
   - Select additional specialty role, as required.
5. Click **OK**.

Delete a User Account

To delete a user account:

1. Select the user account.
2. On the toolbar, click **Delete User**.
3. Click **OK**.
4. Click **Yes** to confirm.

Unlock a User Account

For security purposes, a user account is locked after an incorrect password is entered more than the configured number of times.

To unlock a user account:

1. Select the user account.
2. On the toolbar, click **Unlock User**.

   The user account is unlocked and the user must enter a new password at next logon.
3. Click **OK**.

Disable a User Account

For security purposes, you may want to disable a user account temporarily, for example, extended leave or vacation.

To disable a user account:

1. Select the user account.
2. On the toolbar, click **Disable User**.

   The icon for a disabled user account is black and white (); the icon appears in color () when it is enabled.

Tip: To enable a disabled user account, click Enable on the toolbar.

3. Click **OK**.

Reset a Password

You can reset a user password anytime. For example, if a user forgets his or her password, you can reset it so that he or she can enter a new password.

The internal policies at your facility control the password format and the expiration period.

To reset a password:

1. Select the user account.
2. On the toolbar, click **Reset Password**.
3. Enter a new password.
4. Retype the password to confirm.
5. Click **OK**.

Modify a User Account

To modify a user account:

1. Select the user account.
2. On the toolbar, click **User Details**.
3. Modify the account details on the **User Information** tab or the **IBIS TRAX-3D Settings** tab as required.

Tip: To restore account details you changed without closing the window, click **Reset**.

4. Click **OK**.

CHAPTER 3

Backups and Maintenance

This section covers the following topics:

About Backups

To guard against loss of data in the event of a system failure, as well as to allow for off-site data storage, each IBIS TRAX-3D installation is provided with a backup device. This device, controlled by the backup software, automatically schedules on-site and off-site backups of the IBIS database.

For a description of the different platforms available, see Types of Platforms (page 14). The backup procedure for each platform is specific to the platform, and not to the installed IBIS product; a Data Concentrator or a Correlation Server.

Note: If the Data Concentrator is promoted as a domain controller, and that domain controller assumes the role of infrastructure master, the data and log files are automatically included in the scheduled backups.

Backup media are rotated to ensure that a long history of the contents of the IBIS database is created. If an error is discovered in the database, the backup media can be consulted and used to restore the database.

User Notification

To inform users of the system status, an automatic notification is sent when the backup tapes (platform A) or off-site media should be rotated, or if there is a backup error. The server will also make a series of one-second beeps.

A notification system automatically sends notices to all the IBIS TRAX-3D workstations that are on the same network. Notifications are sent hourly, when the monitoring system is triggered to run.

To control the broadcast of notifications, a list of the target workstations can be placed in a configuration file. Contact FT Support for more information.

Procedures for Platform A

Platform A uses individual tapes for backups. The backups are scheduled to run at a fixed time.

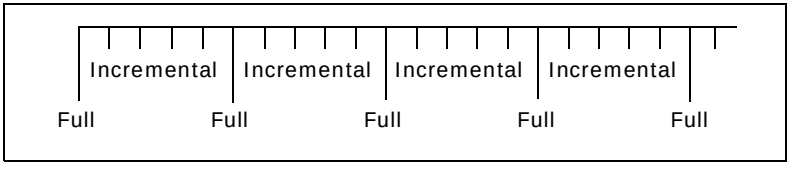
On-site Backup

There are two types of backups; full and incremental. Together they provide an eight-week recovery window.

Backup Type	Frequency	Description
Full	Weekly	A full backup backs up all the stored data. The IBIS database is shut down during the backup; however, users can continue to work on the Acquisition Stations. Performed: Fridays at 11:00 p.m.
Incremental	Daily	An incremental backup backs up only data that was created or modified since the last backup. The IBIS database is not shut down. Performed: Monday to Thursday nights at 11:00 p.m.

Note: Only BRASSTRAX-3D and BULLETTRAX-3D users can use the system during the full backup. Notify MATCHPOINT+ users when full backups are scheduled to occur.

