SafeCopy Accreditation

Electronic Discovery

Electronic Discovery (also ***E-Discovery*** or ***eDiscovery***) refers to discovery in legal proceedings such as litigation, government investigations, or Freedom of Information Act requests, where the information sought located, secured, and searched with the intent of using it as evidence in a civil or criminal legal case in electronic format (often referred to as electronically stored information or ESI). Electronic discovery is subject to rules of civil procedure and agreed-upon processes, often involving review for privilege and relevance before data are turned over to the requesting party.

E-discovery can be carried out offline on a particular computer or it can be done in a network. Court-ordered or government sanctioned hacking for the purpose of obtaining critical evidence is also a type of e-discovery.

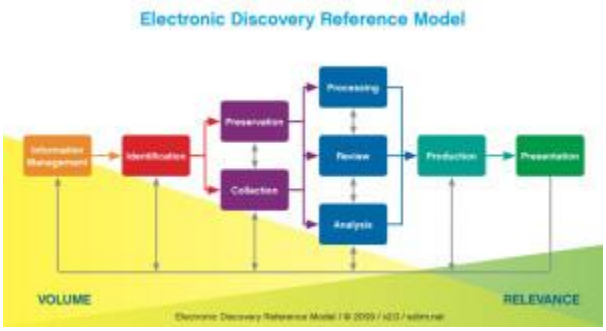
Computer Forensics, also called cyberforensics , is a specialized form of e-discovery in which an investigation is carried out on the contents of the hard drive of a specific computer. After physically isolating the computer, investigators make a digital byte-by-byte copy of the hard drive and the original computer is usually locked in a secure facility to maintain its pristine condition. All investigation is done on the digital copy.

Electronic information is considered different from paper information because of its intangible form, volume, transience and persistence. The nature of digital data makes it extremely well-suited to investigation. For one thing, digital data can be electronically searched with ease, whereas paper documents must be scrutinized manually. Furthermore, digital data is difficult or impossible to completely destroy, particularly if it gets into a network. This is because the data appears on multiple hard drives and because digital files, even if deleted, can be undeleted. In fact, the only reliable way to destroy a computer file is to physically destroy every hard drive where the file has been stored.

Electronic information is usually accompanied by metadata that is not found in paper documents and that can play an important part as evidence (for example the date and time a document was written could be useful in a copyright case). The preservation of metadata from electronic documents creates special challenges to prevent spoliation. In the United States, electronic discovery was the subject of amendments to the Federal Rules of Civil Procedure (FRCP), effective December 1, 2006, as amended on December 1, 2015. In addition, state law now frequently also addresses issues relating to electronic discovery. Other jurisdictions around the world also have rules relating to electronic discovery, including Part 31 of the Civil Procedure Rules in England and Wales.

Stages of Process

The Electronic Discovery Reference Model (EDRM) is a ubiquitous diagram that represents a conceptual view of these stages involved in the e-discovery process.



Information Governance

Information Governance, or **IG**, is the management of information at an organization. Information governance balances the use and security of information. Information governance helps with legal compliance, operational transparency, and reducing expenditures associated with legal discovery. An organization can establish a consistent and logical framework for employees to handle data through their information governance policies and procedures.

Identification

The Identification Phase is when potentially responsive documents are identified for further analysis and review. In Zubulake v. UBS Warburg, Hon. Shira Scheindlin ruled that failure to issue a written legal hold notice, whenever litigation is reasonably anticipated, will be deemed grossly negligent. This created the idea of legal holds, eDiscovery, and electronic preservation.
Custodians who are in possession of potentially relevant information or documents are identified. To ensure a complete identification of data sources, data mapping techniques are often employed. Since the scope of data can be overwhelming in this phase, attempts are made to reduce the overall scope

during this phase - such as limiting the identification of documents to a certain date range or search terms to avoid an overly burdensome request.

Preservation

A duty to preserve begins upon the reasonable anticipation of litigation. During preservation, data identified as potentially relevant is placed in a legal hold. This ensures that data cannot be destroyed. Care is taken to ensure this process is defensible, while the end-goal is to reduce the possibility of data spoliation or destruction. Failure to preserve can lead to sanctions. Even if the court ruled the failure to preserve as negligence, they can force the accused to pay fines if the lost data puts the defense "*at an undue disadvantage in establishing their defense.*"

Collection

Once documents have been preserved, collection can begin. Collection is the transfer of data from a company to their legal counsel, who will determine relevance and disposition of data. Some companies that deal with frequent litigation have software in place to quickly place legal holds on certain custodians when an event such as legal notice is triggered, and begin the collection process immediately. Other companies may need to call in a digital forensics expert to prevent the spoliation of data. The size and scale of this collection is determined by the identification phase.

Processing

During the processing phase, native files are prepared to be loaded into a document review platform. Often, this phase also involves the extraction of text and metadata from the native files. Various data culling techniques are employed during this phase, such as deduplication and de-NISTing. Sometimes native files will be converted to a petrified, paper-like format (such as PDF or TIFF) at this stage, to allow for easier redaction and bates-labeling. Modern processing tools can also employ advanced analytic tools to help document review attorneys more accurately identify potentially relevant documents.

Review

During the review phase, documents are reviewed for responsiveness to discovery requests and for privilege. Different document review platforms can assist in many tasks related to this process, including the rapid identification of potentially relevant documents, and the culling of documents according to various criteria (such as keyword, date range, etc.). Most review tools also make it easy for large groups of document review attorneys to work on cases, featuring collaborative tools and batches to speed up the review process and eliminate work duplication.

Production

Documents are turned over to opposing counsel, based on agreed-upon specifications. Often this production is accompanied by a load file, which is used to load documents into a document review

platform. Documents can be produced either as native files, or in a petrified format (such as PDF or TIFF), alongside metadata.

Types of ESI

Any data that is stored in an electronic form may be subject to production under common eDiscovery rules. This type of data has historically included email and office documents, but can also include photos, video, databases, and other filetypes.

In the process of electronic discovery, data of all types can serve as evidence. This can include text, images, calendar files, databases, spreadsheets, audio files, animation, Web sites and computer programs. Even malware such as viruses, trojans and spyware can be secured and investigated. Email can be an especially valuable source of evidence in civil or criminal litigation, because people are often less careful in these exchanges than in hard copy correspondence such as written memos and postal letters.

Also included in e-discovery is ***raw data***, which Forensic Investigators can review for hidden evidence. The original file format is known as the ***native*** format. Litigators may review material from e-discovery in one of several formats: printed paper, ***native file***, or a petrified, paper-like format, such as PDF files or TIFF images. Modern document review platforms accommodate the use of native files, and allow for them to be converted to TIFF and Bates-stamped for use in court.

The nature of digital data makes it extremely well-suited to investigation. For one thing, digital data can be electronically searched with ease, whereas paper documents must be scrutinized manually. Furthermore, digital data is difficult or impossible to completely destroy, particularly if it gets into a network. This is because the data appears on multiple hard drives and because digital files, even if deleted, can be undeleted. In fact, the only reliable way to destroy a computer file is to physically destroy every hard drive where the file has been stored.

Electronic Messages

In 2006, the U.S. Supreme Court's amendments to the Federal Rules of Civil Procedure created a category for electronic records that, for the first time, explicitly named emails and instant message chats as likely records to be archived and produced when relevant.

One type of preservation problem arose during the Zubulake v. UBS Warburg LLC lawsuit. Throughout the case, the plaintiff claimed that the evidence needed to prove the case existed in emails stored on UBS' own computer systems. Because the emails requested were either never found or destroyed, the court found that it was more likely that they existed than not. The court found that while the corporation's counsel directed that all potential discovery evidence, including emails, be preserved, the staff that the directive applied to did not follow through. This resulted in significant sanctions against UBS.

Some archiving systems apply a unique code to each archived message or chat to establish authenticity. The systems prevent alterations to original messages, messages cannot be deleted, and the messages cannot be accessed by unauthorized persons.

The formalized changes to the Federal Rules of Civil Procedure in December 2006 and in 2007 effectively forced civil litigants into a compliance mode with respect to their proper retention and management of electronically stored information (ESI). Improper management of ESI can result in a finding of spoliation of evidence and the imposition of one or more sanctions including an adverse inference jury instructions, summary judgment, monetary fines, and other sanctions.

In some cases, such as Qualcomm v. Broadcom, attorneys can be brought before the bar and risk their livelihood.

Databases and Other Structured Data

Structured data typically resides in databases or datasets. It is organized in tables with columns and rows along with defined data types. The most common are Relational Database Management Systems (RDBMS) that are capable of handling large volumes of data such as Oracle, IBM DB2, Microsoft SQL Server, Sybase, and Teradata. The structured data domain also includes spreadsheets (not all spreadsheets contain structured data, but those that have data organized in database-like tables), desktop databases like FileMaker Pro and Microsoft Access, structured flat files, xml pages, data marts, data warehouses, etc.

Voicemail

Voicemail is often discoverable under electronic discovery rules. Employers may have a duty to retain voicemail if there is an anticipation of litigation involving that employee.

Reporting Formats

Although petrifying documents to static image formats (tiff & jpeg) had become the standard document review method for almost two decades, native format review has increased in popularity as a method for document review. Because it requires the review of documents in their original file formats, applications and toolkits capable of opening multiple file formats have also become popular. This is also true in the ECM (Enterprise Content Management) storage markets which are converging quickly with ESI technologies.

Petrification involves the conversion of native files into an image format that does not require use of the native applications. This is useful in the redaction of privileged or sensitive information, since redaction tools for images are traditionally more mature, and easier to apply on uniform image types. Efforts to redact similarly petrified PDF files have resulted in the removal of redacted layers and exposure of redacted information, such as social security numbers and other private information.

Traditionally, electronic discovery vendors had been contracted to convert native files into TIFF images (example: 10 images for a 10-page Microsoft Word document) with a load file for use in image-based discovery review database applications. Increasingly, database review applications have embedded native file viewers with TIFF-capabilities. With both native and image file capabilities, it could either increase or decrease the total necessary storage, since there may be multiple formats and files associated with each individual native file. Deployment, storage, and best practices are becoming especially critical and necessary to maintain cost-effective strategies.

Structured data are most often produced in delimited text format. When the number of tables subject to discovery is large or relationships between the tables are of essence, the data are produced in native database format or as a database backup file.

Common Issues

A number of different people may be involved in an electronic discovery project: lawyers for both parties, forensic specialists, IT managers, and records managers, amongst others. Forensic examination often uses specialized terminology (example: *image* refers to make a picture copy of a document (tiff and/or pdf) or the acquisition of digital media, which can lead to confusion).

