Nuix Imager

USER GUIDE

Version 9.10.0

August 2022

nuix

Nuix Imager User Guide

Nuix Imager is a standalone application that acts as a powerful forensic imaging tool. Nuix Imager allows you to create images from files and folders and networks to cloud repositories such as email accounts, Microsoft SharePoint, Dropbox, Google Drive, Amazon S3, and many more; and to preview and triage evidence sources so only relevant data is captured.

User features

Use Nuix Imager to:

- Create forensic images of all the data sources Nuix Workstation is able to process
- Create images from files, folders, and networks to cloud repositories such as email accounts, Microsoft SharePoint, Dropbox, Google Drive, Amazon S3, and many more
- Export evidence in a number of ways

Application features

Nuix Imager:

- Collects data from multiple sources, including hard drives, files, email servers, and cloud storage services
- Supports all platforms that Nuix Workstation supports: Windows, macOS, Linux
- Runs in a portable mode, such as from a USB flash drive, on either a Windows or a Linux machine
- Runs in a non-portable mode on either a Windows or a macOS machine

License requirements

Acquire licenses from a dongle attached to the same machine, or from a remote license server.

For a list of licenses that you can use to run Nuix Imager, see Licence Profiles.

Install Nuix Imager

This section covers how to do the following:
- Install Nuix Imager on portable versions (either on a Windows machine or a Linux machine)
- Install Nuix Imager on non-portable versions (either on a Windows machine or a macOS machine)
- Install the associated add-ons (FFmpeg and FFprobe and, if required, the IBM (Lotus) Notes Cient)
- Check for missing dependencies via System Diagnostics
- Uninstall Nuix Imager (if required)

Nuix Imager is in two versions:
- **A portable version**: Available for Windows or Linux OSs, this can run without being installed.
- **A non-portable version**: Available for macOS or Windows OSs, you must install this on a local machine.

If upgrading your version of Nuix Imager, you do **not** need to uninstall a previous version, as the installer package automatically overwrites any previous version when installing the new version. (However, if for a reason other than upgrading your version of Nuix Imager you would like to uninstall and remove the product, then see the relevant 'Uninstalling Nuix Imager' procedure at the end of this section.)

If you experience any issue with installing Nuix Imager in either portable or non-portable versions, refer to Troubleshooting issues for detailed information on how to attempt to resolve the issue.

Install on portable versions

In addition to being a standalone application, Nuix Imager can be run directly from a USB drive or any portable device to collect evidence. When Nuix Imager is launched in portable mode, you are prompted to select the license before proceeding.

Install on a Windows OS

To set up and use the portable version of Nuix Imager on a Windows machine:

1. From the Nuix Customer Portal, download the portable bundle for Windows.
2. Unzip the contents of the downloaded ZIP archive to a USB drive or any portable device.
3. To configure the locations used for logs, temp files, and user data, open the *portable-config.properties* file located within the root of the archive.
   By default, *portable-config.properties* is configured to redirect all data into a directory named *portable-user-data*, which exists in the portable bundle.

Install on a Linux OS

To set up and use the portable version of Nuix Imager on a Linux machine:

1. From the Nuix Customer Portal, download the portable bundle for Linux.
2. Extract the contents of the downloaded tar gz archive to a USB drive or any portable device.
3. To configure the locations used for logs, temp files, and user data, open the *portable-config.properties* file located within the root of the archive.
   By default, *portable-config.properties* is configured to redirect all data into a directory named *portable-user-data*, which exists in the portable bundle.

portable-config.properties

The settings in this file manage the paths to store the data.

Setting	Description	Example
user-data-directory	Redirects all user data (metadata profiles, settings, and so on) to the specified directory.	`user-data-directory=portable-user-data`
log-directory	Redirects all logs to the specified directory.	`log-directory=logs`
temp-directory	Redirects all temporary files to the specified directory.	`temp-directory=temp`
redirect-all	Redirects all user-data, logs, and temporary files to the specified directory.	`redirect-all=portable-user-data`

Install on non-portable versions

The non-portable version of Nuix Imager is available in two ways:
- As part of an installation of Nuix Workstation on a local machine
- As a standalone version on a local machine

Install on a Windows machine

To set up and use the non-portable version of Nuix Imager on a Windows machine:

1. From the Nuix Customer Portal, download and open the Nuix Imager Installer package.
2. Accept the license agreement and click **Install** to start the installation.
   The progress bar appears, showing the status of the installation.
3. Once the installation is complete, click **Finish** to exit the wizard.

Install on a macOS machine

Nuix Imager for macOS is provided with a 64-bit installer for all license types. Once you install the hardware and any prerequisite software, you can install Nuix Imager.

To install Nuix Imager on a macOS:

1. From the Nuix Customer Portal, download and open the Nuix Imager Installer package.
2. Accept the license agreement to start the installation with default options.
   The installation progresses and the Nuix application icon appears.
3. To complete the Nuix Imager installation, drag and drop the Nuix icon into the **Applications** folder.
   Nuix Imager is now installed successfully.
4. To open it, double click Nuix in the **Applications** folder.

Install add-ons

Add-ons for Nuix Imager include the FFmpeg and FFprobe add-on, and the IBM Notes Client.

Install FFmpeg and FFprobe add-on

To install the FFmpeg and FFprobe add-on:

1. Download and open the **FFmpeg and FFprobe** package.
   The zip file contains FFmpeg, FFprobe, licenses, and README files.
2. Copy the FFmpeg and FFprobe files to one of the locations in the following table:

Operating System	Copy Location
Windows	*Program Files/Nuix/Nuix <x.x>/bin*
macOS	*- /usr/local/bin* or the default location for MacPorts *-/opt/local/bin*.
Linux	*- /opt/local/bin*

Install IBM Notes Client

IBM (Lotus) Notes Client (x86), v8.5.3 or v9.0 is required for processing encrypted IBM Notes archives.

Check dependencies via System Diagnostics

When Nuix Imager is started for the first time, the **System Diagnostics** window appears. The **Dependencies** tab shows whether or not the prerequisites are installed.

1. Review this list to ensure that all of the expected prerequisites are installed.
   For each dependency not found, the following prompt appears: **I understand the consequences of lacking this dependency**.
2. To confirm that Nuix Imager should run without these dependencies, select them individually, and click **OK.**

See Troubleshooting issues for more information on how to use the diagnostic information on this window.

Uninstall Nuix Imager (if required)

You do **not** need to uninstall Nuix Imager before upgrading to a newer version of the application. If you need, for any reason, to uninstall this application, follow:

Uninstall on a Windows machine

To uninstall Nuix Imager on a Windows machine:

1. Navigate to **Start**, select **Control Panel** and then **Programs and Features**.

2. From the list of programs, select **Nuix Imager x.x** and click **Uninstall**.
3. In the confirmation message that appears, click **Yes**.
   Nuix Imager is successfully uninstalled.

Uninstall on a macOS machine

To uninstall Nuix Imager on a macOS:

1. Open the Finder, and navigate to the **Applications** folder.
2. Find **Nuix Imager** and drag it to the Trash can.

Alternatively:

1. Open the Launchpad and find Nuix Imager.
2. Click and hold the icon until it starts to wiggle.
3. Click the X that appears in the upper-left corner.
4. Confirm the deletion in the window that appears.

Start Nuix Imager

This section covers how to do the following:
- Start Nuix Imager with a physical dongle
- Start Nuix Imager with Cloud License Server
- Reset the User Account password

Start Nuix Imager with a physical dongle

To start Nuix Imager:

1. Ensure that Nuix Management Server is installed on you machine.
2. Insert the Nuix dongle into an available USB port.
3. Navigate to **Start** and select **Control Panel > Administrative Tools > Services**.
4. In the Services window, select **Nuix Server** and click **Start** to start the service.
5. Navigate to **Start > All Programs > Nuix** and double-click **Nuix Imager** to start Nuix Imager.
6. In the **Licence Selection** window, select:
    a. The license source and enter valid login details.
    b. The type of license to run if there is more than one type available.
7. Click **OK** for the Nuix Imager home page to appear.

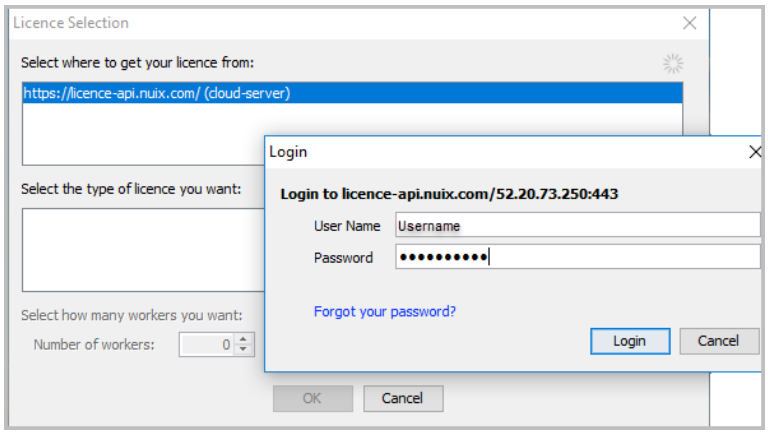
If Nuix Imager does not successfully start, access the logs at: *%localappdata%\Nuix\Logs* or contact Nuix Support at https://nuix.service-now.com/support.

Start Nuix Imager with Nuix Cloud License Server

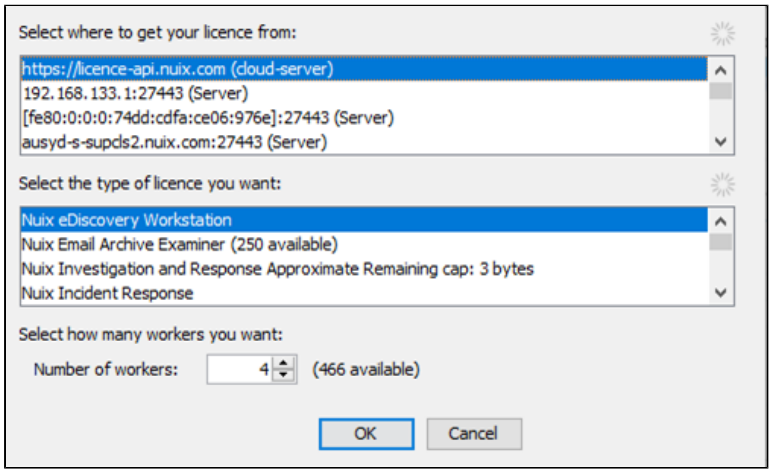
Nuix Cloud License Server is a global license server that integrates with Nuix Imager. It provides an in-house licensing solution run on Amazon Web Services (AWS). When Nuix onboards you an end user, you are given a License user account. If you have not received yours, contact Nuix Support.

To start Nuix Imager using Nuix Cloud License Server:

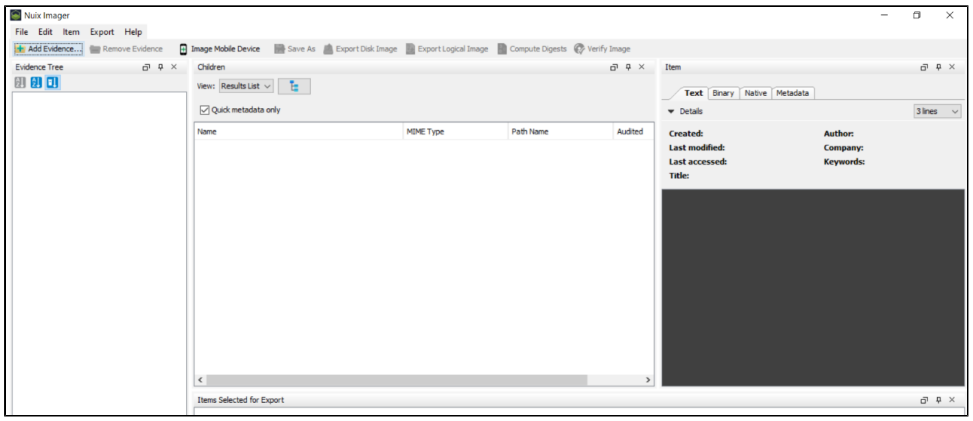
- Start Nuix Imager.
  For example, on a Windows computer, open the **Nuix Imager <X.X>** application.
- In the **Licence Selection** window, select the cloud license server (https://licence-api.nuix.com/).
- In the **Login** window, enter your user name and password, and then click **Login**.



- Select the type of license and click **OK**. Then:
  - For worker-based licenses, ensure you select at least one license worker.
  - For user-based licenses, you do not have the option to choose the number of workers.



The Nuix Imager home page appears.