The following diagram illustrates the frequency of the scheduled backups and the eight-week recovery window.



Changing Tapes

At the beginning of each week, a new tape must be inserted into the tape backup device. From Monday to Thursday, incremental backups are done on the tape. On Friday, a full backup is done on the same tape and the backup tape is changed.

After the full backup has been completed, the tape is automatically ejected from the tape drive. Monday morning at 4:00 a.m., a notification message is sent asking for a Media Insert (the next tape in the sequence). The next sequentially numbered tape must be inserted into the drive for the backup process to continue at the next scheduled time (by default 11:00 p.m.). For example, if the last tape to be used was TAPE_2B, you must insert TAPE_3B. The tape expected is also displayed in the notification message.

Caution: It is important to always use the next sequentially numbered tape as displayed in the notification message. Failure to do so will result in data not being backed up.

Tape Sequence

The IBIS TRAX-3D system comes with two sets of tapes. Each set contains four tapes covering four weeks of data, creating an eight-week record of the database. One set is labeled Series A and the other is labeled Series B.

The tape sequence is as follows:

- TAPE_1A
- TAPE_2A
- TAPE_3A
- TAPE_4A
- TAPE_1B
- TAPE_2B
- TAPE_3B
- TAPE_4B

Missed Backups

If a backup is missed, the backup job for that particular day will be skipped and notifications will be sent to insert the correct tape. Backups will continue to be skipped until the correct tape in the sequence has been inserted.

For example, if a full backup was completed on Friday using Tape_2A, the tape drive will be expecting Tape_3A to be inserted on the following Monday. If Tape_3A is not inserted on Monday, the server will beep and notifications will be sent to insert the correct tape. Backups will be stalled until Tape_3A has been inserted into the tape drive during the week. If for some reason, Tape_3A is not inserted at some point during the week, the full backup will be missed on Friday and the tape drive will request the next tape in the sequence the following Monday, namely Tape_4A.

Off-site Storage

To ensure that a backup is available in case of fire or other disaster, the tape series that is not currently being used should be held in an off-site storage area.

When each tape in Series A has been used, send the tapes off-site and switch to the Series B tapes. When the tapes in Series B have been used, switch back to Series A. This means you must retrieve the Series A tapes from off-site storage and send the Series B tapes to your storage facility.

Tape Cleaning

Over time, the digital tape device collects debris that separates the recording head from the tape and interferes with the recording process. When this debris has accumulated, the CLEAN/MEDIA light on the device lights up. When this happens, use the cleaning tape provided.

To clean the tape drive:

1. Press UNLOAD to eject the current tape from the device.
2. Replace the current tape in the drive with the cleaning tape.

   The cleaning tape was included with the backup tapes at system installation.
3. Run the tape to the end.

   The tape is ejected automatically when it reaches the end.

4. Replace the cleaning tape with the backup tape that was previously in use.

Note: The CLEAN/MEDIA light can indicate any tape problem. If the CLEAN/MEDIA light lights up even after the cleaning tape has been used, insert a different recording tape. If the light goes out, the first recording tape you tried might be damaged. If the light still does not go out, the drive might be malfunctioning. In either case, contact FT Support for maintenance or replacement tapes.

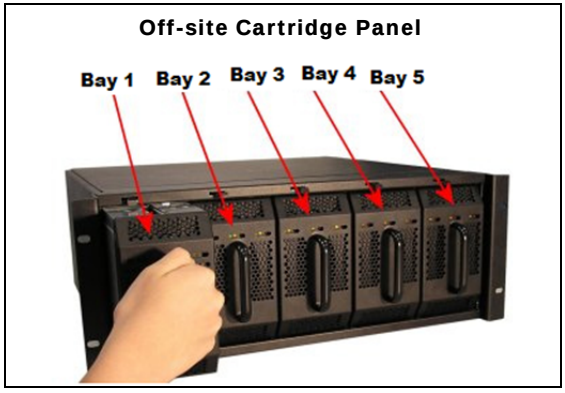
The cleaning tape is good for 20 uses. After that, the device will not accept it. The drive will unload the tape and the CLEAN/MEDIA light will stay lit. Therefore, after each use, mark the tape's label to keep track of how many times it has been used. When your cleaning tape approaches 20 uses, contact FT Support for information on obtaining a replacement.