While attorneys involved in case litigation try their best to understand the companies and organization they represent, they may fail to understand the policies and practices that are in place in the company's IT department. As a result, some data may be destroyed after a legal hold has been issued by unknowing technicians performing their regular duties. To combat this trend, many companies are deploying software which properly preserves data across the network, preventing inadvertent data spoliation.

Given the complexities of modern litigation and the wide variety of information systems on the market, electronic discovery often requires IT professionals from both the attorney's office or vendor, and the parties to the litigation to communicate directly to address technology incompatibilities and agree on production formats. Failure to get expert advice from knowledgeable personnel often leads to additional time and unforeseen costs in acquiring new technology or adapting existing technologies to accommodate the collected data.

Emerging Trends

TECHNOLOGY-ASSISTED REVIEW

Technology-assisted review (TAR) - also known as computer-assisted review or predictive coding -involves the application of supervised machine learning or rule-based approaches to infer the relevance, privilege, or other categories of interest of ESI. Technology-assisted review has evolved rapidly since its 2005 inception.

Following research studies indicating its effectiveness, TAR was first recognized by a U.S. court in 2012, by an Irish court in 2015, and by a U.K. court in 2016. In 2015 a U.S. court declared that it is "*black letter law that where the producing party wants to utilize TAR for document review, courts will permit it*".

Convergence with information governance

Anecdotal evidence for this emerging trend points to the business value of information governance (IG), defined by Gartner as the specification of decision rights and an accountability framework to encourage desirable behavior in the valuation, creation, storage, use, archival, and deletion of information. It includes the processes, roles, standards, and metrics that ensure the effective and efficient use of information in enabling an organization to achieve its goals.

As compared to eDiscovery, information governance as a discipline is rather new. Yet there is traction for convergence [b]. eDiscovery - as a multibillion-dollar industry - is rapidly evolving, ready to embrace optimized solutions that strengthen cyber security (for cloud computing).

Since the early 2000s eDiscovery practitioners have developed skills and techniques that can be applied to information governance. Organizations can apply the lessons learned from eDiscovery to accelerate their path forward to a sophisticated information governance framework.

E-discovery is an evolving field that goes far beyond mere technology. It gives rise to multiple legal, constitutional, political, security and personal privacy issues, many of which have yet to be resolved.

IMPORTANCE OF ELECTRONIC FILE COLLECTIONS

Incomplete and undocumented electronic discovery collections occur every day and the results are costly to both clients and their legal counsel. Litigation is what attorneys do for a living so clients expect their attorneys to guide them through the entire process. However, litigation is a burden to clients in that it is both costly and distracts client staff from their core business. In the past, few would argue that the failure to properly advise a client on how a file cabinet of physical documents should be handled during litigation was potential malpractice.

Now that most documents are electronic and the file cabinets are computer networks, the failure to properly advise a client on handling electronic data is potential malpractice in the form of spoliation and missing evidence. Advising clients about proper file collection methods must be considered from the beginning of each case. Using processes and applications that preserve and verify collected electronic files with minimal impact on client systems is critical. Without them, creating defensible and verifiable electronic discovery productions and evidence authentication is difficult, if not impossible.

COMMON MISTAKES IN FILE COLLECTIONS

Normally, a discovery request is created and the corporate IT department or other client employees copy relevant files or directories to disks or a USB drive. From the client's perspective, this is the least costly way to collect data. However, it can be the most costly way in the long run. The integrity of files collected from corporate servers and client machines are in jeopardy because many electronic document collections are completed using tools that lack the ability to confirm results and properly document the process. Attorneys need to advise clients as to proper collection techniques. While not every case warrants a full third party forensic collection, every case does warrant a defensible and verifiable electronic data collection process. Discussion about when a full third party forensic collection is needed is beyond the scope of this article but the possible need must be considered before the decision is made to move forward with a different class of collection.

INCOMPLETE FILE COLLECTIONS

Electronic file collection projects can take many hours or days and contain hundreds of thousands, if not millions, of files. The software used to copy and burn files often lack a verification process; therefore, files that are skipped, partially copied or corrupted go unnoticed.

Incomplete and corrupted file collections pose an unseen danger as reviewers may never know that a relevant file was unavailable or unsearchable. The best way to ensure that all relevant files are identified, properly copied and delivered without error includes:

- Hash verification for every file.
- Log incomplete copies, files in use or skipped files.
- Maintain descriptive error logs.
- Proactive error reporting and feedback.
- Verification (chain of custody) log.

Recommending that clients use file collection methods that include these options helps ensure all electronically produced files are intact and available for review.

COMMON PROBLEMS IN E-DISCOVERY COLLECTIONS

The most common issues in e-discovery that are overcome using proper e-discovery software

1. Files in Long Paths Are Skipped

Anyone who has worked in E-Discovery for any length of time has encountered problems working with files that are located in paths greater than 255 characters.

Microsoft Windows and many other applications can't access files where the total number of characters (including folder and file name) exceeds 255.

It is common for a custodian's computer or the company's file shares to store files in long paths. Missing all files that are stored in long paths is a frequent problem when backing up or collecting files. Often there is no warning or notification that a long file path was encountered; therefore, users are unaware that potentially critical information was not captured.

The problem is compounded when opposing counsel begins asking questions as to why specific documents weren't produced. One of the hardest obstacles to overcome is the perception that documents were purposely withheld or a less than credible collection process was used to produce electronic data.

2. Altered File and Folder Timestamps

During normal file copy operations, Microsoft Windows creates new and updates existing file system timestamps on the new copies as well as the originals. This often causes problems later when the

file metadata is imported into attorney review platforms and needs to be organized or searched. Creating an accurate timeline of events is a critical component in the discovery process and not having access to the original file timestamps can quickly become an issue. Microsoft Office and other applications files have internal metadata that can work as a backup to help determine the date a file was created or edited. However, internal timestamps will still differ from the file system timestamps.

Additionally, many file types do not contain internal metadata and the only record of when a file was created is contained within the file system metadata. It is critical to use copy utilities that can preserve both file and folder timestamps during an e-discovery collection to ensure proper timelines can be created during review.

3. Incomplete Collection Projects

Recovering from interruptions, identifying missed files and easily correcting is not possible using Microsoft Windows file copying as well as many other free and paid copy applications. Additionally, several disk imaging applications must restart if an error occurs while writing files to the container.

Network outages, computer restarts and end user job cancellation are very common during e-discovery collections. The ability to easily identify which files had trouble as well as which ones remain to be copied is critical to ensure the collection is defensible.

Those who have been involved in any kind of large scale collection or backup project are intimately aware of these issues and most likely spent many hours or days attempting to complete a project and ensure all files were copied. Yet they are often not 100% confident that the job completed successfully and has detailed logs to confirm the process.

4. Client System Modification

Current collection efforts should include using applications and processes that preserve the native states on servers and individual client PCs. However, many file collection utilities require an installation on corporate systems, which can introduce multiple obstacles:

- Corporate IT policies may prevent installing new software without prior approval.
- Transferring software licenses between systems may require purchasing multiple copies or contacting the developer.
- Collection software may not have all file dependencies on the target computer.

File collection software should ideally be portable and run without installation. The “zero footprint” software option preserves the native state of the servers and client machines.

5. Over-Collecting

Due to the amount of data that can now reside on corporate servers and individual custodian PCs, many companies and legal counsel seek ways to reduce the amount of data at the point of collection. In many

cases, keyword search, date ranges, deduplication, deNisting and other criteria are applied. It is not uncommon to have the data produced reduced by 90% and more, which can be a considerable cost savings.

Culling data at the point of collection can make a lot of sense. However, before deciding to apply keywords at the point of collection, there are certain dangers that need to be considered. The complete keyword list needs to be finalized if there is only one chance to collect information from the producing party. Why is settling on keywords so critical? The answer is that any additional keyword revisions will only apply to the collected information and not across all original sources. To further explain, assume a corporation has 10 terabytes of information that needs to be collected and only 500 gigabytes is produced that matched keyword searching and other criteria. The 500GB is what will be available for searching during e-discovery processing and review. If additional keywords are considered relevant and need to be applied to the collected data, there will be 9.5 terabytes of data that is now excluded from the search because it is still sitting back on the corporate servers and custodian PCs because it never matched the original keywords and wasn't produced. Therefore, it is critical that the attorneys understand that additional changes will only be applied to the already filtered information and not the entire universe of the original documents.

6) Files Skipped During Keyword Searching

Leaving potentially relevant documents behind due to encryption is another issue that occurs when keyword searching at the point of collection.

Why? Corporate IT departments and IT legal professionals often use programs to search their networks and PC's for files containing keywords and then produce a list of files that need to be collected. However, many don't realize that any files that were password protected or encrypted were skipped because a keyword search could not be applied.

To further explain, when a user applies a password to a file, the contents are "scrambled," for lack of a better term, which is what allows the file to be protected so the contents are not easily viewed by other applications. When the keyword search process encounters the file, it will not be able to see the original content or find matching data. Therefore, any potentially relevant files that are encrypted will be left behind unless the application searching the data is designed to identify these encrypted files and ensure the user knows they exist.

Why not just decrypt and search them on-the-fly to determine if they are a keyword match? Decrypting a file could take anywhere from a few seconds, to many years depending on the complexity. Clarifying if a file should be decrypted often needs to be discussed between a client and their legal counsel. The most efficient way to handle encrypted files during collection is to identify, copy and create a list so they can be reviewed and determine if a decryption process needs to be used. Leaving them behind is not the answer; however, many processes in place do exactly that. If your company or legal counsel decides on a targeted collection, it would be advised to ask what process and applications are going to be used.

7) Optimal Keywords Are Missed

Keyword hit preview and reporting are very useful because they can list the files that are a match and provide a preview of what would be collected before copying. Often keywords are applied only to find out that the collected files and emails do not match expectations. When this happens, the keyword search criteria need to be altered and in some cases, going back to the sources is not an option.

CONSISTENT RESULTS

When attorneys and their support staff are not involved in recommendations or implementing best practices for file collections (or fail to even know what the best practices are), the quality of the file productions can suffer and client claims for malpractice can result. When individuals responsible for file collections are not familiar with adequate collection tools, they may resort to file copy utilities that do not include verification or they do not know how to set the options.

Common copy utilities have dozens of options, which if not used in the right combination, can cause a number of issues. Additionally, there can be a higher likelihood of problems if multiple parties attempt to replicate the same settings. It is important to ensure that file collections are consistent across multiple projects. Using intuitive tools that require minimal end user interaction is preferred.

SUMMARY

Preserving, verifying and documenting electronic discovery collections confirm that relevant files are acquired. It also helps legal departments avoid spoliation and demonstrates to their clients they are implementing best practices. As inside counsel, general counsel and corporate IT departments learn more about litigation readiness, it becomes more important that their partnering legal departments keep abreast of the changes and are the ones leading the way. Being proactive and recommending the proper methods and tools for ESI collections will ensure consistent results and provide a *heads-up* on any issues encountered. Many legal departments and service providers rely on Pinpoint Labs software tools for active file collections because collections results are confirmed, incomplete jobs are immediately reported and the process is thoroughly documented.