Reset the user account password

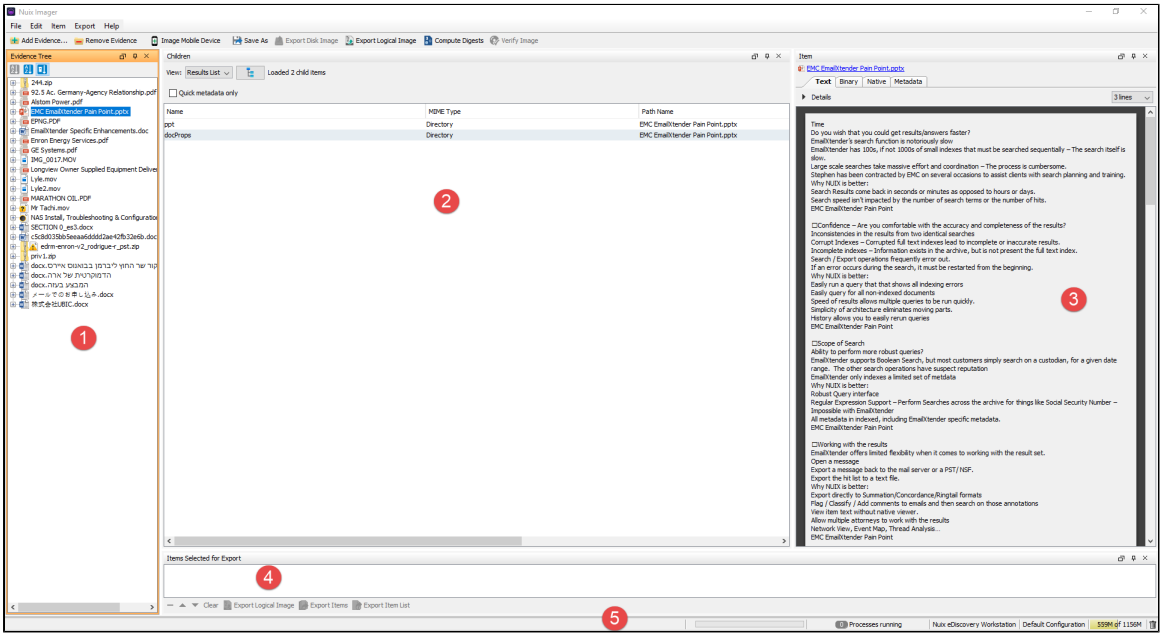
To reset the user account password:

1. Reset your user account password using any of the following methods:
   - **Cloud License Login Server:** Log into CLS Login Server and click **Reset password**.
   - **Nuix Workstation:** During the license selection process in Nuix Workstation, click **Forgot your Password?** in the Login screen.
   - **Nuix Imager:** If you are signed out of Nuix Workstation and open Nuix Imager, during the license selection process, click **Forgot your Password?** in the Login screen.
2. In the Reset Password screen that appears, enter your user name and click **SEND RESET PASSWORD LINK**.
   The reset password link is sent to your registered email account.
3. Access the link and reset your password.

User interface

This section details the main components of the Nuix Imager interface. As indicated by the numbers in the following image, they comprise:

1. Evidence Tree pane
2. Children pane
3. Item pane
4. Items Selected for Export
5. Status bar



From this screen, you can remove, rearrange or resize evidence, using any of the views to better suit your needs.

To return the views to their default layout, select **Reset Layout** from the **File** menu.

The menus and tabs provide you with more detailed and granular access to the user interface. Once evidence is added into Nuix Imager, preview and triage the content to eliminate any irrelevant evidence and curate the evidence to be exported.

Evidence Tree pane

The Evidence Tree pane lists all the evidence added. Navigate through the evidence and select the required item. The selected item's details are populated in the Children and Item panes.

Select to sort the evidence tree in one of the following ways:

- **Unsorted**: To list items in their original order, where possible.
- **Sorted**: To list items alphabetically.
- **Sorted containers first**: To list evidence alphabetically, with containers at the top of the list.

Children pane

The Children pane displays the contents and details of evidence containers added to Nuix Imager. The files and directories displayed are determined by the items selected in the Evidence Tree pane. Results appear in a list form by default, but if a directory contains images, change the view to an image gallery to review the contents of the images.

To change the view in the Children pane:

1. Click the **View** drop-down list.
2. Select either of the following views:
    - **Results List**: To display results as a list that includes item metadata.
      The option to view **Quick Metadata Only** displays only basic metadata of the selected items.
    - **Images**: To display only images contained in the containers. All other files or containers are hidden.

Find descendants of the items by clicking  . It calculates and displays the number of child items loaded.

Item pane

The Item pane comprises of information and tools that allow you to view the item itself, the metadata associated with the item, and additional information to help analyze the context of the item.

It displays the complete, hierarchical path that shows all parent items for the item being previewed. You can view the items in the path by clicking any folder link, which opens a new result set. The Item pane includes the following tabs to present different views of the item's content and associated metadata:

- Text
- Binary
- Native
- Image (only appears if the item previewed is an image)
- Metadata

Text tab

This tab displays the extracted text of the item and details about the item and is selected by default. Click **Details** to show or hide a subset of the metadata processed for the item, based on MIME type.

Use the drop-down list at top right to view a summary of the text, a selected number of lines, or the full text. Your selection is remembered when you view the next item.

Binary tab

This tab displays the hex and allows you to search the raw data structure at a binary level. This tab provides options that allow you to decode values recovered from unsupported file types and file fragments or unknown binary files.

Select the required data decode format from the drop-down list at the bottom of the pane, and then select the first byte to interpret the complete data field.

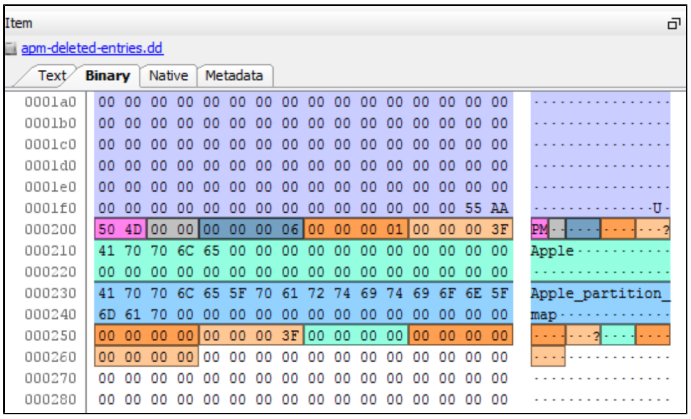
Binary Templates

Nuix Workstation supports highlighting and decoding binary data using binary templates stored in the user data directory. For example, a decoded Apple Partition Map can be highlighted in the template as:

```
class ApplePartitionEntry < BinData::Record
  endian :big

  string :magic, :length => 2, :colour => $magic_colour
  uint16 :reserved, :colour => $reserved_colour
  uint32 :partition_count, :colour => '#74A1C1'
  uint32 :partition_start, :colour => $offset_colour
  uint32 :partition_size, :colour => $size_colour
  string :partition_name, :length => 32, :colour => $name_colour
  string :partition_type, :length => 32, :colour => $type_colour
  uint32 :start_sector, :colour => $offset_colour
  uint32 :data_size, :colour => $size_colour
  uint32 :status, :colour => '#93FFE0'
  uint32 :boot_code_start, :colour => $offset_colour
  uint32 :boot_code_size, :colour => $size_colour
  string :padding, :length => 0x19c

end
```



Matching

If a matcher is registered as part of the template definition then the highlighting is automatically applied when an item is viewed in the binary view. Matching can be done against the binary directly, or against the source data item being viewed.

A binary based matcher(for NTFS file records)

```
register_matcher ->(matcher) {
  if (matcher.ascii(0, 4) == 'FILE')
    return NtfsFileRecord.new
  end
}
```

A context based matcher (for GPT partition tables)

```
register_matcher ->(matcher) {
  if (matcher.mime_type == 'application/x-disk-image' &&
      matcher.get_property('Partition Table Type') == 'EFI PART')
    return GptPartitionMap.new
  end
}
```

Decoding

Once a template is selected, it is applied to the binary to decode it. The decoding syntax is based on the Ruby bindata gem, and it loosely has three parts for each template structure: the declaration, the endianness, and the fields.

`class NtfsFileRecord < BinData::Record`	The template declaration. It creates a new template so it directly extends from BinData::Record, although it is possible to have a common base template (see NtfsAttributeCommon in NTFS.btpl).
`endian :little`	Sets the endianness for the template. NTFS, an x86-based format is little endian, but some Mac and Unix formats are big endian.

`string :magic, :length => 4, :colour => $magic_colour`
`uint16 :fixup_offset, :colour => $offset_colour`
`uint16 :fixup_count, :colour => '#93D2FF'`
`uint64 :usn, :colour => $usn_colour, :description => 'Update sequence number'`
`uint16 :sequence_number, :colour => '#93D2FF'`
	The field declarations, which start with a field type, then a name prefixed with a colon. For example, :usn. The remaining parameters are usually optional but can include the color to apply to the field, and a description for the tooltip text.

`end`	Closes the declaration.

Native tab

This tab uses a native viewer (external application) to view the selected item. Using the native viewer is disabled by default, so the selected item will not load. To enable it, click **Show Preview Options**. Once enabled, the item appears by the external application. The **Launch** button in the preview pane is also enabled.

The **Native** tab currently supports the following native viewers:

Program	Document Type	File Types
- Microsoft Office - Office viewer programs - Open Office - Libre Office	- Word documents - Excel spreadsheets - PowerPoint presentations - Open Office documents - Rich Text Format (RTF) - plain text - Microsoft Works word processor documents	**Word**: *.doc; *.dot; *.wps; *.wpt; *.docx; *.docm; *.dotm; *.dotx **Excel**: *.xlsb; *.xlsx; *.xlsm; *.xltx; *.xlk; *.vml**PowerPoint:** *.pptx; *.pptm; *.ppsx; *.ppsm; *.potx; *.potm**Open office and Libreoffice**: sxw; *.stw; *.doc; *.xml, *.rtf' *.sdw
Microsoft Visio	Visio documents	*.vsd; *.vst; *.vss; *.vsdx; *.vssx; *.vstx; *.vdx; *.vsx; *.vtx
Microsoft Project	Project 95 files are text stripped Project 98 files and later versions are supported	*.mpp; *.mpt
Microsoft Outlook	Outlook emails	*.pst; *.ost; *.msg
Windows Live Mail	EML files	*.eml; *.mht; *.zmc
Adobe Acrobat	PDF files	*.pdf
Internet Explorer	HTML Documents	*.html
Hangul Word Processor (HWP) viewer	Hangul word processor documents and presentation files	*.hwp; *.hwt
Autodesk TrueView viewer	DWG files are supported for: - 2004 version 16.0 release 18 - 2005 version 16.1 - 2010 version 18.0 - 2013 version 19.0	*.dwg; *.dxf; *.dwf

Metadata tab

This tab displays the metadata associated with the previewed item, including properties and Nuix-defined metadata.

Image tab

When you preview an item that is an image, an **Image** tab automatically opens, and the following information lists under **Details**:

- **Width**: Side-by-side measurement of the image, in pixels.
- **Height**: End-to-end measurement of the image, in pixels.
- **Colour Depth**: Number of bits used for each color component, in pixels.

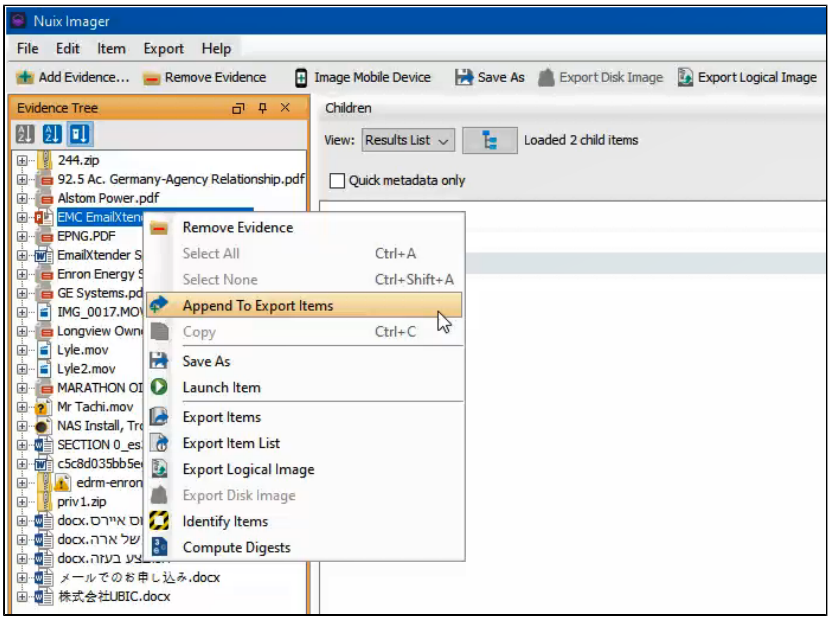
Click	To...
	Turn ON or OFF a solid background for images with transparent sections.
	Rotate the image counterclockwise.
	Rotate the image clockwise.
	Adjust the zoom for the image. The default is set to 100% but you can adjust it to any of the following (%): 10, 25, 50, 75, 100, 125, 150, 200, 400, and 800.

Items Selected for Export View pane

This pane allows you to append items that you export together as a set.

To add an item or directory to the items selected for export:

1. Right-click an item or directory from either the Evidence Tree or Children pane.
2. Select **Append To Export Items** to add the selected items to the **Items Selected for Export View** pane.



Once evidence is added, you can perform additional actions such as remove items, change the order of items in the list, or export the items using any of the following options:

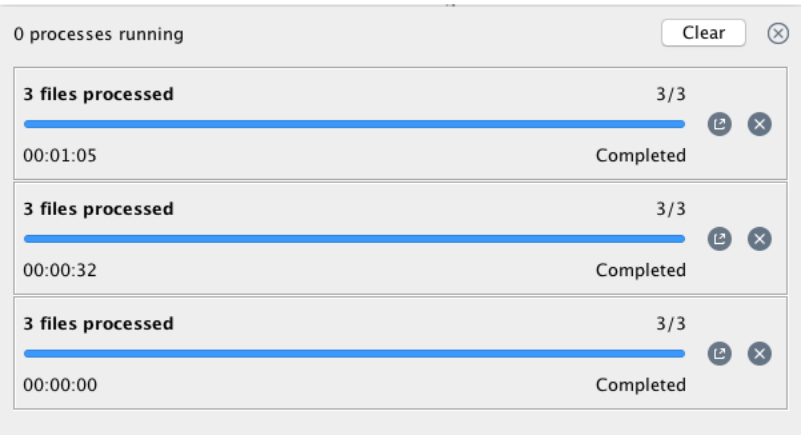
- **Export Logical Image**: To export the items in the pane to a Nuix Logical Image file. See the Take a Nuix logical image section for additional details.
- **Export Items**: To export items to a specified directory, and opt to include one of the following:
  - **Item details report**: A CSV file of metadata for all items in the export.
  - **Compute MD5 digests**: An MD5 digest (hash) for every item exported.
  - **Compute SHA-1 digests**: An SHA-1 digest (hash) for every item exported.
- **Export Item List**: To generate an item details report and optionally include the MD5 and SHA-1 digests for each item in the view without exporting the actual items.

