MAGNET AUTOMATE™

USER GUIDE

CONTENTS

MAGNET AUTOMATE

Magnet AUTOMATE is a platform that your organization can use to create a distributed workflow for digital forensic applications. Magnet AUTOMATE can help make evidence discovery more efficient by automating the steps between tasks, such as acquiring forensic images, searching the evidence source with AXIOM Process, and post-processing steps such as creating reports. You can integrate just about any application into your workflow provided that it has a command-line interface (CLI) or application programing interface (API).

AUTOMATE Essentials is a streamlined offering of Magnet AUTOMATE, which installs one controller and one node on a computer. It also includes several default workflows and configures default Magnet Forensics applications so that you can start creating cases right away.

AUTOMATE Enterprise provides the workflow building and automation functionality from Magnet AUTOMATE, while being tailored towards enterprise usage with its ability to acquire evidence from remote computers and the Microsoft cloud platform.

Assumptions

Before using Magnet AUTOMATE, this guide assumes that you:

- Understand that Magnet AUTOMATE is a tool that can help automate manual, repetitive tasks in the digital forensic process. However, forensic examiners must still be able to 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 a web browser.

What's new

Version	Description
3.19	• Updated View run logs to describe changes to the updated Log file tab.
3.18	• Updated View run logs to note that you can now export run logs while a case is processing.
3.17	• Created the Magnet AUTOMATE User Guide. • Added View case output and review evidence. • Added Help resources.

Common terms in Magnet AUTOMATE

The following are common terms in digital forensics and in the Magnet AUTOMATE 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 AUTOMATE (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 acquisition** - Acquisition of cloud evidence from a supported cloud platform, such as the Microsoft 365 platform.
- **Controller** - The computer (or VM) designated as the Magnet AUTOMATE server. The controller sends working instructions to the nodes and runs a web server that hosts the front end web application.
- **Custom field** - A field in Magnet AUTOMATE used to capture case details or evidence source details when a new case is being created.
- **Data validation** - When a workflow requires data to be moved or copied from one location to another, Magnet AUTOMATE can check the integrity of the data by hashing it before and after it has been moved or copied.
- **Element** - An object you can add to a workflow in Magnet AUTOMATE. Element types include: application, drive, image, hardware imager, merge, pass / fail, stop for merge, and watch folder. You can configure the settings for each element in a workflow.
- **Evidence item** - An artifact in Magnet AUTOMATE 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 template** - A template in Magnet AUTOMATE to streamline the exporting process by predetermining the export's artifact types, columns, and format options. When you create an export, you can save the settings for use in future exports.
- **Extraction** - The process of retrieving artifacts from an image.
- **Hardware imager** - A physical imaging device that creates an image (or copy) of the current state of another hardware device. You can add hardware imagers to your workflows, allowing you to automate the imaging process in your cases.

- **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.
- **Image path** - The default location for images in Magnet AUTOMATE so that users can choose the paths from a list instead of typing them in manually each time they create a case.
- **Keyword list** - A text file in Magnet AUTOMATE containing keywords and regular expressions to search for. Depending on the different types of cases that you process, you might have different keyword lists for each workflow.
- **Linear processing** - The most basic type of workflow in Magnet AUTOMATE is a linear workflow. In a linear workflow, each element is connected in a sequential order. Each step in the workflow must complete before the next one can start.
- **Merge workflow** - A workflow in Magnet AUTOMATE designed for cases that require multiple evidence sources merged into a single Magnet AXIOM case (for example, if you need a consolidated report for multiple evidence units).
- **Node** - The computer (or VM) in Magnet AUTOMATE where you intend to run workflow applications from. If your workflow uses only one node, you can install the node service on the same system where you installed the controller service. Nodes can have a specific function, such as imaging or processing, or you can configure all nodes in your network to perform any workflow task.
- **Node workspace** - A node's storage location in Magnet AUTOMATE for data such as logs and temporary files for the applications it runs.
- **Output path** - The default location in Magnet AUTOMATE where case output is saved to.

- **Parallel processing** - A parallel workflow in Magnet AUTOMATE can have multiple paths, each of which runs independently of the other paths. In this type of workflow, more than one application can run simultaneously, if they're on separate paths.
- **Password list** - A text file (.txt) in Magnet AUTOMATE that lists potential passwords to decrypt some types of encrypted images in your Magnet AUTOMATE workflows.
- **Portable case** - An export type in Magnet AUTOMATE that allows you to share the Magnet AXIOM case with an unlicensed user. In a portable case, you can browse artifacts and add tags and comments using an unlicensed version of AXIOM Examine and send those back to the owner to review and merge into the original case.
- **Remote acquisition** - Deploying an agent to remotely gather evidence from Windows, macOS, and Linux computers to complete targeted investigations on an as-needed basis.
- **Run log** - Displays logging information for a run in a central log, while the case is running and after it's complete. The run log lists output from each application in the order that the applications are run in the workflow. Logs also indicate which nodes are used to run each application.
- **Run summary** - Displays information about an individual workflow run in a case, such as the time of start and completion, paths to the output and source files, and the completion status.
- **Watch folder** - A workflow element in Magnet AUTOMATE that is mapped to a folder on a computer or shared network location. Magnet AUTOMATE watches the location for images. When Magnet AUTOMATE detects an image in that folder, it automatically creates a case and adds it to the dashboard.
- **Workflow** - A predefined sequence of events in Magnet AUTOMATE to automatically image and/or process evidence in a case. A workflow consists of a single source element (the type of evidence that the workflow is designed to process) and one or more application elements (the applications performing the imaging/processing).
- **Workflow application** - An application in a workflow to image or process evidence in Magnet AUTOMATE. This can be a hardware imager, forensic application, or another third-party tool.

- **Workflow variables** - Values in Magnet AUTOMATE that aren't specified until you run a case. For example, the ${DRIVE} variable is defined during case creation when you select a drive to process. Each of the variables that are available for use are displayed in the Command-line variables pane when configuring your applications.
- **Workflow plugin** - A pair of JSON and PowerShell files located in a unique folder, containing the variables, parameters, and arguments required to run an application in a workflow. In Magnet AUTOMATE, a workflow plugin can simplify setting up an application, enabling reuse in multiple workflows.

Roles in Magnet AUTOMATE

Magnet AUTOMATE has two types of roles, each with a distinct set of permissions. Depending on your organization, you may have a single user or multiple users that fulfill multiple roles and responsibilities in Magnet AUTOMATE.

- **Admin** - This role has full access in Magnet AUTOMATE, with all pages and functionality visible. Admins can set up and manage users, nodes, applications, case types, workflows, hardware imagers, workflow plugins, and global settings for workflows. Admins can also create cases using workflows. A lab manager or forensic examiner could fulfill the admin role.
- **User** - This role has limited access in Magnet AUTOMATE, with some pages and functionality visible. Users can manage their profile and create cases using workflows. A forensic examiner could fulfill the user role.

Role permissions

Task	Admin	User
View the Dashboard	Yes	Yes
View the Cases page	Yes	Yes
View the Configuration pages	Yes	No
View the Settings pages	Yes	No
Add nodes and applications	Yes	No

Task	Admin	User
Configure global settings	Yes	No
Manage workflows (create, edit, import, export)	Yes	No
Create cases	Yes	Yes
Manage all users' cases (cancel, delete, prioritize case queue, retry)	Yes	No
Manage their own cases (cancel, delete, retry)	Yes	Yes
View and edit personal account settings; export personal account activity	Yes	Yes
Manage users (add users, edit user profiles, delete users, view user account activity)	Yes	No

Help resources

Product documentation

The following Magnet AUTOMATE product documentation is available from the Support Portal:

- **Magnet AUTOMATE System Requirements (PDF)** - overview of Magnet AUTOMATE architecture and system requirements. This guide is for users with the Admin role and IT stakeholders.
- **Magnet AUTOMATE Administrator Guide (PDF/HTML)** - install Magnet AUTOMATE, manage users, set up nodes and workflow applications, configure global settings for workflows and cases, add custom fields for case and evidence details, set up hardware imagers, monitor and report on system usage and performance, backup and data recovery, and troubleshooting. This guide is for users with the Admin role.
- **Magnet AUTOMATE Workflow Builder Guide (PDF/HTML)** - create basic and advanced workflows, export and import workflows, create workflow plugins, and integrate additional applications and tools. This guide is for users with the Admin role.
- **Magnet AUTOMATE User Guide (PDF/HTML)** - manage your user profile, create cases, monitor case status, view case output and review evidence, monitor and report on system usage and performance, and troubleshooting. This guide is for users with

the User role.