WHY SAFECOPY

https://youtu.be/cB8W2jC6Wk0

Pinpoint SafeCopy enables you to make forensically sound copies of files located on any of your local or network drives.

With SafeCopy, you can:

- Select multiple directories for copy
- Use a file list as a source for your collection
- Filter your collections by file extension or date
- Create a Chain of Custody log file utilizing hashes calculated from the source and destination files
- Utilize two different copy engines consisting of:
  Our new and improved, multithreaded SafeCopy engine or
  Microsoft's RoboCopy with SafeCopy's easy to use interface with selectable switches
- Copy and preserve long file paths (up to 32,000 characters)
- Resume SafeCopy jobs in the event of a system reboot, crash or other problem
- Have errors reported real-time should the hash values of your source and destination file not match
- Save job settings for reuse in multiple environments
- Use variables to get the most out of your saved SafeCopy jobs

These features make SafeCopy the professional's choice for any type of application, from computer forensics to data backup.

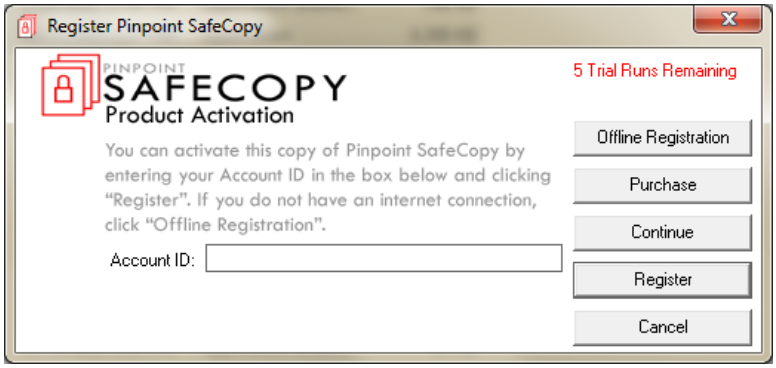
SafeCopy Nomad- Download and Activate

Online Activation

An advantage of the Nomad Edition is the ability to move it from drive to drive. Once activated on a drive, you can perform your collection and move the license to another device.

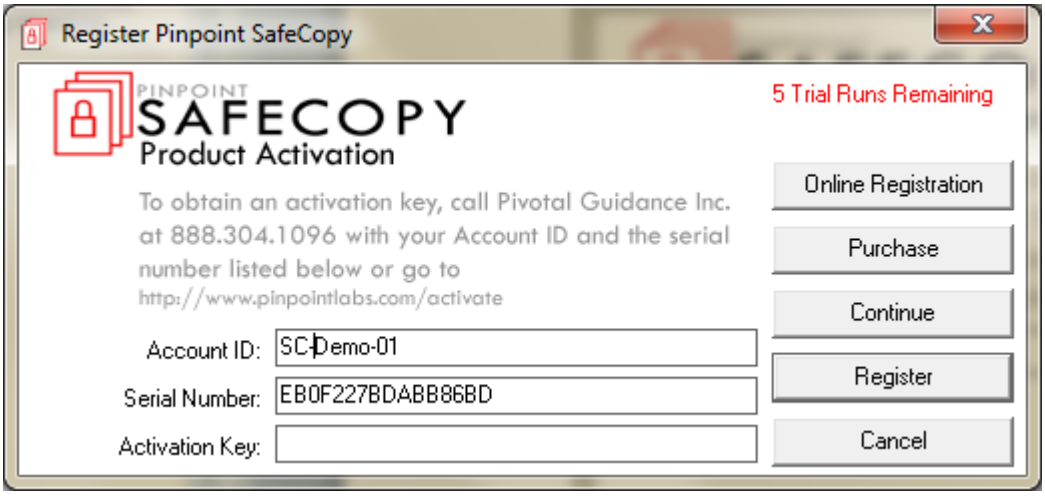
https://youtu.be/OiQENDexMb4

To activate SafeCopy Portable Edition, follow these steps:



- Download Pinpoint Labs SafeCopy Nomad Edition
- Extract the .zip file contents to your external device (hard drive, flash drive, etc.)
- Run the executable (PinpointSafecopy.exe)
- Enter licensing information (Account ID) to activate the product using online activation
- Exit and restart the application

OFFLINE ACTIVATION



Should a firewall block the connection to the licensing server, offline activation can be accomplished by doing the following:

- Enter your Account ID and click ***Offline Registration***. A serial number will be generated. Call or email support@pinpointlabs.com with your Account ID and the serial number
- An activation key will be generated for you. Enter this in the space provided and click ***Register***.
- Exit and restart the application.

The ***Tools*** menu has an option to ***Deactivate License***, restoring the license to be used again elsewhere. Once you have placed the .zip file contents onto another external device, you can activate the license using your same Account ID.

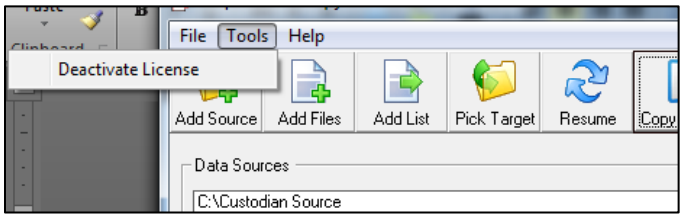
SafeCopy Server - Download and Activate

https://youtu.be/PPmCq_yC45A

The **SafeCopy Server Edition** is contained in a single .zip file. To activate **SafeCopy Server Edition**:

- Download the archive file specified in your order confirmation email
- Unzip the entire archive file contents to a shared folder or drive
- Launch SafeCopy Server Edition (IMPORTANT – Make sure to register/run SafeCopy from the network (UNC) path, not a mapped drive path)
- Enter the Account ID provided
- Exit and restart the application (IMPORTANT – Make sure to register/run SafeCopy from the network (UNC) path, not a mapped drive path)
- After SafeCopy Server Edition is registered, you can access it from systems which have network access to the application folder. You must register and run the utility from the UNC path (i.e., ***\\Server1\SCServer***).
- A local SafeCopy Server Edition installation is not required; it is designed to run from the source directory.

Another advantage of Server Edition is the ability to move it from shared folder/drive to shared folder/drive. Once activated on a shared folder/drive, you can perform your collection(s) and move the license to another shared folder/drive. The ***Tools*** menu has an option to ***Deactivate License***, restoring the license to be used again elsewhere.

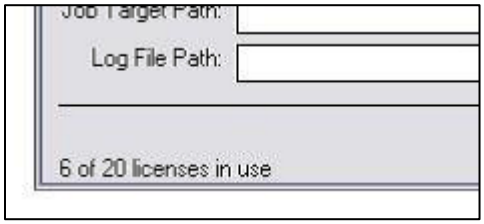


Once you have placed the .zip file contents onto another shared folder/drive, you can activate the license using your same Account ID.

SERVER EDITION OPERATION

SafeCopy Server Edition can be registered and run from a shared folder on a network, an individual computer, or a Network Attached Storage (NAS) device.

The Server Edition is licensed by concurrent user, which means that you can run the number of licenses purchased from different systems or on the same computer. The basic Server Edition includes three (3) concurrent user licenses. If you choose to run multiple jobs from the same system, one concurrent license will be used for each job. SafeCopy Server Edition displays the number of concurrent licenses running in the lower left hand corner of the main window.



If you are running multiple sessions on the same computer, a number will appear in the title and progress bars to help track individual projects.

SERVER EDITION CONCURRENT USERS

You may purchase additional SafeCopy Server Edition client licenses from Pinpoint Labs. To update SafeCopy Server Edition so that it reflects additional licenses, please follow these steps:

1. Launch SafeCopy Server Edition
2. Select ***Refresh User Licenses*** from the Help Menu (requires Internet access).
3. Confirm the number of concurrent licenses listed in the lower left hand corner of the screen.

SERVER EDITION CONCURRENT USERS – UPDATE NOTES

- It is best to exit out of all sessions except the one that you are using to update
- The update will not be reflected on running sessions
- If the total does not immediately update, then exit and restart SafeCopy Server Edition. After restart, select ***Refresh User Licenses***.
- When you register SafeCopy Server Edition, it is licensed to the specific network location that it was activated. SafeCopy Server Edition will not run if the application folder is moved to a different location once it has been registered.

File Tab

Pinpoint SafeCopy enables you to make forensically sound copies of files located on any of your local or network drives.

SAVING AND LOADING SAFECOPY JOBS

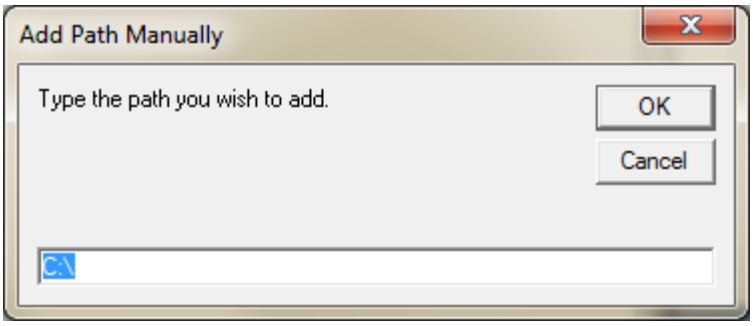
SafeCopy supports the ability to save job settings and reuse them for later jobs, including the use of variables in the job and target paths.

Once you have filled out the job settings, or as much of it as you would like to save, click on the File tab and select ***Save Job***. This will open your file window and allow you to choose where to save the job. These saved job files have the.***sc*** extension.

To open a saved job, or one that you have already run (using the _jobfile.scj that gets created in the logs path when a job runs), click on the File tab and select ***Load Job***. This will open a window that allows you to locate the SafeCopy job you would like to run. From this window, you can choose ***.sc*** files, which are SafeCopy jobs that were saved using the ***Save Job*** option above, or ***.scj*** files, which are SafeCopy jobs that have already been run.

You can also save the settings you have chosen in ***Copy Options*** as your default startup settings by clicking on the File menu and selecting ***Save Current Options as Default***. Source and target paths are not saved with this method.

