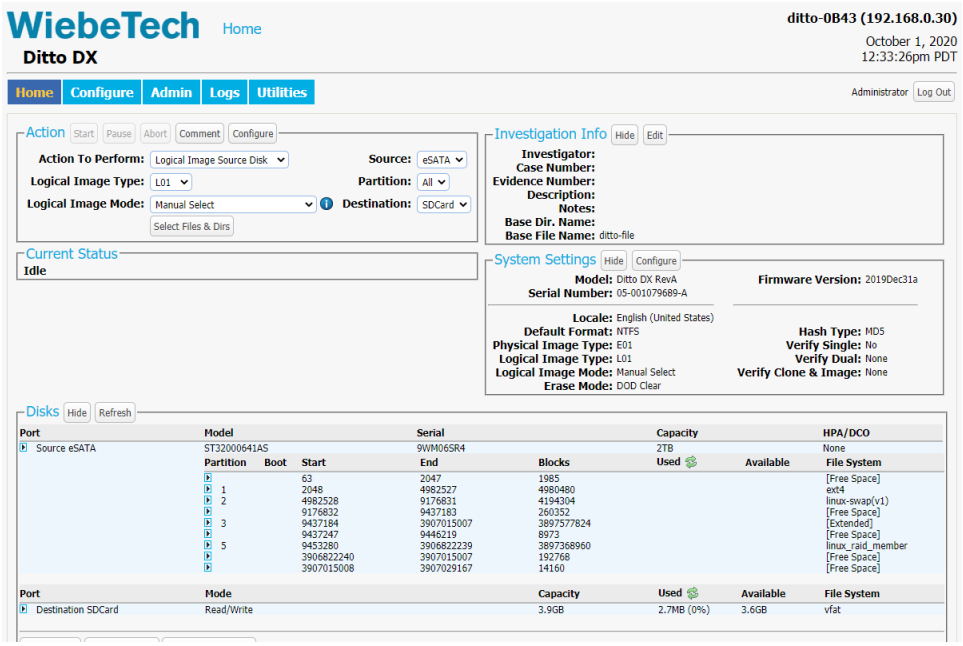


Ditto Imager Interfaces

User Manual

A6-3172-00 Rev. 1.1

Limitation of Liability

In no event will CDSG or its suppliers be liable for any costs of procurement of substitute products or services, lost profits, loss of information or data, computer malfunction, or any other special, indirect, consequential, or incidental damages arising in any way out of the sale of, use of, or inability to use any CDSG product or service, even if CDSG has been advised of the possibility of such damages. In no case shall CDSG's liability exceed the actual money paid for the products at issue. CDSG reserves the right to make modifications and additions to this product without notice or taking on additional liability.

FCC Compliance Statement: "This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation."

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at this own expense.

In the event that you experience Radio Frequency Interference, you should take the following steps to resolve the problem:

1. Ensure that the case of your attached drive is grounded.
2. Use a data cable with RFI reducing ferrites on each end.
3. Use a power supply with an RFI reducing ferrite approximately 5 inches from the DC plug.
4. Reorient or relocate the receiving antenna.

Table of Contents

1. INTRODUCTION

The Ditto® drive imager family of products allow you to capture evidence from suspect computers in a forensically sound way. Each Ditto drive imager may also be accessed remotely from a geographic location separate from where the Ditto physically rests. This document covers the interfaces available on the original Ditto Forensic FieldStation, the Ditto DX Forensic FieldStation, the Ditto x86 BE, and the Ditto x86 SE.

This user manual will teach you how to use both interfaces available in all these devices; the Ditto Graphical User Interface (GUI) or the non-graphical text interface, which is accessible from the front panel on the standalone Ditto and Ditto DX Forensic FieldStation devices and from the boot menu of the Ditto x86.

For help with specific hardware features available on your Ditto device, please refer to that device's specific user documentation.

1.1. KEY CONCEPTS

This section defines several key concepts you need to know to get the most out of your Ditto.

- **Ditto GUI:** This is the graphical user interface (GUI) of the Ditto operating system (OS), and it is the most powerful way to manage your Ditto hardware. It is sometimes also called the browser interface, referring to the fact that the you can use a web browser to remotely access the Ditto GUI. This manual exclusively uses the term "Ditto GUI".
- **Text Interface:** This is the non-graphical text-based user interface for the Ditto OS. It was initially designed for the original Ditto Forensic FieldStation as a way to operate the hardware without connecting it to a computer. It's now used even on Ditto drive imagers without a front LCD panel, like the Ditto x86. Sometimes the terms "Text Interface" and "Front Panel" may be used interchangeably, but this manual takes care to refer to the text-based user interface by the term "Text Interface" and reserve the use of the term "Front Panel" for the LCD display and navigation buttons that physically exist on the Ditto Forensic FieldStation and Ditto DX Forensic FieldStation models
- **Front Panel:** This refers to the LCD display and navigation buttons that physically exist on the Ditto Forensic FieldStation and Ditto DX Forensic FieldStation models. The Front Panel is how you access the Text Interface on these models.
- **Source Disk:** This is a disk or drive that the Ditto can read from *but not* write to, forensically preserving them as evidence.

  WARNING
  All evidence or "target" disks should be treated as Source Disks and you should avoid connecting them to the Destination Side of a Ditto Forensic FieldStation or Ditto DX Forensic FieldStation, or to any other non-write-blocked device in order to forensically preserve them as evidence.

- **Destination Disk:** This is a disk or drive that the Ditto can read from *and* write to. These are disks where Ditto can store copies of evidence found on Source Disks or Source Networks.

TIP

On the Ditto x86, any USB drive that is connected to the host system is treated by default as a Source Disk and is write-protected, but using the Ditto GUI, you can change it to a Destination Disk. On the "Home" Screen, navigate down to the "Disks" panel, click on the disk name under the "Port" column and select **Toggle Disk Src/Dst**.

- **Source Network:** This is a network that the Ditto can read from *but not* write to, forensically preserving the volumes on that network as evidence. These networks are physically connected to the Ditto Forensic FieldStation and Ditto DX FieldStation via their Source Ethernet ports.
- **Destination Network:** This is a network that the Ditto can read from and write to. These are networks where Ditto can store copies of evidence found on Source Disks or Source Networks. These networks are physically connected to the Ditto Forensic FieldStation and Ditto DX FieldStation via their Destination Ethernet ports, and are networks that the Ditto x86 can detect that are connected to its host computer.
- **Control Network:** This is the network used to connect to the Ditto DX Forensic FieldStation from a web browser. It is located on the rear of the Ditto DX.
- **Front Panel:** This is the top face of the Ditto Forensic FieldStation and Ditto DX Forensic FieldStation. It contains the status lights and the LED display and navigation buttons you use to access the Text Interface on these products. The Ditto DX also provides an LED status light bar. Consult your product's hardware documentation for more information.
- **Source Side:** This is where you physically connect Source Disks and Source Networks to the Ditto Forensic FieldStation or Ditto DX Forensic FieldStation. It is located on the left side of both products.
- **Destination Side:** This is where you physically connect Destination Disks and Destination Networks to the Ditto Forensic FieldStation or Ditto DX Forensic FieldStation. It is located on the right side of both products.
- **Control Side:** This is where you physically connect accessories to the Ditto DX Forensic FieldStation when you don't want them to take up ports on the Source Side or Destination Side. It is located on the rear of the Ditto DX.

NOTE

Older documentation previously referred to the Source, Destination, and Control Sides as 'interfaces'. This terminology has been changed to prevent confusion with the Text Interface non-graphical user interface, which is software-based and not a hardware feature.

1.2. "DITTO LOGS" STORAGE LOCATION AND BEHAVIOR

Ditto logs, language translation/internationalization files, AutoSelect logical image profiles, and network capture filters are stored together in the same volume. Captured evidence stored on the "Ditto Logs" storage location can also be found here, which is important to keep in mind if you are using a Ditto x86 SE especially. The location of these files is different depending on the Ditto model you are using.

1.2.1. HOW TO ACCESS THE "DITTO LOGS" STORAGE LOCATION

Ditto Forensic FieldStation and Ditto DX Forensic FieldStation: These files are stored on the SD card connected to the unit. To access these files, remove the SD card from your Ditto hardware, insert it into your computer, and open it.

Ditto x86: These files are stored onboard the Ditto x86 in a separate "Ditto Logs" volume. To access these files, connect the Ditto x86 to a computer already booted into a Mac, Windows, or Linux operating system and open the "Ditto Logs" volume that appears on your computer.

1.2.2. "DITTO LOGS" STORAGE BEHAVIOR

All Ditto models treat System logs differently if the "Ditto Logs" storage location is unavailable.

