MAGNET AXIOM™

USER GUIDE

CONTENTS

Assumptions and requirements

Before using Magnet AXIOM, this guide assumes that you:

- Understand that Magnet AXIOM is a digital forensics tool made of two components: AXIOM Process, which extracts evidence, and AXIOM Examine, which analyzes evidence. However, forensic examiners must still interpret and contextualize the evidence.
- Have a basic understanding of digital forensic concepts.
- Have a basic understanding of computer hardware, software, mobile phones, storage devices, and the cloud.
- Are familiar with your organization's investigative policies, procedures, and jurisdiction.
- Are familiar with using the computer where Magnet AXIOM is installed.

To learn more about how to equip and optimize your system for Magnet AXIOM, sign in to the Support Portal to read the system requirements article.

What's new

Version	Description
8.0.0	• Updated Available features to indicate extended Comae support. • Added acquiring EC2 Snapshot. • Added View mobile evidence. • Added Export messages and attachments to share with legal reviewers. • Updated information about route view in View evidence with geographical data.
7.10.0	• Added Available features. • Updated EC2 Export and S3 Files to include new authentication types. • Added View evidence with geographical data and updated Browse and dig deeper into artifacts with information about Route view.
7.9.0	• Updated Create exports for specific evidence types to include exporting summary information about an evidence source. • Updated Export evidence to share with stakeholders to include related items for chat messages in load file exports. • Updated Files and folders to include a note concerning FAT32 Last Accessed Date/Time values. • Updated Files and folders to include the new Files and Folders imaging process.
7.8.0	• Added the following overview topics: Assumptions and requirements, Common terms in Magnet AXIOM, and Functions.
7.7.0	• Updated Files and folders to include ExFAT deleted file support. • Updated Endpoint to include TLS1.3 support. • Updated Export evidence for Magnet REVIEW to include the Magnet

Version	Description
	REVIEW SaaS option.
7.6.0	- Updated Connect to an agent to include a file and folder listing from the endpoint. - Updated Endpoint to reference the supported evidence items. - Updated Microsoft user account to include client credentials authentication method. - Updated View raw artifact data in Text and hex to include viewing data as protobuf. - Updated View Windows registry data to include collapsing items.
7.5.0	- Updated Search with YARA rules to include support for YARA rules from a Git repository. - Updated Apple to include iMessage as a separate acquisition source. - Updated Add endpoint manually to include Windows manual endpoints can be specified using an FQDN. - Updated Filter by criteria in the evidence Search and filter evidence to include filter sets. - Added Save filter sets. - Updated Customize AXIOM Examine settings across cases settings across cases to include media preview settings.
7.4.0	- Updated Create an agent to include a link to the article AXIOM Cyber signed macOS agents. - Updated Find more artifacts to include a link to the article Creating custom artifacts from SQLite database hits. - Updated Image to include a link to the article Change the character set encoding in Magnet AXIOM to match the encoding of .zip files. - Updated Customize processing settings to include GrayKey/VeraKey discovery settings. - Updated View database tables to include the protobuf viewer.

Version	Description
	- Updated Create exports for specific evidence types to include a link to the article Understanding PST exports.
7.3.0	- Updated Load evidence from mobile devices to include connect to VeraKey. - Updated Create exports for specific evidence types and Export evidence to share with stakeholders to include the JSON export type and excluding evidence from exports. - Updated Search and filter by keywords to include removing keywords from a case.
7.2.0	- Updated Customize hashing settings to include SHA 256 hash option. - Updated Endpoint to include encryption comment. - Updated Cloud to include encryption comment.
7.1.0	- Updated Decrypt evidence to indicate Symantec Endpoint Encryption account password is required. - Added Delete an agent to detail steps for deleting a AXIOM Cyber agent. - Added Merge evidence back into the original case to cover merging a portable case and merging tags and comments from Magnet REVIEW. - Updated Browse and dig deeper into artifacts with information about the updates to conversation view. - Updated Customize log collection and diagnostics to include enhanced file source exception reporting. - Updated Customize processing settings to include image hash verification in the scan summary.
7.0.0	- Added Update a shared agent configuration to detail recommended steps when modifying a shared agent configuration.

Version	Description
	• Added Shared agent configuration to include support for creating and managing a shared agent configuration. • Added Create a shared agent configuration to cover creating a shared agent configuration. • Added Connect to existing shared agent configuration to detail how to connect to an existing shared agent configuration. • Added Privileged content to describe the ability to manage privileged content. • Updated Create an agent to include a description of the new Shared agent type. • Updated Calculate hash values and find matches to include support for RDSv3 format. • Updated Windows memory to include the Comae plug-in. • Updated Image to support .rar5 images without CRC. • Updated Analyze pictures with Magnet.AI to include Thorn AI. • Updated View email evidence to include newly supported email artifacts in the Email explorer. • Updated Export evidence for Magnet REVIEW to include exporting tags and comments. • Updated Export evidence to share with stakeholders with information about including related items in a load file export.

Common terms in Magnet AXIOM

The following are common terms in digital forensics and in the Magnet AXIOM user interface:

- **Acquisition** - The process of creating an image of digital data. For more information, see Image.
- **Agent** - A standalone executable process that gets deployed to a remote computer to perform a remote acquisition.
- **Artifact** - Information left behind by a digital program. Examples of artifacts include pictures, chat messages, the date a user accessed a file, and items in an internet browser history. Users are usually not aware that these artifacts are being created, and they are often difficult to manipulate. Artifacts can be used to determine what happened, where it happened, when it happened, who it happened to, how it happened, who did it and what their intention was. The terms artifact and evidence item are often used interchangeably in this guide.
- **Carving** - The process of identifying and recovering hidden or deleted files in digital data.
- **Case** - A container in Magnet AXIOM (and other Magnet Forensics products) used to collect information related to an investigation. Examples of case information can include metadata, evidence sources, artifacts, and reports.
- **Case summary** - Displays high-level information about a case, such as when the case started and the number of runs associated with the case.
- **Cloud** - A global network of remote servers that tech companies use to store data and run infrastructure for their applications. Each company has its own policies regarding the sharing of application data. The country in which the company is based might also have further regulations around data sharing. Cloud data can only be accessed through a mutual assistance request; however, this data can be ingested into Magnet AXIOM. Although this requires a lot of effort, it could provide better insights into a case.
- **Cloud acquisition** - Acquisition of cloud evidence from a supported cloud platform, such as the Microsoft 365 platform.

- **Endpoint** - A Windows, macOS, or Linux workstation where an AXIOM Cyber agent is deployed.
- **Evidence item** - An artifact in Magnet AXIOM that could be potential evidence in an investigation. For more information, see Artifact.
- **Evidence source** - A physical or digital source obtained in an investigation that can be imaged to extract artifacts. Examples of evidence sources include computer hard drives, mobile phones, USB flash drives, and cloud accounts.
- **Export** - A copy of an artifact saved in a different file format which may be required by a different application to read the file.
- **Extraction** - The process of retrieving artifacts from an image.
- **Hash** - A unique sequence of letters and numbers calculated by an algorithm that are assigned to an artifact. A hash value essentially represents a "digital fingerprint" for an artifact. Most digital forensic software can check the hash value of an artifact against various hash set databases to verify if the artifact is known, for example, a specific picture or video. In addition, most digital forensic software can perform hash value checking to verify an artifact has not been corrupted or modified.
- **Image** - In digital forensics, an image refers to a copy, or duplicate, of digital data from an evidence source, such as a computer drive, mobile device, or cloud-based social media platform. Digital forensic software makes images of digital data so that examiners can analyze it without modifying the original evidence.
- **Ingestion** - The process of adding digital data to digital forensic software. For example, adding artifacts extracted from an image to Magnet AXIOM.
- **Keyword** - A word which can be searched for and used to filter evidence.
- **Parsing** - The process of transforming data from one form to another, often to make the parsed data legible to humans.
- **Privileged content** - Information in Magnet AXIOM that is not relevant to a case or includes information that is deemed privileged by the courts or judicial system (for example, communications with a lawyer or a doctor).
- **Tag** - A label you can apply to artifacts in Magnet AXIOM to flag the significance of different pieces of evidence and help you categorize all the evidence that is collected.

- **YARA rule sets** - A kind of programming language typically used to detect instances of malware by defining variables that contain patterns found within the code of similar malware.

Functions

AXIOM Process and AXIOM Examine provide forensic examiners complementary sets of functionality.

Use **AXIOM Process** to:

- Acquire evidence from computer, mobile, and cloud sources
- Decrypt, scan, and extract information from supported forensic image and media formats

Use **AXIOM Examine** to:

- View and analyze captured evidence and extracted information
- Create exports and reports of notable evidence

Available features

Depending which AXIOM license you have, different features are available.

Note: If you bought or renewed your license before AXIOM 7.10, the license types may vary from those listed below. AXIOM Core Term customers have access to the same features as AXIOM Essentials. AXIOM Term customers have access to the same features as AXIOM Advanced.

Processing

Feature	AXIOM perpetual licenses	AXIOM Essentials	AXIOM Advanced	AXIOM Premier	AXIOM Cyber
Computer acquisition and processing	X (license dependent)	X	X	X	X
Mobile device acquisition and processing (including GRAYKEY integration)	X (license dependent)	X	X	X	X
Cloud acquisition (included platforms vary depending on license)	X (optional)		X	X	X
Remote computer acquisition					X
Processing of	X		X	X	X

Feature	AXIOM perpetual licenses	AXIOM Essentials	AXIOM Advanced	AXIOM Premier	AXIOM Cyber
select downloaded data packages	(optional)				
Warrant return processing	X (optional)		X	X	X
Vehicle forensics	X	X	X	X	X
Advanced keyword searching	X	X	X	X	X
Magnet.AI media categorization	X	X	X	X	X
Hash set integration	X	X	X	X	X
Privileged content search and exclusion	X	X	X	X	X
YARA rules					X
Comae memory analysis		X	X	X	X

Examining

Feature	AXIOM perpetual licenses	AXIOM Essentials	AXIOM Advanced	AXIOM Premier	AXIOM Cyber
Add, remove,	X	X	X	X	X

Feature	AXIOM perpetual licenses	AXIOM Essentials	AXIOM Advanced	AXIOM Premier	AXIOM Cyber
reprocess evidence					
Artifacts explorer	X	X	X	X	X
Case dashboard	X	X	X	X	X
Connections explorer	X	X	X	X	X
Create export / report	X	X	X	X	X
Email explorer			X	X	X
Extract text from files using OCR	X	X	X	X	X
File system explorer	X	X	X	X	X
Hex decoder	X	X	X	X	X
Magnet.AI categorization	X	X	X	X	X
Media explorer	X	X	X	X	X
Potential cloud evidence leads (Case dashboard)	X	X	X	X	X
Reduce exposure to illicit content (reminders and media obfuscation)	X	X	X	X	X
Registry explorer	X	X	X	X	X
Route view (Artifacts explorer)		X	X	X	X

Feature	AXIOM perpetual licenses	AXIOM Essentials	AXIOM Advanced	AXIOM Premier	AXIOM Cyber
Timeline	X	X	X	X	X
Update hash sets with new media categorizations	X	X	X	X	X
VirusTotal hash verification					X

Getting started with Magnet AXIOM

Using AXIOM Process, you can acquire forensic images, load existing images, and run scans on those images all from the same interface. After processing is complete, you can review the evidence in AXIOM Examine.

Start a case

Your first step is to start your case. You can create a new case in AXIOM Process, or if you've already created a case, you can also add evidence to an existing case by browsing to a case or opening a recent case. If you choose to add evidence to an existing case, certain information—such as the case number, search type, keyword lists, and more—will be locked down based on the settings from the original search.

If you skip a step that's required, AXIOM Process flags it with a warning symbol !, and you won't be able to start processing until the step is complete.

Provide case details

Specify basic information about your case such as the case number, the case type, where you want to save your case files and acquired evidence, and more. The details you provide here are included in several reports or export types such as portable case, JSON, HTML, and PDF.

Custom case types

AXIOM Process provides a set of default case types. However, you can also define your own case types. To define your own case types, create a text file called custom_types.txt in the root directory of AXIOM Process. The default location of AXIOM Process is C:\Program Files\Magnet Forensics\Magnet AXIOM\AXIOM Process. Enter each type on a new line. AXIOM Process supports ASCII, UTF-8, UTF-16, and UTF-32 encoding of the custom types file. Case types defined in the custom_types.txt file appear in the Custom Types list in the Case details page.

Define custom case types

1. Create a .txt file
2. Save the file as **custom_types.txt** in the root folder of AXIOM Process.
3. Enter each custom type on a new line.
4. Save your changes to the file.

Add your evidence sources

Add your evidence sources—computer, mobile, or cloud—and specify whether you are acquiring or loading evidence. Choose to acquire evidence if you want AXIOM Process to create an image of a computer drive, mobile device, or cloud-based social media platform. Choose to load evidence if you are uploading existing forensic images, files, or folders.

If you have multiple forensic images, you can add them all to the same case.

Configure processing details

Configure advanced processing features so that you can use to get more out of your search, such as adding keywords, calculating hash values, categorizing evidence using Magnet.AI, searching for custom file types, and more.

Configure artifact details

Select the artifacts that you want to include or exclude from your search. Depending on the type of license that you have, you might have computer artifacts, mobile artifacts, cloud artifacts, or a combination.

Analyze evidence

After you finish configuring each step in AXIOM Process, click **Analyze evidence** to start scanning the evidence. AXIOM Examine opens automatically to display any evidence that is recovered. The *Analyze evidence* screen indicates what percentage of the scan is complete along with information about search definitions and thread details.

After the search completes, there might be additional steps to complete. If you configured AXIOM Process to find more artifacts using the Dynamic App Finder, you might have to configure the artifacts that it discovers.

When a search completes, you can view a summary of the completed search—including any exceptions that might have occurred. You can also view the scan summary from the Case dashboard in AXIOM Examine. Unprocessed files are also tagged in AXIOM Examine with the *Exceptions* system tag.

Examine the evidence

You can examine your evidence in a number of different ways, including seeing an overview of your case using the Case dashboard or browsing the evidence using specific explorers. You can filter evidence to narrow your focus, tag and add comments to important evidence, categorize media evidence with Project VIC or CAID hash lists or your own lists, and more.

Export or share the evidence

You can export your evidence to share with other stakeholders in many different formats, including Excel, XML, HTML, PST, PDF, and more. You can also collaborate on a case with other examiners and stakeholders by creating a portable case.

ACQUIRE AND LOAD EVIDENCE

Add your evidence sources—computer, endpoint, mobile, or cloud—and specify whether you are acquiring or loading evidence. Choose to acquire evidence if you want AXIOM Process to create an image of a computer drive, mobile device, or cloud-based social media platform. Choose to load evidence if you are uploading existing forensic images, files, or folders.

If you have multiple forensic images, you can add them all to the same case.

Computer

Loading computer evidence

Supported evidence source	Supported OS	Description
Drives	Windows	Perform a triage investigation to load evidence from drives, such as HDD, SSD, USB, and SD flash, and more. AXIOM Process supports Windows drives. It is highly recommended to use an acquired image of the drive.
Files and folders	Windows Mac	Use this option to perform a triage investigation of

Supported evidence source	Supported OS	Description
	Linux Chromebook	files or folders that you have stored locally on your computer. This option supports files and folders from Windows, macOS (APFS, HFS+ and HFSX) Linux and Chromebook. It is highly recommended to use an image of the collection.
Images	Windows Mac Linux Chromebook	Load computer images. For information about the images that AXIOM Process supports, see the supported images and file types.
Volume shadow copy	Windows	Locate Volume Shadow Copy files that are present on a connected Windows drive or image.
Memory	Windows	Load Windows memory dump files.

Acquire computer evidence

AXIOM Process supports both acquiring connected Windows drives and loading evidence from the following computer evidence sources.

Supported evidence source	Supported OS	Description
Drives	Windows	Acquire evidence as an image from drives, such as HDD, SSD, USB, and SD flash, and more. AXIOM Process supports Windows drives.

AXIOM Process can obtain images from many types of Windows-based external drives that are physically connected to your computer such as:

- HDD
- SSD
- USB

- SD flash drives
- Other external drives

AXIOM Process can't detect and image network-attached storage (NAS) devices over the network. If the computer that's running AXIOM Process is connected directly to the NAS with a USB cable, detection of the device and imaging work as expected.

Acquire a drive

You can search images on network drives by providing a path to the network drive using the format \\drive\folder.

If you've installed the Passware plugin, AXIOM Process detects whether a drive is encrypted. For information about decrypting drives and cracking passwords, see Decrypting evidence.

1. In AXIOM Process, click **Evidence Sources** > **Computer** > **Windows** > **Acquire Evidence**.
2. Select a drive, and then click **Next**.
3. If prompted, provide encryption details for the drive.
4. Select the type of image you want to acquire, and then click **Next**.
5. From the **Search type** drop-down, select the type of search you want to complete for the drive.
6. To continue setting up your case, click **Next**.

Image options for drives

There are four imaging options for Windows-based drives that you can choose from. The option that you choose should reflect your time constraints and the type of data that you're looking for.

IMAGE TYPE		Description	EVIDENCE
Full	Entire contents of the drive in E01 format	These options represent a physical image of the drive and typically take the longest. During this type of acquisition, AXIOM Process copies the entire con-	A physical image of the entire drive.

IMAGE TYPE		Description	EVIDENCE
	Entire contents of the drive in raw format	tents of the drive into a single .E01 file or .raw file.	
	All files and folders	This option represents a logical image that contains all files and folders. During this type of acquisition, AXIOM Process copies all files and folders into a single, compressed .zip file. The .zip file maintains the original folder structure that existed on the drive. Depending on how many files are in the drive and the amount of logical data available, acquisition time will vary.	A full, logical file system image that includes all files and folders. This does not include deleted files and/or unallocated space.
Quick	Targeted acquisition	This option represents a logical image of the drive. During this type of acquisition, AXIOM Process copies files such as system files, user profiles, and more into a single, compressed .zip file. The locations that AXIOM Process targets are typically the ones that are most likely to contain evidence. This option is typically the fastest.	Pagefile, Hibernation File, Master File Table, USN Journal, Event Logs, Setup API Logs, Windows Registry Hives, LNK Files, User Profiles, Prefetch Files

Load computer evidence

AXIOM Process can load evidence from the following supported evidence source types:

Note: You can load evidence using the **Drive** or **Files and Folders** workflow however some information about the artifacts will not be available once the evidence source has been moved or modified. Whenever possible it's highly recommended to use an image as the evidence source.

Search types

Depending on your evidence type, you can select the type of search that you want AXIOM Process to run.

Tip: If you don't know the type of file system that you're running a search on, the file system is not supported using a full or quick search, or you don't have a password to decrypt the drive, use the Sector level option. Selecting the Sector level option forces AXIOM Process to search an evidence source bit by bit, so it doesn't matter how the file system is structured.

Search type	Description
Full	Searches all areas of a drive or image for artifacts. This method processes fragmented files more effectively than other methods.
Quick	Searches the most common areas of your computer where evidence can be found. Common areas include default application data directories, the Windows registry, user profiles, and My Documents.
Sector level	Reads raw data from the hard drive and searches for artifacts that can be carved out and pieced together from that data, with no understanding of the underlying files and folders.
Custom	A combination of any of the above options that you tailor to your specific needs.

Areas included in a Quick search

When completing a quick search, AXIOM Process searches common areas of the file system. Common areas include any paths that are specified as important by the artifacts you're including in your search as well as any Users and Documents and Settings folders. For Windows file system searches, AXIOM Process will also search the default locations of common browsers.

File system type	Items included in quick search
HFS	Swap file Common areas including: • Application support • Library • Users • Documents • Desktop • Downloads • Videos • Pictures • Root
NTFS	Page file and Swap file $LogFile $MFT Common areas including: • Documents and Settings • ProgramData • User directory • User local settings • Program Files

File system type	Items included in quick search
	- Program Files (x86) - Desktop
EXT	All files and folders
FAT and exFAT	All files and folders
YAFFS	All files and folders
F2FS	All files and folders
APFS	Quick search not available for APFS

Windows drive

> Note: You can load evidence using the **Drive** or **Files and Folders** workflow however some information about the artifacts will not be available once the evidence source has been moved or modified. Whenever possible it's highly recommended to use an image as the evidence source.

You can search any locally connected Windows-based media such as computer and USB drives without first imaging them. Select any attached media or any partitions within the drive instead.

If you can't see mapped drives, you can make them visible by adding a DWORD value to the registry. For more information about creating the DWORD value, sign in to the Customer Portal to review the following article: Show mapped drives in AXIOM Process.

If you've installed the Passware plugin, AXIOM Process detects whether a drive is encrypted. For information about decrypting drives and cracking passwords, see Decrypting evidence.

1. In AXIOM Process, click **Evidence Sources** > **Computer** > **Windows** > **Load evidence** > **Drive**.
2. Select the drives and partitions that you want to search, and then click **Next**.
3. If prompted, provide encryption details for the drive.
4. For each drive or partition, from the **Search type** drop-down, select the type of

search you want to complete for the drive.

5. To continue setting up your case, click **Next**.

Files and folders

AXIOM Process will search files and folders from Windows, macOS, Linux, and Chromebooks. During the search, AXIOM Process will automatically create an image (.zip) of the specified files and folders and save the image in the acquired evidence location.

> Note: Network locations (Mapped drives and Local network) are not currently supported for automatic local image creation. Copy the collection to a .zip on the examination workstation and use the .zip as the evidence source image.

Load a file or folder

If you can't see mapped drives, you can browse to the mapped file's original location using the Folder browser, or you can make them visible by adding a DWORD value to the registry. For more information about creating the DWORD value, log in to the Customer Portal to review the following article: Show mapped drives in AXIOM Process.

> Note: For files and folders on a mobile operating system, use the mobile evidence source option instead.

1. In AXIOM Process, click **Evidence sources** > **Computer** >**Windows**, **Mac**, or **Linux** > **Load evidence** > **Files and folders**.
2. Complete one of the following options:
   - From the displayed network or disks, browse to and select the files or folders you want to search, and then click **Next**.
   - Click **Folder browser** to browse to a folder stored locally on your computer, and then click **Select folder**.
   - Click **File browser** to browse a file stored locally on your computer, and then click **Open**.
3. Continue setting up your case.

Supported file systems

File system	Type	Supported data
Linux	ext2, ext3, ext4, F2Fs, XFS*, LVM2 (XFS*)	metadata
macOS	APFS, HFS+, HFSX	metadata
NAND	YAFFS2	metadata
Windows	NTFS	metadata (including metadata from the Master File Table and Windows Security), deleted files
	FAT12, FAT16, FAT32**	metadata, deleted files
	exFAT	metadata, deleted files, and deleted file metadata

* Only XFS version 5 supported.

**Last Accessed Date/Time artifacts from a FAT32 file system are saved as a Date/Time in UTC with a time value representing 12:00:00AM, for example, 26/09/00:00:00. For more information, sign in to the Support Portal to read the following article: FAT32 and Last Accessed Date/Time.

Image

AXIOM Process can search Windows, macOS, Linux, and Chromebook images from other evidence sources. For more information about the computer images that AXIOM Process supports, see the Supported images and file types.

You can also search images on network drives by providing a path to the network drive using the format \\drive\folder.

Load an image

When you load an image, if you've installed the Passware plugin, AXIOM Process can detect whether an evidence source is encrypted and the encryption method used (where possible). You can also attempt to decrypt software-encrypted evidence from an APFS-formatted macOS computer, without requiring the Passware plugin. For information about decrypting drives and cracking passwords, see Decrypting evidence.

1. In AXIOM Process, click **Evidence sources** > **Computer** > **Platform** > **Load evidence** > **Image**.
2. Browse to your file and click **Open**.
3. Select the partitions or specific files and folders that you want to include in your search.
4. If prompted, provide encryption details for the image.
5. To continue setting up your case, click **Next**.

Supported images and file types

Image/file type	Supported extensions	Segmented image support
Advanced Forensics File images	.AFF4, .AFF4-L *Some AFF4-L formats are unsupported*	*Supported*
**Archive files	.cpio, .cpio.gz, .crash, .docx, .hpak, .gz, .gzip, .pptx, .rar, .tar, .tar.gz, .tgz, .xlsx, .zip, .zip.001, .z00, .z01, .7z, .7z001	*Supported:* .gzip, .rar, .rar5, .zip, .zip.001, .7z.001
EnCase images	.E01, Ex01, .L01, .Lx01	*Supported*
FTK images	.AD1	
macOS disk images	.dmg	*Not supported*
RAW images	.bif, .bin, .dd, .dmp, .fip, .ima, .img, .mfd, .mem, .raw, .vfd	*Supported:* DD (.000, 001, .0000, .0001, .00001, etc.)
*Virtual machine images	.vdi, .vhd, .vhdx, VMDK, XVA	*Supported:* .vmdk flat-type segmented files (*-

Image/file type	Supported extensions	Segmented image support
		f001.vmdk, *-flat.vmdk)

* Virtual Machine artifacts listed in additional sources must be extracted from the source image and scanned separately.

**.zip files that were created using encoding different than AXIOM's default encoding, may not be properly displayed in AXIOM Examine. Sign in to the Support Portal to read the following article: Change the character set encoding in Magnet AXIOM to match the encoding of .zip files.

Volume shadow copy

Volume shadow copy runs as a service (volume shadow service) on a Windows computer to create backups or snapshots of files or volumes (including user files).

When you complete a full search of a disk, volume shadow copies are included but sometimes provide only partial results. You can use the *Volume shadow copy* option in AXIOM Process to natively parse a volume shadow copy—this option provides more detail about where artifacts were recovered from. You can select entire volume shadow copies or expand the copy to select specific files that you want to search.

To load a volume shadow copy:

1. In AXIOM Process, click **Evidence sources** > **Computer** > **Windows** > **Load evidence** > **Volume shadow copy**.
2. Depending on your evidence source, choose one of the following options:
   - To select a connected disk, click **Drive**.
   - To select an existing image, click **Image** and browse to your file.
3. Select the shadow copies or specific files that you want to include in your search.
4. To continue setting up your case, click **Next**.

Windows memory

Memory dumps contain a record of all the data currently stored in memory at the time the dump occurs. These files can contain information about a user's activity on the computer that might have otherwise been lost when the system crashed or was shut down. The information available in a memory dump can be especially helpful in incident response investigations as they contain information about which processes are running and which files are opened by the user.

You can acquire a memory dump from a target's computer using MAGNET DumpIt for Windows, Magnet RAM Capture, or a third-party product.

In AXIOM Process, you can load Windows memory dumps in their native file format (for example, .raw, core dumps, or .bin) and scan them for artifacts just like you would with a drive. For example, you can search for known malware and recover the names of processes and IP addresses, giving you insight into malware investigations.

Load memory dump file

AXIOM Process: **Computer** > **Windows** >**Load evidence** > **Memory** > **Load memory dump file**

To begin processing your memory dump, click **load memory dump file** and browse to select the memory dump file. If the memory dump is a valid file, proceed with selecting a memory plug-in.

Select a memory plug-in

Depending on your license and the memory dump file selected, you may have an additional option to use the Comae memory plug-in in addition to the Volatilty memory plug-in to perform memory analysis.

For more information about selecting a memory plug-in, sign in to the Support Portal to read the following article: Selecting memory plug-in with AXIOM Cyber.

Comae memory plug-in

You can use Comae to perform memory analysis of a Windows memory dump for the following conditions:

- Current active license that includes the Comae memory analysis feature. For more information, see Available features.
- The Windows memory dump is a core or mini-dump with a file header matching: PAGEU64, PAGEDUMP, or MDMP.

Internet connectivity is required for Comae to download files for application memory analysis.

In addition to offering support for newer operating systems such as Windows11, Comae can decrease processing time since you do not need to select a memory profile.

We recommend using the Comae plug-in to perform memory analysis on a crash dump generated by Magnet DumpIt for Windows since both products were developed by Comae Technologies.

> Note: By default, The MFT Memory artifact is not enabled since it can significantly increase processing time. See the following to view the settings for MFT scan
>
> 1. In AXIOM Process, click **Artifact details** > **Computer artifacts** > **Memory**
> 2. Select or clear the **MFT** option for the artifact.
> 3. Continue setting up your case.

Volatilty memory plug-in

Volatility supports the following images and file types for memory analysis.

Image/file type	Supported extensions
Crash dumps	.crash, .dmp
Other Volatility-supported formats	.hpak
Raw images	.raw, .dd, .img, .ima, .vfd, .flp, .bif, .bin, .dmg, .mem, .mdf
VirtualBox Core Dumps	.elf
Virtual Machine Saved State	.vmss, .vmsn, .vmem

When analyzing memory dumps using Volatility a memory profile is required. Each memory dump has a corresponding profile based on its operating system. You can indicate the profile or have AXIOM Process attempt to find the appropriate profile. Having AXIOM Process identify the memory profile could take considerable time, depending on the size of the memory dump.

See the following topic for more information about Volatity memory profiles

Include memory artifacts in your search

In AXIOM Process, you can specify the individual memory artifacts that you want to include in your search.

1. In AXIOM Process, click **Artifact details** > **Computer artifacts** > **Memory**.
2. Select the memory artifacts you want to search for.
3. Continue setting up your case.

If you used Volatility to scan the memory dump, each artifact corresponds to a Volatility command. For example, the Processes (pslist) artifact allows you to see which processes ran on a system, and the Process Security Identifiers (getsids) artifact allows you to view the Security Identifiers associated with processes. For more information about Volatility commands that correspond to memory artifacts, see the Volatility Foundation's Command Reference.

Volatity memory profiles

Find the Volatility profile of a memory dump

You can find the profile of a memory dump using the build number of its operating system. After you've located the build number, you can find a Volatility profile that matches the build at www.github.com/volatilityfoundation/volatility/wiki/2.6-Win-Profiles. To learn if the profile is supported by AXIOM Process, see Volatity memory profiles.

To find the build number, do one of the following:

- If the memory dump was recovered from a drive that was already processed using AXIOM Process, complete the following steps:
  1. Open the case in AXIOM Examine.
  2. In the Artifacts explorer, browse to the **Operating System Information** artifact and locate the **Version Number** fragment.
- If the memory dump is on a drive that hasn't been processed, complete the following steps:
  1. On the computer where the memory dump was created, press the **Windows key** + **R** to open the Run dialog.

2. In the **Run** dialog, type **winver** and click **OK**.
3. In the **About Windows** dialog, locate the **OS Build number**.

Load a memory dump with a known Volatility profile

If you know the profile of a memory image, you should manually select the profile to reduce scan time.

1. Browse to your memory dump file and click **Open**.
2. Select **I want to select the profile myself**.
3. In the **Image profile** drop-down list, select the appropriate image profile.
4. For faster memory analysis, in the **KDbg address** field, provide the Kernel Debug (KDbg) address of the profile.
5. To continue setting up your case, click **Next**.

Load a memory dump with an unknown profile

Each memory dump has a corresponding profile, based on its operating system. If you don't know the profile of a memory dump, AXIOM Process can perform a KDbg scan to attempt to find recommended profiles.

Warning: Performing a KDbg scan can take a significant amount of time.

1. Browse to your memory dump file and click **Open**.
2. Select **I want AXIOM Process to provide a list of recommended image profiles**, and then click **Next**.

   AXIOM Process performs a KDbg scan to attempt to identify the profile. You can view the results of this scan in the case summary text file in your case folder.

   Once AXIOM Process finishes identifying profiles, its recommendations appear in the **Image profile** drop-down list. If more than one recommendation appears, you can click **Advanced images profile selection** to view details about the recommended profiles and make an informed selection.

3. In the **Image profile** drop-down list, select an image profile.
4. To continue setting up your case, click **Next**.

Supported memory profiles

Windows version	Profiles
Windows 10	Win10x64
	Win10x64_10240_17770
	Win10x64_10586
	Win10x64_14393
	Win10x64_15063
	Win10x64_16299
	Win10x64_17134
	Win10x64_17763
	Win10x64_18362
	Win10x64_19041
	Win10x86
	Win10x86_10240_17770
	Win10x86_10586
	Win10x86_14393
	Win10x86_15063
	Win10x86_16299
	Win10x86_17134
	Win10x86_17763
	Win10x86_19041

Windows version	Profiles
Windows 2016	Win2016x64_14393
Windows 2012	Win2012R2x64 Win2012R2x64_18340 Win2012x64
Windows 8	Win81U1x64 Win81U1x86 Win8SP0x86 Win8SP1x64 Win8SP1x64_18340 Win8SP1x86
Windows 7	Win7SP0x64 Win7SP0x86 Win7SP1x64 Win7SP1x64_23418 Win7SP1x64_24000 Win7SP1x86 Win7SP1x86_23418 Win7SP1x86_24000
Windows 2008	Win2008R2SP0x64 Win2008R2sP1x64 Win2008R2SP1x64_23418 Win2008R2SP1x64_24000

Windows version	Profiles
	Win2008SP1x64 Win2008SP1x86 Win2008SP2x64 Win2008SP2x86
Windows Vista	VistaSP0x64 VistaSP0x86 VistaSP1x64 VistaSP1x86 VistaSP2x64 VistaSP2x86
Windows 2003	Win2003SP0x86 Win2003SP1x64 Win2003SP1x86 Win2003SP2x64 Win2003SP2x86
Windows XP	WinXPSP1x64 WinXPSP2x64 WinXPSP2x86 WinXPSP3x86

MFT File

The $MFT (Master File Table) file is found on NTFS (Windows) machines and maintains a record of file information such as:

- Directory location
- Physical location on the drive
- Metadata

In AXIOM Process, you can quickly parse the $MFT file to triage computers with suspicious activity.

After reviewing the results in AXIOM Examine you determine that a more thorough search is required, acquire an image of the computer (not just the $MFT) and process it.

Load MFT file

AXIOM Process: **Computer** > **Windows** >**Load evidence** > **MFT File** > **Select MFT file**

Decrypt evidence

For many evidence sources, if you installed the Passware plugin, AXIOM Process detects whether an evidence source is encrypted and, where possible, the type of encryption method that was used. You can also attempt to decrypt software-encrypted evidence from an APFS-formatted macOS computer, without requiring the Passware plugin.

For supported encryption types, you can provide known decryption credentials such as passwords and recovery keys, to decrypt the evidence source before AXIOM Process searches it. For some evidence sources, if you don't know the password, you can try cracking it–otherwise, AXIOM Process attempts a sector-level search of the drive.

For Windows 10 devices that have BitLocker Device Encryption turned on (including many Microsoft Surface Pro devices), AXIOM Process will automatically decrypt the device if the encryption is suspended, also known as a clear key state. If AXIOM Process is unable to automatically decrypt the device, you're prompted to provide known decryption credentials for the device.

In AXIOM Process, a locked icon appears beside both decrypted and encrypted partitions, as it's not guaranteed that AXIOM Process will successfully decrypt the drive.

During a search, AXIOM Process adds the decrypted evidence source and the password that successfully decrypted the evidence source to the Location for acquired evidence that you configured for the case. For decrypted evidence from a macOS computer with the APFS file system, you'll find a decrypted image for each partition. Before you attempt to decrypt an evidence source, make sure you have enough space for the decrypted images.

Supported encryption types

Encryption type	What's supported
BitLocker	All versions up to and including Windows 10, including BitLocker To Go Note: If the device was encrypted on a system with a TPM (Trusted Platform Module), the recovery key is required to decrypt the image. The password will not decrypt the image.
DriveCrypt	DriveCrypt 5.8 and later DriveCrypt 5.44 and later
FileVault and FileVault 2	All versions of macOS formatted with HFS+ (non-system partitions are not supported) or APFS
McAfee Drive Encryption	McAfee 7.x and later (non-system partitions are not supported)
PGP Whole Disk Encryption (PGP WDE)	PGP Desktop 9.x - 10.x (encrypted drives can't currently be decrypted using administrator credentials)
Symantec Endpoint Encryption	All versions (requires Symantec Endpoint Encryption account password)
TrueCrypt	TrueCrypt 5.0 and later (hidden and system partitions are not supported)
VeraCrypt	All current versions are supported with the exception of UEFI. Encryption ciphers supported: AES, Serpent, Twofish

Encryption type	What's supported
	Encryption ciphers not supported: Kyznyechik, Magma, Carmellia Hash functions supported: RIPEMD-160, SHA256, SHA512, Whirlpool Hash functions not supported: Streebog

Known password or recovery key

If you know the password or recovery key for an evidence source, you can attempt to decrypt it. For evidence from a macOS computer with the APFS file system, AXIOM Process supports user passwords or personal recovery keys, and, in some cases, might be able to display a password hint.

1. In the **Decryption option** drop-down list, click **I have the password/recovery key**.
2. In the **Password/Recovery key** field, provide a password or recovery key.
3. To verify that the password is correct, click **Check**.
4. To finish setting up your case, click **Next**.

FileVault-encrypted evidence source with a password and a wipe key

You need both a password and a wipe key to decrypt a macOS (HFS+ and HFSX) evidence source that is encrypted by FileVault. To recover the wipe key, search the recovery partition of the macOS computer.

1. In AXIOM Process, click **Evidence Sources** > **Computer** > **Mac** > **Files and folders**.
2. Select the check box beside the recovery partition.
3. Finish setting up your case.
4. Once processing is complete, extract the following file: **EncryptedRoot.plist.wipekey**. This file is usually stored at **\Recovery HD\com.apple.boot.P\System\Library\Caches\com.apple.corestorage\EncryptedRoot.plist.wipekey**.

To decrypt the evidence source:

1. In AXIOM Process, click **Evidence Sources** > **Computer** > **Mac** > **Images** or **Files and folders**.
2. Browse to or select the evidence source you want to decrypt, and then click **Next**.
3. In the **Key file** field, provide the wipe key.
4. In the **Password** field, provide the known password.
5. To verify that the password is correct, click **Check**.
6. For each item, select the type of search you want to complete.
7. To continue setting up your case, click **Next**.

McAfee-encrypted evidence source with a machine key

If you don't know the password for a McAfee-encrypted evidence source, you can attempt to decrypt it using a machine key. Machine keys are Base64 strings that must be 44 characters long and are unique to each computer. If you provide a machine key in the correct format but the key is incorrect (for example, the key is not associated with the evidence you are trying to decrypt), AXIOM Process attempts to decrypt the evidence source but creates an image without any results.

You obtain a machine key from the McAfee administrator. You find the key at the bottom of the XML file, between the <MfeEpeExportMachineKey> tags.

In AXIOM Process, when you attempt to decrypt a drive, only the largest partition appears to be available, as McAfee encrypts entire drives and not individual partitions.

1. In the **Decryption option** drop-down list, click **I have the machine key**.
2. In the **Machine key** field, paste the 44-character machine key from the XML file.
3. To verify that the password is correct, click **Check**.
4. To continue setting up your case, click **Next**.

VeraCrypt-encrypted partition with a password and a PIM

You need both a password and a Personal Iterations Multiplier (PIM) to decrypt VeraCrypt-encrypted partitions. The PIM specifies the number of iterations used by the header key derivation function. The higher the PIM, the more secure the encryption is. For more information about the PIM, see the VeraCrypt PIM documentation.

Note: If you enter the wrong PIM, VeraCrypt won't be able to decrypt the partition.

1. In the **Decryption option** drop-down list, select **I have the password**.
2. In the **Password** field, provide the known password.
3. In the **Personal iterations multiplier** field, provide the **PIM**.
4. To verify that the PIM and password are correct, click **Check**.
5. To continue setting up your case, click **Next**.

Crack the password

To crack the password of a drive, you must be using AXIOM Process with the Passware plugin. You must also have a password list file in .txt format.

With the dictionary attack capabilities of the Passware plugin, you can use custom password lists, in .txt format, to attempt to decrypt drives, mobile devices, and images. Passware reads each new line as a separate password. Additionally, Passware reads spaces at any point in the line as part of the password.

You can use the AXIOM Wordlist Generator to retrieve a list of keywords from the devices in your case. This tool writes keywords to a .txt file that you can use to decrypt drives, mobile devices, and images.

McAfee, APFS, and FileVault-encrypted evidence sources can't be decrypted using password cracking.

Warning: Password cracking can take a significant amount of time and system resources, and isn't guaranteed to work. To save time, consider cracking encrypted sources separately from sources with known passwords.

1. In the **Decryption option** drop-down list, select **I want to crack the password**.
2. Click **Browse** and browse to the location of the .txt file.
3. To continue setting up your case, click **Next**.

The Analyze evidence screen displays the cracking progress and the number of passwords that have been attempted. If the drive is successfully decrypted, the blue locked icon changes to the blue unlocked icon and AXIOM Process begins searching the drive immediately.

If password cracking is successful, that source is skipped during processing. You can find the correct password, decryption duration, and more in the Passware XML report file. This file is located in your case folder and will have a similar name to the decrypted image.

Cloud

Acquire cloud evidence

Use AXIOM Cloud to get the most complete story using data from the cloud. In addition to cloud-based user accounts, you can ingest warrant return packages, user-requested archive files (for example, Google Takeout), and publicly available information from Twitter and Instagram.

With a AXIOM Cyber license, you can access Microsoft 365 and Google Workspace accounts with administrator credentials and selectively acquire evidence, and you can acquire evidence from Amazon S3 and EC2, and Microsoft Azure virtual machines.

AXIOM Cloud is available with a valid cloud license. To find out how to purchase a cloud license, contact sales@magnetforensics.com.

Acquired evidence encryption

All cloud-based evidence source acquisitions are encrypted, and the encryption methods vary for each source.

Changes to supported cloud services and content

When acquiring cloud evidence, AXIOM Process acquires live data. If a supported platform makes a change to their product, this change might affect the types of services or content AXIOM Process can acquire and process. For a current list of any known changes to our ability to acquire data from our supported platforms (including specific artifacts that might be impacted), please log in to the Customer Portal to read the following article: Status of supported cloud acquisition platforms.

Amazon

You can acquire evidence from the following Microsoft User account services:

S3 Files

EC2 Export

EC2 Snapshot

Support data sources by authentication type

The following types of data can be acquired from an AWS account.

Amazon Web Services

Authentication type	2FA/MFA support	Data sources
Security credentials	✓	• AWS S3 Files • AWS EC2 Export • AWS EC2 Snapshot
Session credentials	N/A	• AWS S3 Files • AWS EC2 Export

For a complete list of supported cloud data sources by authentication type, review supported cloud data sources by authentication type.

S3 Files

Step 1: Sign in to an AWS account

To sign in to and acquire S3 files, you must provide authentication details for the AWS account required for your organization's AWS configuration. Depending on your organization's AWS configuration, you might be prompted to provide additional authentication details. You can find these authentication details in the AWS Management Console. For more information about how to find each of the required authentication details, review the Find AWS authentication details article in the Magnet Forensics Support Portal.

1. In AXIOM Process, click **Evidence sources** > **Cloud** > **Acquire evidence**.
2. Confirm that you have proper search authorization.
3. Click **Amazon**.
4. Provide the required authentication details for the AWS account.
5. Click **Sign in**.

Step 2: Select a date range

After you gain access to the Amazon account, you can select a date range to acquire data from. By default, AXIOM Process acquires data from as far back in time as possible for the account. Acquiring some accounts can take a long time depending on the amount of data they contain, so you might want to narrow the date range to decrease the amount of time the acquisition takes.

1. In the **Date range** drop-down list, select one of the following options:
   - To acquire data *after* a specified date, click **After**.
   - To acquire data *before* a specified date, click **Before**.
   - To acquire data *between* two specified dates, click **Custom date range**.
2. Click the **calendar icon** and choose a date.

Step 3: Select services and content

After you gain access to the AWS account, you can specify that you want to acquire an S3 bucket, and then select the buckets or files that you want to download.

1. In **Select services and content**, select the **S3 Files** source type option.
2. In the **Content** column, click **Edit.**
3. Select the buckets or files that you want to acquire.
4. To continue setting up your case, click **Next**

Supported data sources by authentication type

The following types of data can be acquired from an Amazon S3 bucket.

Amazon Web Services

Authentication type	2FA/MFA support	Data sources
Security credentials	✓	• AWS S3 Files • AWS EC2 Export • AWS EC2 Snapshot
Session credentials	N/A	• AWS S3 Files • AWS EC2 Export

EC2 Export

When you create a new case in AXIOM Process, you can acquire a single EC2 instance with a single S3 bucket. If you want to acquire additional instances, add them as a new evidence source after the original search completes.

AXIOM Process supports acquiring EC2 instances for Amazon Linux and Ubuntu Server SSD volume types.

Amazon does not allow direct downloading from an EC2 instance, so to acquire evidence from an EC2 instance, AXIOM Process initiates an export in AWS which copies the EC2 instance and its associated drives to create an image. AWS then exports this image to an S3 bucket.

When acquiring an EC2 instance, you do not need to specify a date range. Date ranges are applicable to directly acquiring S3 buckets only.

Note: There are typically costs associated with transferring data from AWS over the internet to a local machine. When you acquire evidence from AWS, you might be charged a nominal fee per GB of data downloaded based on your storage plan. For more information about specific charges you might incur, please consult the Amazon S3 pricing plans.

Prerequisites for acquiring an EC2 instance

To acquire evidence from an Amazon EC2 instance, there are several prerequisites you should be aware of. For detailed information about how to prepare for acquiring an EC2 instance, review the prerequisites for acquiring an EC2 instance article in the Magnet Forensics Support Portal.

Step 1: Sign in to an AWS account

To sign in to and acquire an EC2 instance, you must provide authentication details for the AWS account required for your organization's AWS configuration. Depending on your organization's AWS configuration, you might be prompted to provide additional authentication details. You can find these authentication details in the AWS Management Console. For more information about the authentication details required and where to find them, review the Prepare the AWS authentication details for AXIOM article in the Magnet Forensics Support Portal.

1. In AXIOM Process, click **Evidence sources** > **Cloud** > **Acquire evidence**.
2. Confirm that you have proper search authorization.
3. Click **Amazon**.
4. Provide the required authentication details for the AWS account.
5. Click **Sign in**.

Step 2: Select services and content

After you gain access to the AWS account, you can specify that you want to acquire an EC2 instance, and then select the EC2 instance that you want to download.

1. In **Select services and content**, select the **EC2 Export** source type option.
2. In the **Content** column, click **Edit.**
3. In the **Select EC2 instances to download** section, search for the EC2 instance or

click **View all instances**.

4. In the table, select the EC2 instance that you want to download, and then click **Next**.

Supported data sources by authentication type

The following types of data can be acquired from an Amazon EC2 instance.

Amazon Web Services

Authentication type	2FA/MFA support	Data sources
Security credentials	✓	• AWS S3 Files • AWS EC2 Export • AWS EC2 Snapshot
Session credentials	N/A	• AWS S3 Files • AWS EC2 Export

For a complete list of supported cloud data sources by authentication type, review supported cloud data sources by authentication type.

Step 3: Define export details

To download an EC2 instance, AXIOM Process initiates an export in AWS. This export copies the EC2 instance and all of the drives associated with it to create an image. Next, AWS exports the image to an S3 bucket.

To export an image to an S3 bucket, you must provide some information about the export such as the disk image format and the S3 bucket you want to export the image to. To help organize your evidence in the S3 bucket, you can optionally provide a prefix to add to the name of the image of the EC2 instance. For example, you could add the target's name as the prefix value.

AXIOM Process supports VHD, VMDK, and RAW disc images formats for images of an EC2 instance.

1. In the **Export description** field, provide a description for the exported EC2 instance.
2. In the **Disk image format** drop-down, select a format for the image of the exported EC2 instance.

3. In the **S3 bucket** field, type the name of the S3 bucket where you want to store the image.
4. In the **S3 prefix** field, optionally provide a prefix to add to the name of the image of the EC2 instance.
5. When you've finished selecting services and content, click **Next** to continue setting up your case.

> Note: Storing an image of an EC2 instance in an S3 bucket might incur monthly costs. After you've successfully acquired the EC2 instance, consider removing the image from the S3 bucket to avoid additional expenses.