Add Path Manually

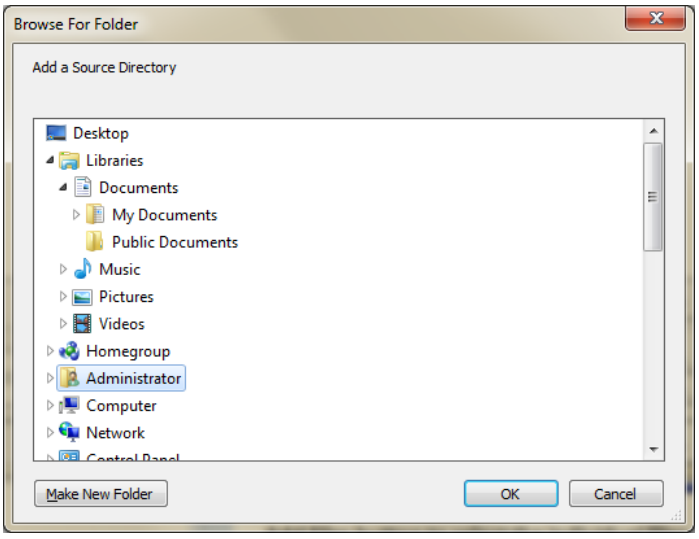


Add a file or folder by clicking Add Path Manually and enter the path as a source for your data collection.

Add a Source Directory

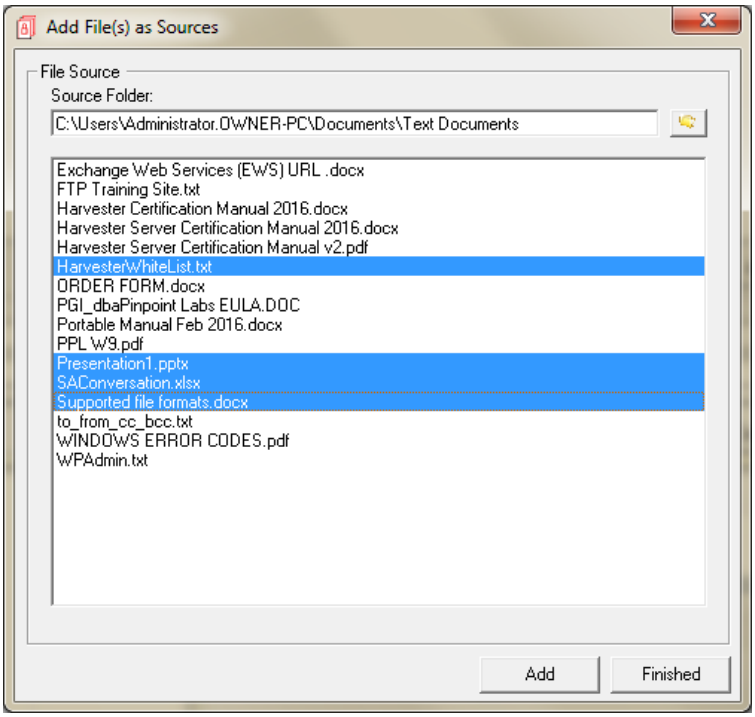
SafeCopy allows for the selection of one or many directories to be copied to the destination of your choosing. By using the ***Add*** button located at the bottom of the window, you can select each directory to be copied in the ***Browse for Folder*** window that appears.

Folders can also be added by using the ***File*** menu or using the ***Add a Source Directory*** icon.



Add Source Files

You can add individual files by using the ***Add Files*** button in the toolbar. An interface appears allowing you to browse and select the individual files you need to copy, then click ***Add***. When you are done selecting files, click ***Finish***.



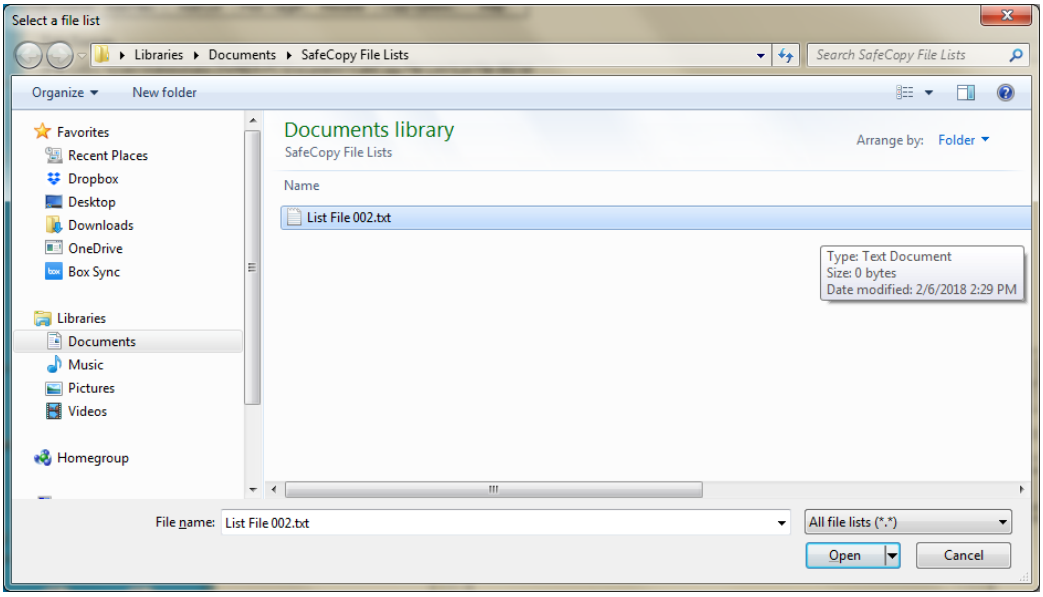
Files can be added by using the ***File*** menu or using the ***Add Files*** icon.

Drag and Drop

Files and folders can be dragged into the sources field for collection. It should also be noted that *dragging and dropping* the file list to the ***Data Sources*** window will merely add the file list as a single file to be copied. You must use the ***Add List*** button for your file list to be the source for your data collection.

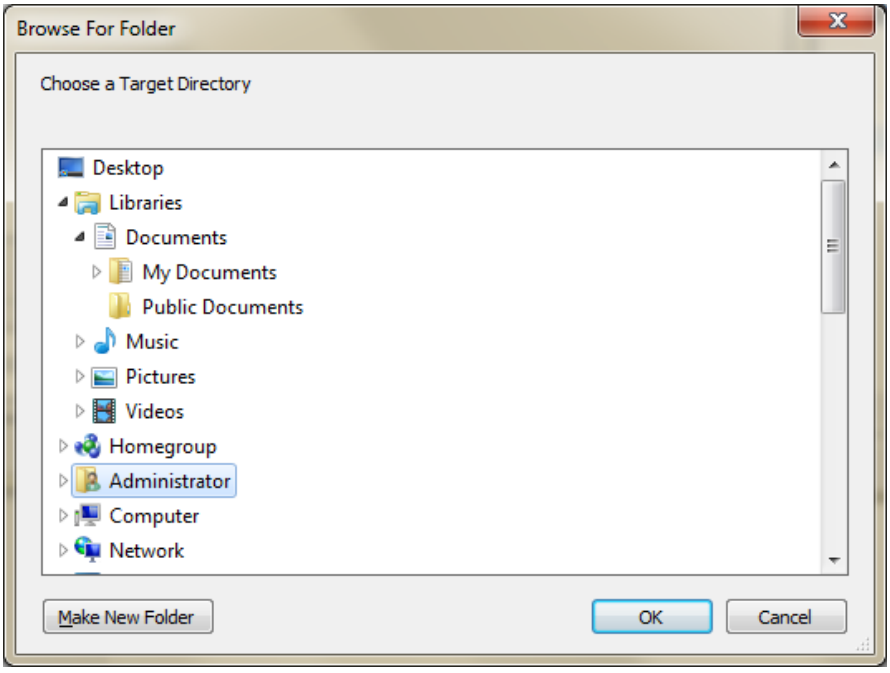
Add Sources From List

SafeCopy enables you to use a file list, including an error list as the source for your data collection. By clicking the ***Add List*** button, you will be able to browse to the location and select the list to be used. A file list can be any text file (.txt, .csv, .log), so long as the full file path is the only field in the text file. You might need to strip away other columns of data in another utility prior to using the file list in SafeCopy.



SELECT THE DESTINATION

Once you have chosen what needs to be copied, select your destination directory in the field named Choose a Target Directory by browsing to the location. If a sub-folder does not exist, SafeCopy will create it for you.



A destination directory can also be selected by using by using the ***File*** menu or the ***Choose a Target Folder*** icon. The ***Browse for Folder*** window appears so you can choose where the files will be copied.

LOCATION FOR LOG FILES

The output directory for log files, including the Chain of Custody verification log, the SafeCopy .scj file, and an error log (if any occur) can be chosen using the ***Log File Path*** input. You can ***Browse for Folder*** or type in the directory. By default, the output directory will be the destination for the copied files.

USING VARIABLES IN SAFECOPY

SafeCopy supports the use of a handful of variables in the target and logs paths that allow you to tailor a one-size-fits-all job file for use on multiple computers. Below is the list of variables and what each translates into:

[SCDrive] – This variable translates to the drive letter that SafeCopy is running from. This variable is useful for the Nomad Edition, where the program itself is likely to be running from the drive that will be receiving the collected files. Example: ***[SCDrive]\Collection*** would translate to ***F:\Collection*** at job runtime.

[CName] – This variable translates to the computer name of the computer that is running SafeCopy. This variable is useful in both the Server and Nomad editions to separate files by the computer they were collected from. Example: ***\\MyCollectionServer\Target\[CName]*** running on a computer named ***WORKSTATION3*** would translate to ***\\MyCollectionServer\Target\WORKSTATION3***