- **Ditto Forensic FieldStation and Ditto DX Forensic FieldStation:** If there is no SD card present, logs created since the Ditto's last power cycle are stored in volatile memory and are lost when the Ditto is powered down.
  Previously created system logs, translation files, AutoSelect logical image profiles, and network capture filters stored on the SD card are unavailable.
- **Ditto x86:** When using the Text Interface or the standard Ditto GUI (called "Ditto x86" and "Ditto x86 - Kiosk" in the boot menu, respectively), your system logs are saved to a partition called "Ditto Logs." This partition is accessible from your host computer.
  When you choose the "Ditto x86 - Kiosk Non-persistent" option from the boot menu, the Ditto x86 boots into a version of the Ditto GUI that acts as if there is no onboard storage available. Logs created during the current session are stored in volatile memory and are lost when the Ditto x86 is powered down.
  Previously created system logs, language translation/internationalization files, AutoSelect logical image profiles, and network capture filters stored in the "Ditto Logs" partition are unavailable.
  However, even in "Ditto x86 - Kiosk Non-persistent" mode, short reports that you save will be stored to the "Ditto Logs" storage location.

1.3. "DITTO DATA" STORAGE

The Ditto x86 comes with on-board storage called "Ditto Data". It is available as a "Destination" disk on both the Ditto x86 BE and the Ditto x86 SE and can be used to store data collected from various imaging or other actions. However, the Ditto x86 BE's model's storage space is more limited than the Ditto x86 SE's.

To retrieve the contents on the "Ditto Data" volume, connect the Ditto x86 to a computer already booted into a Mac, Windows, or Linux operating system and open the "Ditto Data" volume that appears on your computer.

2. DITTO GUI

Users of every Ditto product can access the Ditto GUI remotely via a web browser. Ditto x86 users can also access the Ditto GUI from the boot menu by selecting "Ditto x86 - Kiosk". Refer to your specific product's documentation for more information.

2.1. FAMILIARIZE YOURSELF WITH THE DITTO GUI

2.1.1. ICONS USED IN THE DITTO GUI

The Ditto GUI uses several icons that may be clicked on to perform certain actions.

ICON	ACTION
Information	Opens a window with a brief description of the setting the information icon appears next to.
Refresh	Refreshes the field that the icon appears next to in order to give updated information.
Reset	Loads the defaults for the setting that the Refresh icon appears next to.
Add	Adds a user defined field to a list of items.
Remove	Removes a user defined field from a list of items.
Local Storage Indicator	Indicates that the translation file for the selected locale is stored in the logs storage location (SD card or Ditto Logs volume, depending on Ditto model) instead of directly on the Ditto.
Encryption Lock	Indicates the attached disk is encrypted.
Encryption Unlocked	Indicates that the attached disk has an encryption that has been unlocked.
Security Lock	Indicates that the attached disk is locked with a password.
Security Unlocked	Indicates that the attached disk has a password that has been unlocked.

2.1.2. USER ACCOUNT CONTROL

Each Ditto drive imager product employs a user account system to control access to its features. In the Ditto GUI, the “Login” screen presents you with the ability to log in through http, or you can click the **Secure Login (HTTPS)** link to log in securely. Accept the certificate and/or continue to the website, even if your browser tells you it does not recognize it.

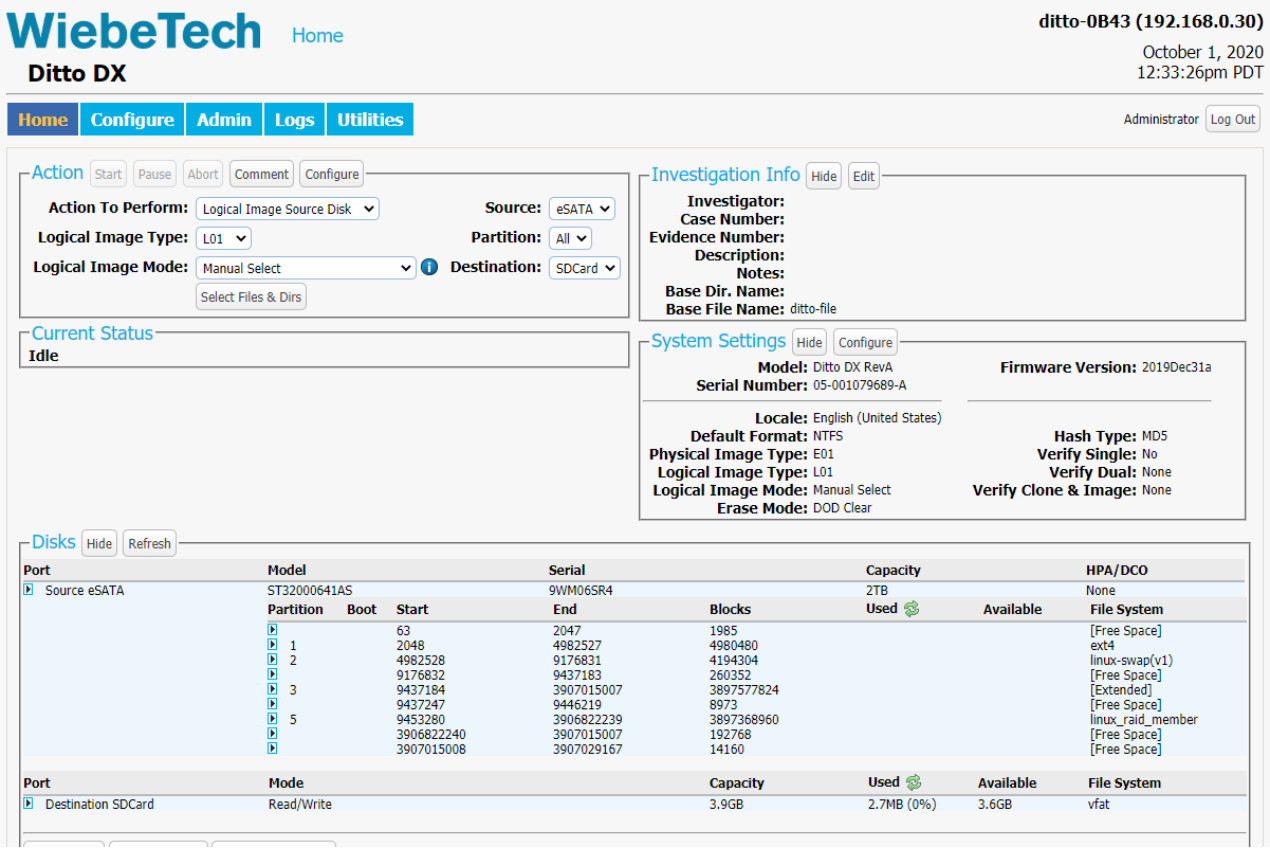
The default user name and password for the Administrator account are both “**admin**”. WiebeTech recommends that you change the admin account password and create user accounts for individual users as best data management practices.

You can also control access to various features on the front panels of both the Ditto Forensic FieldStation and the Ditto DX Forensic FieldStation products by editing the permissions for the "panel" user account in the Ditto GUI (see Section 2.4: Admin Screen, page 60).

Click on the **Log Out button** in the top right of the Ditto GUI to log out.

2.2. HOME SCREEN

The “Home” screen is where you will perform most of your operations with your Ditto drive imager, and is the default screen to load upon logging into the Ditto GUI. Click on the **Home tab** to access the “Home” screen from any other area.



The "Home" screen.

2.2.1. ACTION

The “Action” panel lets you start, abort, and document the following actions. The “Start” button begins the action. The “Abort” button stops the action in progress. Click the **Comment button** to write a note that will be appended to the log. Click the **Configure button** to modify the default settings for each action, which can also be modified on the “Configure” screen (see Section 2.3: Configure Screen, page 40).

IMPORTANT

Ditto x86 users: Performing actions requires an active license. Each brand new Ditto x86 comes with a year-long subscription. If you need to renew your subscription, see Section 6.2: Renewing a Subscription, page 97.

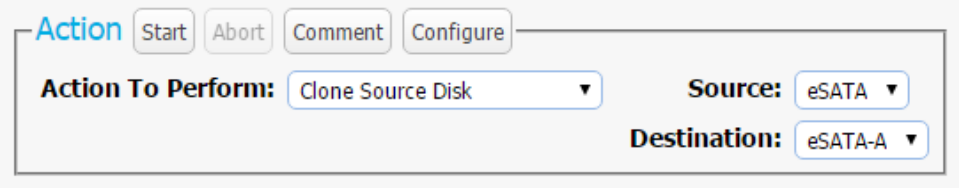
If you know your subscription is active but you cannot perform actions, then it may need to be validated with an Internet connection. See Section 6.3: Validating a Subscription, page 97.