EC2 Snapshot

When you create a new case in AXIOM Process, you can acquire multiple or a single EC2 instance to snapshot.

AXIOM Process supports acquiring EC2 snapshots for all volumes, including encrypted.

When acquiring an EC2 snapshot, you do not need to specify a date range. Date ranges are applicable to directly acquiring S3 files only.

> Note: There are typically costs associated with transferring data from AWS over the internet to a local machine. When you acquire evidence from AWS, you might be charged a nominal fee per GB of data downloaded based on your storage plan. For more information about specific charges you might incur, please consult the Amazon S3 pricing plans.

Prerequisites for acquiring an EC2 instance

To acquire evidence from an Amazon EC2 instance, there are several prerequisites you should be aware of. For detailed information about how to prepare for acquiring an EC2 instance, review the prerequisites for acquiring an EC2 instance article in the Magnet Forensics Support Portal.

Step 1: Sign in to an AWS account

To sign in to and acquire an EC2 snapshot, you must provide authentication details for the AWS account required for your organization's AWS configuration. Depending on your organization's AWS configuration, you might be prompted to provide additional authentication details. You can find these authentication details in the AWS Management Console.

For more information about the authentication details and permissions required, sign in to the Support Portal to read the following article: Defining AWS snapshot details in AWS.

1. In AXIOM Process, click **Evidence sources** > **Cloud** > **Acquire evidence**.
2. Confirm that you have proper search authorization.
3. Click **Amazon**.
4. Provide the required authentication details for the AWS account.
5. Click **Sign in**.

Step 2: Select data to acquire

After you gain access to the AWS account, select EC2 Snapshot, and then select the EC2 instances to snapshot.

1. In **Select data to acquire**, select the **EC2 Snapshot** option and then click **Add to selection**.
2. In the **Select EC2 instances to snaphot** section, search for or select the EC2 instances. Click **Next**.

Step 3: Define snapshot details

When acquiring an EC2 snapshot, you can acquire the snapshot in the context of a **Target account** or a **Security account**. The context you select determines which values AXIOM requires to acquire the snapshot.

Target account

The acquisition of the AWS snapshot occurs within the target account. This means that the new volume, the forensic imaging instance, and the S3 destination bucket, are all within the same space as the target instances being investigated.

Security account

The acquisition of the AWS snapshot is completed in a separate account from the target account. The encrypted snapshots are then created using a KMS key from the target account's volumes and then shared with the security account. The forensic account role is assumed and the remaining steps are completed within this security account. Snapshots are attached to a forensic imaging ec2 instance to manage the imaging process. Once the imaging process completes, the images are available in an S3 bucket within the security account.

For more detailed descriptions of the options, required permissions, and to downloads scripts to facilitate the export details, sign in to the Support Portal to read the following article: Defining AWS snapshot details in AWS.

Step 4: Items to acquire

Once the status of all the data source items indicate **Done**, click **Next** to proceed with the acquisition.

Supported data sources by authentication type

The following types of data can be acquired from an AWS account.

Amazon Web Services

Authentication type	2FA/MFA support	Data sources
Security credentials	✓	• AWS S3 Files • AWS EC2 Export • AWS EC2 Snapshot
Session credentials	N/A	• AWS S3 Files • AWS EC2 Export

For a complete list of supported cloud data sources by authentication type, review supported cloud data sources by authentication type.

Cloud-based user accounts

To acquire evidence from the cloud, you can sign in to an account with the target's user name and password, or–for some platforms–an authentication token that AXIOM Process discovers during a search or creates itself. For some cloud platforms, you can also acquire activity that is accessible to the public.

For a list of the supported cloud platforms and the license required, see Supported cloud platforms and services.

Preparing a cloud account for acquisition

For more information about preparing cloud accounts for acquisition, see the help topic for the cloud platform you are trying to acquire.

Acquire a cloud user account

When you create a new case in AXIOM Process, you can acquire a single account for each cloud platform or service. If you want to add additional accounts, Add, remove, or reprocess evidence in a case after the original search completes.

After your search completes, you can find the login credentials for each cloud account that you acquire in the **Cloud Accounts Information** artifact in AXIOM Examine so that you can easily acquire additional information from the account later. You can also acquire additional information from the cloud by Acquire more data from a cloud account found during a search or decrypting a WhatsApp backup using a recovered decryption key.

Each service and platform is saved in a separate folder, each containing an attachments folder. The files are saved in the same structure that appears in the account online and in the File system view in AXIOM Examine.

If your agency requires that you use AXIOM Process through a proxy server, you can still use AXIOM Cloud to acquire users' accounts for Box.com, Dropbox, Facebook, Google, Instagram, and Microsoft. For more information about how to use AXIOM Process through a proxy server, see Connect to the internet using a system proxy.

Change the container type for cloud acquisitions

You can save cloud acquisitions in AFF4-L or ZIP containers. The default container type for cloud acquisitions is AFF4-L.

1. In AXIOM Process, on the **Tools** menu, click **Settings**.
2. In **Imaging** > **Cloud acquisition container**, select one of the following options:
    - AFF4-L
    - ZIP
3. Click **Okay**.

Supported cloud platforms and services

Platform / service	AXIOM Cloud	AXIOM Cyber
Amazon Web Services		✓
Apple	✓	✓
Box.com (User)	✓	✓
Box.com (Admin)		✓
Dropbox	✓	✓
Facebook	✓	✓
Google (User)	✓	✓
Google (admin)		✓
IMAP / POP	✓	✓
Instagram (User account)	✓	✓
Instagram (Public activity)	✓	✓
Lyft	✓	✓
Mega	✓	✓
Microsoft (User)	✓	✓
Microsoft (Microsoft 365 Admin)		✓

Platform / service	AXIOM Cloud	AXIOM Cyber
Microsoft Azure		✓
Microsoft Teams		✓
Slack		✓
Twitter (User account)	✓	✓
Twitter (Public activity)	✓	✓
Uber	✓	✓
WhatsApp (Google Drive Backup)	✓	✓
WhatsApp (QR code access)	✓	✓

For a complete list of supported cloud data sources by authentication type, review supported cloud data sources by authentication type.

Apple

When you acquire an Apple user account, you must take the following steps:

1. Authenticate the account
2. Select the data to acquire

Before you begin, see Acquire a cloud user account for considerations that apply to all cloud account acquisitions.

Authenticate the account

> Note: When AXIOM Process gains access to an account, the owner of the account might receive an email notifying them that someone has signed in to their account.

When acquiring an Apple account, you can authenticate using the username and password, or a token. The types of data that you can acquire using the username and password or token authentication methods is the same, however the data available might be limited to the permissions of the token.

Authentication steps

1. In AXIOM Process, click **Evidence sources** > **Cloud** > **Acquire evidence**.
2. Confirm that you have proper search authorization.
3. Click **Apple**.
4. Authenticate with your chosen method.

Select the data to acquire

Select a date range

After you gain access to a cloud account, you can select a date range to acquire data from. By default, AXIOM Process acquires data from as far back in time as possible for the account. Acquiring some accounts can take a long time depending on the amount of data they contain, so you might want to narrow the date range to decrease the amount of time the acquisition takes.

1. In the **Date range** drop-down list, select one of the following options:
   - To acquire data *after* a specified date, click **After**.
   - To acquire data *before* a specified date, click **Before**.
   - To acquire data *between* two specified dates, including those dates selected, click **Custom date range**.
2. Click the **calendar icon** and choose a date.

Supported data sources by authentication type

The following types of data can be acquired from an Apple account.

Apple

Authentication type	2FA/MFA support	Data sources
Username/Password	✓ SMS code verification is not supported	• iCloud Backup • iCloud Drive • iCloud Mail • iCloud Photos

Authentication type	2FA/MFA support	Data sources
		• iMessage

For a complete list of supported cloud data sources by authentication type, review supported cloud data sources by authentication type.

- iCloud drive files
- iCloud photos - AXIOM Process acquires all photos within the date range. Last activity is noted in the evidence source.
- iCloud mail - AXIOM Process acquires all mail within the date range, including any that is deleted or placed in folders.
- iCloud backup - AXIOM Process acquires all backups available within the date range for each device in the account. An iCloud backup contains a copy of the information from participating devices, synced to iCloud. iCloud backup data can include:
    - App data
    - Apple watch backups
    - Device settings
    - Home screen and app organization
    - iMessage, SMS, and MMS messages
    - Photos and videos (iPhone, iPad, and iPod touch devices only)
    - Purchase history from Apple services
    - Ringtones
    - Visual Voicemail password (requires the SIM card that was in use during backup)
- iMessage - AXIOM Process acquires all iMessages associated for the authenticated user account.

Select the services

From the **Select services and content** section, select the content you want to acquire and then click **Next**.

Box.com

When you acquire a Box.com user account, you must take the following steps:

1. Prepare the account to be acquired
2. Authenticate the account
3. Select the data to acquire

Before you begin, see Acquire a cloud user account for considerations that apply to all cloud account acquisitions.

Prepare the account to be acquired

Before you acquire the account, you might need to perform some steps that will allow the account to be acquired. Review the following articles to help you prepare the account:

- To acquire a Box.com account, you might need to configure the Admin Console in Box.com to allow access to AXIOM Process. If the Box.com administrator limited which third-party applications can connect to the Box.com account, you'll receive an error. For more information on how to ensure the account is ready for acquisition, see Configure a Box.com account for acquisition.
- A co-admin account must have Edit settings and apps for your company enabled to acquire other accounts. For steps on how to configure a co-admin account with Edit settings, see Configure a Box.com co-admin account to acquire accounts.

Authenticate the account

> Note: When AXIOM Process gains access to an account, the owner of the account might receive an email notifying them that someone has signed in to their account.

You can authenticate a Box.com account using a username and password or using a token. The data that can be acquired differs based on the type of account (user or admin) that you are acquiring. The authentication method does not change the data that can be acquired.

Authentication steps

1. In AXIOM Process, click **Evidence sources** > **Cloud** > **Acquire evidence**.
2. Confirm that you have proper search authorization.
3. Select **Box.com**.
4. Authenticate with your chosen method.

Select the data to acquire

Data by account type

The type of data that you can acquire from a Box.com account varies depending on the type of account you are logged in as.

Account type	Files and folders	User events	Enterprise events
User/admin	✓ Includes last modified date and size	✓	
Admin	✓ Includes last modified date and size, as well as files and folders from other accounts.		✓

Select a date range

After you gain access to a cloud account, you can select a date range to acquire data from. By default, AXIOM Process acquires data from as far back in time as possible for the account. Acquiring some accounts can take a long time depending on the amount of data they contain, so you might want to narrow the date range to decrease the amount of time the acquisition takes.

1. In the **Date range** drop-down list, select one of the following options:
   - To acquire data *after* a specified date, click **After**.
   - To acquire data *before* a specified date, click **Before**.
   - To acquire data *between* two specified dates, including those dates selected, click **Custom date range**.
2. Click the **calendar icon** and choose a date.

Supported data sources by authentication type

The following types of data can be acquired from a Box.com account.

Box.com

Authentication type	2FA/MFA support	Data sources
Username/Password	✓	• Box.com Enterprise Events • Box.com Files • Box.com User Events
Token	N/A	• Box.com Enterprise Events • Box.com Files • Box.com User Events

For a complete list of supported cloud data sources by authentication type, review supported cloud data sources by authentication type.

Select the services

From the **Select services and content** page, select the content you want to acquire and then click **Next**.

Dropbox

When you acquire a Dropbox account, you must take the following steps:

1. Authenticate the account
2. Select the data to acquire

Before you begin, see Acquire a cloud user account for considerations that apply to all cloud account acquisitions.

Authenticate the account

> Note: When AXIOM Process gains access to an account, the owner of the account might receive an email notifying them that someone has signed in to their account.

When acquiring a Dropbox account, you can authenticate using the username and password, or a token. The types of data that you can acquire using the username and password or token authentication methods is the same, however the data available may be limited to the permissions of the token.

Authentication steps

1. In AXIOM Process, click **Evidence sources** > **Cloud** > **Acquire evidence**.
2. Confirm that you have proper search authorization.
3. Click **Dropbox**.
4. Authenticate with your chosen method.

Select the data to acquire

You can acquire files and folders from Dropbox. By default, AXIOM Process acquires data from as far back in time as possible for the account. Acquiring some accounts can take a long time depending on the amount of data they contain, so you might want to narrow the date range to decrease the amount of time the acquisition takes. The date range logic applies to the following metadata properties and includes files that match the "from" and "to" date:

- Client modified: The modification time set by the desktop client when the file was added to Dropbox. This time is not verified and should not be used to determine if a file has changed or not.
- Server modified: The last time the file was modified on Dropbox.
- Time taken: The timestamp when the photo or video was taken.

Select a date range

1. In the **Date range** drop-down list, select one of the following options:
   - To acquire data *after* a specified date, click **After**.
   - To acquire data *before* a specified date, click **Before**.
   - To acquire data *between* two specified dates, click **Custom date range**.
2. Click the **calendar icon** and choose a date.

Supported data sources by authentication type

The following types of data can be acquired from a Dropbox account.

Dropbox

Authentication type	2FA/MFA support	Data sources
Username/Password	✓	Dropbox Files
External Browser Authentication	✓	Dropbox Files
Token	N/A	Dropbox Files

For a complete list of supported cloud data sources by authentication type, review supported cloud data sources by authentication type.

Select the services

From the **Select services and content** section, select the content you want to acquire and then click **Next**.

Facebook

When you acquire a Facebook user account, you must take the following steps:

1. Authenticate the account
2. Select the data to acquire

Before you begin, see Acquire a cloud user account for considerations that apply to all cloud account acquisitions.

Authenticate the account

> Note: When AXIOM Process gains access to an account, the owner of the account might receive an email notifying them that someone has signed in to their account.

When acquiring a Facebook account, you can only authenticate using the username and password.

Authentication steps

1. In AXIOM Process, click **Evidence sources** > **Cloud** > **Acquire evidence**.
2. Confirm that you have proper search authorization.
3. Click **Facebook**.
4. Authenticate with your username and password.

Select the data to acquire

Select a date range

By default, AXIOM Process acquires data from as far back in time as possible for the account. Acquiring some accounts can take a long time depending on the amount of data they contain. Using a date range will not affect acquisition time. The date range logic applies to posts and messages posted or sent within the date range, including the dates selected.

1. In the **Date range** drop-down list, select one of the following options:
   - To acquire data *after* a specified date, click **After**.
   - To acquire data *before* a specified date, click **Before**.
   - To acquire data *between* two specified dates, click **Custom date range**.
2. Click the **calendar icon** and choose a date.

Supported data sources by authentication type

The following types of data can be acquired from a Facebook account.

Facebook Public

Authentication type	2FA/MFA support	Data sources
Customer Provided account Username/Password	✓	• Friends list • Profile information • Timeline posts

Facebook User Account

Authentication type	2FA/MFA support	Data sources
Username/Password	✓	• Friends list • Profile information • Mobile timeline posts • Messenger messages

For a complete list of supported cloud data sources by authentication type, review supported cloud data sources by authentication type.

Select the services

From the **Select services and content** section, select the content you want to acquire and then click **Next**.

Google

When you acquire a Google user account, you must take the following steps:

1. Prepare the account to be acquired
2. Authenticate the account
3. Select the data to acquire

Before you begin, see Acquire a cloud user account for considerations that apply to all cloud account acquisitions.

Prepare the account to be acquired

Before you acquire the account, you might need to perform some steps that will allow the account to be acquired. Consider if any of the following scenarios applies to you:

- To allow Magnet AXIOM to access data from user accounts under an administrator's Google Workspace account, you must configure the administrator account to give read-only access to user data in the domain. For steps on how to configure these settings in the admin console, see Configure the Google Admin console to give access to Google Workspace user accounts
- Two-factor authentication is used to verify a user's identity by requiring extra authentication information, such as a number code in addition to login credentials. For more information on how to access the additional authentication information, see Accessing cloud accounts that use two-factor authentication.

Authenticate the account

Note: When AXIOM Process gains access to an account, the owner of the account might receive an e-mail notifying them that someone has signed in to their account.

There are a few different authentication methods you can use when acquiring a Google account. Each authentication method gives you access to different types of data on the target account. The data that you can acquire from an account differs between admin and user accounts, regardless of the authentication method used. The authentication methods include:

- Username and password - Use this option if you have the user name and password of the account. For more information on the differences between acquiring a user and admin account, see Authenticate a Google account using the user name and password through AXIOM Process or AXIOM Cloud Authenticator
- Google Chrome authentication (advanced) - Use this option if you are having trouble authenticating in AXIOM Process. You must download the AXIOM Cloud Authenticator browser extension before authenticating.

After you authenticate the account, close the browser window and return to AXIOM Process to continue with the acquisition. Any additional browser activity will be logged against the target account.

- For more information on the differences between acquiring a user and admin account, see Authenticate a Google account using the user name and password through AXIOM Process or AXIOM Cloud Authenticator.
- External browser authentication - Use this option if you are having trouble authenticating in AXIOM Process.
- Account token - Use this option if you have an account token that you found in a search. For more information on locating and using a token from a search, see Add cloud evidence using recovered passwords and tokens.

For instructions on how to authenticate the account, see Authentication steps. For more information on selecting data from the account, see Select the data to acquire.

Authenticate a Google account using the user name and password through AXIOM Process or AXIOM Cloud Authenticator

A Google Workspace administrator has different privileges than other users. With an administrator account, you can access data from the signed-in account, as well as the user accounts that the administrator has access to. If you choose to access admin account data only, you will only have access to the data from the admin account that you provide credentials for. Logging in with the account's user name and password or through gives you access to all data in the account.

When you are acquiring data from an admin and user account, be aware that the date range configured applies to all selected accounts, however the type of data that you acquire from each account is set on a per account basis. Accounts that do not have read access cannot be added as evidence sources.

Authentication steps

1. In AXIOM Process, click **Evidence sources** > **Cloud** > **Acquire evidence**.
2. Confirm that you have proper search authorization.
3. Select **Google**.
4. Authenticate with your chosen method.
5. (Optional for admin accounts authenticated with user name and password) Add user accounts:
    a. Select **Add user accounts**.
    b. In the Add user accounts dialog, search for an account.

       You can search against user names and email addresses. Accounts with read access as well as those that do not have read access are included in the search.
    c. To select an account, you can select a result from the auto suggestion list, or after entering a search value, press **Enter** and then select one or more accounts from the table.
    d. Click **Add accounts** to add the selected accounts as evidence sources.
6. If you authenticated with an admin account and you want to add it to the acquisition, select **Add authenticated admin account**.
7. To set the data to be acquired for each account, click **Select data to acquire** next to the account you want to configure.

Select the data to acquire

Select a date range

After you gain access to a cloud account, you can select a date range to acquire data from. By default, AXIOM Process acquires data from as far back in time as possible for the account. Acquiring some accounts can take a long time depending on the amount of data they contain, so you might want to narrow the date range to decrease the amount of time the acquisition takes.

1. In the **Date range** drop-down list, select one of the following options:
   - To acquire data *after* a specified date, click **After**.
   - To acquire data *before* a specified date, click **Before**.
   - To acquire data *between* two specified dates, including those dates selected, click **Custom date range**.
2. Click the **calendar icon** and choose a date.

When acquiring Google Drive, AXIOM Process acquires all files and folders that are present within the date range even if the relevant date times (creation, accessed, modified) are before the date range.

Supported data sources by authentication type

The following types of data can be acquired from a Google account.

Google

Authentication type	2FA/MFA support	Data sources
• Username/Password • Chrome authentication (advanced)	✓	• Gmail • Google Activity • Google Audit Logs • Google Calendar • Google Connected Apps • Google Drive Activity* • Google Drive Files • Google Drive Version History • Google Hangouts • Google Photos • Google Stored Passwords • Google Timeline Locations • Recent Devices
External Browser Authentication	✓	• Gmail • Google Audit Logs • Google Calendar

Authentication type	2FA/MFA support	Data sources
		• Google Drive Activity* • Google Drive Files • Google Drive Version History • Google Photos
Token	N/A	• Gmail • Google Audit Logs • Google Calendar • Google Drive Files • Google Photos

*The following MIME types will have metadata available in your acquisition, but are not supported for download:

- application/vnd.google-apps.audio
- application/vnd.google-apps.drive-sdk
- application/vnd.google-apps.fusiontable
- application/vnd.google-apps.map
- application/vnd.google-apps.photo
- application/vnd.google-apps.unknown
- application/vnd.google-apps.video

For a complete list of supported cloud data sources by authentication type, review supported cloud data sources by authentication type.

Select the data

1. From the **Select Google data to acquire** page, select the category of data you want to acquire.
2. Select the sub-categories of data you want to include in the acquisition and then click **Next**.
3. At this point, you can proceed with adding additional data from the account, or you can click **Add to evidence sources** to add the data to the case.

Instagram

When you acquire an Instagram user account, you must take the following steps:

1. Authenticate the account
2. Select the data to acquire

Before you begin, see Acquire a cloud user account for considerations that apply to all cloud account acquisitions.

Authenticate the account

> Note: When AXIOM Process gains access to an account, the owner of the account might receive an email notifying them that someone has signed in to their account.

When acquiring an Instagram account, you can only authenticate using the username and password of the account.

Authentication steps

1. In AXIOM Process, click **Evidence sources** > **Cloud** > **Acquire evidence**.
2. Confirm that you have proper search authorization.
3. Click **Instagram**.
4. Authenticate with the username and password.

Select the data to acquire

Select a date range

By default, AXIOM Process acquires data from as far back in time as possible for the account. Acquiring some accounts can take a long time depending on the amount of data they contain, so you might want to narrow the date range to decrease the amount of time the acquisition takes.

1. In the **Date range** drop-down list, select one of the following options:
   - To acquire data *after* a specified date, click **After**.
   - To acquire data *before* a specified date, click **Before**.
   - To acquire data *between* two specified dates, click **Custom date range**.
2. Click the **calendar icon** and choose a date.

Supported data sources by authentication type

The following types of data can be acquired from an Instagram account.

Instagram Public Activity

Authentication type	2FA/MFA support	Data sources
Customer Provided account Username/Password	✓	Instagram Posts

Instagram User Account

Authentication type	2FA/MFA support	Data sources
Username/Password	✓	• Instagram Posts • Instagram DMs

For a complete list of supported cloud data sources by authentication type, review supported cloud data sources by authentication type.

Select the services

From the **Select services and content** section, select the content you want to acquire and then click **Next**.

Lyft

When you acquire a Lyft user account, you must take the following steps:

1. Authenticate the account
2. Select the data to acquire

Before you begin, see Acquire a cloud user account for considerations that apply to all cloud account acquisitions.

Authenticate the account

> Note: When AXIOM Process gains access to an account, the owner of the account might receive an email notifying them that someone has signed in to their account.

Authentication steps

1. In AXIOM Process, click **Evidence sources** > **Cloud** > **Acquire evidence**.
2. Confirm that you have proper search authorization.
3. Click **Lyft**.
4. Authenticate with the username and password for the account.

Select the data to acquire

Select a date range

After you gain access to a cloud account, you can select a date range to acquire data from. By default, AXIOM Process acquires data from as far back in time as possible for the account. Acquiring some accounts can take a long time depending on the amount of data they contain, so you might want to narrow the date range to decrease the amount of time the acquisition takes.

1. In the **Date range** drop-down list, select one of the following options:
   - To acquire data *after* a specified date, click **After**.
   - To acquire data *before* a specified date, click **Before**.
   - To acquire data *between* two specified dates, including those dates selected, click **Custom date range**.
2. Click the **calendar icon** and choose a date.

Supported data sources by authentication type

The following types of data can be acquired from a Lyft account.

Lyft

Authentication type	2FA/MFA support	Data sources
Username/Password	✓	• Lyft Profile Information • Lyft Trip Information

For a complete list of supported cloud data sources by authentication type, review supported cloud data sources by authentication type.

Select the services

From the **Select services and content** section, select the content you want to acquire and then click **Next**.

Microsoft User account services

You can acquire evidence from the following Microsoft User account services:

Azure

Microsoft user account

Acquiring evidence from a Microsoft Teams user account

> Note: Only one Microsoft evidence source can be included in a case. Each Microsoft evidence source must be in a separate case.

Azure

> Note: This feature is only available for AXIOM Cyber users.

When you acquire an Azure account, you must take the following steps:

1. Prepare the account to be acquired
2. Authenticate the account
3. Select the data to acquire

Before you begin, see Acquire a cloud user account for considerations that apply to all cloud account acquisitions.

Prepare the account to be acquired

To sign in and acquire an Azure virtual machine in AXIOM Process, an Azure Active Directory administrator needs to create a new role-based access (RBAC) role and register a new service principal with the RBAC role that Magnet AXIOM can use. For more information on how to complete these steps, see Find Azure authentication details.

Authenticate the account

> Note: When AXIOM Process gains access to an account, the owner of the account might receive an email notifying them that someone has signed in to their account.

1. In AXIOM Process, click **Evidence sources** > **Cloud** > **Acquire evidence**.
2. Confirm that you have proper search authorization.
3. Click **Azure**.
4. Authenticate with the account credentials.

Select the data to acquire

1. Select the machine(s) that you want to acquire.
2. Uncheck the box if you would like to keep the image in Azure after the image has been successfully acquired.

Note: Storing an image of an Azure virtual machine might incur monthly costs. After you've successfully acquired the virtual machine, consider removing the image from Azure to avoid additional expenses.

Supported data sources by authentication type

The following types of data can be acquired from an Azure account.

Azure

Authentication type	2FA/MFA support	Data sources
Azure credentials login	N/A	Azure VM

For a complete list of supported cloud data sources by authentication type, review supported cloud data sources by authentication type.

Microsoft Teams

Note: This feature is only available for AXIOM Cyber users.

When you acquire a Microsoft Teams account, you must take the following steps:

1. Prepare the account to be acquired
2. Authenticate the account
3. Select the data to acquire

Before you begin, see Acquire a cloud user account for considerations that apply to all cloud account acquisitions.

Prepare the account to be acquired

To acquire evidence from Microsoft Teams user accounts, you might need to configure Active Directory in Microsoft Azure to allow access to the Magnet Forensics application and give access to user accounts. For more information see Configure Microsoft Azure to give access to Microsoft Teams.

Authenticate the account

Note: When AXIOM Process gains access to an account, the owner of the account might receive an email notifying them that someone has signed in to their account.

There are a few different authentication methods you can use when acquiring a Microsoft Teams account. Each authentication method gives you access to different types of data on the target account. The authentication methods include:

- Username and password - Use this option if you have the username and password of the account.
- External browser authentication - Use this option if you are having trouble authenticating in AXIOM.
- Account token - Use this option if you have an account token that you found in a search. For more information on locating and using a token from a search, see Add cloud evidence using recovered passwords and tokens.

Authentication steps

1. In AXIOM Process, click **Evidence sources** > **Cloud** > **Acquire evidence**.
2. Confirm that you have proper search authorization.
3. Click **Microsoft Teams**.
4. Authenticate with your chosen method.

Select the data to acquire

Select a date range

After you gain access to a cloud account, you can select a date range to acquire data from. By default, AXIOM Process acquires data from as far back in time as possible for the account. Acquiring some accounts can take a long time depending on the amount of data they contain, so you might want to narrow the date range to decrease the amount of time the acquisition takes.

1. In the **Date range** drop-down list, select one of the following options:
   - To acquire data *after* a specified date, click **After**.
   - To acquire data *before* a specified date, click **Before**.
   - To acquire data *between* two specified dates, including those dates selected, click **Custom date range**.
2. Click the **calendar icon** and choose a date.

Supported data sources by authentication type

The following types of data can be acquired from a Microsoft Teams account.

Microsoft Teams

Authentication type	2FA/MFA support	Data sources
Username/Password	✓	• Microsoft Teams Chats • Microsoft Teams Channels
External Browser Authentication	✓	Same as Username/Password
Token	N/A	Same as Username/Password
Client Credentials*	N/A	• Microsoft Teams Chats • Microsoft Teams Channels

* Available only with a Cloud Premium license. Voice messages are currently unsupported.

Client credentials - This method acquires data at the organization level. Use this option if you have a Cloud Premium license and Administrator access to your Azure Portal. For more information about obtaining client credentials, sign in to the Support Portal to read the following article: Sign in to Microsoft using client credentials. For a complete list of supported cloud data sources by authentication type, review supported cloud data sources by authentication type.

Select the services

From the **Select services and content** section, select the content you want to acquire and then click **Next**.

Microsoft user account

When you acquire a Microsoft account, you must take the following steps:

1. Prepare the account to be acquired
2. Authenticate the account
3. Select acquisition filters
4. Select the data to acquire

Before you begin, see Acquire a cloud user account for considerations that apply to all cloud account acquisitions.

Prepare the account to be acquired

Before you acquire the account, you might need to perform some steps that will allow the account to be acquired. Consider if any of the following scenarios applies to you:

- To acquire evidence from Microsoft user accounts, you might need to configure Active Directory in Azure to allow access to Magnet Forensics International, Inc application and give access to user accounts. For more information on how to configure Azure, see Configure Microsoft Azure to give access to Microsoft user accounts.
- Microsoft 365 accounts with administrator privileges often have access to more data than typical user accounts. With a global administrator account, you might be able

acquire more data including audit logs and other users' mailboxes. By default, administrator accounts don't have read access to other users' mailboxes. For more information on how to configure read access to only the accounts you want to acquire as part of an investigation, or all accounts, see Configure an Microsoft 365 account for acquisition.

- If you have a Microsoft 365 account with administrator privileges, you can give examiners access to other users' SharePoint accounts. When you give examiners access to other users' SharePoint accounts, they also get access to those users' OneDrive accounts. If you would like to provide examiners with this level of access, see Give examiners access to users' Microsoft 365 SharePoint and OneDrive accounts

Authenticate the account

Note: When AXIOM Process gains access to an account, the owner of the account might receive an email notifying them that someone has signed in to their account.

There are a few different authentication methods you can use when acquiring a Microsoft account. Each authentication method gives you access to different types of data on the target account. The data that you can acquire from an account differs between admin and user accounts, regardless of the authentication method used. The authentication methods include:

- Username and password - Use this option if you have the username and password of the account.
- External browser authentication - Use this option if you are having trouble authenticating in AXIOM.
- Account token - Use this option if you have an account token that you found in a search. For more information on locating and using a token from a search, see Add cloud evidence using recovered passwords and tokens.
- Client credentials - This method acquires data at the organization level. Use this option if you have a Cloud Premium license and Administrator access to your Azure Portal.

For more information about obtaining client credentials, sign in to the Support Portal to read the following article: Sign in to Microsoft using client credentials.

Authentication steps

1. In AXIOM Process, click **Evidence sources** > **Cloud** > **Acquire evidence**.
2. Confirm that you have proper search authorization.
3. Click **Microsoft**, then **Microsoft account**.
4. Authenticate with your chosen method.

select acquisition filters

Use acquisition filters to reduce the size of evidence and narrow the scope of the evidence collected.

Select date range

After you gain access to a cloud account, you can select a date range to acquire data from. By default, AXIOM Process acquires data from as far back in time as possible for the account. Acquiring some accounts can take a long time depending on the amount of data they contain, so you might want to narrow the date range to decrease the amount of time the acquisition takes.

1. In the **Date range** drop-down list, select one of the following options:
   - To acquire data *after* a specified date, click **After**.
   - To acquire data *before* a specified date, click **Before**.
   - To acquire data *between* two specified dates, including those dates selected, click **Custom date range**.
2. Click the **calendar icon** and choose a date.

Select Outlook mail keywords

Use a single keyword list to limit the content acquired from a Microsoft Outlook mail account. Keywords will only filter Outlook mail acquisitions and will not be used to filter other Microsoft applications.

Keyword lists must be .txt files and each search term must appear on a new line. A keyword list can contain up to 30 keywords. Each keyword must be minimum of 2 characters in length.

> Note: Keyword lists with more than 10 entries can significantly increase the time to acquire larger Outlook mail accounts.

For more information about best practices and limitations on using keywords to acquire Microsoft mail accounts, log in to the Customer Portal to read the following article: Using keyword lists and date ranges for Microsoft mail acquisitions.

1. Select **Add keywords**.
2. Click **Add keyword list**.
3. Browse to the location of the keyword list.
4. Click **Open**.

Select data to acquire

You can access data from the authenticated account and the user accounts the authenticated account has administrator privileges for. The services associated for the selected account, privileges, license type, and the method used to authenticate, will determine which Outlook applications are available. For more information about the applications that can be acquired by authentication method and license type, see Application availability by authentication method.

Select SharePoint data

Select the SharePoint sites to acquire from the authenticated account's organization. SharePoint can only be accessed at an organization level. SharePoint is only available with the Cloud Premium license.

1. Select **Add SharePoint data to acquire** or **Edit SharePoint data**.
2. Expand the explorer to view available Sites/folders or perform a text search for a Site.
3. **Select all** or select individual Sites/folders.
4. Click **Next**.

Select user account data

Add user accounts and the authenticated account you wish to acquire.

- **Add user accounts**
  1. Search for accounts in your Microsoft Workspace.
  2. Select the check box for the accounts you wish to include.
  3. Click **Add accounts**.
- **Add authenticated account** Select this option to include the authenticated user in the acquisition.

Once the user accounts have been selected, click **Select data to acquire** for each user account to define the applications to acquire.

Select Microsoft data to acquire

Depending on the type of user account and permission available for the authenticated user, you may acquire data from OneDrive in addition to Outlook.

Select Outlook applications

Select and customize which Outlook applications to acquire.

Acquire Outlook mail

1. **Select All** or select individual folders.
2. Click to expand a folder to view and select nested sub-folders.
3. Click **Next**.

Note: The number beside each Outlook folder represents the count of messages in the current folder only. It does not include the count for any sub-folders.

Acquire OneDrive files and folders

Select the files you want to acquire from the authenticated account's OneDrive account.

1. **Select All** or individual folders.
2. Click to expand a folder to view and select nested sub-folders.
3. Click **Next**.

Supported data sources by authentication type

The following types of data can be acquired from a Microsoft account.

Microsoft

Authentication type	2FA/MFA support	Data sources
Username/Password	✓	• Office365/Microsoft Mail • OneDrive Files • OneDrive Version His-

Authentication type	2FA/MFA support	Data sources
		tory - Office365 Outlook Contact - Office365 Audit Logs* - Sharepoint * - Office365 Outlook Calendars
External Browser	✓	Same as Username/Password except Office365 Audit Logs are not available.
Token	N/A	Same as Username/Password except Office365 Audit Logs are not available.
Client credentials*	N/A	- Office365/Microsoft Mail - OneDrive Files - Office365 Outlook Contact - Sharepoint - Office365 Outlook Calendars

* Available only with a Cloud Premium license.

For a complete list of supported cloud data sources by authentication type, review supported cloud data sources by authentication type.

Add to evidence sources

1. Once the user accounts have been configured select **Next**.
2. From the Evidence sources page select **Go to processing details** or **Select evidence source** to include additional non Microsoft source evidence items.

Note: Only one Microsoft evidence source can be included in a case.

Mega

When you acquire a Mega user account, you must take the following steps:

1. Authenticate the account
2. Select the data to acquire

Before you begin, see Acquire a cloud user account for considerations that apply to all cloud account acquisitions.

Authenticate the account

Note: When AXIOM Process gains access to an account, the owner of the account might receive an email notifying them that someone has signed in to their account.

Authentication steps

1. In AXIOM Process, click **Evidence sources** > **Cloud** > **Acquire evidence**.
2. Confirm that you have proper search authorization.
3. Click **Mega**.
4. Authenticate with your chosen method.

Select the data to acquire

Select a date range

The date range set applies to files that are created, modified, or accessed within the date range.

After you gain access to a cloud account, you can select a date range to acquire data from. By default, AXIOM Process acquires data from as far back in time as possible for the account. Acquiring some accounts can take a long time depending on the amount of data they contain, so you might want to narrow the date range to decrease the amount of time the acquisition takes.

1. In the **Date range** drop-down list, select one of the following options:
    - To acquire data *after* a specified date, click **After**.
    - To acquire data *before* a specified date, click **Before**.
    - To acquire data *between* two specified dates, including those dates selected, click **Custom date range**.
2. Click the **calendar icon** and choose a date.

Supported data sources by authentication type

The following types of data can be acquired from a Mega account.

Mega.NZ

Authentication type	2FA/MFA support	Data sources
Username/Password	✓	Mega Files

For a complete list of supported cloud data sources by authentication type, review supported cloud data sources by authentication type.

Select the services

From the **Select services and content** section, select the content you want to acquire and then click **Next**.

Slack

Note: This feature is only available for AXIOM Cyber users.

When you acquire a Slack account, you must take the following steps:

1. Prepare the account to be acquired
2. Authenticate the account
3. Select the data to acquire

Before you begin, see Acquire a cloud user account for considerations that apply to all cloud account acquisitions.

Prepare the account to be acquired

Before you acquire the account, you might need to Configure Slack to allow access to AXIOM Process.

Authenticate the account

> Note: When AXIOM Process gains access to an account, the owner of the account might receive an email notifying them that someone has signed in to their account.

When acquiring a Slack account, you can authenticate using the username and password, or a token. The types of data that you can acquire using the username and password or token authentication methods is the same, however the data available may be limited to the permissions of the token.

Select the data to acquire

Select a date range

By default, AXIOM Process acquires data from as far back in time as possible for the account. Acquiring some accounts can take a long time depending on the amount of data they contain, so you might want to narrow the date range to decrease the amount of time the acquisition takes. The date range logic applies to posts and messages posted or sent within the date range, including the dates selected.

1. In the **Date range** drop-down list, select one of the following options:
   - To acquire data *after* a specified date, click **After**.
   - To acquire data *before* a specified date, click **Before**.
   - To acquire data *between* two specified dates, click **Custom date range**.
2. Click the **calendar icon** and choose a date.

Supported data sources by authentication type

The following types of data can be acquired from a Slack account.

Slack

Authentication type	2FA/MFA support	Data sources
Username/Password	✓	• Slack Public Channels • Slack Private Channels • Slack DMs • Slack Direct Group Messages
Token	N/A	Same as Username/Password

For a complete list of supported cloud data sources by authentication type, review supported cloud data sources by authentication type.

Select the services

From the **Select services and content** section, select the content you want to acquire and then click **Next**.

Twitter

When you acquire a Twitter account, you must take the following steps:

1. Authenticate the account
2. Select the data to acquire

Before you begin, see Acquire a cloud user account for considerations that apply to all cloud account acquisitions.

Authenticate the account

> Note: When AXIOM Process gains access to an account, the owner of the account might receive an email notifying them that someone has signed in to their account.

When acquiring a Twitter account, authenticate using the username and password.

Select the data to acquire

Select a date range

After you gain access to a cloud account, you can select a date range to acquire data from. By default, AXIOM Process acquires data from as far back in time as possible for the account. Acquiring some accounts can take a long time depending on the amount of data they contain, so you might want to narrow the date range to decrease the amount of time the acquisition takes.

1. In the **Date range** drop-down list, select one of the following options:
   - To acquire data *after* a specified date, click **After**.
   - To acquire data *before* a specified date, click **Before**.
   - To acquire data *between* two specified dates, including those dates selected, click **Custom date range**.
2. Click the **calendar icon** and choose a date.

Supported data sources by authentication type

The following types of data can be acquired from a Twitter account.

Twitter Public Activity

Authentication type	2FA/MFA support	Data sources
N/A	N/A	• Tweets • Followers • Following

Twitter User Account

Authentication type	2FA/MFA support	Data sources
Username/Password	✓	Twitter Posts Twitter DMs Twitter Users

For a complete list of supported cloud data sources by authentication type, review supported cloud data sources by authentication type.

Select the services

From the **Select services and content** section, select the content you want to acquire and then click **Next**.

Uber

When you acquire an Uber account, you must take the following steps:

1. Authenticate the account
2. Select the data to acquire

Before you begin, see Acquire a cloud user account for considerations that apply to all cloud account acquisitions.

Authenticate the account

Note: When AXIOM Process gains access to an account, the owner of the account might receive an email notifying them that someone has signed in to their account.

Authentication steps

1. In AXIOM Process, click **Evidence sources** > **Cloud** > **Acquire evidence**.
2. Confirm that you have proper search authorization.

3. Click **Uber**.
4. Authenticate with your chosen method.

Select the data to acquire

Select a date range

After you gain access to a cloud account, you can select a date range to acquire data from. By default, AXIOM Process acquires data from as far back in time as possible for the account. Acquiring some accounts can take a long time depending on the amount of data they contain, so you might want to narrow the date range to decrease the amount of time the acquisition takes.

1. In the **Date range** drop-down list, select one of the following options:
   - To acquire data *after* a specified date, click **After**.
   - To acquire data *before* a specified date, click **Before**.
   - To acquire data *between* two specified dates, including those dates selected, click **Custom date range**.
2. Click the **calendar icon** and choose a date.

Supported data sources by authentication type

The following types of data can be acquired from an Uber account.

Uber

Authentication type	2FA/MFA support	Data sources
Username/Password	✓	Uber Trip History

For a complete list of supported cloud data sources by authentication type, review supported cloud data sources by authentication type.

Select the services

From the **Select services and content** section, select the content you want to acquire and then click **Next**.

WhatsApp

Limitations to the WhatsApp acquisition include:

- Only the previous year's worth of data can be acquired using cloud authentication.
- You might not be able to acquire all messages from accounts with a large amount of data.

In these instances, you might be able to acquire the remaining messages from the device that created the messages or a WhatsApp backup.

When you acquire a WhatsApp account, you must take the following steps:

1. Authenticate the account
2. Select the data to acquire

Before you begin, see Acquire a cloud user account for considerations that apply to all cloud account acquisitions.

Authenticate the account

Note: When AXIOM Process gains access to an account, the owner of the account might receive an email notifying them that someone has signed in to their account.

There are a few different authentication methods you can use when acquiring a WhatsApp account. Each authentication method gives you access to different types of data on the target account. The authentication methods include:

- QR code access - You must have access to WhatsApp on the device. The QR code method does not include acquiring WhatsApp backup data. The device being scanned must have a strong internet connection.

- Google drive backup - The backup will only be available if the user has WhatsApp backup turned on for their Google account.
    - User name and password - Might require multi-level authentication.
    - Google Chrome extension (advanced) - You must download the AXIOM Cloud Authenticator browser extension before authenticating.

Authentication steps

1. In AXIOM Process, click **Evidence sources** > **Cloud** > **Acquire evidence**.
2. Confirm that you have proper search authorization.
3. Select **WhatsApp**.
4. Authenticate with your chosen method.

Select the data to acquire

Select a date range

After you gain access to a WhatsApp account, you can select up to the previous year's worth of data for the account. Acquiring some accounts can take a long time depending on the amount of data they contain, so you might want to narrow the date range to decrease the amount of time the acquisition takes.

1. In the **Date range** drop-down list, select one of the following options:
    - To acquire data *after* a specified date, click **After**.
    - To acquire data *before* a specified date, click **Before**.
    - To acquire data *between* two specified dates, including those dates selected, click **Custom date range**.
2. Click the **calendar icon** and choose a date.

Supported data sources by authentication type

The following types of data can be acquired from a WhatsApp account.

WhatsApp Google Drive

Authentication type	2FA/MFA support	Data sources
• Username/Password • Chrome authentication (advanced)	✓	WhatsApp backup

WhatsApp QR Code

Authentication type	2FA/MFA support	Data sources
QR code scanned by phone with WhatsApp account	N/A	WhatsApp Chats

For a complete list of supported cloud data sources by authentication type, review supported cloud data sources by authentication type.

These data types are grouped under the same artifact:

- Groups
    - Participants - Participant names include the name set on the user's WhatsApp profile. If the contact's profile name is not provided, the name appears empty and only the author's phone number is shown.
- Chats
    - Text messages
    - Image messages
    - Document messages
    - Audio messages
    - Video messages
    - Extended text messages (only replies to quoted messages are supported)
- Contacts - Contact names include the name set on the user's WhatsApp profile, not the name set for the contact on the target's device.

Select the services

From the **Select services and content** section, select the content you want to acquire and then click **Next**.

Public activity

You can acquire publicly available activity from Twitter, Instagram, and Facebook. When you create a new case in AXIOM Process, you can acquire a single date range and user name for each platform. If you want to search for additional date ranges and user names, you can add them as a new evidence source after the original search completes.

> Note: Depending on the amount of data available, acquiring public activity can take a long time, so you should narrow the date range to decrease the amount of time the acquisition takes and to find the most important evidence.

Understanding what publicly available data you can acquire

In some situations, AXIOM Process might not be able to acquire all public activity.

Public Twitter activity, such as Retweets, content filtered by Twitter from public search results, protected Tweets, user accounts that are not completely configured, or Tweets that are not part of the supported history of the Twitter Standard Search API. The returned results might vary depending on which Tweets the Twitter algorithms make available on the Advanced Search page at a given time.

AXIOM Process might not be able to acquire some public Instagram activity, such as if the Instagram posts are later made private.

The data available to acquire from Facebook depends on the privacy settings set by the target account. For example, if the target user set the audience for their posts to be "Friends alone", the posts can only be acquired if the Facebook account you signed in to in AXIOM Process is a friend of the target user. Additionally, if friends of the target account have deactivated their Facebook accounts, these accounts might not be displayed by Facebook and will not be acquired by AXIOM Process.

Acquire public activity from Twitter

You can acquire publicly available activity from Twitter without requiring authentication information for specific users. When you search for publicly available Twitter activity from a specific user name, include the complete handle.

Make sure that you include the @ symbol (for example, @MagnetForensics) and format the user name correctly. For example, Twitter user names must be less than 15 characters and include only alphanumeric characters (letters A-Z and numbers 0-9) and underscores.

1. In AXIOM Process, click **Evidence sources** > **Cloud** > **Acquire evidence**.
2. Confirm that you have proper search authorization.
3. Click **Twitter** > **Twitter public activity**.
4. Select the **Date range** you want to acquire data from.
5. In the **User name** field, provide the user name of the account whose public activity you want to acquire.
6. Select the services and content you want to acquire.
7. To continue setting up your case, click **Next**.

Acquire public activity from Instagram

Instagram offers a limited subset of data publicly before requiring viewers to sign in to an account. To fully acquire the publicly available data, you must sign in to an Instagram account. You can use any active Instagram account to acquire public activity.

> Note: AXIOM Process will not store the account credentials in the case and will only use the credentials for the purposes of acquiring data.

After signing in to an Instagram account, choose whether you want to acquire public activity for a specific user name or hashtag. Instagram user names must be less than 30 characters and can include letters, numbers, periods and underscores. You do not need to include the @ or # symbol prior to the user name or hashtag.

1. In AXIOM Process, click **Evidence sources** > **Cloud** > **Acquire evidence**.
2. Confirm that you have proper search authorization.

3. Click **Instagram** > **Instagram public activity**.
4. To acknowledge the message indicating that you need to sign into an account, click **Next**.
5. Provide a user name and password for any active Instagram account, and then click **Log in**.
6. Select the **Date range** you want to acquire data from.
7. Select whether you want to acquire posts from a specific **user name** or **hashtag**.
8. Provide the user name of the account whose public activity you want to acquire or provide the hashtag you want to search for.
9. Click **Check** to confirm that the account exists and that it is set to public.

   > Note: To acquire the data of a private account, you must log in to the target Instagram user account. To learn more about acquiring data from a private account, see Cloud-based user accounts.

10. To continue setting up your case, click **Next**.

Acquire public activity from Facebook

Facebook offers a limited subset of data publicly before requiring viewers to sign in to an account. To fully acquire the publicly available data, you must sign in a Facebook account. You can use any active Facebook account to acquire public activity.

> Note: AXIOM Process will not store the account credentials in the case and will only use the credentials for the purposes of acquiring data.