Status bar

The status bar displays the license being used and the number of processes running in the background.

View the status of background processes by clicking **Processes Running**. It displays:

- The currently running background processes.
- The elapsed time for each background process.
- Options to:
  - Stop or cancel currently running background processes.
    A dialog box prompts you to confirm that you want to stop a process.
  - Clear completed background processes.



Menus and their options

Nuix Imager contains the following menus which are separately detailed in the following pages:

- **File** menu: This contains commands for working with evidence and configuring Nuix Imager.
- **Item** menu: This contains several ways to display the evidence imported into the application.
- **Export** menu: This contains several ways to export the evidence imported into the application, and allows you to curate items together and export items as a set or individually.

These options are also available as icons in the space above the Evidence View.

File menu options

The **File** menu in Nuix Imager contains commands for working with evidence and configuring Nuix Imager.

Command	Function
Adding Evidence	Adds evidence files to a case on selection of one of the following options: • Add Files • Add Split-DD Image • Add This Computer • Add Local Disks • Add Centera Cluster This option is only available for the Email Archive Examiner and Ultimate Workstation licenses. See License Profiles for the list of licenses Nuix offers. See the Add Evidence in Nuix Imager section for more information.
Remove Evidence	Removes the item selected in the Evidence Tree pane from Nuix Imager.
Remove All Evidence	Removes all the items in the Evidence Tree pane from Nuix Imager.
Image Mobile Device	Takes an image of a mobile device. Instructions for both Android and iOS devices can be found on Imaging Mobile Devices.
Save As	Saves the files in Nuix Imager. Then you can rename the file according to your file-naming conventions.
Export Disk Image	Export evidence from Nuix Imager to a more convenient location. See the Export menu options section for more details.
Export Logical Image	Exports a Logical Image. See the Export menu options section for more details; and the Take a Nuix logical image section for more information on the images themselves.
Global Options	Sets configuration options for Nuix Imager. See the Configure Global Options section for more details.
Reset Layout	Restores the layout of Nuix Imager to its original configuration, losing all previous changes.
Sign out and Exit	Allows a user to sign out of their user account in Nuix Imager. **Note:** Only available only for Cloud License Server users. It is **not** an option supported on macOS. If you sign in or out of Nuix Workstation, you are also signed in or out of Nuix Imager. If you exit Nuix Workstation *without* signing out, Nuix Imager does not require you to enter your login credentials when returning.
Exit	Exits Nuix Imager.

All these options are also available as icons in the space above the Evidence View.

Item menu options

The **Item** menu in Nuix Imager contains several ways to show the evidence imported into the application.

Command	Function
Identify Items	Identifies unknown items after ingestion.
Compute Digests	Computes, on selection of one of the following options, the relevant file digest: • **Generate Item details report**: To produce a CSV file that includes metadata for all items included in the export. • **Compute MD5 digests**: To produce an MD5 digest (hash) for every item exported. • **Compute SHA-1 digests**: To produce a SHA-1 digest (hash) for every item exported.
Verify Image	Verifies your image data after exporting the disk image.
Launch Item	Opens the selected item in the supported application. A warning appears to notify you that if the file is malicious, and opening it could compromise your system. If the machine running Nuix Imager has a means of mitigating this, or the file is not malicious, click **Yes** or **Always Yes**.
Show in Parent Binary	Shows the selected item in the binary structure of its parent item.
Show in NTFS $MFT	Shows the selected item in the NTFS Master File Table.
Show in FAT Directory	Shows the selected item in its File Allocation Table (FAT) directory.
Show in File System	Shows the selected item in the file system.

Export menu options

Through its **Export** menu, Nuix Imager provides several ways to export the evidence imported into the application, and allows you to curate items together and export items as a set or individually.

Alternatively, you can select the required item and right-click it to view its context menu and select the required command.

Command	Function
Append to Export Items	The appended items appear in the **Items Selected for Export** pane.
Export Disk Image	To export the disk image of the evidence to an output directory, see *Export disk image* under Export evidence for details.
Export Logical Image	To export a logical image of evidence, see *Export logical image* under Export evidence for details.
Export Items	Export the items to the selected directory. Select the following options, if required: • Generate Item details report • Compute MD5 digests • Compute SHA-1 digest
Export Item List	Export the list of items to the selected directory, using one of the following options, if required: • Generate Item details report • Compute MD5 digests • Compute SHA-1 digest

Configure Global Options

Configure the settings in Nuix Imager through Global Options.

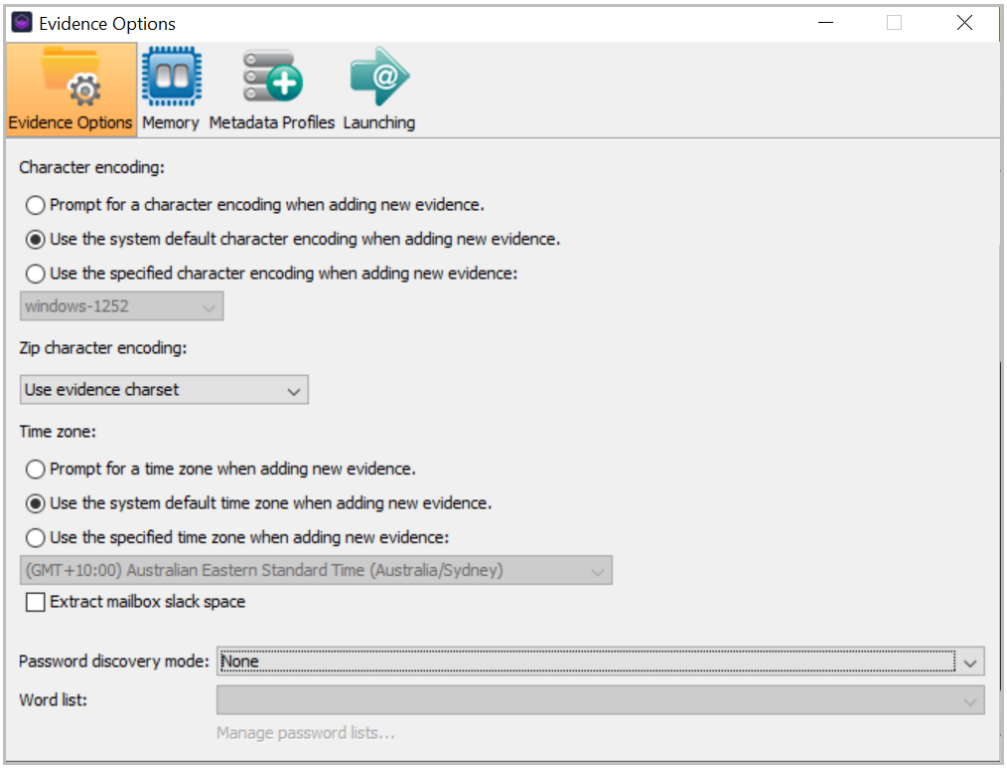
To set the global options, click **File** and select **Global Options.**

Evidence Options tab

Evidence options enable you to configure the settings required for working with the evidence.

In the Evidence Options window, configure the following:

- Evidence Options
- Memory
- Metadata Profiles
- Launching



Character encoding

Select the required option to set for character encoding:

- Prompt for a character encoding when adding new evidence.
- Use the system default character encoding when adding new evidence. This is the default setting.
- Use the specified character encoding when adding new evidence. Select an encoding format from the list. Windows 1252, UTF-8, and Adobe Standard Encoding are the most frequently used and appear at the top of the list as a result.

Zip character encoding

Select the Zip file encoding charset from the list.

Time zone

Select the required option to set for time zones:

- Prompt for a time zone when adding new evidence.
- Use the system default time zone when adding new evidence.
  (Default setting).
- Use the specified time zone when adding new evidence.
  The system default time zone appears by default when selected. To update, select the appropriate one from the list.
- Extract mailbox slack space.
  Select this option to remove the empty (slack) space in your mailbox during importing.

Password discovery mode

A password bank is a password repository used to decrypt password-protected files during discovery and processing. Password banks are used to decrypt files, enabling you to manage password lists by adding them manually or importing a word list using a .txt file. When using a password bank, Nuix Imager runs passwords against each encrypted file until it finds a match.

Select **Word list** to add a word list. By default, the Password discovery mode is set to None.

Word list

If you selected Word list as the Password discovery mode, add the required word list using a .txt file. The word lists created then appear in the drop-down list indicating the number of words in the list.

Click **Manage password lists** to update the word lists using the following options.

Icon	Description
	Add an entry
	Edit the selected entry. To import a list from your computer, click **Import Words**. To export your created list, click **Export Words.** **Note:** To import or export words, use Plain Text files (*.txt).
	Remove the selected entry.
	Move the entry up in the lists.
	Move the entry down in the lists.

Memory tab

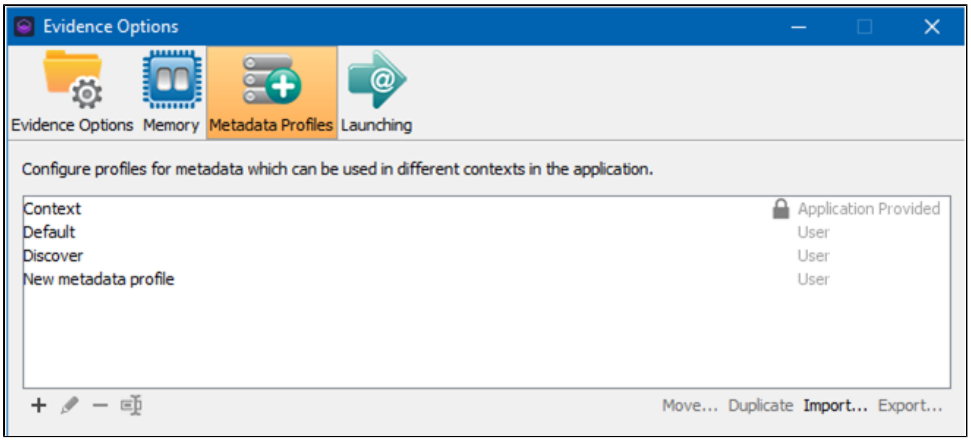
The **Memory** option allows you to configure the amount of RAM made available to Nuix Imager. Increase or decrease this value depending on the size of the case being ingested. Ensure to reserve some memory for load and export workers when adjusting this setting.

The default setting for Application memory is 1,300 (1.3 MB). Adjust to any value, in 128 MB increments, by using the up and down arrows, from 788 MB up to 17,044 MB.

Note: Restart Nuix Imager for the changes to take effect.

Metadata Profiles tab

Metadata is the data that provides information about other data, facilitating a clear analysis of data. Metadata Profiles enable you to configure profiles for metadata fields. You can create profiles specifically for a Case, User, or Local Computer. You can also export or import a previously defined profile from a file.



To create a metadata profile:

1. In the **Metadata Profiles** window, click the plus icon **(+)** to add a profile.
2. To define the scope of the profile, select one of the following:
   - **Case**
   - **User**
   - **Local Computer**

1. In the **Create Metadata Profile** dialog box, click the plus icon **(+)** to select the metadata type.
2. Use the **Filter** option to select the required metadata, and click **OK**.
   The selected metadata is added to the profile.
3. Then perform the following actions on the selected metadata:

Action	Description
	To modify/update the selected metadata.
	To delete the selected metadata.
	To move the selected metadata up in the list.
	To move the selected metadata down the list.

4. Click **OK** to save the profile. Rename the profile as required.

More actions to apply to metadata

Action	Description
	To modify or update the selected metadata profile.
	To permanently delete the selected metadata profile.
	To rename the selected profile.
Move	To move the selected profile to another scope.
Duplicate	To create a copy of the selected profile.
Import	To import a Nuix metadata profile file.
Export	To export the Nuix metadata profile file.

For details on metadata, see the *Building Metadata Profiles* section in the Nuix Workstation User Guide.

Launching tab

The **Launching** tab allows you to set the default application you want to use when opening items on the **Native** tab in the **Item** pane.

To set the default application to use when opening items on the **Native** tab:

1. Click the **Launching** tab.

2. Select one of the following formats:
   - **EML:** Standard message format (RFC822) and default option.
     Windows systems and other email programs mostly default to using Outlook Express.
     The prompt to configure this may still display even if you close the configuration window.
   - **MSG:** Microsoft Outlook individual files
   - **NSF**: IBM (Lotus) Notes mailbox

Add evidence

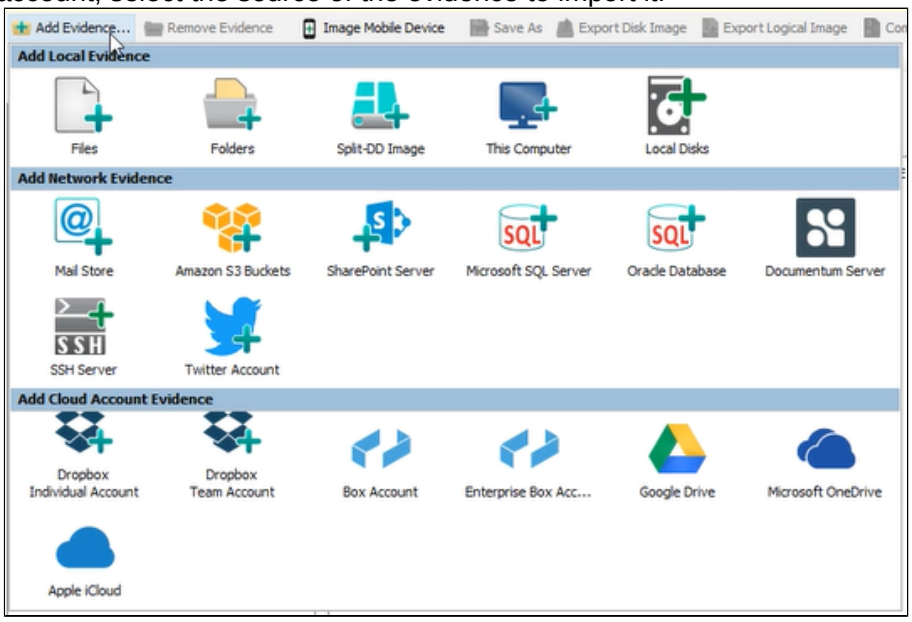
Locations of evidence

Nuix Imager simplifies the process of adding evidence extracted from the following locations:

- A **local computer**
- A **connected network**, including from:
  - Amazon S3 buckets
  - Documentum servers
  - Exchange servers
  - Mail stores
  - Microsoft Office 365
  - Microsoft SQL servers
  - Oracle databases
  - Secure Shell (SSH) servers
  - SharePoint servers
  - Twitter accounts
- A **Cloud account**, including from:
  - Apple iCloud accounts
  - Box accounts
  - Dropbox accounts
  - Google accounts
  - OneDrive accounts

Ways to add evidence

1. Click **Add Evidence** at the top left of the menu bar, and from a local computer, a network or a cloud account, select the source of the evidence to import it.