- **Magnet AUTOMATE Essentials Quick Start Guide (PDF)** - install and configure AUTOMATE Essentials, create a case, monitor the status of a case, view case output and review evidence, and troubleshooting. This guide is for users with the Admin and User roles.
- **Magnet AUTOMATE Quick Start Guide (PDF)** - install and configure the controller and one node on a computer, and then create a simple workflow and case. This guide covers the basics of installing, configuring, and using Magnet AUTOMATE and is for users with the Admin and User roles.
- **Magnet AUTOMATE CLI Reference (PDF/HTML)** - integrate applications into workflows using the CLI. This guide is for users with the Admin role.
- **Magnet AUTOMATE API Reference (HTML)** - integrate applications into workflows using the Magnet AUTOMATE Rest API. This guide is for users with the Admin role.
- **Magnet AUTOMATE Release Notes (HTML)** - the latest features, fixed issues, and known issues. This is for all users.

Video tutorials

To help you understand how to use Magnet AUTOMATE, several video tutorials are available from the Magnet Tutorial Hub in the Support Portal. For example:

- Magnet AUTOMATE: An Overview
- Creating a Case in Magnet AUTOMATE
- Creating a workflow in Magnet AUTOMATE
- Case Status and Troubleshooting in Magnet AUTOMATE

Professional Services

Magnet Professional Services work with agencies to consult on opportunities where the Magnet Digital Investigation Suite can help achieve their goals. For example, Magnet Professional Services can help you with workflow building, incorporating other digital forensics tools into Magnet AUTOMATE, migrating your environment, and how to script or build a process in Magnet AUTOMATE.

Technical Support

- **Technical Support Engineers** - provide assistance with answering your questions about Magnet AUTOMATE product usage or functionality, your Magnet AUTOMATE deployment, or potential issues you may encounter.
- **Support Portal** - Submit a support case or manage your existing cases, find solutions to common troubleshooting questions, product documentation, how-to articles, known issues, and additional resources.

SIGN IN

Supported browsers

For an optimal experience, access Magnet AUTOMATE using an up-to-date version of one of the following browsers on a desktop computer:

- Chrome
- Firefox
- Edge

Warning: To ensure that Magnet AUTOMATE functions correctly, do not prevent scripts from running in your browser (in the browser options or a third-party blocker).

Sign in to Magnet AUTOMATE

You can access the Magnet AUTOMATE web application from any computer on your network, provided that you have the IP address for the computer that hosts the controller service.

1. In a browser, type http://*[IP address]* or http://*[hostname]* into the address bar.
2. Do one of the following:
   - If you're the administrator, create a new account with admin privileges, and then sign in using the new account credentials.
   - If you're a user, sign in with the username and password that your administrator provided.

Sign out of Magnet AUTOMATE

To prevent unauthorized access, make sure you sign out of Magnet AUTOMATE at the end of each session.

1. In Magnet AUTOMATE, click your user name.
2. Click **Sign out**.

MANAGE YOUR USER PROFILE

From your user profile in Magnet AUTOMATE, you can edit your name, email address, and password.

Tip: By default, your email address appears as your user name in the Magnet AUTOMATE header. When you edit your user profile, change the email address in the **Name** field to your preferred name.

1. In Magnet AUTOMATE, click your user name > **View profile**.
2. Change your name, email, or password as necessary.
3. Click **Save**.

View your user account activity

You can view all of your user account activity in Magnet AUTOMATE and export the results as a .csv file for reporting purposes.

1. In Magnet AUTOMATE, click your user name > **My activity**.
2. To save your activity as a .csv file, click **Export activity**.

CREATE A CASE USING A WORKFLOW

Once a workflow is available, you can create a case using that workflow. In your case, you provide details such as the case number and output location, and select one or more evidence sources to process. For each evidence source, you can assign a specific type of workflow to process that evidence source, for example, you might have a CSAM workflow that processes mobile devices and another CSAM workflow that processes computer hard drives.

Note: AUTOMATE Essentials includes several default workflows that you can use to create a case. If you are an administrator, you can create your own workflow. For more information, see the Magnet AUTOMATE Workflow Builder Guide.

1. In Magnet AUTOMATE, click **Cases > Create new case**.
2. In the **Case details** section, provide a case number for the case in the **Case number** field, and click **Continue**.
   Tip: Your administrator may add custom fields that display in your case. For example, they may add a field called Examiner name that captures the name of the examiner processing the case. In addition, several fields on the case creation screen may be exposed as variables that you can use. Variables allow you to define a workflow using a placeholder that isn't populated until you create the case. For more information, contact your administrator or see the Magnet AUTOMATE Workflow Builder Guide.
3. In the **Evidence source** section, from the **Workflow** drop-down, select the type of workflow to run on the evidence source.
4. Depending on the workflow you selected, an evidence source type is automatically selected under **Evidence sources**. Provide details about one of the following selected evidence source types:
   - **Cloud platform** For details, see Cloud platform options.
     Note: This feature is only available for AUTOMATE Enterprise users.
   - **Connected drive**. For details, see Connected drive options.
   - **Hardware imager**. For details, see Hardware imager options.

  - **Image**. For details, see Image options.
  - **Remote computer** For details, see Remote computer options.
    Note: This feature is only available for AUTOMATE Enterprise users.
5. Click **Add evidence source**.
6. To add additional evidence sources to the case, repeat steps 3-5 for each evidence source and click **Continue**.
   If you added multiple evidence sources, a **Merge Workflow** section appears.
   - Choose a merge evidence sources option:
     - **Merge evidence sources**: This option creates an AXIOM case for each evidence source and a consolidated AXIOM case containing all evidence sources. In the **Workflow** drop-down, select a merge workflow to run on the evidence sources. If one does not exist, create a merge workflow (if you have administrator permissions) or contact your administrator to create one.
     - **Don't merge evidence sources**: This option creates an AXIOM case for each evidence source, offering you more granular organization of the evidence sources in a Magnet AUTOMATE case.
   - In the **Output path** field, use the default output path or type a new output path for the merge workflow.
7. Click **Submit case** or **Submit and create another**. Once a case is submitted, it's immediately added to the Magnet AUTOMATE queue for processing.

After the workflow starts, you can view the progress of your case in the Existing cases section on the Cases page. For information about managing cases, see Monitor the status of cases.

Image options

Option	Description
Work node	Allows you to specify a single node to run the entire workflow on, or select "First available" to run the workflow on the first node that becomes free. This option is only available if you select a workflow that is configured as a localized workflow. In a distributed workflow, the individual tasks in a workflow can be

Option	Description
	distributed amongst whatever nodes are available. **Note:** For AUTOMATE Essentials, there is only a single node.
Path to the image	A full path to the location of the image. You can browse to the image if you previously added a default image location. This field is exposed as a workflow variable called ${IMAGE_PATH}. After selecting an evidence source for a case, the file browser remains expanded, displaying the folder and selected evidence source. To reset the file browser to the default closed state and check for updates to evidence sources, click **Refresh**.
Platform	The platform of the image. After an image is selected, Magnet AUTOMATE attempts to detect the platform of the image automatically. You can also select a platform manually. However, if a platform is explicitly specified in a workflow, the workflow does not use the value specified during case creation. If AXIOM Process uses the **Use detected platform** option in the workflow, it will use the value specified during case creation. This field is exposed as a workflow variable called ${PLATFORM}.
Keychain	Allows you to specify a keychain file to decrypt application data in an iOS device. This field is available only if you choose **Image** as the **Evidence source** and **iOS** as the **Platform**. If AXIOM Process uses the **Use detected platform** option in the workflow and you choose an iOS image, the **Keychain** field also appears. In the **Keychain path** field, type or browse to the path and file name of the .plist keychain file for the selected iOS image. The keychain file appears in the workflow run summary and the **Keychain path** field if you retry the workflow that used the keychain file. To successfully load an iOS image and keychain file for processing:

Option	Description
	• The iOS image must use the following naming convention: {image name}_files_full.zip. For example, 7d40ef7bda29d4f52_files_full.zip. • The keychain file must use the following naming convention: {image name}_keychain.plist. For example, 7d40ef7bda29d4f52_keychain.plist. • The iOS image and keychain file must reside in the same folder. For example, D:\Storage\CASE-001\Images\iOS\7d40ef7bda29d4f52_files_full.zip and 7d40ef7bda29d4f52_keychain.plist **Important:** If the keychain is not in the same folder and doesn't contain the same file naming convention as the image, a "Keychain was not found" error message displays.
Decryption option	Allows you to specify a password or password list to decrypt the image, or attempt to automatically decrypt the image using passwords from files in the image. For more information on password lists, see the Magnet AUTOMATE Administrator Guide. This field is available only if the detected image is encrypted and Magnet AUTOMATE has support for decrypting that type of image. iOS and Android backups and UFD / UFDX are supported for decryption. For encrypted UFDX image files, you cannot specify a password or password list. Instead, Magnet AUTOMATE will attempt to decrypt the image using passwords from the UFD files. Encrypted APFS images and images encrypted with tools such as VeraCrypt, TrueCrypt, FileVault, FileVault 2, Symantec PGP, BitLocker, and BitLocker To Go are flagged as unsupported for decryption when they're loaded into a case (or detected by a watch folder). If you have another decryption tool in your workflow that supports these images, you can continue processing them in your workflow. You can also decrypt the images outside your workflow using Magnet AXIOM. To skip the built-in decryp-

Option	Description
	tion step, select the **Do not attempt decryption** option. **Continue running the workflow if decryption is unsuccessful**: This option is available only for encrypted images that Magnet AUTOMATE supports decryption for. If you select this option, your workflow is permitted to continue to the next element of the workflow even if decryption is unsuccessful. If this setting is turned off and decryption fails, Magnet AUTOMATE sends the workflow run to Failed cases.
Evidence number	The evidence number to apply to the image. This field is exposed as a workflow variable called ${EVIDENCE_NUMBER}.
Output path	Type a new or existing output path. This field is exposed as a workflow variable called ${OUTPUT_PATH}.

Connected drive options

Option	Description
Imaging node	The node where you want imaging to take place. **Note:** For AUTOMATE Essentials, there is only a single node.
Connected drive	The connected drive that you want to create an image of. Workflow variable: ${DRIVE}.
Platform	The platform of the connected drive. This field is exposed as a workflow variable called ${PLATFORM}.
Evidence number	The evidence number to apply to the drive. Workflow variable: ${EVIDENCE_NUMBER}.
Output path	Type a new or existing output path. Workflow variable: ${OUTPUT_PATH}.

Hardware imager options

Option	Description
Work node	Allows you to specify a single node to run the entire workflow on, or select "First available" to run the workflow on the first node that becomes free. This option is only available if you select a workflow that is configured as a localized workflow. In a distributed workflow, the individual tasks in a workflow can be distributed amongst whatever nodes are available. **Note:** For AUTOMATE Essentials, there is only a single node.
Hardware imager	The nicknames and types of hardware imagers on your network. For example: Atola1 - Atola TaskForce or GRAYKEY1 - GRAYKEY. If no hardware imagers are available in the drop-down, add one or more hardware imagers to Magnet AUTOMATE.
Connected drives	All drives currently connected to a TaskForce hardware imager. This field is available only if you choose TaskForce. From the drop-down, choose a connected drive.
Select evidence	All the evidence sources stored on a GRAYKEY hardware imager. This field is available only if you choose GRAYKEY. To see the images available for download, click an evidence source.
Select images	The images stored on a GRAYKEY hardware imager for a selected evidence source. Choose the images to download from the connected GRAYKEY hardware imager. If you selected an iOS evidence source and the keychain for that evidence source was acquired by GRAYKEY, the following option displays: **Use the passwords and decryption keys in the keychain to decrypt application data**. By default, this option is enabled.
Platform	The platform of the image. This field is available only if you

Option	Description
	choose GRAYKEY. This field is exposed as a workflow variable called ${PLATFORM}.
Evidence number	The evidence number to apply to the image. This field is exposed as a workflow variable called ${EVIDENCE_NUMBER}.
Output path	Type a new or existing output path. This field is exposed as a workflow variable called ${OUTPUT_PATH}.

Remote computer options

Option	Description
Hostname/IP Address	The hostname or IP address of the remote computer to acquire.
Evidence number	The evidence number to apply to the remote computer evidence. Workflow variable: ${EVIDENCE_NUMBER}.
Output path	Browse to or type a new or existing output path. Workflow variable: ${OUTPUT_PATH}.

Cloud platform options

Option	Description
User account	The email address of the target's Microsoft user account to add to the acquisition. A user account is only applicable when acquiring Outlook, OneDrive, Chats, or Channels cloud evidence from the Microsoft cloud platform.
Filter by date and time range	Choose the period of time to acquire cloud data from: • **After**: Includes cloud data from after the specified date/time. • **All dates**: Includes cloud data from all dates.

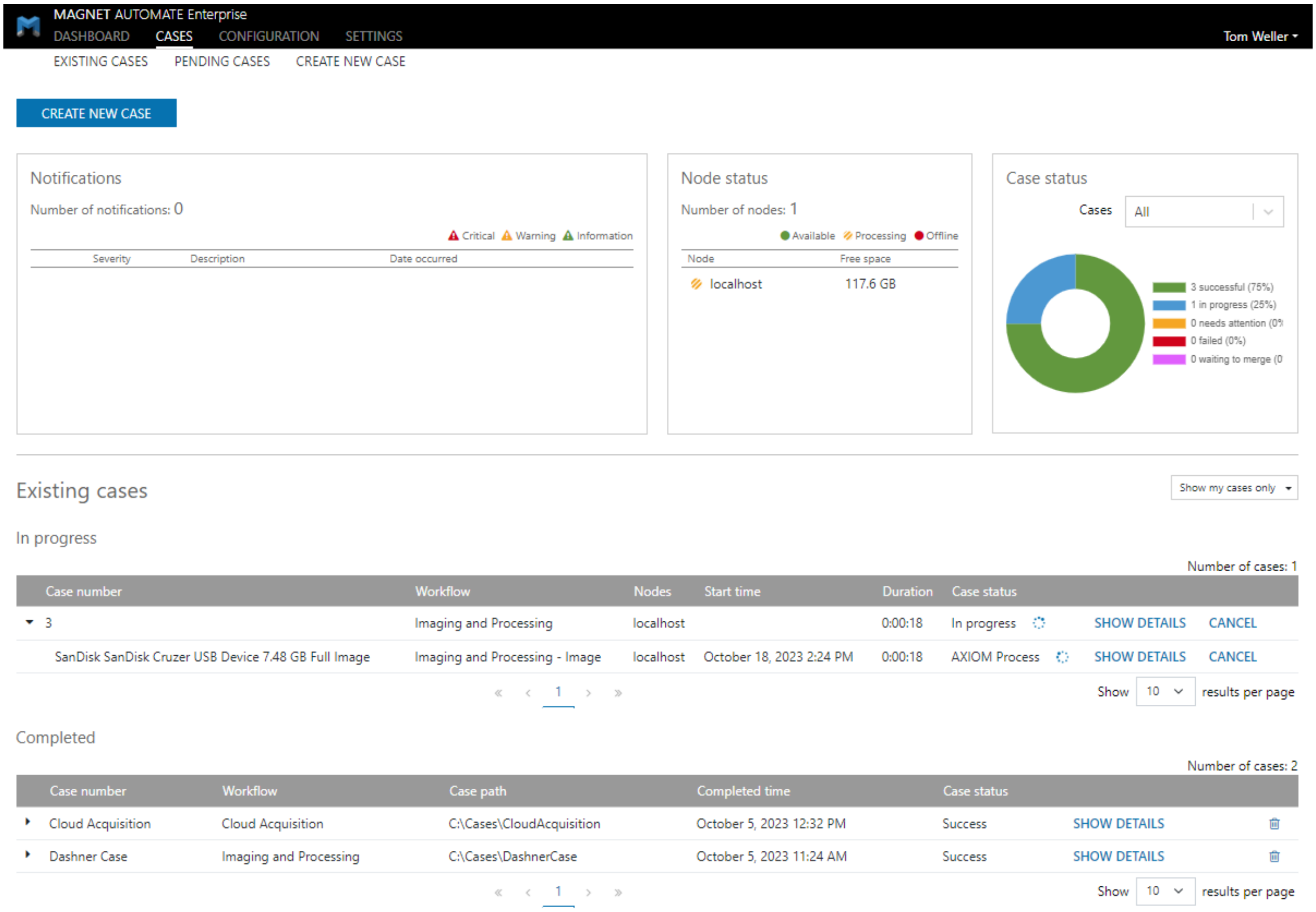
Option	Description
	• **Before**: Includes cloud data from before the specified date/time. • **Between**: Includes cloud data from the start and/or end date, as well as any dates between.
Imaging node	The node where you want imaging to take place.
Evidence number	The evidence number to apply to the cloud evidence. Workflow variable: ${EVIDENCE_NUMBER}.
Output path	Browse to or type a new or existing output path. Workflow variable: ${OUTPUT_PATH}.