After signing in to a Facebook account, enter the URL of the target Facebook account whose activity you want to acquire. Make sure that you include the full URL, including "https://". Usually, the URL looks like "https://www.facebook.com/*unique user ID*/".

1. In AXIOM Process, click **Evidence sources** > **Cloud** > **Acquire evidence**.
2. Confirm that you have proper search authorization.
3. Click **Facebook** > **Public activity**.

4. To acknowledge the message indicating that you need to sign into an account, click **Next**.
5. Provide a user name and password for an Instagram account, and then click **Log in**.
6. Select the **Date range** you want to acquire data from.
7. In the **Target profile URL** field, provide the URL of the target Facebook account whose activity you want to acquire.
8. To continue setting up your case, click **Next**.

Supported Cloud data sources by authentication

When acquiring evidence from a cloud-based account, Magnet AXIOM acquires live data. If a supported platform makes a change to their product, this change might affect the types of services or content Magnet AXIOM can acquire and process.

Sign in to the Customer Portal to view the status of supported cloud acquisition platforms for more information concerning platform availability.

Amazon Web Services

Authentication type	2FA/MFA support	Data sources
Security credentials	✓	• AWS S3 Files • AWS EC2 Export • AWS EC2 Snapshot
Session credentials	N/A	• AWS S3 Files • AWS EC2 Export

Apple

Authentication type	2FA/MFA support	Data sources
Username/Password	✓ SMS code verification is not supported	• iCloud Backup • iCloud Drive • iCloud Mail • iCloud Photos • iMessage

Azure

Authentication type	2FA/MFA support	Data sources
Azure credentials login	N/A	Azure VM

Box.com

Authentication type	2FA/MFA support	Data sources
Username/Password	✓	• Box.com Enterprise Events • Box.com Files • Box.com User Events
Token	N/A	• Box.com Enterprise Events • Box.com Files • Box.com User Events

Dropbox

Authentication type	2FA/MFA support	Data sources
Username/Password	✓	Dropbox Files
External Browser Authentication	✓	Dropbox Files
Token	N/A	Dropbox Files

Facebook Public

Authentication type	2FA/MFA support	Data sources
Customer Provided account Username/Password	✓	• Friends list • Profile information • Timeline posts

Facebook User Account

Authentication type	2FA/MFA support	Data sources
Username/Password	✓	• Friends list • Profile information • Mobile timeline posts • Messenger messages

Google

Authentication type	2FA/MFA support	Data sources
• Username/Password • Chrome authentication (advanced)	✓	• Gmail • Google Activity • Google Audit Logs • Google Calendar • Google Connected Apps • Google Drive Activity* • Google Drive Files • Google Drive Version History • Google Hangouts • Google Photos • Google Stored Passwords • Google Timeline Locations • Recent Devices
External Browser Authentication	✓	• Gmail • Google Audit Logs • Google Calendar • Google Drive Activity* • Google Drive Files • Google Drive Version History • Google Photos
Token	N/A	• Gmail • Google Audit Logs • Google Calendar • Google Drive Files • Google Photos

*The following MIME types will have metadata available in your acquisition, but are not supported for download:

- application/vnd.google-apps.audio
- application/vnd.google-apps.drive-sdk
- application/vnd.google-apps.fusiontable
- application/vnd.google-apps.map
- application/vnd.google-apps.photo
- application/vnd.google-apps.unknown
- application/vnd.google-apps.video

IMAP/POP

Authentication type	2FA/MFA support	Data sources
Username/Password	N/A	Cloud IMAP/POP emails

Instagram Public Activity

Authentication type	2FA/MFA support	Data sources
Customer Provided account Username/Password	✓	Instagram Posts

Instagram User Account

Authentication type	2FA/MFA support	Data sources
Username/Password	✓	• Instagram Posts • Instagram DMs

Lyft

Authentication type	2FA/MFA support	Data sources
Username/Password	✓	• Lyft Profile Information • Lyft Trip Information

Mega.NZ

Authentication type	2FA/MFA support	Data sources
Username/Password	✓	Mega Files

Microsoft

Authentication type	2FA/MFA support	Data sources
Username/Password	✓	• Office365/Microsoft Mail • OneDrive Files • OneDrive Version History • Office365 Outlook Contact • Office365 Audit Logs* • Sharepoint * • Office365 Outlook Calendars
External Browser	✓	Same as Username/Password except Office365 Audit Logs are not available.
Token	N/A	Same as Username/Password except Office365 Audit Logs are not available.
Client credentials*	N/A	• Office365/Microsoft Mail • OneDrive Files • Office365 Outlook Contact • Sharepoint • Office365 Outlook Calendars

* Available only with a Cloud Premium license.

Microsoft Teams

Authentication type	2FA/MFA support	Data sources
Username/Password	✓	• Microsoft Teams Chats • Microsoft Teams Channels
External Browser Authentication	✓	Same as Username/Password

Authentication type	2FA/MFA support	Data sources
Token	N/A	Same as Username/Password
Client Credentials*	N/A	- Microsoft Teams Chats - Microsoft Teams Channels

* Available only with a Cloud Premium license. Voice messages are currently unsupported.

Slack

Authentication type	2FA/MFA support	Data sources
Username/Password	✓	- Slack Public Channels - Slack Private Channels - Slack DMs - Slack Direct Group Messages
Token	N/A	Same as Username/Password

Twitter Public Activity

Authentication type	2FA/MFA support	Data sources
N/A	N/A	- Tweets - Followers - Following

Twitter User Account

Authentication type	2FA/MFA support	Data sources
Username/Password	✓	- Twitter Posts - Twitter DMs - Twitter Users

Uber

Authentication type	2FA/MFA support	Data sources
Username/Password	✓	Uber Trip History

WhatsApp Google Drive

Authentication type	2FA/MFA support	Data sources
• Username/Password • Chrome authentication (advanced)	✓	WhatsApp backup

WhatsApp QR Code

Authentication type	2FA/MFA support	Data sources
QR code scanned by phone with WhatsApp account	N/A	WhatsApp Chats

Available cloud platforms by license type

Platform / service	AXIOM Cloud	AXIOM Cyber
Amazon Web Services		✓
Apple	✓	✓
Box.com (User)	✓	✓
Box.com (Admin)		✓
Dropbox	✓	✓
Facebook	✓	✓
Google (User)	✓	✓
Google (admin)		✓
IMAP / POP	✓	✓
Instagram (User account)	✓	✓
Instagram (Public activity)	✓	✓
Lyft	✓	✓
Mega	✓	✓
Microsoft (User)	✓	✓
Microsoft (Microsoft 365 Admin)		✓
Microsoft Azure		✓

Platform / service	AXIOM Cloud	AXIOM Cyber
Microsoft Teams		✓
Slack		✓
Twitter (User account)	✓	✓
Twitter (Public activity)	✓	✓
Uber	✓	✓
WhatsApp (Google Drive Backup)	✓	✓
WhatsApp (QR code access)	✓	✓

Load cloud evidence

You can load the following cloud-based evidence sources: AXIOM Cloud images, Apple warrant returns, Facebook Download Your Information archives, Facebook warrant returns, Instagram Download Your Data archives, Instagram warrant returns, Google Takeout archives, Google warrant returns, iCloud backups, Microsoft Office 365 Unified Audit Logs, Skype exports, Skype warrant returns, Slack archives, and Snapchat warrant returns, and Twitter warrant returns.

When you acquire a cloud evidence source, AXIOM Process creates a .zip file containing the hashed cloud image. You can load this cloud image into AXIOM Processif you want to process the evidence as a part of another case.

Note: AXIOM Process allows you to load and process warrant return files provided by Apple, Facebook, Google, Instagram, Skype, and Snapchat. Sometimes, the platform providing the warrant return file make changes to its format which might impact the ability for AXIOM Process to process the warrant return package.

For a current list of any known changes to our ability to process warrant returns and the approximate dates of warrant returns AXIOM Process is known to support, please log in to the Customer Portal to read the following article: Status of supported cloud acquisition platforms. If you are unable to process a warrant return outside of these dates, please contact Magnet Technical Support.

Load a cloud image

Before you load a cloud image, make sure you have the appropriate user permissions to access the file.

If you're loading an Apple warrant return, make sure you decrypt the package using the instructions provided by Apple. For more information, log in to the Customer Portal to review the Prepare Apple warrant returns for acquisition article. After you've decrypted the package, AXIOM Process can decrypt encrypted backups contained within the decrypted warrant return.

If you're loading a .zip file from the Facebook Download your Information option, make sure the content is in JSON format. By default, Facebook downloads the information in HTML. For steps on how to download the .zip file, see How do I download a copy fo my information on Facebook?

1. In AXIOM Process, click **Evidence sources** > **Cloud** > **Load evidence**.
2. Select the type of image you want to load.
3. Browse to the image and click **Open**.
4. To continue setting up your case, click **Next**.

> Note: If you load an AXIOM Cloud .zip file that was created in a newer version of AXIOM Process than the version you are currently using, it's possible that you might recover less evidence.

Supported evidence sources

You can load the following cloud evidence sources in AXIOM Process:

Platform	AXIOM Cloud	AXIOM Cyber	Image type	Description
Apple	✓	✓	Warrant return	Use this option to load .zip files provided by Apple for warrant returns.
Apple	✓	✓	iCloud backup	Use this option to load manifest.plist files generated for encrypted

Platform	AXIOM Cloud	AXIOM Cyber	Image type	Description
				and non-encrypted iTunes backups.
	✓	✓	Warrant return	Use this option to load .zip files provided by Apple for warrant returns.
Facebook	✓	✓	Warrant return	Use this option to load .zip files provided by Facebook for warrant returns.
	✓	✓	Download Your Information	Use this option to load .zip files generated from the Download Your Information (JSON) option in Facebook.
Google	✓	✓	Google Takeout	Use this option to load .mbox files, and .zip files that are generated when a Google Takeout archive is created.
	✓	✓	Warrant return	Use this option to load .zip files provided by Google for warrant returns.
Instagram	✓	✓	Warrant return	Use this option to load .zip files provided by Instagram for warrant returns.
	✓	✓	Download Your Data	Use this option to load .zip files generated from the Data Download (JSON) option in

Platform	AXIOM Cloud	AXIOM Cyber	Image type	Description
				Instagram.
Magnet Forensics	✓	✓	AXIOM Cloud image	Use this option to load an AXIOM Cloud image that has already been acquired from a supported cloud platform or service. Magnet AXIOM can acquire data from the following platforms and services: • Amazon Web Services • Azure • Apple • Box.com • Dropbox • Facebook • Google • IMAP/POP • Instagram • Lyft • Mega • Microsoft • Microsoft 365 • Slack • Twitter

Platform	AXIOM Cloud	AXIOM Cyber	Image type	Description
				• Uber • WhatsApp
Microsoft Office 365 Unified Audit Logs		✓	Audit logs	Use this option to load Microsoft Unified Audit log .csv files generated using the Microsoft Security and Compliance Center.
Skype	✓	✓	Warrant return	Use this option to load .zip files provided by Skype / Microsoft for warrant returns.
	✓	✓	Skype export	Use this option to load .tar files generated from the Export files and chat history option in Skype.
Slack		✓	Slack archives	Use this option to load .zip files of Slack archives (JSON) files generated from the standard and corporate workspace data exports in Slack.
Snapchat	✓	✓	Warrant return	Use this option to load .zip files provided by Snapchat for warrant returns.
Twitter	✓	✓	Warrant return	Use this option to load .zip files provided by Twitter for warrant returns.

Endpoint

Note: This feature is only available for AXIOM Cyber users.

Acquiring evidence from an endpoint

Use AXIOM Process to acquire evidence from remote Windows, macOS, and Linux endpoints and complete targeted investigations of individuals on an as-needed basis—without the need for additional infrastructure. Create an agent, deploy the agent to an endpoint, connect to the agent, download items of interest, and add the items to your case—all from AXIOM Process.

Agents are standalone executable processes that you deploy to and run on an endpoint. Once the agent is running, it attempts to make a connection back to AXIOM Process at a defined interval. While connected to the agent, select and download items of interest to your investigation. Once you've downloaded evidence, remove the agent or keep the agent on the endpoint if you plan to download additional evidence in the future.

AXIOM Process supports the remote acquisition of drives, memory, and logical files from the file system even if the drive is encrypted. For more information about supported evidence items by operating system, see Supported evidence items.

If you lose connection to the agent while downloading evidence, AXIOM Process automatically reconnects to the agent when available. You can also configure the agent to persist on the endpoint if the computer is shut down due to a restart or a crash. AXIOM Process will automatically resume downloading any evidence that was still in progress, which means that you don't need to restart your investigation if you lose connection to the endpoint (including after a restart).

Acquired evidence encryption

AXIOM uses TLS1.3 (RSA-2048 asymmetric encryption) for the handshake. After the connection is established, the cyber workstation and the endpoint negotiate and then determine the most secure encryption method for the acquisition.

Prerequisites for remote acquisition

To acquire evidence from an endpoint using AXIOM Process, make sure that you meet the following requirements:

Operating system	Prerequisites
Windows	• You have administrative credentials for the endpoint, ideally a domain admin account rather than local admin account. If you cannot use a domain admin account, consider a domain user in the local administrators group on the target. Please work with your IT department for support in creating a domain user account. • The endpoint has Microsoft .NET Framework of 4.5.2 or later. • You have enabled Windows Management Instrumentation (WMI) and Remote Service Management in the Windows Defender Firewall settings for the endpoint.
macOS	• You have an account on the endpoint, ideally an admin account to have access to the most data. • You've enabled Remote Login on the endpoint. • The endpoint has either HFS+ or APFS file systems and is running macOS 10.12 (Sierra) or later.
Linux	• You have administrative credentials for the endpoint with root permissions. • The endpoint has RedHat Linux 7, RedHat Linux 8, CentOS 7, CentOS 8, Amazon Linux 2, or Ubuntu 21.04. Although other Linux versions might be supported, AXIOM Process was tested with these versions. • Endpoints running RedHat Linux 6 or CentOS 6 have the following library versions: ◦ glibc 2.17

Operating system	Prerequisites
	◦ libstdc++ 4.8.2 ◦ libicu 50.X or disable globalization

Manage agents and endpoints

Note: This feature is only available for AXIOM Cyber users.

To review or acquire data from an endpoint, create and deploy a new agent to the endpoint or connect to an existing agent on that endpoint from the Manage agents and endpoints page.

Manage agents

In the Agents section, view and manage all the agents you've created in AXIOM Process:

- View details about your agents
- Create a new agent
- Manage shared agent configuration
- Deploy an existing agent to a new endpoint
- Open the folder where the agent is saved on the examiner workstation
- Delete an agent

Agent details

Item	Description
Agent ID	The unique ID to identify the agent in AXIOM Process. If you didn't enter an Agent ID when configuring the agent, AXIOM Process automatically created a unique ID for you.
Agent file name	The file name (or executable name) for the agent.
Saved location	The full path of the location where the agent is stored on the examiner workstation. Click the file path to open the folder.

Item	Description
Operating system	The type of operating system the agent was configured to acquire data from.
Agent type	Shared or Ad-hoc.
Created date/time	The date and time when the agent was created.

Manage endpoints

In the Endpoints section, view all the available endpoints for each agent. By default, the table is sorted by hostname in alphabetical order.

- View details about the endpoints you previously deployed agents to
- Connect to an endpoint
- Select multiple endpoints
- Redeploy an agent to the endpoint
- Delete an endpoint
- Download evidence from a queued collection
- Add endpoint manually

Endpoint details

Item	Description
Hostname	The hostname of the endpoint.
IP address	The IP address of the endpoint.
Agent status	The activity status of the agent. This can be **Online** or **Offline** depending on the agent status on the endpoint or **Agent expired** if the agent self-destructed on that endpoint and you can no longer connect to it.
Operating system	The operating system of the endpoint.
Last known online time	The last known time that the endpoint was online.
Approximate self-destruct time	The approximate time when the agent self-destructed on that endpoint and you can no longer connect to it.

Item	Description
Data acquired	The amount of data acquired from the remote acquisition on the endpoint.

Download evidence from a queued collection

A queued collection is a collection of evidence downloaded from multiple endpoints in sequence. Setting up a queued collection is useful for downloading the same type of evidence from more than one endpoint since you only need to specify the collection details once for all the endpoints in the queue. You can set up a queued collection to download targeted locations and a full memory dump from the endpoints.

Before selecting multiple endpoints, make sure you have completed all the steps on the agent configuration page since all the endpoints in the queue will need to use the same agent and will have the same collection details. You can only select up to 15 endpoints at a time.

Manage offline endpoints in the queue

You can customize how AXIOM Process manages offline endpoints in the queue on the **Specify multiple endpoint collection settings** page, under **Queue management settings**.

You can configure how to manage an offline endpoint in the queue by specifying how long to wait for the endpoint to come online before moving to the next item, and whether to move an offline endpoint to the end of the queue or skip the endpoint entirely. If you choose to skip the endpoint, the status in the **Evidence sources** table will be **Failed**.

When an offline endpoint has been moved to the bottom of the queue, you can specify the number of times to retry before skipping the endpoint entirely. A skipped endpoint will appear as **Failed** in the **Evidence sources** table. You can also choose to wait for the endpoint to come online.

Monitor the status of evidence collection

You can monitor the status of evidence collection from each endpoint on the **Downloading status** screen. If the status is **Memory profile needed**, you must provide the correct image profile based on the operating system build number to process the memory image. To add the memory profile, hover over the endpoint and click **Select memory profile**. In the **Select profile** pop-up modal, upload the required image.

After evidence collection from each endpoint has been processed, you can proceed to add the collection to evidence sources. If the status for all endpoints is failed, you will need to cancel the acquisition.

Create a queued collection

1. On the **Manage agents and endpoints** screen, click **Select multiple endpoints**.
2. In the **Select multiple endpoints** table, select the agent to acquire data from.
3. Under the agent name, select the endpoints for your data collection. Click **Next**.
4. On the **Select items to download** screen, select a location profile, the targeted locations and full memory dump. Click **Next**.
5. On the **Specify multiple endpoint collection settings** screen, review the **Endpoint connection settings**.
6. Click **Begin queued collection**.
7. On the **Downloading status** screen, you can monitor the status of evidence collection from each endpoint.
8. Click **Add to evidence sources**. If the status for all endpoints is failed, you will need to click **Cancel the acquisition**.

On the **Evidence sources** screen, you should now see entries for all the endpoints in the queued collection and you can continue to processing details.

Add endpoint manually

Note: This feature is only available for AXIOM Cyber users.

Create an endpoint manually and define the collection before the agent comes online. Once the endpoint has the agent installed and comes online, the acquisition can begin.

Note: When using shared agents, each cyber workstation participating in a shared agent configuration must be manually add the endpoints to perform an acquisition.

1. From the **Manage agents and endpoints** or **Connect to endpoints** screen, click **Add endpoint manually**.
2. Provide the **Hostname/IP address**. Windows manual endpoints can be specified using an FQDN.
3. Select the **Agent ID**. The agent ID can only be selected when creating the endpoint manually from the **Manage agents and endpoints** screen.
4. Click **Add endpoint**.

Once the endpoint has been created, you can define the collection as a single collection or part of a queued collection.

Create an agent

Note: This feature is only available for AXIOM Cyber users.

AXIOM Process: Click **Evidence sources** > **Remote computer** > **Create new agent**

Agents are executable programs that are deployed to endpoints that connect to examination workstations for the purposes of acquiring data remotely. To create a new agent, specify the agent type, provide optional agent masking details, and connectivity details. AXIOM Process remembers some of the details so that you don't need to fill them in next time you open AXIOM Process to create a new agent.

Agent ID

Provide a unique value to identify the agent. If you don’t enter an Agent ID, AXIOM Process will automatically create a unique ID for you.

Operating system

From the drop-down list, select which operating system you want to create the agent for.

Agent type

- **Shared** agents can connect to cyber workstations defined in a shared agent configuration. When creating a shared agent, the port specified for incoming connections must be the same for all cyber workstations participating in the shared agent configuration. Any changes to the shared agents will require an updated configuration code to be applied to all cyber workstations participating in the shared agent configuration. See Update a shared agent configuration to understand how changes affect an existing shared agent configuration.
- **Ad-hoc** agents can only connect with the examiner workstation that created the agent.

Agent masking details

Note: macOS agents are created as signed applications. Agent masking details for macOS agents are not configurable since application details are provided at time of agent creation. For more information about signed macOS agents, sign in to the Support Portal to read the following article: AXIOM Cyber signed macOS agents.

Agent masking details are metadata you can provide to help disguise the agent on the endpoint to look like a typical system process. This can help prevent the target user from noticing that there is a remote acquisition application running on their computer.

Click **show more details** to configure additional masking details. The details you provide populate fields for the executable file in locations like the Properties or Get Info dialogs.

Item	Description
File name	The file name (or executable name) for the agent.
File description	The name of the agent as you want it to appear in the application properties.
Company	The company name as you want it to appear when a user hovers over the agent executable file.

Item	Description
Product name	The product name of the agent as you want it to appear in the application properties. For many applications, this value is often the same as the file description.
Copyright	The copyright details that you want to appear in the application properties.
Legal trademarks	The trademark information that you want to appear in the application properties.

Survive shutdown of endpoint

You can optionally configure the agent to persist on the endpoint if the computer is shut down due to a restart or a crash. Depending on the operating system of the endpoint, the agent will be installed as a Windows service, macOS background process (daemon), or a Linux service. The name of the service or daemon on the endpoint is determined by the information you populate in the File description and File name fields when you configure the agent. By default, the service or daemon is named after the File description. If no File description is provided, the File name is used instead.

Note: If you're actively downloading evidence from the endpoint at the time of the shut down, the agent will automatically resume downloading evidence once the endpoint restarts. If you completed your investigation prior to the shut down and disconnected from the agent, the agent will persist on the endpoint in an idle state. Reconnect to begin downloading evidence again.

Connectivity details

Connectivity details provide information about the computer that is going to deploy the agent including the IP address and port. You can also configure how often you want the agent to attempt to connect back to AXIOM Process once it's deployed and the amount of time after which the agent will stop trying to make a connection back to AXIOM Process.

Item	Description
Examiner work-	The IP address, host name, or machine name of the computer that's

Item	Description
station host name or IP address	running AXIOM Process.
Port	A port on the computer deploying the agent that AXIOM Process will bind to locally. This is the port that the agent calls back on and the port that AXIOM Process listens on. You should choose a port that is not reserved by another process, is not currently in use, or blocked by any local or network firewalls. Consider coordinating with your IT team to determine which ports could be used as there might be policies that explicitly block specific ports or ranges.
Reconnect delay	The amount of time (in seconds) that the agent will wait between unsuccessful connection attempts to AXIOM Process. The default value is 10 seconds.
Disconnected keep alive	The amount of time (in seconds, minutes, hours, or days) after which the agent will stop trying to make a connection back to AXIOM Process. The default value is 1 day.
Proxy connection method	If your organization routes network traffic through a proxy, configure the agent to connect back to AXIOM Process using a proxy. Depending on the operating system the agent is created for, configure the agent to automatically detect proxy settings or manually set a proxy server. Select Auto-detect proxy settings so that the agent automatically looks for a proxy auto-configuration (PAC) file on the endpoint and tries to use those settings. Select Manually set a proxy server to set the proxy server you want the agent to use to connect back to AXIOM Process. Provide the proxy server IP address and the proxy server port. Note: If you configure a Windows agent to survive the shutdown of an endpoint, you must manually set the proxy server details. Agents cannot auto-detect proxy settings when running as a Windows service.

Item	Description
	For more information on the prerequisites for enabling the agent proxy option, log in to the Customer Portal and review the Prerequisites proxy support article.

After you create the agent, review the agent details, and then deploy the agent.

Deploy an agent

Note: This feature is only available for AXIOM Cyber users.

Deploy the agent to the endpoint so you can then connect and select the data you want to acquire. Depending on the needs of your investigation, you can:

- Deploy a new agent that you created for a specific case or investigation.
- Deploy an agent that you previously created to a new endpoint.
- Redeploy an expired agent to an existing endpoint.

To deploy an agent, you must provide information about the endpoint including the IP address, user name and password, and the location where you want to store the agent on the endpoint. The user account must have local administrative permissions on the endpoint.

Note: AXIOM Process does not support deployment of agents on all machines across a network or enterprise such as installing an agent on a Gold Build image.

If you’re unable to deploy an agent to an endpoint using the built-in deployment solution in AXIOM Process, log in to the Customer Portal to review the Deploying an agent to a remote computer using a third-party solution article.

Deploy a new agent

If you created a new agent, continue the workflow in AXIOM Process to deploy the agent to the endpoint.

1. On the **Manage agents and endpoints** screen, click **Deploy agent**.
2. Provide information about the endpoint that you want to deploy the agent to.
3. Click **Deploy agent**.

After the agent successfully deploys the endpoint, connect to the agent.

Deploy an existing agent to a new endpoint

You can deploy an agent that you previously created to a new endpoint.

1. On the **Manage agents and endpoints** screen, in the **Agents** table, hover over the agent and click **Deploy agent**.
2. On the **Review agent details** screen, click **Deploy agent**.
3. Provide information about the endpoint that you want to deploy the agent to.
4. Click **Deploy agent**.

After the agent successfully deploys the endpoint, connect to the agent.

Redeploy an agent to an endpoint

If you previously deployed an agent to the endpoint, but the agent expired, you can redeploy the agent. If you previously deployed an agent to the endpoint, and the agent is still available, you can connect to the agent instead.

1. On the **Manage agents and endpoints** screen, in the **Endpoints** table, hover over the endpoint and click **Redeploy agent**.
2. On the **Review agent details** screen, click **Deploy agent**.
3. Provide information about the endpoint that you want to deploy the agent to.
4. Click **Deploy agent**.

After the agent successfully deploys the endpoint, connect to the agent.

Troubleshooting deployment failures

If the deployment attempt fails, check the information you provided to deploy the agent is correct such as the correct user name and password for the endpoint. For more information about troubleshooting deployment failures, please log in to the Customer Portal and review the following articles:

- Deploying the agent for remote acquisition fails (Windows)
- Deploying the agent for remote acquisition fails (macOS)
- Deploying the agent for remote acquisition fails (Linux)

If your issue persists, consider using an alternative method to deploy the agent to the endpoint, and then proceed to the "Connect to agent" step.

Endpoint deployment details

Item	Description
Remote computer IP address	The IP address, host name, or machine name of the endpoint you're going to deploy the agent to.
User name	The user name for the administrator account you're using to log in to the endpoint. The user account must have local administrative permissions on the endpoint. These credentials are used to authenticate the copy of the agent to the endpoint as well as to run the executable as an administrator. To acquire evidence from a Windows computer, you should consider using a domain account as Windows might prevent you from remotely deploying or running the agent if you use a local admin account. If you cannot use a domain admin account, consider a domain user in the local administrators group on the endpoint. Please work with your IT department for support in creating a domain user account.
Password	The password for the administrator account you're using to log in to the endpoint.

Item	Description
Agent location on remote computer	The location where you want to store the agent on the endpoint. Consider storing the agent in a location where it's unlikely to be noticed such as C:\Windows\Temp\, /private/var/, or /usr/local. The administrator account you use to deploy the agent must have permission to access this location.

Connect to an agent

Note: This feature is only available for AXIOM Cyber users.

Connect to the agent on the endpoint to select the data you want to acquire. You can connect to a newly deployed agent or to an agent that was previously deployed to an endpoint.

Enable searching and filtering in the file browser

To search, sort, and filter the files and folders from the endpoint in AXIOM Process, configure the agent to start downloading information about the file system structure as well as file and folder metadata. After connecting to the endpoint, the agent builds an index of the file system structure to help you get to the evidence faster. This also downloads a file and folder listing of the endpoint after the acquisition completes.

While connecting to the endpoint, select items from Targeted locations that you're interested in downloading. The Files and drives and Memory options become available after a successful connection.

Remote acquisitions often require downloading large amounts of data over the network. If network usage is a concern, you can help reduce the amount of data that gets sent by compressing it on the endpoint before downloading. For more information, see Compressing data before downloading.

Connect to a newly deployed agent

Once the agent has successfully deployed to a new endpoint, connect to the agent.

1. On the **Deploy agent** screen, click **Connect to agent**.
2. Follow the instructions in AXIOM Process to customize your connection settings.
3. On the **Connect to endpoints** screen, in the **Endpoints for this agent** table, hover over the endpoint you want to connect to, and then click **Connect to endpoint**.

After successfully connecting to the agent, you can download items from the endpoint.

Connect to an agent previously deployed to an endpoint

If you previously deployed an agent to an endpoint, and the agent has not expired, you can connect to it directly from the Manage agents and endpoints screen. If you previously deployed an agent to the endpoint, but the agent expired, make sure that you redeploy the agent.

Note: If you're connecting to an agent that was created and deployed using an older version of AXIOM Cyber, AXIOM Process automatically updates the agent before attempting to connect.

1. On the **Manage agents and endpoints** screen, in the **Endpoints** table, hover over the agent and click **Connect to endpoint**.
2. Follow the instructions in AXIOM Process to customize your connection settings.
3. Click **Connect to endpoint**.

After successfully connecting to the agent, you can download items from the endpoint.

Troubleshooting connection failures

For information about troubleshooting connection failures, please log in to the Customer Portal and review the following articles:

- Connecting to the agent for remote acquisition fails (Windows)
- Connecting to the agent for remote acquisition fails (macOS)
- Connecting to the agent for remote acquisition fails (Linux)

Endpoint connection details

Item	Description
Hostname	The hostname of the endpoint.
IP address	The IP address of the endpoint.
Agent status	The activity status of the agent. This can be **Online** or **Offline** depending on the agent status on the endpoint or **Agent expired** if the agent self-destructed on that endpoint and you can no longer connect to it.
Operating system	The operating system of the endpoint.
Last known online time	The last known time that the endpoint was online.
Approximate self-destruct time	The approximate time when the agent self-destructed on that endpoint and you can no longer connect to it.
Data acquired	The amount of data acquired from the remote acquisition on the endpoint.

Delete an agent

AXIOM Process: Click **Evidence sources** > **Remote computer**

Remove an agent from an endpoint

1. On the **Manage agents and endpoints** screen, in the **Endpoints** table, hover over an entry.
2. Click the trash icon to delete the agent from the endpoint.

The agent will receive a self-destruct command when it checks in with the Cyber workstation.

Delete an agent

1. On the **Manage agents and endpoints** screen, in the **Agents** table, hover over the agent.
2. Click the trash icon to delete the locally saved agent.

The agent will automatically delete itself based on the agent's disconnected keep alive setting.

> If an endpoint was restarted and the agent was not configured to start up as a service, you may need to remove the agent manually from the endpoint.

Remove the agent manually

Since the agent is just an executable, you can simply remove the agent from the endpoint.

1. In the Windows Search Bar, type: **Run**.
2. In the Run window, type: **\\<IP_AddressOfRemoteMachine>\C$**.
3. Provide a username and password with Administrative permissions, if prompted.
4. Once the Windows Explorer is open, navigate to the location of the deployed agent.
5. Delete the agent.

If you are unable to delete the agent because the file reports as being open in another program, you will have to stop the agent on the endpoint before you can delete it. You can remote in to the endpoint and use the task manager to end the agent process or Remove the agent using PsExec.

Remove the agent using PsExec

Ensure you have downloaded and installed PsExec and you have administrative permissions on the endpoint.

In the Windows Search Bar, type **cmd** and open a Command Prompt as an Administrator.

1. Navigate to the folder where PsExec was installed. Example: **cd c:\psexec**.
2. To open the endpoint's command prompt on your machine, type **psexec \\<IP_AddressOfRemoteMachine> cmd**.
3. Navigate to the location of the deployed agent. Example: **cd c:\dontlookhere**.
4. To terminate the process forcefully, type: **taskkill /F IM <NameOfAgent.exe>**.
5. To force delete the agent from the endpoint, type: **del /f <NameOfAgent.exe>**.
6. To close the PsExec session, type **exit**.

Download items from endpoints

Note: This feature is only available for AXIOM Cyber users.

You can download items from a single or multiple endpoints. Depending on the operating system of the endpoint, select the drives, files and folders, and memory that you want to download. To save time searching the complete list of files and folders, select targeted locations to view a list of typical files and folders that you might want to download. Once AXIOM Process connects to the endpoint, you have access to download more data.

Note: If you stop and delete an agent from the endpoint while evidence items are still downloading, AXIOM Process includes partial results in the image from the items that were still downloading.

AXIOM Process provides a count of the number of potential items to download from the location you selected and indicates how many items have been downloaded successfully. To find out more details about why an item might not have downloaded, you can review the log.txt log file. Before the search is started, this log is in the install directory of AXIOM Process. The default is C:\Program Files\Magnet Forensics\Magnet AXIOM\AXIOM Process\log.txt. After the search begins, this log is moved to the case folder.

You can manually refresh the list of files and folders, drives, and memory processes. If you refresh a list, any items you previously selected remain selected. If a list item was deleted from the endpoint, the item is removed from the list.

Supported evidence items

Item	Operating system	Description
Targeted locations	Windows, macOS, Linux	Includes a list of typical files and folders and volatile artifacts that you might want to download during a remote acquisition such as user folders, browser activity, and system files. This list includes both default system targeted locations as

Item	Operating system	Description
		well as targeted locations that you've added. For more information about the system added items included in the Targeted locations table, see Default targeted locations.
Files and drives	Windows, macOS, Linux	**Files and folders**: This option represents a logical image that contains all files and folders on the file system. A files and folders search provides logical access to any connected, unencrypted drives on the endpoint and allows you to see the files as the target user sees them. If the drive is unencrypted and AXIOM Process can access a byte stream level and it rebuilds the file system in AXIOM Process. If the drives are encrypted, AXIOM Process can access viewable files only due to limitations in Windows operating system APIs.
	Windows	**Drives**: This option represents a physical image of the drive. You can select and download individual partitions or the complete drive. AXIOM Process downloads a raw binary, byte-for-byte copy of the drive including any encryption that might be present. If the drive is encrypted, you must have an encryption key to access the data.
Memory	Windows, Linux	Includes full memory acquisition and/or individual processes running on the endpoint. Where applicable, you can also view the parent process and parent process ID that launched an individual process. AXIOM Process downloads the memory space for that process as raw binary data.

Download targeted locations

Note: This feature is only available for AXIOM Cyber users.

Targeted locations are typical files and folders and volatile artifacts that you might want to download during a remote acquisition. This list includes both default system targeted locations as well as targeted locations that you've added. For more information about adding your own targeted locations to this list, review Add custom targeted locations.

Location profile

Use location profiles to quickly select multiple targeted locations at once. For more information about managing location profiles, review Manage location profiles.

Targeted locations

When downloading evidence from a single or multiple endpoints, you can select a Location profile, or items from the Targeted locations list even before the agent connects to the endpoint(s). While the agent connects to the endpoint(s), these items are put in a pending state. After a successful connection, AXIOM Process begins downloading the items automatically.

Follow the steps below to download targeted locations from a single endpoint. If you're downloading targeted locations as part of a queued collection, see Create a queued collection for more information.

1. On the **Review and select the data from the target computer** screen, click **Targeted Locations**.
2. In the **Targeted locations** table, select the items that you want to download.
3. Click **Next**.

Default targeted locations

Windows

Item	Description	Examples
$LogFile	Download the $LogFile from the endpoint.	C:\$LogFile
$MFT	Download the Master Table File ($MFT) from the endpoint.	C:\$MFT
All users - Desktop items	Download items from the default Desktop folder location for all users.	C:\Users\[user_name]\Desktop*.*
All users - Documents	Download items from the default Documents folder location for all users.	C:\Users\[user_name]\Documents*.*
All users - Downloaded items	Download items from the default Downloads folder location for all users.	C:\Users\[user_name]\Downloads*.*
All users - Folders	Download items from the default User folder location for all users.	C:\Users\[user_name]*.*
Event logs	Download event logs from the endpoint.	C:\Windows\System32\config\ C:\Windows\System32\winevt\Logs
Pagefile.sys	Download the pagefile.sys file from the endpoint.	C:\pagefile.sys
Registry files	Download registry files from the endpoint.	C:\Windows\System32\config\*.dat C:\Users\[user_name]\NTUSER.dat
Swapfile.sys	Download the swap-	C:\swapfile.sys

Item	Description	Examples
	file.sys file from the endpoint.	
Web browsing activity	Download web browsing activity such as history, temporary internet files, download history, cookies, and more for Chrome, Firefox, Internet Explorer, 360 Safe Browser, and Opera.	C:\Users\[user_name]\appdata\local\google\chrome C:\Users\[user_name]\NTUSER.dat
Volatile artifacts	Active Connections	netstat
	Active Users	query user
	DNS Cache (English support only)	ipconfig /displaydns
	Firewall Rules (English support only)	netsh advfirewall
	Network ARP Info	arp -a
	Network Shares (English support only)	Get-SmbShare
	Prefetch List	dir /b /s %SYSTEMDRIVE%\Windows\Prefetch\*.pf
	Process List	tasklist /V
	Scheduled Jobs	wmic job list
	Scheduled Processes	schtasks
	Services	sc queryex type=service state=all

macOS

Item	Description	Examples
All users - Desktop items	Download items from the default	/Users/[user_name]/Desktop/*.*

Item	Description	Examples
	Desktop folder location for all users.	
All users - Documents	Download items from the default Documents folder location for all users.	/Users/[user_name]/Documents/*.*
All users - Downloaded items	Download items from the default Downloads folder location for all users.	/Users/[user_name]/Downloads/*.*
All users - Folders	Download items from the default User folder location for all users.	/Users/[user_name]/*.*
All users - Pictures	Download items from the default Pictures folder location for all users.	/Users/[user_name]/Pictures/*.*
App Store downloads	Download a history of App Store downloads from the endpoint.	/Library/Receipts/InstallHistory.plist

Item	Description	Examples
Bash	Download bash sessions for all users.	/Users/[user_name]/.bash_sessions/*.* /Users/[user_name]/.bash_history /Users/[user_name]/.bashrc;/Users/[user_name]/.zsh_sessions/*.* /Users/[user_name]/.zsh_history; /Users/[user_name]/.zshrc
Daily.out	Download the Daily.out file from the endpoint.	/private/var/log/daily.out
Finder MRU	Download information about recently accessed paths in the Finder application for all users.	/Users/[user_name]/Library/Preferences/com.apple.finder.plist
FSEvents	Download information about file system events for all users.	/.fseventsd/*.*
iCloud data	Download iCloud data for all users	/Users/[user_name]/Library/Application Support/iCloud/Accounts/*.* /Users/[user_name]/Library/Application Support/CloudDocs/session/db/*.*
iOS backups	Download iOS backups for all	/Users/[user_name]/Library/Application Support/MobileSync/Backup/*.*

Item	Description	Examples
	users.	
Lockdown folder	Download lockdown files for all users.	/private/var/db/lockdown/*.*
Quarantine files	Download files with a quarantine flag from the endpoint.	/Users/[user_name]/Library/Preferences/com.apple.LaunchServices.QuarantineEventsV2
Spotlight shortcuts	Download Spotlight shortcuts for all users.	/Users/[user_name]/Library/Application Support/com.apple.spotlight.Shortcuts /Users/[user_name]/Library/Application Support/com.apple.spotlight/com.apple.spotlight.Shortcuts /Users/[user_name]/Library/Application Support/com.apple.spotlight/com.apple.spotlight.Shortcuts.v3
Unified logs	Download unified logs from the endpoint.	/private/var/db/diagnostics/*.*
Web browsing activity	Download web browsing activity such as history, temporary internet files, download history, cookies, and more for Chrome, Firefox,	/Users/[user_name]/Library/Application Support/Google/Chrome/Default/*.* /Users/[user_name]/Library/Caches/Google/Chrome/Default/*.*

Item	Description	Examples
	Opera, and Safari.	
Volatile artifacts	Active Connections	netstat
	Active Users	w
	Network ARP Info	arp -an
	Network Shares (English support only)	sharing -l
	Process List	ps a
	Scheduled Processes	crontab -l
	Services	launchctl list

Linux

Item	Description	Examples
All users - Folders	Download items from the default User folder location for all users.	/home/[user_name]/*.*
Bash history	Download bash sessions for all users.	/home/[user_name]/.bash_history
Recent files	Download information about the recent files that were accessed by all users.	/home/[user_name]/.local/share/recently-used.xbel
Scheduled tasks	Download scheduled tasks for all users.	/var/spool/crontabs/*.* /var/spool/atjobs/*.*

Item	Description	Examples
SSH files	Download SSH files for all users.	/home/[user_name]/.ssh/*.*
Startup items	Download startup items for all users.	/etc/systemd/system/*.* /usr/lib/systemd/system/*.*
System files	Download system files for all users.	/etc/hostname; /etc/hosts /var/lib/NetworkManager/*.* /var/lib/dhclient/*.* /var/lib/dhcpd/*.*
System logs	Download system logs for all users.	/var/log/*.*
Trash	Download trash items for all users.	/home/[user_name]/.local/share/Trash/*.*
Web browsing activity	Download web browsing activity such as history, temporary internet files, download history, cookies, and more for Chrome and Firefox.	/home/[user_name]/.config/google-chrome/*.* /home/[user_name]/.mozilla/firefox/*.*
Volatile artifacts	Active Connections	ss -apn || netstat -anop
	Active Users	w
	DNS Cache	journalctl -u systemd-resolved
	Firewall Rules (English support only)	firewall-cmd --list-all
	Network ARP Info	ip -s neigh || arp -env
	Process List	ps a
	Scheduled Processes	crontab -l
	Services	systemctl --type=service --all

Download files and drives

> Note: This feature is only available for AXIOM Cyber users.

Download files and folders (representing a logical image that contains all files and folders) or drives (for Windows only, representing a physical image). When you download a logical image that contains files and folders, you have the option of using ZIP or AFF4-L as the container type. The default container type for logical images is AFF4-L.

> Note: When acquiring evidence from a macOS computer, you might see some items in the Select data to download file tree that have been greyed-out such as fifo, charspecial, or socket. While the file system reports these items as files, they either contain no data or the data is not readable, and they cannot be acquired.

Download Drives

1. On the **Review and select the data from the target computer** screen, click **Files and drives**.
2. Under **Select data to download**, click **Drives**.
3. To turn on compression for the download, select the **Compress data on the remote computer before downloading** option.
4. Select the items that you want to download.
5. Click **Next**.

Download files and folders

You can select specific files and folders you want to acquire from the endpoint. If you configured the agent to download information about the file system structure after connecting, you can also apply date range filters, search for words or search terms in a selected folder, and sort and filter by file name, extension, or size.

Note: Sometimes the agent is unable to access certain files or folders, so these items will not appear when browsing or searching the file system. For example, the agent might not have permissions to access them.

1. On the **Review and select the data from the target computer** screen, click **Files and drives**.
2. Under **Select data to download**, click **Files and folders**.
3. If applicable, search, sort, and filter the files and folders to help find key evidence.
4. Select the items that you want to download.
5. Click **Next**.

Filter by date range

Apply date range filters to only display files in a certain time frame. By default, AXIOM Process acquires data from as far back in time as possible for the endpoint. Because s Some acquisitions can take a long time depending on the amount of data they contain, consider narrowing the date range to decrease the amount of time the acquisition takes.

Note: You can apply date range filters when they are available once AXIOM Process has finished downloading the file system details.

1. In the **Date range** drop-down list, select one of the following options:
   - To acquire data *after* a specified date, click **After**.
   - To acquire data *before* a specified date, click **Before**.
   - To acquire data *between* two specified dates, click **Custom date range**.
2. Click the **calendar icon** and choose a date. You will need to choose two dates if you selected **Custom date range** in step 1.
3. Click **Apply filter**.

Note: Search results include any files or folders whose created, accessed, modified, or added dates match the date range filter that you applied.

Search by word or search term

You can search the files and subfolders in the folder you're currently viewing for specific words or search terms. To search the entire endpoint for a specific term, navigate to the top level of the computer from the file tree.

Note: If a date range has been specified, the search results will only display files corresponding to that date range. If you want to display all the files including the searched text, click **Clear filter** beside the **column drop-down** to return to **All dates** before searching.

1. Navigate to the folder you want to search.
2. Enter the text you want to search for in the search bar.
3. Click **Go**.

Filter by column

You can filter files and folders by some of the available columns, such as by file extension or file size.

1. In AXIOM Process, right-click the header of a column and select **Filter on column**.
2. Complete one of the following options:
   - For numeric columns, specify a range or an exact value to filter on.
   - For string columns, specify a search term.
3. Click **Search**.

To clear a filter, right-click the header of a column and select **Clear filter**.

Download memory

Note: This feature is only available for AXIOM Cyber users.

You can select and download memory processes running on an endpoint. Memory processes can be collected from individual endpoints or from multiple endpoints, as part of a queued collection. When downloading memory processes from an individual endpoint, you can download individual memory processes or complete a full memory acquisition. When downloading from multiple endpoints, you can only acquire the full memory. Downloading memory is currently available for Windows computers only.

When downloading a full memory dump, consider turning on compression for the download. Compressing data can help improve acquisition times. For more information, see Compressing data before downloading.

Follow the steps below to download individual memory processes or complete a full memory acquisition from a single endpoint. If you're completing a full memory acquisition as part of a queued collection, see Create a queued collection for more information.

1. On the **Review and select the data from the target computer** screen, click **Memory**.
2. Complete one of the following options:
   - To select individual memory processes to download from the endpoint(s), select **Individual processes**, and then choose the processes you want to acquire.
   - To download a full memory dump from the endpoint, select **Full memory acquisition**.
3. Click **Next**.

Add custom targeted locations

Note: This feature is only available for AXIOM Cyber users.

Add your own targeted locations to the default list in Magnet AUTOMATE Enterprise. To add a custom targeted location, provide a description and at least one path for the folders or files that you want to acquire.

Note: This feature is only available for AUTOMATE Enterprise users.

A path can be either a valid Windows, macOS, or Linux path that points to a folder or a file. For Windows acquisitions, use a backslash (\) as a path separator. For macOS and Linux acquisitions, use a slash (/) as a path separator. AXIOM ProcessMagnet AUTOMATE validates the paths that you provide and considers the operating system of the agent. For example, if you're creating a custom targeted location while completing a remote acquisition with an agent created for macOS computers, AXIOM ProcessMagnet AUTOMATE looks for a slash (/) as the path separator.

Include wildcard characters in the paths you create to serve as placeholders for items like all user names, all file names, and more.

1. On the **Select targeted locations** screen, click **Add new targeted location**.
2. Select the click **Add new targeted location** option, and then click **Add new targeted location**.
3. In the **Description** field, provide a name for the targeted location.
4. In the **Paths to acquire** field, provide one or more paths for the folders or files that you want to acquire.
5. Click **Okay**.

The custom targeted locations that you add are available in the Targeted locations list for future remote acquisitions that correspond to the same operating system.

Wildcard characters

Wildcard character	Description	Example paths
[ROOT]	Represents the root folder of the drive. Use [ROOT] at the beginning of a path to indicate that you want to use the path for any drive letter that might exist on the endpoint.	**Windows**: [ROOT]\Users\[user_name]\Desktop*.* **macOS**: [ROOT]/private/ **Linux**: [ROOT]/home/

Wildcard character	Description	Example paths
[user_name]	Represents the name of any user's account. Include [user_name] in the path to indicate that you want to use the path for any user folder. Note: For Windows and macOS, the [user_name] wildcard can only appear after the Users folder.	**Windows**: C:\Users\[user_name]\Desktop\ **macOS**: /Users/[user_name]/Desktop/ **Linux**: /home/[user_name]/.bash_history
*	Represents any file name and must be combined with an extension (for example, *.txt) to indicate that you only want to download files of that type within the specified folder. Note: The * wildcard can only be used at the end of the path.	**Windows**: C:\Windows\System32\config\*.dat **macOS** : /Library/Preferences/SystemConfiguration/*.plist **Linux**: /etc/sysconfig/*.conf

Wildcard character	Description	Example paths
.	Represents all files in the folder. To indicate that you want to acquire a folder, the path should end with a trailing slash (\) or the wildcard *.* Note: The *.* wildcard can only be used at the end of the path	**Windows**: C:\Program Files\Magnet Forensics*.* **macOS**: /Users/[user_name]/Downloads/*.* **Linux**: /home/[user_name]/*.*

Add evidence from the endpoint to your case

Note: This feature is only available for AXIOM Cyber users.