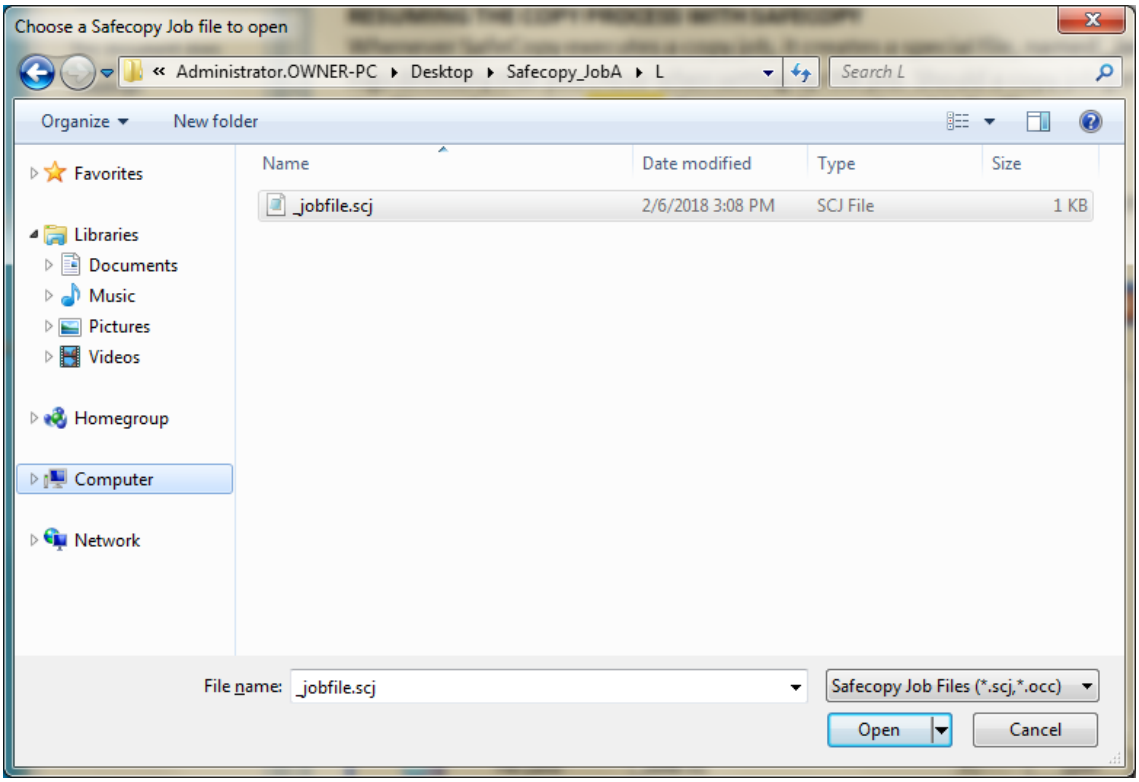
[UName] – This variable translates to the username of the user running SafeCopy. This is useful when you need to keep track of which user is logged on for which set of files being collected. Example: If the logged on user is ***carol.peters***, then ***F:\UserFiles\[UName]*** would translate to ***F:\UserFiles\carol.peters***

[Date] – This variable translates to the day, month, and year the job was run in short format. Example: ***F:\CollectedFiles\[Date]*** would translate to ***F:\CollectedFiles\25-Sep-12*** if the job was run on September 25th, 2012.

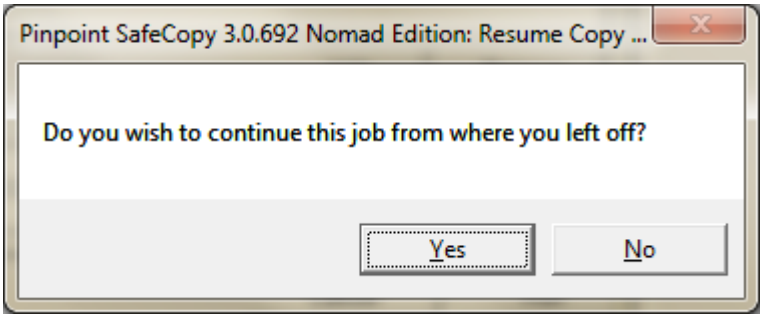
[DateTime] – This variable translates to the day, month, year, hour (in 24-hour local time), minute and second that the job was run. Example: ***F:\Jobs\[DateTime]*** would translate to ***F:\Jobs\26Sep12-152956*** for a job run on September 26th, 2012 at 3:29:56 in the afternoon local time. This variable comes in handy if you anticipate that the same computer will need to run the same job multiple times in a row or if you need to keep track of when each collection was done throughout the course of a day.

RESUME

Whenever SafeCopy executes a copy job, it creates a special file, named ***_jobfile.scj*** which is saved in the logs directory that you chose when setting up the job. Should a copy job get terminated unexpectedly, this file can be used to resume the copying from where it left off.



Once the ***_jobfile.scj*** has been selected in the logs folder of the copy job that was interrupted, click ***Open*** and a confirmation window will appear.



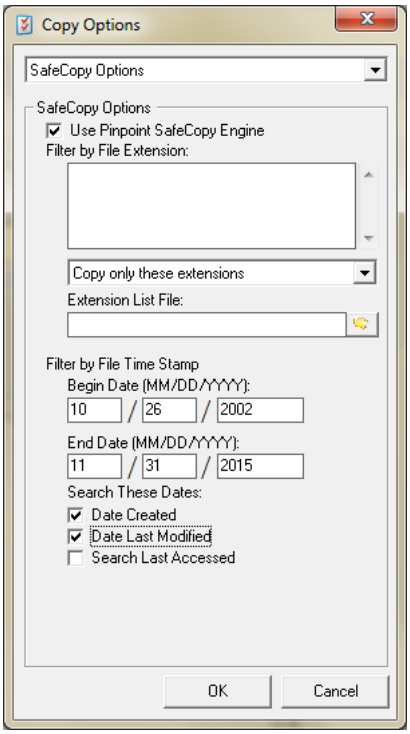
Clicking ***Yes*** will resume the copying process, while clicking ***No*** will return you to the SafeCopy interface.

SafeCopy jobs can be resumed by choosing the option in the ***File*** menu or clicking the ***Resume*** icon.

SafeCopy Options

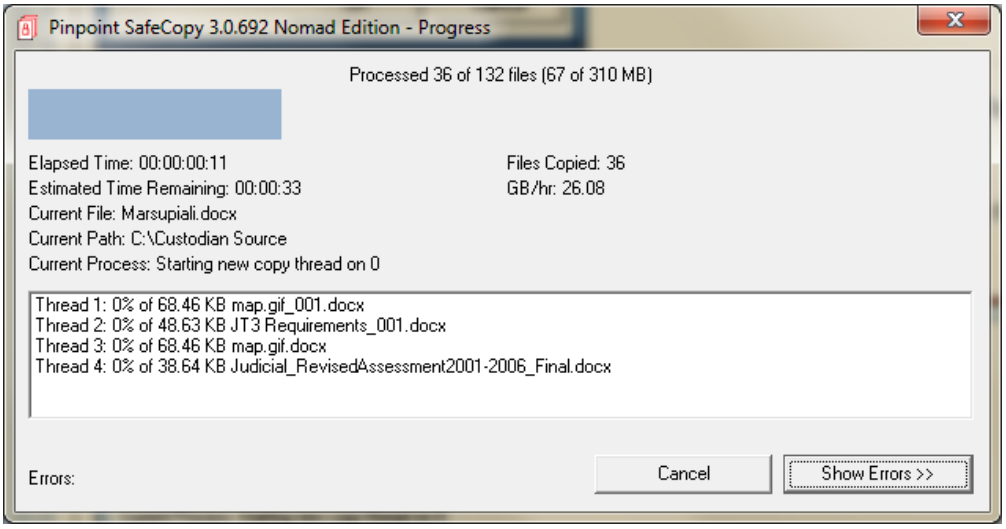
Using the SafeCopy Engine

The SafeCopy engine gives you the ability to copy files and their timestamps to a new location. Using the SafeCopy engine over the RoboCopy engine allows you to use extension and date filters in your search and will generally result in a substantial increase in throughput.



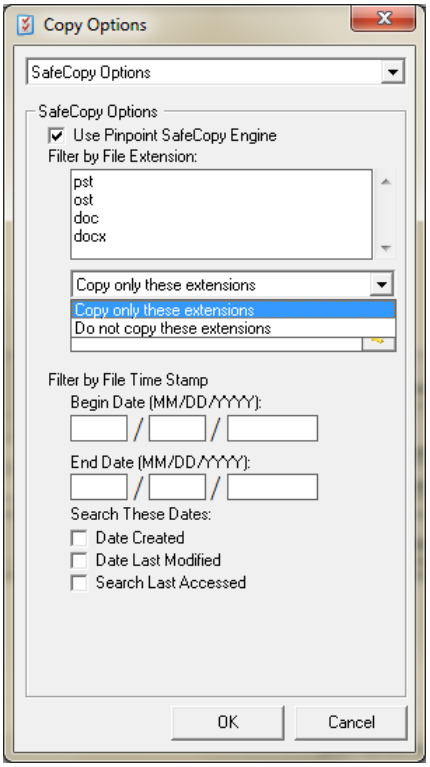
To use the SafeCopy engine to copy the files to a new location, open the ***Copy Options*** and click on the check box marked ***Use Pinpoint SafeCopy Engine***.

When the SafeCopy engine is used to make copies, the progress window shows the status of the entire job as well as the individual files being processed and by which thread.



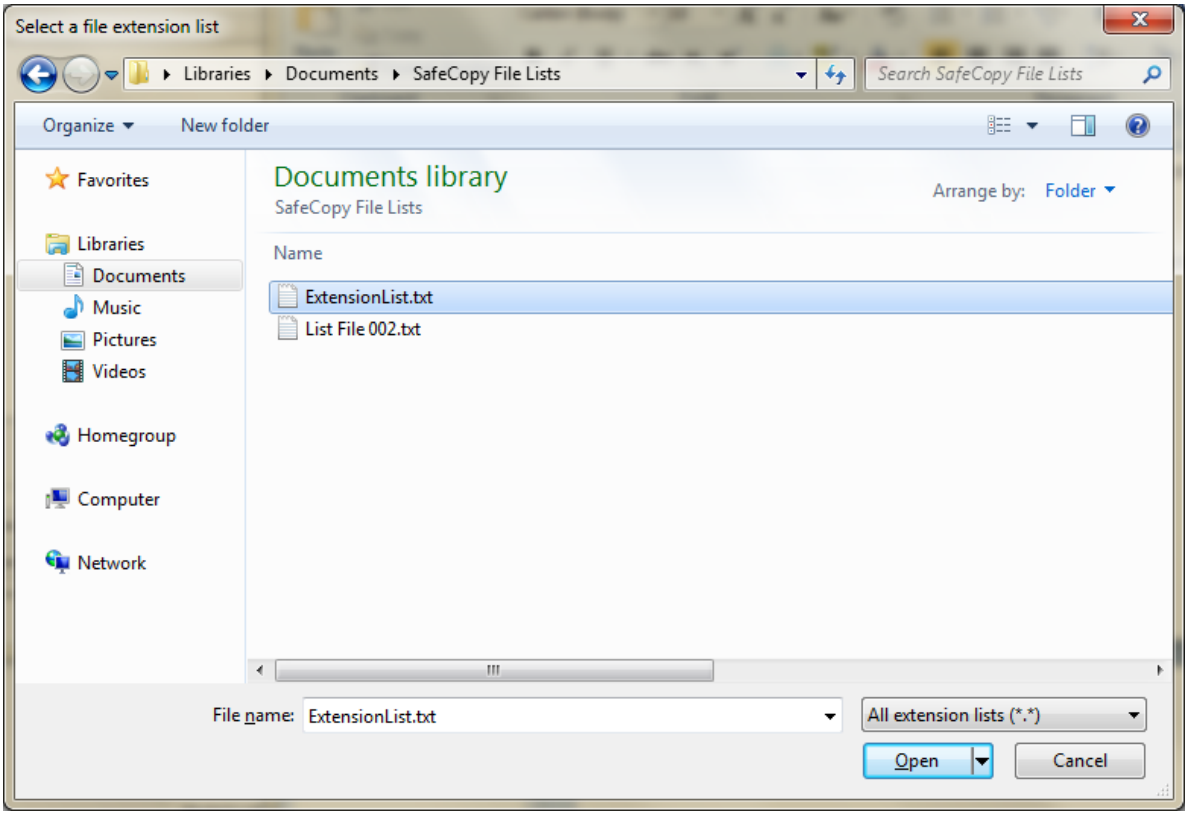
Filter by File Extension (Include/Exclude)

If you are using the SafeCopy engine, SafeCopy will allow you to filter the data you collect by file extension.