MONITOR THE STATUS OF CASES

View cases

From the Cases page, you can see an overview of all cases (yours and those created by other users), including completed cases, cases that are currently processing, and cases that are waiting for more information before they can start. You can drill down into each case to view information about the individual runs and workflows that are associated with that case number.

When you sign in, the Cases page displays by default, ensuring that you immediately see the status of your cases. If the Cases page is not visible, click **Cases**.



Notifications

Number of notifications: 0

Severity	Description	Date occurred

Node status

Number of nodes: 1

Node	Free space
localhost	117.6 GB

Case status

Existing cases

In progress

Number of cases: 1

Case number	Workflow	Nodes	Start time	Duration	Case status		
3	Imaging and Processing	localhost		0:00:18	In progress	SHOW DETAILS	CANCEL
SanDisk SanDisk Cruzer USB Device 7.48 GB Full Image	Imaging and Processing - Image	localhost	October 18, 2023 2:24 PM	0:00:18	AXIOM Process	SHOW DETAILS	CANCEL

« ‹ 1 › » Show 10 results per page

Completed

Number of cases: 2

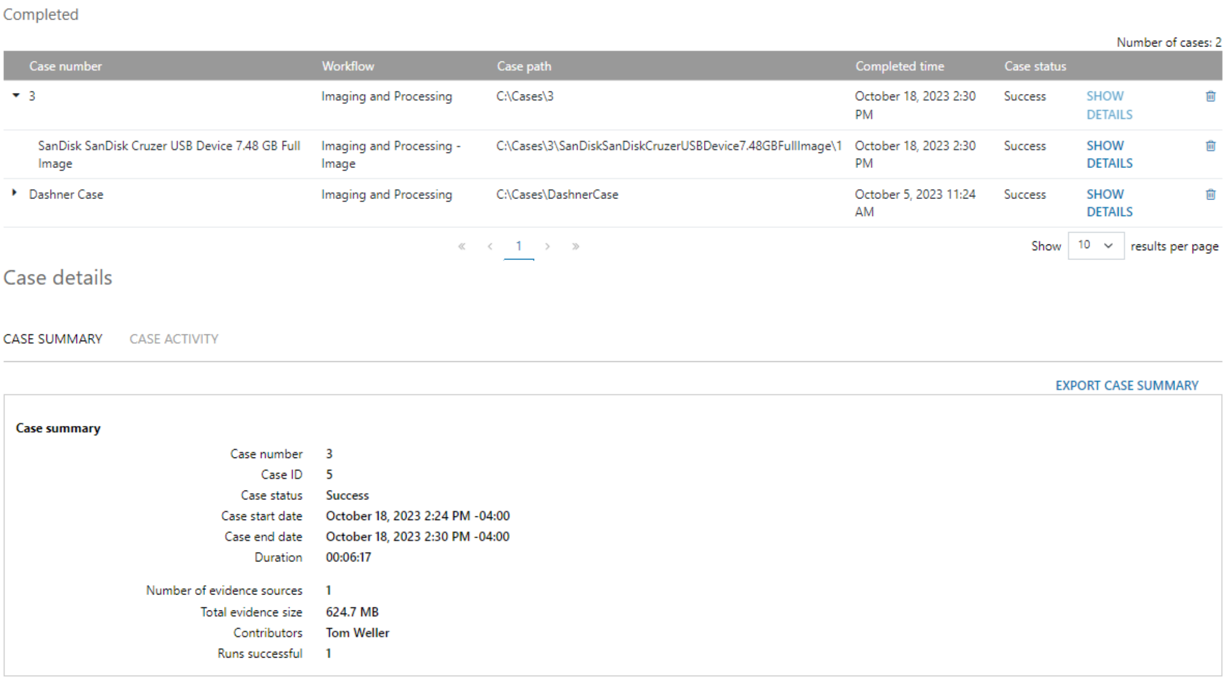
Case number	Workflow	Case path	Completed time	Case status	
Cloud Acquisition	Cloud Acquisition	C:\Cases\CloudAcquisition	October 5, 2023 12:32 PM	Success	SHOW DETAILS
Dashner Case	Imaging and Processing	C:\Cases\DashnerCase	October 5, 2023 11:24 AM	Success	SHOW DETAILS

« ‹ 1 › » Show 10 results per page

View case and run summaries

From the Existing cases section on the Cases page, you can view case and run summaries for in progress and completed cases.

- Case summaries display high-level information about the case, such as when the case started and the number of runs associated with the case.



Completed

Number of cases: 2

Case number	Workflow	Case path	Completed time	Case status		
▾ 3	Imaging and Processing	C:\Cases\3	October 18, 2023 2:30 PM	Success	SHOW DETAILS	🗑
SanDisk SanDisk Cruzer USB Device 7.48 GB Full Image	Imaging and Processing - Image	C:\Cases\3\SanDiskSanDiskCruzerUSBDevice7.48GBFullImage\1	October 18, 2023 2:30 PM	Success	SHOW DETAILS	🗑
▸ Dashner Case	Imaging and Processing	C:\Cases\DashnerCase	October 5, 2023 11:24 AM	Success	SHOW DETAILS	🗑