Procedures for Platform B

Platform B includes automated features that minimize maintenance, including a disk-to-disk backup process.

Platform B provides on-site and off-site backups as follows:

- On-site backups are stored on disks that cannot be removed.
- Off-site backups are stored on a removable disk cartridge so the off-site media can be rotated and stored safely at an off-site location. For expansion options, there are five off-site disk bays.



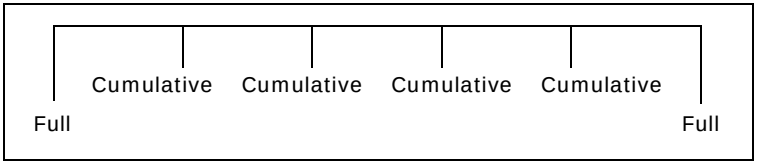
Note: Typically, one bay is dedicated to the off-site backup for each Data Concentrator or Correlation Server in the configuration. For installations with multiple servers, the bays are labeled accordingly.

On-site Backup

There are two types of backups; full and cumulative incremental. Together they guarantee a four-week recovery window. A much longer period can be recorded for recovery; the exact period depends on the available space on the disk.

Backup Type	Frequency	Description
Full	Monthly	A full backup backs up all the stored data. The IBIS database is not shut down during the backup; therefore, there is no work interruption. Performed: Every four weeks on Friday at 8:00 p.m.
Cumulative Incremental	Weekly	An incremental backup backs up only data that was created or modified since the last cumulative or full backup. Performed: Every Wednesday at 8:00 p.m.

The following diagram illustrates the frequency of the scheduled backups and the four-week recovery window.



Off-site Backup

The off-site backup is a full and independent backup of the IBIS database. The schedule is not linked to the schedule of the full on-site backup.

There are two off-site cartridges, one is labeled "Off-site 1" and the other is labeled "Off-site 2". They are rotated so that one can be stored securely at an off-site location and the other can record the next period. The off-site cartridge is the only cartridge that is rotated.

The rotation policy for the off-site media is configurable. The default policy settings are: rotate cartridge after the off-site backup is complete and do not overwrite the previous off-site backup.

The off-site backup disk is active only when the off-site backup is being created. A flashing blue light indicates the activity. This is the only time the cartridge cannot be removed; wait to receive a notification when the backup is completed.

Backup Type	Frequency	Description
Off-site	Biweekly	A full backup backs up all the stored data. The IBIS database is not shut down during the backup; therefore, there is no work interruption. Performed: Every two weeks on Saturday at 8:00 p.m.

Rotate Off-site Media

If the default rotation policy is enabled, the off-site cartridge must be rotated after the off-site backup is complete.

To rotate the off-site cartridge:

1. On the off-site disk panel, identify the cartridge that is labeled either "Off-site 1" or "Off-site 2", depending on the rotation.
2. Make sure the cartridge is not active. An active cartridge should never be removed.

Note: A flashing blue light indicates that the cartridge is active and should never be removed. The green "power" light indicates that the cartridge is inactive and can be removed safely.

3. On the top of the bay, release the cartridge by moving the lock to the left.
4. Using the handle, slowly slide the cartridge out and set it aside.
5. Insert the second off-site cartridge that has been retrieved from off-site storage.

   When the cartridge is completely inserted, the bay locks automatically.

To prepare the cartridge for off-site storage:

1. Place the off-site cartridge that you removed in the provided carrying case.
2. Arrange to send it to your off-site storage facility.