You may then need to supply valid credentials and additional connection information. This depends on the evidence location you select.

Refer to the *Images* section in the Nuix Supported File Types document for details on file types that Nuix Imager supports.

2. Drag and drop evidence from your computer into the Evidence Tree on the left-hand side of Nuix Imager.
   Do this after you find the local, network, or cloud account evidence.

Access local evidence

Local evidence is an individual file or directory that is accessible from the computer currently running Nuix Imager. This includes mapped network drives. The following options are available to import.

Option	Description
Files	Select files from a computer, network, or external drive (For example, PST, EDB, NSF, MBOX, and so forth.)
Folders	Select a directory that includes all files to be processed.
Split-DD Image	Select the initial DD image file from a directory to add to the case. **Note:** DD files can be segmented image format files. All file segments for the same image must reside within the same directory. Adding the initial of the leading segment file adds the remaining segments as well. Choose this option to add any kind of split file.
This Computer	To include all available files contained on the local computer, including logical and physical drives attached to the computer.
Local Disks	To add a specific local disk from the local computer.
Centera Cluster	Connects to and extracts source data directly from a Centera Cluster. **Note:** The Centera Cluster option is only available for the Email Archive Examiner and Ultimate Workstation licenses. In the dialog box that appears, use the drop-down menu next to each of the following to select a valid file: • IP address file • Clip file Once you have selected the files, click **OK**.

Extract network evidence

Network evidence is the content hosted on a local server that is accessible through a network connection. Nuix Imager allows you to connect to and directly extract the data from the following:

- Amazon S3 buckets
- Documentum servers
- Exchange servers
- Mail stores
- Microsoft Office 365
- Microsoft SQL servers
- Oracle databases
- Secure Shell (SSH) servers
- SharePoint servers
- Twitter accounts

This section details how to connect to these servers, stores, databases and accounts in the alphabetic order they are listed in.

Extract from Amazon S3 buckets

To connect to and extract source data directly from Amazon S3 buckets using web services, complete these fields:

Field	Description
Saved Credentials	Allows you to select a saved credential from the list. They are stored for the evidence type in Global Options or Preferences.
Allow credential discovery automatically discovers credentials when they are not supplied.	
Access Key	Enter your Amazon-provided Access Key and Secret Key for the S3 account.
Secret Key	
Endpoint	Optionally, enter the URL of the S3 server to connect to a specific region, for example, https://s3.amazonaws.com.
Bucket (along with Path)	Enter a bucket name. If none is specified, then all buckets in the account will be ingested. You can limit the ingestion to a specifically named bucket or to a folder in the bucket by specifying a bucket name followed by a path. If this is omitted, all buckets in the account are ingested, for example, "com.company.testbucket/nested/folder".

If a bucket that allows anonymous access is supplied, then credentials are not needed. Otherwise, you **must** provide one of the following:

- Access Key and Secret Key provided by Amazon for the S3 account
- Credential store, by selecting a previously stored set of credentials
- Credential discovery, to automatically discover credentials from the AWS library and include a system property

The ingestion can be limited to a specifically named bucket or to a folder in the bucket by specifying a bucket name followed by a path, for example, "com.company.testbucket/nested/folder". If you do not specify a bucket, then all buckets in the account are ingested.

You can usually leave the endpoint unspecified. However, you can use it to force the service to connect to a particular S3 server, useful when connecting to a specific region.

Extract from a Documentum server

To connect to and extract source data from OpenText Documentum Server:

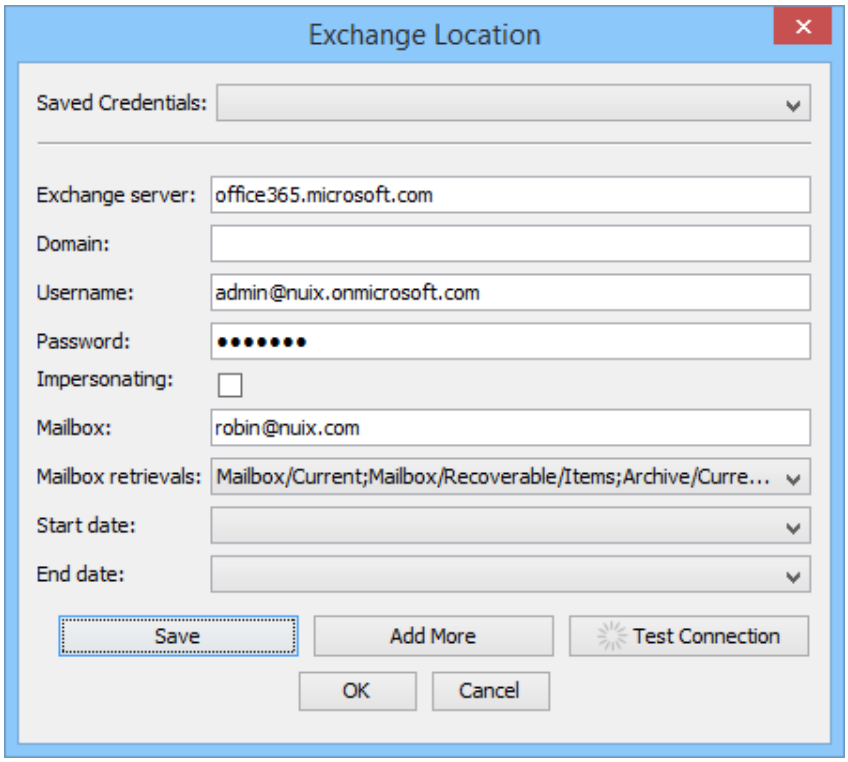
1. Select the **Documentum Server**, so the **Documentum Location** window appears.
2. Provide the following:
    a. Server address
    b. Port
    c. User credentials
    d. Domain, query (by default, the query is “*select * from dm_document*”)
    e. Your docbase
    f. Your property file (this must be a valid file)
3. Click **Retrieve Docbases** to ensure you are connected to the server and retrieve the docbases.
4. Click **OK** to process data.

Extract from an Exchange server

This procedure can also be used to connect to an Office 365 instance of Exchange.

To connect to and extract source data directly from an exchange server (2007-2016) using Exchange Web Services (EWS):

1. In the **Exchange Location** dialog box, in **Saved Credentials**, provide the appropriate credentials to collect information from this source.
2. Specify the **Exchange server**.
   A valid Exchange server takes the following form: "https://ex2010.company.com/ews/exchange.asmx ". This example can also be specified as "ex2010.company.com" or with an IP address and the protocol, allowing the path to the web service to be added automatically.
3. Specify the Domain, Username and Password.
4. Select the **Impersonation** checkbox *if* you want to act as though you are the client for the purposes of retrieving the evidence.
5. Specify the Mailbox, .
6. In **Mailbox retrievals**, select the individual name of the user’s Mailbox and Archive, and select the check boxes for the folders you want to process.
7. Select the **Start date** and **End date** for the data being added, using the dropdown calendars.
8. Click **Save** to save these credentials in the credential store.
   These credentials can be loaded and/or saved when adding EWS mailboxes to evidence. To learn more about managing the connection and authentication information, see the *Credentials* section in the *Configuring Global Options* section.
9. Click **Add More** to add multiple mailboxes found at the same location by entering the user’s settings and pressing Ctrl + Enter to add mailboxes. Repeat until you have entered the credentials for all mailboxes in a specified location.
10. Once you have configured all the options, click **Test Connection** to ensure you are connected to the server, and click **OK**.



Use a Mail Store

To connect and extract data through a mail store:

1. Select an individual mail store via POP or IMAP.
   Use this method to connect to Novell GroupWise or for corporate mail servers that support POP and IMAP connections, and for loading Gmail, Hotmail, and other Internet-stored email data.
2. In the **Add Mail Store** dialog box, specify the following
   a. In **Mail store profile** select one the following: Gmail, Outlook, Yahoo!, Apple, AOL, Zoho, Mail.com, Yandex, GMX, and inbox.com
   b. In **Mail store type** select one the following: POP, POP+SSL, IMAP, IMAP+SSL, and GroupWise.
   c. Enter the server hostname and server port.
   d. Enter your user name and password.
   e. Click **OK**.

Note: Connecting to corporate mail servers can result in exporting large volumes of data, and therefore putting a heavy strain on the server. As best practice, store a binary copy of the items harvested from a Mail Store as pointers to items can often change within mail servers.

Once you have configured all the options, click **Test Connection** to ensure you are connected to the server, and then click **OK**.

Extract from Microsoft Office 365

Use this connector to retrieve data from Microsoft sources including Teams, Exchange, and SharePoint. This procedure involves that you do the following in this order:

1. Connect and extract source data directly
2. Configure connection details for the connector
3. Specify users or team names
4. Apply additional filters for ingested data

Nuix Connector for Microsoft Office 365 Guide

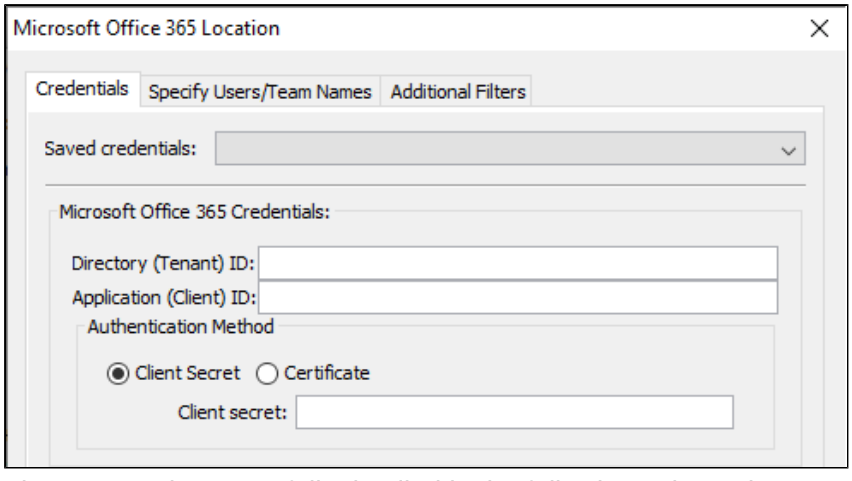
To use this feature, your Azure tenant must be configured by an Azure Global Administrator to enable authentication and specify the appropriate API data permissions. Refer to the *Nuix Connector for Microsoft Office 365 Guide* for more information about the connector and the Azure tenant configuration process. Download PDF documents from the Nuix Customer Portal.

To avoid reduced performance and potential data loss resulting from connection throttling, it is recommended to not use more than four workers when ingesting data from Office 365. If ingesting a single Exchange mailbox, the total number of workers should be further reduced to a maximum of two to ensure the best performance.

Connect and extract source data directly

To connect to and extract source data directly from a Microsoft 365 instance hosted on Azure:

1. Open the **Microsoft Office 365 Location** dialog box, and on its three tabs:
   a. Configure connection details for the connector.
   b. Specify users or team names.
   c. Apply additional filters for the data to be ingested.



   These procedures are fully detailed in the following sub-sections.
2. When you have defined options on all three tabs, review your selections and click **OK.**

Configure connection details for the connector

To configure connection details for the connector:

1. On the **Credentials** tab, enter details generated for the Nuix authentication application when registered in the Microsoft Azure portal.
   Contact your Azure Global Administrator if you need this information, OR if you previously saved the credentials for this connection, select them from the **Saved credentials** menu.

Property	Required	Description
Directory (Tenant) ID	Yes	The ID of the Azure Active Directory (AAD) tenant where the authentication application was registered.
Application (Client) ID	Yes	The application ID of the registered authentication application

2. Select one of the following authentication methods:

Method	Required	Description
Client Secret	Yes	Provide the authentication key string associated with the Application (Client) ID.
Certificate	Yes	Provide a PKCS#12 based private key certificate and password. **Note**: The certificate file must have a `.PFX` or `.P12` file extension.

3. Select the services and associated data types to ingest using the connector, as follows:

Service	Data Type	Description
Teams	Team Calendars	Retrieve Teams calendar data from all teams that a specific user is a member of. **Note**: If selected, you must provide credentials for a Microsoft Teams user to retrieve calendar data.
	Team Channels	Channel data such as chat messages and attachments from all public channels within a team. **Note**: User emoji reactions to chat messages are included as child items of the parent message.
	User Calendars	Individual user calendar data from the members of a team.
	User Chats	Chat messages from one-on-one or group conversations that take place outside of a public channel. **Note**: See the section on *Private Chat Limitations* for additional information at the end of the '*Use Microsoft Office 365*' topic.
Exchange	User Emails	Individual user mailboxes. **Tip**: Select Extract from mailbox slack space when configuring your data processing settings to also retrieve lower-level folders from the mailbox.
	User Contacts	Personal contacts that have been saved by individual users.
	Organizational Contacts	Contacts created by an administrator are shared with all users in an organization. Also known as Mail Contacts within Exchange.
SharePoint	SharePoint Data	Collect data from SharePoint sites, subsites, lists, and users. **Note**: The retrieval of SharePoint list attachments is not supported.

