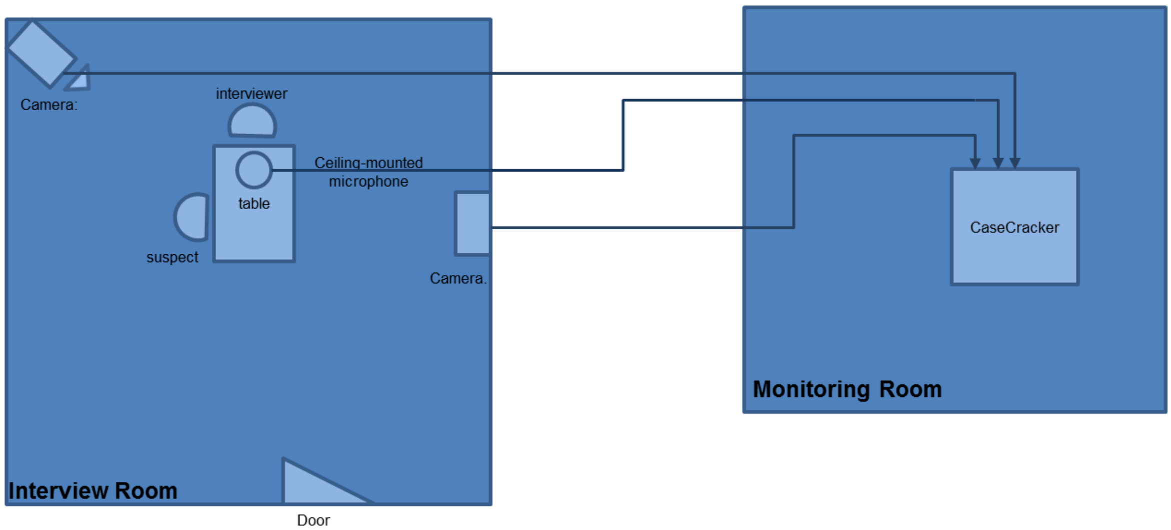
CaseCracker Administrator Manual

For version 4.2 of CaseCracker Interview Management System; last revised July 2014

Table of Contents

1. System Overview

The CaseCracker Interview Management System is designed for the recording of law enforcement interviews. It typically consists of an interview room, containing a covert microphone and one or two covert or overt cameras. Elsewhere in the building, an interview monitoring station contains the CaseCracker workstation, as pictured below:



The remainder of this document details the operation of the system from the perspective of an administrator of the system. User tasks are covered in a separate document, titled "CaseCracker User Manual". Please familiarize yourself with this document first.

NOTE: Unless otherwise noted, the tasks outlined in this manual require you to be logged in to the system with administrator privileges.

2. Users and Groups

The general mode of operation of the CaseCracker system is that each user, *including administrators*, should log in using their own account. This preserves the integrity of the event log, since actions on the system are logged with the name of the currently-logged-in user. As an administrator, you must create accounts for all users before they can use the system.

a. ***Special Accounts:*** CaseCracker is shipped with two special user accounts that cannot be deleted: the *Administrator* and *root* accounts.

   The *Administrator* is the top-level (or master) administration account. By default, the password for the *Administrator* user is '**welcome**', though this can be changed by logging in as *Administrator* and selecting Tools > Set Password from the menu bar.

The *root* user provides privileged access to the underlying Linux operating system, and should be used only under the instruction of a Cardinal Peak support engineer. The password for the *root* user is always the same as the password for the *Administrator* user.

NOTE: You should change the password of the *Administrator* user immediately!

b. ***System Groups:*** Groups allow the visibility of any interview to be limited to the selected group of users, preventing non-members from unauthorized access. As an administrator, it is your responsibility to create and maintain groups. Note that using groups in CaseCracker is optional and it is quite common for small departments to use the system without ever having to create any groups.

CaseCracker allows an unlimited number of groups to be created for purposes of segmenting interviews recorded on the CaseCracker system. The groups can have an unlimited number of users. We will cover how to manage user accounts on page 3.

1. *To add, modify, and delete groups*, select Tools > Manage Groups from the main menu. The following dialog will appear, showing all the currently-configured groups:

2. *To add a new group:* Click the ‘Add New…’ button. The following dialog box appears:

The Group Name is typically a department (Internal Investigations, Detectives, Homicide, etc.), but can be anything that is meaningful to the department.

The Group Members box allows the administrator to select the members of the group by checking the box to the left of the user names or using the ‘Select All’ or ‘Clear All’ buttons.

NOTE: Deleting a group will not delete the users and sessions associated with the group; it will merely de-associate the group’s sessions from the group’s members, i.e. the members of the deleted group will no longer be able to access the sessions in the deleted group, except if a user owns/created any particular session.

c. ***User Accounts:*** Each user of the CaseCracker system should have their own user account, which allows the user to log into the system.

1. *To add, modify, and delete user accounts:* Select Tools > Manage Users from the main menu. The following dialog will appear, showing all the currently-configured user accounts:

2. *To add a new user:* Click the 'Add New…' button. The following dialog box appears:

The Full Name of the user is typically their first and last names, potentially including their rank.

The Sort By field is used for sorting this user's name appropriately in lists. It is typically their last name. As you enter the user's Full Name, the system will attempt to guess the appropriate value for the Sort By field, but you may need to correct it.