Once you've selected all the evidence from the endpoint, and the evidence items have finished downloading, you can begin to add the evidence to your evidence sources. First, AXIOM Process will complete some additional processing steps such as archiving items, hashing the archive, and checking for encryption and RAM.

AXIOM Process creates an archive of the downloaded evidence in the location that you specified for your case files. In the same location, you'll find a log file that provides details about the remote acquisition such as the date and time the archive was created, the MD5 and SHA1 hashes, and device information for the endpoint.

If AXIOM Process detects encryption for supported encryption types, you can provide known decryption credentials such as passwords and recovery keys to decrypt the evidence source before a search. For more information, see Decrypt evidence.

If you've downloaded memory from a Windows computer, in most cases, AXIOM Process can automatically select the correct image profile. If AXIOM Process detects multiple memory images or doesn't currently support the memory image, you're prompted to select an image profile. For more information about processing memory, see Windows memory.

Add evidence to your case

When you add evidence from the endpoint as an evidence source, you can decide whether you want to keep the agent installed on the endpoint or delete the agent. If you plan to download additional evidence items in the future, consider keeping the agent installed on the endpoint.

1. On the **Select items to download** screen, **Next**.
2. Complete one of the following options:
   - To keep the agent installed on the endpoint, click **Keep agent**.
   - To delete the agent from the endpoint, click **Delete agent**.
3. If prompted to decrypt an encrypted evidence source, select a decryption option and provide the password or recovery key.
4. If prompted, select a image profile.
5. Click **Add to evidence sources**.
6. Continue setting up your case.

AXIOM Process creates one .zip file for logical evidence, one .zip file for memory processes, one .bin file for full memory acquisition (RAM dump), and one .bin file for physical evidence. The file names for each evidence source include descriptive information such as the computer name and the local date/time the .zip or .bin files were generated.

Customize remote acquisition settings

Note: This feature is only available for AXIOM Cyber users.

Change the agent default location

When configuring a new agent in AXIOM Process, the agent is automatically saved to the default location (C:\). When creating an agent, you can save the agent to a shared location that is accessible to other users. To change the agent default location, complete the following task:

1. In AXIOM Process, on the **Tools** menu, click **Settings**.
2. In the **Remote acquisition** section, under **Agent default location**, click **Browse** to open the file folder browser and select the location where you want to store the agent on your computer.
3. Click **Okay**.

Automatically remove an agent from the endpoint

You can configure AXIOM Process to automatically delete the agent from an endpoint after the remote acquisition completes.

1. In AXIOM Process, on the **Tools** menu, click **Settings**.
2. In the **Remote acquisition** section, under **Agent removal**, select the option to automatically delete the agent from the endpoint.
3. Click **Okay**.

Compressing data before downloading

Remote acquisitions often require downloading large amounts of data over the network. If network usage is a concern, you can help reduce the amount of data that gets sent by compressing it on the endpoint before downloading. Compressing the data can also speed up the overall acquisition time on slower networks. However, on faster networks, you might see an increase to the total acquisition time as compressing the data takes longer than transferring it on those networks.

Some acquisition types are more receptive to compression than others. RAM acquisitions are generally a good candidate for compression as in some cases RAM data can be compressed by 80% or more. On the opposite side of the spectrum, compressing an encrypted drive won’t result in meaningful improvements on the size of the download. If you’re downloading files that are already compressed on the endpoint, you won’t see much benefit to compressing them again.

Compressing data can cause a noticeable usage of system resources on the endpoint. If the data that you're acquiring doesn't compress well, or if you're concerned about the subject noticing the increase in system resource usage, you might want to consider skipping the compression step.

Compress data before downloading

You can turn on the compression setting globally for drive, file and folder, targeted location, and RAM dump downloads from the Settings menu. Only RAM process downloads cannot currently be compressed. You can also override the global compression setting while you configure individual drive and RAM dump downloads.

To turn on compression for all supported acquisition types:

1. In AXIOM Process, on the **Tools** menu, click **Settings**.
2. In the **Remote acquisition** section, under **Compression**, select the **Compress data on the remote computer before downloading** option.
3. Click **Okay**.

Change the container type for downloads

Remote acquisitions can save their data in ZIP or AFF4-L containers. Some remote acquisition methods do not support AFF4-L and will always use ZIP regardless of the default type that is selected. The default container type for supported methods is AFF4-L.

1. In AXIOM Process, on the **Tools** menu, click **Settings**.
2. In the **Remote acquisition** section, under **Logical acquisition container**, select your preferred container type.
3. Click **Okay**.

Manage location profiles

Note: This feature is only available for AXIOM Cyber users.

Use location profiles to create groups of targeted locations for performing repeated collections. For more information about adding your own targeted locations to this list, review Add custom targeted locations.

You can select or manage location profiles even before the agent connects to the endpoint(s). Location profiles are available from the Select targeted locations screen when connecting to a single endpoint or from the Select items to download screen proceeding the Selecting multiple endpoints screen.

You can only select a single location profile per collection. Once a location profile is created, you can edit, delete or create a duplicate location profile.

Create a new location profile

1. Select **Manage profiles** then **Create new**.
2. Provide a **Profile name**.
3. Select several targeted locations or **Select all**.
4. Select **Create profile**.

Once you have created the location profile, it will be available for selection on the Review and select the data from the target computer screen in the **Location Profile** drop-down list.

Edit a location profile

1. Select **Manage profiles**.
2. Select a **Profile name**, and then Select **Edit**.
3. Update the **Profile name** or modify the selected targeted locations.
4. Select **Save** or **Discard changes**.

Duplicate a location profile

Creating a duplicate location profile allows you to make changes to a new location profile while retaining the settings of the original location profiles.

1. Select **Manage Profiles**.
2. Select a **Profile name** then **Duplicate**.

3. Update the **Profile name** and modify the selected targeted locations.
4. Select **Create Profile**.

Shared agent configuration

Note: This feature is only available for AXIOM Cyber users.

A shared agent configuration provides you with the ability to extend the management of endpoint acquisitions beyond the single cyber workstation that created the agent. Create a shared agent configuration with deployed shared agents to allow multiple cyber workstations to manage an acquisition of a single or multiple endpoints.

Review the following topics to learn more about creating and managing a shared agent configuration.

Create a shared agent configuration

Connect to existing shared agent configuration

Update a shared agent configuration

Creating a shared agent

Create a shared agent configuration

Note: This feature is only available for AXIOM Cyber users.

AXIOM Process: Click **Evidence sources** > **Remote computer** > **Managed shared agent configuration**

A shared agent configuration allows multiple cyber workstations to manage shared agents and acquisitions of endpoints. Cyber workstations can either create a new shared agent configuration or Connect to existing shared agent configuration.

Create new shared agent configuration

Creating a shared agent configuration starts with adding the current workstation as the first cyber workstation. Once you have identified the current workstation by its **Hostname/IP address**, you can add additional cyber workstations to the shared agent configuration.

> Tip: For best results, follow the steps below in order when creating a shared agent configuration. Log in to the Customer Portal to read the following article: Creating a shared agent configuration in AXIOM Cyber.

1. Create a new shared agent configuration.
2. Add cyber workstations.
3. Create a shared agent.
4. Provide the configuration code.
5. Add endpoints manually.

Requirements:

- You have Administrator access to the cyber workstation.
- The same SSL certificate is installed on all cyber workstations participating in the shared agent configuration.
- The same port is available for incoming connections as other cyber workstations participating in the shared agent configuration.

Create a new shared agent configuration

On the current cyber workstation, launch AXIOM Cyber and perform the following steps.

1. Select **Remote acquire** > **Manage shared agent configuration**.
2. Select **Create a new shared agent configuration**.
3. Provide the **Hostname/IP address** of the current workstation.
4. Select an agent certificate. **Browse** to the location of the SSL certificate.
5. Click **Next**.

Hostname/IP address

Provide the **Hostname/IP address** of the current workstation.

Agent certificate

You must install SSL certificates in both the **Personal** and **Trust Root Certificate Authorities folder** on each cyber workstation participating in the shared agent configurations.

To select the SSL certificate installed in the local Windows certificate store, perform the following steps.

1. Click **Browse** to open **Tools** > **Settings**.
2. Under **Shared agent certification**, click **Browse**.
3. Click **More choices**.
4. Once you have selected the SSL certificate, click **OK** to accept.

For more information about installing and using SSL certificates, log in to the Support Portal to read the following article: SSL certificates and shared agent configuration.

Add cyber workstations

You can have multiple cyber workstations in the shared agent configuration capable of managing deployed shared agents and performing acquisitions of endpoints. Cyber workstations can be added after a shared agent configuration is complete. However, it is recommended that you include all the participating cyber workstations during the creation of the shared agent configuration.

On the current cyber workstation, launch AXIOM Cyber and perform the following steps.

1. Select **Remote acquire** > **Manage shared agent configuration**.
2. Select **Add workstation** and provide the **Hostname/IP address** of the cyber workstation you wish to include.
3. To add multiple cyber workstations, click **Add additional workstation** and provide the **Hostname/IP address** for each.
4. Click **Next** then **Close**.

Once complete, each cyber workstation will have to Connect to existing shared agent configuration.

Remove cyber workstations

Each cyber workstation has the ability to remove a cyber workstation from a shared agent configuration.

1. On the current cyber workstation, launch AXIOM Cyber.
2. Select **Remote Computer** > **Manage agents and endpoints** > **Manage shared agent configuration**.
3. Hover over a workstation and click the trash icon to delete.
4. Confirm the choice by clicking **Delete workstation** or **Cancel**.
5. Click **Next**.

Once a cyber workstation has been removed, the local configuration code will need to be reset on the cyber workstation to fully leave the shared agent configuration.

Refer to Update a shared agent configuration to understand how changes affect an existing shared agent configuration.

Create a shared agent

You can create a shared agent from any cyber workstation in a shared agent configuration. However, its highly recommended to create the shared agent on the same workstation that created the shared agent configuration and after all cyber workstations have been defined. If any changes are made to the shared agent configuration or the shared agents, the configuration code of each cyber workstation may differ as the configuration code is not synced across cyber workstations automatically.

On the current cyber workstation, launch AXIOM Cyber and perform the following steps.

1. Select **Remote Computer** > **Manage agents and endpoints**.
2. Select **Create new agent**.
3. Provide an **Agent ID** to uniquely identify the agent and specify the **Operating system** the shared agent will be deployed to.
4. For the **Agent type** select **Shared agent**.

5. Provide optional configuration details such as **Agent masking details** and if the agent is to survive a shutdown of the endpoint.
6. Provide the same **Port** the agent will use to communicate with any cyber workstation participating in the shared agent configuration.
7. Click **Create agent**.

Provide the configuration code

After you add the cyber workstations in the shared agent configuration they require a configuration code to actually join the shared agent configuration. This configuration code contains the connectivity information of all cyber workstations participating in the shared agent configuration and the shared agents.

Note: The configuration code is not synced across cyber workstations automatically. Anytime there is an update to the shared agent configuration or shared agents, only the configuration code on the current workstation is updated. You must distribute the updated configuration code to all cyber workstations participating in the shared agent configuration.

To obtain the configuration code, launch AXIOM Cyber and perform the following steps.

1. Select **Remote acquire** > **Manage shared agent configuration**.
2. Select **View configuration**.
3. Select **Copy configuration**. The configuration code has been copied to the clipboard.
4. Open a text editor and paste the contents.
5. Save the file ensuring the formatting has been preserved.
6. Click **Back**.

Tip: This value can be saved in a text file or sent in an email providing the formatting of configuration code remains unchanged. Some applications may insert unwanted formatting, such as line breaks or word wrapping.

For more information about the configuration code, refer to the following topic: Update a shared agent configuration.

Add endpoints manually

On each cyber workstation participating in the shared agent configuration, you must manually add endpoints before they can perform an acquisition of an endpoint. You can add endpoints before or after you deploy a shared agent.

If you are creating a shared agent configuration, you can manually add the endpoints at this time.

On the current cyber workstation, launch AXIOM Cyber and perform the following steps.

1. Select **Remote acquire** > **Manage shared agent configuration**.
2. Click **Add endpoint manually**.
3. Provide the **Hostname/IP address** of the endpoint and select the **Agent ID**.
4. Click **Add endpoint**.

Cyber workstations defined in the shared agent configuration must first join an existing shared agent configuration before you can add endpoints manually. Refer to the topic Connect to existing shared agent configuration for more information about joining a shared agent configuration.

Connect to existing shared agent configuration

> Note: This feature is only available for AXIOM Cyber users.

Connecting to a shared agent configuration allows the current cyber workstation to manage shared agents and perform acquisitions of endpoints.

Requirements

If you haven't created a shared agent configuration, or you do not have one or more of the listed requirements, see Create a shared agent configuration for more information.

- The current cyber workstation is defined in an existing shared agent configuration.
- The most recent configuration code.
- The same SSL certificate is installed on all cyber workstations participating in the shared agent configuration.

- The same port is available for incoming connections as other cyber workstations participating in the shared agent configuration.

Connect to a shared agent configuration

To connect the current cyber workstation to a shared agent configuration, launch AXIOM Cyber and perform the following steps.

1. Select **Remote acquire** > **Manage shared agent configuration**.
2. Select **Connect to existing shared agent configuration**.
3. Select an **Agent certificate**.
4. Locate the **Configuration code** that was provided earlier and paste the contents.
5. Select **Apply configuration** to validate the configuration.

If the configuration validation failed, ensure the configuration code is the most recent and has not been modified.

To learn more about using the configuration code as it relates to connecting to an existing shared agent configuration, see Update a shared agent configuration.

Add endpoint manually

After connecting to a shared agent configuration, you must Add endpoint manually to perform an acquisition.

Update a shared agent configuration

> Note: This feature is only available for AXIOM Cyber users.

When you make any changes to a shared agent configuration, the changes are also applied in the configuration code on the local cyber workstation. The configuration code contains references and connectivity details of the cyber workstations participating in the shared agent configuration and the shared agents known to the current cyber workstation.

Some of the changes that will update the configuration code include:

- Cyber workstations (added, updated, or removed).
- Replaced or new SSL certificates.
- Shared agents (added, updated or removed).

The configuration code is not automatically synced across cyber workstations. If you make any changes to the shared agent configuration after its initial creation, the configuration code of each cyber workstation may differ.

It's imperative that all cyber workstation participating in a shared agent configuration have the same configuration code. See Create a shared agent configuration for more information about obtaining and providing the configuration code to all cyber workstations participating in the shared agent configuration.

Applying updated configuration code

Use the reset local configuration code when the current cyber workstation has been removed from a shared agent configuration or when you need to update your local configuration code.

For more information about removing a cyber workstation from a shared agent configuration, see the following topic: Remove cyber workstations

Update local configuration code

Update your local configuration when another cyber workstation has made changes to the shared agent configuration or the shared agents. Once the configuration has been reset, you can paste the contents of the updated configuration code.

To reset the local configuration code on the current cyber workstation, launch AXIOM Cyber and perform the following steps.

1. Select **Remote acquire** > **Manage shared agent configuration**.
2. Select **Reset local configuration**.
3. Click **Back**.

Create an agent

Note: This feature is only available for AXIOM Cyber users.

AXIOM Process: Click **Evidence sources** > **Remote computer** > **Create new agent**

Agents are executable programs that are deployed to endpoints that connect to examination workstations for the purposes of acquiring data remotely. To create a new agent, specify the agent type, provide optional agent masking details, and connectivity details. AXIOM Process remembers some of the details so that you don't need to fill them in next time you open AXIOM Process to create a new agent.

Agent ID

Provide a unique value to identify the agent. If you don’t enter an Agent ID, AXIOM Process will automatically create a unique ID for you.

Operating system

From the drop-down list, select which operating system you want to create the agent for.

Agent type

- **Shared** agents can connect to cyber workstations defined in a shared agent configuration. When creating a shared agent, the port specified for incoming connections must be the same for all cyber workstations participating in the shared agent configuration. Any changes to the shared agents will require an updated configuration code to be applied to all cyber workstations participating in the shared agent configuration. See Update a shared agent configuration to understand how changes affect an existing shared agent configuration.
- **Ad-hoc** agents can only connect with the examiner workstation that created the agent.

Agent masking details

Note: macOS agents are created as signed applications. Agent masking details for macOS agents are not configurable since application details are provided at time of agent creation. For more information about signed macOS agents, sign in to the Support Portal to read the following article: AXIOM Cyber signed macOS agents.

Agent masking details are metadata you can provide to help disguise the agent on the endpoint to look like a typical system process. This can help prevent the target user from noticing that there is a remote acquisition application running on their computer.

Click **show more details** to configure additional masking details. The details you provide populate fields for the executable file in locations like the Properties or Get Info dialogs.

Item	Description
File name	The file name (or executable name) for the agent.
File description	The name of the agent as you want it to appear in the application properties.
Company	The company name as you want it to appear when a user hovers over the agent executable file.
Product name	The product name of the agent as you want it to appear in the application properties. For many applications, this value is often the same as the file description.
Copyright	The copyright details that you want to appear in the application properties.
Legal trademarks	The trademark information that you want to appear in the application properties.

Survive shutdown of endpoint

You can optionally configure the agent to persist on the endpoint if the computer is shut down due to a restart or a crash. Depending on the operating system of the endpoint, the agent will be installed as a Windows service, macOS background process (daemon), or a Linux service. The name of the service or daemon on the endpoint is determined by the information you populate in the File description and File name fields when you configure the agent. By default, the service or daemon is named after the File description. If no File description is provided, the File name is used instead.

Note: If you're actively downloading evidence from the endpoint at the time of the shut down, the agent will automatically resume downloading evidence once the endpoint restarts. If you completed your investigation prior to the shut down and disconnected from the agent, the agent will persist on the endpoint in an idle state. Reconnect to begin downloading evidence again.

Connectivity details

Connectivity details provide information about the computer that is going to deploy the agent including the IP address and port. You can also configure how often you want the agent to attempt to connect back to AXIOM Process once it's deployed and the amount of time after which the agent will stop trying to make a connection back to AXIOM Process.

Item	Description
Examiner workstation host name or IP address	The IP address, host name, or machine name of the computer that's running AXIOM Process.
Port	A port on the computer deploying the agent that AXIOM Process will bind to locally. This is the port that the agent calls back on and the port that AXIOM Process listens on. You should choose a port that is not reserved by another process, is not currently in use, or blocked by any local or network firewalls. Consider coordinating with your IT team to determine which ports could be used as there might be policies that explicitly block specific ports or ranges.
Reconnect delay	The amount of time (in seconds) that the agent will wait between unsuccessful connection attempts to AXIOM Process. The default value is 10 seconds.
Disconnected keep alive	The amount of time (in seconds, minutes, hours, or days) after which the agent will stop trying to make a connection back to

Item	Description
	AXIOM Process. The default value is 1 day.
Proxy connection method	If your organization routes network traffic through a proxy, configure the agent to connect back to AXIOM Process using a proxy. Depending on the operating system the agent is created for, configure the agent to automatically detect proxy settings or manually set a proxy server. Select Auto-detect proxy settings so that the agent automatically looks for a proxy auto-configuration (PAC) file on the endpoint and tries to use those settings. Select Manually set a proxy server to set the proxy server you want the agent to use to connect back to AXIOM Process. Provide the proxy server IP address and the proxy server port. Note: If you configure a Windows agent to survive the shutdown of an endpoint, you must manually set the proxy server details. Agents cannot auto-detect proxy settings when running as a Windows service. For more information on the prerequisites for enabling the agent proxy option, log in to the Customer Portal and review the Prerequisites proxy support article.

After you create the agent, review the agent details, and then deploy the agent.

Mobile

Acquiring mobile evidence

Using AXIOM Process, you can acquire mobile devices as well as load existing images, files, and folders previously acquired from mobile devices.

When you image a mobile device, specifying the operating system alerts AXIOM Process as to which set of artifacts should be scanned for, as data resides in different locations depending on the operating system. While some artifacts (i.e. Facebook, Twitter, WhatsApp, etc.) can be parsed from multiple mobile operating system types, the location and structure of the data can vary on each operating system.

Method	Supported evidence source	Description
Acquire evidence	Android	Use this option to acquire evidence from an Android device. For Android devices running version 2.1 and later, AXIOM Process can obtain full images from rooted Android devices and quick images from other Android devices.
	iOS	Use this option to acquire evidence from an iOS device. AXIOM Process can obtain a quick image from iOS devices (version 5.0 and later) and full images from jailbroken iOS devices.
	Kindle Fire	Use this option to acquire evidence from a Kindle Fire device.
	Media devices that support MTP	Use this option to acquire evidence from media devices that support the media transfer protocol (MTP). Examples of media devices that typically support MTP include digital cameras, feature phones, and smartphones such as Android, iOS, BlackBerry, and Windows Phone.
Load evidence	Images and files and folders	Use this option to load existing images, files, and folders from supported Android, iOS, Windows Phone, and Kindle Fire devices.

Android

Acquiring an Android Device

For Android devices running version 2.1 and later, AXIOM Process can obtain full images from rooted Android devices and quick images from other Android devices.

- A **quick** image is a comprehensive logical image that contains both user data and some native application data. AXIOM Process attempts multiple acquisition methods to get you as much information as possible from the device, as quickly as possible, so that you can start examining the evidence right away.
- A **full** image is a physical or file-system logical image. During this type of acquisition, AXIOM Process copies the entire contents of a device into a single file (either a .raw file or a .zip file, depending on the device). With a full image, you have a higher possibility of recovering data from unallocated space (that is, deleted files).

If you're unable to acquire either a quick or a full image, another option for some devices is to acquire media.

Review the Supported acquisition methods for Android devices topic for more information about which acquisition methods are available for specific Android versions.

In addition to acquiring evidence from an Android device, you can load existing images and files and folders.

Access to data on Android devices

The type of image that you can acquire from a device depends on the level of access that you have. Acquiring a full image requires that you have privileged access to the device. Privileged access indicates that you have an enhanced level of permissions which allow you to interact with the device in ways that a regular user can't.

On Android devices, having *root access* gives you enhanced permissions so that you can run apps that need access to certain system settings, flash custom images to the device, and more.

For full images, if an Android device is not rooted, AXIOM Process attempts to gain privileged access to the device using tested rooting methods. AXIOM Process creates a log file documenting the process, and indicates which roots are tried and whether any are successful.

Supported acquisition methods for Android devices

Full images are formatted as .raw files and quick images are formatted as .zip files.

	OS	Method	Evidence
Full	Android 2.1 and later**	Linux DD command	Recover a full physical image of the device's flash memory. Evidence collected includes all files, folders, user data, native data, and unallocated space.
Quick	Android 2.1 to 8+	Android Debug Bridge (ADB) mode	Contents of any external storage (for example, an SD card).
	Android 2.1 to 8+	Agent application	Call logs, SMS/MMS, browser history, and user dictionary.
	Android 4.0 and later	ADB backup / agent application	Third-party application user data. Some native device data including SMS/MMS, browser history, calendar, call logs, BT devices, WiFi hot spots, user accounts, and user dictionary. Contents of any external storage (for example, an SD card).
	Android (Samsung models only)	MTP bypass	Pictures, videos, and any other files discoverable via MTP.

** Requires a rooted device. In some cases, AXIOM Process can root the device for you.

Prepare an Android device for image acquisition

Before you acquire an image from an Android device, verify that your computer and device are set up correctly.

To make sure AXIOM Process can connect to the Android device and acquire the most complete forensic image possible, there are several options that you need to set.

Tip: If you don't want your search criteria to be saved in the recent search history on the device, don't use the magnifying glass on the mobile device to search for settings or other information.

- Turn on the device.
- Connect the device to the computer using a sync cable (not a charging cable).
- Charge the device to at least 50%.
- Unlock the device.
- Turn on airplane mode.
- Verify the device is running Android 2.1 or later.
- Set the USB option to charging. On some devices, you must set this option each time the USB cable is reconnected or the device is restarted.
- Turn off USB mass storage (on devices with micro SD capabilities). If this option is turned on, the device might unmount the SD card, resulting in less data being acquired during a quick image.
- Turn on USB debugging/developer mode. On most devices, you turn on developer mode by tapping on the build number until the "You are now a developer" message appears on the screen.
- Verify that USB debugging/develper mode is in turned on. On some devices, you must turn this setting on after you turn on USB debugging/developer mode. In **Settings** > **Developer options**, turn on **USB debugging**.
- Set the screen to stay awake. In **Settings** > **Developer** options, turn on **Stay awake**.
- Trust the computer that the device is connected to. When you connect the device to the computer, follow the device's on-screen instructions.
- Turn off the Verify apps via USB or Verify apps: Block or warn setting. In **Settings** > **Developer options**, turn off **Verify apps via USB**. The wording of the setting might vary depending on the device manufacturer.

- Allow the installation of applications from unknown sources. In **Settings** > **Security**, turn on **Unknown Sources**. The wording of the setting might vary depending on the device manufacturer.

Tip: You must turn on USB debugging mode before you receive a prompt to trust the computer. To revoke the trust setting, in **Settings** > **Developer options** tap **Revoke USB debugging authorizations**.

Turn on USB debugging for Android devices

Depending on the type of Android device, there are different ways to turn on USB debugging or developer mode. Here's how you can turn on USB debugging for a few popular devices:

Type of device	Turn on USB debugging
Android 2.x+	In **Settings** > **Applications** > **Development**, tap the **Enable USB Debugging** option.
Android 4.2+	In **Settings** > **About phone**, tap the **Build Number** field approximately 7 times until "You are now a Developer" displays on the screen.
HTC One (M7/M8/M9)	In **Settings** > **About** > **Software information** > **More** > **Build number**, tap the **Build Number** field approximately 7 times until "You are now a Developer" displays on the screen.
LG G2/G3 Samsung Galaxy	In **Settings** > **About phone** > **Software information** > **Build number**, tap the **Build Number** field approximately 7 times until "You are now a Developer" displays on the screen.
Stock Android	In **Settings** > **About phone**, tap the **Build Number** field approximately 7 times until "You are now a Developer" displays on the screen.

Bypass the lock screen on an LG device

If a LG Android device is locked and you don't have the passcode, you can attempt to bypass the lock screen in AXIOM Process. AXIOM Process supports bypassing the lock screen for many LG devices but does not currently support LG Nexus devices.

After successfully bypassing the lock screen, you can perform an acquisition of the device without needing the passcode.

1. In AXIOM Process, click **Evidence Sources** > **Mobile** > **Android** > **Acquire Evidence** > **Advanced (Lock Bypass)** > **LG Electronics** > **Lock bypass**.
2. Follow the instructions in AXIOM Process.
3. To start an acquisition of the device, click **Next** and select start an unlocked acquisition workflow for the device.

Downgrading apps

Some newer mobile device apps block access to their data. You can choose to temporarily install a previous version of the app that provided access to the data, acquire the evidence, and then install the original app back on the device again.

When acquiring a quick image of a device running Android 6.0 and earlier, you can turn on app downgrading in AXIOM Process.

Warning: There are risks associated with app downgrading. You might change data on the device when you use this feature.

Device drivers for popular Android device manufacturers

If you're connected to the Internet while using AXIOM Process, AXIOM Process attempts to download the appropriate drivers for the mobile device that you're imaging. If the correct driver can't be found, you might have to visit the device manufacturer's website to download the driver. Here are the links to download drivers for a few popular devices:

- HTC: www.htc.com/us/software
- LG: www.lg.com/us/support
- Motorola: support.motorola.com
- Nexus: developer.android.com
- Samsung: developer.samsung.com
- Sony: developer.sony.com/develop/drivers/

Acquire a locked Android device

As the development of smartphone software advances, it becomes increasingly difficult to gain privileged access to the device. When a device is locked, you might be prevented from being able to extract any data.

To help you acquire the most complete forensic image as possible, AXIOM Process supports several advanced mobile acquisition methods that increase your chances of getting a full image of the device. Some methods require that you flash the device with a recovery image, while others take advantage of download modes or device hardware features.

For more information about acquiring Android devices using Advanced lock bypass, review the following articles about acquisition methods for popular device manufacturers in the Customer Portal. For some acquisition methods, you can also download recovery images and drivers.

Hardware / Manufacturer	Acquisition method	Image type
Samsung	Flash a recovery image of a Samsung device	Full image
	Acquire a Samsung device using MTP bypass	Quick image
Motorola	Acquire a Motorola device using bootloader bypass	Full image
LG	Acquire an LG device using download mode	Full image
MTK chipsets	Acquire an MTK device using download mode	Full image
	Acquire an MTK device using an SD card backup	Logical image
Qualcomm chipsets	Acquire a Qualcomm device using EDL mode	Full image
All Android devices	Flash a custom recovery image of an Android device	Full image

Acquire an unlocked Android device

If the Android device you want to acquire is unlocked, and you can turn on USB debugging, you can you attempt to acquire a full or a quick image of the device using Android Debug Bridge (ADB). Acquiring a full image requires privileged (root) access.

1. Start the ADB workflow in AXIOM Process: Click **Evidence Sources** > **Mobile** > **Android** > **Acquire Evidence** > **ADB (Unlocked)**.
2. Follow the instructions in AXIOM Process.
3. To continue setting up your case, click **Next**.

Customize Android acquisition settings

Create segments for Android images

You can specify the size of the image segments that you want AXIOM Process to create when it acquires evidence from Android and drive images. Each option represents a different size that reflects its storage capabilities. By default, image segmentation is turned off.

1. In AXIOM Process, on the **Tools** menu, click **Settings**.
2. In **Imaging** > **Image segmentation**, select a format from the drop-down list.
3. Click **Okay**.

Restore device state for Android devices

While AXIOM Process acquires evidence from Android devices, it installs an agent application onto the device to assist with recovering data. When the scan completes, AXIOM Process can remove the agent application from the device. By default, the agent application is left on the device.

1. In AXIOM Process, on the **Tools** menu, click **Settings**.
2. In **Imaging** > **Restore mobile device state**, select the **Remove agent application** option.
3. Click **Okay**.

iOS

Acquiring an iOS device

AXIOM Process can obtain a quick image from iOS devices (version 5.0 and later) and full images from jailbroken iOS devices.

- A **quick** image is a comprehensive logical image that contains both user data and some native application data. AXIOM Process attempts multiple acquisition methods to get you as much information as possible from the device, as quickly as possible, so that you can start examining the evidence right away.
- A **full** image is a physical or file-system logical image. During this type of acquisition, AXIOM Process copies the entire contents of a device into a single file (either a .raw file or a .zip file, depending on the device). With a full image, you have a higher possibility of recovering data from unallocated space (that is, deleted files).

If you're unable to acquire either a quick or a full image, another option for some devices is to acquire media.

In addition to acquiring evidence from an iOS device, you can load existing images and files and folders such as including encrypted iOS backups and GrayKey images.

Access to data on iOS devices

The type of image that you can acquire from a device depends on the level of access that you have. Acquiring a full image requires that you have privileged access to the device. Privileged access indicates that you have an enhanced level of permissions which allow you to interact with the device in ways that a regular user can't. Gaining privileged access to an iOS device is often achieved by jailbreaking the device.

On iOS devices, a jailbreak uses an exploit or security vulnerability in the software to give you enhanced permissions to the operating system. For early iOS versions, these permissions allowed you to get a full image of the device, but for iOS 5.0 and later, the encryption allows only a logical image to be obtained.

Jailbreaks are often discovered after the release of a new iOS version. The timing of their availability depends on how difficult it is to find the vulnerability in the software. For many modern iOS devices, there are no public jailbreaks available. You should monitor public jailbreaks to stay current.

Supported acquisition methods for iOS devices

Both full images and quick images from an iOS device are formatted as .zip files.

	OS	Method	Evidence
Full	iOS 5 to 10+ **	SSH	For jailbroken iOS devices, AXIOM Process recovers a full logical file system dump that includes all of the files, folders, user data, and native data.
Quick	iOS 5 to 11+	iTunes backup process	Third-party application user data. Some native device data, including: SMS/MMS and iMessage, calendar, and call log.
	iOS 5 to 11+	Apple File Conduit	Camera pictures, ringtones, and iTunes books.
	iOS 8 and earlier	File relay	Some native device data, including: complete photo album, SMS/MMS and iMessage, address book, typing cache, geolocation cache, application screen shots, WiFi hot spots, voicemail, and native email metadata.

** Requires a jail-broken device.

Prepare an iOS device for image acquisition

Before you acquire an image from an iOS device, verify that your computer and device are set up correctly.

To allow AXIOM Process to connect to the iOS device and acquire the most complete forensic image possible, there are several options that you need to set. After setting these options, you should also perform an encrypted backup. AXIOM Process can often extract more evidence from an iOS device if it first creates an encrypted backup of the device. An encrypted backup can include information that isn't available in a normal quick image, such as saved passwords (iOS keychain), health data (HealthKit), smart home data (HomeKit), and more.

Tip: If you don't want your search criteria to be saved in the recent search history on the device, don't use the magnifying glass on the mobile device to search for settings or other information.

- Verify your computer is running the latest version of iTunes.
- Turn on the device.
- Connect the device to the computer using a sync cable (not a charging cable).
- Charge the device to at least 30%.
- Unlock the device.
- Turn on airplane mode.
- Verify that the device is running iOS 5 or later.
- Turn off screen lock or set it to the maximum amount of time.
- Set the screen timeout or sleep mode to stay awake, or to the maximum amount of time.
- Trust the computer that the device is connected to. When you connect the device to the computer, follow the device's on-screen instructions. On iOS 8 and later, to revoke trust, tap **Settings** > **General** > **Reset** > **Reset Location & Privacy**.

Acquire an encrypted iOS backup

During the acquisition setup, AXIOM Process automatically prompts you for an encryption password if you choose the Quick image option. After the search starts, AXIOM Process creates an encrypted backup of the device and then decrypts the backup using the password that you provide. After imaging completes, AXIOM Process removes the password from the device.

1. In AXIOM Process, click **Evidence sources** > **Mobile** > **iOS** > **Acquire evidence**.
2. Select the device, and then click **Next**.
3. Select the **Quick** image type and click **Next**.
4. In the **Encrypted iTunes backups** dialog, provide a password to use for encryption and click **Okay**.
5. To continue setting up your case, click **Next**.

Acquire a jailbroken iOS device

You can extract a full image from an iOS device if the device is jailbroken, and SSH is installed. When SSH is configured, it allows you to interact with the device in ways that a regular user can't. You can run commands on the device, access the file system, or install third-party applications.

When you connect a jailbroken iOS device to AXIOM Process, it attempts to detect SSH automatically. If the device is supported, AXIOM Process indicates that it has *privileged access* to the device. If AXIOM Process can't connect to the device, only the Quick image option is available.

> Note: AXIOM Process no longer supports AFC2 as a service to communicate with iOS devices. This service was often used by jailbreak tools such as Cydia but is less commonly supported in newer jailbreaks.

Connecting to a device using SSH

When AXIOM Process detects that SSH is present on an iOS device, it attempts to connect to the device automatically by using the default SSH credentials (username: root, password: alpine).

If the SSH credentials are not set to the default values, AXIOM Process prompts you to provide the correct credentials to attempt to connect again.

If connecting to the device using SSH is unsuccessful, AXIOM Process will attempt to connect to the device using TCP and will require the device to be connected to the network.

Acquire a full image from a jailbroken iOS device

To acquire a full image of an iOS device, AXIOM Process must have privileged access to the device.

1. In AXIOM Process, click **Evidence sources** > **Mobile** > **iOS** > **Acquire evidence**.
2. Select the device to acquire, and then click **Next**.
3. Select the **Full** image type.
4. To continue setting up your case, click **Next**.

Kindle Fire

Acquiring a Kindle Fire device

AXIOM Process includes support for acquiring evidence from Kindle Fire devices. Kindle Fire uses a custom version of the Android operating system. While AXIOM Process supports acquisition of Android devices, using the Kindle Fire acquisition method provides support for Kindle-specific applications and artifacts. For example, Kindle Fire devices use the Amazon Silk browser, which uses Amazon Web Services (AWS) and stores browser-related artifacts differently than other Android devices. AXIOM Process searches the Amazon Silk browser for evidence such as remnants from AWS on the device.

In addition to acquiring evidence from a Kindle device, you can load existing images and files and folders previously acquired from the device.

To acquire evidence from a Kindle Fire device, complete the following steps:

1. In AXIOM Process, click **Evidence sources** > **Mobile** > **Kindle Fire** > **Acquire evidence**.
2. Select the device, and then click **Next**.
3. Select the type of image you want to acquire, and then click **Next**.
4. Continue setting up your case.

Media device (MTP)

Acquiring media and files through MTP

Using the media transfer protocol (MTP), you can acquire media and files–including pictures, videos, audio files, documents, downloads, application data, and user data–from a media device. If other acquisition methods don't work for smartphones, MTP can sometimes bypass certain encryption methods and passwords so you can obtain a logical acquisition of the device.

You can use the MTP option with media devices that support the media transfer protocol (MTP), including: digital cameras, feature phones, and smartphones like Android, iOS, BlackBerry, and Windows Phone.

Before you begin: To acquire evidence from smartphones using MTP, the USB charging option must be set to Media Transfer Protocol.

1. In AXIOM Process, click **Evidence sources** > **Mobile** > **Media device (MTP)**.
2. Select the device, and then click **Next**.
3. Select the type of image you want to acquire, and then click **Next**.
4. Continue setting up your case.

SIM cards

Acquiring SIM cards

You can acquire mobile phone SIM cards and create a logical image of the SIM card files. This type of image contains all of the dedicated and elementary files available on the SIM card but is not a byte for byte copy of the SIM card.

Before you begin: Install the drivers required by your SIM card reader hardware and make sure that the SIM card reader is connected to your computer.

1. In AXIOM Process, click **Evidence sources** > **Mobile** > **SIM card**.
2. Select the SIM card, and then click **Next**.
3. Select the type of image you want to acquire, and then click **Next**.
4. Continue setting up your case.

Load evidence from mobile devices

In addition to acquiring mobile devices, AXIOM Process can search previously acquired images, files, and folders from Android, iOS, Windows Phone, and Kindle Fire devices.

Load a mobile image

Note: The VeraKey option is only available for AXIOM Cyber users.

Use this option to process previously acquired images (including GrayKey or VeraKey category based extractions) from mobile devices.

Keychain and keystore files

If you acquired an iOS or Android image using GrayKey, VeraKey, or an iOS Cellebrite checkra1n extraction, you can optionally provide an Android keystore or an iOS .plist keychain when you load the evidence source.

The keychain and keystore files both contain passwords and decryption keys for the applications on the device. AXIOM Process will process the file first to extract the passwords and decryption keys, and then use those items to decrypt application data to give you access to more data. The decrypted results will automatically appear in AXIOM Examine.

iOS keychain

For information about processing an iOS GrayKey or VeraKey image, sign in to the Support Portal to read the following article: Load a GrayKey or VeraKey image.

Android keystore

For information about using the Android keystore and Graykey images, sign in to the Support Portal to read the following article: Decrypt app data using the Android keystore and GrayKey.

Cellebrite

For information about processing unrecognized Cellebrite image formats, sign in to the Support Portal to read the following article: Processing unrecognized UFD/UFDX formats in AXIOM article.

1. In AXIOM Process, click **Evidence sources** > **Mobile**.
2. Select the operating system for the image that you want to load.
3. Click **Load evidence** > **Image**.
4. Browse to the image you want to load and click **Open**.
5. Select the specific files and folders you want to load.
6. Enter a keychain file (Applies only to iOS Cellebrite checkra1n extractions):
    a. Next to the **Keychain file** field, click **Browse**.
    b. Browse to the keychain file you want to load and then click **Open**.
    c. After the keychain file validates, click **Next**.
7. To continue setting up your case, click **Next**.

Load files and folders from a mobile device

During the search, AXIOM Process will automatically create an image (.zip) of the specified files and folders and save the image in the acquired evidence location.

1. In AXIOM Process, click **Evidence sources** > **Mobile**.
2. Select the operating system for the files or folders that you want to load.
3. Click **Load evidence** > **Files and folders**.
4. Complete one of the following options:
    - From the displayed network or disks, browse to and select the files or folders you want to search. Click **Next**.
    - Click **Folder browser** to browse to a folder stored locally on your computer. Click **Select folder**.
    - Click **File browser** to browse to a file stored locally on your computer. Click **Open**.
5. Continue setting up your case.

Load an encrypted iOS backup

> Warning: Before you connect an iOS device to iTunes, you must first ensure that the **Prevent iPods, iPhones, and iPads from syncing automatically** option is turned on before you connect the device. If you don't turn this setting on first, there's a chance that you might contaminate your evidence by syncing external data to your device.

1. In AXIOM Process, click **Evidence sources** > **Mobile** > **iOS** > **Load evidence**.
2. Complete one of the following options:
   - To load an image of an encrypted iOS backup, click **Image**.
   - To load an encrypted backup file, click **Files and folders**.
3. Browse to the encrypted iTunes backup, and then click **Open**.
4. When prompted, provide the password, and then click **Check**.
5. Click **Okay**.
6. Continue setting up your case.

After AXIOM Process finishes searching the evidence, you'll see two evidence sources in AXIOM Examine—one for the original encrypted source and one for the decrypted backup.

Supported images and file types

Image/file type	Supported extensions	Segmented image support
Advanced Forensics File images	.AFF4, .AFF4-L *Some AFF4-L formats are unsupported*	*Supported*
Archive files	.ab, .cpio, .cpio.gz, .dar, .docx, .gz, .gzip, .pptx, .rar, .tar, .tar.gz, .tgz, .xlsx, .zip, .zip.001, .z00, .z01, .7z, .7z001	*Supported:* .gzip, .rar, .zip, .zip.001, .7z.001
Cellebrite images	.ufd, .ufdx	*Supported*

Image/file type	Supported extensions	Segmented image support
EnCase images	.E01, Ex01, .L01, .Lx01	*Supported*
FTK images	.AD1	
RAW images	.bif, .bin, .dd, .dmp, .fip, .ima, .img, .mfd, .mem, .raw, .vfd	*Supported:* DD (.000, 001, .0000, .0001, etc.)

Vehicles

Loading evidence from vehicles

AXIOM Process can report evidence such as Routes, Trackpoints, and Waypoints by reading exported IVO files recovered using iVe from vehicles.

You will need to make sure that you choose the Magnet export option from iVe so AXIOM Process can read your IVO file(s).

Load a Magnet IVO image from a vehicle

During the search, AXIOM Process will automatically create an image (.zip) of the specified files and folders and save the image in the acquired evidence location. Use this option to process previously acquired images from vehicles.

1. In AXIOM Process, click **Evidence sources** > **Vehicle** > **iVe**.
2. Click **Files and folders**.
3. On the **Add files and folders** screen, complete one of the following options to load .ivo file(s):
    - From the displayed network or disks, browse to and select the files or folders you want to search. Click **Next**.
    - Click **Folder browser** to browse to a folder stored locally on your computer. Click **Select folder**.
    - Click **File browser** to browse to a file stored locally on your computer. Click **Open**.
4. To continue setting up your case, click **Next**.

PROCESSING DETAILS

Configure advanced processing features so that you can use to get more out of your search:

Search archives and mobile backups

During processing, AXIOM Process can search archive files (such as .zip and .tar files) and mobile backup files (such as Android backup (.ab) files and iOS backup folders). To search mobile backups, the mobile backup files must be decrypted. You can provide potential passwords for AXIOM Process to use to decrypt the device. You can also choose the number of layers of nested archives and mobile backups that AXIOM Process searches.

After processing completes, you can open and search the contents of any discovered archives or mobile backups in AXIOM Examine.

Search archives and mobile backups

1. In AXIOM Process, click **Processing details** > **Search archives and mobile backups**.
2. To search archive files, click the **Search archives** option.
3. To search mobile backups, click the **Search mobile backups** option. Make sure you add potential passwords for AXIOM Process to use to decrypt the device.
4. Continue setting up your case.

Decrypt mobile backups

For AXIOM Process to search mobile backups, the mobile backup files must be decrypted. Add potential passwords for AXIOM Process to use to decrypt the device.

1. In AXIOM Process, click **Processing details** > **Search archives and mobile backups**.
2. In the **Mobile backup passwords** field, provide each potential password on its own line.
3. Continue setting up your case.

Set the number of nested archive and mobile backup search layers

You can choose the number of layers of nested archives and mobile backups that AXIOM Process searches (to a maximum of 100 layers).

1. In AXIOM Process, click **Processing details** > **Search archives and mobile backups**.
2. In the **Nested archives and mobile backups** field, type the number of nested archive and mobile backup layers that you want AXIOM Process to search for.
3. Continue setting up your case.

Turn off searching for archives and mobile backups

If you turn off these settings, AXIOM Process will not search for nested archives or mobile backups.

1. In AXIOM Process, click **Processing details** > **Search archives and mobile backups**.
2. To turn off searching archives, clear the **Search archives** option.
3. To turn off searching mobile backups, clear the **Search mobile backups** option.
4. Continue setting up your case.

Decode file-based encryption

Note: This feature is only available for AXIOM Cyber users.

Some of your evidence sources may contain encrypted files. It is possible that even some decrypted evidence sources may contain some encrypted files. AXIOM Process supports decrypting evidence using Dell Credant/Dell Data Protection Encryption (DDPE).

Use the Decode file-based decryption option to apply DDPE decryption to the selected evidence source. AXIOM Process decrypts the files with DDPE offline. Once processed, AXIOM Process creates a secondary evidence source for just the decrypted version of the files. The decrypted evidence source can be found in the acquired evidence location that you configured for the case.

Only DDPE files will appear in the new evidence source, and will correspond with their original location in the file system. Encrypted files may still appear as artifacts in the primary evidence source if they match artifact generation patterns.

For more information on decrypting a particular evidence source, see Decrypt evidence.

Decrypt file-based encryption

1. In AXIOM Process select **Processing details** > **Decode file-based encryption**.
2. Select **Dell Credant/ Dell Data Protection Encryption.**

3. Provide a **Recovery file**.
4. Enter a **Password** then select **Check the password**.
5. Select the **Evidence source**. You can only decrypt one evidence source at a time. Only evidence sources that are applicable for decryption will be available. For example, you cannot select unpartitioned space.
6. Continue with your search.

Add keywords to a search

AXIOM Process: Click **Processing details** > **Add keywords to search**

AXIOM Examine: In the Artifacts explorer, on the Filters bar, click **Keyword lists** > **Add keywords**

Use keywords and regular expressions to search or filter large amounts of text in the evidence. Keywords that you include in your search are added to the Keywords filter in the Artifacts explorer in AXIOM Examine. If you selected to tag privileged content for review in Examine, you can filter the privileged content using the Tags and comments filter.

Search types

Consider whether an Artifacts or an All content search makes more sense for your case. Artifact searches are faster whereas all content searches take longer but are more thorough.

Artifacts

- Artifact keyword searching looks for keywords in only the artifacts that AXIOM Process can or has recovered. As part of this process, encrypted or encoded artifacts are decrypted into plain text that can be searched using keywords.
- Search results are limited to the artifacts that AXIOM Process supports but hits are found quickly.
- In AXIOM Examine, each of the keywords and regular expressions that you get a result

on are added to the Keywords filter.

- You can turn on or turn off an entire list of items by clicking on the file name.