In this option panel, you can enter multiple file extensions, separated by lines or commas, to filter by those file types. You can also choose whether to include or exclude files with those file extensions in the dropdown box.

In the ***Extension List File*** section, you can use a text file containing multiple file extensions by browsing to the file using the button next to the field.

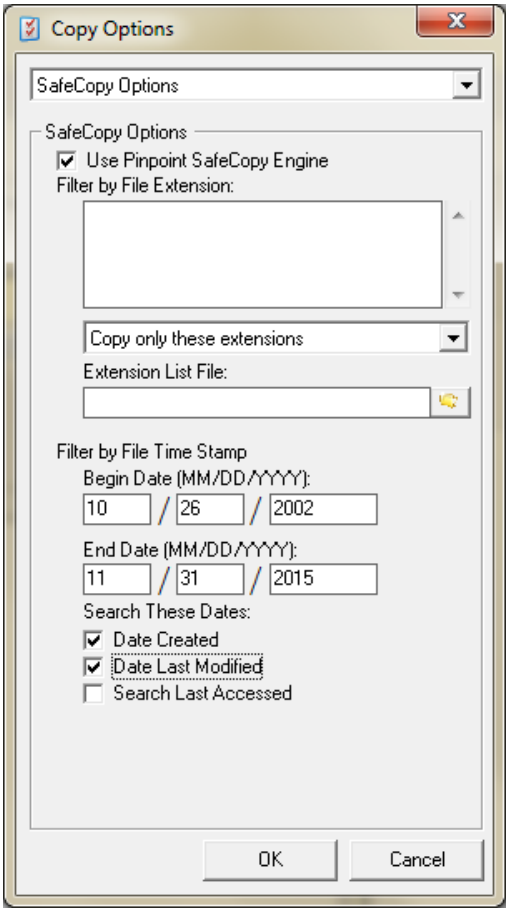


An extension list file should be a normal text file containing a comma-separated list of extensions that you wish to use. The upper limit of the number of simultaneous entries that are supported by SafeCopy is 32,000.

Filter by File Time Stamp

Using the SafeCopy engine, SafeCopy also allows you to filter the data you collect by date. Once you enter the date range for the files you wish to collect, you can also choose the date fields you wish to search for files in this date range.

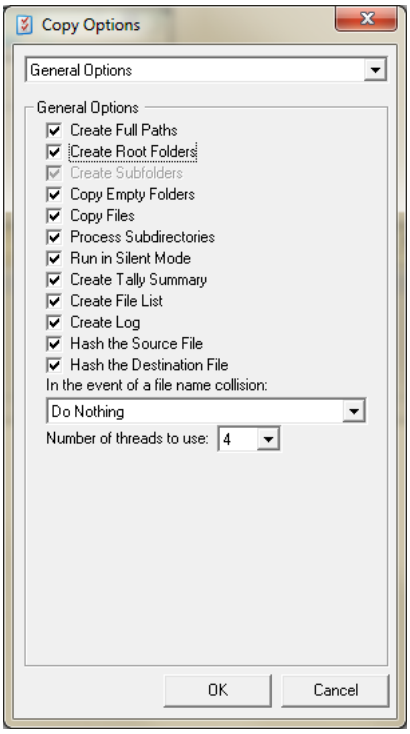
- *Created*
- *Last Modified*
- *Last Accessed*



By clicking ***OK***, these settings will be applied to the collection you perform using the SafeCopy engine.

Copy Options

General Options



The **General Options** screen gives a number of checkboxes which can modify the properties of the collection performed. These options are detailed below:

Create Full Paths will allow the destination directory to contain a full path of all files and directories that are collected or copied. When selected, the option to ***Create Root Folders*** is also available.
Create Root Folders will create a directory for the drive letter or UNC name of the source path. This is useful when the source consists of multiple drives or UNC paths, where each will have a folder containing the files and folders contained therein.
Create Subdirectories will create matching subdirectories for each subdirectory in the source. This option is selected by default, but can be deselected in the event that you need to force all matching files into the same directory.
Copy Empty Folders will make a copy of each folder encountered in the search, whether or not it contained any matching files. Deselecting this option will only create target side folders for sources that contained matching files.
Copy Files will copy all matching files. Deselecting this option will enumerate all of the files according to the criteria you set, but will not copy them. This is useful for determining the number and size of the files in question before actually running the collection job.
Process Subdirectories will recursively search all subdirectories beneath the source folders you have selected. This is the default option. Deselecting this option will only search the chosen directories and ignore any subdirectories.
Run in silent mode will allow any Windows errors that occur during the process of a collection to be bypassed, writing them to the ***_silent.log*** file instead.
Create Tally Summary will write the contents of the summary screen to a text file called ***tally.txt***.

The summary screen is shown at the end of the run and contains information about the number and total size of the files copied as well as elapsed time, overall speed, and the number of errors encountered.

Create File List will create a text file containing the source paths of all of the files matching the filter criteria. This is useful if you need a list of all of the files that were copied. Alternatively, when combined with unchecking of the ***copy files*** option, it allows you to generate a list of all the files that would be copied with the current criteria without actually performing the copy.

Create Log will create a verification log matching the source files and their metadata to the destination files and their metadata. This log, a comma separated values file (***_verification_log.csv***), includes the following fields for each file:

- Date/Time Copied (The time the copy took place)
- Hashes Match (A Y/N field indicating whether or not the source and destination hashes match)
- TS Exact Match (A Y/N field indicating whether the timestamps for the source and destination are an exact match. In cases of disparate file systems, the time stamps will only match down to the lowest available time delimiter of the target file system.)
- Long Path (A Y/N field indicating whether or not the destination file is in a path exceeding the 255 character limit for Windows Explorer. SafeCopy can copy into and out of long paths, but Windows Explorer cannot reach nor tally these files.)
- Source Path (This field contains the full path to the source file, including the drive letter and file name.)
- Source Created Date (This field indicates the creation time of the source file.) Source Modified Date (This field indicates the last modification time of the source file.)
- Source Last Access Date (This field indicates the last accessed time of the source file.)
- Source Size (This field contains the size of the source file in bytes.)
- Source MD5 (This field contains the MD5 hash value of the source file. This field is omitted if the ***Hash Source File*** box is not checked.)
- Dest Path (This field contains the full path to the destination file, including the drive letter and file name.)
- Dest Created Date (This field indicates the creation time of the destination file.)
- Dest Modified Date (This field indicates the last modification time of the destination file.)
- Dest Last Access Date (This field indicates the last accessed time of the destination file.)
- Dest MD5 (This field contains the MD5 hash value of the destination file.)
- Error Messages (If any errors occurred during the copying of this file, they will appear in the column as well as in the error log.)

Hash the Source File will determine the MD5 hash value of the source file and write it to the verification log.

Hash the Destination File will determine the MD5 hash value of the destination file and write it to the verification log. When both ***Hash the Source File*** and ***Hash the Destination File*** are checked, the hashes are also compared against one another for validation purposes during the copy process.
In the event of a file name collision handles the various options for dealing with two files of the same name in the same target folder:

- **Overwrite Existing Files** will cause the existing file to be replaced with the copy.
- **Rename Files on Collision** will cause a new file to be created with a numerically incremented file name. For example, if the file "***Test.txt***" already exists in our target folder, the copy will be "***Test(1).txt***". The new names are reflected in the verification log.
- **Do Nothing** will cause files that already exist in the target to be skipped. This is useful in the cases where you need to "*fill in the blanks*" between subsequent copy jobs.

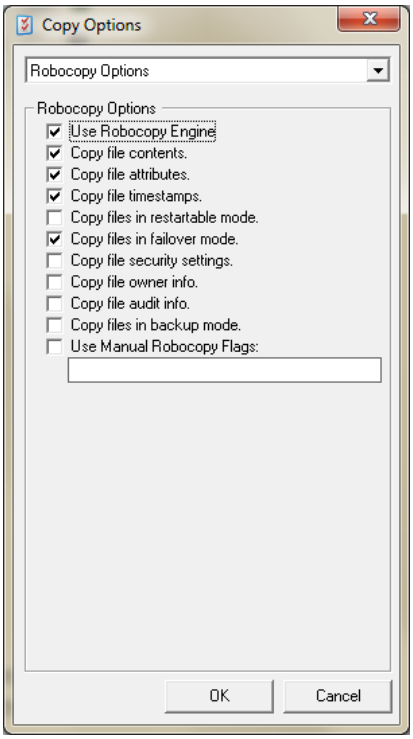
Number of threads to use This option allows you to choose the number of simultaneous copy threads that SafeCopy will use. By default, the program will poll the number of processor cores on the computer running it and set the thread count to that number. You can set it higher or lower to maximize efficiency in your environment

NOTE: Using the ***Create Log, Hash the Source File*** and ***Hash the Destination File*** options will result in a detailed Chain of Custody log file saved in the directory chosen in the ***Log File Path***. Additionally, any errors resulting from the calculated MD5 hash values not matching will be shown in the progress window during the copying process.
You can also save the settings you've chosen in ***Copy Options*** as your default startup settings by clicking on the File menu and selecting ***Save Current Options as Default***.
NOTE: Source and target paths are not saved with this method.

RoboCopy Options

In addition to its own engine, SafeCopy can also use the RoboCopy utility from Microsoft to copy files to a new location without changing the metadata or the timestamps of the file. This feature requires RoboCopy XP or newer to be accessible from the system shell.

To use the RoboCopy engine to copy the files to a new location, open up the ***Copy Options***, select ***RoboCopy Options*** from the dropdown box, and click on the check box marked ***Use RoboCopy Engine***. This screen will also display the options that allow for the easy selection of the most commonly used RoboCopy switches.



For advanced users with the need for other switches, the use ***Manual RoboCopy Flags*** checkbox will allow you to enter the desired switches in the adjacent field.

