HASH SETS MANAGER

INSTALLATION AND CONFIGURATION GUIDE

CONTENTS

INSTALLING AND CONFIGURING HASH SETS MANAGER

Use Hash Sets Manager to upload and manage multiple hash sets in a single centralized database. You can upload hash sets from organizations such as Project VIC or CAID, or custom hash list files, then use these hash sets to categorize illicit media, identify known files of interest, and exclude known non-relevant files such as standard icons and screen savers.

Once your Magnet Forensics product is integrated with 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.

Hash Sets Manager is a beta product.

SYSTEM REQUIREMENTS

Hash Sets Manager runs on a host computer in your organization that meets the requirements below.

Item	Requirements
Operating system	Windows 10
Operating system server	Windows Server 2016 or Windows Server 2019
CPU	Quadcore CPU or better If you have an AMD x86_64 CPU, you need a Bulldozer or later processor If you have an Intel x86_64 CPU, you need one of the following processors: • A Sandy Bridge or later Intel Core processor • A Tiger Lake or later Intel Celeron or Intel Pentium processor
RAM	Minimum 32 GB (See Estimating storage requirements for more information) We don't recommend that you run Hash Sets Manager on a system with active Non-Uniform Memory Access (NUMA) (See Additional requirements for running MongoDB with NUMA hardware for more information)
Storage	Attached SSD with 110 GB for OS and binaries, plus additional space for hash sets database storage (SeeEstimating storage requirements for more information)

ESTIMATING STORAGE REQUIREMENTS

By default, the Hash Sets Manager database process uses half of the available RAM on a system. For optimal performance, we recommend that your system has twice as much RAM storage as what is required for storing your hash sets.

To determine how much storage you need for your hash sets, see Estimate by record count and Estimate by hash set.

Estimate by record count

To estimate the storage you will need, multiply the number of total expected hashes in your hash sets by the average hash size listed in the table below.

Hash set type	Average hash size
Media categorization	521 bytes
Non-relevant files	167 bytes
Known files	170 bytes

Estimate by hash set

If you are using hash sets from an organization such as Project VIC, CAID, or NIST, you can estimate the necessary RAM storage based on the hash set sizes listed below.

> Note: There are no known file hash sets available for storage estimation, as these hash sets are specific to each organization.

Hash set	Hash set size
Media categorization from Project VIC (USA)	7 GB
Media categorization from CAID (UK)	23 GB

Hash set	Hash set size
Non-relevant NSRL RDS hash sets from the NIST website under "UDF images of RDS 2.77 CDs" and "RDSv3 Version 2022.12.1 Delta - December 2022 zip Downloads." ### RDS v2 For RDS v2.77, we recommend using one of the following hash sets: • iOS RDS • Legacy RDS • Android RDS • Modern RDS (unique) > Note: While Hash Sets Manager supports other modern RDS v2 hash sets, the unique hash set has duplicates removed. Other modern hash sets include a large number of duplicate records that can take a significant amount of time to load. ### RDS v3 For RDS v3, you must use the minimal or delta versions of the hash sets. Download and unzip the files, then upload the applicable file to Hash Sets Manager: • Minimal hash sets: The file ending in "minimal.db" • Delta hash sets: The file ending in "delta.sql" > Warning: Do not edit the contents or file name of the RDS v3 hash set before uploading it to Hash Sets Manager.	16 GB (based on RDS Version 2.74)

ADDITIONAL REQUIREMENTS FOR RUNNING MONGODB WITH NUMA HARDWARE

Hash Sets Manager uses MongoDB servers and clients. When MongoDB runs on a system with Non-Uniform Memory Access (NUMA), operational issues can occur, such as slow performance and high system process usage.

In version 2.6 and later, MongoDB checks for NUMA settings on a Windows system. If the NUMA configuration might degrade performance, the MongoDB log will include a warning.

To learn more about NUMA, see the article NUMA (Non-Uniform Memory Access): An Overview.

To determine what you can do to avoid operational issues with a NUMA system, see the MongoDB documentation.

INSTALLING HASH SETS MANAGER

INSTALL HASH SETS MANAGER FOR USE WITH MAGNET AUTOMATE

Install the latest version of Hash Sets Manager from the Magnet AUTOMATE installation folder so that you can integrate it with Magnet AUTOMATE.