NOTE

If you attach a disk with a master password or a BIOS user password on it, it will display in the "Disks" panel below the "Action" panel with a Lock icon and you will be unable to select it for use in any actions unless you unlock it first. To unlock the disk, see Section : How to Unlock a Disk, page 35.

CLONE SOURCE DISK

The Ditto drive imager makes an exact duplicate of the source disk on one or two destination disks.



The "Action" panel on the "Home" screen, showing the options available for the "Clone Source Disk" action.

TIP

While performing this action, the Ditto drive imager can also hash the source disk using the MD5, SHA-1, SHA-256, MD5 & SHA-1, or MD5 & SHA-256 algorithms. Select the hash type under the "System Settings" panel on the "Home" screen. See Section 2.2.3: System Settings, page 29 and Section 2.3.1: System, page 41.

To clone, follow these steps:

1. Select **Clone Source Disk** from the "Action to Perform" drop-down box.
2. Select the source disk to clone from the "Source" drop-down box.
3. Select the destination disk from the "Destination" drop-down box.

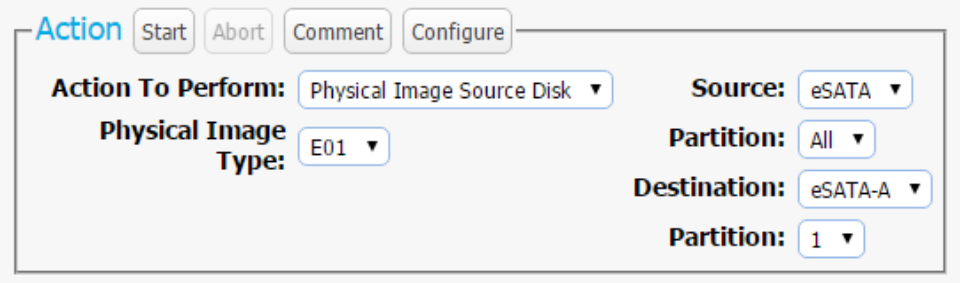
Destination disks do not have to be the same physical media as the source disk, but each must be larger than the source disk.

4. Click the **Start button**. A “Completed” message box will pop up when the action has finished. Click on the message to continue.

You can view the results of the action by scrolling down to the “System Log” panel on the “Home” screen. Find and click on the latest link, which will be denoted by a filename with a date/timestamp format: “S_yyyymmddhhmmss”. Alternatively, you can click on the **Logs button** from the top menu bar.

PHYSICAL IMAGE SOURCE DISK

The Ditto drive imager creates an E01 or DD image of the source disk on one or two destination disks.



The “Action” panel on the “Home” screen, showing the options available for the “Physical Image Source Disk” action.

TIP

While performing this action, the Ditto drive imager can also hash the source disk using the MD5, SHA-1, SHA-256, MD5 & SHA-1, or MD5 & SHA-256 algorithms. Select the hash type under the “System Settings” panel on the “Home” screen. See Section 2.2.3: System Settings, page 29 and Section 2.3.1: System, page 41.

For the fastest performance, we recommend utilizing an NTFS file system for Windows, HFS+ for Mac, and XFS or EXT4 for Linux machines. To create a physical image, follow these steps:

1. Select **Physical Image Source Disk** from the “Action to Perform” dropdown box.
2. Select which type of physical image you would like to create from the “Physical Image Type” drop-down box. The image types available are **E01** or **DD**. You can modify which image type appears by default in the drop-down box on the “Home” screen’s “System Settings” section (see Section 2.2.3: System Settings, page 29) or on the “Configure” screen’s “System” tab (see Section 2.3.1: System, page 41).
3. Select the source disk to image from the “Source” drop-down box.
4. Select which partition(s) to image from the “Partition” drop-down box. Choose **All** to image the entire source disk.

5. Select the destination disk from the “Destination” drop-down box.
   To image to two destination disks at the same time, “Dual Destinations” must be enabled in the “Configure” screen → “System” tab → “Advanced Settings” section. Once enabled, the first destination disk and its partition can be chosen from the “Destination” and “Partition” drop-down boxes, and the second destination and its partition can be chosen from the “Destination 2” and “Partition 2” drop-down boxes.

   NOTE
   Destination disks do not have to be the same physical media as the source disk, but each must be larger than the source disk. Using E01 compression can help.

6. Click the **Start button**. A “Completed” message box will pop up when the action has finished. Click on the message to continue.

TIP
If you need to abort or pause a "Physical Image Source Disk" action, you can resume it at a later time using the "Resume Physical Image" action. See Section : Resume Physical Image, page 18.

You can view the results of the action by scrolling down to the “System Log” panel on the “Home” screen. Find and click on the latest link, which will be denoted by a filename with a date/timestamp format: “S_yyyymmddhhmmss”. Alternatively, you can click on the **Logs button** from the top menu bar.

PAUSING A DD IMAGE ACTION

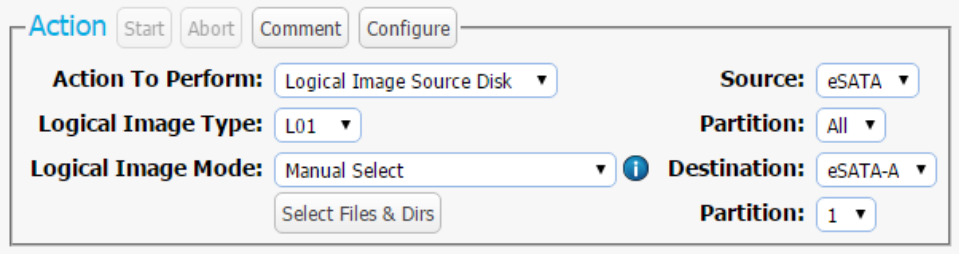
You can pause a Physical Image Source Disk action while it is creating a DD image type. To do so, click the **Pause button** in the "Action" panel. The action will be paused and saved and you will now be able perform other actions with your Ditto.

To resume the image action, choose **Resume Physical Image** from the "Action to Perform" drop-down box and follow the instructions in Section : Resume Physical Image, page 18.

NOTE
E01 images cannot be paused or resumed.

LOGICAL IMAGE SOURCE DISK

Logical imaging allows an investigator to quickly scan the contents of a hard disk and image only the files and folders relevant to the investigation into an L01, ZIP, TAR, or LIST file format. Data can be imaged to one or two destination disks.



The "Action" panel on the "Home" screen, showing the options available for the "Logical Image Source Disk" action.

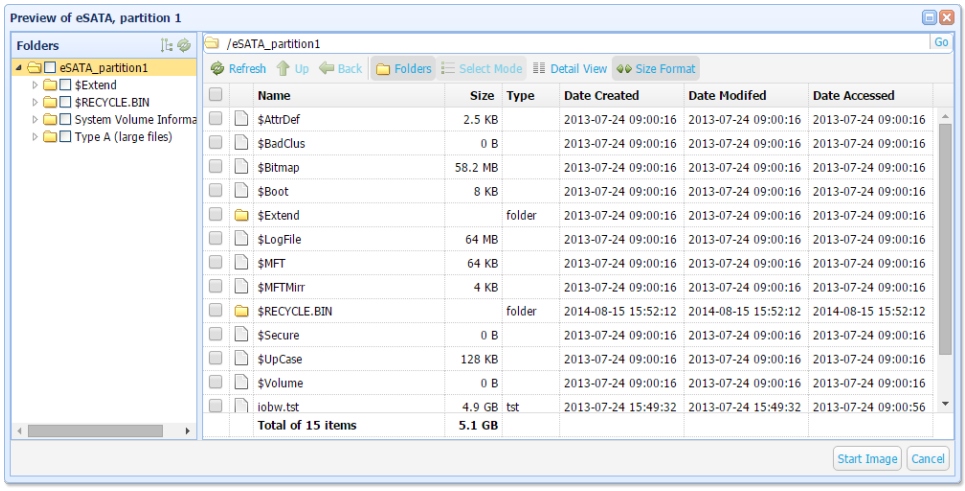
To create a logical image, follow these steps:

You can view the results of the action by scrolling down to the "System Log" panel on the "Home" screen. Find and click on the latest link, which will be denoted by a filename with a date/timestamp format: "S_yyyymmddhhmmss". Alternatively, you can click on the **Logs button** from the top menu bar.