For all services, traditional and modern OneDrive for Business attachments are included as child items of the parent item.

Tip: Click **Save Credentials** to store the provided credentials to a profile for later reuse. If Certificate-based authentication is selected, only the path to the certificate on the local file system and associated password is saved. The certificate file is not stored within the profile.

---

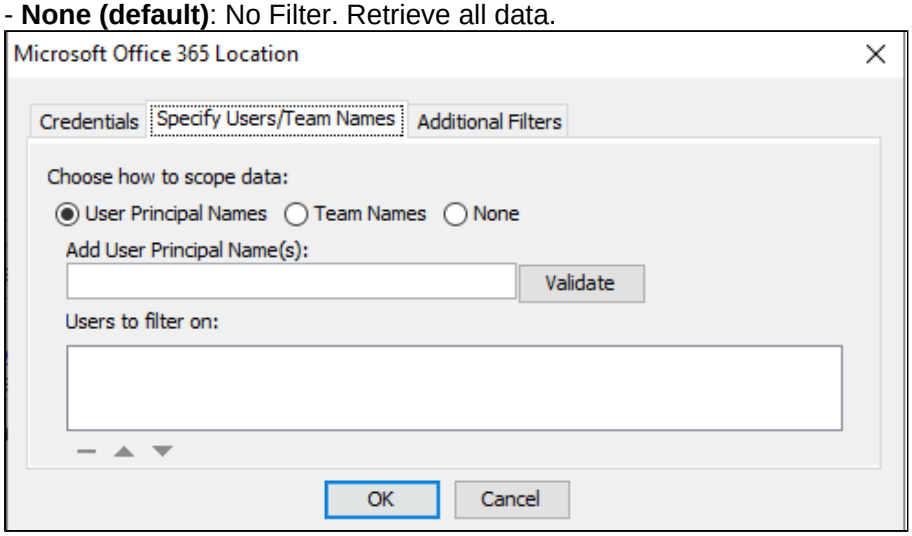
4. Click **Test Connection** to verify the connection details.
5. Once verified, proceed to the next section to define filters on the remaining tabs of the connector or click **OK.**

Also see *Private Chat Limitations* and *Workaround* at the end of this *Use Microsoft Office 365* topic.

Specify users or team names

To narrow the data retrieved from the Microsoft Office 365 connection by filtering on specific users and or Team names:

1. On the **Specify Users/Team Names** tab, select one of the following filters listed at the top of the tab:
   - **User Principal Names**: To retrieve data from specified users only.
     (A User Principal Name (UPN) is the name of a Windows Active Directory system user in the format of an email address. For example, john.doe@domain.com.)
   - **Team Names**: Retrieve data from specified teams only.
   - **None (default)**: No Filter. Retrieve all data.



2. In **User Principal Name(s)**, based on the selected filter, enter a semicolon-separated list of either UPNs *or* Team names.
   (SharePoint data is unable to be filtered by UPN.)
3. Click **Validate** to verify the entries and add them to the filter.
   If any names are invalid, the connector will specify which values could not be found.

Tip: Prior to starting ingestion, you can view a list of available user and team names by selecting **None** as the filter option and then **OK** to exit the connector configuration. Proceed to the Pre-Filter Evidence view to see results. You can also use Nuix Imager to preview the data set.

---

4. Once validated, click **OK** to return to the **Add/Edit Evidence** page or proceed to the next tab to define additional filters on the remaining tab of the connector.

Apply additional filters for ingested data

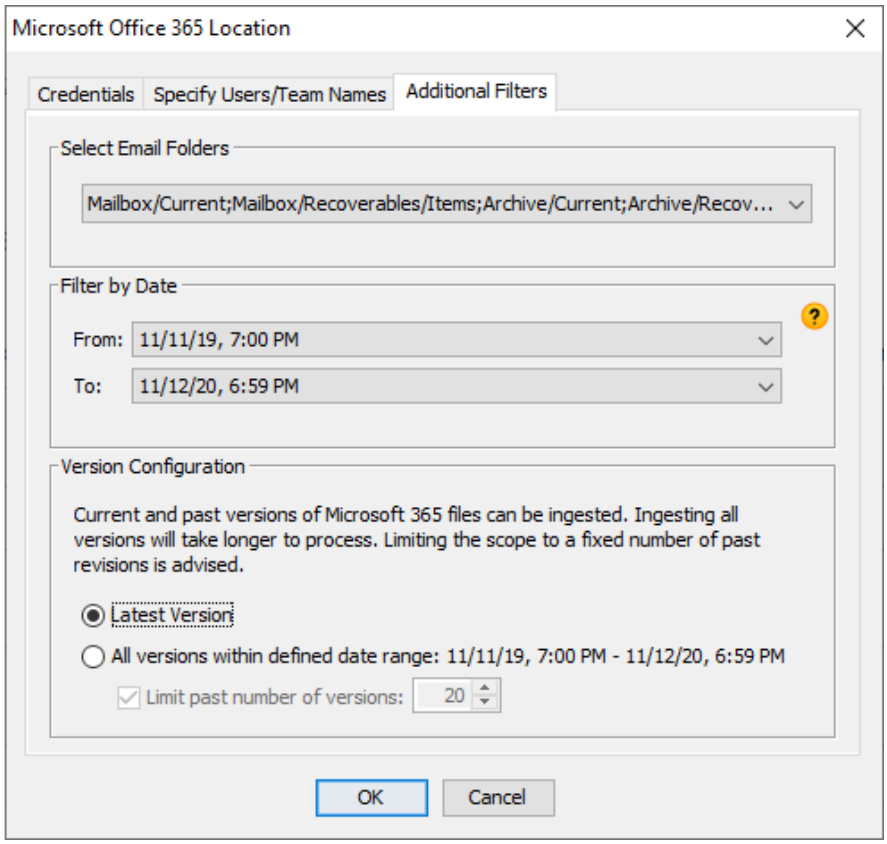
To apply additional filters to the data being ingested:

1. On the **Additional Filters** tab, in **Select Email Folders**, select one of the following to specify the types of Exchange mailbox folders to retrieve:

Note: If you did not select the Exchange service on the **Credentials** tab, this filter will not affect data.

- **Account:** All mailbox folders available within the account
- **Mailbox**: Current mailbox data and recoverables such as deletions and purges.

- **Archive**: Archived mailbox data and archived recoverables such as deletions and purges.
- **Public Folders**: Shared folders within an organization.



Exchange Limitations: In-Place archives included within user mailboxes and Inactive mailboxes cannot currently be collected using the Microsoft Graph API.

Data from inactive mailboxes, however, can be extracted using the Microsoft Security & Compliance Center and then ingested. See the Microsoft topic: Search and export the contents of an inactive mailbox for more information.

2. Under **Filter by Date**, use the calendar selectors to define how to retrieve only the items that have a Last Modified date within the specified date range.

Note:

If there is no Last Modified date, the item's Creation Date is used. The filter defaults to one year, starting 365 days prior to the current date. If retrieving calendar data, the date range **cannot** exceed five years (1825 days).

This filter only applies to the following Office 365 item types:
- Exchange mail messages
- Teams chat messages
- Calendar events (filtered by scheduled event start time)
- Resources from SharePoint and OneDrive for Business

---

3. Under **Version Configuration**, choose either of the following options:
   - **Latest Version** to ingest the latest version of a file or attachment (selected by default)

- **All versions within defined date range** to ingest all available versions within a specified date range, and verify that the displayed date range is correct.
  Only files with a Last Modified date within the range will be ingested.
  To modify the date range, update the **From** and **To** values in the **Filter by Date** section.

4. Optionally, select the **Limit past number of versions** checkbox to restrict the number of retrieved versions to a specified number.

This filter applies to all files and attachments retrieved from Microsoft 365 in which versions are maintained, including data from SharePoint, OneDrive for Business, and Teams.

After ingestion is complete, the following version-related metadata is included on all applicable items and can be viewed and queried in the case:

Metadata	Value	Description
`Flag: versioned`	boolean	Indicates that multiple versions of the selected item exist and have been ingested.
`Flag: current_version`	boolean	Indicates if an item is the most recent version. Determined at the time of ingestion.
`Property: Version Age`	integer	Identifies the version of the selected item in relation to the latest known version. A value of 0 represents the latest version. Each increment of 1 indicates a subsequent older version. **Warning**: If you update the data in a case by reloading the source data or scanning for new child items, the Version Age of an item changes if newer versions of that item are found.
`Property: Version Group ID`	string	A unique identifier that is used to link all versioned items from a single original document. The Version Group ID value is derived from the original item's `ID` value.
`Property: Version Value`	integer	Identifies the exact version of the selected item based on source data. **Note**: Microsoft 365 uses a basic sequential numbering method (1.0, 2.0, 3.0) when assigning version values. Other data sources may assign non-readable values, such as a hash, when defining this value.

The following table contains example queries that can be used after ingestion to locate versioned items within a case:

Example Query	Description of Results
`flag:versioned`	Returns all items that have multiple versions.
`flag:(versioned AND current_version)`	Returns the latest version of each item that has multiple versions.
`flag:(versioned AND NOT current_version)`	Returns all versions of an item except for the latest version.
`integer-properties:"Version Age":(0 to 10)`	Returns the most recent version (indicated by `0`) and the previous 10 versions.

`properties:"Version Value:2.0"`	Returns all items that have a version value that matches the value specified in the query (2.0).
`properties:"Version Group ID: <GROUPIDGUID>"`	Returns all versions of an item, including the original, that match the group ID specified in the query.

When finished, review your selections on the previous tabs or click **OK.**

Private Chat Limitations

Due to restrictions in how private chat data is retrieved using the Microsoft Graph API, certain limitations exist when determining the recipients of specific messages within a chat. Limitations include:

- Chat/conversation IDs are only generated when a new chat is initiated. The generated ID is persisted for the entire life of the chat, regardless of whether participants are later added or removed.
- The To communication metadata property, which identifies the participants of a chat, represents only the list of participants that are included in the chat at the time of ingestion. Due to this limitation, the following must be considered:
  - New participants who are added to an existing conversation are identified in the metadata as a chat recipient. However, based on the chat history settings selected when adding the new participant, they may or may not have been granted access to view messages that were sent prior to them joining the chat.
  - Participants who left a chat after receiving messages will not be identified in the metadata as a recipient at all.

Workaround: To establish a complete view of recipients and verify who received messages from a private chat conversation, examine the specified private conversation from the /Users/<userName>/Chats directory of each suspected participant.
For example:
To verify if John saw a specific private chat message, examine the messages located in /Users/John /Chats. Looking at the same chat but from a different participant, /Users/Jane/Chats, may not properly confirm if John saw a specific message because Jane's chat history may be incomplete and reflect only a portion of the conversation due to the limitations previously noted.

Extract from a Microsoft SQL Server

To connect to and extract source data directly from a live Microsoft SQL Server engine instance:

1. Ensure the following:
   a. Your Database Administration procedures are current, including backup and recovery. The engine instance must be configured to allow TCP/IP connections.
   b. You remove any firewall restrictions between the Nuix Workstation application and the database instance to allow the connection.
   c. The engine instance is live but idle.
   Any concurrent activities performed when the content is being read or being reviewed and analyzed can produce inconsistent Nuix Workstation results.
   d. The credentials used to connect to the Database have the necessary permissions to read the content.
   Nuix recommends you use the System Administrator (‘sa’) account, or another account with a fixed server role ‘sysadmin’. Ask your Database Administration support for more information.
   Find further information on the Microsoft SQL Server product at https://www.microsoft.com/en-us/sql-server.

2. In the **MS SQL Server Instance** dialog box, specify the server name and username and password.
3. Optionally specify the following parameters, as necessary:
    a. Instance name (depends on the engine configuration)
    b. Domain (requires credentials to access the server)
    c. Query (the consistent SQL query to filter the content)
    A query parameter is an advanced option that allows you to specify the SQL query to obtain the data, including the use of SQL JOIN to combine different databases and tables. It is intended for users with proficient SQL knowledge.
4. To select all data from a known list of databases and/or tables, use the Pre-Filter Evidence dialog box to specify the required data.
5. Click **Test Connection** to ensure you are connected to the server.
6. Click **OK** to process data.
7. Check your database client utility if you encounter a problem while connecting.

Use an Oracle database

To connect to and extract source data directly from a live Oracle database instance:

1. Heed all warnings stated in the previous **Use Microsoft SQL Server** section.
2. In the **Oracle Instance** dialog box, enter the following parameters:
    a. In **Database**, also known as the <database> description, is one of the following:

```
//<host>:<port>/<service>
<host>:<port>:<SID>
<TNSName>
```

    This Database value connects to a database with service litmus through port 1521 of host myserver:

```
 //myserver:1521/litmus
```

    This Database value connects to the same database using the SID inst1:

```
myserver:1521:inst1
```

    b. Enter the user name and password.
    c. In **Role**, specify the role to connect as. For example, when connecting with the “SYS” user account, the role should be “SYSDBA” or “SYSOPER”.
    d. In **Query**, specify if you want to supply an SQL SELECT query to filter the content, including the use of SQL JOIN to combine different databases and tables.
    e. In **Max Rows**, specify how to limit the number of rows returned from each table.
    f. Click **Test Connection** to ensure you are connected to the server.
    g. Click **OK** to process data.
    h. Check your database client utility if you encounter a problem while connecting.