OBTAINING ROBOCOPY

RoboCopy is freely available from Microsoft as part of the Windows Server 2003 Resource Kit and has shipped with most versions of Windows since Windows Vista. The system requirements and additional information concerning the operational capacity of RoboCopy and the other resource kit components are available from Microsoft. Additional end user agreements between you and Microsoft may apply.

ROBOCOPY IN THE SHELL

In order for Pinpoint to be able to access it, RoboCopy must be available from the Windows shell. It may already be available in the shell, but if not, the easiest way to make it available is to copy the ***robocopy.exe*** file from the Windows Server 2003 Resource Kit to your system directory (usually ***C:\WINDOWS\system32***).

LIMITATIONS OF ROBOCOPY

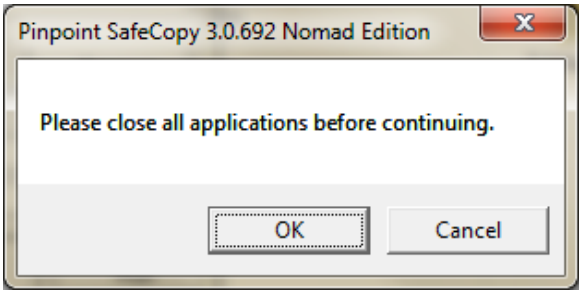
In certain instances, RoboCopy will not be able to copy all of the file system information that was available for the original file. These instances concern the complexities of the source and destination file systems. If the source file system is NTFS and the destination is FAT32, the auditing information and the last few least significant digits of the timestamps will be lost because there is no corresponding data point in FAT32 to which this information can be copied. Similar instances have been noted with Joliet, FAT16, FAT12, and a variety of other disparate file systems.

Validation for files copied with the RoboCopy engine in SafeCopy also take longer due to the method used by RoboCopy to copy the files. In addition, RoboCopy from within the confines of SafeCopy can only run in single-threaded fashion.

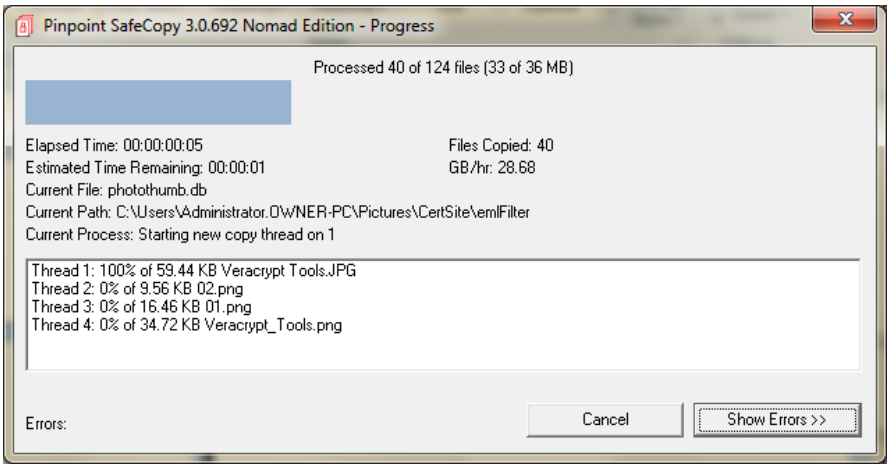
Execute the Copy

Job Runtime

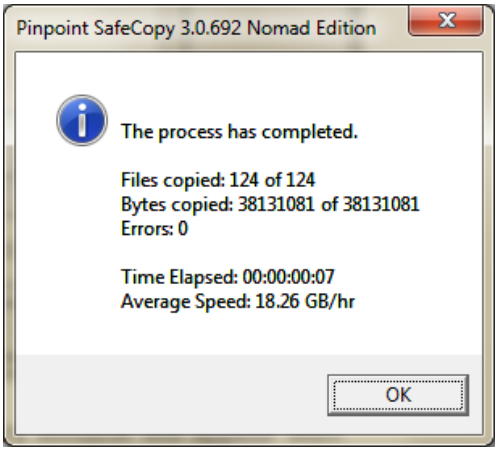
Once the source and destination directories have been selected, and the settings have been chosen, click the ***Run*** button. A window will appear to inform you to close all other applications.



A progress window will appear indicating the progress of the copies being made.



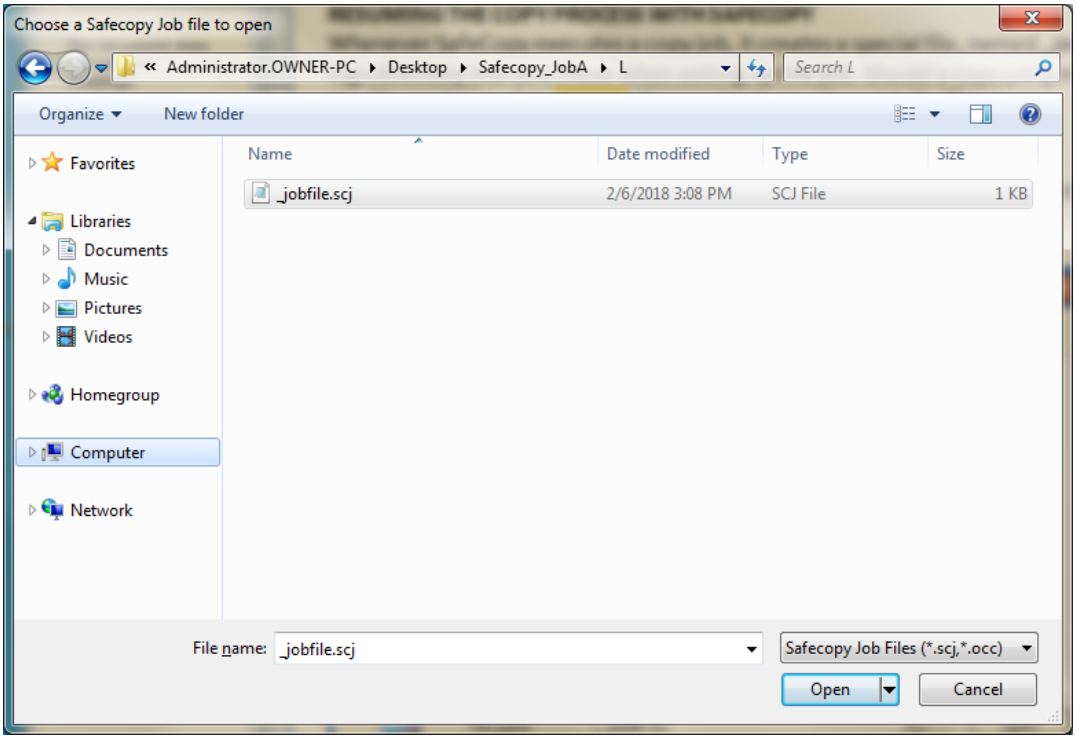
Once the process has been completed, a summary window will appear with the statistics for the job that was completed.



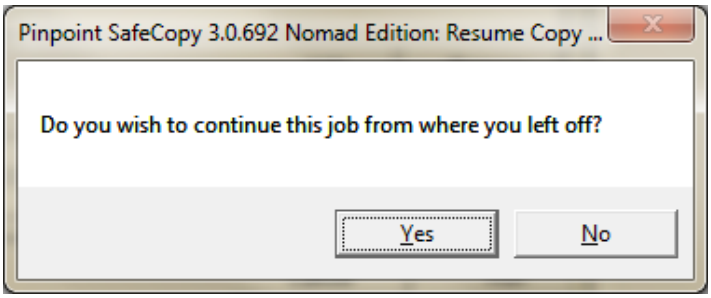
Using the steps outlined above, a mirror copy will be made of all the directories, subdirectories, and files that were selected. These copies retain the original timestamps, original metadata and file contents.

Resume

Whenever SafeCopy executes a copy job, it creates a special file, named ***_jobfile.scj*** which is saved in the logs directory that you chose when setting up the job. Should a copy job get terminated unexpectedly, this file can be used to resume the copying from where it left off.



Once the ***_jobfile.scj*** has been selected in the logs folder of the copy job that was interrupted, click ***Open*** and a confirmation window will appear.



Clicking ***Yes*** will resume the copying process, while clicking ***No*** will return you to the SafeCopy interface.

SafeCopy jobs can be resumed by choosing the option in the ***File*** menu or clicking the ***Resume*** icon.

SafeCopy Logs

Create Log will create a verification log matching the source files and their metadata to the destination files and their metadata. This log, a comma separated values file (***_verification_log.csv***), includes the following fields for each file:

- **Date/Time Copied** (The time the copy took place)
- **Hashes Match** (A Y/N field indicating whether or not the source and destination hashes match)
- **TS Exact Match** (A Y/N field indicating whether the timestamps for the source and destination are an exact match. In cases of disparate file systems, the time stamps will only match down to the lowest available time delimiter of the target file system.)
- **Long Path** (A Y/N field indicating whether or not the destination file is in a path exceeding the 255 character limit for Windows Explorer. SafeCopy can copy into and out of long paths, but Windows Explorer cannot reach nor tally these files.)
- **Source Path** (This field contains the full path to the source file, including the drive letter and file name.)
- **Source Created Date** (This field indicates the creation time of the source file.)
- **Source Modified Date** (This field indicates the last modification time of the source file.)
- **Source Last Access Date** (This field indicates the last accessed time of the source file.)
- **Source Size** (This field contains the size of the source file in bytes.)
- **Source MD5** (This field contains the MD5 hash value of the source file. This field is omitted if the "Hash Source File"box is not checked.)
- **Dest Path** (This field contains the full path to the destination file, including the drive letter and file name.)
- **Dest Created Date** (This field indicates the creation time of the destination file.)

- **Dest Modified Date** (This field indicates the last modification time of the destination file.)
- **Dest Last Access Date** (This field indicates the last accessed time of the destination file.)
- **Dest MD5** (This field contains the MD5 hash value of the destination file.)
- **Error Messages** (If any errors occurred during the copying of this file, they will appear in the column as well as in the error log.)