1. Select **Logical Image Source Disk** from the "Action to Perform" drop-down box.
2. Select which type of logical image you would like to create from the "Logical Image Type" drop-down box. The format options available are L01, TAR, ZIP, or LIST. (You can modify which logical image type appears by default in the drop-down box on the "Configure" screen's "System" tab. See Section 2.3.1: System, page 41).

   TIP
   "Logical Image Source Disk" actions create a report of directories and files chosen from the source disk as well as their file sizes and any error messages encountered. This report can be viewed from within the Ditto GUI and can be exported as an Excel spreadsheet. See Section : Logical Image Report, page 64.

3. Select the Logical Image profile from the "Logical Image Mode" drop-down box. See Section : Logical Image Profiles, page 16 at the end of this subsection for information on what each profile does. See Section 4.4: AutoSelect Logical Image Profiles, page 84 for information on how to create your own profiles.
4. Select the source disk to image from the "Source" drop-down box, then choose which partition(s) to image from the "Partition" drop-down box underneath the "Source" drop-down box. If you select "All", partitions will be imaged sequentially.
5. Select the destination disk for the logical image from the "Destination" drop-down box, then choose the destination disk partition from the "Partition" drop-down box underneath.
6. If you chose any other Logical Image Mode besides "Manual Select", click the **Start button** at the top of Action section. A "Completed" message box will pop up when the action has finished. Click on the message to continue.
   If you chose "Manual Select", follow these steps:
   a. Click on **Select Files & Dirs**. A dialog box will open.
   b. Use the navigation tree to select the files and folders you wish to image.



The file navigation tree.

c. Click the **Start button** at the bottom of the dialog box. A “Completed” message box will pop up when the action has finished. Click on the message to continue.

LOGICAL IMAGE PROFILES

The Logical Image action can automatically search for files that fit the following Logical Image profiles. The action will search for specific file extensions.

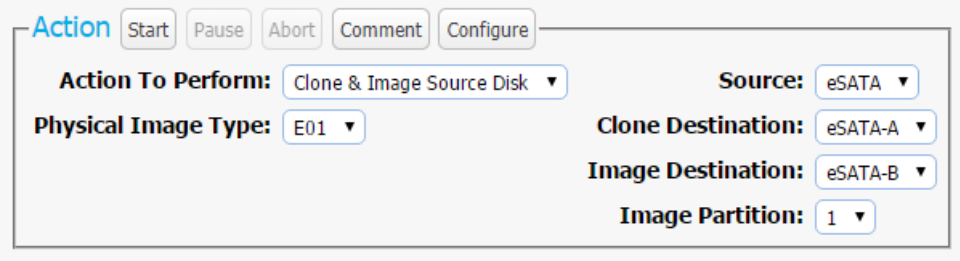
- **Manual Select:** Enables the “Select Files & Dirs” button so that you can manually select which files to logically image.
- **All Files and Dirs:** Images all files and directories.
- **All Except Windows:** Images all files and directories except for the Windows directory.
- **All Except Windows and Programs:** Images all files and directories except for the Windows, Program Files, Program Files (x86), and ProgramData directories.
- **All Users - Windows:** Images the Windows “Users” directory.
- **All Temporary - Windows:** Images the Windows/Temp and Temp directories.
- **All Except Swap and Hibernate:** Images all files and directories except files named hiberfil.sys, pagefile.sys, Win386.swp, and 386part.par.
- **All Media Files:** Images all .avi, .jpeg, .jpg, .wav, and .mov files, as well as all files with extensions beginning in “.mp” (.mpeg, .mp4, .mp3, etc.) and all files with extensions beginning in “.m4” (.m4a, .m4v, etc.).
- **All Office Files:** Images all .txt and .pdf files, as well as all files with extensions beginning in “.doc”, “.xls”, “.ppt” (.doc, .docx, .xlsx, .pptx, etc.).
- **All Financial Files:** Images all .ifx, .ofx, .qfx, .qif, and .tax files.

You may also add your own customized logical image profiles to this drop-down list. To do so, see Section 4.4: AutoSelect Logical Image Profiles, page 84.

CLONE AND IMAGE SOURCE DISK

This action simultaneously creates a clone of the source disk on one destination disk and creates an image on a second destination disk.

IMPORTANT
Two destination disks are required for this action.



The "Action" panel on the "Home" screen, showing the options available for the "Clone & Image Source Disk" action.

TIP
While performing this action, the Ditto drive imager can also hash the source disk using the MD5, SHA-1, SHA-256, MD5 & SHA-1, or MD5 & SHA-256 algorithms. Select the hash type under the "System Settings" panel on the "Home" screen. See Section 2.2.3: System Settings, page 29 and Section 2.3.1: System, page 41.

To simultaneously create a clone and a physical image of the source disk, follow these steps:

You can view the results of the action by scrolling down to the "System Log" panel on the "Home" screen. Find and click on the latest link, which will be denoted by a filename with a date/timestamp format: "S_yyyymmddhhmmss". Alternatively, you can click on the **Logs button** from the top menu bar.

1. Select **Clone & Image Source Disk** from the "Action to Perform" drop-down box.
2. Select the source disk to clone and image from the "Source" drop-down box.
3. Select the destination disk for the clone from the "Clone Destination" drop-down box and the destination disk for the image from the "Image Destination" drop-down box.

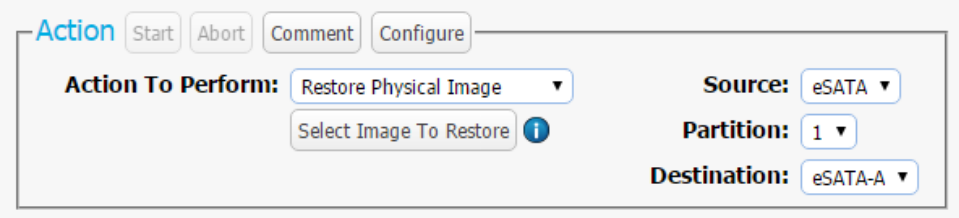
   IMPORTANT
   Destination disks do not have to be the same physical media as the source disk, but each must be larger than the source disk.
4. Select the destination disk partition on which to save the image file from the "Image Partition" drop-down box.
5. Select which type of physical image you would like to create from the "Physical Image Type" drop-down box. The image types available are **E01** or **DD**. You can modify which image type appears by

default in the drop-down box on the “Configure” screen’s “System” tab (see Section 2.3.1: System, page 41).

6. Click the **Start button**. A “Completed” message box will pop up when the action has finished. Click on the message to continue.

RESTORE PHYSICAL IMAGE

Image files of an entire disk or partition can be restored to a new disk using this action. The image file must be in either E01 or DD format. Image files of a single partition will be restored as if the original had no partitions. The destination disk must also be the same size as or larger than the original.



The “Action” panel on the “Home” screen, showing the options available for the “Restore Physical Image” action.

To restore a physical image, follow these steps:

1. Select **Restore Physical Image** from the “Action to Perform” drop-down box.
2. From the “Source” drop-down box, select the source disk where the physical image you wish to restore resides.
3. From the “Partition” drop-down box, choose the partition on the source disk where the physical image resides.
4. Select the destination disk for the image from the “Destination” drop-down box.

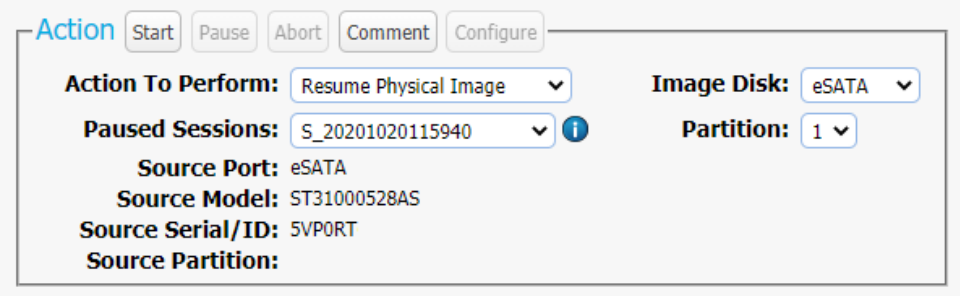
> **IMPORTANT**
> Destination disks must be larger than the source image.

5. Click the **Select Image to Restore button**, navigate to the physical image you wish to restore, select the image file to restore. If the image was originally created as a set of files, you may select any file in the set.
6. Click the **Start Restore button**. The Ditto drive imager will begin restoring the image to the destination disk.

You can view the results of the action by scrolling down to the “System Log” panel on the “Home” screen. Find and click on the latest link, which will be denoted by a filename with a date/timestamp format: “S_yyyymmddhhmmss”. Alternatively, you can click on the **Logs button** from the top menu bar.