Extract from a Secure Shell (SSH) server

To connect to and extract source data directly from a Secure Shell (SSH) Server:

1. Select the **Secure Shell (SSH) Server** option to view the following settings enabled and set or selected by default:
    a. **Port:** Set to 22 - which you can adjust up or down using the arrows to the right of the box.

   b. **Access Remote Files:** If you use this, you can set an Initial remote folder to speed up initial remote access.
      This is helpful if you want to narrow the scope of the data by using a certain directory.
   c. **SSH Key Pair Authentication**
2. Enter your Host Information, User Name and, if you selected Password Authentication, a password for the remote access you want to set up.
3. Optionally, also select **Access Remote Disks**.
4. If necessary, also select a Key Folder from which to select files.
5. If you use a “sudo” password, which allows access to write-protected files and folders, enter it in this box.
   Using a user name and password instead of a key pair automatically attempts sudo access on read-protected files.
6. Click **Test Connection** to ensure you are connected to the server.
7. Click **OK** to process data.

Extract from a SharePoint server

Nuix Workstation supports SharePoint extraction from servers hosted in O365 Online or On-premise servers.

To access the required SharePoint server, you must have an administrator account to select from the following:

- **O365 Online:** Microsoft provides online SharePoint servers hosted in O365 or the Azure environment.
  If you deploy your server in Azure or directly and use the servers that Microsoft provides, then you need the clientId/clientSecret of a 'SharePoint Add-In App', and do not need a SharePoint account credential.
- **On-premise:** If you deploy the server on premises, ensure you have the user credentials for the administrator account or any account you want to investigate.

To add a SharePoint Server:

1. Create a server URL hosted in O365 Online or Azure environment.
2. Create a domain name, for example, if the server URL is https://website.com then 'website.com' (URL without protocol) is the domain name.
3. Assign permissions to the client ID generated in the previous step,

```
<AppPermissionRequests AllowAppOnlyPolicy="true">
   <AppPermissionRequest Scope="http://sharepoint/content/sitecollection" Right="Read" />
</AppPermissionRequests>
```

   OR

```
<AppPermissionRequests AllowAppOnlyPolicy="true">
  <AppPermissionRequest Scope="http://sharepoint/content/sitecollection" Right="Read" />
  <AppPermissionRequest Scope="http://sharepoint/content/sitecollection/web" Right="Read" />
  <AppPermissionRequest Scope="http://sharepoint/content/sitecollection/web/list" Right="Read" />
</AppPermissionRequests>
```

   OR, if you have tenancy permissions:

```
<AppPermissionRequests AllowAppOnlyPolicy="true">
```

```
    <AppPermissionRequest Scope="http://sharepoint/content/tenant" Right="Read" />
</AppPermissionRequests>
```

4. Click **Trust It** to continue.
5. Enter the SharePoint location details:

Field	O365 Online/ Azure	On-premise
SharePoint server	Enter the server URL hosted in O365 online or Azure environment or the exact URL of the site that is being collected.	Enter the endpoint URL to the SharePoint server for On-premise.
Domain	Enter the domain name. For example, if the server URL is https://website.com , then enter 'website.com' (URL without protocol) as the domain name.	Enter the domain name of this user. Nuix recommends to leave it empty if you just want to use the REST services.
Username	Enter the clientId of a SharePoint Add-In app.	Enter the username of the account you want to investigate or the username of an administrator account of this server.
Password	The client secret of the SharePoint Add-In app.	Enter the appropriate password associated with your username.

6. Select **Test Connection** to test the connection and credentials.
7. Click **OK**.

Configure SharePoint Servers to use REST APIs

The SharePoint servers do **not** provide access to REST APIs by default. You must configure them on the servers to be able to invoke them.

Configure On-premise SharePoint servers

Ensure you have Nuix Workstation and a SharePoint server on the same network.

To configure for On-premise servers, use basic authentication in Internet Information Services (IIS).

To update the settings in IIS:

1. Log in to the virtual machine on which the SharePoint server is hosted.
2. Go to **IIS**, select **Sites**, select **Intranet**, right-click **Basic Authentication**, and then click **Enable**.

To update the settings in the SharePoint server:

1. Select the **Settings** option in the top right corner of the main page and click **Site settings**.
2. Select **Users and Permissions** and click **Show users** to see all the user details.
3. Select the **Everyone** check box and click **Edit User Permissions**.
4. Select one of the following permissions and click **OK**.
    a. **Full Control**: for full control
    b. **Read**: for permission to view pages and list items and download documents

Configure O365 servers

To configure an O365 server:

1. Create a SharePoint Add-In, and to register the Add-in in SharePoint:
    a. Navigate and log in to the SharePoint online site.
    b. Navigate to the Register Add-in page by entering the URL in the browser as *https://<sitename>.SharePoint.com/_layouts/15/appregnew.aspx*
    c. Generate your Client Id and Client Secret and click **Create**. Ensure the Redirect URI requests an 'HTTPS'.
    All information regarding the Add-In appears. Record the details for future reference.
2. On registering the Add-In, set permissions to access the SharePoint data. Set the Read permission level to the web scope to be able to read the web information:
    a. Navigate to the SharePoint site and enter the URL 'https://<sitename>.sharepoint.com/_layouts/15/appinv.aspx' in the browser. It redirects you to the Grant permission page.
    b. Enter the Client ID in the App Id text box and click **Lookup**. It populates the value for the following fields: Title, App Domain, and Redirect URL.
    If Lookup does not populate the other field values, enter them manually.
    c. Update the Permission Request XML as follows and click **Create**.

```
<AppPermissionRequests AllowAppOnlyPolicy="true">
   <AppPermissionRequest Scope="http://sharepoint/content/sitecollection" Right="Read" />
   <AppPermissionRequest Scope="http://sharepoint/content/sitecollection/web" Right="Read"
/>
   <AppPermissionRequest Scope="http://sharepoint/content/sitecollection/web/list" Right="
Read" />
</AppPermissionRequests>
```

    d. In the page that appears, click **Trust It**. This enables you to invoke the REST APIs on the server.

Permissions required for SharePoint ingestion

To perform a SharePoint Collection you can use the built-in Contribute/Design/Full permissions or you can create a custom permission level that includes browsing and opening features.

The recommended way to configure this, for a Nuix ingestion account that has true read-only permissions to SharePoint, is to:

1. Create a new permission level, which is a copy of the Read permission level with the browse directories permission enabled.
2. Create a new group with this new permission level.
3. Add the Nuix ingestion user to this group.
4. Provide this user's credentials to Nuix for ingestion.

Extract from a Twitter account

This option supports Twitter historical data by getting a list of the recent tweets with an approximate return of up to the latest 3,200 tweets. On selecting this option, the Twitter Historical Data window appears.

Note: This feature requires users to have their own API key.

To connect to and extract source data directly from a Twitter account:

1. Create a Twitter App and Access Token, as follows (which is only a recommendation):
    a. Register your own Twitter developer account at https://developer.twitter.com/.
    b. Create your own app at https://developer.twitter.com/en/docs/basics/authentication/guides/access-tokens.
    c. Obtain an access token at https://developer.twitter.com/en/docs/basics/getting-started, where you can also perform steps 1 and 2 as well.
2. Enter your Twitter account details with the Consumer Key, Consumer Secret, Access Token, Access Token Secret, and Screen Name.
3. Click **Test Twitter Connection** to check if your Internet connection to Twitter is working, your credentials are authorized, and if the screen name you provided is valid.

Import cloud account evidence

Cloud account evidence is content stored using a cloud storage service. Nuix Imager allows you to connect to and directly import the data from the following cloud accounts:
- **Apple iCloud, Google** and **Microsoft OneDrive** accounts
- **Box** and **Dropbox** accounts

This section details how to connect to these accounts in the alphabetic order they are listed in.

Import from an Apple iCloud, Google Drive, or OneDrive account

Add Apple iCloud account

To connect to and extract source data from your Apple iCloud account, including iCloud drive files, iOS backup, and ubiquity data:

Note: Two-Factor Authentication is supported for iCloud data, but not for iOS backups.

---

1. On receipt of your two-factor authentication code on your device, provide your account and password information.
2. Click **Test Connection** to ensure you are connected to the server, then click **OK**.

Add a Google Drive account

To connect to and extract source data from your Google Drive account:

1. Select the **Add Google Drive Account** option to open the Google sign-in window.
2. Enter your Google sign-in details.
3. Click **Allow** once you are ready to authenticate.

Add Microsoft OneDrive account

To connect to and extract source data from your Microsoft OneDrive:

1. Select the **Add Microsoft OneDrive Account** option to open the Microsoft sign-in window.
2. Enter your Microsoft sign-in details.
3. Click **Allow** once you are ready to authenticate.

Import from Box and Dropbox accounts

Connect to and extract source data from either a Team or Individual Dropbox account.

Add a Box account

1. Select the **Box Account** option. The Box login page appears.
2. Enter your login details, and click **Authorize.**

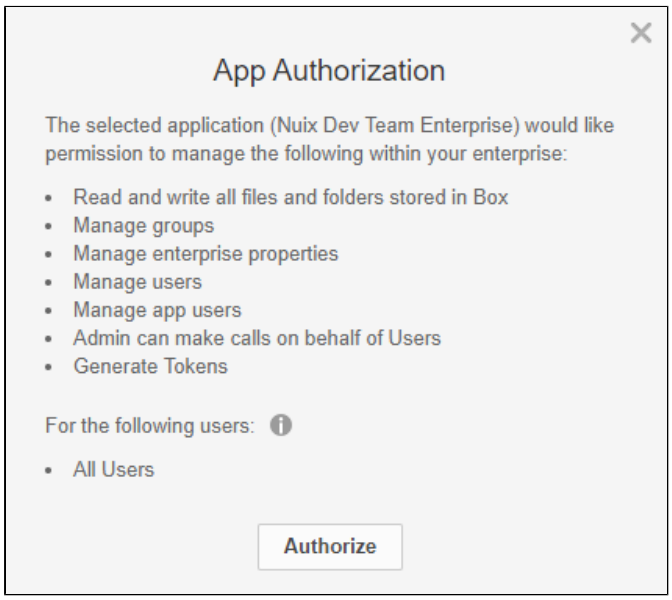
Add an Enterprise Box account

To connect to and extract source data from your Enterprise Box account:

1. Sign up for a developer account at https://app.box.com/developers/console.
2. Create an Enterprise App using the **OAuth 2.0 with JWT authentication** option for Server authentication.
   This allows you to retrieve folders from your Box account with a Developer token.
3. In the **Advanced Features** section, enable **Perform Actions as Users** and **Generate User Access Tokens**, and click **Save**.
4. Next, generate a Certificate to allow your browser to download the config.json file.

   Note: Store the config.json file you create securely, as you cannot download it again.

5. Sign in to your Box account, and from the Admin Console, go to **Enterprise Settings** and then to the **Apps** tab to authorize your new app.
6. When prompted to supply an API key, do so in the value next to ‘clientID’ in the config.json file.
7. When the following screen appears, confirm all details match your setup and click **Authorize**.



Add Dropbox team account

To add a Dropbox team account:

1. Select the **Add Team Account** option. The Dropbox login page appears.
2. Enter the login credentials, and click **Sign in**. The team account authentication page appears.
3. Click **Allow** to proceed. In the Pre-Filter Evidence panel, a list of all the accounts in the team appears.
4. Select the accounts to ingest and click **OK**.

Add Dropbox individual account

To add a Dropbox individual account:

1. Providing the credentials to the account to ingest per the preceding *Add Dropbox team account*. In the Pre-filter Evidence panel, only the individual account is listed to ingest.
2. Click **OK** to proceed.

Export evidence

Through its **Export** menu, Nuix Imager provides several ways to export the evidence imported into the application, and allows you to curate items together and export items as a set or individually.

This sections covers the following topics:
- Export a disk image
- Export a logical image
- Export items of evidence as a report or digest
- Export a list of evidence items as a report or digest

Export a disk image

To export the disk image of the evidence to an output directory:

1. In Nuix Imager, select the **Export** menu, and the **Export Disk Image** option.
2. Under **General Settings**, enter or select details as follows:
    a. In **Image Type**: Select either RAW or E01.
    b. In **Output Directory**: Enter the directory where the output file is saved after export.
    c. In **Image Base Name**: Enter the name given to the image export.
    d. In **Case Number**: Enter the reference number of the case where the image is exported. This number depends on how cases are named.
    e. In **Evidence Number**: Enter the reference number of the piece of evidence where the image is exported to. This number depends on the way evidence is named.
    f. in **Examiner**: Enter the examiner for the case.
    g. In **Description**: Enter a brief description of the images.
    h. In **Notes**: Enter a brief note about the image.
    i. In **Model Number**: Enter the number for the disk being exported.
    j. In **Serial Number**: Enter the serial number of the device being exported.
    k. In **Verify image after writing**: Select to have Nuix Imager verify the data after exporting.
3. Under **Image Settings**, complete details as follows:
    a. In **Compression Type**: Select the type of compression to be used during the export:
        - **No Compression**
        - **Fastest Compression** (default setting)
        - **Smallest File Size**
    b. In **Split Image into Segments**: Select this check box to split the image.
    c. In **Segment Size**: If you have selected the preceding option, then enter the size of each segment. The default setting is 2GB.
    The progress of the export appears, including the export rate (how fast the export is occurring) and the estimated remaining time.
4. To view the current status of the binary template, click the arrow in the Current binary block.
On export completion, a confirmation message appears.
5. Click **OK** to exit the window.

Alternatively, select the required item of evidence, right-click it and from a context menu, select **Export Disk Image**.

Export a logical image

To export a logical image of the evidence to an output directory:

1. In Nuix Imager, select the **Export** menu, and the **Export Logical Image** option.
2. Enter or select details as follows:
    a. In **Output Directory**: Enter the directory where the output file is saved after export.
    b. In **Image Base Name**: Enter a name for the image export is populated by default. Update the name, if required.
    c. In **Case Number**: Enter the reference number of the case you are exporting the image to.
    d. In **Evidence Number**: Enter the reference number of the piece of evidence you are exporting the image to.
    e. In **Examiner**: Enter the examiner for the case.
    f. In **Description**: Enter a brief description of the image.
    g. In **Notes**: Enter a brief note about the image.
    h. In **Compression**: Select one of these compression types to use during the export:
        - **No Compression**
        - **Fastest Compression** (default setting)
        - **Smallest File Size**
3. To view the current status of the binary template, click the arrow in the Current binary block.
   On export completion, a confirmation message appears.
4. Click **OK** to exit the window.