The Password and Confirm Password fields allow you to set the user's initial password. The default password is 'welcome'.

If the 'Force user to change password on next login' box is checked, the user will be required to change their password the next time they log in. We recommend checking this box.

The Permissions field allows you to determine the permissions for the user, which include:

- The Annotate permission allows a user to add, edit, and delete annotations and flags during playback. It is always possible to add annotations and flags during recording, regardless of the setting in this dialog.
- The Export permission allows a user to burn a DVD or to export an audio file a video file, a snapshot, the list of annotations and other PDF/CSV reports.
- The Backup/Restore permission allows a user to backup a session that can later be restored to CaseCracker. See pages 13-15 for more information on how to backup/restore. This will provide an archival copy of the interview with annotations and flags that can be restored to CaseCracker later.

  NOTE: This file can only be read by CaseCracker software.

- The Delete permission allows a user to immediately delete a session, to change its deletion date, and to prevent it from being automatically deleted. The Delete permission has 3 options: no one can delete the session, only the user who owns the session may delete it, and user may delete any session regardless of if they own the session or not.
- The Administrator permission gives the user administrator level access to the system. Administrators are denoted with a red icon in the User Manager dialog.

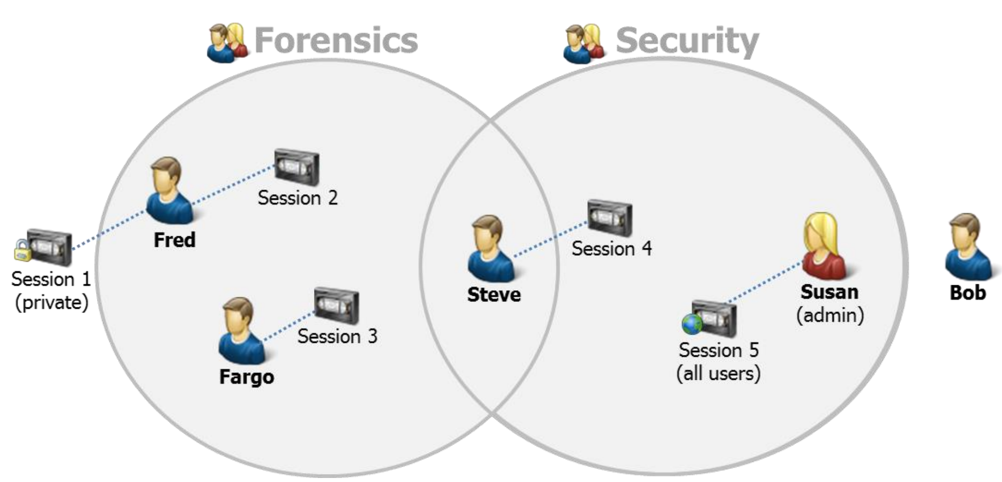
  NOTE: We recommend you limit the number of people who have this permission, as it is possible for a user with administration privileges to inadvertently misconfigure important system parameters.
- The Groups field is used to select the groups that the user will be a member of. If no groups are selected, the user will only see their own interviews or any interview marked for "All Users" by his/her original author.

3. *To edit an existing user:* Select the user's name from the User Manager and click the 'Edit…' button. See the description, on page 4, under *To add a new user* for an explanation of this dialog box.

4. *To delete an existing user:* Select the user's name from the User Manager and click the 'Delete…' button. You will be prompted to confirm your action.

   NOTE: Deleting a user will not delete the video(s) associated with that particular user. Those videos will still be accessible by members of the group the video is associated with. If the video was marked as "Interviewer Only", an administrator may assign the video to a new user or group using the "Change Session Information" option.

For an example of group and user accounts, consider a CaseCracker system configured with the following users and groups:



The *Forensic* group members are Fred, Fargo, and Steve. The *Security* group members are Steve and Susan.

- **Fred** can see sessions 1, 2, 3 and 5 because he is the owner of session 1 and 2; session 3 is in the *Forensic* group, which he is a member of; and session 5 is available to 'All Users'.

- **Fargo** can see sessions 2, 3 and 5 because he is the owner of session 3; session 2 is in the *Forensic* group, which he is a member of; and session 5 is available to 'All Users'. He cannot see session 1, as *Fred* kept this session private; and he cannot see session 4, as Steve has recorded this session in the *Security* group.

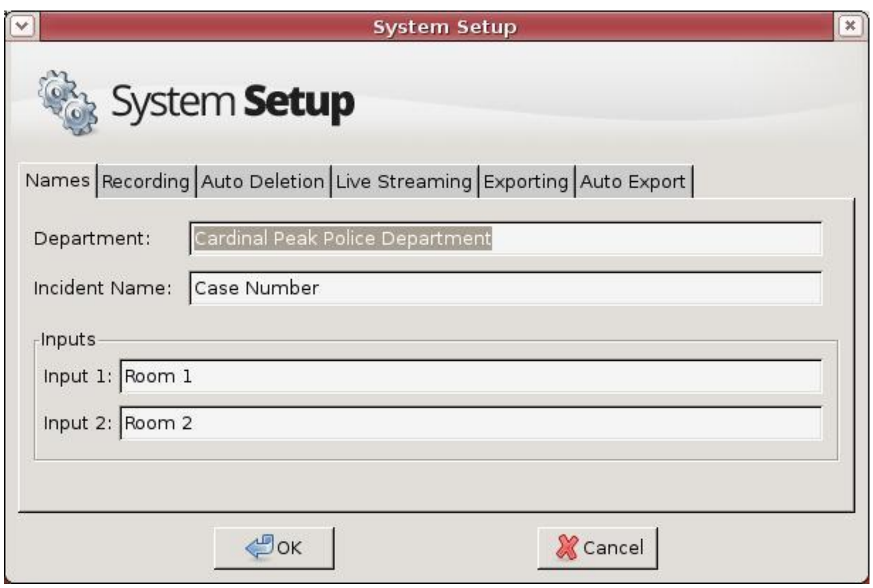
- **Steve** can see sessions 2, 3, 4 and 5 because he is the owner of session 4; session 2 and 3 are in the *Forensic* group, which he is a member of; and session 5 is available to 'All Users'. He cannot see session 1, as *Fred* kept this session private.