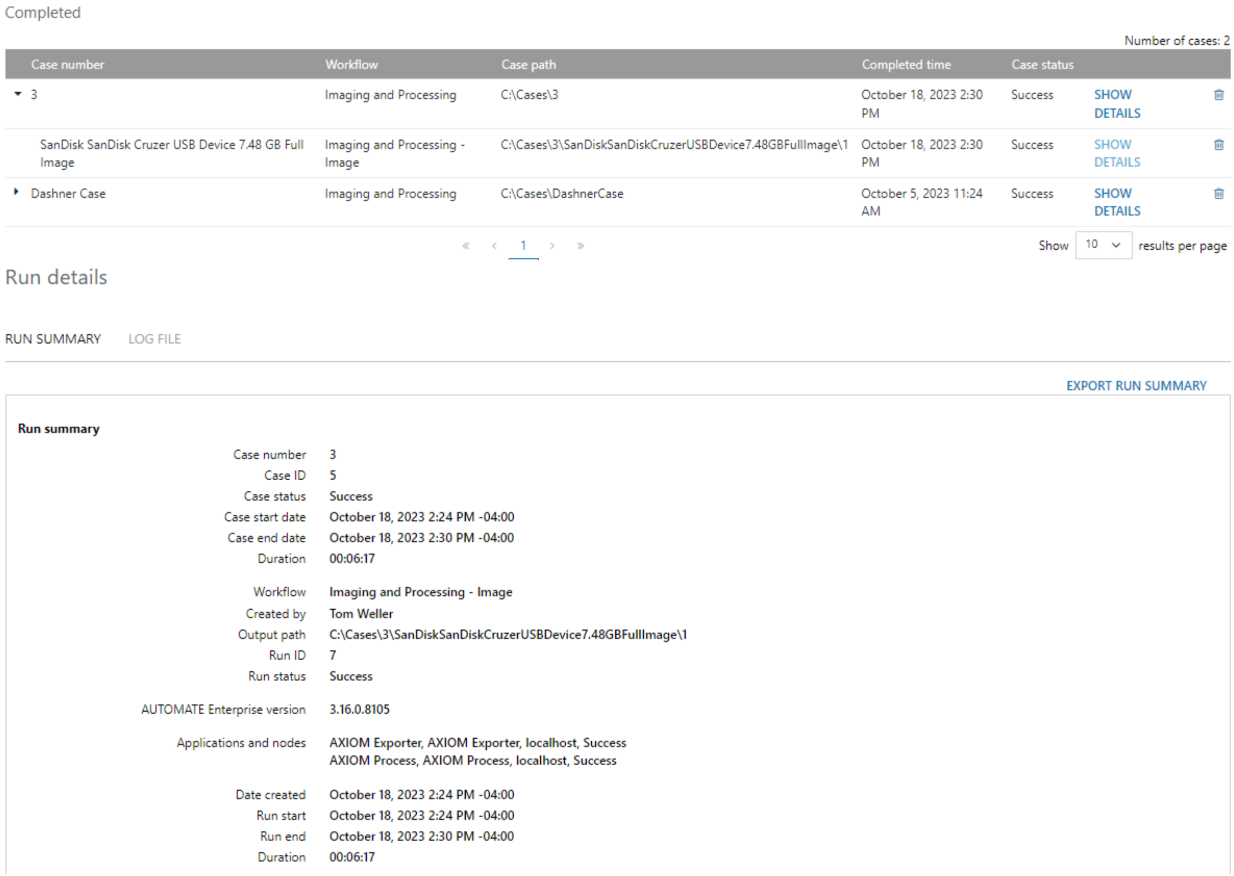
Show 10 results per page

Case details

Case summary

Case number	3
Case ID	5
Case status	Success
Case start date	October 18, 2023 2:24 PM -04:00
Case end date	October 18, 2023 2:30 PM -04:00
Duration	00:06:17
Number of evidence sources	1
Total evidence size	624.7 MB
Contributors	Tom Weller
Runs successful	1

- Run summaries display information about individual workflow runs (referred to as runs) in a case, such as the time of start and completion, paths to the output and source files, and the completion status.



Completed

Number of cases: 2

Case number	Workflow	Case path	Completed time	Case status		
▾ 3	Imaging and Processing	C:\Cases\3	October 18, 2023 2:30 PM	Success	SHOW DETAILS	🗑
SanDisk SanDisk Cruzer USB Device 7.48 GB Full Image	Imaging and Processing - Image	C:\Cases\3\SanDiskSanDiskCruzerUSBDevice7.48GBFullImage\1	October 18, 2023 2:30 PM	Success	SHOW DETAILS	🗑
▸ Dashner Case	Imaging and Processing	C:\Cases\DashnerCase	October 5, 2023 11:24 AM	Success	SHOW DETAILS	🗑

Run details

Run summary

Case number	3
Case ID	5
Case status	Success
Case start date	October 18, 2023 2:24 PM -04:00
Case end date	October 18, 2023 2:30 PM -04:00
Duration	00:06:17
Workflow	Imaging and Processing - Image
Created by	Tom Weller
Output path	C:\Cases\3\SanDiskSanDiskCruzerUSBDevice7.48GBFullImage\1
Run ID	7
Run status	Success
AUTOMATE Enterprise version	3.16.0.8105
Applications and nodes	AXIOM Exporter, AXIOM Exporter, localhost, Success AXIOM Process, AXIOM Process, localhost, Success
Date created	October 18, 2023 2:24 PM -04:00
Run start	October 18, 2023 2:24 PM -04:00
Run end	October 18, 2023 2:30 PM -04:00
Duration	00:06:17

Track version numbers of digital forensic tools

To track the version numbers of the digital forensic tools used in your cases, each run summary and log records the Magnet AUTOMATE version and versions of the applications used. To record application versions, you must include the version numbers when adding the applications to your nodes.

Report on your cases

To report on your cases, run summaries and logs are automatically included in the AUTOMATE Run Logs folder of each workflow run. The run summary and log are saved as .txt files in the following formats, respectively: <run finish time 24-hr format>-run-summary-<run ID>.txt and <run finish time 24-hr format>-run-<run ID>.txt. For example,

\\Automate\Cases\0001\AUTOMATE Run Logs\13_39_53-run-summary-1.txt and 13_39_53-run-1.txt.

> Note: Run summaries generated by manually exporting logs from the user interface use the client computer's timezone. Run summaries generated automatically in the Automate Run Logs folder from the API use the controller's timezone.

To view a case or run summary:

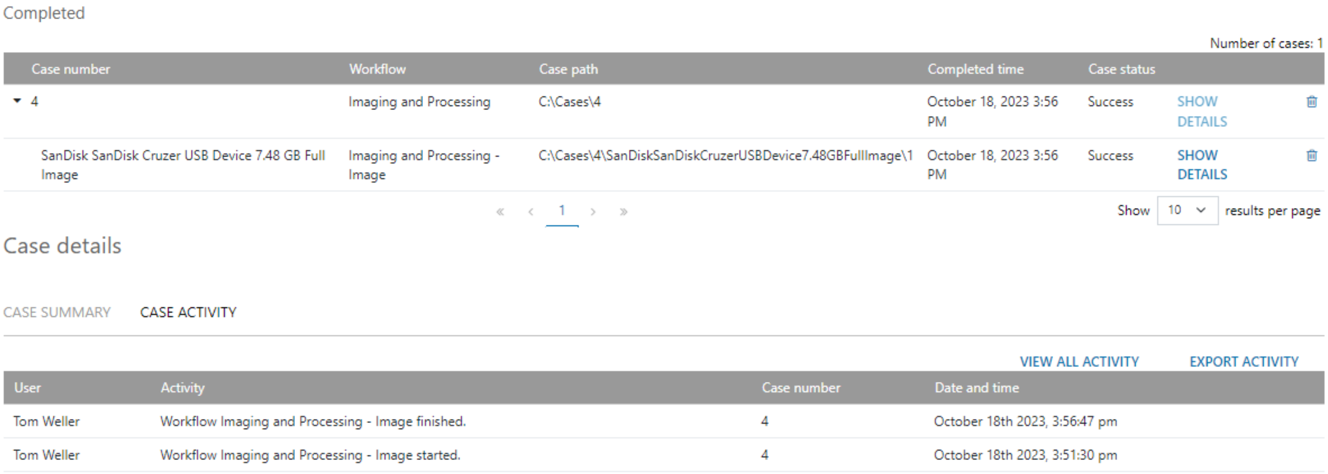
1. In Magnet AUTOMATE, click **Cases**.
2. By default, only cases created by you display in the **Existing cases** section, ensuring that you immediately see all of your in progress and completed cases that may require attention. To view all cases that are in progress and completed, click the **Show my cases only** drop-down list and select **Show all cases**.
3. In the **In progress** or **Completed** sections, expand a case.
4. For the case or run that you want to view the summary for, click **Show details**.
5. Optionally, to manually export a summary after processing is complete:
   - To export a case summary as a .txt file, under **Case details**, click **Export case summary**.
   - To export a run summary as a .txt file, under **Run details**, click **Export run summary**.

View user activity associated with cases

From the Existing cases section on the Cases page, you can view information about user activity associated with each case. For example, cases being created or changed, cases starting and completing, or user information being added or changed. This is useful for reporting on cases.

1. In Magnet AUTOMATE, click **Cases**.
2. By default, only cases created by you display in the **Existing cases** section, ensuring that you immediately see all of your in progress and completed cases that may require attention. To view all cases that are in progress and completed, click the **Show my cases only** drop-down list and select **Show all cases**.

3. In the **In progress** or **Completed** sections, expand a case.
4. Click **Show details** for the case that you want to view the activity for.
5. Click **Case activity**.



Completed

Number of cases: 1

Case number	Workflow	Case path	Completed time	Case status		
▾ 4	Imaging and Processing	C:\Cases\4	October 18, 2023 3:56 PM	Success	SHOW DETAILS	🗑
SanDisk SanDisk Cruzer USB Device 7.48 GB Full Image	Imaging and Processing - Image	C:\Cases\4\SanDiskSanDiskCruzerUSBDevice7.48GBFullImage\1	October 18, 2023 3:56 PM	Success	SHOW DETAILS	🗑

Case details

User	Activity	Case number	Date and time
Tom Weller	Workflow Imaging and Processing - Image finished.	4	October 18th 2023, 3:56:47 pm
Tom Weller	Workflow Imaging and Processing - Image started.	4	October 18th 2023, 3:51:30 pm

The table displays the user that initiated the action, the activity, the case number associated with the activity, and the time the activity occurred.