Alternatively, select the required item of evidence, right-click it and from a context menu, select **Export Logical Image**.

See Take a Nuix logical image for other information.

Export items of evidence as a report or digest

To export items of the evidence to a selected directory as a report or a digest type:

1. In Nuix Imager, select the **Export** menu, and the **Export Items** option.
2. Select one of the following options:
    - **Generate Item details report**
    - **Compute MD5 digests**
    - **Compute SHA-1 digest**
3. Click **OK** to exit the window.

Export a list of evidence items as a report or digest

To export the list of evidence items to a selected directory as a report or a digest type:

1. In Nuix Imager, select the **Export** menu, and the **Export Item List** option.
2. Select one of the following options:
    - **Generate Item details report**
    - **Compute MD5 digests**
    - **Compute SHA-1 digest**
3. Click **OK** to exit the window.

View encrypted data by OS

This section explains full disk encryption by operating platform.

View encrypted data in a Windows OS

Adding a logical drive as evidence enables you to inspect an encrypted disk in the Windows OS.

For example, if *C:// *is encrypted using BitLocker, viewing the contents of \\.*PhysicalDrive0* shows the encrypted volume, but the file system is not readable.

Adding the logical drive *C:// *enables the contents of the file system to be read as long as Windows has decrypted the volume.

View encrypted data in a macOS/FileVault

Under macOS, the kernel creates a second disk device for the unencrypted copy of a FileVault drive. For example, if the original device is named *rdisk0*, then a device called *rdisk1* is created for the unencrypted copy of the drive.

The device numbers do not have to be in sequential order. A device with the name *rdisk3* may map to *rdisk6*. Examining the serial number that is extracted into metadata from both top-level devices shows the same serial and model numbers for both devices.

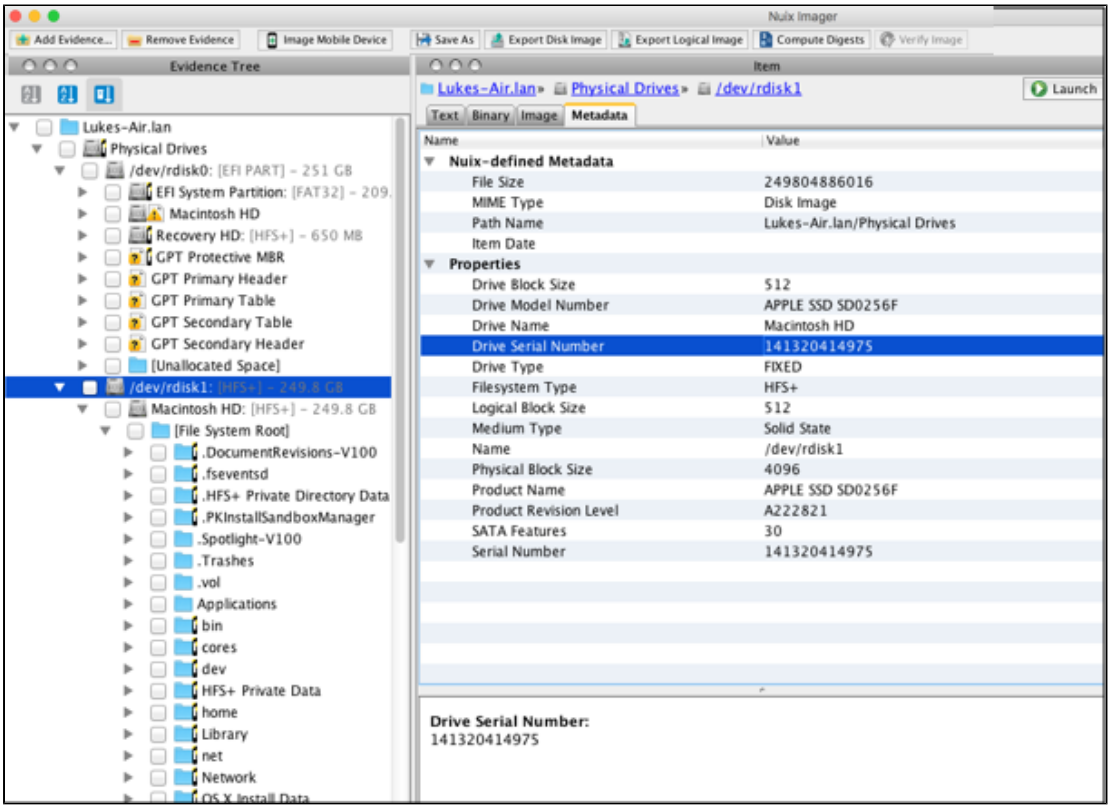


Image mobile devices

Nuix Imager can be used to image mobile devices such as phones, tablets, and watches (Apple and Android) to a logical image.

Prerequisites

To image an iOS or Android device, you must configure the device to trust the imaging computer.
To image an Android device, you must do a little more. Details follow in *Image an Android device*.

Set up iOS devices

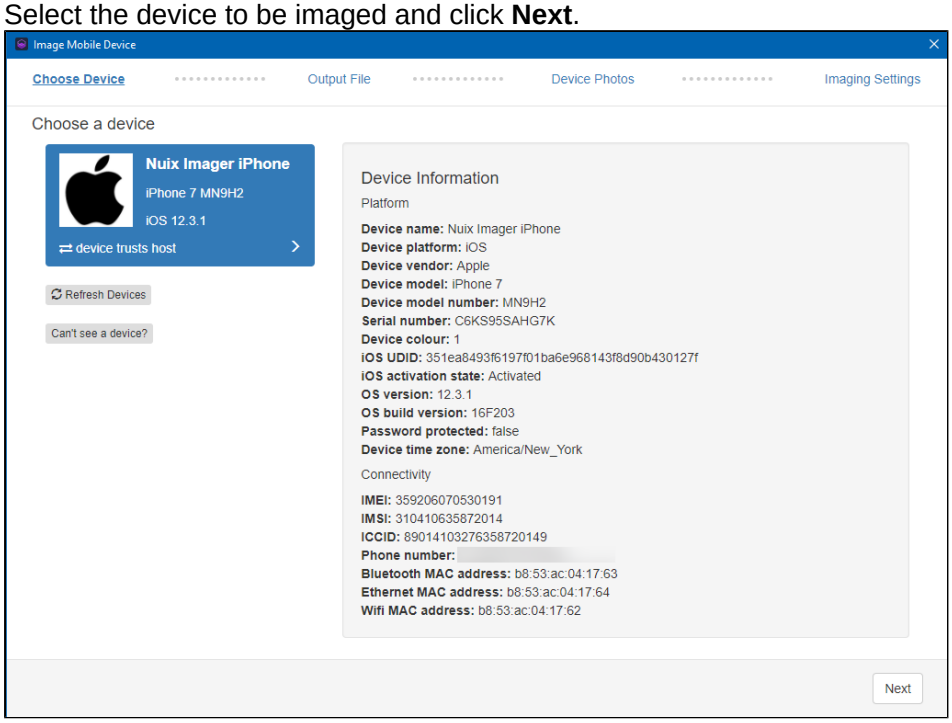
While Nuix Imager can extract the Calls and SMS databases from iOS devices, the Nuix Workstation engine does not currently support the decoding of the current database formats.

Nuix plans to support decoding of the latest Calls and SMS databases from iOS devices in a future release of Nuix Imager. In the meantime, contact Nuix Support for a workaround, should you need this feature for your iOS device extraction.

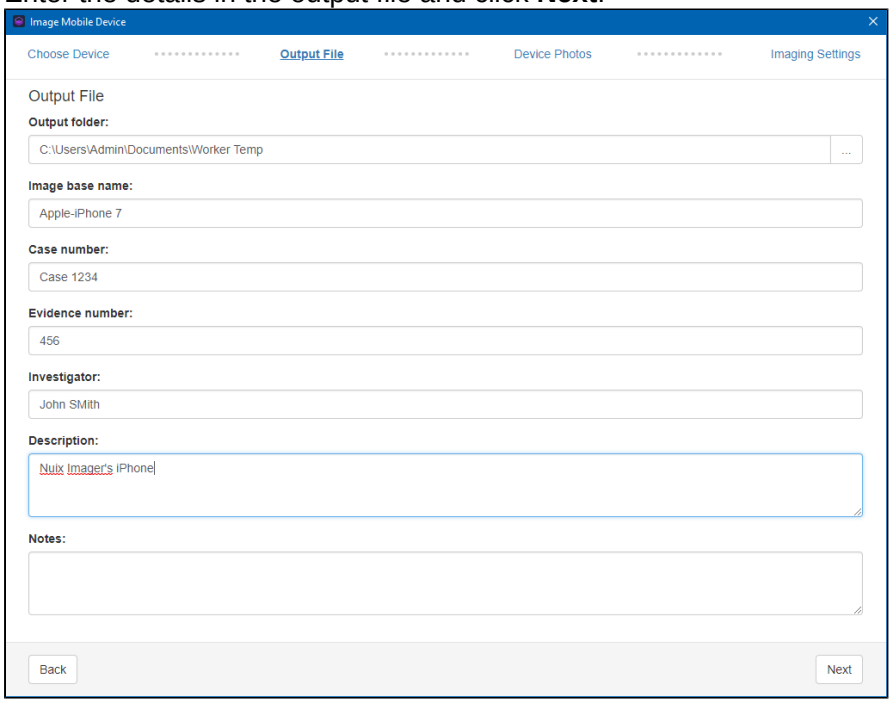
Image an iOS device

To image an iOS mobile device:

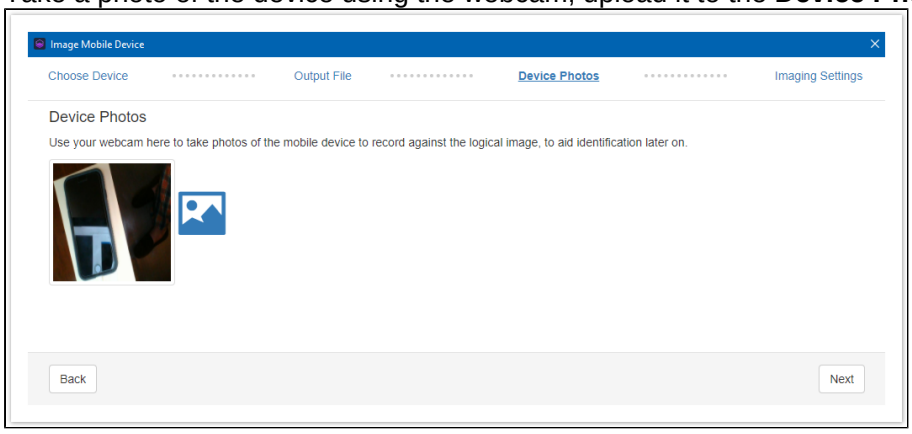
1. Select **File > Image Mobile Device** from the menu.
2. Select the device to be imaged and click **Next**.



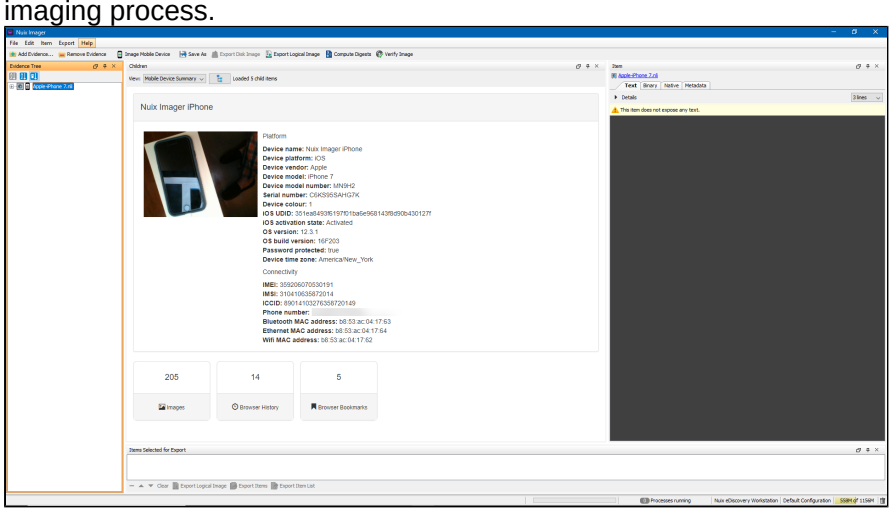
3. Enter the details in the output file and click **Next**.



4. Take a photo of the device using the webcam, upload it to the **Device Photos** tab, and click **Next**.



5. On the **Imaging Settings** tab, select **Image via Agent**, and click **Start Imaging**.
6. On completion, the newly created image automatically opens for you to inspect the result of the imaging process.



Set up an Android device

To set up an Android device:

1. Ensure the Android Debug Bridge (ADB) drivers are installed on the Windows computer for the Android device.
2. Navigate to **Settings,** select **About Phone/About Device > Software Info**, and tap the build number (as if it were a button) until **developer mode** is enabled.
   This normally takes about five to seven times.
3. Navigate to **Settings,** then go into **Developer Options** and enable **USB debugging**.
4. For first-time connections only, the following message appears:
   'Allow connections from a computer being used for USB debugging on the Android device being set up.'
   This message continues to appear unless you select **Always Trust**. The location of this setting can vary with the manufacturer or OS version of the device.

Note: Due to the many different versions of available Android devices, the preceding procedure may vary by Operating System and device. The amount of data extracted will also be impacted by these factors.