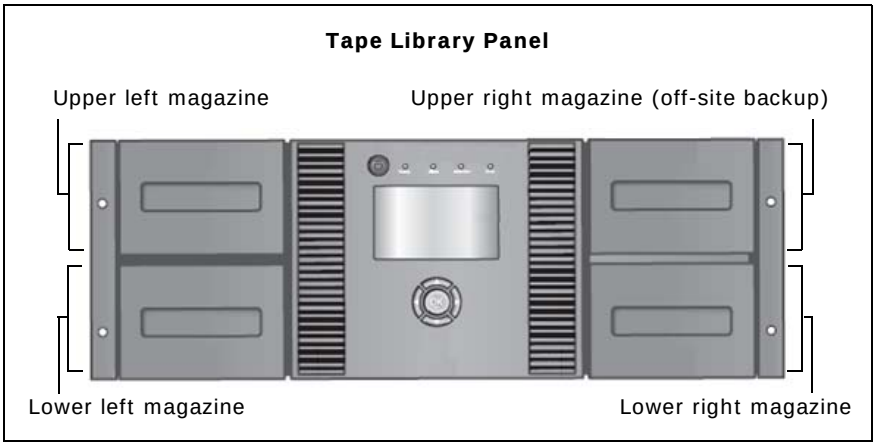
Note: The removable cartridge is a durable and reliable media. It has a protector tray complete with fan, temperature alarm and reliable connectors.

Failed Backup

If for some reason, the on-site or off-site backup fail, the IBIS database will shut down immediately. A notification is sent when the hourly monitoring system it triggered to run. Contact FT Support to restart the database and resolve any issues with the backup process.

Procedures for Platform C

Platform C uses a tape library that contains four tape magazines, each of which can hold twelve tapes. The upper right side magazine is reserved for the off-site backup.



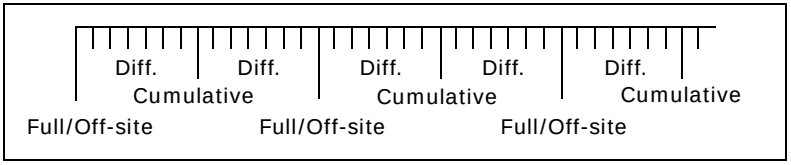
On-site Backup

There are three types of backups; full, cumulative incremental, and differential incremental. Together they guarantee a four-week recovery window.

Backup Type	Frequency	Description
Full	Biweekly	A full backup backs up all the data that is stored. The IBIS database is not shut down during the backup; therefore, there is no work interruption. Performed: Every two weeks on Friday at 8:00 p.m., offset from cumulative incremental backup.

Backup Type	Frequency	Description
Cumulative Incremental	Biweekly	An incremental backup backs up only data that was created or modified since the last full backup. Performed: Every two weeks on Friday at 8:00 p.m., offset from full backup.
Differential Incremental	Daily	A differential backup backs up only data that was created or modified since the last backup, of any type. Performed: Daily at 8:00 p.m.

The following diagram illustrates the frequency of the scheduled backups and the four-week recovery window.



Off-site Backup

The schedule for the off-site backup is linked to the schedule of the full backup. After every full backup is complete, a copy is created on the off-site magazine. There are two off-site magazines, one is labeled Off-site Magazine 1 and the other is labeled Off-site Magazine 2. They are rotated every two weeks so that one can be stored securely at an off-site location and the other can record the next period. The off-site magazine is the only magazine that is rotated.

Backup Type	Frequency	Description
Off-site	Biweekly	A copy of the full backup backs up all the stored data. The IBIS database is not shut down during the backup; therefore, there is no work interruption. Performed: Every two weeks on Saturday at 8:00 p.m.

For additional security, access to the tape library is controlled by a user name and password. Contact FT Support for access information.

To eject the off-site magazine:

1. Open the rack monitor keyboard and log on with the user name and password provided by FT Support.
2. On the desktop, double-click the **Eject Magazine** icon.
3. Click **Unlock Right Magazines**.
4. Wait for the message to indicate that the upper and lower magazines on the right side are unlocked.
5. Remove the upper magazine that is labeled either "Off-site Magazine 1" or "Off-site Magazine 2", depending on the rotation.