RESUME PHYSICAL IMAGE

This action resumes a Physical Image action of a DD image after it has been paused or aborted (see Section : Pausing a DD Image Action, page 14. It is only available on the Ditto GUI.



The "Action" panel on the "Home" screen, showing the options available for the "Resume Physical Image" action.

NOTE
E01 images cannot be paused or resumed.

To resume a Physical Image DD, please follow these steps:

1. Select **Resume Physical Image** from the "Action to Perform" dropdown box.
2. Choose the disk that you are resuming an image of from the "Image Disk" drop-down box.
3. Choose the partition that you are imaging from the "Partition" drop-down box.
4. The Ditto will automatically display a listing of paused sessions of the chosen disk and partition in the "Paused Sessions" drop-down box. Choose the session you would like to resume.

   TIP
   Sessions are named according to this date/timestamp format:
   "S_yyyymmddhhmmss"

5. Click the **Start button**.

NOTE
You may optionally choose the "Ditto Logs" storage location from the "Image Disk" and "Partition" drop-down boxes to display a list of all the paused Physical Image DD XML files stored there, regardless of whether the correct Source Disk is connected.

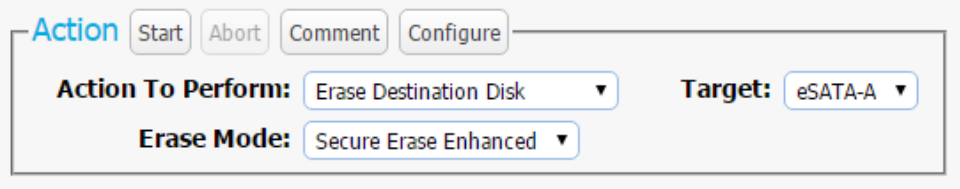
TIP

If the "Source Model" and "Source Serial/ID" text turns red, it indicates one of two errors:

- That the original Source Disk that was being physically imaged is not connected. Please ensure you have connected the Source Disk that the currently selected paused session was imaging from.
- That the original Source Disk that was being physically imaged is not selected in the "Image Disk" and "Partition" drop-down boxes. Please ensure you've selected the correct Source Disk and partition from these boxes.

ERASE DESTINATION DISK

The Ditto drive imager erases the destination disk using your preferred Erase Mode. The Erase Modes available are Clear Partition Table, Quick Erase, LBA/Offset Pattern, Custom Erase, Secure Erase Normal, Secure Erase Enhanced, DOD Clear, DOD Sanitize, NIST800-88 Clear, and NIST800-88 Purge.



The "Action" panel on the "Home" screen, showing the options available for the "Erase Destination Disk" action.

To erase a disk, follow these steps:

You can view the results of the action by scrolling down to the "System Log" panel on the "Home" screen. Find and click on the latest link, which will be denoted by a filename with a date/timestamp format: "S_yyyymmddhhmmss". Alternatively, you can click on the **Logs button** from the top menu bar.

1. Select **Erase Destination Disk** from the "Action to Perform" drop-down box.
2. Select the Erase Mode to use from the "Erase Mode" drop-down box.

   TIP

   You can modify which erase mode appears by default in the drop-down box on the "Configure" screen's "System" tab. See Section 2.3.1: System, page 41.

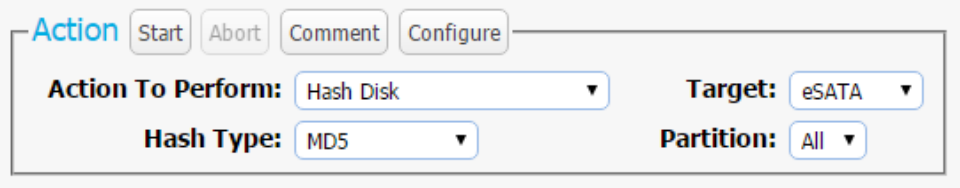
3. Select the target destination disk(s) from the "Target" drop-down box.
4. Click the **Start button**. A "Completed" message box will pop up when the action has finished. Click on the message to continue.

FORMAT AFTER ERASE

You can configure the Ditto drive imager to automatically format a disk after you erase it. Click on the **Configure tab** to go to the "Configure" screen. Then click on the **Erase tab** and make sure that "Format After Erase" is checked for each of the erase modes for which you'd like to enable this setting.

HASH DISK

The Ditto drive imager will hash any source or a destination disk using your preferred algorithm. Hash values are saved in the System Log. The available algorithms are MD5, SHA-1, SHA-256, MD5 & SHA-1, or MD5 & SHA-256.



The "Action" panel on the "Home" screen, showing the options available for the "Hash Disk" action.

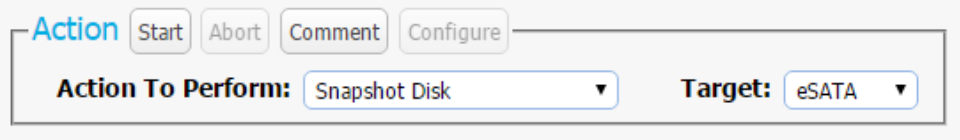
To hash a disk, follow these steps:

1. Select **Hash Disk** from the "Action to Perform" drop-down box.
2. Select your preferred hash algorithm from the "Hash Type" drop-down box. (You can modify which hash algorithm appears by default in the drop-down box on the "Configure" screen's "System" tab (see Section 2.3.1: System, page 41).
3. Select the target disk from the "Target" drop-down box.
4. Select the partition you want to hash from the "Partition" drop-down box.
5. Click the **Start button**. A "Completed" message box will pop up when the action has finished. Click on the message to continue.

You can view the results of the action by scrolling down to the "System Log" panel on the "Home" screen. Find and click on the latest link, which will be denoted by a filename with a date/timestamp format: "S_yyyymmddhhmmss". Alternatively, you can click on the **Logs button** from the top menu bar.

SNAPSHOT DISK

The Ditto drive imager captures extended disk information about the selected target disk. This includes S.M.A.R.T., hdparm, USB, and SED information. What information is reported depends on the disk interface and disk capabilities.



The "Action" panel on the "Home" screen, showing the options available for the "Snapshot Disk" action.

To create a snapshot of a disk, follow these steps:

1. Select **Snapshot Disk** from the “Action to Perform” drop-down box.
2. Select the target disk from the “Target” drop-down box.
3. Click the **Start button**. A “Completed” message box will pop up when the action has finished. Click on the message to continue.

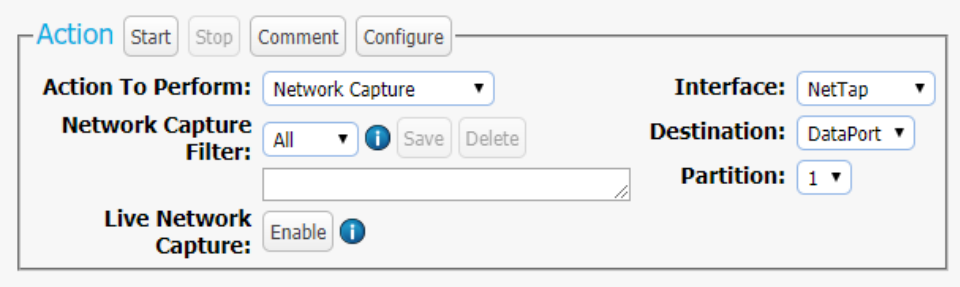
You can view the results of the action by scrolling down to the “System Log” panel on the “Home” screen. Find and click on the latest link, which will be denoted by a filename with a date/timestamp format: “S_yyyymmddhhmmss”. Alternatively, you can click on the **Logs button** from the top menu bar.

Scroll to “eSATA Extended Disk Info” to see recorded data, including S.M.A.R.T. and hdparm information.

NETWORK CAPTURE

NOTE
This action is only available on the Ditto Shark or when the Ditto Network Tap Module is being used with the Ditto Forensic FieldStation or Ditto DX Forensic FieldStation.

The Network Capture action provides two methods of capturing network traffic that can be combined and used simultaneously if you wish.



The "Action" panel on the "Home" screen, showing the options available for the "Network Capture" action.

The "PCAP Network Capture" method captures network traffic and stores it in a series of incremented PCAP files on the local target destination.

The "Live Network Capture" method captures network traffic in real-time and outputs it to a remote monitor that uses a third-party Wireshark network protocol analyzer.

The "Simultaneous PCAP and Live Network Capture" method shows you how to use both these methods simultaneously.