Portable License Manager

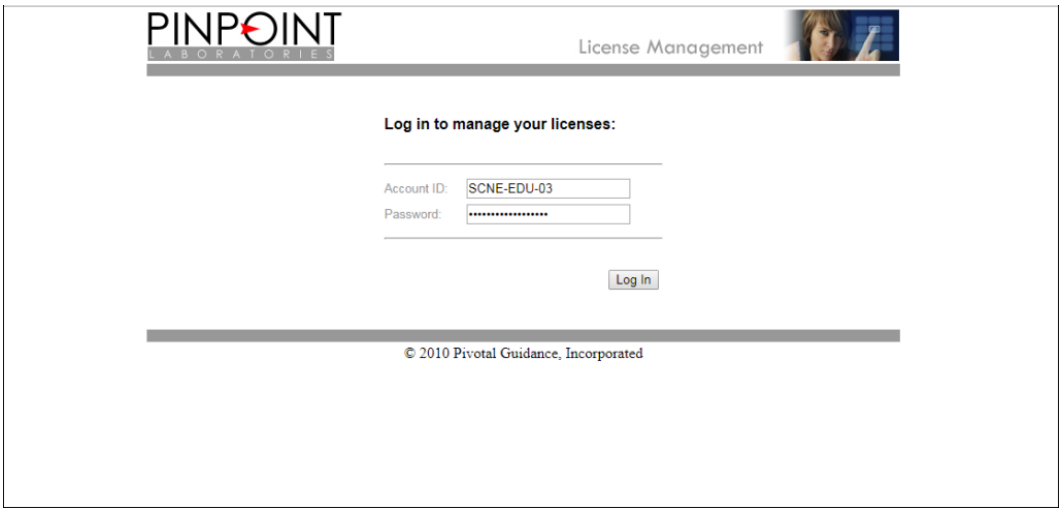
There are numerous ways for the end-users to use portable license manager to their advantage.

Go to *pinpointlabs.com\portal* and log in with the Account ID and password included in your PLM Registration email from Pinpoint Labs.

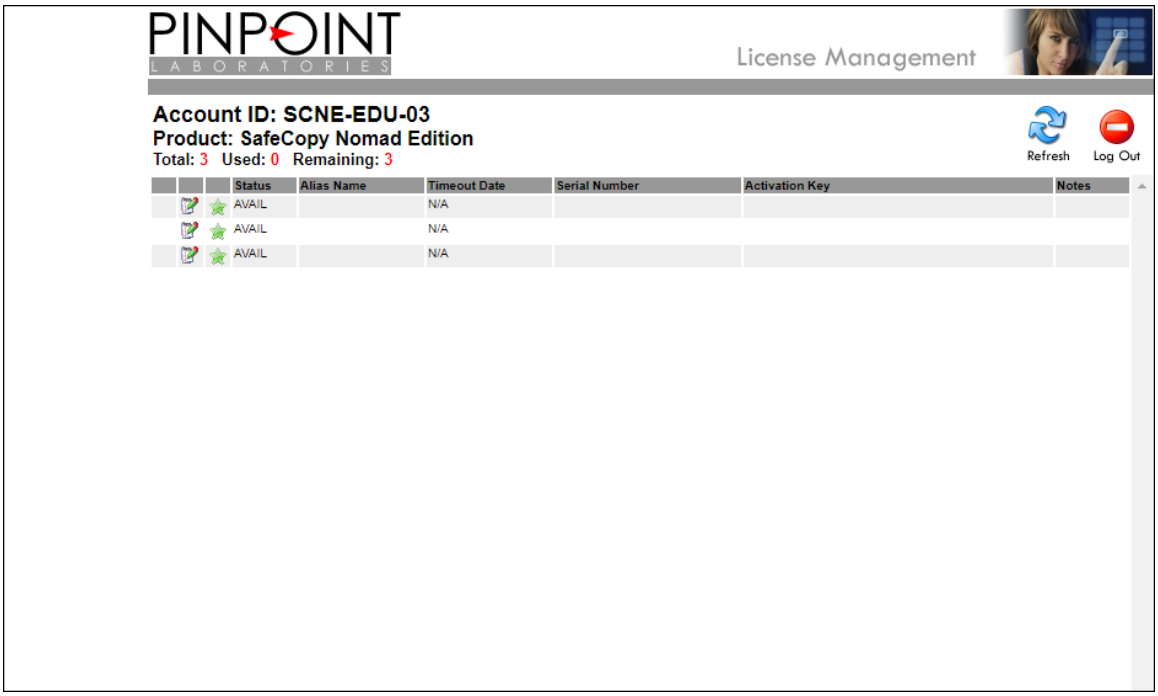
Reference: Portable License Manager Training Video

https://youtu.be/DVZPNvRYO44?list=PLts2Dn6cg3jYfKAGP5jCIw8jiJf89AstM

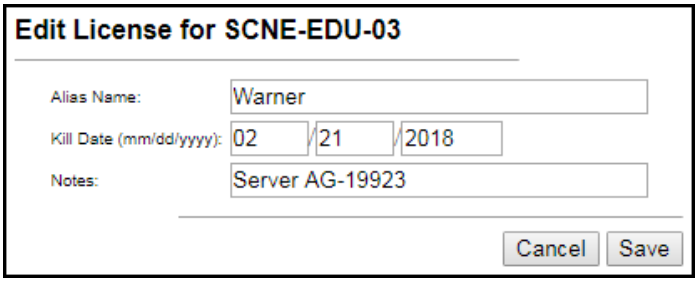
As an example, we have created a demo account with three SafeCopy licenses, and will use a combination of aliases and time-outs.



Click on the Edit License icon to create an alias. *An alias is used in place of the account ID* and is chosen by the user.



As an example I will use word 'Warner' as the alias.

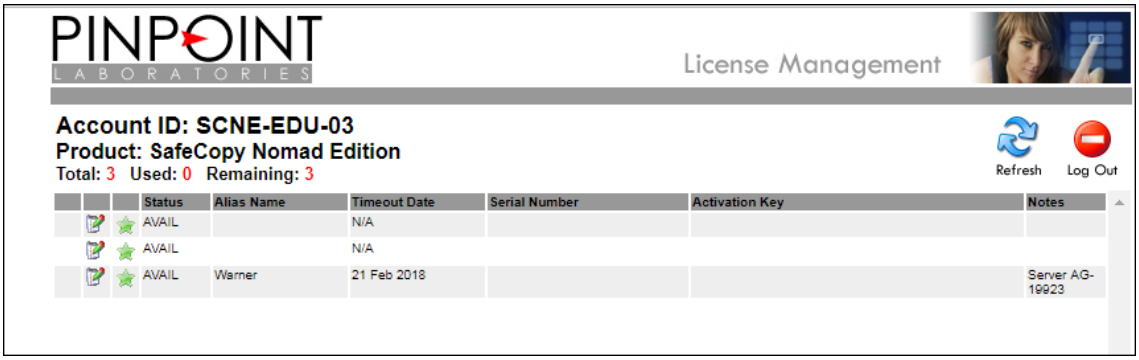


Adding a time-out (or *kill date*) protects licenses from becoming inaccessible in the event of a system or drive failure, machine or drive re-purposing, or lost media.

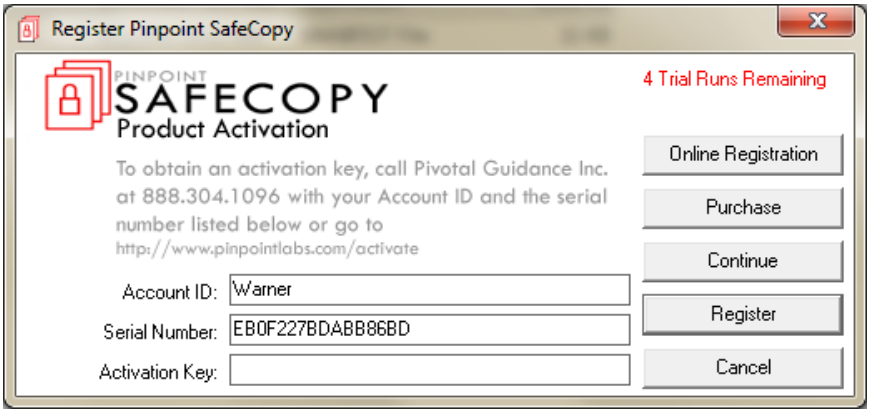
The kill date can be as little as one day, and for effective license management we recommend no more than 15 days for portable drives.
To prevent unauthorized use of an available license, entering an earlier date than present can keep the license from being activated until the date is changed.

The same principal applies to activating directly on a computer. The Alias can be the name of the computer or department, and the kill date could be used as a safeguard the event of accidental deletion of the Harvester folder or a system crash on the PC.

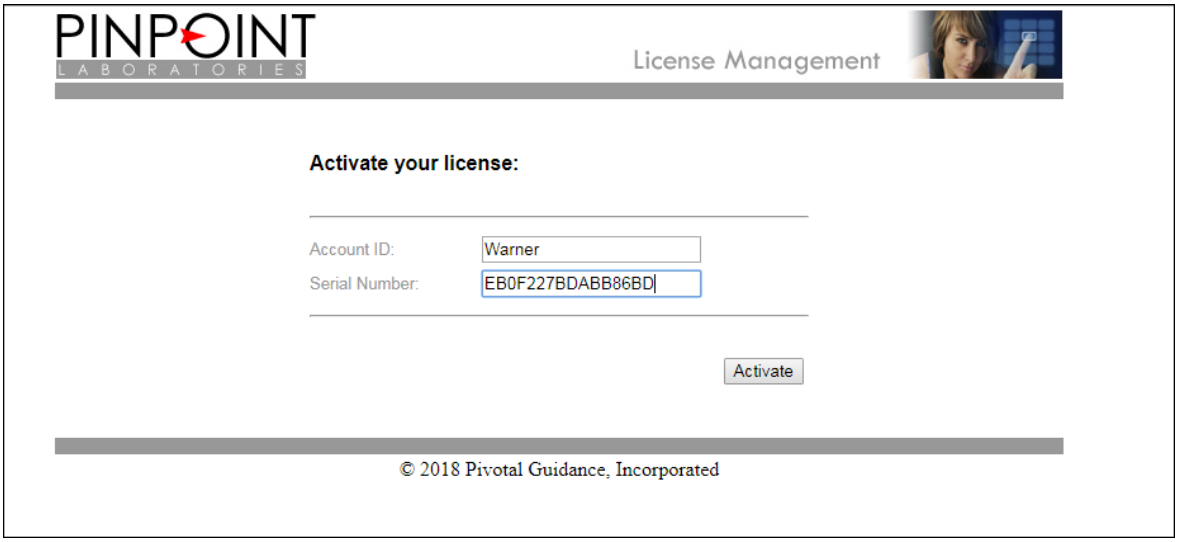
Instructions or reminders can be placed in the Notes section. (This field is optional for license administrator and the end-user).



To activate, the user may use online activation, but if firewalls or lack of internet prevents online activation, the user has other options.



Log into pinpointlabs.com/activate on another computer or mobile phone, ***enter your alias*** from above and the serial number generated by SafeCopy or Harvester, and click Activate.



Type or paste the activation code into the field provided, and click Activate to complete registration.

NOTE: *The PLM cannot deactivate an activated license*. If a license is activated without a kill date, it must be manually deactivated.

CONTACT US

Software Training & Certification

Phone: 888-304-1069 x 102
http://www.pinpointlabs.com
Email: training@pinpointlabs.com