> **Before you begin**: Make sure you have downloaded Magnet AUTOMATE version 3.2 or later.

1. In your Magnet AUTOMATE installation folder, open the Hash Sets Manager setup application file.
2. Select a language to run the installer in, and then click **Ok**.
3. In the installation wizard, follow the steps.

   > Tip: We recommend using the default Web server port and MongoDb port. Make sure you copy down the port number so that you and other members of your organization can use it to access the Hash Sets Manager portal in a web browser later.

4. Click **Install**.

After the installation completes, you can visit the Hash Sets Manager portal by opening a web browser and entering the URL of the portal, which consists of the server IP address followed by the port number. For example, the default URL is https://127.0.0.1:20443.

INSTALL HASH SETS MANAGER FOR USE WITH AXIOM PROCESS

Install the latest version of Hash Sets Manager from the Magnet Idea Lab so that you can integrate it with AXIOM Process.

Before you begin: Make sure you have downloaded AXIOM Process version 6.3.0 or later.

1. In an internet browser, visit www.magnetidealab.com.
2. Sign in to the Magnet Idea Lab.
3. Click **Projects** > **Active Projects**.
4. Scroll down to Hash Sets Manager and click **Learn more**.
5. Click **Request Access**.
6. After you receive an email granting you access, click the link in the email and download the Hash Sets Manager installer.
7. On your computer, open the Hash Sets Manager setup application file.
8. Select a language to run the installer in, and then click **Ok**.
9. In the installation wizard, follow the steps.

   Tip: We recommend using the default Web server port and MongoDb port. Make sure you copy down the port number so that you and other members of your organization can use it to access the Hash Sets Manager portal in a web browser later.

10. Click **Install**.

After the installation completes, you can visit the Hash Sets Manager portal by opening a web browser and entering the URL of the portal, which consists of the server IP address followed by the port number. For example, the default URL is https://127.0.0.1:20443.

UNINSTALL HASH SETS MANAGER

1. On the **Start** menu, open **Settings**.
2. In the Settings window, click **Apps**.
3. Under Apps & features, scroll down and click **Magnet Hash Sets Manager**.
4. Click **Uninstall**.
5. In the window that appears, click **Yes**.

6. After Hash Sets Manager is uninstalled, restart any open instances of your Magnet Forensics products that were integrated with Hash Sets Manager.

SETTING A MEDIA CATEGORIZATION LIST

Before you can upload hash sets for media categorization, you must determine which media categories are visible in Hash Sets Manager.

You can:

- Use the default “United States (Project VIC)” list of media categories
- Select a different list of media categories
- Import and select a new list of media categories

USE THE DEFAULT MEDIA CATEGORIZATION LIST

1. In Hash Sets Manager, click **Settings**.
2. Under Media categorization list, verify that **United States (Project VIC)** is selected.

SELECT A MEDIA CATEGORIZATION LIST

1. In Hash Sets Manager, click **Settings**.
2. Under Media categorization list, select an option from the drop-down list.

IMPORT A NEW MEDIA CATEGORIZATION LIST

You can import a list of media categories to use in your hash sets, such as Project VIC or CAID media categories, that are not already included in the default media categorization lists. You can import XML files that have been exported from AXIOM Examine or another forensic tool.

1. In Hash Sets Manager, click **Settings**.
2. Under Media categorization list, click **Import list**.
3. Select a file, then click **Open**.
4. Select the new list from the drop-down list.

CUSTOMIZE THE SELECTED MEDIA CATEGORIZATION LIST

You can select which media categories you want to enable for your selected media categorization list.

1. In Hash Sets Manager, click **Settings**.
2. Under Media categorization list, select the categories you want to enable.

UPLOADING HASH SETS TO HASH SETS MANAGER

Add hash sets of media categories, known files, and non-relevant files to Hash Sets Manager by importing related hash list files.

UPLOAD A HASH SET

You can upload industry standard hash sets from organizations such as Project VIC / CAID or NIST. You can also upload custom text files. To learn more about hash list file formatting, see Hash set requirements.