All content

- Searching for keywords in all content is a byte for byte search of data in the encoding type that you specify. AXIOM Examine supports ASCII, UTF-7, UTF-8, UTF-16, and UTF-32. If you're not sure which encoding type to use, select them all.
- During an all content keyword search, AXIOM Process or AXIOM Examine will look for matching bytes in little-endian byte order for keywords encoded using UTF-16 and UTF-32. Keywords encoded using ASCII, UTF-7, and UTF-8 are endianness independent and read byte by byte.
- Case-sensitive search is only available for all content searches. Select the Case sensitive option next to the search term or keyword list.
- AXIOM Process and AXIOM Examine look for keywords across the entire evidence source—not just the artifacts that it recovers.
- Searching all content for keywords can increase processing time significantly, but AXIOM Process and AXIOM Examine can find hits in data (including deleted content) without a corresponding artifact type. During an all content search, AXIOM Examine will process keyword snippets from the selected evidence sources only. Afterwards, AXIOM Examine will search all artifacts in the case for matches.
- In AXIOM Examine, in the Artifacts explorer, each of the keywords and regular expressions that you get a result on are added as new keyword snippets. If a keyword result is found on an item that is both an artifact and resides in the file system (for example a result on a document discovered in unallocated space) the keyword is counted twice. It appears as a result on the artifact itself and as a new keyword snippet.

Privileged content

- Privileged content keyword lists perform an Artifacts search to exclude content from the Artifacts explorer or to tag matching content for review in AXIOM Examine.
- Use privileged content keywords when configuring your case in AXIOM Process. Select **Artifact details** > **Privileged content**.

- The formatting requirements for privileged content keyword lists are similar to other keywords lists.
- Upon successful completion of a search, the selected privileged content filtering options are available in the Case information.txt.
- If you selected to tag privileged content for review in Examine, you can filter the privileged content using the Tags and comments filter.

Note: Results in the File system explorer are not affected when filtering privileged content.

Using AXIOM Examine while adding keywords

While processing evidence sources for keywords is in progress, you can continue working in your case, however, searching evidence for keywords can be resource intensive. Depending on your workstation, interacting with AXIOM Examine might become slower than normal while keywords finish processing.

If you stop processing keywords while AXIOM Examine is adding results from the keyword search to your case, only the partial results will be added to your case. After you stop processing, AXIOM Examine will add the partial results to the search index and keyword list filter, which might take some time.

Format your keyword list

- Must be a.kws or .txt file.
- Each search term must appear on a new line.
- A single file can contain both keywords and regular expressions.
- A keyword list that contains ASCII characters defaults to the ASCII encoding type.
- If a keyword list contains non-ASCII characters, only non-ASCII characters are encoded as UTF-8.
- Limit the size of your keyword list to 30 entries to reduce processing time.
- Avoid using keywords with fewer than 3 characters to avoid irrelevant matches being found in your case.

Regex

A regular expression is a pattern that you define using a sequence of letters, numbers, and special characters. AXIOM Process and AXIOM Examine support the .NET Framework syntax for creating regular expressions. For more information about using regular expressions in AXIOM, sign in to the support portal to read the following article: Add regular expressions to search in Magnet AXIOM.

Extract text from files (OCR)

Using optical character recognition (OCR) technology, AXIOM Examine can extract text from PDF documents (including text in email PDF attachments, text in scanned documents and text from pictures in PDF documents) and from picture artifacts. OCR is optimized to extract text from pictures in PDF documents, scanned documents, and pictures of documents. While OCR can extract text from other types of pictures, such as pictures of scenery, results might vary. This feature is available to extract text for Latin characters.

You can configure OCR to run automatically during the post-processing actions portion of a search. If you don't run OCR immediately after a search, you can do so later from AXIOM Examine.

After processing the files, you can view the extracted text in the *Text extracted using OCR* preview card in AXIOM Examine. Additionally, you can search the extracted text from these files using the keyword search in AXIOM Examine, and you can include text extracted using OCR as an attachment for artifacts in HTML exports.

Text extraction using OCR is available with an active Magnet AXIOM Complete, AXIOM Cyber, or Magnet AXIOM Examine license.

> Note: Text extraction using OCR is currently unavailable in the Media explorer.

Start extracting text from files after processing completes

You can configure AXIOM Process so that AXIOM Examine begins extracting text from files immediately after your case finishes processing.

Note: Running OCR requires more processing time. To decrease processing time, consider running OCR from AXIOM Examineafter your case finishes processing.

1. In AXIOM Process, click **Processing details** > **Extract text from files (OCR)**.
2. Under **Process files using optical character recognition (OCR)**, select the files you want to extract text from.
3. Continue setting up your case.

Extract text from files in your case

If you didn't previously configure AXIOM Process to extract text from files after your case finished processing, you can run OCR from AXIOM Examine. If you add more evidence to your case, you must run OCR again to extract text from new PDF documents and pictures. AXIOM Examine will only process the new files.

Note: OCR is optimized to extract text from pictures in PDF documents, scanned documents, and pictures of documents. While OCR can extract text from other types of pictures, such as pictures of scenery, results might vary.

1. In AXIOM Examine, on the **Process** menu, click **Extract text from files (OCR)**.
2. From the **Extract text from files** dialog, select the types of artifacts that you want to extract text from.
3. If applicable, select the items you want to process.
4. Click **Process artifacts**.

While text extraction is in progress, you can view the evidence that has already been processed. In the status bar, click **Show results**.

View text extracted from files

After AXIOM Examine extracts text from pictures in PDF documents and picture artifacts, you can view the extracted text in the Text extracted using OCR preview card in AXIOM Examine. The Text extracted using OCR preview card is available in the Artifacts, File system, Timeline, and Connections explorers .

You can also apply the Extracted text (OCR) content types filter to view all evidence items where text was extracted using OCR. For more information about filtering evidence, review the Filter by criteria in the evidence topic.

> Note: If a PDF document or picture was recovered through carving, text extracted using OCR will not appear in the Text extracted using OCR card in the File system explorer. You must view extracted text for carved evidence from the Artifacts explorer.

Include text extracted using OCR in an export

When you export evidence using the HTML export type, and you enable the option to include previews and file attachments, text extracted using OCR is included as an .txt file in your export. For more information about configuring exports / reports, see Configure artifact details.

Calculate hash values and find matches

> AXIOM Process: Select **Processing details** > **Calculate hashes and find matches**
>
> AXIOM Examine: Select **Process** > **Categorize pictures and videos by hash value**

By calculating hash values for all files and importing hash sets of known files, AXIOM Process automatically searches and categorizes evidence for you. AXIOM Process remembers your previous selections the next time you create a new case or add evidence to an existing case.

Calculate hash values for all files

During a search, AXIOM Process can calculate unique hash values for each file. In AXIOM Examine, you can then quickly search for, compare, or filter those files based on known hash sets (for example, NSRL hash sets).

Calculating hash values slows down processing times. By default, files larger than 500 MB will not be hashed though you can customize the file size limit for hashing.

1. In AXIOM Process, click **Processing details** > **Calculate hashes and find matches**.
2. In **Calculate hash values for all files**, select **Calculate hash values for all files**.
3. Continue setting up your case.

Import local hash lists for known files

If you want to quickly see if known files exist in your evidence, you can import a list of hash values for files that might be of interest to your case.

Hash lists must be .txt files containing MD5 or SHA1 hashes (such as NSRL files), with each hash on a separate line. After you add a hash list, you can provide a tag that gets applied to the files. You can view the matching files in the File system explorer in AXIOM Examine.

Tip: Instead of searching for hashes using local hash list files, as outlined below, you can also use hash sets stored in your organization's Magnet Hash Sets Manager database. To learn more, see Find matching hashes using Magnet Hash Sets Manager.

1. In AXIOM Process, click **Processing details** > **Calculate hashes and find matches**.
2. Select the option to **Calculate hash values for all files**.
3. In **Tag known files with matching hash values**, click **Add hash list**.
4. Browse to the location where you saved the hash list and click **Open**.
5. If applicable, clear the **Enabled** option next to any previously imported hash list files that you don't want to use for this search.
6. In the **Tag** field, provide a name for the tag.
7. Continue setting up your case.

Ignore non-relevant files in a search using local hash lists

If you don’t want common operating system files like icons, wallpapers, system files, and so on to clutter up your evidence, you can exclude them by providing their hash values in a hash set. Ignoring non-relevant files is subject to the specified size limit for hash files.

Hash lists must be .txt files containing MD5 hashes (such as NSRL files), with each hash value declared on its own line. Even though the files are excluded from the Artifacts explorer, you can still view the files in the File system explorer. For more information about the new RDSv3 format and how to use it, sign in the Customer Portal to read the following article: Recommended NSRL datasets in AXIOM.

> Tip: Instead of searching for hashes using local hash list files, as outlined below, you can also use hash sets stored in your organization's Magnet Hash Sets Manager database. To learn more, see Find matching hashes using Magnet Hash Sets Manager.

1. In AXIOM Process, click **Processing details** > **Calculate hashes and find matches**.
2. Select the option to **Calculate hash values for all files**.
3. In **Ignore non-relevant files**, click **Add hash list**.
4. Browse to the location where you saved the hash sets, and then click **Open**.
5. If applicable, clear the **Enabled** option next to any previously imported hash sets that you don't want to use for this search.
6. Continue setting up your case.

Customize hashing settings

Set the format for hash values

AXIOM Process can create hash values in MD5, SHA256, and SHA1 formats.

1. In AXIOM Process, on the **Tools** menu, click **Settings**.
2. In **Hashing** > **Hash formats**, select the hashing formats that you want to use.

Prevent hashing of large files

When you set up a search, you can add files that contain hash values. AXIOM Process then uses these values to ignore non-relevant files or automatically categorize pictures. In either case, AXIOM Process must hash every file it encounters during a search to compare to the hash lists. Hashing very large files can take a long time, so you can set the maximum size of files to hash to help improve search times. The default value is 500 MB.

1. In AXIOM Process, on the **Tools** menu, click **Settings**.
2. In **Hashing** > **File size limit for hashing**, select the **To optimize processing time, don't calculate hashes for files larger than** option.
3. Type the maximum file size (in MB) that you want to create hash values for.
4. Click **Okay**.

Set the location where you store hash values

You can change the location where imported hash sets are stored. If you change the location where imported hash values are stored, AXIOM Process must restart to apply the change.

1. In AXIOM Process, on the **Tools** menu, click **Settings**.
2. In **Hashing** >**Hash value storage location**, browse to the location you want imported hash values to be stored and click **Select folder**.
3. Click **Okay**.

To apply the changed location of the hash set database, AXIOM Process must restart.

If the hash set on your computer isn't stored in the new location that you choose, AXIOM Process must move it to the new location before it restarts.

If there is no hash set on your computer, AXIOM Process creates an empty HashList.db file at the new location you choose before it restarts.

Categorize media automatically by hash value

Note: To help streamline AXIOM Cyber investigations, Project VIC and CAID features are unavailable by default. To use these features, you must first Customize log collection and diagnostics.

AXIOM Process: Select **Processing details** > **Calculate hashes and find matches**

AXIOM Examine: Select **Process** > **Categorize pictures and videos by hash value**

Import hash lists that contain known pictures and videos so that AXIOM Process automatically searches and categorizes these evidence sources for you.

In addition to your own .txt files, you can import .json files from organizations like Project VIC and CAID, which allow for the sharing of hash sets between law enforcement organizations for the purpose of identifying media related to child exploitation. When you import Project VIC hash lists, you can view additional VICS metadata in AXIOM Examine such as tags, series, distributed media, identified victims, and more.

You can also enable PhotoDNA to use *fuzzy matching* to help identify even more pictures. With PhotoDNA enabled, AXIOM Process can identify pictures that are similar in appearance to existing Project VIC pictures and categorize them in the same way.

Tip: Instead of searching for hashes using local hash list files, as outlined below, you can also use hash sets stored in your organization's Magnet Hash Sets Manager database. To learn more, see Find matching hashes using Magnet Hash Sets Manager.

Select local hash sets to use to categorize media

You can select the hash sets you want to use to categorize pictures and videos found in your evidence sources. If you haven't previously imported local hash lists, add local hash lists and configure your hash sets first.

1. In AXIOM Process, click **Processing details** > **Calculate hashes and find matches**.
2. In the **Categorize pictures and videos by hash value** table, select the local hash sets you want AXIOM Process to use to categorize evidence.
3. If applicable, clear the **Enabled** option next to any hash sets that you don't want to use for this search.
4. Continue setting up your case.

When your search completes, AXIOM Examine adds each category number it gets hits for to the Media categorizations filter. When you categorize media using Project VIC hash lists, you can view VICS attributes and values in Media category details and filter by VICS attributes using the Media attributes (VICS) filter.

Manage local picture and video hash sets

To automatically categorize picture and video evidence by hash value, import local hash lists into AXIOM Process. These lists can be from organizations like Project VIC and CAID or your own files. Hash lists must be .json files or .txt files containing MD5, SHA1, or PhotoDNA hashes. For .txt files, each hash must be declared on its own line.

After you import a local hash list, you can add the hash list to a new or existing hash set, for example, when you want to update a Project VIC or CAID hash set with incremental updates downloaded from Hubstream.

> Tip: If you haven't previously configured your hash sets in AXIOM Process, set up your media categorization profile in AXIOM Examine by choosing a media categorization list. You can choose pre-set media categorization profiles for Canada (Project VIC), International (Project VIC), the United States (Project VIC), and the United Kingdom (CAID), or you can add a new list or import a list of media categories. When you choose a media categorization list in AXIOM Examine, you'll see the category names and colors you're familiar with when managing picture and video hash sets in AXIOM Process.

1. In AXIOM Process, click **Processing details** > **Calculate hashes and find matches**.
2. In **Categorize pictures and videos by hash value**, click **Add hash list**.
3. In **Step 1**, click **Select hash list**.

4. Browse to the hash list you want to import and click **Open**.
5. In **Step 2**, complete one of the following options:
   - To add the imported hash list to an existing hash set, select the hash set you want to update.
   - To add the imported hash list to a new hash set, click **Add new hash set**. Provide a name for the hash set and click **Add**.
6. In **Step 3**, complete one of the following options:
   - If the hash list you imported is a .txt file, from the drop-down, select the category you want to update in the hash set and click **Update hash set**. Repeat for other categories you want to update.
   - If the hash list you imported is a .json file, select the categories you want to update in the hash set and click **Update hash set**.
7. When you've finished updating your hash sets, click **Close**.

Set the priority of local media hash sets

If a matching hash value appears in more than one hash set with different categories applied to it AXIOM Process will apply the assigned category from the higher priority hash set.

1. In AXIOM Process, click **Processing details** > **Calculate hashes and find matches**.
2. In the **Categorize pictures and videos by hash value** table, click the hash set to reprioritize.
3. In the **Priority** column, click the up or down arrow to change the priority.

Enable PhotoDNA

If you import hash sets in AXIOM Process for the purpose of picture categorization, you can use PhotoDNA and fuzzy matching to help identify more pictures. Using PhotoDNA, AXIOM Process can identify pictures that have been modified to change their hash values and pictures that are similar in appearance to existing Project VIC pictures.

In addition to finding matching pictures with identical hashes, PhotoDNA also uses fuzzy matching to find similar pictures with slight modifications. A user may have modified a picture by re-sizing, cropping, or drawing over it, by adding a watermark, or by changing the resolution. Even with these changes, PhotoDNA can identify the picture as similar to the original picture. PhotoDNA works by converting pictures into a black-and-white format, dividing them into squares, and calculating a numerical value for each square. These values, which represent the shading in each square, are the PhotoDNA signature or hash of a picture.

When categorizing media using Project VIC or another hash set, PhotoDNA will categorize matches as non-pertinent only if there is a cryptographic hash match (MD5 or SHA1). PhotoDNA will not categorize media as non-pertinent for matches alone.

PhotoDNA is only available to law enforcement. To request a password, visit www.magnetforensics.com/photodnaregistration.

1. In AXIOM Process, on the **Tools** menu, click **Settings**.
2. In **Hashing** > **Enable photo DNA**, provide the password that you received from Magnet Forensics.
3. Click **Okay**.

Find matching hashes using Magnet Hash Sets Manager

Use Magnet Hash Sets Manager to upload and manage multiple hash sets in a single centralized database. You can upload media hash sets from organizations such as Project VIC or CAID, or custom hash list files, then use these hash sets to categorize illicit media, tag known files, or ignore non-relevant files.

Once your Magnet Forensics product is integrated with Magnet Hash Sets Manager, your team members can use it to access all the uploaded hash sets it contains to match files by hash across their cases. From AXIOM Examine, you can also Manually apply media categories to case evidence.

To download the Magnet Hash Sets Manager installer and guide, visit the free tools page on the customer portal.

Integrate Magnet Hash Sets Manager with AXIOM Process or AXIOM Examine

1. In AXIOM Process or AXIOM Examine, on the **Tools** menu, click **Settings**.
2. In the Settings window, click **Product integrations**, and select **Hash Sets Manager**.

3. Provide a server IP address and port, then click **Connect to server**.
4. After the connection is successful, click **Okay**.

Search for matches from hash sets using Magnet Hash Sets Manager

After you've integrated Magnet Hash Sets Manager with AXIOM Process, you can use hash sets from the centralized database to categorize media, tag known files, and ignore non-relevant files in your case.

1. In AXIOM Process, when you're creating or adding evidence to a case, under Processing details, click **Calculate hashes and find matches**.
2. If you want to use hash sets to search for known or non-relevant files, select the option to **Calculate hash values for all files**.
3. Under Search for matches from hash sets, if you haven't already integrated Magnet Hash Sets Manager with AXIOM Process, click **Integrate with Magnet Hash Sets Manager**.
    a. In the Settings window, under Product integrations, select **Magnet Hash Sets Manager**.
    b. Provide a server IP address and port, then click **Connect to server**.
4. Scroll down to the hash set type you want to search for.
5. In the table, in the Enabled column, select the hash sets you want to use to search for evidence in your case.
6. Continue processing your evidence.

Set the priority of media hash sets

If a matching hash value appears in more than one hash set with different categories applied to it AXIOM Process will apply the assigned category from the higher priority hash set.

1. In AXIOM Process, click **Processing details** > **Calculate hashes and find matches**.
2. In the **Categorize pictures and videos by hash value** table, click the hash set to reprioritize.
3. In the **Priority** column, click the up or down arrow to change the priority.

Analyze chats with Magnet.AI

Magnet.AI chat categorization can detect possible grooming/luring and sexual content in chat messages. When Magnet.AI categorizes chat messages, it tags the entire conversation or a group of messages in the conversation. Currently, Magnet.AI supports categorization of chat messages in English only.

For optimal performance of this feature, see optimizing the performance of Magnet.AI

Start categorizing chats after processing completes

You can configure AXIOM Process so that AXIOM Examine begins categorizing chats immediately after your case finishes processing.

1. In AXIOM Process, click **Processing details** > **Analyze chats with Magnet.AI**.
2. Under **Categorize chats with Magnet.AI**, select the chat categories you want Magnet.AI to categorize.
3. Continue setting up your case.

Categorize chats in your case

If you didn't previously configure AXIOM Process to categorize chats immediately after your case finished processing, you can start categorizing chats from AXIOM Examine.

Using Magnet.AI can be resource intensive. You can configure how AXIOM Examine allocates system resources to either prioritize categorizing evidence with Magnet.AI quickly or to allow you to continue to reviewing evidence in AXIOM Examine while Magnet.AI is still processing.

1. In AXIOM Examine, on the **Process** menu, click **Categorize chats with Magnet.AI**.
2. In the **System resource allocation** drop-down list, choose how you want AXIOM Examine to allocate system resources while categorizing chats.
3. Select the chat messages you want Magnet.AI to categorize, and then click **Next**.
4. Select the chat categories you want Magnet.AI to categorize.
5. Click **Categorize chats**.

While Magnet.AI categorization is in progress, you can view the evidence that has already been categorized. In the status bar, click **Show results**.

Analyze pictures with Magnet.AI

AXIOM Process: Select **Processing details** > **Analyze pictures with Magnet.AI**

AXIOM Examine: Select **Process** > **Categorize pictures with Magnet.AI**

Categorize Pictures with Magnet.AI

Magnet.AI picture categorization can detect possible items in pictures or files that contain pictures (such as pictures embedded in a .doc file). To improve Magnet.AI picture categorization potential, turn on Enhanced picture categorization of video.

Depending on the number of pictures being categorized in the case, categorizing pictures might take a while. Some categories, such as handwriting, hate symbols, human faces, human hands, and license plates, require additional processing time. While Magnet.AI is still processing, you can continue to review the evidence in AXIOM Examine.

Note: When you categorize pictures using Magnet.AI, if AXIOM Examine detects a GPU on your computer, and the GPU has more than 126 MB of free memory, it automatically attempts to use it. Using a GPU instead of a CPU can significantly decrease the time it takes to categorize pictures.

For more information about optimal performance of this feature, see Optimize the performance of Magnet.AI.

Tip: To learn more about Magnet.AI categories and performance, sign in to the Support Portal to read the following articles:

- Magnet.AI picture categories and content types
- Understanding the performance of Magnet.AI picture categorization

Integrate Thorn AI model for categorization

Thorn provides improved models for categorizing pictures as possible child abuse and nudity. Thorn is free of charge and only available to law enforcement agencies.

Select **Edit** beside the Thorn integration status to enable Thorn integration in **Product Integrations** by requesting an activation key.

Start categorizing pictures after processing completes

You can configure AXIOM Process so that AXIOM Examine begins categorizing pictures immediately after your case finishes processing.

> Tip: When categorizing pictures with Magnet.AI, we recommend that you save picture attachments to the case rather than access them from the original source. For more information, see Save picture attachments to the case.

1. In AXIOM Process, click **Processing details** > **Analyze pictures with Magnet.AI**.
2. Under **Categorize pictures with Magnet.AI**, select the picture categories you want Magnet.AI to categorize.
3. Continue setting up your case.

Categorize pictures in your case

If you didn't previously configure AXIOM Process to categorize pictures immediately after your case finished processing, you can start categorizing pictures from AXIOM Examine.

Using Magnet.AI can be resource intensive. You can configure how AXIOM Examine allocates system resources to either prioritize categorizing evidence with Magnet.AI quickly or to allow you to continue to reviewing evidence in AXIOM Examine while Magnet.AI is still processing.

1. In AXIOM Examine, on the **Process** menu, click **Categorize pictures with Magnet.AI**.
2. In the **System resource allocation** drop-down list, choose how you want Magnet AXIOM to allocate system resources while categorizing pictures.
3. Select the pictures you want Magnet.AI to categorize, and then click **Next**.

4. Select the picture categories you want Magnet.AI to categorize.
5. Click **Categorize pictures**.

While Magnet.AI categorization is in progress, you can view the evidence that has already been categorized. In the status bar, click **Show results**.

Remove a tag from categorized chats and pictures

If you think that Magnet.AI has incorrectly categorized evidence, you can remove the tag.

1. In AXIOM Examine, right-click the tagged evidence.
2. Click **Add/remove tag**.
3. Click an existing tag to remove it.

Build picture comparison manually

Before you find similar pictures, you must build picture comparison in your case so that Magnet.AI can analyze each picture file.

If you haven't changed the setting to build picture comparison automatically, or performed any picture categorization using Magnet.AI, you must manually trigger building picture comparison in your case. If you add more evidence to your case, you must build picture comparison again for new picture files to be included in similar picture searches. Magnet.AI will only analyze the new picture files.

To build picture comparison, in AXIOM Examine, on the **Tools** menu, click **Build picture comparison**.

Picture comparison will build in the background while you continue working in your case.

Build picture comparison automatically

You can set picture comparison to build automatically after you process your case.

1. In AXIOM Process, under Processing details, click **Analyze pictures with Magnet.AI**.
2. Under **Build picture comparison**, select the checkbox.

3. Continue setting up your case.

If you turn on this setting using either method, it will remain on for the next case unless you clear it again.

Find similar pictures

After you've built comparison for the pictures in your case, you can select a reference picture that you want to find similar pictures for. You can either select a reference picture from your case, or you can import an external picture.

> Note: Magnet.AI will search all uncorrupted picture files in your case. However, if the case contains more than 10,000 pictures, AXIOM Examine can only show a maximum of 10,000 of the most similar pictures in the search results.

Find similar pictures using a picture in your case

You can select a reference picture from your case or import an external picture. Select a picture from the Media explorer, or from the Artifacts or File system explorer in Row, Column, Classic, or Thumbnail view.

1. In AXIOM Examine, select a picture.
2. In the **Preview** window, click **Find similar pictures**.

Find similar pictures using an imported picture

You can import an external picture to use as a reference picture. Pictures that you import are not added to the case as evidence.

1. In AXIOM Examine, right-click a picture.
2. Click **Find similar pictures** > **Import picture**.
3. Select the picture file you want to import, and then click **Open**.
4. In the **Confirm selected picture** dialog, click **Okay**.

View similar pictures

If you found similar pictures from the Media explorer, you can view the matching results in the Media explorer. If you found similar pictures from the Artifacts or File system explorer, you can view the matching results in the Thumbnail view of the Artifacts explorer. AXIOM Examine automatically sorts the results from most similar to least similar.

Matching results are sorted from most similar to least similar in the Media explorer and in Thumbnail view only. If you examine the matching results in another view, the results will not be sorted. If you return to the Media explorer or Thumbnail view, the matching results will be sorted if you haven't removed the Similar pictures filter.

Select the number of pictures to show

After AXIOM Examine finds similar pictures, you can select the number of search results to show, up to a maximum of 10,000 pictures.

1. On the filters bar, click **Similar pictures**.
2. In the Similar pictures filter box, in the **Pictures to show** number box, use the arrows to increase or decrease the number. Or, enter a number.
3. Click **Okay**.

Add CPS data to a case

In AXIOM Process: Click **Processing details** > **Add CPS data to search** > **Add CPS export file**.

In AXIOM Examine: Click **Process** > **Add CPS export file**.

Note: To help streamline investigations, this feature is unavailable for AXIOM Cyber users by default. To use this feature, you must first Customize log collection and diagnostics.

To help protect children that are targeted by suspects using the internet, the Child Rescue Coalition's Child Protection System (CPS) collects online data that tracks person-to-person activity such as IP addresses, file hashes, person-to-person user GUIDs, and more.

You can include CPS evidence in your search in AXIOM Process or add evidence from the CPS to your case in AXIOM Examine.

Search for evidence that matches data from the CPS

You can add evidence from the CPS to your case by importing the .csv files into AXIOM Process. Once you import the .csv file into AXIOM Process and process your case, Magnet AXIOM automatically identifies and tags evidence in your case that matches data in the CPS export.

After processing is complete, AXIOM Examine tags the matching data in the Artifacts and File system explorers.

Search with YARA rules

Note: This feature is only available for AXIOM Cyber users.

Use YARA rules, to identify matching files in an image. One or more rules make up a rule set. A rule set is stored in a YARA file. Rules can be public or private.

When performing a search, AXIOM Process searches against all rules in the rule set. AXIOM Process displays results against the overall public rule. There is no limit to the number of rule sets you can apply to a scan. However, be aware that your scan times might increase with the number of rule sets you apply to your scan.

Manage YARA rules

You can use any of the rule sets included in AXIOM Process or you can import or manually create your own rule sets. Rule sets must be compatible with YARA 4.0.2. Imported or manually created rule sets are validated only when you add them to the search.

Updates to YARA rules

When the included rule sets have an update, they will be included with the AXIOM release. AXIOM will add new rules, remove deprecated rules, recreate previously deleted rules, and any modified YARA rules will be reset to the original or latest version. You can add any removed deprecated rules back into AXIOM from saved directories or as individual imports.

Use YARA rules from YARA files

You can add your own YARA files from saved directories, Git repositories, or as individual imports.

Sync folders with YARA rules

To add your own rule sets from saved directories, you can declare one or more folders where your YARA rule sets are stored. AXIOM Process will identify any .yar or .yara files in these folders, and any subfolders, and make the rule sets from these folders available for use when processing evidence. Should you update the files in the saved directories, navigate away from the screen and then return to the YARA rules screen to display the updated content. The default location for YARA rules is \Magnet Forensics\Magnet AXIOM\YARA\.

1. Open AXIOM Process.
2. Select **Processing Details**.
3. Select **Search with YARA rules**.
4. Next to Reading rule sets from synced folder, click **Edit**.
5. Under YARA rule folder(s), select **Add a new location**.
6. Click **Browse** and select where your YARA rules are stored.
7. Add new locations as needed.

Upload YARA rules

You can upload a rule set in a YARA file from anywhere on your workstation. When you upload a YARA file, the file is imported into one of the declared sync folders.

1. Open AXIOM Process.
2. Select **Processing Details**.
3. Select **Search with YARA rules**.
4. Select **Add new rule set**.
5. Select **Upload a .yar or .yara file**.
6. Set the **Location** where the uploaded YARA file will be imported to.
7. Click **Add new rule set**.

Your YARA file now appears in the list of rule sets and the contents are stored in the synced folder.

Git repository

Use a Git repository to add YARA rules to AXIOM Process.

1. Open AXIOM Process.
2. Select **Processing Details**.
3. Select **Search with YARA rules**.
4. Select **Add new rule set**.
5. Select **Git repository**.
6. Provide a valid root directory of a **Git URL** repository to add. AXIOM Process will raise a warning if the provided Git URL is not a root directory. Any YARA rules found at the specified root directory or sub directories will be added.
7. Click **Add new rule set**.

Once added, the YARA rules found at the specified Git URL will be listed. Select **Sync GIT repositories** to pull and update all YARA rule sets from the Git repositories. The **Location** where the uploaded YARA files will be imported to is not configurable.

Manually create a YARA rule set

Manually created rule sets can be saved to any of the directories you have declared for your YARA rules. If you have not saved any directories, your new YARA rule set will be saved to the default location.

1. Open AXIOM Process.
2. Select **Processing details**.
3. Select **Search with YARA rules**.
4. Select **Add new rule set**.
5. Select **Manually enter YARA rule set**.
6. Provide a unique name for the rule set.
7. Enter the rule set content.
8. Set the **Location** where the rule set should be stored.

Find more artifacts

Use the Dynamic App Finder

During a search, AXIOM Process might discover SQLite databases for applications that aren’t currently supported by AXIOM Process. You can configure AXIOM Process to extract data from these databases. For more information about creating custom artifacts from SQLite database hits, sign in to the Support Portal read the following article: Creating custom artifacts from SQLite database hits.

When you enable the Dynamic App Finder, AXIOM Process looks for databases that contain certain types of data (conversations, geolocation data, website URLs, and person identifiers).

> Warning: Turning this feature on can increase search times significantly.

1. In AXIOM Process, click **Processing details** > **Find more artifacts**.
2. Select the **Allow AXIOM to search for more artifacts** option.
3. Continue setting up your case.

After the search completes, you can view and configure the recovered artifacts in AXIOM Process on the Customize artifacts screen.

Search for custom file types

During a search, AXIOM Process might discover file types that aren't currently supported by AXIOM artifacts. You can use the Custom file types list to configure AXIOM Process to create artifacts for these file types. Magnet Forensics provides several file types to get you started, and you can add your own custom file types.

If AXIOM Process recovers any custom file types, AXIOM Examine displays the hits in the Artifacts explorer under the category heading you configured in the Custom file types list. AXIOM Process does not index or search file type artifact hits that it discovers–you should review hits for file type artifacts manually.

You can change where the Custom file type list is saved. You can also add more file types and choose which file types you want AXIOM Process to search for.

Warning: Turning this feature on can increase search times significantly.

Add custom file types

Add file types to the Custom file types list so that AXIOM Process creates artifact hits for file types discovered during a search. After AXIOM Process completes its search, you can view recovered custom file type artifacts in AXIOM Examine. You must have Microsoft Excel or an equivalent application installed on your computer to open the Custom file type list.

Warning: Only one person can open the Custom file type list at a time. If the list is saved to a shared network, you must close the list on your computer before anyone else can open it.

1. In AXIOM Process, click **Processing details** > **Find more artifacts**.
2. Under **Edit custom file types**, click **Edit custom file types list**. AXIOM Process opens the file in your default spreadsheet application.
3. In the Custom file type list, add your file types. The file includes instructions about what data you should include. Review the Custom file type list fields topic for more information about each column in the spreadsheet.

4. Save and close the document.
5. To load the new file types in AXIOM Process, under **Find more artifacts** > **Edit custom file types**, click **Refresh**.

Turn off searching for specific file types

You can turn off searching for file type categories or specific file type artifacts. If you turn off a category, AXIOM Process won't search for any of the file types grouped in the category.

1. In AXIOM Process, click **Artifact details**.
2. Depending on what platform you specified for your custom artifact, click **Customize computer artifacts**, **Customize mobile artifacts**, or **Customize cloud artifacts**.
3. On the **Select artifacts to include in case** screen, select the appropriate **Cateogory**.
4. Clear the check box for any specific custom artifacts.
5. Continue setting up your case.

Custom file types list fields

Column name	Description
Category	Choose an artifact category from the options provided. These categories correspond to the artifact categories available in AXIOM Examine. The category you choose determines where the file type artifact will appear in the Artifacts explorer in AXIOM Examine. You can't enter your own category name.
Name	Enter the name of the file type artifact, as you want it to appear in AXIOM Examine. To search for multiple headers and/or footers for the same file type, enter the file type multiple times in the list using the same Category and Name. AXIOM Examine will display hits for the file type as a single artifact. Note: AXIOM Process will not process custom file type artifacts that have the same name as artifacts already supported by AXIOM artifacts.

Column name	Description
Description	A description of the custom file type you're searching for. Providing a description is helpful to other examiners who might be using the Custom file types list.
Extensions	To identify files by their file extension, or parse, enter one or more file extensions. To enter multiple extensions, separate each value by a semi-colon. File extensions are not case sensitive and you can include or exclude a period.
Header	To identify files by their binary content, or carve, enter the hexidecimal byte header. Enter each byte as "\x" followed by the two-character hex header value. Specifying a header can improve the search performance of AXIOM Process because the software knows where to search. Warning: If you type a common header such as "OO" or "F", search times increase significantly. You can enter a header value with or without providing a footer value. Depending on whether you specify just a header, just a footer, or both, AXIOM Process searches the file differently. For more information, see Searching for headers and footers in custom file types.
Header offset	If the file's header does not occur at the beginning of a file, enter the header offset. The header offset is expressed as a numeric value greater than zero. This is an optional value. If you do not provide a value, the header offset is assumed to be zero.
Footer	To identify files by their binary content, or carve, enter the hexidecimal byte footer. Enter each byte as "\x" followed by the two-character hex header value. Specifying a footer can improve the search performance of AXIOM Process because the software knows where to search.

Column name	Description
	You can enter a footer value with or without providing a header value. Depending on whether you specify just a header, just a footer, or both, AXIOM Process searches the file differently. For more information, see Searching for headers and footers in custom file types.
Footer offset	If the file's footer does not occur at the end of a file, enter the footer offset. The footer offset is expressed as a numeric value greater than zero. This is an optional value. If you do not provide a value, the footer offset is assumed to be zero.
Maximum size of data to carve	In bytes, specify the maximum amount of data that you want to carve, beginning from the header offset, for a particular file type artifact hit. The maximum size of data to carve is expressed as a numeric value greater than zero. This is an optional value. If you don't provide a value, AXIOM Process will carve 1 KB of data. If you specify a maximum of 0 bytes to carve and turn on the Remove duplicates setting, AXIOM Examine will display a single artifact hit if the header signature is located in multiple locations in the file. Depending on whether you specify just a maximum file size, AXIOM Process searches the file differently. For more information, see Searching for headers and footers in custom file types.

Search for headers and footers in custom file types

Depending on whether you specify just a header, just a footer, or both, Magnet AXIOM searches the file differently.

Header	Footer	Result
Yes	No	If you specify a maximum size of data to carve, AXIOM Process saves data from the beginning of the file to the number of bytes you specify.

Header	Footer	Result
		If you do not specify a maximum size, AXIOM Process saves data from the beginning of the file to up to 1 KB of data.
No	Yes	AXIOM Process saves only the footer data you specify.
Yes	Yes	AXIOM Process saves the file data from the header you specify to the footer you specify. If you specify a maximum size of data to carve, AXIOM Process saves data from the beginning of the file to the footer you specify. If you do not specify a maximum size, AXIOM Process saves data from the beginning of the file to up to 1 KB of data.

Change the location of the Custom file types list

You can move the Custom file types list to another location, such as a shared network to easily collaborate with other examiners.

1. In AXIOM Process, click **Processing details** > **Find more artifacts**.
2. Under **Custom file types list location**, click **Change location**.
3. Browse to the location you want to save the custom file type list to.
4. Click **Okay**.

SELECT ARTIFACTS TO INCLUDE IN A SEARCH

Depending on your evidence sources and the type of license that you have, you might be able to search for computer artifacts, mobile artifacts, cloud artifacts, or a combination. If you've added custom artifacts in AXIOM Process or turned on searching for custom file type artifacts, you can also search for custom artifacts.

> Note: Certain artifacts depend on Windows components to recognize artifact hits. If Windows updates are applied to your Forensic workstation you might see hit count differences when scanning previously processed evidence using the same version of AXIOM Process.

Select artifacts to include in your search

By default, AXIOM Process includes all available artifacts for your evidence sources in a search. You can select the specific artifacts or artifact categories that you want to include or exclude from your search.

1. In AXIOM Process, click **Artifact Details**.
2. Click **Customize computer artifacts**, **Customize mobile artifacts**, or **Customize cloud artifacts**.
3. Select the specific artifacts or artifact categories that you want to include in your search.
4. If necessary, configure the options for the artifacts that you want to include in your search.
5. Continue setting up your case.

Search for custom artifact

You can search for custom artifacts if you've loaded custom artifacts in AXIOM Process or turned on searching for custom file type artifacts.

For more information about searching for custom artifacts, see Searching for custom artifacts.

Decrypt artifacts

For some artifacts, you can provide potential passwords or decryption keys to try to decrypt the user's account or data.

If this option is available for a specific artifact, you'll find an **Options** link below the artifact name with the ability to provide a password or decryption key.

Configure media artifact options

Save picture attachments to the case

By default, AXIOM Process accesses picture attachments from the original source, rather than copy and save the pictures to the case folder. This behavior saves storage space in your case file, but requires that you have constant access to the evidence source to view the attachments while you work on your case. If the evidence source needs to be mounted (for example, with a volume shadow copy), if you plan on creating a portable case, or if you aren't concerned about storage space and longer processing times, you can turn off this setting.

If you choose to save picture attachments to your case, your case folder size can increase. The pictures will be saved to the attachments database in your case folder.

> Note: .tiff, .raw, and .3fr files, as well as carved pictures and thumbnails are saved to the case regardless of this setting.

1. In AXIOM Process, click **Artifact details** > **Computer or Mobile artifacts** > **Media**.
2. Under the **Pictures** artifact, click **Options**.

3. Clear the **Access pictures from the source (do not save to case)** option, and then click **Okay**.
4. Continue setting up your case.

Extract EXIF data from pictures

By default, AXIOM Process extracts EXIF (Exchangeable Image File Format) data from picture artifacts such as GPS longitude and latitude, original size, software, and more. You can use this data in AXIOM Examine in several ways such as filtering evidence or in the World map view (which plots all Google Maps, Google Maps Tiles, geo-enabled apps, and picture coordinates from EXIF data on a world map).

1. In AXIOM Process, click **Artifact details** > **Computer or Mobile artifacts** > **Media**.
2. Under the **Pictures** artifact, click **Options**.
3. Select or clear the **Extract EXIF data** option, and then click **Okay**.
4. Continue setting up your case.

Detect skin tone in pictures and videos

By default, AXIOM Process uses a skin tone detection algorithm to detect skin tone in picture, video, and carved video artifacts to help identify explicit content. For video artifacts, skin tone detection is limited to the still frames captured from the video.

1. In AXIOM Process, click **Artifact details** > **Computer or Mobile artifacts** > **Media**.
2. Under the **Pictures or Videos** artifact, click **Options**.
3. Select or clear the **Detect skin tone** option, and then click **Okay**.
4. Continue setting up your case.

When AXIOM Process finishes searching the evidence, you can filter evidence in the case by skin tone percentage in AXIOM Examine.

Set the maximum dimensions for saved pictures

To help save storage space in your case file, you can set a maximum width or height for saved pictures (while preserving the aspect ratio of the picture).

1. In AXIOM Process, click **Artifact details** > **Computer or Mobile artifacts** > **Media**.
2. Under the **Pictures or Videos** artifact, click **Options**.
3. Select the **Resize to a maximum width/height of** option and specify the maximum dimension (in pixels), and then click **Okay**.
4. Continue setting up your case.

Create video previews using still frames

You can configure AXIOM Process to create a preview of video files using still frames (static images taken from the video). If enabled, AXIOM Process will attempt to capture up to 10 still frames evenly spaced throughout the video. You can view the previews of video artifacts in AXIOM Examine.

1. In AXIOM Process, click **Artifact details** > **Computer or Mobile artifacts** > **Media**.
2. Under the **Pictures or Videos** artifact, click **Options**.
3. Select the **Create a preview using still frames** option.
4. Click **Okay**.
5. Continue setting up your case.

Save videos to your case

By default, AXIOM Process saves a thumbnail picture for the videos it recovers, not the full content. If you have access to the source image, you can always export the full content of the video even if you set AXIOM Process to save only thumbnail pictures, or, if you don't have enough space for the video files in the location where your case is saved. You can still stream the videos in AXIOM Examine. If you want AXIOM Process to include the full content of the videos it discovers, you can enable the option to save videos to your case.

If you choose to save video attachments to your case, your case folder size can increase. The videos will be saved to the attachments database in your case folder.

Note: If the evidence in your case is from a VSC or ISO image, you must save the video to your case to get a preview of the video in the case. Consider exporting VSC and ISO images and processing them separately from the rest of your evidence.

1. In AXIOM Process, click **Artifact details** > **Computer or Mobile artifacts** > **Media**.
2. Under the **Videos** artifact, click **Options**.
3. Select the **Save videos up to** option and specify the maximum size for the videos. The default maximum size is 500 MB.
4. Click **Okay**.
5. Continue setting up your case.

Customize the maximum size of saved carved videos

AXIOM Process saves carved videos to your case. You can customize the maximum length of carved videos that you want to recover.

1. In AXIOM Process, click **Artifact details** > **Computer or Mobile artifacts** > **Media**.
2. Under the **Videos** artifact, click **Options**.
3. In the **Carved video size** field, specify the size of carved videos that you want to save. The default size is 20 MB.
4. Click **Okay**.
5. Continue setting up your case.

Manage artifact profiles

If you search for similar sets of artifacts regularly, you can create artifact profiles to help save you time when setting up your case. You can share the profiles you create with other examiners, and import profiles created by others.

Create an artifact profile

By default, AXIOM Process searches for all applicable artifacts each time you create a case. You can create your own custom artifact profiles to search for specific artifacts or artifact categories of your choosing. Creating custom artifact profiles can be particularly helpful if you regularly search for similar artifacts or artifact categories.

1. In AXIOM Process, click **Artifact Details**.
2. For each of **Computer artifacts**, **Mobile artifacts**, and **Cloud artifacts**, select the artifacts you want to include in the artifact profile.
3. Click **Profile options** > **Save profile as**.
4. In the **Save profile as** field, provide a name for your artifact profile.
5. Click **Okay**.

Update an artifact profile

You can add or remove artifacts from your artifact profile after you've created it.

1. In AXIOM Process, click **Artifact Details**.
2. For each of **Computer artifacts**, **Mobile artifacts**, and **Cloud artifacts**, select the artifacts you want to include in the artifact profile.
3. From the **Profile** drop-down, select the artifact profile you want to update.
4. Click **Profile options** > **Save profile**.

Import an artifact profile

You can import artifact profiles created by other examiners into AXIOM Process.

1. In AXIOM Process, click **Artifact Details**.
2. Click **Customize computer artifacts**, **Customize mobile artifacts**, or **Customize cloud artifacts**.
3. On the artifacts page, click **Profile options** > **Import profile**.

4. Browse to the location of the profile that you want to import.
5. Select the profile, and then click **Open**.

You can now find your imported artifact profile in the **Profile** drop-down list.

Export an artifact profile

You can share artifact profiles that you've created with other examiners by exporting the profile from AXIOM Process.

1. In AXIOM Process, click **Artifact Details**.
2. Click **Customize computer artifacts**, **Customize mobile artifacts**, or **Customize cloud artifacts**.
3. On the artifacts page, click **Profile options** > **Export profile**.
4. Browse to where you want to save the profile and click **Save**.

Set a default artifact profile

By default, AXIOM Process searches for all applicable artifacts each time you create a case using the artifact profile *All artifacts*. You can set a default artifact profile so that AXIOM Process automatically selects a specific group of artifacts to search when you create a case and load your evidence.

1. In AXIOM Process, click **Artifact Details**.
2. Click **Customize computer artifacts**, **Customize mobile artifacts**, or **Customize cloud artifacts**.
3. From the **Profile** drop-down, choose the artifact profile you want to set as the default selection.
4. Click **Profile options** > **Set as default**.

Rename an artifact profile

1. In AXIOM Process, click **Artifact Details**.
2. Click **Customize computer artifacts**, **Customize mobile artifacts**, or **Customize cloud artifacts**.
3. From the **Profile** drop-down, choose the artifact profile you want to rename.
4. Click **Profile options** > **Rename profile**.
5. In the **New name** field, provide the new name for the profile.
6. Click **Okay**.

Delete an artifact profile

1. In AXIOM Process, click **Artifact Details**.
2. Click **Customize computer artifacts**, **Customize mobile artifacts**, or **Customize cloud artifacts**.
3. From the **Profile** drop-down, select the artifact profile you want to update.
4. Click **Profile options** > **Delete profile**.

Parse and carve artifacts

By default, AXIOM Process will parse and carve for all the artifacts you have selected. On the initial search you also have the option to only parse artifacts. If necessary, you can later carve the same artifacts.

Parse and carve selected artifacts

This option takes the most time but will gather the most information from the file system and unallocated space. To maximize the data returned, most artifacts have a carving component included.

Only parse selected artifacts

This option will shorten processing time, but some items embedded within files or unallocated space will be missed. If you choose to only parse artifacts, you can carve the same artifacts later.

Reprocess artifacts with carving

Evidence sources that were selected to be parsed can be reprocessed using carving.

> Note: Only those artifacts that were initially parsed can be reprocessed with carving. You cannot modify which artifacts are reprocessed with carving.

Carve parsed artifacts

1. In AXIOM Examine, select **Process** > **Reprocess artifacts with carving**. If the evidence sources have already been carved, **Reprocess artifacts with carving** will be unavailable.
2. AXIOM Process will open. You have the option to skip this notification for future reprocessing.
3. At the Case Details home screen, select **Evidence Sources**.
4. Select a row in the table to choose the evidence source to be reprocessed with carving.
5. Select **Go to artifact details**, and then view which artifacts will be carved in each of the **Artifact Details**.

   > Note: When reprocessing artifacts with carving, the option to **Carve parsed artifacts** is auto selected and cannot be changed.

6. Select **Analyze evidence**.
7. Once complete, continue reviewing the evidence in AXIOM Examine.

Learn more about parsing and carving in AXIOM

- To learn more about the difference between parsing and carving, sign in to the Support Portal to read the article Understanding parsing and carving.
- To learn which artifacts are recovered using carving only, open the Artifact Reference Guide by clicking **Help** > **Documentation** > **Artifact Reference**. Go to **Learn more about artifacts** > **Recovered artifacts by carving only**.

Privileged content

AXIOM Process: Click **Artifact details** > **Privileged content**

Privileged content

Evidence sources often contain information that you as an investigator are not permitted to view. Evidence sources may also include artifacts that require reviewing to be deemed as privileged.

When you need to manage privileged content in your case, you can use privileged content lists to exclude matches from the Artifacts explorer, or to tag artifacts for review in AXIOM Examine.