View activity for all cases

To view all activity for all cases, click **View all activity**.

Report on case activity

To export the activity as a .csv file for reporting purposes, click **Export activity**.

Prioritize queued cases

When you have multiple cases queued for processing, you can prioritize the cases that you want to start processing first. When you prioritize a case, it's moved to the top of the queue and the workflow runs that it contains are processed next. Each of the other cases that are queued are moved down one spot. Cases that are already processing are not affected by prioritization and continue to process as normal.

Note: Cases that include a merge workflow run might not behave as expected when they're prioritized. The pre-merge workflows in the case will run first when the case is prioritized, but the merge workflow must wait until they're finished before it can start. Other cases might start processing before the merge workflow is able to start.

1. In Magnet AUTOMATE, click **Cases**.
2. In the **Existing cases > In progress** section, click **Process next** on the **In queue** case that you want to move up to the top of the queue.

The case moves up to the top of the queue and each other queued case moves down one spot.

Add additional information to pending cases

Cases appear on the Pending cases screen when additional information is required before they can start processing. For example, watch folder workflows that contain encrypted images can appear on the Pending cases screen to allow you to provide a password (if decryption is supported for that image type). After you resolve any issues with a pending case, the workflow moves to the Existing cases screen.

1. In Magnet AUTOMATE, click **Cases > Pending cases**.
2. In the **Pending cases** section, expand a case.
3. On the workflow that you want to provide additional information for, do one of the following depending on the reason the case is pending.
   - To provide information about the case or evidence item, click **Add details**.

     Magnet AUTOMATE opens the **Create new case** screen where you can provide any additional information that is required.
   - To provide a password to attempt decryption with, click **Add password**.

     Magnet AUTOMATE opens the **Create new case** screen where you can provide the password to decrypt the image with.
   - To provide the platform of the image if auto-detection fails, click **Add platform**.

     Magnet AUTOMATE opens the **Create new case** screen where you can provide the platform to process the image with.

Merge results from a watch folder workflow

When a watch folder workflow contains a Stop for merge element, each run that it completes appears on the Pending cases screen with a case status of "Waiting to merge". Once you have two or more successful workflow runs in a case, you can finish the merge by selecting a merge workflow. The merge workflow merges the .mfdb files from each individual run and completes any additional steps that it includes, such as post-processing and exporting.

1. In Magnet AUTOMATE, click **Cases > Pending cases**.
2. In the **Pending cases** section, expand a case.
3. On any run that displays the **Waiting to merge** status, click **Merge**.
4. In the **Case details** section, click **Continue** without changing any existing information.
5. In the Evidence source section, ensure that all the items that you want to merge are listed in the table.

   > Tip: At this stage, it's important that you do not edit any details for the listed evidence sources. If you do edit an item, the workflow must reprocess the new information you provided. If you want to remove an item from the merge, click the delete icon (🗑). Deleting the item only prevents it from being included in the merge, it does not delete the workflow run itself.

6. Click **Continue**.
7. In the **Workflow** drop-down, select a merge workflow to merge the results.
8. Click **Create case**.

Retry a failed workflow

If a workflow fails to complete, you can retry that run on the Cases page without having to create a new case.

1. In Magnet AUTOMATE, click **Cases**.
2. In the **Completed** section, click **Retry** on the case that contains the failed run.
3. Select the **Reprocess** checkbox for each failed run that you want to retry.
4. If you need to edit any evidence source details before you reprocess, click **Edit** and update any required details.
5. Click **Submit case** to reprocess the evidence.

Cancel a workflow

You can cancel individual runs or entire cases that are in progress.

Important: When you cancel a run or case, data from incomplete workflow tasks are lost. However, any outputs that are already complete are copied to the final output location.

1. In Magnet AUTOMATE, click **Cases**.
2. In the **In progress** section, click **Cancel** on the case or the individual workflow that you want to cancel.
3. Click **Continue**.

The case or run stops processing and the status changes to Cancelling. Any outputs that are already complete are copied to the final output location.

Delete a case

You can delete completed cases from the Cases page if they're no longer useful in Magnet AUTOMATE.

Important: After you delete each run in a case, it's removed from the Cases page and cannot be restored. Any case outputs created by the case are *not* deleted from the file system. Before you delete a case, check your organization's data retention policies.

1. In Magnet AUTOMATE, click **Cases**.
2. In the **Completed** section, click the trash icon (🗑) for the case that you'd like to delete.

View run logs

From the Existing cases section on the Cases page, you can view logging information for each run in a central log, while the case is running and after it's complete. The run log lists output from each application in the order that the applications are run in the workflow. Logs also indicate which nodes are used to run each application. Viewing a run log can be useful for reporting purposes or troubleshooting errors in a run.

Track version numbers of digital forensic tools

To track the version numbers of the digital forensic tools used in your cases, each run summary and log records the Magnet AUTOMATE version and versions of the applications used. To record application versions, you must include the version numbers when adding the applications to your nodes.

Report on your cases

To report on your cases, run logs and summaries are automatically included in the AUTOMATE Run Logs folder of each workflow run. The run log and summary are saved as .txt files in the following formats, respectively: <run finish time 24-hr format>-run-<run ID>.txt and <run finish time 24-hr format>-run-summary-<run ID>.txt. For example, \\Automate\Cases\0001\AUTOMATE Run Logs\13_39_53-run-1.txt and 13_39_53-run-summary-1.txt.

Note: Run summaries generated by manually exporting logs from the user interface use the client computer's timezone. Run summaries generated automatically in the Automate Run Logs folder from the API use the controller's timezone.

Logging levels in a run log

In a run log, the higher the logging level, the more important and urgent the message is. In descending order, the following logging levels may appear in a run log:

- SEVERE - indicates a serious failure that prevents Magnet AUTOMATE from functioning. This type of error usually requires shutting down or restarting the controller and/or nodes to resolve the issue.
- ERROR - indicates an error with a component that prevents specific functionality from working. You may be able to continue running Magnet AUTOMATE; however, the resolution to the issue may require restarting the controller and/or nodes.
- WARNING - indicates a warning about a potential issue with a component. Generally, this logging level is not concerning unless you are troubleshooting a known issue. Warning messages might inform some of the behavior you experience with a known issue.
- INFO - indicates an informational message about normal system functioning, for example, the license server refreshing the current license.

For more information about troubleshooting issues in a run log, see Troubleshooting.

To view a run log:

1. In Magnet AUTOMATE, click **Cases**.
2. In the **In progress** or **Completed** sections, expand a case.
3. For the run that you want to view the log for, click **Show details**.
4. Click the **Log file** tab. By default, information appears in column format, displaying the timestamp and corresponding log file message. To view the run log in full screen, click the **Full screen** icon (⛶). To change the display and copy options, click **Options**.
5. To search the run log for specific messages, enter a keyword in the text box. For example, if the run failed, search for "ERROR" to help you find potential causes of the issue(s) you are experiencing.

6. Optionally, to download the run log as a .txt file during processing or after processing is complete, click the **Download log file** icon (📥).

VIEW CASE OUTPUT AND REVIEW EVIDENCE

Once a case completes in Magnet AUTOMATE, you can view the output and open the resulting Case.mfdb file for a full forensic analysis in Magnet AXIOM or AXIOM Cyber. If the workflow included AXIOM Exporter, you can also share the resulting report with case stakeholders.

Note: The output of a case depends on the type of workflow and the applications used to process the evidence. Workflows are defined by users with the Admin role.

View case output

Tip: To easily locate the output path for a case, in Magnet AUTOMATE, open the run summary associated with the case. The Output path field in the run summary displays the full path to the output.

1. In Windows Explorer, navigate to your default case output folder.
2. Open the folder that corresponds to the case number.
3. Open the folder that corresponds to the processed evidence source and then the folder for the corresponding run number.