- **Susan** can see all sessions because she is an administrator. If she wasn't an administrator she would only see session 4 and 5 because she is the owner of session 5; session 4 is in the *Security* group, which she is a member of.

- **Bob** can only see session 5 because this session is available to 'All Users'. He cannot see session 1, because *Fred* kept this session private, or sessions 2, 3, or 4 because he is not member of either of the groups associated with these sessions.

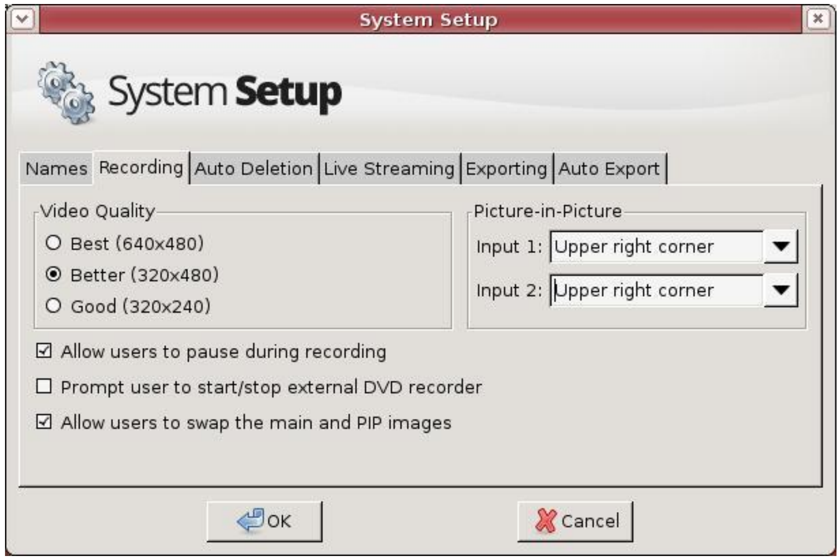
3. <u>Setup</u>

To enter setup, select Tools > Setup and the following dialog will appear:



a. Select the <u>Names</u> tab to enter the name of the <u>Department</u>. The <u>Incident Name</u> field is customizable to your agency, for example, Case Number. The <u>Inputs</u> field refers to the names of up to two recording inputs (i.e. your Room names).

b. Select the Recording tab to configure recording parameters:



The video quality setting controls the tradeoff between high video quality, on the one hand, and longer recording capacity, on the other.

- Good quality is designed to be sufficient for most applications. It is roughly equivalent to VCR quality.

- Better quality offers higher video resolution and clarity. It is better than VCR quality, but not quite as good as movie-level DVD quality.

- Best quality setting provides the highest resolution available, however, it places demand on the system's CPU and results in large file sizes.

- Picture-in-Picture (PIP) enables or disables PIP and determines in which quadrant on the monitor the small box appears.

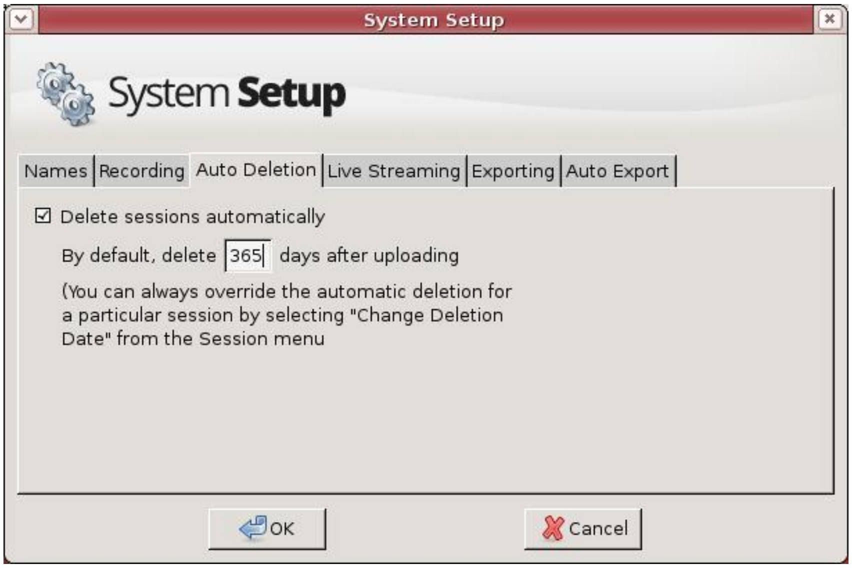
- If the Allow users to pause during recording box is checked, users will be permitted to pause recording.