Privileged content lists perform searches on artifacts only. Search results are limited to the artifacts that AXIOM Process supports but hits are found quickly.

To begin filtering privileged content, check **Identify/remove privileged content in the case**.

Exclude privileged content in the case

This option is selected by default and will exclude all matches from appearing in the Artifacts explorer in your case.

Matches will also be excluded from the Artifacts explorer if they contain a privileged content keyword match in the file path and have a hash match using **Tag known files with matching hash values**. See Calculate hash values and find matches for more information about using hash lists for known files.

Note: The data is still present in the case and available through the File system explorer.

Tag privileged content for review in AXIOM Examine

This option will tag matching artifacts in AXIOM Examine without excluding results.

The default tag value for each privileged content list is *Privileged content*. You can provide a custom tag value for each privileged content list or reuse an existing tag. Privileged content tag values can not be empty or match an existing system tag (for example, *Evidence*, *Of interest*, *Bookmark*).

Once the search is complete, the privileged content tag is available in the Tags and Comments filter bar in AXIOM Examine. You can manage the privileged content tags in AXIOM Examine as you would any other tag. See Add a tag or comment to evidence for more information.

Privileged content lists

The requirements and recommendations of creating privileged content lists are identical to keyword lists. You can use keywords and regular expressions in your privileged content lists.

Format your privileged content list

- Must be a.kws or .txt file.
- Each search term must appear on a new line.
- A single file can contain both keywords and regular expressions.
- A keyword list that contains ASCII characters defaults to the ASCII encoding type.
- If a keyword list contains non-ASCII characters, only non-ASCII characters are encoded as UTF-8.
- Limit the size of your keyword list to 30 entries to reduce processing time.
- Avoid using keywords with fewer than 3 characters to avoid irrelevant matches being found in your case.

Regex

A regular expression is a pattern that you define using a sequence of letters, numbers, and special characters. AXIOM Process and AXIOM Examine support the .NET Framework syntax for creating regular expressions. For more information about using regular expressions in AXIOM, sign in to the support portal to read the following article: Add regular expressions to search in Magnet AXIOM.

Add privileged content list

Privileged content keywords

For each entry in the privileged content lists, indicate if the value is a keyword or Regex/GREP search. For more information about using regular expressions, log on the Customer Portal to read the following article: Add regular expressions to search in Magnet AXIOM

View results in Case information

Upon successful completion of a search, the privileged content filtering options can be viewed in the Case information file from AXIOM Examine. On the Case dashboard, under Case overview, scroll down to Case information. Click **Open case information file**.

When processing the case with the Exclude privileged content in the case option, the case information will include the privileged content keywords and the counts of excluded artifacts for each. Once an artifact is excluded by a keyword match, it will not be searched for further privileged content keywords.

For example, if an artifact contains matches for two keywords (*keyword1, keyword2*), the Case information will indicate a count of 1 for *keyword1* and 0 for *keyword2* since the artifact was excluded by *keyword1*.

Date range filter

By default, AXIOM Process does not restrict artifact hits to a specific date range, and artifacts without a time stamp will be included in the case.

Date range filter

> Note: The date range filter only works for evidence that contains a UTC time stamp. Local time behaves like a string rather than a time stamp, so artifacts with local times will not appear in the results even if their time stamp matches the selected time period. To learn more about the behavior of local and UTC time stamps, see Understanding sorting and filtering for artifacts with local time stamps.

Features such as Magnet.AI and Media Categorization rely on the artifacts being created within the Artifact explorer. Files such as Media could be missed by these features if they are not within the filtered date range.

Applying a date range affects all evidence explorers and views with the exception of the File system and Registry explorers.

As artifacts can have multiple date values, only one date value must be within the range to be included. For example, an artifact can have a created date value outside of the date range, but if it has a modified date value that is within the date range, it will be included. When applying a date range you can also choose to exclude artifacts hits that do not include a time stamp.

1. In AXIOM Process click **Artifact details** > **Date range filter**.
2. Select the **Date range** you want to filter by.
3. Leave the checkbox selected if you want to include artifacts hits that do not include a time stamp.
4. Continue setting up your case.

ADD CUSTOM ARTIFACTS

With the frequency that new applications and services are released to the market, custom artifacts can help you keep up to date with artifacts that might not be supported by AXIOM Process. In a corporate environment, you can use custom artifacts to recover data from proprietary applications. In addition to creating your own artifacts, you can browse the Artifact Exchange to search for, download, and install custom artifacts that other organizations have created and uploaded.

In addition to adding custom artifacts in AXIOM Process, you can find more artifacts by enabling the Dynamic App Finder and configuring the Custom file types list to search for artifacts that aren't currently supported by AXIOM Process.

What is a custom artifact?

A custom artifact is an XML file or a Python script that contains instructions for recovering a particular type of evidence. Typically, custom artifacts are targeted towards new applications or features that AXIOM Process does not yet support. Because custom artifacts aren't developed and maintained by Magnet Forensics, they're not required to go through the same level of testing as fully supported AXIOM Process artifacts, so they can often be developed and released faster.

Custom artifacts can contain executable code and are run in an unsandboxed Python environment with administrator privileges. Running in an environment without restrictions gives custom artifacts a lot of power and flexibility, but you must ensure that the source from where you obtain a custom artifact is trusted.

Create a custom artifact

For information about downloading, contributing, and creating your own custom artifacts, visit the Artifact Exchange.

Add custom artifacts to AXIOM Process

After you've created your own custom artifact or downloaded a custom artifact from the Artifact Exchange, you can load it into AXIOM Process.

1. In AXIOM Process, on the **Tools** menu, click **Manage custom artifacts**.
2. Click **Add new custom artifact** and browse to where you saved the artifact.
3. Select the artifact and click **Okay.**

AXIOM Process saves artifact definition templates to the *AXIOM Process/plugins* folder.

Confirm the artifact loaded correctly

1. In AXIOM Process, click **Artifact details**.
2. Depending on what platform you specified for your custom artifact, click **Customize computer artifacts**, **Customize mobile artifacts**, or **Customize cloud artifacts**. If you didn't specify a platform, the artifact is available in each option.
3. On the **Select artifacts to include in case screen**, select the **Custom artifacts** option.
4. Confirm that the custom artifacts you loaded to the plugins folder are visible.

If an artifact is not available, there might be a problem with the artifact schema. Check the log.txt file in the plugins folder for details.

When you've successfully loaded your custom artifacts in AXIOM Process, you can include them in a search.

View custom artifacts in AXIOM Examine

AXIOM Examine displays custom artifacts in the Artifacts explorer under the **Custom** heading. When you add a custom artifact to a case for the first time, they don't appear under **Evidence** if AXIOM Examine is already open. To view your custom artifacts, you must close AXIOM Examine and reopen the case.

EXAMINE EVIDENCE

To learn about examining evidence in AXIOM, select one of the topics below.

Places to start when examining evidence

Set up and customize AXIOM Examine

Adjust examining preferences

The default settings of AXIOM Examine may not work for every case. You can Adjust the appearance of your case in AXIOM Examine and Customize AXIOM Examine settings across cases.

Integrate external products and features

To enhance your use of AXIOM Examine, you can Integrate external products and features with AXIOM Examine, such as exporting directly to Magnet REVIEW or searching for hash matches with Magnet Hash Sets Manager.

How AXIOM Examine handles external links and files

Suspicious links in the evidence

By default, AXIOM prevents users from clicking on internet links that appear in an artifact's preview card, in case these links are not secure or unauthorized. If you want you or other AXIOM users on your computer to be able to access these links, you can Allow internet connection from the Preview card.

Suspicious files and scripts

Often, the evidence that you examine includes executable files or scripts (including those embedded in other artifacts such as PDF files or documents). Please note that AXIOM Examine never runs executable files or scripts contained in your evidence (whether examined from AXIOM Examine or a portable case)–including if you try to open an executable file with an external application.

Review your case based on the type of evidence you've gathered

Use specialized explorers and views to find relevant evidence, such as certain artifact categories or media with hash matches. Below are some recommendations for starting points in each explorer.

In the explorers, you can continue to narrow down to important data by filtering, searching, and categorizing evidence.

Drill down to important evidence using the case dashboard

When you first open a case in AXIOM Examine, the case dashoard displays summary information.

- If you're interested in a particular subset of data, such as an artifact category, keyword match, or media category, click the appropriate link from the Places to start column to filter on it and get a closer look.

- If you're interested in data from a particular evidence source, select it from the left navigation window to review it on its own dashboard, as well as information such as a unique device identifier and serial number.
- If you're interested in cloud-based evidence, select **Insights** from the left navigation pane and, if cloud account credentials were recovered in the evidence, you can try to Acquire more data from a cloud account.

Take an artifacts-first approach

To gain insight into your evidence using an artifacts-first approach, including viewing artifacts on a world map or reading a user's chat threads, Browse and dig deeper into artifacts.

Learn about the relationships between artifacts

To learn how artifacts relate to each other or where files originated, Discover connections.

View specific kinds of evidence in their own explorer

To view email evidence in a similar format as they would have appeared in the user's original email application, View email evidence.

To view media evidence in a thumbnail view with features for categorization, blurring or hiding explicit content, and stacking duplicate items, View media evidence in the Media explorer.

View raw file system or registry data

To view the file structure of the drive that data was acquired from, including unallocated space and volume slack, as well as raw data such as SQLite, LevelDB, or binary data, Explore the file system.

To view important information about system hardware, installed programs and settings, and user profiles, View Windows registry data.

View APFS metadata from macOS systems

Files on macOS computers can contain a number of additional attributes associated with each file on the file system. For evidence from macOS computers with APFS, you can view additional attributes from the spotlight database as well as extended attributes in the APFS metadata card. View common attributes of interest in the Artifacts explorer and a full list of available attributes in the File system explorer. For attributes that have binary information, see View raw artifact data in Text and hex.

Browse and dig deeper into artifacts

Use the *Artifacts explorer* to browse artifact groups and select the specific types of artifacts that you want to view in more detail. For example, in a corporate espionage investigation, you might want to focus your efforts on the operating system artifacts. In a fraud case, you might want to focus on email and web-related artifacts.

In the Artifacts explorer, you can also customize how evidence is displayed. There are also a number of specialized artifact views that you can use to consolidate certain types of artifacts, such as chat artifacts, media, or those with date/time or geolocation data.

To learn more about the artifacts that Magnet AXIOM can recover, see the Artifact Reference Guide.

Use refined results as a starting point

In the Artifacts explorer, in the left navigation pane, click **Refined results** and select a refined result artifact.

Use the *refined results* artifact category as a starting point when browsing artifacts in your case. AXIOM Process analyzes artifact evidence and extracts specific fragments that are commonly important in forensic examinations, then groups these fragments into themes that may help you start your investigation. For example, AXIOM identifies Google Searches in various artifacts from an evidence source, then groups them under a refined result.

From a refined result, you can browse to the parent artifact by clicking the original artifact link in Details.

To learn more about refined results, see the refined results section in the Artifact Reference Guide.

View mobile evidence

Use the mobile tab to view installed applications on a mobile device. Select an application to view a selection of its associated artifacts.

To learn more about mobile view, see View mobile evidence.

View chat threads using conversation view

In the Artifacts explorer, above the top right corner of the Evidence table, in the view drop-down list, select **Conversation view**.

Use *conversation view* to see messages as a back-and-forth dialog, in a format similar to the application that the messages are from. Conversation view displays chat messages in chronological order based on most recent chat activity.

Select a conversation to view all the individual chat messages included in that conversation, as well as details such as number of participants, display names, number of messages, and more.

Compare evidence type baselines using histogram view

In the Artifacts explorer, above the top right corner of the Evidence table, in the view drop-down list, select **Histogram view**.

Histogram view provides a graphical representation of all the results in your case for each type of artifact. Use Histogram view to build a visual baseline for your case to compare with other cases. This can help you build a profile of common investigation types and identify cases that fall outside the norm. For example, if you’re able to build a baseline of the common artifacts that are found in a case and then compare it with others, any variations that stand out might warrant further analysis.

- Click **Save as baseline** to create a baseline .ini file for comparison with later cases.
- Click **Load baseline** to open a previous baseline histogram and display it alongside the current case to identify discrepancies in the current case.

View media evidence using thumbnail view

In the Artifacts explorer, above the top right corner of the Evidence table, in the view drop-down list, select **Thumbnail view**.

Use *Thumbnail view* to view and categorize the media evidence in your case. To learn more, see Manually apply media categories to case evidence.

Tip: To view media evidence using thumbnails with more specialized features, build the Media explorer instead. To learn more, see View media evidence in the Media explorer.

Find data from a geographical location or follow a target's movement using maps and routes

In the Artifacts explorer, above the top right corner of the Evidence table, in the view drop-down list, select **World map view** or **Route view**.

World map view plots all artifacts that have geolocation data on a world map. You can view individual plotted points or clusters which appear where a large number of plotted points exist. World map view is useful if you have an idea of where an incident occurs and want to see if there are other artifact results that coincide with that location.

Route view generates a series of possible paths based on artifacts with geographical data from a particular evidence source. Use routes to follow movement of target users, for example to confirm if a suspect and victim crossed paths.

To learn more, see View evidence with geographical data.

View the source of an artifact

Use source linking to quickly view an item's original source in the file system or Windows Registry. Verify artifacts and dig deeper into the raw data where they were pulled from, such as text and hex data.

View the source of an artifact in the file system

For an artifact created from one or more files in the file system, view the original file system locations where the artifact comes from.

1. In the Artifacts explorer, select an evidence item.
2. Under Details > Evidence information, click the Source link.

Note: Some artifacts might have more than one source link, which means that the artifact is comprised of data from multiple locations.

When you click the source link, AXIOM Examine switches to the File system explorer. To learn more about examining the raw data from the file system source, see Explore the file system and View raw artifact data in Text and hex.

View registry entries for an artifact

For artifacts that are created from the Windows registry, you can view the original registry keys where the artifacts come from.

1. In the Artifacts explorer, select an evidence item.
2. Under Details > Evidence information, click the Location link.

Note: Not all artifacts have associated registry data. Some artifacts might have more than one location link, meaning that the artifact contains information from multiple registry locations.

When you click the location link, AXIOM Examine switches to the Registry explorer. To learn more about examining the raw data at the registry source, see View Windows registry data and View raw artifact data in Text and hex.

View mobile evidence

In AXIOM Examine, in the Artifacts explorer, click the **Mobile** tab. Select an app to view its associated artifacts.

Use the mobile view to filter for artifacts associated with a specific app that a user installed on their device. The mobile view shows a rebuilt version of the user's wallpaper and installed apps, including apps supported by Magnet AXIOM as well as apps that Magnet AXIOM doesn't recover apps for.

Recommendations for viewing different mobile artifacts

The following might be included under the mobile tab:

- Some artifacts and information about the app, such as settings
- Files and data whose associated apps aren't installed on the mobile device

To view data from the mobile device that might not be available in the mobile explorer, click the **Artifacts** tab and clear filters.

When you select an app, by default, AXIOM Examine only shows you key artifacts for that app, which Magnet AXIOM deems most relevant to an investigation. To show all associated artifacts instead and get a more in-depth, technical look at the user's activity, click **View options** > **Show all artifacts for app**.

Always view relevant artifacts in column view

By default, mobile view opens artifacts for the selected app in the view that best corresponds to the app. To adjust this setting and always open column view instead, click **View options** > **Always open column view**.

View evidence with geographical data

Using the world map, view clusters and individual artifacts on a map where they occurred. Using routes, follow a target's movements on a map over a specific period of time.

Before you begin

To use world map view and route view, make sure you've completed the following steps:

- Connect to the internet or an offline map server
- Build world map

Connect to the internet or an offline map server

If you have internet connection, the world map automatically connects to an online map server. If you're working on a computer without internet access, Connect to an offline map server.

Build world map

By default, world map data doesn't build when you create a case. Before you can use world map view or route view, you must first build the world map. You can configure AXIOM Examine to Build explorers automatically.

In AXIOM Examine, on the **Tools** menu, click **Build world map**.

While the world map is building, you can continue to examine your case. After you've built the initial world map, AXIOM Examine refreshes maps and routes if you add new evidence.

Find data from a geographical location using world map view

In the Artifacts explorer, above the upper-right corner of the Evidence table, in the view drop-down list, select **World map view**.

World map view plots all artifacts that have geolocation data on a world map. You can view individual plotted points or clusters which appear where a large number of plotted points exist. World map view is useful if you have an idea of where an incident occurs and want to see if there are other artifact results that coincide with that location.

- Click a pin to view basic details, including the date and time of the result.
- Click a pin and click **View details** to see the artifact details in a split screen below the world map view.
- To switch back to a full-screen map, in the upper-right corner of the map view, click the expand icon (⛶) .

Follow a target's movement using routes

Note: This feature is available for AXIOM Cyber users and AXIOM users with Essentials, Advanced, or Premier term licenses.

In the Artifacts explorer, above the upper-right corner of the Evidence table, in the view drop-down list, select **Route view**.

Routes generate a series of possible paths based on artifacts with geographical data from a particular evidence source. Use routes to follow movement of target users, for example to confirm if a suspect and victim crossed paths.

Generate routes

1. From the Artifacts explorer, in the view drop-down list, select **Route view**.
2. In the window that appears, select artifacts, evidence sources, date and time, and click **Next**.
3. Provide a distance and time interval, then click **Calculate routes**.
4. If you're satisfied with the number of routes that will be created, click **Generate routes**.

Tip: To adjust your selections later, click **Route settings**. To further narrow down your data, you can also apply additional filters from the Filters bar.

Set default route settings

For route view, you can select a default distance and time interval for generating routes.

1. In AXIOM Examine, on the **Tools** menu, click **Settings**.
2. In the Settings window, click **Maps and routes**.
3. Under **Default route distance and time**, provide a default number in each of the text boxes.
4. Click **Okay**.

Watch route playback

After you've generated routes, watch a playback of one or more routes on the map.

1. In route view, in the left navigation pane under Routes, select the routes you want to view.
2. At the bottom of the screen, select the playback speed depending on the length of the selected routes: **1x**, **10x**, or **100x**.
3. Optionally, select the tracker icon (◎) so the map automatically pans to follow the target's movement.
4. Click the play button (▶).

Record and export route playback

Record and export the animated playback of one or more routes as an MP4 file to share with stakeholders.

1. In route view, select the routes you want to export and any other playback settings you want to include in the recording.
2. Below the map, click the record button.
3. Click the play button. While the route is recording, you can adjust the settings so they change throughout the video.
4. To end the recording, click the stop button.

5. In the window that appears, to create the export, click **Okay**.
6. To review the export, browse to your case folder and open the exports folder.

Discover connections

The Connections explorer provides a visual representation of how artifact attributes in your case are related. Set the focus on an attribute of interest, like a file name, and then AXIOM Examine draws a map of connections that might otherwise be time-consuming or difficult to discover.

Build connections manually

AXIOM Examine builds connections by comparing attributes for artifact and file system items. By default, connections don't build when you create a case. You can configure AXIOM Examine to Build explorers automatically.

In AXIOM Examine, on the **Tools** menu, click **Build connections**. To view progress while connections are building, in the status bar, click **View details**.

While connections are building, you can continue to examine your case. Once you've built connections initially, AXIOM Examine refreshes the connections if you add new evidence.

Map connections for an artifact or file

In the Artifacts and File system explorers, under Details, a connections icon appears beside the attributes that you can create connections maps for. You can view connections based on different attributes of an artifact, such as hash, file name, sender, recipient, or source.

In the Details card of an artifact or file, click the connections icon . AXIOM Examine switches to the Connections explorer and creates a map with the selected item as the primary node. Use the connections map to learn how that attribute relates to other items in your case.

Navigate a connections map

Below are some tips for how to navigate a connections map. To view an example, log into the Support Portal to see the article Case study: Discovering connections in a case.

Types of nodes and connectors in a connections map

The connections map includes a series of nodes (based on artifact attributes, which provide data about the files themselves) and connectors, which indicate how files are related.

item	Description
Primary node (pink)	The anchor used to create connections. When you click the connections icon for a specific attribute, it becomes the primary node when AXIOM Examine switches to the Connections explorer. To make any node the primary node and center the map on it, double-click a node.
Direct node (blue)	An attribute with a direct connection to the primary node. To view only the connections between a primary node and a direct node, click the direct node.
Selected node (teal)	A direct node you've clicked on. The matching results refresh so you only see artifacts that contain both attributes of the primary and selected node.
Indirect node (gray)	A node that is directly related to a selected node, and indirectly related to the primary node.
Connector	A line that represents the type of connection between two nodes, such as the movement of an artifact or the action a user has taken with a file.

Find points of interest and filter a connections map

To help decide where to focus your examination, hover your mouse over a specific node's connections to view them without redrawing the map.

On the Filters bar, apply one or more filters to the connections map to refine the visible evidence.

- Use the Evidence filter to limit which evidence sources to show connections for.
- Use the Connectors filter to indicate the specific types of connections that you want to see.
- Use the Attributes filter to specify which artifact attributes to include.

View matching results for a selected node

Select a node to view all of the matching artifact results for the node as it relates back to the primary node. For example, if the primary node is a file name, the matching results show all artifacts that contain the file name. To learn more about nodes, see Types of nodes and connectors in a connections map.

Adjust the view of a connections map

Click and drag a node to reposition it.

Click the pop out icon beside the Connections drop-down list to maximize it on a separate monitor.

Save important nodes for future reference

Click and hold a node to save it as a point of reference. As you explore connections in the map, click any node in the Saved nodes bar at the top of the map to return to that view.

Export connections maps

Print or export a connections map as a PDF

If you want to include a map of connections in your report, you can print it to paper or PDF. A printed map includes the primary node and any focus nodes.

1. In AXIOM Examine, in the **Connections explorer**, right-click a node.
2. Click **Print**.
3. Follow the instructions on screen to print the map.

Export a connections map as an HTML file

If you want to include a map of connections in your HTML report, you can save the connections map as an HTML file.

1. In AXIOM Examine, in the **Connections explorer**, right-click anywhere in the map.
2. Click **View source**.
3. In the .txt file that appears, on the **File** menu, click **Save as**.
4. Browse to the location where you want to save the file.
5. Provide a **File name** ending in **.html**.
6. Click **Save**.

View email evidence

Note: This feature is only available for AXIOM Cyber users and AXIOM users with Advanced or Premier term licenses.

In AXIOM Examine, use the Email explorer to view supported email evidence all in one place, in a folder structure that mirrors the application where the data was recovered. In addition to the emails themselves, you can also view related artifacts and artifact details.

Build the Email explorer manually

AXIOM Examine builds the Email explorer using supported email evidence in your case.

On the **Tools** menu, click **Build email explorer**.

You can see the build progress in the Email explorer or the status bar. While the Email explorer is building, you can continue to browse through your case and add tags, comments, filters, and profiles.

After you've built the Email explorer initially, AXIOM Examine prompts you to rebuild the Email explorer if you add new evidence.

View data in Email explorer

The Email explorer displays email data in a way that mirrors the structure folder of the application where the evidence was recovered from, though there might be some discrepancies due to the nature of the recovered data. To learn more about these discrepancies, log in to the Support Portal to read the article Unexpected data structures in email explorer.

Tag emails and attachments in the Email explorer

In the Email explorer, you can select individual emails or attachments and add tags or comments. You can also enable AXIOM Examine to automatically tag emails and attachments together.

1. In the Email explorer, right-click the emails or attachments that you want to tag.
2. Click **Add / Remove tag**.
3. Select the tag that you want to apply.
4. In the window that appears, select either the **Tag the email and its attachments together** or **Tag the email or attachment only** option.
5. Click **Continue**.

After you apply a tag, the tag color appears beside the email artifact and, if applicable, next to its attachments in the preview window. You can change your selection later in Allow the Email explorer to tag email attachments.

View media evidence in the Media explorer

Note: To help streamline investigations, this feature is unavailable for AXIOM Cyber users by default. To use this feature, you must first Customize log collection and diagnostics.

Use the *Media explorer* to view, sort, and filter media evidence using criteria that are specific to pictures and videos.

The Media explorer *stacks* copies of the same picture or video that were found in different source locations, so you only have to view each media item once.

If AXIOM Examine finds multiple artifacts from the same media file in one source location, you can view related artifacts to see the details of each copy.

Build the Media explorer manually

By default, the Media explorer doesn't build when you create a case. You can configure AXIOM Examine to Build explorers automatically.

In AXIOM Examine, on the **Tools** menu, click **Build media explorer**.

> Note: The **Stack media items by PhotoDNA hash** option is available if you enabled PhotoDNA when you processed your case. Selecting this option will significantly increase the time it takes to build the Media explorer index.

While the Media explorer is building, you can continue to examine your case. Once you've built the Media explorer initially, AXIOM Examine refreshes the Media explorer if you add new evidence.

Tips for exploring media

Filter using media-related criteria

In addition to the regular search and filter options in AXIOM Examine, use the left navigation bar to filter media evidence. For example, if you know that certain evidence came from a particular camera, you can filter on that camera's details.

Select as many filters as you wish, then click **Apply filter** to view only the applicable media results.

Group and sort media evidence

Use the **Group by** option to organize the evidence into groups such as file extension or created date.

Use the **Sort by** option to organize the evidence in ascending or descending order based on attributes such as skin tone percentage.

Note: When you sort media evidence, any items without an applicable value will appear at the end of the sorted list. For example, if you sort by created date, and there's a picture in your case that date/time data couldn't be recovered for, it will appear at the end of the list.

Preview a video in the Media explorer

Preview a video using the thumbnail in the Media explorer.

- Scroll across a video thumbnail to view a preview of the video within the thumbnail.
- To view the video in a larger preview window, double-click the thumbnail and watch the entire video or scroll across the preview to view the video's contents.

Save your progress in the Media explorer

AXIOM Examine automatically saves your progress in the Media explorer. If you click away to another explorer and then return to the Media explorer, you will return to the last media item you selected and all your tags, filters, and settings will remain the way you left them.

Add media categories to the Media explorer

Note: The media categories you add in the Media explorer don't appear in any other explorer.

On the **Tools** menu, click **Manage media categories**. In the Media categorization lists section, you can do one of the following:

- Select an existing media categorization list from Project VIC or CAID. Select which categories to enable, then click **Okay**.
- To use another person's list or one you've created outside of AXIOM, click **Import list**. Select which categories to enable, then click **Okay**.
- To create your own list, click **Add new list**. Name and customize the list, then click **Okay**.

You can then categorize media in the Media explorer. To learn more, see Manually apply media categories to case evidence.

Deduplicate media files using stacks

The Media explorer determines which pictures or videos to stack together by comparing hashes. Stacking prevents you from having to view multiple copies of the same media item while examining evidence.

View media items and details in a stack

In the Media explorer, click the stack icon on the bottom right corner of a thumbnail to view all the items in the stack and a few basic details.

Media stack behavior when tagging and categorizing evidence

Expand the **Tags and comments** pane to apply tags and media categories. When you apply a tag or media category to a stacked picture or video, it will also be applied to all items in the stack.

Media stack behavior when grouping evidence

When you group evidence in the Media explorer, only part of a stack might be applicable to a certain group. The number of items in the stack that appear in a certain group will be visible on the stack thumbnail.

For example, if you've grouped the evidence by date/time, and one item in the stack has a time stamp on one day, and the other item in the stack has a time stamp on another day, a thumbnail will appear in each day's group. Each thumbnail notifies you that "1 out of 2" items is visible in that group.

Change media stack settings

By default, the Media explorer stacks artifacts by MD5 / SHA1 hash. In the Stack by drop-down list, select one of the following options:

- Select PhotoDNA if you selected the option to stack media by PhotoDNA. To learn more about PhotoDNA, see Find matching and similar media using AI and hashes.

- Select None to turn off stacking so that all duplicate media items are visible.

View artifacts related to a single media file

When multiple artifacts refer to the same media file, the Media explorer combines them into one media item, which prevents you from having to view the same picture or video multiple times. For example, a picture acquired from a Dropbox in the cloud will appear in both the Pictures and Cloud Dropbox Files artifacts in the Artifacts explorer.

In the Media explorer, when you click a media item, expand the Details pane. Under Related artifacts, do one of the following:

- Click an individual related artifact to filter on that artifact in the Artifacts explorer.
- Click **View related artifacts** to filter on all related artifacts in the Artifacts explorer.

Edit and export media thumbnails

In the Media explorer, you can preview and edit pictures and video thumbnails, then export them. For example, use the editing features to focus on relevant content or improve visibility.

> Note: When you edit a thumbnail, you aren't changing the picture itself, and there is no damage to the forensic integrity of the file. The changes you make to a thumbnail don't persist after you close the picture preview window.

Edit a picture thumbnail in the Media explorer

1. In the Media explorer, double-click a picture thumbnail.
2. In the preview window, edit the picture using the available settings.
3. Click **Apply**.
4. To export the picture you've just edited, click **Export**.

Edit a video thumbnail in the Media explorer

While video editing capabilities are not currently available in AXIOM Examine, you can edit the video's timelapse preview.

1. In the Media explorer, select a video thumbnail.
2. Expand the **Details** pane.
3. Click the timelapse preview under **Preview**.
4. In the preview window, edit the picture using the available settings.
5. Click **Apply**.
6. To export the picture you've just edited, click **Export**.

View evidence on a timeline

The Timeline explorer organizes artifacts and files by timestamp in an interactive graph. Use the timeline to examine specific time frames and establish spikes or patterns in activity. The timeline can be especially helpful for situations such as:

- If you know approximately when an event occurs and want to look at a user's online activity during that time
- If you've identified an important piece of evidence and want to build a story around it using results that occur before and after.

Build the timeline manually

AXIOM Examine builds the timeline using timestamped evidence from the Artifacts and File system explorers. By default, the timeline doesn't build when you create a case, but you can configure AXIOM Examine to Build explorers automatically.

In AXIOM Examine, on the **Tools** menu, click **Build timeline**.

You can see the progress while timeline is building in the Timeline explorer or the status bar, and continue to browse through your case. Once you've built the timeline initially, AXIOM Examine refreshes the timeline if you add new evidence.

Tips for navigating the timeline graph

Adjust the visible time frame

- To get a closer look at a particular time in the graph, scroll the track wheel on your mouse or toggle the Zoom option.
- To move backward or forward in time, click the graph and drag your mouse left or right. To quickly jump backward or forward in time, you can also click the left and right **Page** arrows above the graph.
- To focus the graph to a specific date range, click the calendar icon next to **Go to date** and choose your desired date range.
- To change how you view the timeline—by years, months, weeks, days, hours, or minutes—change the date type in the drop-down list above the timeline graph.

View hits for a spike of activity

- To view the date and number of hits for a spike, hover over a node in the graph.
- To analyze hits in a spike in the timeline, click a node in the timeline graph. AXIOM Examine automatically jumps to the first timestamped item for the activity spike in the evidence table below the timeline graph.

View different timestamps for one hit

Items that have multiple timestamps appear on the timeline once for each timestamp. To move between timestamps for a single hit, click the **<** or **>** icons underneath the timeline graph where the timestamps are listed, for example, **< 1 of 3 timestamps >**.

Export timeline data

To share evidence from the timeline, export it to a .csv file.

1. In AXIOM Examine, in the **Timeline explorer**, select and right-click items that you want to export.
2. Click **Create report / export**.

3. Next to the **File path** field, click **Browse** and select the location you want to save the export. Click **Select folder**.
4. Click **Create**.

Timeline categories

In addition to the listing details for below the timeline graph, the timeline also labels each item with one of the following categories.

Category	Description	Example
Account usage	Evidence of a user account or system account being accessed or used.	Login/logout Password changes
Browser usage	Evidence of the target using a browser or navigating web related activity on the computer or phone.	Browser last visit date/time Cache/cookies from browsers
Deleted file	Indicates that a file has been deleted. While the file might not be accessible any more, there is a timed record representing its deletion.	Recycle Bin deletion date/time
Device interaction	Indicates the user or system interacted with an external device that was not the computer or phone being examined.	IoT devices such as Google Home, Amazon Echo, OnStar or other cars, and more.
External device/USB usage	Evidence of a USB or other external device being connected to the system.	USB first connect date/time USB last connect date/time
File download	Indicates that a file was downloaded from an external source.	Chrome download activity

Category	Description	Example
		Skype file transfers
File knowledge	Indicates a user or system has interacted with the file in some way, but it might not be known whether the file was actually opened or not.	MAC times
File/folder opening	Evidence of a user opening a file or folder.	Jumplists Shellbags LNK files
Financial transactions	Indicates an exchange of currency or services has occurred.	Wallet transactions Samsung Pay
Network activity	A timestamp of a network action or activity that occurred on the computer or phone.	WiFi connections Authentications RDP activity
Physical location	A timestamp placing the user or device at a specific location at a given time based on GPS coordinates or a physical address.	iOS cached locations Significant locations
Program execution	Evidence of an application or program being run at a specific time.	Prefetch last run time
Social activity	Evidence of public interactions through applications or service.	Instagram posts Tweets Facebook Wall posts
User communication	Evidence of any sort of private or semi-private group chat through applications or services.	Chat messages Email Direct messages

Category	Description	Example
User event	Evidence related to an event outside the system or user's account usage.	Calendar events such as meetings or birthdays

Explore the file system

In AXIOM Examine, the *File system explorer* allows you to drill down through the file system tree of your evidence source, just like you can by using the File Explorer on your own computer. You can also use the File system explorer to view additional content such as unallocated space and volume slack.

View the source of an artifact in the file system

For artifacts that are created from one or more files in the file system, you can view the original file system locations where the artifact comes from.

1. In the Artifacts explorer, select an evidence item.
2. Under Details > Evidence information, click the Source link.

Note: Some artifacts might have more than one source link, which means that the artifact is comprised of data from multiple locations.

View artifacts associated with a file

Similar to how you can view files or registry data associated with an artifact, you can also view artifacts associated with a file.

1. In AXIOM Examine, in the **File system explorer**, right-click a file in **Evidence**.
2. Click **View related artifacts**.

View file system artifacts in an external application

You can view the contents of artifacts using external applications such as HxD, Adobe Acrobat, Google Chrome, Microsoft Word, and so on. The applications that are suggested for each artifact come from recently used Windows programs that are associated with each artifact type.

1. In AXIOM Examine, in the **File system explorer**, right-click a file in **Evidence**.
2. Click **Open with**.
3. Select the application you want to open the artifact with.
4. Click **Okay**.

Check a hashed file for viruses using VirusTotal

Note: This feature is only available for AXIOM Cyber users.

You can upload the hash of a file in your case to VirusTotal to help make informed decisions about how to handle these files on your system. VirusTotal uses antivirus scanners and URL/-domain blocklisting services to inspect files. For added security, AXIOM Examine only shares the hash of the file, rather than the file itself. VirusTotal then compares this hash to its existing records to check if the file has already been scanned for viruses.

1. In AXIOM Examine, in the File system explorer, right-click a file in **Evidence**.
2. Click **Check with VirusTotal**.
3. In the window that appears, click **Open VirusTotal**.

If a file with a matching hash has already been uploaded to VirusTotal, a table will appear with the results of the scan. If the file has not yet been uploaded, VirusTotal will open with an **Item not found** screen.

Add files from the File system explorer to the Artifacts explorer

You can add files from the File system explorer to the Artifacts explorer. Looking at all of your information in one explorer makes consolidating this information for reporting purposes easier.

1. In AXIOM Examine, in the **File system explorer**, right-click a file in **Evidence**.
2. Click **Save file as artifact**.

In the Artifacts explorer, you can see the new artifact in the Examiner defined group in Files.

Display files and folders recursively

By default, when you click a folder, the File system explorer behaves how you might expect a file system navigation tool to behave–when you click a folder, its immediate children are displayed in Evidence. However, you can change this behavior so that not only the selected folder's children are visible, but also its subfolders' children as well. This customization helps reduce the amount of clicking that you have to do to browse the file system hierarchy.

1. In AXIOM Examine, in the **File system explorer**, click the **Selected folder only** drop-down.
2. Select the **All subfolders** option.

Save files and folders

In the File system explorer, you can save files and folders locally to your computer. When you save files and folders, AXIOM Examine saves the original file along with any associated metadata.

1. In AXIOM Examine, in the **File system explorer**, right-click a file or folder in **Evidence**.
2. Click **Save file / folder to**.
3. Browse to where you want to save the file or folder and click **Select folder**.

Save databases

While a database is in use on a live system, it creates temporary files to store data. To properly save this type of database to your computer, make sure that you save the temp files in addition to the .db file. If you save only the .db file, the database appears to be empty when you open it on your computer.

To learn more about databases, see View database tables.

Create artifacts using file snippets

While using the File system explorer, you might come across important evidence that isn't already associated with an artifact. If you want to display this evidence alongside other artifacts and include it in your exports, you can save the content manually.

1. In AXIOM Examine, in the **File system explorer**, right-click a file in **Evidence**.
2. In **Text and hex** for that file, select the group of hex or text characters that you want to create an artifact for.
3. Right-click the selection and click **Display as artifact**.

The new artifact appears in the Artifacts explorer in the Examiner defined group. The Details for the new artifact lists the size of the file, the name of the analyst who added the artifact to the case, and the date that the artifact was added.

You can also create artifacts from registry data. To learn more, see Exploring the registry.

View database tables

In the File system explorer, you can view SQLite and LevelDB databases.

View SQLite databases

Note: The SQLite viewer only displays records that were live and active at the time of acquisition. Although Magnet AXIOM can recover non-live records for supported artifacts, they only appear in the Artifacts explorer, rather than the SQLite viewer.

When you examine a database in the SQLite viewer in the File system explorer, select the table in the database that you want to view from the **Select table** drop-down.

Search and filter data in the table

- Search all fields in the current table by clicking **Find** and providing a search term.

- Query the data by building and executing SQL queries directly in the SQLite viewer. Include JSON features in the query to look into JSON data within a cell and return data from inside that text block.
- Refine the data you see in the table by applying one or more filters.

Customize the view of the table

- Customize how you view data in the table by choosing which columns you want to show or hide or by reordering the columns by dragging the column headers to a new position.
- Freeze columns by dragging the vertical blue bar across the table. Columns to the left of the vertical blue bar will be visible while scrolling through the rest of the table.
- Change the encoding of a column in the table by right-clicking the column header and selecting a new encoding type.

View BLOB data

View BLOB (Binary Large Object) data by right-clicking the data and selecting one of the following options:

- To preview the BLOB data, click **View as picture**. In the previewer, you can zoom in on the picture, rotate the picture, and more.
- To view the BLOB data in an external viewer, click **Open with** and select a viewer.
- To view BLOB data in a property list (plist) viewer, right-click the data and click **View as plist**.
- To view BLOB data in a protobuf (protocol buffers) viewer, right-click the data and click **View as protobuf**.

Save and export table data

- Export the data in the table to a .csv or .xlsx file. If you apply a filter or query the data, only data currently shown in the table is included in the export.
- Copy cell data or save BLOB image data by right-clicking the data and selecting **Copy** or **Save as**.

View LevelDB databases

Note: The LevelDB viewer only displays records that were live and active at the time of acquisition. Although Magnet AXIOM can recover non-live records for supported artifacts, they only appear in the Artifacts explorer, rather than the LevelDB viewer.

When you examine a database in the LevelDB viewer in the File system explorer, select the table in the database that you want to view from the **Select table** drop-down.

Search and filter data in the table

- Search all fields in the current table by clicking **Find** and providing a search term.
- Sort and filter the data by column.

Change encoding to make text in the table readable

The LevelDB viewer displays both the raw data and encoded data in separate columns. You can also change the encoding of a column in the table by right-clicking the column header and selecting a new encoding type.

View BLOB data

View BLOB (Binary Large Object) data by right-clicking the data and selecting one of the following options:

- To preview the BLOB data, click **View as picture**. In the previewer, you can zoom in on the picture, rotate the picture, and more.
- To view the BLOB data in an external viewer, click **Open with** and select a viewer.
- To view BLOB data in a property list (plist) viewer, click **View as plist**.

Copy or save table data

Copy cell data or save BLOB image data by right-clicking the data and selecting **Copy** or **Save as**.

View Windows registry data

The Windows Registry stores important information about system hardware, installed programs and settings, and user profiles. If any of your evidence sources contain Windows registry data, AXIOM Examine links artifacts and files directly to these registry entries in the *Registry explorer*.

View registry entries for an artifact

For artifacts that are created from the Windows registry, you can view the original registry keys where the artifacts come from.

1. In the Artifacts explorer, select an evidence item.
2. Under Details > Evidence information, click the Location link.

Note: Not all artifacts have associated registry data. Some artifacts might have more than one location link, meaning that the artifact contains information from multiple registry locations.

Navigate the registry

The registry is organized in a hierarchical structure, similarly to the file system on a computer. Instead of files and folders, the registry contains hives, keys, subkeys, and registry entries.

- In the left navigation pane, you can find all the separate registry hives in the registry.
- Double-click a hive to view its keys (signified with folder icons).
- Expand a key to view its subkeys (signified with folder icons).
- If you’ve expanded multiple items and want to return to a more collapsed view, right-click an item and select the option to **Collapse the current item**, **Collapse all nested items**, or **Collapse all items in tree**.

Review a registry entry

After expanding a hive and its keys, in Evidence, click a registry entry to view its details on the right.

- Each registry entry is a name/value pair. The possible types of data for a registry value are: string, expandable string, integer, and binary.
- Registry entry information includes general information such as the registry key name and type.
- If a registry entry's name is '(default)', the entry was not renamed by the user.
- If a registry entry's data is defined as '(value not set)', the registry entry was not changed by the user.
- Evidence information includes source information and links to the hive file in the file system. To learn more, see Explore the file system.
- Depending on the type of key value, you might also be able to see text and hex data. To learn more, see View raw artifact data in Text and hex.

View raw artifact data in Text and hex

In AXIOM Examine: File system, Timeline, or Registry explorer > select item under Evidence > under Details, find Text and hex > click **Text** or **Hex**

Use *Text and hex* to view the raw data associated with a file. This view allows you to verify the results that AXIOM Examine produces and manually parse out any additional data that might not be included in the details of an artifact.

When to look at the hex source

There might be data encoded in a file, for example a picture, that cannot be parsed. In the Hex source, you can manually extract the data yourself. You can also decode the hex values into common formats, including ASCII, binary, date/time, and more.

When to look at the text view

The Text view converts underlying bytes to ASCII text, which is generally a much cleaner view for text documents and for other ASCII-based data. As an examiner, you can use this feature to verify evidence and keywords.

The default character encoding is unicode (US-ASCII), but you can select from many other character encoding types in the Encoding drop-down list.

Browse to a specific offset

If you know the offset that you want to view, you can browse to it:

1. In Text and hex view, click **Go to** and provide the offset you want to view.
2. On your keyboard, press **Enter**.

Search for a text string or hex value

1. In Text and hex view, click **Find** and provide the string or hex value you want to search for.
2. Select the search method that you want to use: **Text string** or **Hex value**.
3. On your keyboard, press **Enter**.

Decode hex values

You can decode hex values into other formats to analyze the information in that specific format.

Note: You can only decode up to 10 KB of data at one time.

1. In Hex view, click **Decode**.
2. Click and drag hex values to select them.

AXIOM Examine automatically decodes the selection and displays the information under Decode at the bottom of the Text and hex card.

View text and hex data in a protobuf viewer

View data in a protobuf (protocol buffers) viewer and navigate the data as you would when you View database tables

1. In the text or hex viewer, select the data you want to view.
2. Right-click the selected data and click **View as protobuf**.

Save or copy text or hex data

You can save or copy a selection of text or hex data for use at a later time. To save or copy the data:

1. In Text and hex view, click and drag to select text or hex values.
2. Right-click and select **Save selection** or **Copy selection.**
3. If you chose to save the hex data, browse to the location where you want to save the data.
4. Provide a file name (ending in .txt), and then click **Save**.

Create artifacts using raw data

You might come across important files or registry data that aren't already associated with an artifact. You can save this content as an artifact to review it in the Artifacts explorer and review or export it with other evidence.

1. In Text and hex view, click and drag text or hex values to select them.
2. Right-click the selection and click **Display as artifact**.
3. When the artifact has been created, click **View artifact** in the status bar to navigate to it in the Artifacts explorer.

The new artifact appears in the Artifacts explorer in the *Examiner defined* group, and includes the name of the user who created the artifact in Details.

You can also create artifacts from file snippets. To learn more, see Create artifacts using file snippets.

TAGS, COMMENTS, AND PROFILES

To learn more about tags, comments, and profiles in AXIOM Examine, select one of the topics below.

Add a tag or comment to evidence

Use tags and comments to organize your case and easily return to items of interest. Use AXIOM Examine's system tags or create your own to suit your case. After you tag evidence, you can use the Tags and comments filter to show only those items that are of interest to you.

Set up tags in your case

Create a custom tag

Create custom tags that are specific to your investigation and then apply those tags to evidence in your case.

1. In AXIOM Examine, on the **Tools** menu, click **Manage tags**.
2. Click **Add tag**.
3. In the **Enter new tag** field, type a name for the tag, and then click **Add**.
4. If you want to change the color associated with the tag, click the current color, and then choose a new color.
5. If you want to change the shortcut assigned to the tag, in the **Shortcut** drop-down list, choose a different option.
6. Click **Okay**.

Import tags

Import a list of tags to your case. Files must be .json or .txt format and each tag value must appear on its own line.

1. In AXIOM Examine, on the **Tools** menu, click **Manage tags**.
2. Click **Import tags**.
3. Browse to the .json or .txt file you want to import, and then click **Open**.
4. Optionally, customize the name, color, and shortcut for the tags.
5. Click **Okay**.

Export tags

Export your list of tags to share with other examiners. You can export your list of tags to either .json or .txt format.

1. In AXIOM Examine, on the **Tools** menu, click **Manage tags**.
2. Click **Export tags**.
3. Browse to the location where you want to save your tags and provide a name for the file.
4. From the **Save as type** drop-down, select the file format you want to use, and then click **Save**.
5. Click **Okay**.

Merge tags into the original case

After you've exported evidence for use in another Magnet Forensics tool, you can merge tags and comments from that case back into your original case. To learn more, see Merge tags and comments back into the original case.

Tag evidence

1. In AXIOM Examine, under Evidence, right-click the item or group of items that you want to tag.

2. Click **Add / Remove tag**.
3. Select the tags that you want to apply.

Tip: You can also apply tags using shortcuts. To view and change the shortcuts for each tag, click **Tools** > **Manage tags**.

Note: Tags automatically sync between artifacts and file system items, but some tags only appear in the explorer where they are applied. To learn more about the behavior of tags between explorers, log in to the Support Portal to read the article Tag syncing between explorers in AXIOM Examine.

Tag emails and attachments in the Email explorer

Note: This feature is only available for AXIOM Cyber users.

In the Email explorer, you can select individual emails or attachments and add tags or comments. You can also enable AXIOM Examine to automatically tag emails and attachments together.

1. In the Email explorer, right-click the emails or attachments that you want to tag.
2. Click **Add / Remove tag**.
3. Select the tag that you want to apply.
4. In the window that appears, select either the **Tag the email and its attachments together** or **Tag the email or attachment only** option.
5. Click **Continue**.

After you apply a tag, the tag color appears beside the email artifact and, if applicable, next to its attachments in the preview window. You can change your selection later in Allow the Email explorer to tag email attachments.

Add a comment to an item

1. In AXIOM Examine, under Evidence, select the item that you want to comment on.
2. Expand **Tags, comments & profiles**, and then click **Add comment**.
3. Type a comment and click **Okay**.

System tags

In addition to allowing you to Create a custom tag, AXIOM Examine includes a set of system tags that you can use or customize.

Tag	Default keyboard shortcut
Bookmark	Spacebar
Evidence	CTRL + 1
Of interest	CTRL + 3
Exceptions	CTRL + 4

Note: When a search completes, you can view a summary of any files that were not fully processed due to artifact timeouts. These files are tagged in AXIOM Examine with the *Exceptions* system tag. The Exceptions system tag is not included in any exports or reports.