For example, in a simple image processing workflow that uses AXIOM Process and AXIOM Exporter, Magnet AUTOMATE creates the following output folders and files in C:\Cases\6600\DashnerWin10PC\1:

- AUTOMATE Run Logs folder:
    - 12_28_12-run-1.txt - output from each application in the order that the applications are run in the workflow.
    - 12_28_12-run-summary-1.txt - information about individual runs in the case,

such as the time of start and completion, paths to the output and source files, and the completion status.

- AXIOM_Exporter folder:
    - Report.html - an HTML case report that provides a case overview, evidence overview, keyword matches, and a list of artifacts recovered from the evidence source.
    - Attachments included in the report.
- AXIOM_Process folder:
    - Case.mfdb file - a case file that you can open in Magnet AXIOM or AXIOM Cyber for a full forensic analysis.
    - Case Information.txt - case details from AXIOM Process (application settings, selected search items, selected evidence source, and final results of the search).
    - Various log files related to the processing of the evidence source and output.

Review evidence

For a full forensic analysis in Magnet AXIOM or AXIOM Cyber, open the Case.mfdb file in the AXIOM_Process folder.

> Tip: When you open a Case.mfdb file in Magnet AXIOM or AXIOM Cyber, use tags and comments in either tool *before* creating a report of your findings. This ensures that this additional information is also included in your report.

ENHANCE YOUR DIGITAL INVESTIGATION WITH OTHER MAGNET FORENSICS TOOLS

- **Share evidence with other stakeholders in Magnet REVIEW**

  Magnet AUTOMATE can export case output to Magnet REVIEW so that you can share case evidence with other stakeholders. By creating a workflow with Magnet REVIEW as a custom application, Magnet AUTOMATE uploads exported evidence directly to the cloud, where case stakeholders can review evidence from a supported browser.

- **Categorize media evidence in Griffeye Analyze DI**

  In cases that involve a large amount of media, Magnet AUTOMATE can create a media export of the evidence so that you can categorize the media in Griffeye Analyze DI. By creating a workflow with AXIOM Exporter and choosing Project VIC as the export type, Magnet AUTOMATE creates a JSON file that you can import into Griffeye Analyze DI.

- **View case output statistics in Magnet ATLAS**

  Using the API, Magnet AUTOMATE can integrate with Magnet ATLAS, a case management system. When you create a case in Magnet ATLAS, it can initiate a workflow in Magnet AUTOMATE, which then uploads the case details and case output statistics to Magnet ATLAS.

MONITOR AND REPORT ON SYSTEM USAGE AND PERFORMANCE

To quickly assess lab infrastructure health, and provide you with insights for resourcing decisions, the Dashboard in Magnet AUTOMATE provides an overview of usage and statistics for your deployment. For example, you can:

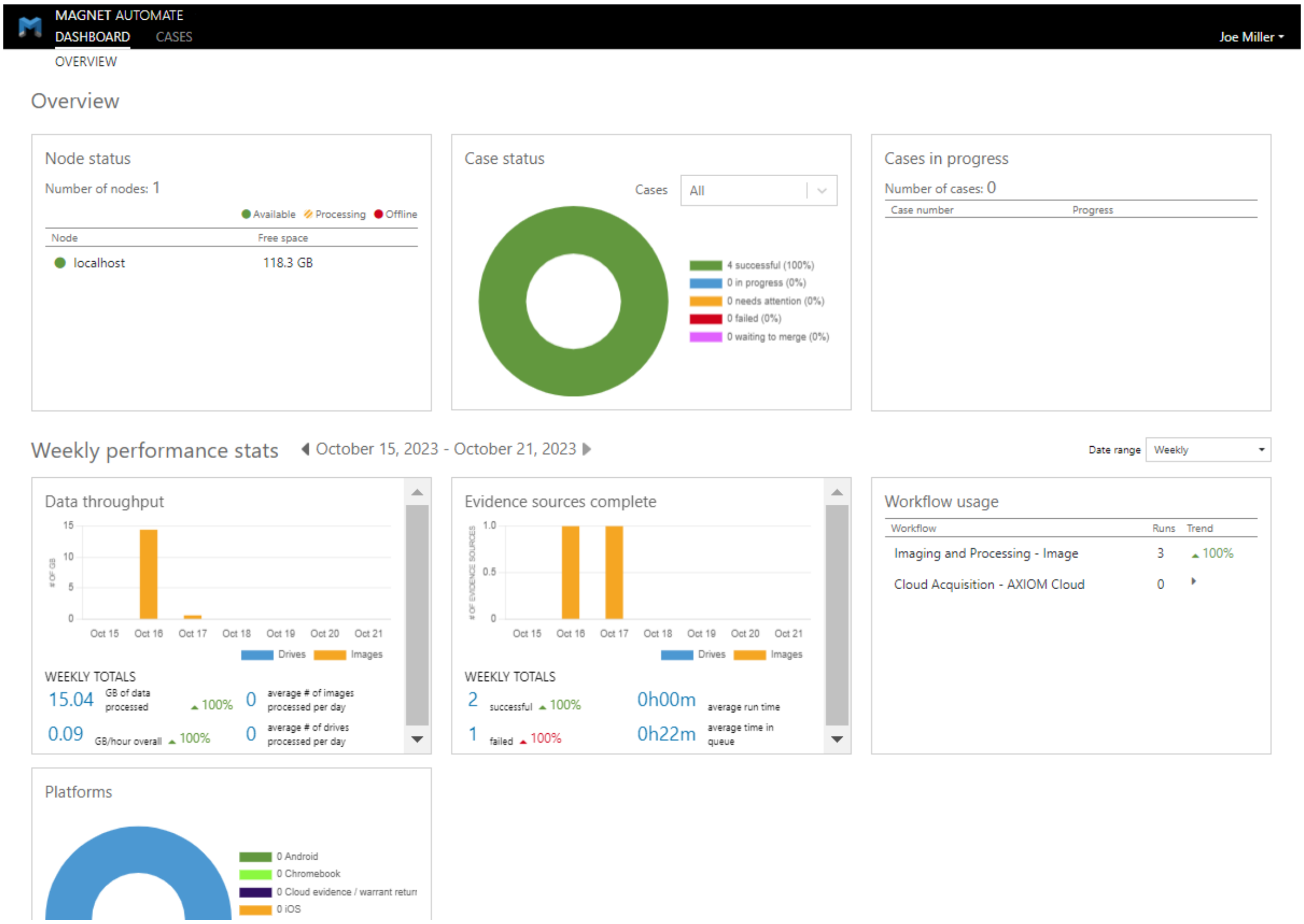
- View the status of all your nodes (available, processing, or offline).
- See an overview of the current case statuses (in progress, needs attention, failed, waiting to merge).

You can also see performance statistics on a daily, weekly, monthly or annual basis. This allows you to easily report to management on the value of your lab investments by tracking overall throughput and efficiency metrics. For example, you can view the following statistics:

- Data throughput: The data processed for each acquisition type (hourly and cumulative).
- Evidence sources complete: The number of successful and failed cases and their average run time and time in the queue.
- Workflow usage: The frequency that each workflow type is used.
- Platforms: The frequency that evidence from a particular platform is being processed by a workflow.

In Magnet AUTOMATE, click **Dashboard**.

Tip: You can filter data in some of the widgets by clicking individual items. For example, clicking items in the legend for the Case status widget removes or adds them from the circle graph.



Overview

Node status

Number of nodes: 1

● Available ⚡ Processing ● Offline

Node	Free space
● localhost	118.3 GB

Case status

Cases: All

Cases in progress

Number of cases: 0

Case number	Progress

Weekly performance stats

October 15, 2023 - October 21, 2023

Date range: Weekly

Data throughput

WEEKLY TOTALS

15.04 GB of data processed ▲ 100%

0 average # of images processed per day

0.09 GB/hour overall ▲ 100%

0 average # of drives processed per day

Evidence sources complete

WEEKLY TOTALS

2 successful ▲ 100%

0h00m average run time

1 failed ▲ 100%

0h22m average time in queue

Workflow usage

Workflow	Runs	Trend
Imaging and Processing - Image	3	▲ 100%
Cloud Acquisition - AXIOM Cloud	0	▸

Platforms

TROUBLESHOOTING

Tip: If you can't resolve your issue using the troubleshooting tips below, log in to the Magnet Support Portal and submit a case.