PCAP NETWORK CAPTURE

1. Select **Network Capture** from the "Action to Perform" drop-down box.
2. Select the network capture filter from the "Network Capture Filter" drop-down box, or type in the ports you wish to capture in the text box directly below. Use the syntax "port ## or ##" without quotes (e.g. port 80 or 81 or 443).
3. Select **NetTap** from the "Interface" drop-down box.
4. Select the media to which you'd like to save your captured data from the "Destination" drop-down box.
5. Select the partition on the Destination media you want to capture to from the "Partition" drop-down box. The data will be saved to this partition as a series of incremented PCAP files.
6. Ensure that "Live Network Capture" is not enabled.
7. Click the **Start button** to begin capturing network data.
8. When you are finished, click the **Stop button**.

You can view the log of the network capture action by scrolling down to the “System Log” panel on the “Home” screen. Find and click on the latest link, which will be denoted by a fi lename with a date/time-stamp format: “S_yyyymmddhhmmss”. Alternatively, you can click on the Logs button from the top menu bar.

You can view the data retrieved from the network capture action by examining the destination media, which will contain a folder named with the same data/timestamp format: “S_yyyymmddhhmmss”. This folder includes the PCAP files containing the captured data, an XML file containing the log information of the network capture, and—if hashing is enabled—a TXT file that contains each of the generated PCAP fil-es’ MD5 or SHA-1 hash value.

See Section 2.3.1: System, page 41 if you wish to modify the "Hash Type" setting and enable hashing.

LIVE NETWORK CAPTURE

1. Select **Network Capture** from the “Action to Perform” drop-down box.
2. Select the network capture filter from the “Network Capture Filter” drop-down box, or type in the ports you wish to capture in the text box directly below. Use the syntax "port ## or ##" without quotes (e.g. port 80 or 81 or 443).
3. Disregard the “Interface” and “Destination” drop-down boxes.
4. Ensure your third party Wireshark network protocol analyzer is standing by to receive data. If you need help configuring Wireshark itself, click the **Information icon** next to “Live Network Capture” for a link to Wireshark’s remote capture documentation.
5. Click the **Enable button** next to “Live Network Capture” to turn live network capture on.

> **CAUTION**
> Do *not* click the Start button! This button actually enables the PCAP network capture function that captures network traffic to your local destination media. It does *not* en-able live network capture.

6. When you are finished capturing network traffic, click the **Disable button**.

SIMULTANEOUS PCAP AND LIVE NETWORK CAPTURE

1. Using the Ditto GUI, select **Network Capture** from the "Action to Perform" drop-down box.
2. Select the network capture filter from the "Network Capture Filter" drop-down box, or type in the ports you wish to capture in the text box directly below. Use the syntax "port ## or ##" without quotes (e.g. port 80 or 81 or 443).
3. Select **NetTap** from the "Interface" drop-down box.
4. Select the media to which you'd like to save your captured data from the "Destination" drop-down box.
5. Select the partition on the Destination media you want to capture to from the "Partition" drop-down box. The data will be saved to this partition as a series of incremented PCAP files.
6. Ensure your third party Wireshark network protocol analyzer is standing by to receive data. If you need help configuring Wireshark itself, click the **Information icon** next to “Live Network Capture” for a link to Wireshark’s remote capture documentation.
7. Click the **Enable button** next to "Live Network Capture" to turn live network capture on. When you are finished capturing live network traffic, click the **Disable button**.
8. Click the **Start button** to begin capturing network data to your Destination media. When you are finished, click the **Stop button**.

You can view the log of the network capture action by scrolling down to the “System Log” panel on the “Home” screen. Find and click on the latest link, which will be denoted by a filename with a date/timestamp format: “S_yyyymmddhhmmss”. Alternatively, you can click on the Logs button from the top menu bar.

You can view the data retrieved from the network capture action by examining the destination media, which will contain a folder named with the same data/timestamp format: “S_yyyymmddhhmmss”. This folder includes the PCAP files containing the captured data, an XML file containing the log information of the network capture, and—if hashing is enabled—a TXT file that contains each of the generated PCAP files’ MD5 or SHA-1 hash value.

See Section 2.3.1: System, page 41 and modify the "Hash Type" setting to enable hashing.

NETWORK CAPTURE FILTERS

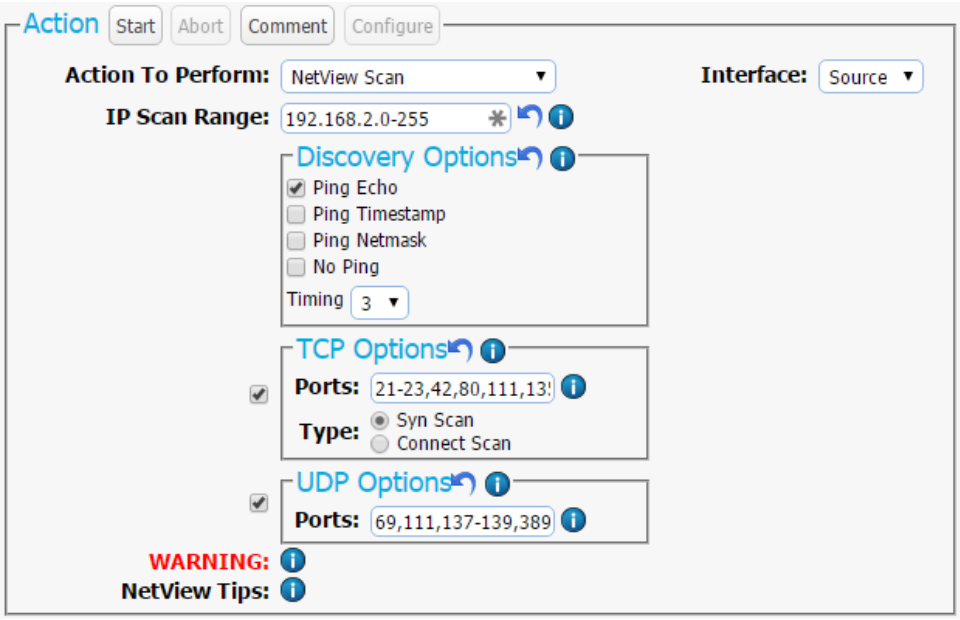
To learn how create or edit capture filters, see Section 4.5: Network Capture Filters, page 85.

NETVIEW SCAN

NetView is a network tool that is used to discover machines on a network and probe them for specific services that they may be running. This capability can help an investigator locate physically hidden computers or quickly determine whether a machine is acting as a data storage device that the Ditto can image.

WARNING

This type of network probing is very noisy and may trigger any IT related Intrusion Detection Devices (IDS's) on the network. Please be sure to run this action in a very controlled and isolated environment.



The "Action" panel on the "Home" screen, showing the options available for the "Netview Scan" action.

To perform a Netview Scan, follow these steps:

1. Select **Netview Scan** from the "Action to Perform" drop-down box.
2. Configure the available options, which are detailed below. See Section : NetView Scan Configuration Options, page 25.
3. When you are finished, press the **Start button**. You should see updates every few seconds that describe the current scan being executed, the number of hosts discovered, and the progress of the current scan. Please note that progress estimates are crude and are still being developed. A "Completed" message box will pop up when the action has finished. Click on the message to continue.

You can view the results of the action by scrolling down to the "System Log" panel on the "Home" screen. Find and click on the latest link, which will be denoted by a filename with a date/timestamp format: "S_yyyymmddhhmmss". Alternatively, you can click on the **Logs button** from the top menu bar.

The "NetView Report" section contains summaries of the discovered hosts, including the IP address, MAC address, and the manufacturer associated with the MAC address if that information can be determined. The "Hostname" will be blank if a DNS lookup could not associate the host's IP address to a name.

NETVIEW SCAN CONFIGURATION OPTIONS

Configure the following options before running a Netview Scan:

INTERFACE SELECTION

The "Interface" drop-down box allows you to tell the Ditto drive imager which Ethernet connection on your Ditto device to use during the NetView Scan.

WARNING

The selected interface will be used when the scan is started. This may create a heavy network traffic load and depending on the “Timing” setting in the “Discovery Options” subsection, may alert your IT department that the network is under some sort of threat.

Ensure that the selected interface is attached to a controlled and isolated network.

IP SCAN RANGE

By default the last octet of the IP address of the selected interface will be scanned. You may change this value and enter a list of IP address, a range of IP addresses, or a combination of both. Click the “Reset” icon to reset the IP Scan Range back to its default value.