Group identifiers to create profiles

AXIOM Examine pulls identifying information into the Identifiers and User Accounts refined results categories. When reviewing these categories, if you notice identifiers for a person of interest in your case, you can apply a profile to those identifiers.

For example, you might create a profile called *Target A* to group the various user names and phone numbers used by that person of interest. Then, you can filter evidence on the profile *Target A* to see activity related to that person.

Set up profiles in your case

Create a profile

1. In AXIOM Examine, on the **Tools** menu, click **Manage profiles**.
2. In the **Enter new profile** field, type a name for the profile, and then click **Add**.
3. Click **Okay**.

Import profiles

Import a list of profiles to your case. Files must be .json or .txt format and each profile value must appear on its own line.

1. In AXIOM Examine, on the **Tools** menu, click **Manage profiles**.
2. Click **Import profiles**.
3. Browse to the .json or .txt file you want to import, and then click **Open**.
4. Optionally, customize the profile names.
5. Click **Okay**.

Export profiles

Export your list of profiles to share with other examiners. You can export your list of profiles to either .json or .txt format.

1. In AXIOM Examine, on the **Tools** menu, click **Manage profiles**.
2. Click **Export profiles**.
3. Browse to the location where you want to save your profiles and provide a name for the file.
4. From the **Save as type** drop-down, select the file format you want to use, and then click **Save**.
5. Click **Okay**.

Apply a profile

When you apply a profile to a specific identifier or user account, AXIOM Examine also applies that profile to every artifact in the case that has that exact identifier or user account.

1. In AXIOM Examine, in the Artifacts explorer, expand the **Refined results** group, and click **Identifiers** or **User Accounts**.
2. Under Evidence, select the artifact or group of artifacts you want to apply a profile to.
3. Expand **Tags, comments & profiles**, in the **Profiles** section, select the profile that you want to associate the identifier or user account with.

SEARCH AND FILTER EVIDENCE

To learn about searching and filtering evidence in AXIOM, select one of the topics below.

Search and filter by keywords

In AXIOM Examine, you can Filter by keyword list or Search for keywords using the search bar.

Filter by keyword list

If you added keywords or keyword lists to your search in AXIOM Process, those lists and keywords appear as filtering options in AXIOM Examine.

In AXIOM Examine, on the Filters bar, click **Keyword lists** and select the keywords or keyword lists you want to filter on.

Add a keyword list

You can add keywords to a case from AXIOM Examine after it's been processed. To learn more about how to add keywords and which options to select, see Add keywords to a search.

Using AXIOM Examine while adding keywords

While processing evidence sources for keywords is in progress, you can continue working in your case, however, searching evidence for keywords can be resource intensive. Depending on your workstation, interacting with AXIOM Examine might become slower than normal while keywords finish processing.

If you stop processing keywords while AXIOM Examine is adding results from the keyword search to your case, only the partial results will be added to your case. After you stop processing, AXIOM Examine will add the partial results to the search index and keyword list filter, which might take some time.

Search for keywords using the search bar

In addition to adding keywords and keyword lists to your case, you can type keywords and search terms into the search bar.

AXIOM Examine filters on matching results and highlights matching text in Evidence and Details.

How search results differ between explorers

Depending on the explorer where you use the search bar, AXIOM Examine searches the evidence differently.

Explorer	Search criteria
Artifacts, Media, and Timeline explorers	• Searches all fragments except for date and time fragments • Searches content of media and documents
File system explorer	• Searches file paths • Does not search content of files
Registry explorer	• Searches keys, values, and data • Use an advanced search to adjust this criteria

Search for keywords using advanced search options

On the Filters bar, click **Advanced** to add more keywords and criteria to a search. Select **Search terms** and use the following options for each search term as needed.

- Select whether you want to **include** or **exclude** the search term.
- To search for the term if it appears near another word or set of characters, select **Is located near another term** and provide the details for the secondary term.

- To search for the whole word rather than partial instances, select **Find whole word only**.
- To search for instances of the word with the same letter case, select **Match case**.

AXIOM Examine filters on matching results and highlights matching text in Evidence and Details.

Search by regular expression

On the Filters bar, click **Advanced** and select **Regex pattern matching** to search your evidence using regular expressions.

A regular expression is a pattern that you define using a sequence of letters, numbers, and special characters. AXIOM Process and AXIOM Examine support the .NET Framework syntax for creating regular expressions. For more information about using regular expressions in AXIOM, sign in to the support portal to read the following article: Add regular expressions to search in Magnet AXIOM.

Search by keyword snippet

You can filter by keyword snippets to see all of the evidence—not just artifacts—that contains a specific keyword. If you turned on keyword search for all content when you set up your case in AXIOM Process, any keyword with a result appears in Keyword snippets.

In the Artifacts explorer, in the left navigation pane, expand the **Keyword snippets** artifact category and select a keyword to filter on the results.

To provide additional context, the keyword snippet includes the 50 bytes that appear before and after the keyword. For more detailed information about a specific keyword result, click the source link to go to the original file.

Remove keywords from a case

If you no longer want to include certain keywords or keyword lists in a case, delete them using the manage keywords wizard.

Note: You can delete an entire keyword list, or a manually entered keyword. You cannot delete an individual keyword from a keyword list. Additionally, any Keyword Snippets artifacts will not be deleted even if the associated keyword list is deleted.

1. In AXIOM Examine, click **Tools** > **Manage keywords**.
2. Delete keyword lists, keywords, or both.
   - Under Keyword lists, hover the mouse over the list you want to delete, then click the garbage can icon on the right side of the table.
   - Under Keywords, hover the mouse over the individual keyword you want to delete, then click the garbage can icon on the right side of the table.
3. Click **Okay**.

Filter by criteria in the evidence

Use the Filters bar to choose which results you want to display. You can apply multiple filters at once to further refine the visible data, and Save filter sets.

To return to the view of all case evidence, click **Clear filters**.

Filter by accessible and inaccessible files

Use the Content types filter to discover which files are considered to be accessible to users and which ones aren't. The filter option only appears if there are **Items inaccessible by users** in the evidence that you are examining.

1. In the Artifacts explorer, on the Filters bar, click **Content types**.
2. Select the **Items accessible by users** or **Items inaccessible by users** option.

Items inaccessible by users

Magnet AXIOM considers files to be **Items inaccessible by users** if they can't be accessed without the use of special recovery or carving tools. These files are recovered from the following locations:

- pagefile.sys
- hiberfil.sys
- swapfile.sys
- $Mft
- $MftMirr
- $Logfile
- $Volume
- $AttrDef
- $Bitmap
- $Boot
- $BadClus
- $Secure
- $Upcase
- $Extend
- Unallocated space
- Unpartitioned space
- File slack
- Uninitialized file area
- Orphaned files
- Overwritten files
- Deleted files

Items accessible by users

Magnet AXIOM considers files to be **Items accessible by users** if they were recovered, either through parsing or carving, from all other locations.

Filter by date and time

Search for evidence during a specific date and time using the absolute date/time filter, or search for evidence around a certain time using the relative/date time filter. The date/time filter is inclusive of the dates and times you've selected.

Note: The date and time filter only works for evidence that contains a UTC time stamp, rather than a local time stamp. Because local time behaves like a string rather than a time stamp, artifacts with local times will not appear in the results even if their time stamp matches the selected time period. To learn more about the behavior of local and UTC time stamps, sign in to the Support Portal to read the article Understanding sorting and filtering for artifacts with local time stamps.

Filter evidence by a specific date or time

View evidence within a specific range of dates and times such as before a date, on a specific day of the week, in a custom time range, and more.

1. On the **Filters** bar, click **Date and time**.
2. Click **Absolute date/time**.

3. Set the **date range** and/or **time range** you want to filter by.
4. Click **Okay**.

Filter on evidence from around the same time as an artifact or file

When you've found evidence relevant to your investigation, you can use the Relative date/time filter to view evidence that might have occurred around the same time.

1. On the **Filters** bar, click **Date and time**.
2. Click **Relative date/time**.
3. In the **Anchor relative to** section, select the date and time you want to use as the anchor.
4. In the **Set range** section, select the range of time you want to filter by.
5. Click **Okay**.

Filter by partial results

Show evidence based on whether a result is complete or partial. Because AXIOM Process searches both allocated and deleted space, recovered artifacts can be a mix of complete and partial results. Partial results are valuable but often require a manual investigation of the underlying data.

1. On the Filters bar, click **Partial results**.
2. Select a filter option and click **Okay**.

Filter by skin tone percentage

To help detect explicit content in media like pictures, video, and carved video, AXIOM Process uses a skin tone detection algorithm. By converting data to an advanced color space and isolating clusters of pixels that appear to be skin, AXIOM Examine filters content based on the overall percentage of skin tone—for all different skin colors—in a specific media file. Values are within a range of 0% and 100%. A value of 0% indicates that there is no skin tone present, while 100% indicates there’s only skin tone present.

1. On the **Filters** bar, click **Skin tone**.
2. Set the skin tone percentage range you want to detect and click **Okay**.

Tip: You can optimize this filter by importing hash lists for files like standard operating system icons and screen savers that are not relevant to your case. AXIOM Examine will ignore these files so that they don't clutter your evidence. For more information, see Ignore non-relevant files.

View a saved or historical filter set

You can view filter sets that you've saved from the current or a different case, or reapply filter sets that you've applied since opening your case.

To learn more, see Save filter sets.

1. In the Artifacts explorer, on the Filters bar, click **Filters**.
2. In the drop-down list, click a filter set:
   - To view a saved filter set, click one of the options under **Filter sets**.
   - To view a previous filter set since opening your case, click one of the options under **Filter set history**.

Sort and filter columns

In AXIOM Examine: In the Artifacts or File system explorer > Column view > Select an artifact, artifact category, or folder from the left navigation pane.

Sort a column

To sort content in a column under Evidence, click the header of the column you want to sort.

Note: If you sort on a column that contains a string that begins with special characters (i.e. not numbers or letters), you can find this evidence at the top or bottom of the column.

Filter a column using a basic search

Set filters on individual columns under Evidence for a particular artifact.

1. Right-click the header of a column and select **Filter on column**.
2. On the **Basic** tab, depending on the type of column, complete one of the following options:
   - For date and time columns, select a start and end date and time.
   - For numeric columns, specify a range or an exact value to filter on.
   - For string columns, specify a search term.
3. Click **Search**.

Filter a column using an advanced search

When using Column view, set advanced filters on columns and complete an advanced search using search terms or regex pattern matching.

Search using multiple words or search terms and choose whether you want to see results for all (an "AND" search) or any (an "OR" search) of the search terms. For each keyword you specify, you can choose to show only the items that include or exclude that word. You can further specify if you want to search for the whole word only, match the case, and search for the term if it appears near another word or set of characters.

To learn more about regex, sign in to the Support Portal to read the article Add regular expressions to search in Magnet AXIOM.

1. Right-click the header of a column and select **Filter on column**.
2. On the **Advanced** tab, select **Search terms** or **Regex pattern matching**.
3. Provide the search terms or regular expressions you want to use, then click **Search**.

Save filter sets

When you apply filters to evidence, save filter sets so you can use them again in the current case, or share them with your other AXIOM cases.

> Note: Filter sets can't be shared or imported to other AXIOM cases if they contain any filters that include case-specific IDs. For example, if you filter on related artifacts from the Media explorer, this filter set can't be shared with other cases because it relies on the Hit IDs of artifacts from the current case.

Save the current filter set

1. In the Artifacts explorer, apply filters to your evidence.
2. On the Filters bar, click **Filters**.
3. In the drop-down list, click **Save filter set**.
4. To save the filter set for use in the current case, provide a name and click **Save**.
5. To save the filter set for use in your other AXIOM cases, provide a name, select the option to **Share this filter set with other cases**, then click **Save**.

Save a previous filter set

AXIOM Examine keeps a history of the filters you've applied since opening the case.

1. In the Artifacts explorer, on the Filters bar, click **Filters**.
2. Under **Filter set history**, click the timestamp of a filter set to reapply it to your case.
3. On the Filters bar, click **Filters**.
4. In the drop-down list, click **Save filter set**.
5. To save the filter set for use in the current case, provide a name and click **Save**.
6. To save the filter set for use in your other AXIOM cases, provide a name, select the option to **Share this filter set with other cases**, then click **Save**.

Import and export filter sets

1. In the Artifacts explorer on the Filters bar, click **Filters**.
2. Under **Filter set history**, click the timestamp of a filter set to reapply it to your case.
3. On the Filters bar, click **Filters**.
4. In the drop-down list, click **Manage filter sets**.
5. In the window that appears, do one of the following:
   - Select one or more filter sets and click **Export**.
   - Click **Import** and select filter sets that you've saved previously.
6. Click **Okay**.

SEARCH AND CATEGORIZE MEDIA

To learn about searching and categorizing media in AXIOM, select one of the topics below.

Select and share media categorization lists

Note: To help streamline AXIOM Cyber investigations, Project VIC and CAID features are unavailable by default. To use these features, you must first Customize log collection and diagnostics.

Select a media categorization list

Select a list of categories to use to tag media in your case. Choose preset media categorization profiles for Project VIC (Canada, International, United States) or CAID (United Kingdom), add a new list, or import a list of media categories.

1. Click **Tools** > **Manage media categories**.
2. In Media categorization lists, select the list you want to use and optionally customize the list.
3. Click **Okay**.

Create a custom list of media categories

Create a custom list of up to 10 categories to use to tag media in your case.

1. Click **Tools** > **Manage media categories**.
2. In Media categorization lists, click **Add new list**.
3. In the table, select the list you created, called "My custom list."
4. Under Customize the media categorization list, in the **List name** field, provide a name for your media categorization list.
5. Customize your list using the options below:
   - To change the color of a category, click the current color, and then choose a new color.
   - To change the name of a category, double-click the current name and provide a new name. Click **Update**.
   - To turn off a category you don't want to use, deselect it from the Enabled column.
   - To indicate that items in the category include illicit or illegal content, select the category in the Illegal column.
6. Optionally, select the default category you want to assign to all visible uncategorized pictures.
7. Click **Okay**.

Import a media categorization list

Import a list of categories to use to tag media in your case. Files must be in XML format.

1. Click **Tools** > **Manage media categories**.
2. In Media categorization lists, click **Import list**.
3. Browse to the XML file that you want to import, and then click **Open**.
4. Click the **Active** option next to the list you created.
5. In the **List name** field, provide a name for your media categorization list.
6. Complete any of the following actions to customize your media categorization list:
   - To change the color of a category, click the current color, and then choose a new color.
   - To change the name of a category, double-click the current name and provide a

new name. Click **Update**.

- To turn off a category you don't want to use, deselect it from the Enabled column.

7. Optionally, select the default category you want to assign to all visible uncategorized pictures.
8. Click **Okay**.

Export a media categorization list

Export your list of media categories to share with other examiners in an XML format.

1. Click **Tools** > **Manage media categories**.
2. In Media categorization lists, select the list that you want to export.
3. Click **Export list**.
4. Browse to the location where you want to save the list.
5. Click **Save**.

Reduce exposure to illicit content

When viewing and categorizing media in AXIOM Examine, consider using the following options to help reduce your exposure to illicit content.

Blur or hide illegal media items

Choose whether or not you want to obscure illicit media in thumbnail previews and in the Details card.

1. Click **Tools** > **Manage media categories**.
2. Click **Media options**.
3. In the **Select media obfuscation options** section, choose whether you want to display, blur, or hide media in illegal categories.
4. Click **Okay**.

Mute videos by default

Choose whether or not you want to be able to hear videos when playing them.

Note: If you choose to mute videos, turning the sound on for a single video in the Preview card does not affect this setting. All other videos remain muted by default.

1. Click **Tools** > **Manage media categories**.
2. Click **Media options**.
3. In the **Select default sound level** section, choose whether you want to mute sound or keep sound on.
4. Click **Okay**.

Set a reminder to stop categorizing media

Consider setting a reminder to stop categorizing media after a specified amount of time or after you've categorized a specified number of items (for example, the number of media items required to make a conviction).

1. Click **Tools** > **Manage media categories**.
2. Click **Reminder options**.
3. In the **Set reminder type** section, choose the type of reminder you want to receive and the applicable settings.
4. Click **Okay**.
5. If you chose a timer-based reminder, in the Media explorer, next to Timer, click **Start**.

Set an end time for media categorization

Consider setting a reminder to stop categorizing media, or avoid starting to categorize media, at a certain time of day (for example, if you want to take a break before the end of your work day). When you reach the time of day that you specify, AXIOM Examine will prompt you to stop categorizing media.

1. Click **Tools** > **Manage media categories**.
2. Click **Reminder options**.
3. In the **Set media categorization end time** section, click the **Remind me to stop categorizing** option and choose a time.
4. Click **Okay**.

Find matching and similar media using AI and hashes

Categorize pictures using Magnet.AI

Using machine learning models trained with real data sets, Magnet.AI identifies and tags pictures that might be of interest in your case, depending on the categories you select.

You can set up Magnet.AI categorization when you create your case in AXIOM Process, or perform the categorization in an existing case in AXIOM Examine. To learn how to categorize media using Magnet.AI, see Analyze pictures with Magnet.AI.

Find similar pictures using Magnet.AI

Using content-based image retrieval technology (CBIR), Magnet.AI helps you identify pictures that are similar to each other in your case. Magnet.AI finds similar pictures based on a picture's general attributes, such as pictures of the same room or pictures with similar scenery, rather than specific details such as small objects or faces.

To find similar pictures, you need to build picture comparison when you create your case in AXIOM Process, or in an existing case in AXIOM Examine. You can then find similar pictures in AXIOM Examine. To learn how to build picture comparison and find similar pictures, see Build picture comparison manually.

Find hash matches

AXIOM can automatically search and categorize evidence for you, if you select the option to calculate hash values for all files and import hash sets of known files.

When you create a case in AXIOM Process, add hash sets from your local database or your organization's central database. You can also add hash sets to an existing case in AXIOM Examine. AXIOM Process remembers your previous selections the next time you create a new case or add evidence to an existing case.

To learn more about hashing in AXIOM, see the following topics:

- Calculate hash values and find matches
- Categorize media automatically by hash value
- Find matching hashes using Magnet Hash Sets Manager

Find pictures with PhotoDNA matches

Using PhotoDNA, AXIOM can identify pictures that have been modified to change their hash values and pictures that are similar in appearance to existing Project VIC pictures. If PhotoDNA was enabled when the case was processed, each valid picture will have a PhotoDNA hash assigned to it. To learn how to enable this setting, see Enable PhotoDNA.

In addition to finding matching pictures with identical hashes, PhotoDNA also uses fuzzy matching to find similar pictures with slight modifications. A user may have modified a picture by re-sizing, cropping, or drawing over it, by adding a watermark, or by changing the resolution. Even with these changes, PhotoDNA can identify the picture as similar to the original picture. PhotoDNA works by converting pictures into a black-and-white format, dividing them into squares, and calculating a numerical value for each square. These values, which represent the shading in each square, are the PhotoDNA signature or hash of a picture.

When categorizing media using Project VIC or another hash set, PhotoDNA will categorize matches as non-pertinent only if there is a cryptographic hash match (MD5 or SHA1). PhotoDNA will not categorize media as non-pertinent for matches alone.

1. In AXIOM Examine, select a picture artifact.
2. In **Details** > **Artifact Information**, find the picture's PhotoDNA hash (alongside its MD5 and SHA1 hashes).
3. Right-click the artifact and click **Find pictures with PhotoDNA matches**.

4. In the **Find pictures with PhotoDNA matches** dialog, select one of the following options:
   - To find identical, unmodified picture matches, click **Exact match**. This option has the same functionality as searching for MD5 and SHA1 hashes.
   - To find a similar picture file that might be a modified version of the selected one, click **Similar match**.
5. Click **Search**.

Manually apply media categories to case evidence

Note: To help streamline AXIOM Cyber investigations, Project VIC and CAID features are unavailable by default. To use these features, you must first Customize log collection and diagnostics.

Categorize media from one of the following locations in AXIOM Examine:

- **Media explorer**
- **Artifacts** explorer > **Thumbnail view**

Before you begin

Before you begin categorizing media, configure the following settings:

- Select, import, or create a media categorization list. See Select and share media categorization lists
- Reduce your exposure to graphic content using reminder and media obfuscation options. See Reduce exposure to illicit content.

In addition to the above options, note the following AXIOM Examine features that can help your investigation:

- While categorizing media, you can view your progress in the Media categorization progress bar.

- When you categorize a picture or video, AXIOM Examine automatically applies the same media category to any other media items in the case with a matching MD5 or SHA1 hash.
- The Media explorer includes helpful features such as stacking duplicate media and viewing related artifacts. See View media evidence in the Media explorer.

Apply a media category to selected pictures or videos

1. Expand the **Tags and comments** pane.
2. Select the thumbnails of the pictures or videos that you want to apply a media category to.
3. Under Tags and comments, in Media categories, click the media category you want to apply, or press the keyboard shortcut (0-9) for the media category you want to apply.

Tip: After you apply a category for a media item, AXIOM Examine automatically selects the next thumbnail so that you can continue to apply media categories to subsequent items.

Apply a media category to all visible uncategorized pictures or videos

1. Expand the **Tags and comments** pane.
2. Under Tags and comments, in Media categories, in the **Set all visible uncategorized pictures to** drop-down, select a media category.
3. Click **Categorize**.

Tip: After you apply a category to all visible uncategorized media, AXIOM Examine automatically displays the next set of uncategorized evidence so that you can continue to apply media categories to subsequent items.

Categorize media files using categorizations from a third party

If you categorized your media for Project VIC using a third-party tool, you can import the .json files to apply those categorizations to the media in your case after initial processing.

1. Click **Process** > **Categorize pictures and videos by hash value**.
2. When AXIOM Process opens, browse to **Processing details** > **Categorize pictures and videos**.
3. In **Categorize pictures and videos by hash value**, click **Add file**.
4. Browse to the location where you saved the .json file and click **Open**.
5. If applicable, clear the **Enabled** column next to any previously imported .json files that you don't want to use for this search.
6. Click **Analyze evidence**.

Share media categorization and hash match results

Update hash set database with new media categorizations or hashes

After you manually categorize pictures and videos in your case, you can add these categorizations to hash sets in your local Magnet AXIOM hash database for use with future cases.

You can also add new media categorization hashes from your case to existing media hash sets from your organization's Magnet Hash Sets Manager database. You or other members of your organization can then access these updated hash sets. To learn more about the Magnet Hash Sets Manager, see Find matching hashes using Magnet Hash Sets Manager.

The next time you create a case in AXIOM Process and search the evidence using hash sets, the search will include the hashes that you've added.

Note: If your administrator has protected a hash set in the Magnet Hash Sets Manager database, a lock icon appears beside it. You can't update protected hash sets from AXIOM Examine.

1. Click **Process** > **Update hash set with new media categorizations**.
2. In **Step 1: Select a hash set to update**, complete one of the following options:
   - To add the hash list to an existing hash set, select the hash set you want to update.
   - To add the hash list to a new hash set, click **Add new hash set**. Provide a name for the hash set and click **Add**.
3. In **Step 2: Select the categories to update in the hash set**, select the categories you want to update in the hash set and click **Update hash set**.
4. When you've finished updating your hash sets, click **Close**.

Export media categorizations from a case to Project VIC or CAID

AXIOM Examine: Select **File** > **Create export / report** > **VICS**

After you've categorized pictures and videos in your case, you can create a JSON export of the reviewer graded media to share with Project VIC or CAID. If you have any media in your case that has been precategorized by CAID but is missing from their database, you can help them fill in these gaps by choosing the option to include attachments for media items that are missing from the CAID database.

This option creates a .json file using the Project VIC specification. For more information about Project VIC, see www.projectvic.org.

If you've enabled a pre-set media categorization country profile, the following categories are included in the export by default:

- Canada (Project VIC): Category 1
- International (Project VIC): Categories 1-2
- United Kingdom (CAID): All categories except 8
- United States (Project VIC): Categories 1-3

After you choose the category metadata you want to include, select the subset of categories you want to include attachments for in the export.

Consider using the following options for CAID exports:

- If you have any media in your case that has been categorized by CAID but is missing from their database, help fill in these gaps by choosing the option to include these missing attachments.
- You can optionally generate a new CaseID value so that the exported data appears as a new case within the CAID database.

ADD, REMOVE, OR REPROCESS EVIDENCE IN A CASE

Add new evidence to a case

AXIOM Process: Click **Browse to case** and select the case you want to add evidence to.

AXIOM Examine: Click **Process** > **Add new evidence to case**.

Tip: When you add new evidence to a case, make sure to provide Scan information in AXIOM Process > *Case details*, so that you can keep track of the separate acquisition instances in a case.

When you add new evidence in AXIOM Process, select your evidence search options the same way that you would for any new case. To learn more, see Processing details

You can continue working in your case in AXIOM Examine while the evidence is being processed. Click **Load new results** to view the evidence that has been processed so far. When processing completes, click **Okay**.

Import CPS evidence

Note: To help streamline investigations, this feature is unavailable for AXIOM Cyber users by default. To use this feature, you must first Customize log collection and diagnostics.

To help protect children that are targeted by suspects using the internet, the Child Rescue Coalition's Child Protection System (CPS) collects online data that tracks person-to-person activity such as IP addresses, file hashes, person-to-person user GUIDs, and more.

You can add evidence from the CPS to your case by importing the .csv files into AXIOM. In AXIOM Examine, click **Process** > **Add CPS export file**.

To learn more, see Add CPS data to a case.

Remove evidence from case

If your case contains multiple evidence sources, you can remove an evidence source and all its associated data.

Warning: Removing an evidence source is a permanent action that can't be undone.

1. In AXIOM Examine, on the **Process** menu, click **Remove evidence from case**.
2. Select the evidence source you want to remove and click **Okay**.
3. To confirm you want to remove the evidence, click **Remove evidence source**.

Reprocess artifacts with carving

During a search, you might have chosen to parse, rather than carve, artifacts in your case. You can carve these artifacts later. For more information about parsing and carving, and to learn how to carve parsed artifacts, see Parse and carve artifacts

Acquire more data from a cloud account

AXIOM Examine: **Case dashboard** > **Insights** > **Potential cloud evidence leads** > Select a cloud account.

Add cloud evidence using passwords and tokens

During a search, if AXIOM Process encounters tokens or passwords for a cloud account, it creates an artifact for them. You can use these passwords and tokens to open AXIOM Process and add a cloud evidence source.

Note the following caveats:

- IMAP/POP email and Apple accounts can't be accessed using this method.
- Passwords manually entered when acquiring cloud evidence are not saved.

1. Under Account details, select a password or token and click **Acquire data from this account**.
2. In the window that appears, click **Open AXIOM Process**.
3. In AXIOM Process, follow the steps to access the account and acquire available evidence.

If the authentication attempts are unsuccessful, AXIOM Process notifies you that you've entered an incorrect password and does not proceed past the sign in screen. An unsuccessful attempt can be due to one of the following reasons:

- The target changed their password
- The token expired

You can attempt to use another password / token, or you can attempt to acquire cloud evidence using an alternative access method.

Attempt to acquire cloud evidence using an alternative access method

If there are no passwords or tokens available, or if acquiring data using a password or token didn't work, you can attempt another access method. The access methods vary depending on the account platform.

1. Under Access Methods, choose an alternative access method and click the link.
2. In the window that appears, click **Open AXIOM Process**.
3. In AXIOM Process, follow the steps to access the account and acquire available evidence.

To learn more about access methods, see Cloud-based user accounts.

EXPORT EVIDENCE

To learn about exporting evidence from AXIOM, select one of the topics below.

Export evidence to share with stakeholders

In AXIOM Examine, create exports to share with stakeholders. Each export type has different settings and configuration options that are best suited to certain kinds of investigations.

Below are some recommendations for how to prepare your evidence for exporting, and when to use different export types depending on the audience or purpose of your export.

Before you begin

Prepare evidence for exporting

Before you create an export, consider the need to Add a tag or comment to evidence or Manually apply media categories to case evidence of interest so that it's easier to select only the necessary items in your export.

Create an export

There are a few different methods you can use to create an export, depending on your needs:

- To export a variety of items that you might have tagged or categorized, click **File** > **Create export / report** to open the exporting wizard and make your selections.
- To export a subset of data that you've filtered down to, or a number of items that you've selected, right-click your selection and click **Create export / report**. In the exporting wizard, under Items to include, select **Items in the current view** or **Selected items only**.

To learn more about which export type and options might be best for your investigation, see the recommendations below.

Note: AXIOM Examine saves exports to your case folder, with a UTC time stamp. Depending on the archive explorer you use to view the exported .zip file, the times of the artifacts might be converted to your local time. You can use tools such as 7-Zip to convert the artifact times back to what you see in AXIOM Examine.

Streamline your exporting workflow

If you are consistently creating a certain kind of export, and have a heavy workload, consider using Streamline your exports using templates and column configurations to streamline your exporting process.

Exclude confidential or non-relevant information

If your case includes data that is confidential or non-relevant to the stakeholder that you're sharing the export with, you can exclude that information. Add an appropriate tag to that content and select the tag from the **Items to exclude** section in the exporting wizard.

Export evidence for non-AXIOM users to investigate

Use a portable case if your export meets some or all of the following requirements:

- Stakeholders who are not technical, or not trained in digital forensics, need to investigate the case.
- Stakeholders without an AXIOM license need to investigate the case.

- You need further input from these stakeholders in the form of tags and comments on a set of evidence in your case.

The portable case exports the evidence you select to a lightweight version of AXIOM Examine, which includes the most necessary features for filtering, viewing, and tagging evidence. Portable cases don't include media categorization features, so we recommend categorizing media before you create the technical case.

To learn more, see Use portable case to collaborate on cases with others.

Export evidence for non-AXIOM users to review

Use an HTML or PDF export for review by stakeholders who don't use AXIOM Examine, or who aren't trained in digital forensics. These formats feature user-friendly displays of the information you select, and can include a summary of case dashboard information.

- Choose an HTML report if you want to include search capabilities, attachments, or the ability to view the export in a web browser.
- Choose a PDF report if you want to print the report, or prevent changes from being made to the file's contents.

Export evidence for further investigation in another tool

Some export types are designed to allow for further investigation or use in another tool.

Export evidence to Magnet REVIEW

Choose the Magnet REVIEW option to upload evidence directly to your organization's Magnet REVIEW cases, or, if you're working offline, to export data to a folder that can be ingested by Magnet REVIEW. To learn more, see Export evidence for Magnet REVIEW.

Export evidence for verification using another tool or script

If your organization uses another forensics tool, which you want to use to verify your evidence, choose the XML export. You can then run this exported evidence through other forensics tools, including those that are script-based.

This option exports all the evidence you select to an .xml file, and, optionally, includes external files in a separate attachments folder. For more information about the structure of the .xml file, log in to the Support Portal to review the Sample XML output article.

Export metadata to import into another tool or script

If your organization uses another forensics tool and you want to share tags and comments with another case in that third-party tool, use the exporting wizard to create a JSON export. This export type includes selected evidence as well as any tags or comments you've added to that evidence in AXIOM.

Export evidence to share it with another organization

Some export types are designed to be shared with other organizations, such as Project VIC or CAID, or other agencies for further investigation.

Export graded media for Project VIC or CAID

> Note: To help streamline AXIOM Cyber investigations, Project VIC and CAID features are unavailable by default. To use these features, you must first Customize log collection and diagnostics.

After you've categorized pictures and videos in your case, you can create a JSON export of the reviewer graded media to share with Project VIC or CAID. If you have any media in your case that has been precategorized by CAID but is missing from their database, you can help them fill in these gaps by choosing the option to include attachments for media items that are missing from the CAID database.

This option creates a .json file using the Project VIC specification. For more information about Project VIC, see www.projectvic.org.

If you've enabled a pre-set media categorization country profile, the following categories are included in the export by default:

- Canada (Project VIC): Category 1
- International (Project VIC): Categories 1-2

- United Kingdom (CAID): All categories except 8
- United States (Project VIC): Categories 1-3

After you choose the category metadata you want to include, select the subset of categories you want to include attachments for in the export.

Consider using the following options for CAID exports:

- If you have any media in your case that has been categorized by CAID but is missing from their database, help fill in these gaps by choosing the option to include these missing attachments.
- You can optionally generate a new CaseID value so that the exported data appears as a new case within the CAID database.

Export data about people of interest for other examiners

Select the identifiers export to create a .json with all the identifiers you've noted in your case, and share this information with other examiners or organizations.

The identifiers export requires you to provide your organization name and contact information, so that if another organization gets a match on one of your identifiers, they can contact you to request more information about your case.

Create exports for specific evidence types

In AXIOM Examine, each export type includes different settings and configuration options that are suited to certain kinds of cases and investigations. Below are some recommendations for when to use an export type depending on the evidence that you intend to export.

Before you begin

Prepare evidence for exporting

Before you create an export, consider the need to Add a tag or comment to evidence or Manually apply media categories to case evidence of interest so that it's easier to select only the necessary items in your export.

Create an export

There are a few different methods you can use to create an export, depending on your needs:

- To export a variety of items that you might have tagged or categorized, click **File** > **Create export / report** to open the exporting wizard and make your selections.
- To export a subset of data that you've filtered down to, or a number of items that you've selected, right-click your selection and click **Create export / report**. In the exporting wizard, under Items to include, select **Items in the current view** or **Selected items only**.

To learn more about which export type and options might be best for your investigation, see the recommendations below.

> Note: AXIOM Examine saves exports to your case folder, with a UTC time stamp. Depending on the archive explorer you use to view the exported .zip file, the times of the artifacts might be converted to your local time. You can use tools such as 7-Zip to convert the artifact times back to what you see in AXIOM Examine.

Streamline your exporting workflow

If you are consistently creating a certain kind of export, and have a heavy workload, consider using Streamline your exports using templates and column configurations to streamline your exporting process.

Exclude confidential or non-relevant information

If your case includes data that is confidential or non-relevant to the stakeholder that you're sharing the export with, you can exclude that information. Add an appropriate tag to that content and select the tag from the **Items to exclude** section in the exporting wizard.

Export summary information about an evidence source

In addition to creating more detailed reports, you may want to export summary information about a mobile device or other evidence source in your case. This export type is a PDF that includes information you would find on the evidence source dashboard, such as details about the device and an artifact type summary.

1. On the Case dashboard, select an evidence source from the left navigation pane.
2. Click **Create evidence source report**.
3. Select the information to include, a file location, and click **Create report**.

Export emails

If you want to export Microsoft Outlook emails or other emails supported by the email explorer, use the PST export option. To learn more about viewing PST exports and understanding the data in them, sign in to the Support Portal to read the article Understanding PST exports.

If you want to export emails and their attachments, consider using the HTML export option.

Export chat threads

AXIOM Examine threads chat message artifacts and displays them in conversation view. To learn more, see View chat threads using conversation view. You can export these chat threads using the following export types:

- To export chat threads that are in the language you use in AXIOM Examine, we recommend using HTML, PDF, or XML.
- To export chat threads that are in another language besides the one you use in AXIOM Examine, we recommend using Excel, HTML, or PDF. For more information, see Export evidence that is in a different language.

When creating your export, you can choose to include only the chat messages you selected, or include the full conversation history of any chat messages you selected.

Export evidence with attachments

If you want to export evidence with attachments, choose an HTML, PDF, or XML export. In the exporting wizard, under Configure artifact details, select the option to include attachments.

Export categorized or graded media

Export graded media for Project VIC / CAID

Note: To help streamline AXIOM Cyber investigations, Project VIC and CAID features are unavailable by default. To use these features, you must first Customize log collection and diagnostics.

After you've categorized pictures and videos in your case, you can create a JSON export of the reviewer graded media to share with Project VIC or CAID. If you have any media in your case that has been precategorized by CAID but is missing from their database, you can help them fill in these gaps by choosing the option to include attachments for media items that are missing from the CAID database.

This option creates a .json file using the Project VIC specification. For more information about Project VIC, see www.projectvic.org.

If you've enabled a pre-set media categorization country profile, the following categories are included in the export by default:

- Canada (Project VIC): Category 1
- International (Project VIC): Categories 1-2
- United Kingdom (CAID): All categories except 8
- United States (Project VIC): Categories 1-3

After you choose the category metadata you want to include, select the subset of categories you want to include attachments for in the export.

Consider using the following options for CAID exports:

- If you have any media in your case that has been categorized by CAID but is missing from their database, help fill in these gaps by choosing the option to include these missing attachments.
- You can optionally generate a new CaseID value so that the exported data appears as a new case within the CAID database.

Export categorized media for review by stakeholders

In AXIOM Examine, you can categorize media. To learn more, see Search and categorize media. To export this categorized media, as well as include the media items as attachments, use a PDF or HTML export.

Protect stakeholder wellness when exporting sensitive media

If your export includes sensitive content that has been categorized in illegal categories and you want to blur it to protect the wellbeing of your stakeholders, use an HTML export. Under Configure artifact details, select **Include previews and file attachments** and **Blur previews for items in illegal categories**.

Export evidence that is in a different language

If you want to share evidence that's in a different language, export it to an Excel, HTML, or PDF file. Excel spreadsheets, HTML files, and PDF files support multi-line UTF-8 encoded text (for example, chat messages in different languages), so you won't see display errors that are common in other types of exports (like .csv files).

Tip: If you created an Excel report and the evidence contains content that appears on multiple lines, for example chat messages, turn on the wrap text feature in Microsoft Excel. (In Excel, press **CTRL + A**. On the toolbar, click **Wrap Text**.)

Export timeline data

The Timeline explorer displays timestamped case data in an interactive graph.

To share evidence from the timeline, export it to a .csv file.

1. In AXIOM Examine, in the **Timeline explorer**, select and right-click items that you want to export.
2. Click **Create report / export**.

3. Next to the **File path** field, click **Browse** and select the location you want to save the export. Click **Select folder**.
4. Click **Create**.

Export connections

The Discover connections displays case data in a connections map. If connections are valuable to your investigation, consider exporting the connections map directly and adding this to your report, rather than just exporting the data from another explorer in a typical table form. You can export connections to a PDF or HTML file.

Print or export a connections map as a PDF

If you want to include a map of connections in your report, you can print it to paper or PDF. A printed map includes the primary node and any focus nodes.

1. In AXIOM Examine, in the **Connections explorer**, right-click a node.
2. Click **Print**.
3. Follow the instructions on screen to print the map.

Export a connections map as an HTML file

If you want to include a map of connections in your HTML report, you can save the connections map as an HTML file.

1. In AXIOM Examine, in the **Connections explorer**, right-click anywhere in the map.
2. Click **View source**.
3. In the .txt file that appears, on the **File** menu, click **Save as**.
4. Browse to the location where you want to save the file.
5. Provide a **File name** ending in **.html**.
6. Click **Save**.

Export memory artifacts (Volatility)

Note: Currently, only memory dumps processed using Volatility allow memory artifacts to be exported from AXIOM Examine.

You can use AXIOM Examine to export memory artifacts from your case to import into other tools. You can choose to export files based on their type:

- Process executable files (procdump)
- Dynamic link library files loaded by the process (dlldump)
- Memory associated with a particular process (memdump)
- Open files in memory (dumpfiles)
- Range of pages described by a VAD node (vaddump)

To export memory artifacts, complete the following steps:

1. In AXIOM Examine, right-click the memory artifact you want to export, and then click **Export memory items**.
2. In the **Export memory items** dialog, complete the following actions:
    a. In **Export details**, provide the **Folder name** and **File path** that you want to use.
    b. In **Items to include**, select the memory items that you want to export.
3. Click **Export**.

Export metadata

Export metadata to import into another tool or script

If your organization uses another forensics tool and you want to share tags and comments with another case in that third-party tool, use the exporting wizard to create a JSON export. This export type includes selected evidence as well as any tags or comments you've added to that evidence in AXIOM.

Export file system metadata

In the File system explorer, you can export the metadata associated with files or folders to a .csv file. By default, AXIOM Examine saves exported metadata to your case folder.

1. In AXIOM Examine, open the **File system** explorer and browse to the file or folder of interest.
2. In **Evidence**, right-click the item you want to export metadata for. To select multiple items, press **CTRL** and click the items. Then, right-click one of the highlighted items.
3. Click **Export details**.
4. Click **Browse to location** and select the location where you want to save the export. Enter a file name.
5. Click **Save file**.

View artifacts in an external application

You can view the contents of artifacts using external applications such as HxD, Adobe Acrobat, Google Chrome, Microsoft Word, and more. The applications that AXIOM Examine suggests for each artifact come from recently used Windows programs that are associated with each artifact type.

1. In AXIOM Examine, in the **Artifacts explorer**, right-click an artifact.
2. Click **Open with**.
3. Select the application that you want to open the artifact with and click **Okay**.

Save artifacts to your computer

When you save artifacts, AXIOM Examine saves the bytes of data that the specific artifact hit is associated with. If the hit is parsed, the entire source file gets saved. If the hit is carved, only a subset of the source file gets saved.

1. In AXIOM Examine, in the **Artifacts explorer**, right-click an artifact group or type, or a single artifact.

2. Click **Save artifact to**.
3. Browse to the location where you want to save the files and click **Select folder**.

Save or copy text or hex data

You can save or copy a selection of text or hex data for use at a later time. To save or copy the data:

1. In Text and hex view, click and drag to select text or hex values.
2. Right-click and select **Save selection** or **Copy selection.**
3. If you chose to save the hex data, browse to the location where you want to save the data.
4. Provide a file name (ending in .txt), and then click **Save**.

To learn more about text and hex, see View raw artifact data in Text and hex.

Export animated route playback

Record and export the animated playback of one or more routes as an MP4 file to share with stakeholders.

1. In route view, select the routes you want to export and any other playback settings you want to include in the recording.
2. Below the map, click the record button.
3. Click the play button. While the route is recording, you can adjust the settings so they change throughout the video.
4. To end the recording, click the stop button.
5. In the window that appears, to create the export, click **Okay**.
6. To review the export, browse to your case folder and open the exports folder.

Export messages and attachments to share with legal reviewers

Note: This feature is only available for AXIOM Cyber users.

There are two export options that allow you to share email or chat message data with legal reviewers on an eDiscovery platform: load file and RSMF (Relativity Short Message Format).

- Select the load file option to export data for use with eDiscovery platforms that support .dat files, such as Relativity.
- Select the RSMF option to export chat messages and attachments for use with Relativity only. To learn which chat artifacts are supported by this export type, sign in to the Support Portal and read the article Supported chat artifacts for RSMF exports.

Select settings for load file exports

Select chat thread settings for a load file

Under Configure artifact details, you have the option to export the chat thread previews together in the same file, or each in a separate file.

- If you want to include additional context for reviewers, and you don't have concerns about further redaction after creating the export, select **Include all selected messages in each native file**. This option includes all messages from the conversation in the file, with a separate file for each conversation.
- If you're concerned about further redaction after creating the export, select **Only display a single message for each native file**. Each message in the conversation will appear in its own file, so you can select which files to upload for reviewers.

Note: Any media embedded in chat messages will be included in the chat message previews.

Include all related items for load file exports

To include attachments for the emails or chat messages you selected, as well as any parent and sibling items if the items you selected are attachments themselves, select the **Export selected items and their attachments or parent items** option. To learn more, sign in to the Support Portal to read the article Exporting attachments and parent items to load files.

Files included in a load file export

The .dat file uses the following Relativity/Concordance default delimiters:

- Column: ASCII 020
- Quote: ASCII 254
- Newline: ASCII 174

In addition to a .dat file, the load file export also includes text files for every included document, and native files for the following artifacts:

- Email (includes a .msg file for each email)
- User created content including pictures, video, audio, and documents (the original file)
- Chat messages from any source (an HTML chat thread is generated for each chat message)
- Examiner-defined and custom artifacts (the original file)

Select chat thread settings for an RSMF export

Under Configure artifact details, you have the option to export the chat thread preview for selected messages only or all messages for the conversation.

- If you want to include additional context for reviewers, and you don't have concerns about further redaction after creating the export, select **Include all messages from the chat thread**. This option includes all messages in the conversation, even the messages you didn't select, with each conversation in a separate .rsmf file.
- If you're concerned about further redaction after creating the export, or you want to limit the information that your reviewers see, select **Only display the selected message in each native file**. This option only includes the messages you selected from the conversation, with each conversation in a separate .rsmf file if messages from multiple conversations were selected.

Note: Any media embedded in chat messages will be included in the chat message previews.

Export evidence for Magnet REVIEW

If your organization uses Magnet REVIEW, you can configure AXIOM Examine to upload evidence directly to a Magnet REVIEW case. If you don't configure this setting, you can also create an export that is compatible with Magnet REVIEW, which you can upload manually.

Configure Magnet REVIEW in AXIOM Examine

Configure AXIOM Examine to be able to upload evidence directly from your case to Magnet REVIEW. You only need to do this configuration once for each instance of Magnet AXIOM.

1. In AXIOM Examine, on the **Tools** menu, click **Settings**.
2. In the Settings window, click **Product integrations**.
3. Under Product integrations, select **Magnet REVIEW**.
4. Enter your organization's Magnet REVIEW **Server URL** and **API key**.
5. Click **Okay**.

Upload evidence from Magnet AXIOM to Magnet REVIEW

To export evidence from Magnet AXIOM and automatically upload it to a Magnet REVIEW case, you'll first need to Configure Magnet REVIEW in AXIOM Examine.

Click **File** > **Upload case to Magnet REVIEW**. In the exporting wizard, make sure the following options are selected:

- Under Items to include > Select Magnet REVIEW export format, select **REVIEW 2.0**. By default, all tags and comments in the case are included, but you can manually select which ones to include under Select applied tags and comments.
- Under Customize formatting options, select the option that applies to your organization:
    - If your organization has its own Magnet REVIEW server, select **Upload to a customer-hosted REVIEW server**

  - If your organization uses Magnet REVIEW in the centralized server, select **Upload to Magnet REVIEW SaaS**. Then, click **Sign in** and provide your credentials.

    > Note: When you upload your case to Magnet REVIEW SaaS, the data will be stored in a cloud server hosted by Magnet Forensics and based in the United States.

- Under Provide additional information, provide a case number. The evidence will upload to that case if it already exists, or it will automatically create a new case if that case number doesn't yet exist.

Export evidence from Magnet AXIOM to your computer

To export evidence from Magnet AXIOM to your computer, which you can later manually upload to Magnet REVIEW, click **File** > **Upload case to Magnet REVIEW**. In the exporting wizard, make sure the following options are selected:

- Under Items to include > Select Magnet REVIEW export format, select **REVIEW 2.0**. By default, all tags and comments in the case are included, but you can manually select which ones to include under Select applied tags and comments.
- Under Customize formatting options, select **Export the data to this computer**.
- Under Preview and save, click **Browse** to provide a file location where AXIOM Examine will save the export. Make sure the location you select has enough storage space for the exported evidence.

AXIOM Examine creates a folder that contains the JSON export and associated attachments. After the export finishes, you can upload evidence using the Magnet REVIEW CLI.

Merge tags and comments into original case

After you've exported evidence for use in Magnet REVIEW, you can merge tags and comments from that case back into your original case. To learn more, see Merge tags and comments back into the original case.

Use portable case to collaborate on cases with others

To collaborate on a case with other examiners and stakeholders, you can create a portable case in AXIOM Examine.

When you share a portable case with other stakeholders, they can explore the evidence, and add their own comments, tags, media categorizations, and bookmarks. Stakeholders don't need to have AXIOM Examine installed to review a portable case.

When they complete their reviews, you can merge their findings back into the original case.

Create a portable case

Create a portable case to share evidence from an investigation with stakeholders who might not be forensic examiners and might not have access to all the case material. You can choose which evidence items you want to include, share all of the evidence you have recovered, or choose specific evidence items such as tagged evidence.