1. In a web browser, enter the URL of the Hash Sets Manager portal, which consists of the server IP address followed by the port number. For example, the default URL is https://127.0.0.1:20443.
2. In Hash Sets Manager, in one of the hash set sections, click **Add hash set.**
3. To protect the hash set so that users can't make changes to it, select **Protect hash set so it is read-only**.
4. Click **Import hash list file**.
5. Select a file, then click **Open**.
6. Under **Configure hash set**, provide a name for the hash set.
7. If you're uploading a media categorization hash set, under **Select categories to import**, select a category for the hashes loaded from this list.
8. Click **Create hash set**.

UPDATE A HASH SET

Add hashes to a hash set by uploading additional hash list files.

You can upload industry standard hash sets from organizations such as Project VIC / CAID, or NIST. You can also upload custom text files. To learn more about hash list file formatting, see Hash set requirements.

1. In a web browser, enter the URL of the Hash Sets Manager portal, which consists of the server IP address followed by the port number. For example, the default URL is https://127.0.0.1:20443.
2. In Hash Sets Manager, next to the hash set that you want to update, click **Update hash set**.
3. To protect the hash set so that users can't make changes to it, select **Protect hash set so it is read-only**.
4. Click **Import hash list file**.
5. Select a file, then click **Open**.
6. If you're updating a media categorization hash set, in the Category drop-down list, select a category for the hashes loaded from this list.
7. Click **Save changes**.

HASH SET REQUIREMENTS

When you upload a hash set, or update an existing hash set, all hash list files must follow the requirements below.

Hash set type	Industry standard files	Custom files
Media categorization	JSON files from Project VIC and CAID	Text files containing only MD5, SHA1, or PhotoDNA hashes, with each hash on a separate line.
Known files	N/A	Text files containing only MD5

Hash set type	Industry standard files	Custom files
		or SHA1 hashes, with each hash on a separate line.
Non-relevant files	NSRL hash sets from NIST in CSV format with columns: "SHA-1","MD5","CRC32","FileName","FileSize", "ProductCode","OpSystemCode","SpecialCode" Hash Sets Manager supports hash sets from the NIST website under "UDF images of RDS 2.77 CDs" and "RDSv3 Version 2022.12.1 Delta - December 2022 zip Downloads." RDS v2 We recommend using one of the following hash sets: • iOS RDS • Legacy RDS • Android RDS • Modern RDS (unique) Note: While Hash Sets Manager supports other modern RDS v2 hash sets, the unique hash set has duplicates removed. Other modern hash sets include a large number of duplicate records that can take a significant amount of time to load.	Text files containing only MD5 or SHA1 hashes, with each hash on a separate line.

Hash set type	Industry standard files	Custom files
	### RDS v3 For RDS v3, you must use the minimal or delta versions of the hash sets. Download and unzip the files, then upload the applicable file to Hash Sets Manager: • Minimal hash sets: The file ending in "minimal.db" • Delta hash sets: The file ending in "delta.sql" Warning: Do not edit the contents or file name of the RDS v3 hash set before uploading it to Hash Sets Manager.	

INTEGRATING HASH SETS MANAGER WITH YOUR MAGNET FORENSICS PRODUCTS

Configure Hash Sets Manager to synchronize hash sets across each workstation running one of the following Magnet Forensics products:

- Magnet AUTOMATE version 3.2 and later
- Magnet AXIOM and Magnet AXIOM Cyber version 6.3.0 and later

INTEGRATING HASH SETS MANAGER WITH MAGNET AUTOMATE

You can configure Hash Sets Manager for use with Magnet AUTOMATE version 3.2 and later.

Integrate Hash Sets Manager with Magnet AUTOMATE

1. In Magnet AUTOMATE, click **Configuration** > **Global**.
2. Under **Hash set database location**, select **Use a hash set database hosted in Hash Sets Manager**.
3. Under **Hash Sets Manager**, provide a server IP address and port. Make sure you include "https://" at the beginning of the server address.
4. Optionally, provide a location for the local cache where AXIOM Process will store hash sets.
5. Click **Save**.

Using Hash Sets Manager in Magnet AUTOMATE workflows

After you've integrated Hash Sets Manager, you can include it in your Magnet AUTOMATE workflows. When you create a workflow and configure Hash Sets Manager application settings,

make sure you select the hash sets you want to enable. To learn more about workflows, see "Setting up workflows" in the Magnet AUTOMATE User Guide.