I can't remember my password

If you can't remember your password, contact a user with the Admin role. They will provide you with a new password and instruct you to change it immediately.

I can't access the Magnet AUTOMATE web application from a browser

If you cannot access the Magnet AUTOMATE web application from a browser, try the following:

- Ensure that you typed the correct URL for your Magnet AUTOMATE instance.
- In the browser, clear the cache and restart the browser.
- If clearing the cache does not work, contact a user with the Admin role.

How do I analyze stack traces in a run log to troubleshoot issues in a workflow?

In a run log, an error appears in the form of a stack trace, which is a collection of function calls an application ran in the workflow up until the error occurred. The first line in a stack trace records the function call that caused the error and then the previous function calls that led up the faulty call. By analyzing a stack trace in a run log, you can see the sequence of events that led to the error and the specific function call that caused it.

For example, in a failed run, the following displays in the run log:

```
[2023-09-18T15:30:29.467Z] Command: "C:\Program Files\Magnet Forensics\Magnet
```

```
AUTOMATE\agent\AXIOM Exporter\exporter.exe"  --case "c:\automate\workspace\NODE-
01\76\2\AXIOM_Process_-_Triage_Communications" --output "c:\automate\workspace\NODE-01\76\2\AXIOM_Exporter_-_Triage_Portable_Case" --examine
"C:\Program Files\Magnet Forensics\Magnet AUTOMATE\agent\AXIOM Exporter\exporter.exe\..\..\AXIOM Examine" --locale "en-us" --timezone "UTC" --type
"ChatPDF" --FinalExportPath "\\10.0.0.200\automate_shared\AUTOMATE_CASES\OWL_
USB\1\AXIOM_Exporter_-_Triage_Portable_Case\ChatPDF"
[Pipeline] fileExists
[Pipeline] powershell
[2023-09-18T15:30:51.467Z] Exporting to ChatPdf...
[2023-09-18T15:30:52.839Z] powershell.exe :
[2023-09-18T15:30:52.839Z] At C:\automate\workspace\NODE-01@tmp\durable-d8276404\powershellWrapper.ps1:3 char:1
[2023-09-18T15:30:52.839Z] + & powershell -NoProfile -NonInteractive -ExecutionPolicy Bypass -Comm ...
[2023-09-18T15:30:52.839Z] +
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
[2023-09-18T15:30:52.839Z]     + CategoryInfo          : NotSpecified: (:String)
[], RemoteException
[2023-09-18T15:30:52.839Z]     + FullyQualifiedErrorId : NativeCommandError
[2023-09-18T15:30:52.839Z]
[2023-09-18T15:30:52.839Z] Unhandled Exception:
[2023-09-18T15:30:52.839Z] System.AggregateException: One or more errors occurred.
---> System.IO.DirectoryNotFoundException: Could not find a part of the path
[2023-09-18T15:30:52.839Z] 'c:\automate\workspace\NODE-01\76\2\AXIOM_Exporter_-_
Triage_Portable_Case\ChatPdf'.
[2023-09-18T15:30:52.839Z]    at System.IO.__Error.WinIOError(Int32 errorCode,
String maybeFullPath)
[2023-09-18T15:30:52.839Z]    at System.IO.FileSystemEnumerableIterator`1.CommonInit()
[2023-09-18T15:30:52.839Z]    at System.IO.FileSystemEnumerableIterator`1..ctor
(String path, String originalUserPath, String searchPattern, SearchOption searchOption, SearchResultHandler`1 resultHandler, Boolean
[2023-09-18T15:30:52.839Z] checkHost)
[2023-09-18T15:30:52.839Z]    at System.IO.DirectoryInfo.EnumerateFiles(String
searchPattern, SearchOption searchOption)
[2023-09-18T15:30:52.839Z]    at Magnet.Utilities.Helpers.DirectoryHelper.GetDirectorySize(String path)
[2023-09-18T15:30:52.839Z]    at Magnet.Export.Api.Exporter.WritePostExportSummary
(IFilteredExportOptions options, IExportSummary exportSummary, DateTime
exportStartTime, IContainer container)
[2023-09-18T15:30:52.839Z]    at Magnet.Export.Api.Exporter.<ExportAsync>d__
0.MoveNext()
```

```
[2023-09-18T15:30:52.839Z] --- End of stack trace from previous location where exception was thrown ---
[2023-09-18T15:30:52.839Z]    at System.Runtime.ExceptionServices.ExceptionDispatchInfo.Throw()
[2023-09-18T15:30:52.839Z]    at System.Runtime.CompilerServices.TaskAwaiter.HandleNonSuccessAndDebuggerNotification(Task task)
[2023-09-18T15:30:52.839Z]    at Magnet.Export.Cli.Runner.ExportRunner.<>c__DisplayClass28_1.<<Export>b__9>d.MoveNext()
[2023-09-18T15:30:52.839Z] --- End of stack trace from previous location where exception was thrown ---
[2023-09-18T15:30:52.839Z]    at System.Runtime.ExceptionServices.ExceptionDispatchInfo.Throw()
[2023-09-18T15:30:52.839Z]    at Magnet.Export.Cli.Runner.ExportRunner.<ForeachExportDefinition>d__26.MoveNext()
[2023-09-18T15:30:52.839Z] --- End of stack trace from previous location where exception was thrown ---
[2023-09-18T15:30:52.839Z]    at System.Runtime.ExceptionServices.ExceptionDispatchInfo.Throw()
[2023-09-18T15:30:52.839Z]    at System.Runtime.CompilerServices.TaskAwaiter.HandleNonSuccessAndDebuggerNotification(Task task)
[2023-09-18T15:30:52.839Z]    at Magnet.Export.Cli.Runner.ExportRunner.<Export>d__28.MoveNext()
[2023-09-18T15:30:52.839Z] --- End of stack trace from previous location where exception was thrown ---
[2023-09-18T15:30:52.839Z]    at System.Runtime.ExceptionServices.ExceptionDispatchInfo.Throw()
[2023-09-18T15:30:52.839Z]    at System.Runtime.CompilerServices.TaskAwaiter.HandleNonSuccessAndDebuggerNotification(Task task)
[2023-09-18T15:30:52.839Z]    at Magnet.Export.Cli.Runner.ExportRunner.<Export>d__22.MoveNext()
[2023-09-18T15:30:52.839Z] --- End of stack trace from previous location where exception was thrown ---
[2023-09-18T15:30:52.839Z]    at System.Runtime.ExceptionServices.ExceptionDispatchInfo.Throw()
[2023-09-18T15:30:52.839Z]    at System.Runtime.CompilerServices.TaskAwaiter.HandleNonSuccessAndDebuggerNotification(Task task)
[2023-09-18T15:30:52.839Z]    at Magnet.Export.Cli.Runner.ExportRunner.<Run>d__21.MoveNext()
[2023-09-18T15:30:52.839Z]    --- End of inner exception stack trace ---
```

```
[2023-09-18T15:30:52.839Z]    at System.Threading.Tasks.Task.ThrowIfExceptional(Boolean includeTaskCanceledExceptions)
[2023-09-18T15:30:52.839Z]    at System.Threading.Tasks.Task.Wait(Int32 millisecondsTimeout, CancellationToken cancellationToken)
[2023-09-18T15:30:52.839Z]    at Magnet.Export.Cli.Program.Export(CommandLineOptions commandLineOptions)
[2023-09-18T15:30:52.839Z]    at Magnet.Export.Cli.Program.Main(String[] args)
```

Reviewing the stack trace, the error appears in the following line:

```
System.AggregateException: One or more errors occurred. ---> System.IO.DirectoryNotFoundException: Could not find a part of the path'c:\automate\workspace\NODE-01\76\2\AXIOM_Exporter_-_Triage_Portable_Case\ChatPdf'
```

Possible reasons the workflow failed include:

- The hyphen in the path name may be causing an issue.
- The path does not exist on the file system.
- The path cannot be accessed by the node running the workflow.

After attempting to resolve the issue, re-run the workflow.

Magnet Forensics

2220 University Ave. E., Suite 300

Waterloo, ON, N2K 0A8

1 (519) 342-0195