Examples:

Range: 10.10.10.0-255
Scans the addresses 10.10.10.0 through 10.10.10.255

Range 2: 10.10.10-12.0-255
Scans addresses 10.10.10.0-255, 10.10.11.0-255, and 10.10.12.0-255

List: 10.10.10.1
Only scans IP address 10.10.10.1

List 2: 10.10.10.2,10.10.10.3
Scans only hosts 10.10.10.2 and 10.10.10.3

Combo: 10.10.10.1,10.10.10.2,10.10.10.50-100
Scans hosts 10.10.10.1, 10.10.10.2 and hosts 10.10.10.50 through 10.10.10.100

DISCOVERY OPTIONS

There are three optional host (machine) discovery options and one “No Ping” port scan option available. By default, the “Ping Echo” option is enabled and will suffice for most use cases. Some machines may be configured to ignore pings and not respond, so there are two other specialized Ping options which may be useful. Click the “Reset” icon to reload the default settings.

- **Ping Echo:** Sends a standard ICMP echo request to each IP address.
- **Ping Timestamp:** Sends a request for a timestamped ICMP packet.
- **Ping Netmask:** Sends a request for the destination’s subnet mask using an ICMP packet.
- **No Ping:** Skips host discovery and forces a port scan, which is useful when the hosts appear to be down.
- **Timing:** Selects a timing interval for scanning a network. “3” is the default setting. Lower numbers are slower and will help you avoid triggering an intrusion detection alert, and higher numbers are faster but may be less accurate, and may cause intrusion detection alerts.

TCP OPTIONS

NetView can optionally scan the specified hosts for open TCP ports. By default, this feature is not enabled. Check the box next to “TCP Options” to enable this feature and expand more options. Click the “Reset” icon to reset all TCP Options back to their default values.

- **Ports:** By default, TCP ports for commonly used services as well as services to which the Ditto may be able to connect are entered into this text box, including ports for NFS, iSCSI, and Samba. Only ports entered into this text box will be scanned.
  NetView IP port ranges may be specified as any combination of lists and ranges. Valid port numbers are between 1 and 65535 (inclusive). A list is in the form: 80,22,23. A range is in the form: 1-40. Both may be combined to form: 22,23,40-50,80,90-91.
- **Syn Scan:** Syn Scan is selected by default and is appropriate for most use cases. The Ditto generates raw IP packets and monitors for responses. This type of scan is also known as “half-open scanning” since it does not open a full TCP connection.
- **Connect Scan:** The Ditto uses a full system-level TCP connection in order to determine what ports are available on the host network. This scan should only be performed by advanced users.

WARNING

The more ports being scanned, the longer the scan will take.

UDP OPTIONS

NetView can optionally scan the specified hosts for open UDP ports. By default, this feature is not enabled. Check the box next to “UDP Options” to enable this feature. Click the “Reset” icon to reset the UDP option back to its default values.

Ports: By default, UDP ports for commonly used services as well as services to which the Ditto may be able to connect are entered into this text box, including NFS, iSCSI, and Samba. Only ports entered into this text box will be scanned. NetView IP port ranges may be specified as any combination of lists and ranges. Valid port numbers are between 1 and 65535 (inclusive). A list is in the form: 80,22,23. A range is in the form: 1-40. Both may be combined to form: 22,23,40- 50,80,90-91.

NOTE

UDP port scanning takes much longer than TCP port scanning due to the fact that open and filtered ports do not typically respond to queries. Therefore, any UDP port scanner will spend time retransmitting its query in case the query or response was lost.

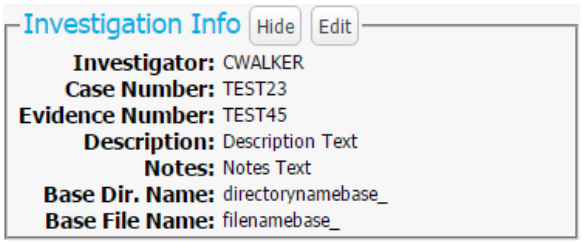
Furthermore, while closed ports do usually respond with ICMP port unreachable messages, hosts tend to limit the number of those messages sent per second, resulting in further delay.

TIPS FOR EFFECTIVE NETVIEW SCANS

1. See https://nmap.orgNmap.org for general information about network scanning.
2. Keep your IP address lists/ranges short. This will mean faster scans and less network traffic.
3. Keep your port lists/ranges short. This will also mean faster scans and less network traffic.
4. Start by deselecting the TCP and UDP scans. Just scanning for the presence of hosts is much quicker than running TCP and UDP scans on a network with an unknown number of machines. Once you have a list of discovered machines, then you can decide whether to TCP and/or UDP scan them all or scan only a subset at a time.
5. TCP scanning must be enabled in order to detect the target's operating system.

2.2.2. INVESTIGATION INFO

The Investigation Info panel groups related information that may also be used in creating custom directories and file names (see Section 2.3.10: Naming, page 58). The "Hide" button allows you to minimize the panel.



The "Investigation Info" panel on the "Home" screen.

Click the **Edit button** to enter information about the Investigator, Case Number, Evidence Number, Description, Notes, Base directory name prefix, and a Base file name prefix for any physical and logical image action.

Each field is filtered to block non-printable ASCII characters. Any characters at the file system level that may not be safe for a directory name or file name will be filtered out and replaced with an underscore. Only printable ASCII characters are currently allowed for directory and filenames. Multiple underscores will also be reduced to a single underscore per naming item.

The Ditto will generate an error message if you enter a non-printable ASCII character or if your message exceeds the 58 character limit. Additionally, when the final directory or filename that uses any of these fields is created, another level of filtering is applied.

WARNING

Using apostrophes (') in the name fields will cause an error when the file or folder name is created. They should not be used in the Investigation Info fields.

USER DEFINED FIELDS

To Add a User Defined Field:

1. Click on the **green plus sign icon** to open the “Add User Defined Field” window.

The “Add User Defined Field” window.

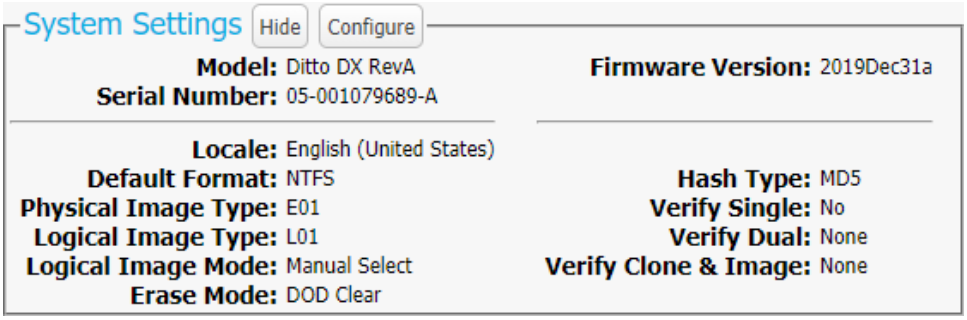
2. Fill out the **Title**, **XML Tag**, and **Value fields**.
   The "Title" is what will display in the Ditto GUI and Text Interface. The XML tag only appears in the configuration and log files. The "Value" is the description.
3. Click the **OK button**.

To Remove a User Defined Field:

- Click on the **green minus sign icon**.

2.2.3. SYSTEM SETTINGS

This section displays the Ditto product model, product serial number, firmware version, and Ditto x86 license status (see Section 6: Licensing and Subscriptions, page 97) in the top section. The most commonly used configuration settings are displayed in the bottom section. These settings are loaded as the default settings for the actions you perform in the “Action” panel.

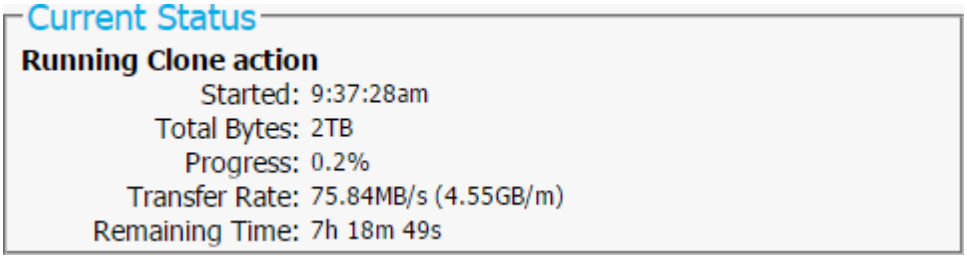


The “System Settings” panel on the "Home" screen from the Ditto DX.

The “Hide” button allows you to minimize the panel. Click the **Configure button** to customize these settings as well as additional advanced settings. See Section 2.3.1: System, page 41 for details on each option.