INTEGRATING HASH SETS MANAGER WITH AXIOM PROCESS AND AXIOM EXAMINE

You can configure Hash Sets Manager for use with Magnet AXIOM and Magnet AXIOM Cyber version 6.3.0 and later.

> Note: Hash Sets Manager integration in AXIOM currently supports media categorization hash sets in version 6.3.0 and later. Known files and non-relevant files are supported in version 6.7.0 and later.

Integrate Hash Sets Manager with AXIOM Process and 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**.

Find matching hashes in AXIOM using Hash Sets Manager

After you've integrated 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 Hash Sets Manager with AXIOM Process, click **Integrate with Hash Sets Manager**.
    a. In the Settings window, under Product integrations, select **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.

EXPORTING HASH SETS FROM HASH SETS MANAGER

After members of your organization have updated a hash set and uploaded their changes to the Hash Sets Manager portal, you can export the hash set to send to other organizations, save as a backup, or search for individual hashes in the file. Hash Sets Manager exports hash sets to the following file types:

- Media categorization: Project VIC JSON file
- Known files: Flat TXT file
- Non-relevant files: Flat TXT file

To export a hash set, follow the steps below.

1. In the Hash Sets Manager portal, in the row of the hash set you want to export, click **Export**.

   > Note: If the status column indicates that a hash set has previously experienced an error during an action, the export option is hidden. Click **Actions** > **Export hash set**.

2. After Hash Sets Manager finishes preparing the hash set export, your internet browser downloads the export file. When the download finishes, open the file.
3. Save the file to the desired location on your computer.

BACKING UP AND RESTORING HASH SETS MANAGER

The MongoDB backup and restore tools are included with your Hash Sets Manager installation. Use these tools to back up your data in Hash Sets Manager and restore it later if required. To learn more about these tools, see the MongoDB documentation at the following address: https://docs.mongodb.com/v4.2/reference/program/.

BACK UP THE HASH SETS MANAGER DATABASE

Back up your Hash Sets Manager data using the MongoDB backup tool.

To learn more about this tool, visit: https://-docs.mongodb.com/v4.2/reference/program/mongodump/.

1. Open a Windows Command Prompt.
2. Change the directory to the tools folder in your Hash Sets Manager installation folder. The default location is “C:\Program Files\Magnet Forensics\Hash Sets Manager\tools\bin”.
3. Enter the following command, with text in italics replaced as necessary using the criteria in the list below:

   ```
   mongodump.exe --gzip --db="CentralHashSets" --port=21443 --dir-r=Folder path
   ```

   - --gzip: Allows MongoDB to create a zipped folder for the backup data.
   - --db: The name of the database in MongoDB to export. In this case, the name is “CentralHashSets”.
   - --port: The port that MongoDB is running on.
     - Make sure that the port matches the one listed in mongod.cfg. By default, the file is located in “C:\Program Files\Magnet Forensics\Hash Sets Manager\storage\bin\mongod.cfg”.

    - Under # network interfaces, locate the port number. The default is 21443, but your organization might use a different port number.
  - --dir: The directory where you want the backed up data to be saved.
4. Press **Enter** to run the command.

RESTORE THE HASH SETS MANAGER DATABASE

If you've backed up your Hash Sets Manager data, you can restore it using the MongoDB restore tool.

To learn more about this tool, visit: https://-docs.mongodb.com/v4.2/reference/program/mongorestore/.

1. Open a Windows Command Prompt.
2. Change the directory to the tools folder in your Hash Sets Manager installation folder. The default location is "C:\Program Files\Magnet Forensics\Hash Sets Manager\tools\".
3. Enter the following command, with text in italics replaced as necessary using the criteria in the list below:

   ```
   mongorestore.exe --gzip --port=21443 --dir=Folder path
   ```

   - --gzip: Allows MongoDB to read the compressed backup file.
   - --port: The port that MongoDB is running on.
     - Make sure that the port matches the one listed in mongod.cfg. By default, the file is located in "C:\Program Files\Magnet Forensics\Hash Sets Manager\storage\bin\mongod.cfg".
     - Under # network interfaces, locate the port number. The default is 21443 , but your organization might use a different port number.
   - --dir: The directory where the backup data was written to.
4. Press **Enter** to run the command.

Magnet Forensics

2220 University Ave. E., Suite 300

Waterloo, ON, N2K 0A8

1 (519) 342-0195

This document was published on 12/19/2022.