- If the Prompt user to start/stop external DVD recorder box is checked, the user will be prompted to start an external DVD recorder at the start of each session and stop at the end of each session.

- If the Allow users to swap the main and PIP images box is checked, users will be able to swap the main camera view with the PIP camera view during recording.

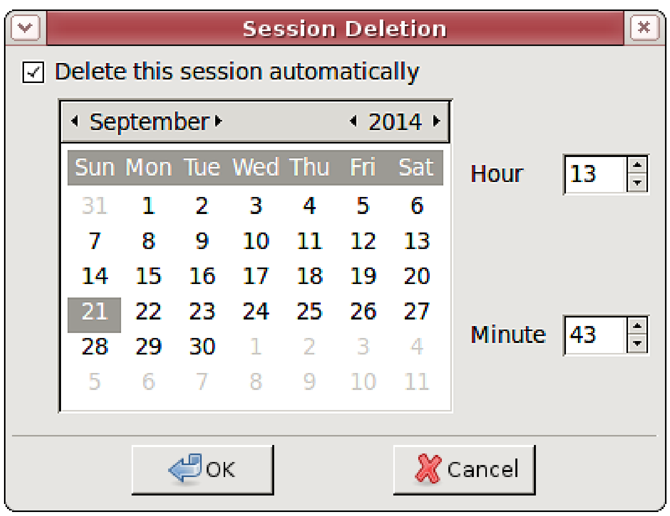
  NOTE: All "swaps" that are made during recording will show on the final recording.

c. Select the Auto Deletion tab to configure deletion settings:



If the 'Delete sessions automatically' box is checked, then the system will automatically delete the video after the specified number of days from the time of recording.

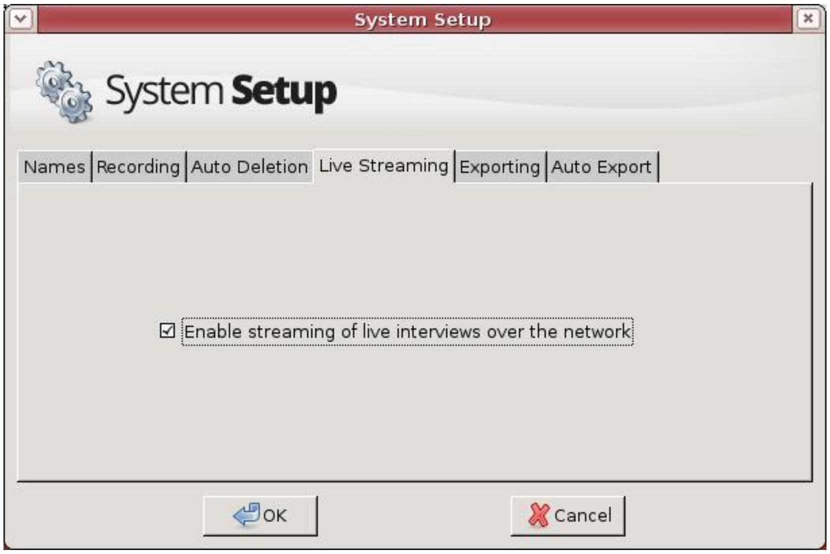
1. *To override the automatic deletion for any particular session:* Select the session in the main window, and then select Session > Change Deletion Date from the main menu. The following dialog box appears:



From this dialog, you can select a new date and time for the session to be automatically deleted. You can also keep it until it is manually deleted, by turning off the 'Delete this session automatically' checkbox. These changes will only affect this session.

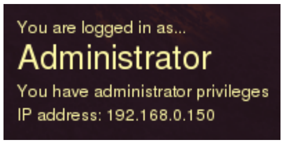
2. *To delete a session immediately:* Select the session in the main window and then select Session > Delete Now from the menu.

d. Select the Live Streaming tab to enable or disable the OnDemand feature.



If the "Enable streaming of live interviews over the network" box is checked, users can use the OnDemand web interface to remotely view both live and previously-recorded sessions. Unchecking this box disables the OnDemand web interface.

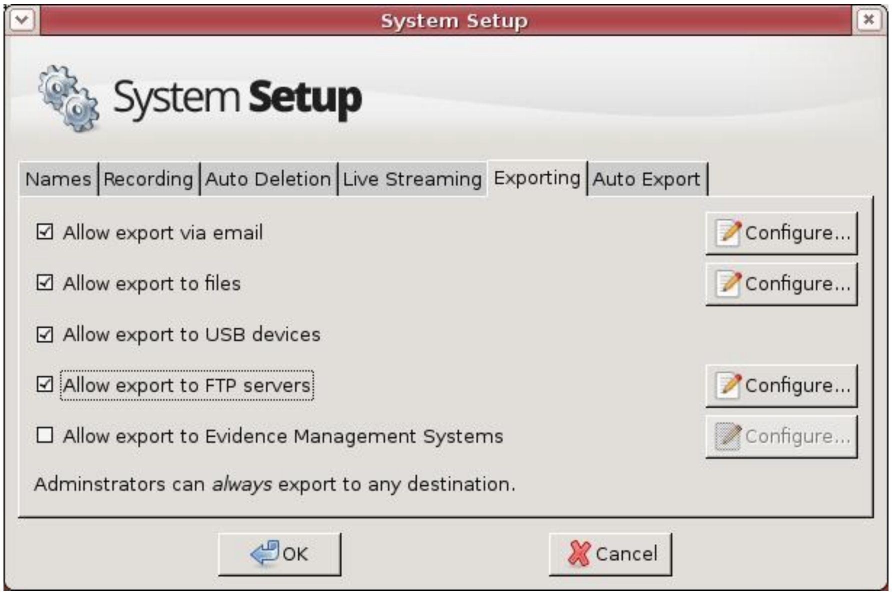
To log in to OnDemand from a remote PC, users must browse to the IP address shown at the bottom left hand corner of the CaseCracker main screen:



OnDemand is supported on Windows Vista, Windows 7, and Windows 8 running Internet Explorer 9-11. More information about OnDemand can be found in the "OnDemand SetUp Manual" document which is located on our website at www.casecracker.com under the resources tab or from your CaseCracker workstation under the Help Menu.

e. The Exporting tab allows exporting of video, audio, image snapshots, annotations, event log, and session report to a variety of different destinations. In order for this functionality to work, you will need to connect CaseCracker to your network and configure the following destination(s) per your department's policy.

Regardless of the settings on this tab, Users who are not Administrators will only be able to export video, audio, image snapshots, and annotations if they have "Export" permission for the session in question; see page 4.

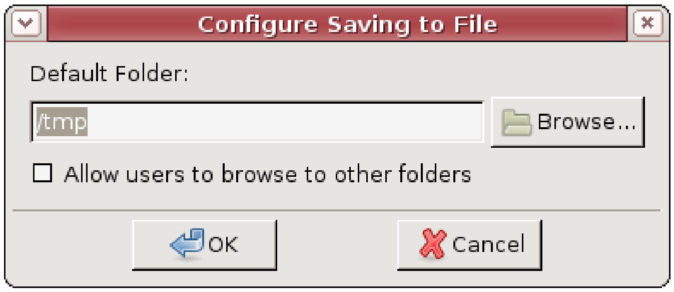


- Allow export via email: If you would like to enable email, check the “Allow export via email” box and click the “Configure” button to the right to view the window below. Enter in your department’s outgoing mail server, authentication (if necessary), and a “from” email address. Click the test button to send a test email to confirm settings.

  NOTE: Video file sizes are limited using this export option.

- Allow export to files: If you would like to enable export to the filesystem (which could be a location on your Department’s network if this CaseCracker workstation is configured as a network client), check the “Allow export to files” box and click the

"Configure" button to the right to view the window below. Use the browse button to choose the default folder that files will be exported to. Checking the "Allow users to browse to other folders" box will allow users to change to other folders within the filesystem.

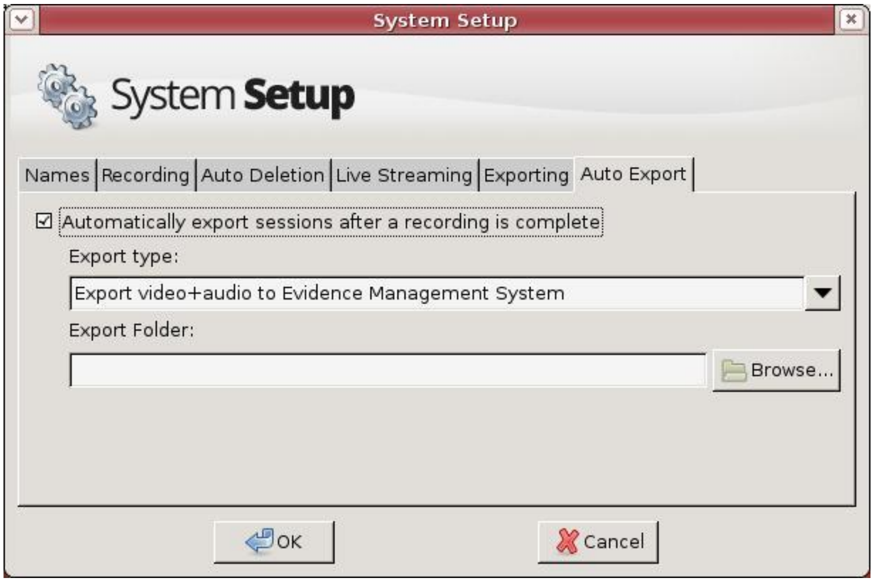


- Allow export to USB devices: If you would like to enable export to USB devices, check the "Allow export to USB devices" box.

- Allow export to FTP servers: If you would like to enable export to a FTP server, check the "Allow export to FTP servers" box and click the "Configure" button to the right to view the window below.

- Allow export to Evidence Management System: If your department uses an Evidence Management System, check the "Allow export to Evidence Management System" box and click the "Configure" button.

f. The Auto Export feature will allow CaseCracker to automatically export a session to an Evidence Management System or as an MPEG-4 to a file location immediately after the session has finished recording.



4. Disk Usage

Your system has been configured with internal hard disk(s) for video and audio storage (this is in addition to the system's root hard disk, which stores the operating system and other software, as well as numerous configuration files). It is possible to add external storage to the system by purchasing one or more Network-Attached Storage (NAS) devices.

NOTE: Due to security considerations and the high data access rates that are required for proper operation, Cardinal Peak only certifies the system for use with certain approved NAS devices. Please contact Cardinal Peak for details.