You can also Streamline your exports using templates and column configurations

1. In AXIOM Examine, right-click an artifact group or items that you want to include in the portable case.
2. Click **Create export / report**.
3. Under **Export / report format**, select **Portable case**.
4. Follow the instructions to customize and create your portable case.

Export evidence from a portable case

From your portable case, you can create Excel, HTML, and PDF reports. You can share these reports with other stakeholders in your case.

1. In AXIOM Examine, click **File** > **Create export / report**.
2. In the window that appears, follow the instructions to create your export.

Export timeline data from a portable case

To share evidence from the timeline, export it to a .csv file.

1. In AXIOM Examine, in the **Timeline explorer**, select and right-click items that you want to export.
2. Click **Create report / export**.
3. Next to the **File path** field, click **Browse** and select the location you want to save the export. Click **Select folder**.
4. Click **Create**.

Merge a portable case

In AXIOM Examine, you can merge a portable case into your case. Merging a portable case allows you to import tags and comments (including those applied in the Timeline explorer), media categorizations, and profiles that other stakeholders have added to the portable case, and combine them with your own notes in the case.

> Note: You can't merge two portable cases together. The portable case must be merged with the original case it was created from.

1. In AXIOM Examine, click **File** > **Merge portable case**.
2. In the window that appears, follow the instructions to merge your portable case and choose what to include from it.

Open a portable case

1. Browse to the portable case folder provided to you by the examiner.
2. In the **Export** folder, double-click the **OpenCase.exe** file.

> Note: Often, the evidence that you examine includes executable files or scripts (including those embedded in other artifacts such as PDF files or documents). Please note that

AXIOM Examine never runs executable files or scripts contained in your evidence (whether examined from AXIOM Examine or a portable case)–including if you try to open an executable file with an external application.

When you've completed reviewing the evidence, you can send the send the portable case folder back to the owner of the original case.

Share a portable case

When you create a portable case in AXIOM Examine, the portable case export includes several files and folders. The export includes an executable file for AXIOM Examine as well as other dependencies.

When you share a portable case with your stakeholders, make sure you provide them with the entire export folder in a read/write format. To help users who haven't used Magnet AXIOM, a PDF file called the *Portable case quick start guide* is automatically included with the portable case.

Features available in portable case

Feature	Availability in portable case
Add CPS export file	Yes
Add, remove, reprocess evidence	No
Artifacts explorer	Yes
Case dashboard	Yes (excluding Magnet.AI, Picture categorization, Import CPS, Import keyword list, and Add/remove evidence)
Column filtering	Yes
Comments	Yes
Connections explorer	No
Conversation view (Artifacts explorer)	Yes

Feature	Availability in portable case
Create a portable case	No
Create export / report (HTML, PDF, and Excel)	Yes
Email explorer	No
Evidence source dashboards (Case dashboard)	Yes
Extract text from files using OCR	No
File system explorer	No
Filter bar	Yes
Hex decoder	No
Histogram view (Artifacts explorer)	Yes
Locate source	No
Keywords	Yes
Magnet.AI categorization	No
Media categorization in Thumbnail view (Artifacts explorer)	Yes
Media explorer	No
Merge portable case into original case	No
Potential cloud evidence leads (Case dashboard)	No
Profiles	Yes
Reduce exposure to illicit content (reminders and media obfuscation)	Yes
Registry explorer	No
Route view (Artifacts explorer)	Yes (if portable case was created from a case with an AXIOM term or AXIOM Cyber license)

Feature	Availability in portable case
Search - Basic	Yes
Search - Advanced	Yes
Tags / bookmarks	Yes
Timeline	Yes (reviewer must manually build the timeline in the portable case)
Update hash sets with new media categorizations	No
World map view (Artifacts explorer)	Yes

Streamline your exports using templates and column configurations

If your cases frequently require you to create similar kinds of exports, use templates and column configurations to help streamline the exporting process by predetermining the artifact types, columns, and format options that are the most useful for different types of investigations. Using templates and column configurations, you can:

- Save your export settings for use in future exports.
- Use AXIOM Examine's system templates.
- Import other users' templates and column configurations.
- Select a template or column configuration as a starting point, but edit the selections during the export workflow as needed.

> Note: Templates are not available for Identifiers, PST, and VICS export formats. These formats are more streamlined, and don't require templates to save time.

Create an export using a template or column configuration

When you create an export, make sure the following settings are selected in order to use a template or column configuration:

- Under Items to include, select **Use a template** and select a template from the drop-down list.
- Under Configure artifact details > Configure columns to include, select **Specific columns only** and select a column configuration from the drop-down list.

Manage templates

Save export settings as a template

When you create an export, you can save the settings for use in future exports of the same format. The template saves your selected artifact types, column configuration, and formatting options, if applicable.

In the exporting wizard, after you've made all the selections for your export, under Preview and save, click **Save settings to template**.

Create a new template

You can create a new template directly from AXIOM Examine.

1. Click **Tools** > **Manage export / report settings**.
2. Under Manage templates, click **Create new**.
3. Follow the steps in the exporting wizard to select a format and the settings you want to include in your template.
4. Under Format options, click **Save template**.

Edit a template

You can edit all user-created templates, but not system-created ones.

1. Click **Tools** > **Manage export / report settings**.
2. Under Manage templates, hover the mouse over the template you want to edit and click **Edit**.

> Tip: If you want to create a template using an existing template as the basis, including a system-created template, you can **Duplicate** the template first, and then edit the copy.

3. Follow the steps in the exporting wizard to make changes to the template.
4. Under Format options, click **Save template**.
5. To rename the template, under **Template name**, double-click the current name. Enter a new name, then click **Update**.

Import a template

> Note: This feature is only available for AXIOM Cyber users.

You can import another user's template to use for your own exports of the same format.

1. Click **Tools** > **Manage export / report settings**.
2. Under Manage templates, click **Import**.
3. Browse to the JSON file that contains the template and click **Open**.

Export a template

You can export a template so that other examiners can use it in their own exports.

1. In AXIOM Examine, click **Tools** > **Manage export / report settings**.
2. Under Manage templates, hover the mouse over the template you want to export and click **Export**.
3. Browse to the folder where you want to save the JSON file, enter a name for the file, and click **Save**.

Manage column configurations

> Note: This feature is only available for AXIOM Cyber users.

Create a column configuration

When you create an export, you can create a new column configuration for use in future exports. You can also configure the sort order (primary, secondary, or tertiary) of the column names for each artifact. After you select a sort option, use the arrows next to the drop-down to indicate the sort direction. By default, ascending order is used (up arrow).

1. Click **Tools** > **Manage export / report settings**.
2. Under Manage column configurations, click **Create new**.
3. Select an artifact from the left navigation menu. For each applicable artifact, you can make the following changes:
   - Select the columns you want to include or exclude.
   - To reorder the columns, drag and drop the column names to your preferred order.
   - To customize the sort order for a column name, from the **Sort order** drop-down, and select a sorting method. Use the arrows to indicate ascending (▲) or descending (▼) order.
4. Click **Save and close**.

Edit a column configuration

You can edit all user-created column configurations, but not system-created ones.

1. Click **Tools** > **Manage export / report settings**.
2. Under Manage column configurations, hover over the column configuration you want to change and click **Edit**.

   > Tip: If you want to create a column configuration using an existing one as the basis, including a system-created one, you can **Duplicate** the column configuration first, and then edit the copy.

3. Select an artifact from the left navigation menu. For each applicable artifact, you can make the following changes:

- Select the columns you want to include or exclude.
- To reorder the columns, drag and drop the column names to your preferred order.
- To customize the sort order for a column name, from the **Sort order** drop-down, and select a sorting method. Use the arrows to indicate ascending (▲) or descending (▼) order.

4. Click **Save and close**.

Import a column configuration

You can import another user's column configuration to use for your own exports.

1. Click **Tools** > **Manage export / report settings**.
2. Under Manage column configurations, click **Import**.
3. Browse to the JSON file that contains the column configuration and click **Open**.

Export a column configuration

You can export a column configuration so that other examiners can use it in their own exports.

1. Click **Tools** > **Manage export / report settings**.
2. Under Manage column configurations, hover the mouse over the column configuration you want to export and click **Export**.
3. Browse to the folder where you want to save the JSON file.
4. Enter a name for the file, and then click **Save**.

MERGE EVIDENCE BACK INTO THE ORIGINAL CASE

To learn about merging evidence in AXIOM, select one of the topics below.

Merge a portable case back into the original case

After you've exported a portable case for a non-AXIOM user to investigate, you can merge the portable case back into your original case. To learn more about creating and sharing portable cases, see Use portable case to collaborate on cases with others.

In AXIOM Examine, you can merge a portable case into your case. Merging a portable case allows you to import tags and comments (including those applied in the Timeline explorer), media categorizations, and profiles that other stakeholders have added to the portable case, and combine them with your own notes in the case.

Note: You can't merge two portable cases together. The portable case must be merged with the original case it was created from.

1. In AXIOM Examine, click **File** > **Merge portable case**.
2. In the window that appears, follow the instructions to merge your portable case and choose what to include from it.

Merge tags and comments back into the original case

In AXIOM Examine: Click **File** > **Merge tags and comments**.

Import tags and comments from Magnet REVIEW

If you exported evidence for upload to Magnet REVIEW, the Magnet REVIEW user can create an export of the tags and comments they applied to the evidence during their investigation. After you receive this export from the Magnet REVIEW user, you can import and merge these tags and comments back into the original case.

To learn more about exporting evidence for use in Magnet REVIEW, see Export evidence for Magnet REVIEW.

Information included in tags and comments exports from Magnet REVIEW

> Export tags and comments is only for evidence sources that were created in Magnet AXIOM. If your case contains evidence sources from different forensic tools, Magnet REVIEW will only export the tags and comments for Magnet AXIOM sources.

Magnet REVIEW exports the following information from your case:

- Tags
  - A reference list of all items that were tagged.
  - A list of the tags included in the case.
- Comments
  - A reference list of all items that have comments applied.
  - All public comments for each item.

How tags and comments from Magnet REVIEW appear in AXIOM Examine

Magnet REVIEW exports all tag and comment content. However, you can refine what is imported into AXIOM Examine through the import process, including which tags or comments you would like to include.

Tags imported into AXIOM Examine will not include the username that assigned the tag. However, comments will include the username that created the comment as well as the date/-time.

CUSTOMIZE AXIOM SETTINGS

To learn about customizing settings in AXIOM, select one of the topics below.

Customize processing settings

Set a default case type

When adding Case details, use the Case type field to specify the type of case you're processing. You can set a default Case type when creating new cases in AXIOM Process.

1. In AXIOM Process, on the **Tools** menu, click **Settings**.
2. In **Preferences** > **Case type**, select a default case type.
3. Click **Okay**.

Enhanced picture categorization of video

AXIOM pulls frames from a video to create a collage of thumbnail images. Magnet.AI can detect potential hits from these video thumbnails. The number of individual frames included in the video thumbnail collage is not constant as it is determined dynamically based on the video length and other factors. For more information about how the video thumbnail collage is created, log in to the Support Portal to read the following article: Video thumbnail collage creation process.

To improve Magnet.AI picture categorization potential, turn on **Enhanced categorization** to create higher resolution individual frame samples.

1. In AXIOM Process, on the **Tools** menu, click **Settings**.
2. In **Preferences** > **Enhanced picture categorization of video**, select the **Enhanced**

categorization option.

3. Click **Okay**.

Save temporary files to a custom location

By default, AXIOM Process stores all temporary files associated with a case to the Cases folder.

1. In AXIOM Process or AXIOM Examine, on the **Tools** menu, click **Settings**.
2. In **Processing** > **Temporary file location**, in the drop-down list, click **Custom location**.
3. Click **Browse** and select the folder where you want to save all temporary files associated with a case.
4. Click **Okay**.

Image hashing and image hash verification

Image hashing

AXIOM Process can calculate a hash value for each evidence source that's being acquired as an E01 or AFF4. This hash value acts like a digital fingerprint for the image, and you can use it to verify that the file has not been tampered with. Hash verification information gets written to the Case Information.txt and .xml files. You can include Image hash verification results in the case dashboard's scan summary in AXIOM Examine. By default, creating hash values for images is turned off.

> If hash verification fails for an AFF4 logical image, the Case Information.txt file lists the files that the verification fails on, but omits the actual hash values for the failed files. To see the hash values for the failed files, refer to the Case Information.xml file.

1. In AXIOM Process, on the **Tools** menu, click **Settings**.
2. In **Processing** > **Image hashing**, select the **Verify the hash value of each acquired image file (E01 and AFF4 only)** option.
3. Click **Okay**.

Image hash verification

When image hashing is enabled, hash verification information gets written to the Case Information.txt and .xml files. You can also include the image hash verification results in the case dashboard's scan summary in AXIOM Examine. Hash verification results are available for E01 and AFF4 images only.

1. In AXIOM Process, on the **Tools** menu, click **Settings**.
2. In **Processing** > **Image hash verification**, select the **Verify the hash value of each image file (E01 and AFF4 only)** option.
3. Click **Okay**.

Turn on Passware encryption features

Using a third-party plugin available from Passware, Inc., AXIOM Process supports the recognition and full disk decryption of drives with a known password or recovery key. When you turn this feature on, future AXIOM Processsoftware updates will also include updates to the Passware plugin.

1. In AXIOM Process, on the **Tools** menu, click **Settings**.
2. In **AXIOM Process settings** > **Passware encryption features**, select the **Turn on encryption and drive decryption features using the Passware plugin** option.
3. Click **Okay**.

Remove the Passware plugin

When you turn off the recognition and full disk decryption of drives feature and restart AXIOM Process, you remove all of the Passware plugin components from your computer. Future AXIOM Process software updates will no longer include updates to the Passware plugin.

1. In AXIOM Process, on the **Tools** menu, click **Settings**.
2. In **AXIOM Process settings** > **Passware encryption features**, clear the **Turn on encryption and drive decryption features using the Passware plugin** option.
3. Click **Okay**.

4. When prompted to remove the Passware plugin, click **Remove**.
5. When prompted, manually restart AXIOM Process.

Connect to the internet using a system proxy

If your agency requires that you use AXIOM Process through a proxy server, you can still use AXIOM Cloud to acquire users' accounts for the following platforms: Box.com, Dropbox, Facebook, Google, Instagram, Lyft, Mega, Microsoft, and Lyft. When AXIOM Process detects a proxy internet connection, it automatically connects to the server using the proxy settings on your computer or prompts you to type your credentials for the server if applicable.

> Note: AXIOM Process currently supports HTTP proxies and not SOCKS4/5 proxies.

To change your proxy settings:

1. In AXIOM Process, on the **Tools** menu, click **Settings**.
2. In **AXIOM Process settings** > **Local area network (LAN) connection settings**, select one of the following settings:
   - If your proxy settings are configured on your computer, select **User system proxy settings**.
   - If you have more than one proxy server available, select **Manual proxy configuration** and provide the hostname and port number.
3. Click **Okay**.

Deduplicating artifact results

When scanning an evidence source, AXIOM Process parses allocated space and carves data from across the entire image (whether it's allocated or unallocated, and a recognized file system or not). By carving data from the entire image, AXIOM Process can uncover files or fragments of data vital to your investigation—however, you're more likely to have duplicate data in your case. Most commonly, AXIOM Process could report the same file recovered through both parsing and carving techniques.

By default, AXIOM Process deduplicates artifact results in your case to help reduce the amount of data you need to examine.

As part of the deduplication process, AXIOM Process looks at the essential information fragments for each artifact and the source of the artifact (the source representing where the data is found and is presented by the Source column in AXIOM Examine), and then assigns a unique value to the artifact. When AXIOM Process encounters a duplicate of an existing unique value, only the first artifact with a unique value is kept. Other artifacts with the identical unique value are discarded as duplicates. For example, with pictures, the unique value is based on the hash of picture. If two pictures are found with the same hash and source, they would be deduplicated.

While parsed hits are always kept (they always have a different source), AXIOM Process will discard duplicates of the hit with the same unique value that were recovered through carving (carved hits will often be incomplete and contain only partial data).

If an identical artifact is found in two different locations (i.e. the source is different), AXIOM Process will not discard the artifact from one location. AXIOM Process treats each path as a unique source, so the artifact will appear in both locations. For example, if an identical picture is discovered in two different places–a downloads folder and a temp folder–the artifact wouldn't be discarded as a duplicate from one location.

For deleted files recovered from unallocated space, only the first artifact with a unique value is kept. If the same artifacts are found in unallocated space on different drives, both artifacts are kept because the sources are different.

For searches of NTFS and FAT file systems, AXIOM Process will automatically deduplicate results from unallocated space if they are covered by a range of space that's occupied by a known deleted file. Only the deleted file hit with an existing $MFT record will be shown in AXIOM Examine. If no $MFT record exists, the hit will be carved from unallocated space.

Remove duplicate artifact results

1. In AXIOM Process, on the **Tools** menu, click **Settings**.
2. In **Processing** > **Duplicates**, select the **Remove duplicates** option.
3. Click **Okay**.

Optimize search times

The easiest way to decrease scan times and increase performance is to add more CPU cores to your system. AXIOM Process is designed to create a separate thread for every core that's available in your system (currently, the upper limit is 32 cores). For the fastest search time, AXIOM Process uses all logical cores on your computer (to a maximum of 32 cores). If you want to use your computer for other tasks during a search, reduce the number of cores. Increasing the clock speed of your CPU is another way that you can improve performance.

In AXIOM Process, you can manually set the number of cores that you want to use:

1. In AXIOM Process, on the **Tools** menu, click **Settings**.
2. Under **Processing** > **Search speed**, in the **Number of cores** drop-down list, select the number of cores you want to use.
3. Click **Okay**.

> Note: Adding additional cores does not improve performance in a linear way. The more cores that your system has, the more work it is for RAM to keep each core busy with new instructions to process. As the number of cores increases, the returns on performance diminish. Whereas increasing the number of cores from 4 to 8 will yield significant improvements, increasing from 8 to 16 has a less noticeable effect. After 8 cores, the easiest way to improve performance is by increasing clock speed.

Optimize the performance of Magnet.AI

To find similar pictures, Magnet.AI must create a large database. For optimal performance of this feature, follow the recommendations below.

- Make sure you have enough space to store the data. Each picture needs approximately 8 KB of space to store the data that Magnet.AI produces.
- Store your case files on an SSD rather than a fixed or external drive. While Magnet.AI can analyze pictures stored on fixed or external drives, performance will not be as efficient.

- Use a computer with a GPU. When you build picture comparison using Magnet.AI, if AXIOM Process detects a GPU on your computer with more than 126 MB of free memory, it automatically attempts to use it. Using a GPU instead of a CPU can significantly decrease the time it takes to build picture comparison.

For recommended system requirements, review the System requirements: Magnet AXIOM and Optimize the performance of Magnet AXIOM articles in the Support Portal.

Change the display language

Changing the display language for AXIOM Process also changes the display language for AXIOM Examine (and the other way around).

1. InAXIOM Process orAXIOM Examine, on the **Tools** menu, click **Settings**.
2. In the **AXIOM Process settings** or **AXIOM Examine** section, in the **Language** drop-down list, click the language that you want to use, and then click **Okay**.
3. To restart and apply the change, click **Now**.

Enable additional features in AXIOM Cyber

By default, the features of AXIOM Cyber are optimized to best support and streamline enterprise investigations. You can turn on additional features related to media grading and categorization.

1. In AXIOM Process or AXIOM Examine, on the **Tools** menu, click **Settings**.
2. In the Settings window, click **AXIOM Examine**.
3. Under **Additional AXIOM features**, select the checkbox.
4. Click **Okay**.
5. In the window that appears, click **Restart now**.

When AXIOM Process or AXIOM Examine restarts, the additional features will be available. If both AXIOM Process and AXIOM Examine are open when you change the setting, you must restart both applications to use the additional features. For more information, sign in to the Support Portal to read the following article: Enable additional AXIOM features in AXIOM Cyber.

Integrate Magnet Hash Sets Manager with AXIOM Process or AXIOM Examine

You can Find matching hashes using Magnet Hash Sets Manager with AXIOM Process and AXIOM Examine to upload and manage multiple hash sets in a single centralized database.

1. In AXIOM Process or AXIOM Examine, on the **Tools** menu, click **Settings**.
2. In the Settings window, click **Product integrations**, and select **Hash Sets Manager**.
3. Provide a server IP address and port, then click **Connect to server**.
4. After the connection is successful, click **Okay**.

Configure GrayKey/VeraKey discovery settings

AXIOM Process can be integrated with GrayKey or VeraKey to automatically download and process Android and iOS images. For more information about the requirements and configuration of GrayKey Verakey discovery service, sign in to the Support Portal to read the following article: GrayKey/VeraKey discovery image processing in AXIOM Process

1. In AXIOM Process, on the **Tools** menu, click **Settings**.
2. In Product Integrations, select **GrayKey/VeraKey Discovery**.
3. Provide the **port number** that has been configured for communication with the GrayKey/VeraKey appliance.
4. Select the location for AXIOM Process to receive completed GrayKey and VeraKey images.
5. Select the location to save processed case files. Each processed image will be a separate case.
6. Click **Start service** to initiate the discovery service. Restart the service to apply any changes made to the GrayKey/VeraKey discovery settings.

Customize imaging settings

Create segments for Android and drive images

You can specify the size of the image segments that you want AXIOM Process to create when it acquires evidence from Android and drive images. Each option represents a different size that reflects its storage capabilities. By default, image segmentation is turned off.

1. In AXIOM Process, on the **Tools** menu, click **Settings**.
2. In **Imaging** > **Image segmentation**, select a format from the drop-down list.
3. Click **Okay**.

Create a hash value for evidence sources

AXIOM Process can create hash values for each evidence source that it acquires. By default, image hashing is turned off.

1. In AXIOM Process, on the **Tools** menu, click **Settings**.
2. In **Imaging** > **Image hashing**, select the **Calculate a hash value for each evidence source that's being acquired** option.
3. Click **Okay**.

Verify hash values for acquired images

AXIOM Process can create a hash value for acquired E01 images and compare it to the hash value of the source image. This process verifies that the image has not been altered. Hash verification information gets written to the Case Information.txt and .xml files. By default, image hash verification is turned off.

1. In AXIOM Process, on the **Tools** menu, click **Settings**.
2. In **Imaging** > **Image hashing**, select the **Verify the hash value of each image (E01 image files only)** option.

Compress images

You can compress the E01 images that AXIOM Process acquires. The **Fast** option provides some compression in a reasonable amount of time. The **Best** option provides the best possible compression, but can take much longer than the fast option. By default, image compression is turned off.

1. In AXIOM Process, on the **Tools** menu, click **Settings**.
2. In **Imaging** > **Compression**, select a compression method.
3. Click **Okay**.

Restore mobile device state for Android devices

While AXIOM Process acquires evidence from Android devices, it installs an agent application onto the device to assist with recovering data. When the scan completes, AXIOM Process can remove the agent application from the device. By default, the agent application is left on the device.

1. In AXIOM Process, on the **Tools** menu, click **Settings**.
2. In **Imaging** > **Restore mobile device state**, select the **Remove agent application** option.
3. Click **Okay**.

Customize examining settings

Adjust the appearance of your case in AXIOM Examine

When you adjust one of the following settings, it will only apply to the case you currently have open.

Make text easier to read by changing the encoding of an artifact

Sometimes, AXIOM Examine does not apply the correct encoding to an item, which causes some characters to become difficult to read. You can choose to change the encoding for a single item, a collection of items, or a whole artifact on a per-attribute basis.

1. In AXIOM Examine, in the Artifacts explorer, select the items you want to change character encodings for.
2. Right-click the selected items and click **Change encoding**.
3. Select your desired encoding settings from the drop-down lists, and then click **Okay**.

Reset your case view

You can revert your case view in AXIOM Examine back to what you see when you first open a case. Resetting your case view forces AXIOM Examine to revert any viewing customizations you set, such as collapsed or expanded information and applied filters.

1. In AXIOM Examine, on the **File** menu, click **Refresh case**.

Customize AXIOM Examine settings across cases

When you adjust one of the following settings, it persists across cases in AXIOM Examine.

Set the default explorer

Although you can use any explorer to browse the evidence in your case, by default, AXIOM Examine opens the Case dashboard explorer. You can change your default explorer.

1. In AXIOM Examine, on the **Tools** menu, click **Settings**.
2. In the Settings window, click **Preferences**.
3. In the **Default explorer** drop-down list, click the explorer that you want to make your default.
4. Click **Okay**.

Change the default view

By default, AXIOM Examine opens the Column view. You can change your default view.

1. In AXIOM Examine, on the **Tools** menu, click **Settings**.
2. In the Settings window, click **Preferences**.
3. Under **Default view**, in the drop-down list, click the view that you want to make your

default.

4. Click **Okay**.

Change the default explorer for the Relative date / time and Similar pictures filters

By default, when you apply the Relative date / time filter, AXIOM Examine displays the results in the Timeline explorer. When you find similar pictures, AXIOM Examine automatically displays the results in the Media explorer. You can change these settings to display the results in another explorer, or choose the **Current explorer** option to display the filtered results in the explorer where you begin the query.

1. In AXIOM Examine, on the **Tools** menu, click **Settings**.
2. In the Settings window, click **Preferences**.
3. Under **Default explorer for filter results**, select an explorer option from either the **Relative date / time filter** or **Similar pictures filter** drop-down list.
4. Click **Okay**.

Set the folder structure for saved files

When you save files from your case to a file / folder, you can set AXIOM Examine to export them in a flat structure with all files in a single folder or maintain the folder structure of the original evidence source. Choose to maintain the original folder structure if your investigation requires that you preserve all time stamps and file locations.

1. In AXIOM Examine, on the **Tools** menu, click **Settings**.
2. In the Settings window, click **Preferences**.
3. Under **Folder structure for saved files**, select one of the options.
4. Click **Okay**.

Allow internet connection from the Preview card

You can allow users to connect to the internet using links in the Preview card. By default, this option is turned off to prevent users from attempting to navigate to websites that might not be secure, or that they might not be authorized to access.

1. In AXIOM Examine, on the **Tools** menu, click **Settings**.
2. In the Settings window, click **Preferences**.
3. Under **Preview card**, select **Allow the preview card to connect to the internet**.
4. Click **Okay**.

Allow video scrubbing in the Media explorer

When you view videos in the Media explorer, you can hover your mouse over a thumbnail to scroll through a preview of the video.

1. In AXIOM Examine, on the **Tools** menu, click **Settings**.
2. In the **Settings** window, click **Preferences**.
3. Under Media preview, select **Allow video scrubbing in the media explorer**.
4. Click **Okay**.

Allow preview when hovering over thumbnails

When you view media in the Artifacts explorer in thumbnail view, you can hover your mouse over a thumbnail to view a larger preview.

1. In AXIOM Examine, on the **Tools** menu, click **Settings**.
2. In the **Settings** window, click **Preferences**.
3. Under Media preview, select **Allow preview when hovering over media in the thumbnail view**.
4. Click **Okay**.

Allow the Email explorer to tag email attachments

Note: This feature is only available for AXIOM Cyber users.

When you tag email evidence in the Email explorer, AXIOM Examine can automatically tag emails and attachments together.

1. In AXIOM Examine, on the **Tools** menu, click **Settings**.
2. In the **Settings** window, click **Preferences**.

3. Under **Tagging in Email explorer**, select **Tag the email and its attachments together**.
4. Click **Okay**.

Change the display theme

By default, AXIOM Examine runs in light mode. You can switch to dark mode to reduce eye strain when you spend long periods of time examining evidence.

1. In AXIOM Examine, on the **Tools** menu, click **Settings**.
2. In the Settings window, click **Preferences**.
3. Under **Display theme**, select **Dark mode** or **Light mode**.
4. Click **Okay**.
5. To restart and apply the change, click **Restart Examine**.

Change the display language

Changing the display language for AXIOM Process also changes the display language for AXIOM Examine (and the other way around).

1. InAXIOM Process orAXIOM Examine, on the **Tools** menu, click **Settings**.
2. In the **AXIOM Process settings** or **AXIOM Examine** section, in the **Language** drop-down list, click the language that you want to use, and then click **Okay**.
3. To restart and apply the change, click **Now**.

Set a default time zone

You can select a time zone to use as the default time zone in your cases.

1. In AXIOM Examine, on the **Tools** menu, click **Manage date / time format**.
2. In the **Time zone** drop-down list, click the time zone you want to default to.
3. Select **Set this time zone as the default for all cases**.
4. Click **Okay**.

Build explorers automatically

Some explorers in AXIOM Examine require you to build them in each case. You can also adjust your settings so that AXIOM Examine automatically builds them after your case has been processed.

1. In AXIOM Examine, click **Tools** > **Settings**.
2. In the Settings window, click **Processing**.
3. Under Post-processing, select the option to automatically build the relevant explorer on case open.

Turn on Software rendering mode to reduce crashes with an outdated GPU or video driver

By default, AXIOM Examine runs in Hardware rendering mode. When AXIOM Examine detects a crash related to rendering, it will automatically turn on Software rendering mode to avoid a similar crash. We don't recommend running AXIOM Examine in Software rendering mode long-term. Make sure that you update your drivers and Windows to the latest versions. After completing these updates, turn off Software rendering mode.

For more information about Software rendering mode, log in to the Customer Portal to read the following article: Running AXIOM Examine in Software rendering mode.

1. In AXIOM Examine, on the **Tools** menu, click **Settings**.
2. In the Settings window, click **Processing**.
3. Under **Software rendering mode**, select **Run AXIOM Examine in Software rendering mode**.
4. Click **Okay**.
5. To restart and apply the change, click **Now**.

Enable additional features in AXIOM Cyber

By default, the features of AXIOM Cyber are optimized to best support and streamline enterprise investigations. You can turn on additional features related to media grading and categorization.

1. In AXIOM Process or AXIOM Examine, on the **Tools** menu, click **Settings**.
2. In the Settings window, click **AXIOM Examine**.

3. Under **Additional AXIOM features**, select the checkbox.
4. Click **Okay**.
5. In the window that appears, click **Restart now**.

When AXIOM Process or AXIOM Examine restarts, the additional features will be available. If both AXIOM Process and AXIOM Examine are open when you change the setting, you must restart both applications to use the additional features. For more information, sign in to the Support Portal to read the following article: Enable additional AXIOM features in AXIOM Cyber.

Set default route settings

For route view, you can select a default distance and time interval for generating routes.

1. In AXIOM Examine, on the **Tools** menu, click **Settings**.
2. In the Settings window, click **Maps and routes**.
3. Under **Default route distance and time**, provide a default number in each of the text boxes.
4. Click **Okay**.

Integrate external products and features with AXIOM Examine

From AXIOM Examine, you can integrate products and features to enhance your use of AXIOM and allow collaboration with other investigators. When you integrate a product or feature, AXIOM will remain connected to it across your cases.

Integrate Magnet Hash Sets Manager to find matching hashes

Configure Find matching hashes using Magnet Hash Sets Manager to synchronize hash sets across each workstation running AXIOM.

1. In AXIOM Process or AXIOM Examine, on the **Tools** menu, click **Settings**.
2. In the Settings window, click **Product integrations**, and select **Hash Sets Manager**.
3. Provide a server IP address and port, then click **Connect to server**.
4. After the connection is successful, click **Okay**.

Integrate the Magnet Prague beta to find matching identifiers

Configure the Magnet Prague beta to search for matching identifiers in your team's cases. To learn more about Magnet Prague, log in to the Support Portal to read the article Search for identifier matches in AXIOM using Magnet Prague.

1. In AXIOM Examine, on the **Tools** menu, click **Settings**.
2. In the Settings window, click **Product integrations**.
3. Under Product integrations, select **Magnet Prague**.
4. Enter the server address and port number where you installed Magnet Prague and click **Connect to server**.

> Tip: If you are connecting to Magnet Prague on the same computer where you installed it, the default settings are:
>
> - Server address: 127.0.0.01
> - Port number: 18443

Integrate Magnet REVIEW to upload cases to your organization's server

Configure AXIOM Examine to be able to upload evidence directly from your case to Magnet REVIEW. You only need to do this configuration once for each instance of Magnet AXIOM.

1. In AXIOM Examine, on the **Tools** menu, click **Settings**.
2. In the Settings window, click **Product integrations**.
3. Under Product integrations, select **Magnet REVIEW**.
4. Enter your organization's Magnet REVIEW **Server URL** and **API key**.
5. Click **Okay**.

To learn more, see Export evidence for Magnet REVIEW

Connect to an offline map server

If you're working on a computer without internet access, you can connect to an offline map server that your organization has set up.

Note: To learn more and troubleshoot connection issues, sign in to the Support Portal to view the article Connecting to an offline map server.

1. In AXIOM Examine, click **Tools** > **Settings** > **Maps**.
2. Under Maps, select the option to **Connect to an offline map server**.
3. Provide a **Server address**, and then click **Connect to server**.
4. If the connection is successful, click **Okay**.

Customize log collection and diagnostics

Collect log information

While it's running, AXIOM Process can collect log information that you can use to help track progress and troubleshoot potential issues. Turning on logging can slow down performance, so you should only turn it on when necessary. You can find the log file for AXIOM Process at: C:\AXIOM\Cases\*<case name>*.

1. In AXIOM Process, on the **Tools** menu, click **Settings**.
2. In **Processing > Logging**, select the **Turn on logging** option.
3. Click **Okay**.

Enhanced file source exception reporting

Enhanced file source exception reporting will result in a more detailed level of logging appearing in the log.txt and sources.log files. Once the scan is complete, a summary of the file source exceptions will be available in the case dashboard's scan summary in AXIOM Examine.

For more information about the types of issues that may occur, their impact, and what actions investigators can take to further investigate the reported exceptions, sign in to the Support Portal to read the following article: AXIOM Process scan exceptions.

Note: The source.log file will be overwritten if you add new evidence to an existing case. If you want to preserve the results of the previous scan, rename the source.log (for example: scan1.-log), or save a copy of the source.log to a folder that is different to the case folder.

1. In AXIOM Process, on the **Tools** menu, click **Settings**.
2. In **Processing > Enhanced file source exception reporting**, select the **Enable enhanced logging in the log.txt and sources.log** option.
3. Click **Okay**.

Send diagnostic information

You can choose to share information about how you use the product with Magnet Forensics. This information can help us improve our products. The type of information that gets sent can include data about how long it took to perform a search and the processing options you used in the search. The information that gets sent *never* includes actual data from the evidence sources that you search.

By default, the collection of diagnostic information is turned off.

1. In AXIOM Process or AXIOM Examine, on the **Tools** menu, click **Settings**.
2. In the **AXIOM Process settings** or **AXIOM Examine** section, under **Diagnostic information**, select the **Automatically gather and send diagnostic information** option.
3. Click **Okay**.

KEYBOARD SHORTCUTS IN AXIOM EXAMINE

Keyboard shortcuts allow you to complete actions by using a key or a combination of keys instead of your mouse.

AXIOM Examine supports keyboard shortcuts on standard QWERTY keyboards.

CTRL + A	Select all
CTRL + C	Copy
CTRL + V	Paste
CTRL + X	Cut
CTRL + B	Manage tags in the Evidence window
CTRL + D	Apply the *Bookmark* tag
CTRL + O	Open a case you have saved on your computer
CTRL + R	Go to the next page in the timeline graph
CTRL + L	Go to the previous page in the timeline graph
CTRL + G	Go to a date range in the timeline
CTRL + PLUS SIGN (+)	Zoom in to the timeline
CTRL + MINUS SIGN (-)	Zoom out in the timeline
CTRL + 1	Apply the *Evidence* tag
CTRL + 3	Apply the *Of interest* tag
CTRL + Z	Undo last grading in the Media explorer
F1	Open the online user guide
SPACEBAR	Click a button, select a check box, select an option or apply the *Bookmark* tag (depending on active user interface control)
ENTER	Equivalent to clicking **Okay** when an option is selected in a menu

ESC	Exit or close a window or filter
PLUS SIGN (+)	Set all visible uncategorized pictures in Thumbnail view to a media category you choose
0 - 9	Apply a media category to the selected the picture or pictures in Thumbnail view
ALT + F4	Quit application
ALT + ENTER	Start a new paragraph line in the **Comments** field
ALT + Number	Switch between explorers. View the number that corresponds to each explorer in the explorer drop-down list.
ALT + SHIFT + Number	Switch between views (for example, Conversation view, Column view, and so on). View the number that corresponds to each view in the view drop-down list.
ALT + Left arrow	Expand or collapse **Navigation**
ALT + Down arrow	Expand or collapse **Tags, profiles & media categories** Tags, comments & profiles
ALT + Right arrow	Expand or collapse **Details**

UPDATE THE PRODUCT

To update to the latest version, download and run the incremental update. Incremental updates include only the changes that have been made to the software since you last updated it, which decreases the time it takes to update.

Only recent versions support incremental updates. If you're running a version that is more than six months old, you must download the entire update from the Customer Portal.

Update while online

1. In AXIOM Process or AXIOM Examine, on the **Help** menu, click **Check for updates**.
2. In the **Update available** window, click **Update**.
3. Follow the instructions in the setup wizard.

Update while offline

If your computer does not have an internet connection, you can download the update on another computer, copy it onto a USB drive, and then transfer it to your computer.

1. In AXIOM Process or AXIOM Examine, on the **Help** menu, click **Check for updates**.
2. Copy the download link from the **Check for updates** window.
3. On a computer that is connected to the internet, open a web browser and paste the link into the address bar.
4. Download the .zip file.
5. Copy the .zip file to a storage device such as a USB key.
6. Connect the USB key to the offline computer and extract the contents of the .zip file.
7. Double-click the installer and follow the instructions in the setup wizard.

Turn off software updates

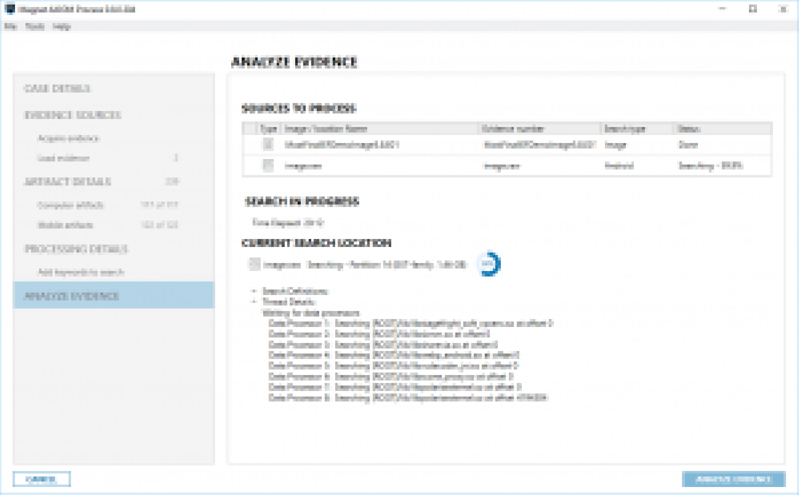
Each time AXIOM Process starts, it automatically checks for software updates. If you turn this option off, you must manually check the Customer Portal for updates.

1. In AXIOM Process or AXIOM Examine, on the **Tools** menu, click **Settings**.
2. In the **AXIOM Process settings** or **AXIOM Examine** section, under **Software updates**, clear the **Check for updates automatically** option.
3. Click **Okay**.

LEARN MORE

Before you set up AXIOM Process and run your first scan, watch some of these videos to get a better understanding of the tools and workflow.

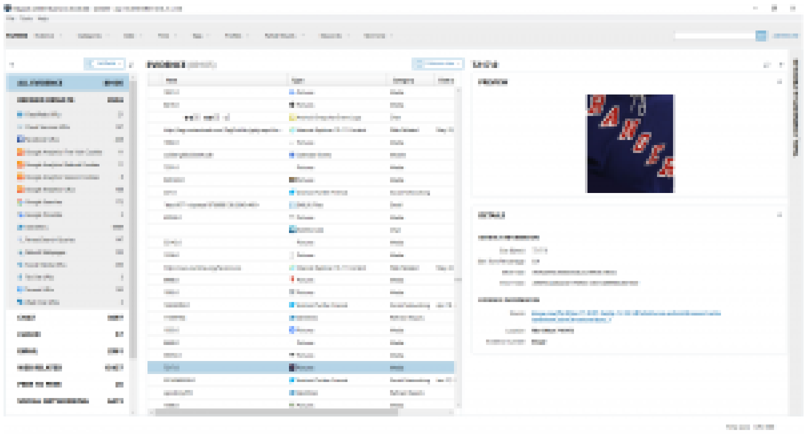
Acquiring and processing evidence



Discover how to use AXIOM Process to acquire and analyze all of your evidence in a single stage by queuing up multiple sources such as computers and smartphones. Select the artifacts you want to search for and customize the options you want to include.

WATCH

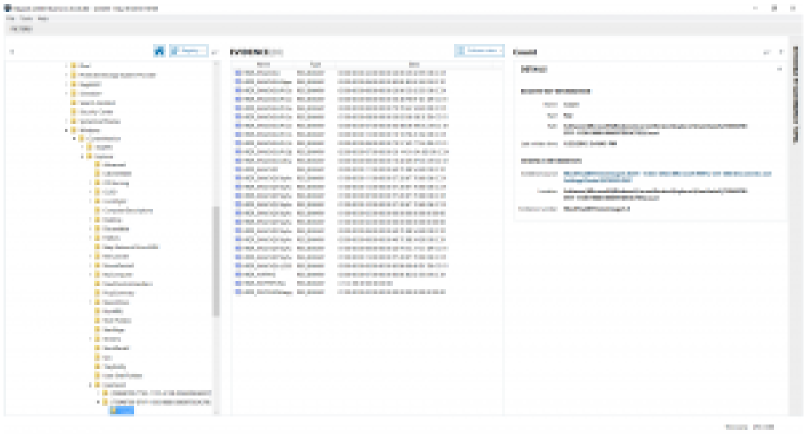
Navigating the file system, registry, and artifacts



Learn how to navigate through evidence using the File system and Registry explorers. You will also learn about key features and methods to search in the Artifacts explorer.

WATCH

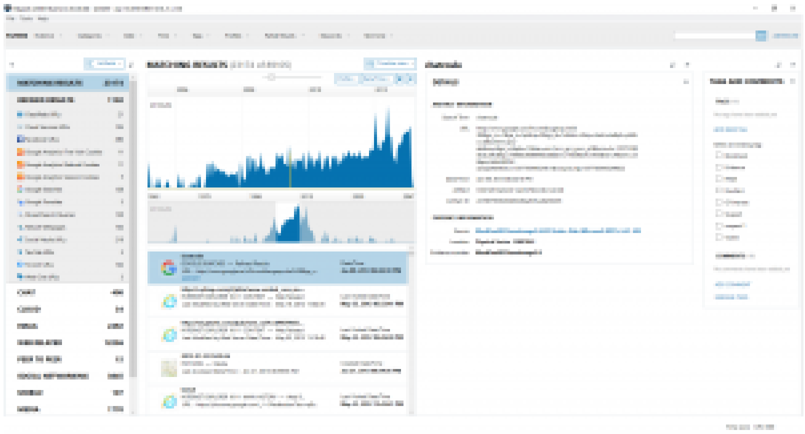
Source linking between the Artifacts, File system, and Registry explorers



With the added functionality of the Artifact, File system, and Registry explorers, source linking provides you a way to quickly navigate between these views without having to click through large file and folder structures. Source linking saves you time and helps you verify the artifacts and dig deeper into the raw data.

WATCH

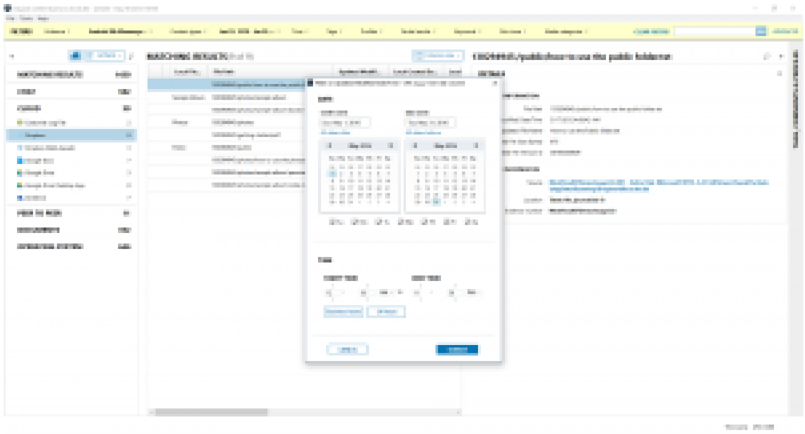
Examining evidence with centralized views



This video shows the various ways you can view evidence. Learn how to use the Chat threading, Classic, Column, Histogram, Row, Thumbnail, Timeline, and World Map views to present data in a way that makes sense to your examination.

WATCH

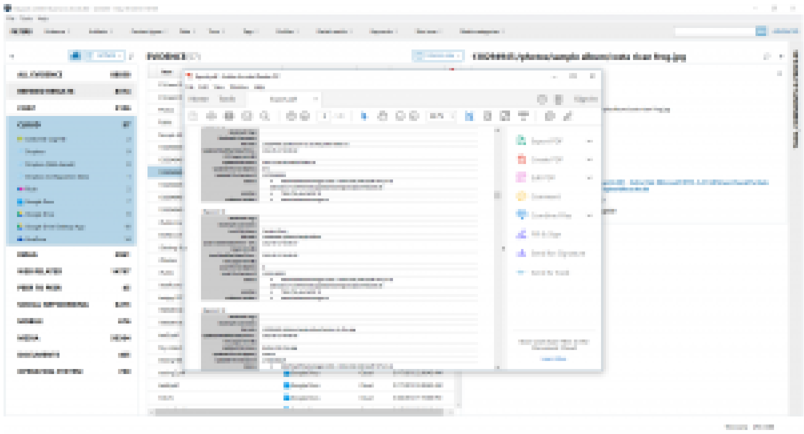
Searching and filtering in AXIOM Examine



Learn how you can use filter stacking to narrow the amount of data you need to analyze and minimize the scope of your investigation.

WATCH

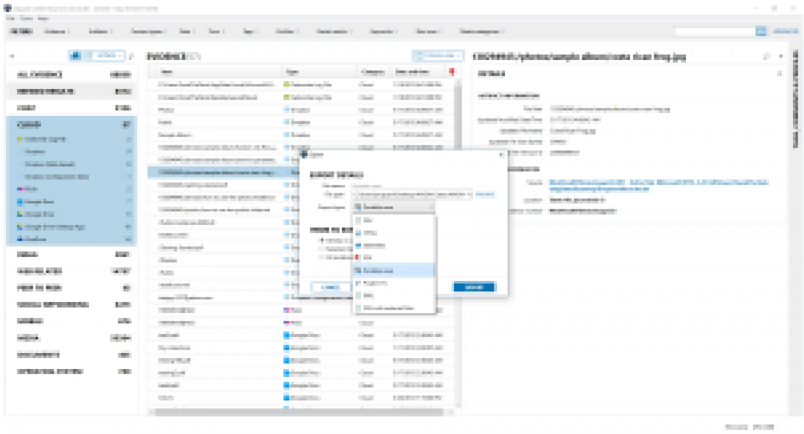
Organizing your exports with tags and comments



You can customize your exports directly in AXIOM Examine to cut down on any editing you have to do on the exports after you generate them. You can also use tags and comments to organize and explain your findings to all of your stakeholders.

WATCH

Collaborating with stakeholders using portable case



Often there are many people involved in an investigation who you need to share your findings with. Portable case enables you to share your data with other stakeholders such as lawyers or investigators who can work with you by adding their own tags, comments, and profiles to assist with the investigation. You can also merge their data back into the main case.

WATCH

Magnet Forensics

2220 University Ave. E., Suite 300

Waterloo, ON, N2K 0A8

1 (519) 342-0195

This document was published on 4/4/2024.