   A timer displays to track the 30 seconds that you have to remove the magazine before it is locked again.
6. Insert the other off-site magazine and wait for the confirmation message to display.
7. Click **Quit**.
8. Log off and then close the rack monitor keyboard.

To prepare the magazine for off-site storage:

1. Wrap the off-site magazine that you removed in antistatic paper.
2. Place it in the carrying case provided.
3. Arrange to send it to your off-site storage facility.

Failed Backup

If for some reason, the on-site or off-site backup fail, the IBIS database will shut down immediately and a notification is sent. Contact FT Support to restart the database and resolve any issues with the backup process.

Tape Cleaning

The tape library contains two cleaning tapes for cleaning the tape drives in the library. The process is completely automated, from detecting when cleaning is required to executing the cleaning.

Preventative Maintenance

Some precautions must be taken to ensure that the backup device and its media remain in top condition. Otherwise, the backup might become damaged or corrupted and the data on them might be lost.

Visual Inspection

Perform a visual inspection periodically to ensure that none of the redundant components have failed. If you encounter a lit LED that is labeled with a caution or heartbeat icon, contact FT Support. It may indicate a component failure that requires attention even though the server is operating normally because of built-in redundancy.

Handling Tapes

Individual tapes used in a tape backup device must be handled carefully to keep them working properly. Never touch the leader or bare tape with your fingers, since skin oils can damage or erase tapes. If a tape has to be moved from a warmer or cooler environment, let it adjust to the temperature of the room where it is to be used before inserting it into the device. Otherwise, the tape might stretch or break.

Do not use adhesive labels on the tapes. Use only the labels provided with the tapes, and only apply those to the front label slot of each tape. Unglued or detached labels can block the recording head of the tape device, preventing recording and possibly damaging the device. Similarly, use only a felt-tip or ballpoint pen to mark the tapes. Microscopic debris from pencils and grease pencils can interfere with the recording mechanism.

Individual tapes for a backup device are provided with protective boxes. Storing tapes in these boxes protects them from dust and humidity. To minimize long-term strain on tapes, store them on their side.

Digital linear tape (DLT) is sensitive to temperature and humidity. To extend tape life, store them at a temperature of 64° to 79° F (18° to 26° C) and a relative humidity of 40% to 60%.

System Diagnostics

Data Recovery Diagnostics

If an Acquisition Station unexpectedly shuts down due to a power failure, system failure, or any other reason, there is a risk that a certain amount of data may become corrupted and lost.

The next time that a user logs on to an Acquisition Station, BRASSTRAX-3D or BULLETTRAX-3D performs a data recovery. If there are any inconsistencies between the restored data and the embedded files located on the Acquisition Station, the information and signatures will be automatically synchronized between the two devices. The application will not start until the data recovery process is complete.

The database diagnostics and synchronization are done automatically; there is no action required by the administrator.

Built-in Tests

After a user opens an application, but before logging on to his or her account, a built-in test is carried out to make sure that the application can run properly.

If a built-in test fails, the Acquisition Station or Analysis Station will display a message alerting the user to the failure. The application will ask the user if he or she wants to continue using the application and, if so requested, will open as usual.

Data Recovery

IBIS products are equipped with an uninterruptible power supply (UPS), which allows for a smooth power-down of the unit should power be cut off unexpectedly. If the IBIS TRAX-3D system unexpectedly shuts down due to a power failure, system failure, or any other reason, there is a risk that a certain amount of data may become corrupted and lost.

The backup media can be used to restore lost data. Otherwise, all the acquisitions missing from the IBIS database would have to be redone.

Before you can continue using the IBIS TRAX-3D applications, the IBIS database must be restored from the backup media.

Restore from Backup Media

In the event of a system crash, Forensic Technology will restore the data from the backup media and/or recover the contents of the IBIS database to the time of the last successful backup prior to the crash. After the recovery is complete, you will be notified by Forensic Technology of any data inconsistencies resulting from the crash.

Index

P

R

S

T

U

W

IBIS® Administration Guide

FORENSIC TECHNOLOGY