1. *To see a list of the configured disks and NAS units:* Select Tools > Manage Disk Storage from the main menu. The following dialog box appears:

The first entry in the list, usually '/data1', refers to the CaseCracker workstation's internal data disk.

Any NAS units you have configured will also appear in this list.

g. *To ascertain a particular session's size and storage location:* Select the session from the main window, and the select Session > Info from the menu. The size and storage location are listed in the bottom of the info window.

h. *To add a NAS to the system:* Please contact Cardinal Peak support for instructions.

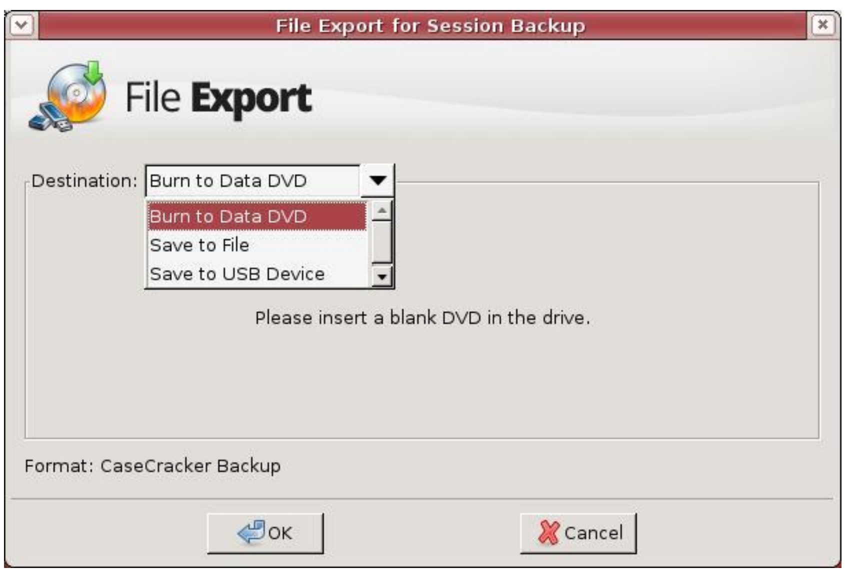
i. *To delete a NAS from the system:* Select the NAS from the list, and click the 'Delete…' button. You will be prompted to confirm your action.

NOTE: When you delete a NAS from the system, you are also deleting all the video stored on that NAS!

5. Backing Up and Restoring Sessions

a. *Backup:* To conserve storage on the hard disk, you can backup a session that can be loaded back to CaseCracker later. You may backup to DVD, file location, or USB device. Select one or more sessions and go to File > Backup session to view the window below. Select the destination and click OK. This will give you an archival copy of the interview with annotations and flags that can be restored to CaseCracker later.

NOTE: This file can only be read by CaseCracker software.



b. *Restoring from a DVD backup:*

1. Insert the DVD backup of the session that you would like to restore into the CD-ROM drive on the CaseCracker unit.

2. Log into CaseCracker as an Administrator or a user with administrative privileges.

3. From the “CaseCracker Main Window”, escape to the shell by selecting Help > Escape to Shell (advanced).

   Type the following into the shell window:

   `cd /media` (press Enter)

   `ls` (press Enter)

   At this point there should be a listing in light blue saying "cdrom"

   If you do not see this, then type:

   `sudo mkdir cdrom` (type your password and press Enter)

   then:

   `sudo mount -t udf /dev/cdrom /media/cdrom` (type your password and press Enter)

4. If you are restoring from a backup created with an earlier version than CaseCracker 3.0 than do the following. Otherwise, skip to step 7.

   Type the following into the shell window:

   `mkdir /tmp/backup-restore` (press Enter)

   `cd /tmp/backup-restore` (press Enter)

   `tar xf /media/cdrom/session-XXX.nut`

   NOTE: Substitute “XXX” with the session ID in the command above.

5. Return to the “CaseCracker Main Window” and select File > Restore from Backup.

6. In the “Please locate the sessioninfo file…” window, double-click on media in the “Folders” column followed by double-clicking cdrom also in the “Folders” column.

   NOTE: If you followed step 6 you will double-click tmp in the “Folders” column followed by double-clicking backup-restore also in the “Folders” column.

7. In the “Files” column, select sessioninfo and select OK.

The restore process will start. Depending on the size of the session it may take several minutes to restore.

8. Once the session has completed restoring, click OK.

9. Return to the Shell window that was previously opened and type the following:

   ```
   sudo umount /media/cdrom
   ```

   Press Enter.

10. Close the shell window.

11. Eject the backup DVD from the CD-ROM drive.

c. *Restoring from a USB backup:*

1. Plug in the USB drive containing the session that you would like to restore to the CaseCracker unit.

2. Log into CaseCracker as an Administrator or a user with administrative privileges.

3. From the “CaseCracker Main Window,” go to File > Restore from Backup.

4. Double-click on media/

5. Double-click on the USB drive.

6. Double-click on the session you would like to restore.

7. Double-click on the file sessioninfo.

8. After the session restores, you must first unmount the USB drive. To do so, select the Help > Escape to Shell (advanced).