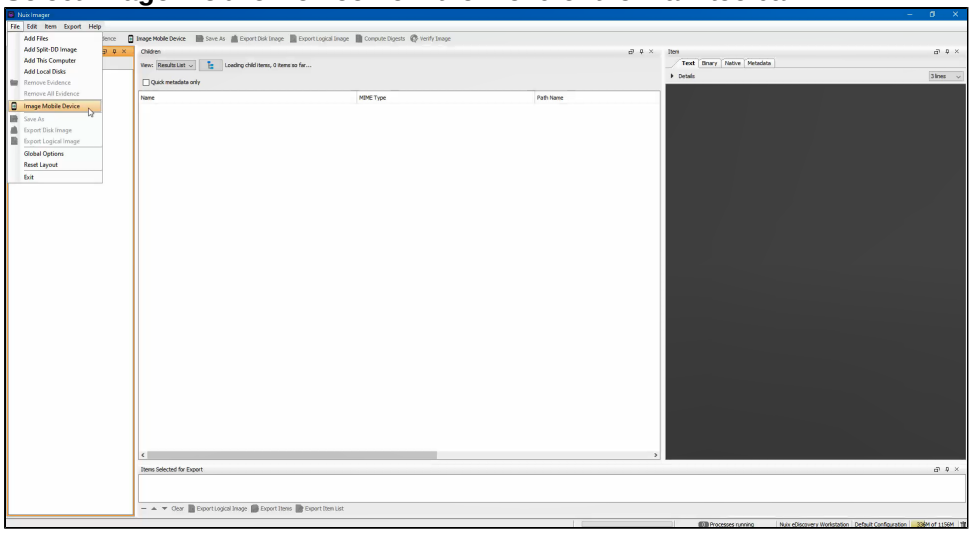
Image an Android device

Before you image an Android device, you **must** do the following:

1. Under **Developer Options**, enable USB debugging.
2. Unlock it so that it can to perform a full backup of the phone.

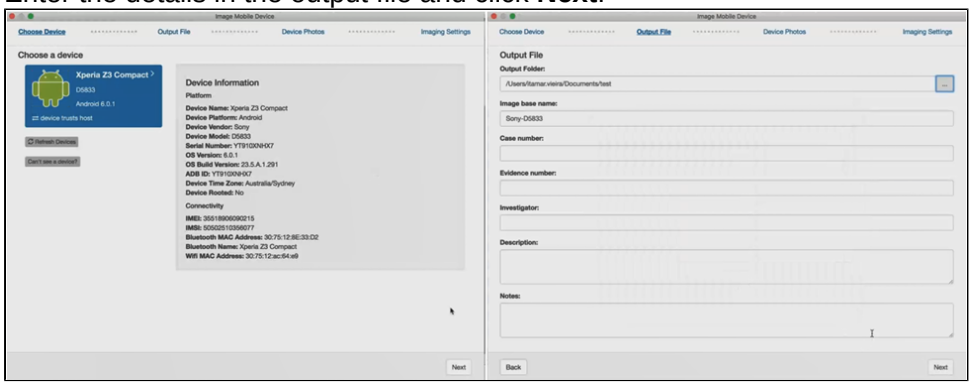
To image an Android device:

1. Select **Image Mobile Device** from the menu or the main toolbar.

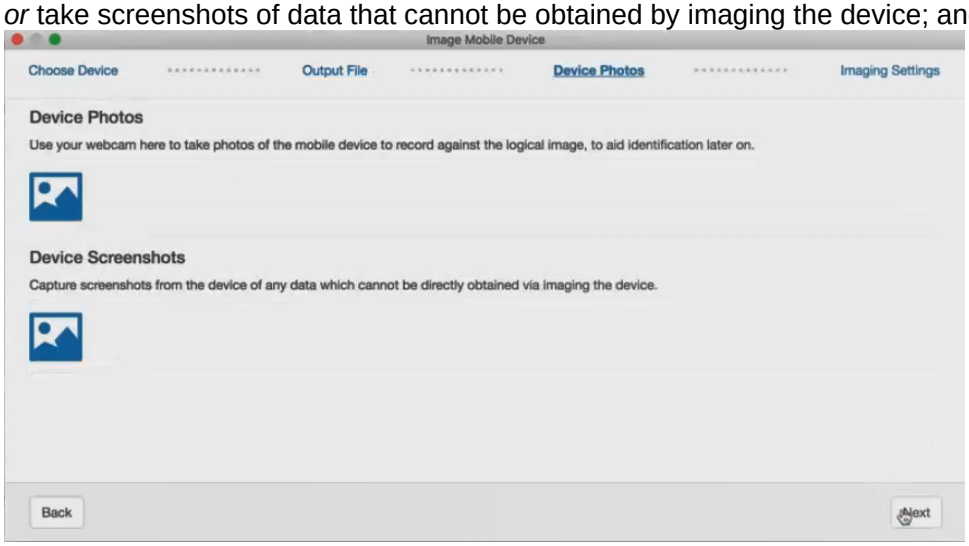


2. Select the device to be imaged and click **Next**.

3. Enter the details in the output file and click **Next**.



4. Optionally, take a photo of the device using the webcam and upload it to the **Device Photos** tab, *or* take screenshots of data that cannot be obtained by imaging the device; and click **Next**.

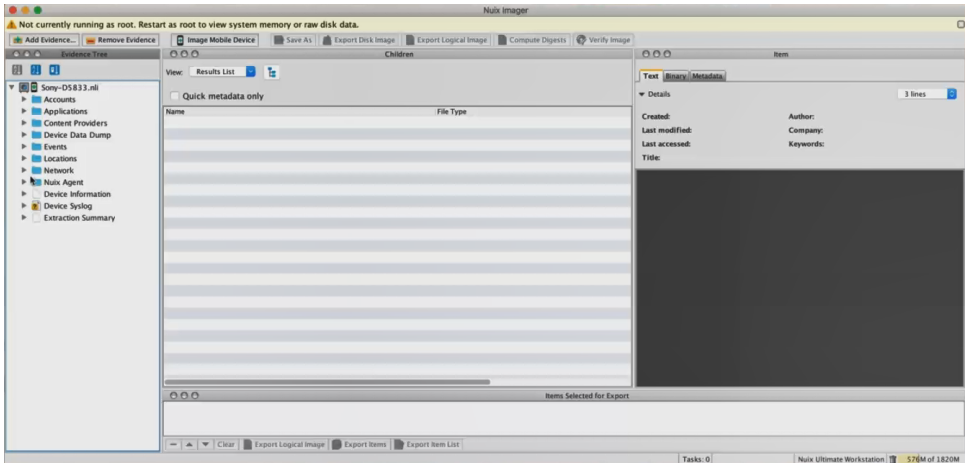


5. On the **Imaging Settings** tab, select one or more of these options: **Perform a backup**, **Image filesystem**, or **Image via agent.**
6. Click **Start Imaging** to start imaging the device.

Note: Your device's media transfer protocol (MTP) interface may yield some additional data. Image this interface to ensure that data is captured.

---

7. On completion, the newly created image automatically opens for you to inspect the result of the imaging process.


Nuix Imager
Not currently running as root. Restart as root to view system memory or raw disk data.
Add Evidence...
Remove Evidence
Image Mobile Device
Save As
Export Disk Image
Export Logical Image
Compute Digests
Verify Image
Evidence Tree
Sony-D5833.nli
Accounts
Applications
Content Providers
Device Data Dump
Events
Locations
Network
Nuix Agent
Device Information
Device Syslog
Extraction Summary
Children
View:
Results List
Quick metadata only
Name
File Type
Item
Text
Binary
Metadata
Details
3 lines
Created:
Author:
Last modified:
Company:
Last accessed:
Keywords:
Title:
Items Selected for Export
Clear
Export Logical Image
Export Items
Export Item List
Tasks: 0
Nuix Ultimate Workstation
576M of 1820M

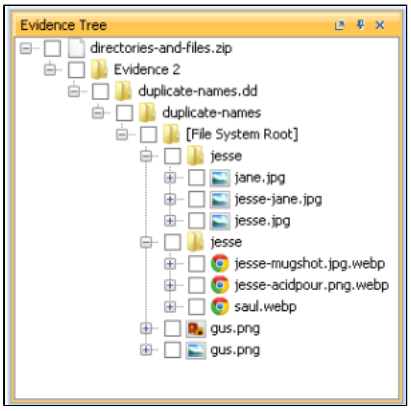
Take a Nuix logical image

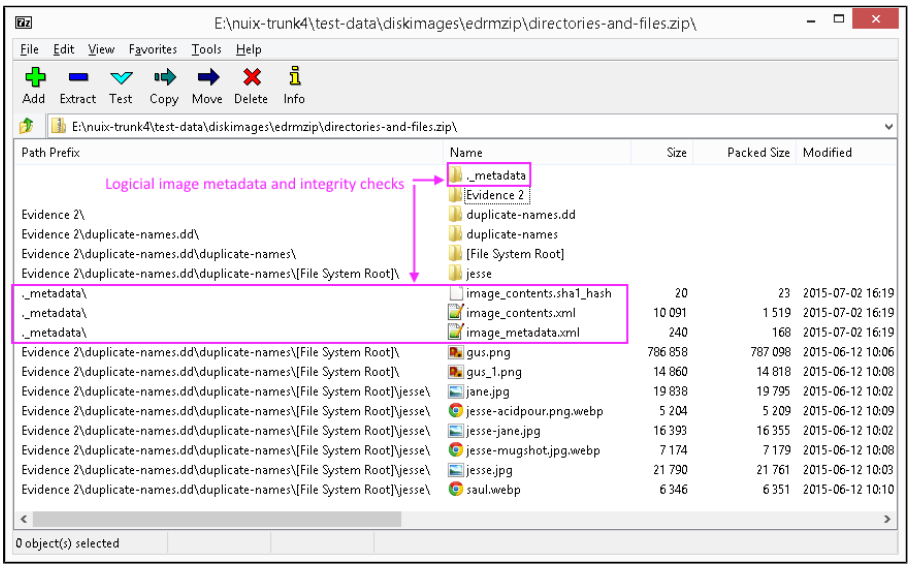
The format of the Nuix logical image has two main components:

- **An EDRM XML load file**: This contains the metadata and integrity, and checks for an image.
- **A ZIP container**: This contains the EDRM load file and all image data.

  The ZIP file is used to store a loosely representative structure of the original data. This structure does not have to match the high-fidelity structure stored in the load file. Similarly, the created, accessed, and modified times may be set on the ZIP entries, but again this is just a display detail for native clients. The actual metadata for an item is stored with the associated document in the EDRM load file.

  The following example displays a logical image opened with Nuix Imager, and then the same image opened with 7–Zip.





Note:

7-Zip places all images into the same directories, but Nuix Imager separates them.

Due to limitations in the ZIP format, duplicate folder names are not allowed. This can occur with NTFS images that include deleted data.

ZIP container

When a logical image is exported, an *.nli* (Nuix Logical Image) file is created in the location that was selected before starting the export. The image file created by Nuix Imager is a standard ZIP64 container. Any standard ZIP container can be a valid container for a Nuix Logical Image.

Metadata directory

Contained in the generated *.nli* image, the *._metadata* directory contains the logical image metadata and integrity checks generated during the export. Any non-standard third-party extensions are also placed in this directory.

A subset of the EDRM XML version 1.2 standard is used to store the metadata, structure, and integrity checks for the documents included in the image and their associated binaries.

Documents

The native path specified for an item is the key used to locate that item's binary inside the ZIP file. The Location URI value specifies the path to an item inside the data tree of a load file.

Note:

Two different directory targets can share the same name. This is shown in the example provided at the beginning of this section.

```
Evidence 2/duplicate-names.dd/duplicate-names/[File System Root]/jesse.
```

In the event of duplication, the load file uses the *Folders* element to resolve the actual file structure.

Restrictions

- Only one single Native file is allowed per document.
- No other files are allowed to be specified (text, PDF, TIFF, and so on).

Troubleshooting issues

This section shows where the Nuix Imager logs reside in a default installation and how to collect them for self-analysis or to send through to Nuix Support.

It is good practice to always attempt to troubleshoot an issue yourself. Nuix suggests you do so by doing the following, in this order:

1. Go to the **Log Directory locations** to find the latest log files to see what they contain.
2. Access the **System Diagnostics**, and possibly generate a diagnostic dump.
3. If you cannot resolve the issue, and need assistance, then:
    a. Return to the latest log folder and zip the entire folder including the time-stamped name of root folder
    b. Submit a ticket with a description of the issue on the Nuix Support Portal, located at https://nuix.service-now.com/support.
    If you do not have an account for the Nuix Support Portal, you can request one on the site.

Log directory locations

Nuix Imager produces detailed logs that can help you identify the cause of issues. When requesting support, always save the logs through System Diagnostics. You can find the full set of logs for your current and previous sessions in their default installation locations. Each time you start Nuix Imager, a new session is created with a new set of logs. Each session has its own time-stamped folder in the default location for your operating system, as detailed in the following table:

Operating System	Log Location
Windows	Navigate to *~\Users\[Current User]\AppData\Local\Nuix\Logs*
macOS	Open the *Console.app*. The logs appear under *~/Library/Logs/«app name»*
Linux	Navigate to *~/.nuix/logs/*

Alternatively, select **Help > Open Log Directory** within the application to navigate the **Logs** folder.

Generate a diagnostic dump

Nuix Imager produces a package of diagnostic information to help troubleshoot any issue. This package contains the logs from the currently open session/case and information regarding the environment, but no actual data from the case.

Note: To redact any sensitive information out of Nuix logs or files from the diagnostics, do not remove the information from these files. Instead, replace the sensitive words or paths with some special characters, for example, xxxxxx. This leaves the log structure intact, which in some cases is very important when reading it as the actual information.

---

1. To access system diagnostics, click **Help > System Diagnostics**.
2. Click **Save to File** and browse the path to save the diagnostics package.
    A zip file downloads containing logs and a variety of artifacts to help troubleshoot your issue.