9. Type the following into the shell window:

   ```
   umount /media/XXX
   ```

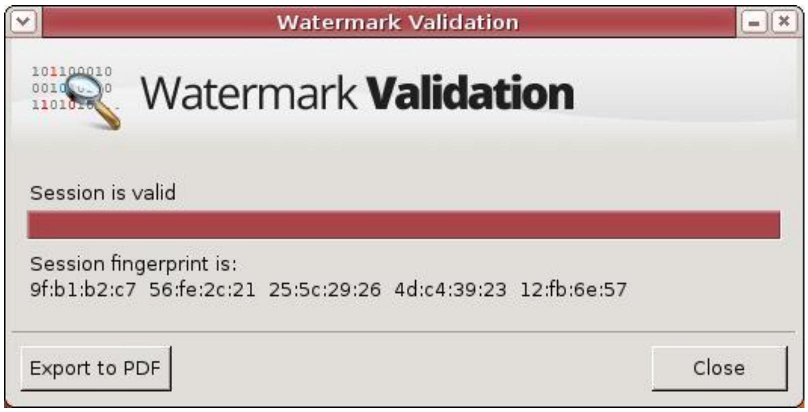
   NOTE: Substitute “XXX” with the name of the USB drive in the command above.

10. Remove the USB drive from the CaseCracker.

6. Validating Watermarks

CaseCracker's watermarking feature verifies that the audio and video associated with a session have not been modified since recording.

a. To validate an interview, highlight the session and select Session > Validate Watermarks. The following window will appear:



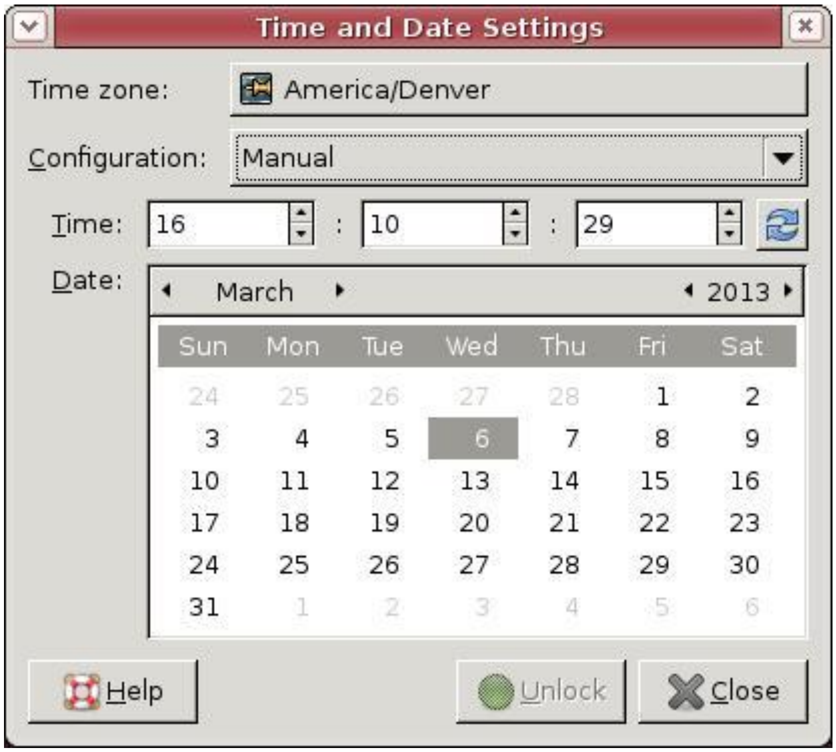
The Export to PDF button will produce a PDF of the session fingerprint.

7. Setting the Time and Date

In order for time and date stamps to work correctly, it is important that the system has an accurate idea of the current time. There are two ways to configure time:

- Using the static method, you simply set the system clock to the correct time and date; from there, the system will keep reasonably accurate time, including making adjustments for daylight savings time as needed.
- Using the dynamic method, your system can be configured to periodically synchronize to the current time over the Internet, using a publicly available timeserver.

a. To configure the time and date, select Tools > Set Time/Date from the main menu. The following dialog will appear:



- To configure the current date and time statically, simply enter the values here and then select a <u>Time Zone</u>.

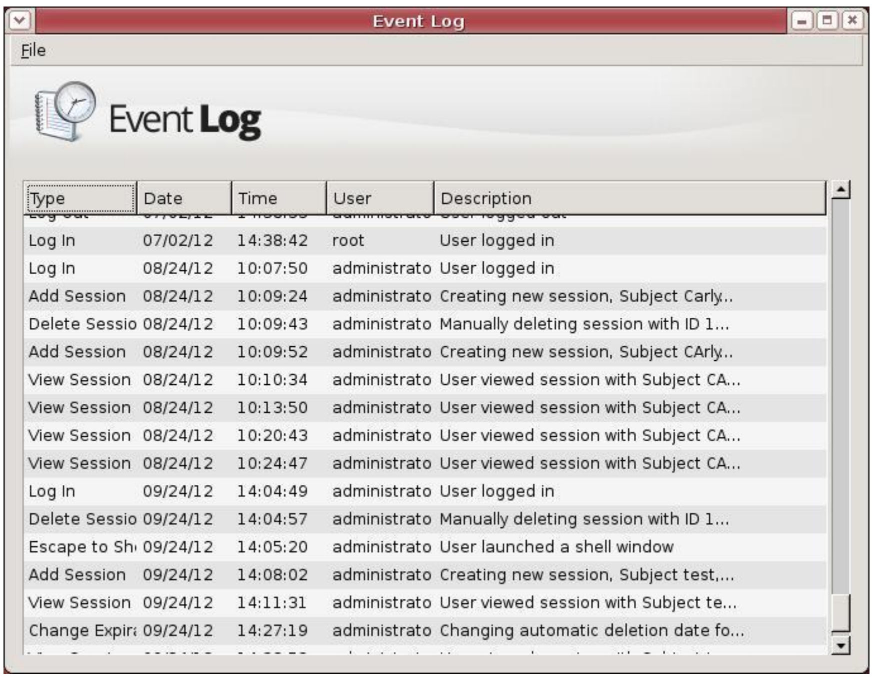
- To configure the system to dynamically synchronize over the network with a public server, choose “Keep synchronized with internet servers” from the Configuration drop down menu. The following window will appear prompting you to choose a time server.

8. Viewing the Event Log

The following actions are logged to the system event log:

- Add (record) a session
- View a session
- Change a session's expiration date
- Delete session
- Add user
- Edit user
- Delete user
- Add filesystem
- Delete filesystem
- Burn DVD
- Change permissions
- Log in
- Log out
- Escape to shell

a. *To access the system event log:* Select File > View Event Log from the main menu. The Event Log viewer appears:



Events are sorted in chronological order.

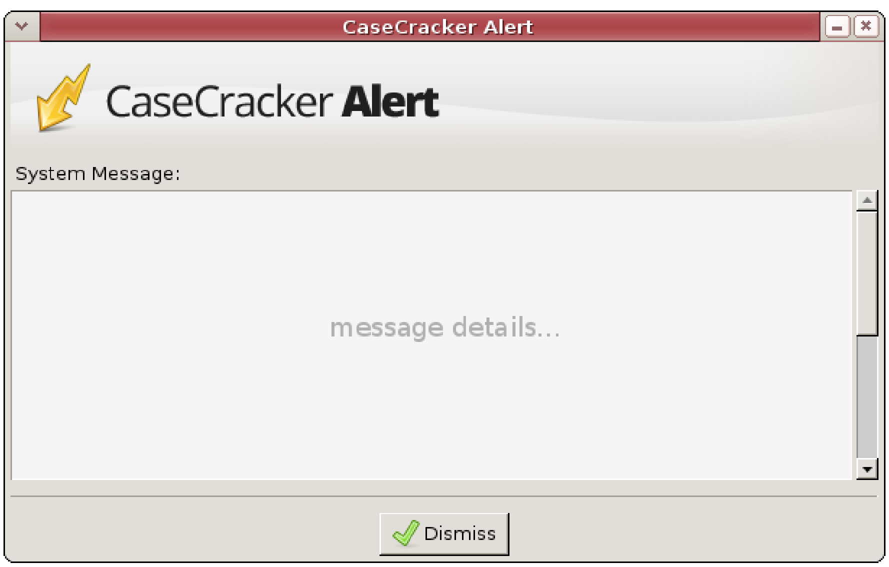
b. *To get more details on any event:* Select it and double-click on it.

c. *To export the Event Log:* Select File > Export Event Log from the Event Log menu. The event log can be exported as a CSV file (compatible with Microsoft Excel) or PDF.

d. *To close the Event Log:* Select File > Close from the Event Log menu, or click the 'X' in the upper right corner of the window.

9. <u>System Alerts</u>

In case of a system event that needs user attention; the "CaseCracker Alert" dialog will be displayed with information about the problem:



There are two types of system alerts:

a. *RAID Alert*: In the unlikely event of a hard drive failure, we've added a special RAID monitoring function to alert the operator of a problem. This feature is only available in some systems and typically means a replacement drive may be needed, soon, to prevent data loss. You should contact CaseCracker support immediately and provide the information displayed in the alert dialog. You can press the "Dismiss" button to close the dialog. The system will keep reminding you if this problem continues.

Important: Failure to address this error could result in a loss of data.

b. *Low Battery Warning*: This alert indicates the laptop battery charge is getting low. Please connect the laptop to the power outlet. Press the "Dismiss" button to close the dialog.

Appendix

Support Tools

In the event your system needs technical support, there are three options available from the Help menu when you're logged in with administrator privileges that aid Cardinal Peak in remotely debugging your system.

Although you should never need to access these options unless instructed to do so by Cardinal Peak, the functionality is as follows:

- Install New Version allows you to install CaseCracker upgrades from an upgrade CD (software support contract required).
- Escape to Shell allows you to access a Linux command prompt. It is intended for expert users only, as it is possible to inadvertently miss configure your system.
- Burn Diagnostic CD allows you to burn a CD that contains a reasonably complete snapshot of the state of your system. You can then send this CD or email the file to Cardinal Peak for analysis.
- Allow Remote Login allows Cardinal Peak to login to your CaseCracker for diagnostic purposes. Your system must be connected to the network to allow remote login.
- Play Test Sound is used to test audio configuration.
- USB Contact Closure Test checks whether or not any USB devices are connected and working properly.

Initial Configuration Checklist

The following checklist provides a handy reference to ensure that you've performed initial system configuration correctly:

____Change Administrator password

____Add groups to the system (optional)

____Add users to the system

____Configure automatic deletion policy

____Configure recording parameters

____Set the time and date

____Configure export options