2.2.4. CURRENT STATUS

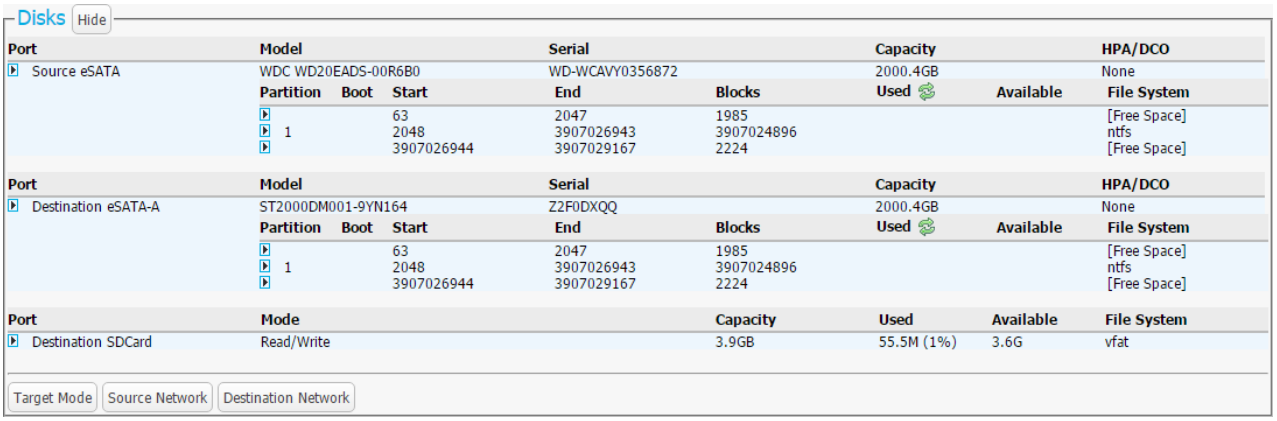
Reports either as “Idle” or displays info about the action that the Ditto drive imager is currently performing.



The “Current Status” panel, displaying a the status of a "Clone Source Disk" action.

2.2.5. DISKS

Displays information about the attached disks that are currently connected to the Ditto.



The “Disks” panel on the “Home” screen.

The “Hide” button allows you to minimize the panel.

You can retrieve the current available space a disk has remaining by clicking the green refresh icon next to the “Used” column header. This is especially useful while running an Action that is currently writing or erasing data from an attached disk.

The “Target Mode” button allows you to present the disks connected to the Ditto as iSCSI disks on a network. This is useful if you wish to use third party data acquisition tools against the disks without creating an image.

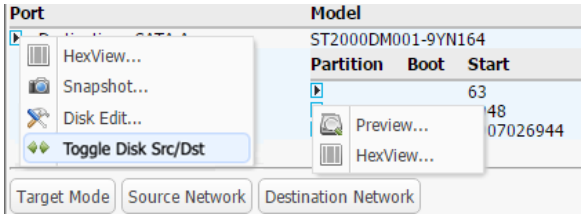
The “Source Network” and “Source Destination” buttons are used for mounting iSCSI devices as well as NFS and SMB shares to the Ditto. For more information, see Section 4: Advanced Features and Functions, page 78.

PREVIEWING AND BROWSING DISKS

To browse or download disk data, or to select files and folders for logical imaging, follow these steps:

> **NOTE**
> If you attach a disk with a master password or a BIOS user password on it, it will display in the "Disks" panel with a Lock icon and you will be unable to preview or browse the disk unless you unlock it first. To unlock the disk, see Section : How to Unlock a Disk, page 35.

1. Click on a partition’s number under the disk’s “Partition” column and select **Preview**.



Drop-down menus for a disk (left) and a disk’s partition (right). The "Toggle Disk Src/Dst" option only appears on the Ditto x86.

2. In the file explorer window that opens, navigate through the files and folders on the disk.

DIRECTORY TOOLBAR AND RIGHT-CLICK CONTEXT MENU ITEMS

ICON	ACTION
Collapse Folder Tree	Collapses the entire folder tree so that only the previewed partition’s folder is visible.
Refresh	Refreshes the folder contents in order to give updated information.
Up	Displays the contents of the parent folder.
Back	Moves back to the previously viewed folder.
Folders	Toggles whether folders are displayed in the contents panel.
Select Mode	Toggles the ability to select individual files for logical imaging.
Detail View/List View	Toggles whether the Size, Type, Date Created, Date Modified, and Date Accessed columns are visible.
Size Format	Changes whether file sizes in the “Size” column are measured as bytes or as megabytes, gigabytes, etc.

ICON	ACTION
View	Opens the selected file. Images and PDF files will open in a preview window. Other files will open a dialog box to download the file to your computer.
Download	Opens a dialog box to download the selected file to your computer.
Hash	Opens an info window with the selected file's name, the currently set hash type, and file size in bytes. You can set the hash type in the "System" tab on the "Configure" screen. See Section 2.3.1: System, page 41.
HexView	Opens the file in the Ditto Forensic FieldStation's built-in hexadecimal/character/string viewer.

HOW TO PERFORM A LOGICAL IMAGE USING THE PREVIEW WINDOW

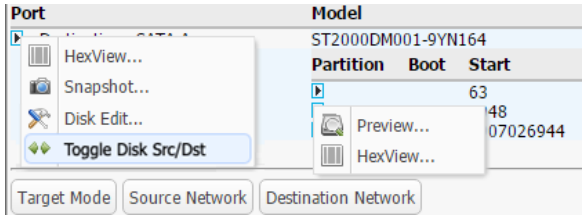
To logically image data using the "Preview" window, follow these steps:

1. Click on the **Select Mode button**.
2. Check the box next to each file or folder you want to logically image.
3. When you are finished, click on the **Stage for Logical Image button** in the lower right corner of the "Preview" window. You will be taken back to the "Home" screen.
4. Use the "Action" control panel as directed in Section : Logical Image Source Disk, page 14 to choose the logical image type, the Source and Source partition, and the Destination and Destination partition.
5. Click on "Select Files & Dirs". You will be asked to confirm whether to start the logical image with the files and folders you have selected, or to select new files and folders. Click **Start Logical Imaging**.

VIEW HEXADECIMAL DATA

To view a disk's hexadecimal data, click on the disk name under the "Port" column and then select Hex-View.

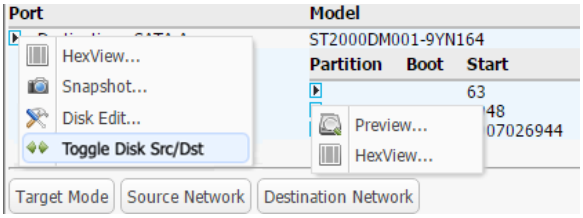
To view a disk partition's hexadecimal data, click on the partition's number under the disk's "Partition" column and then select HexView.



Drop-down menus for a disk (left) and a disk's partition (right). The "Toggle Disk Src/Dst" option only appears on the Ditto x86.

VIEW SNAPSHOT DATA

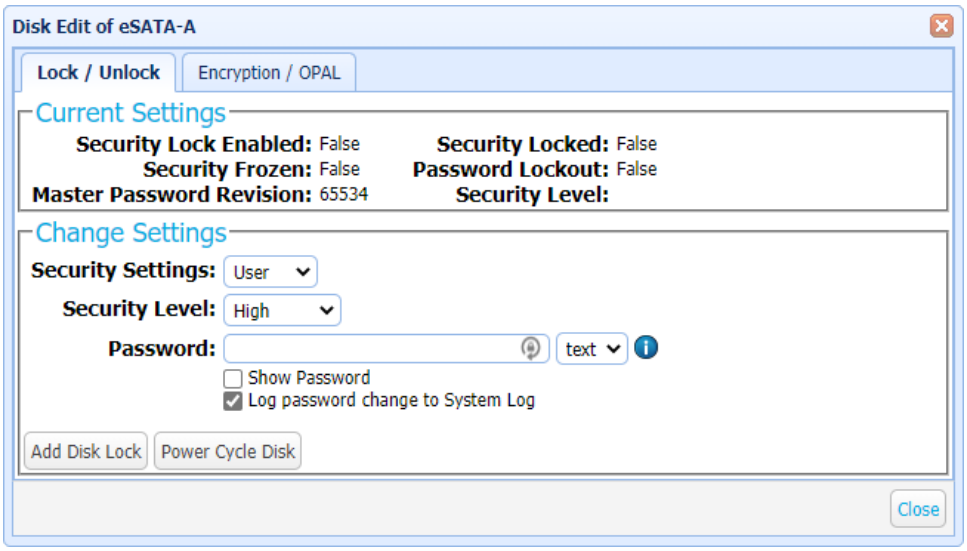
To view a disk's snapshot information, click on the disk name under the "Port" column and then select **Snapshot**.



Drop-down menus for a disk (left) and a disk's partition (right). The "Toggle Disk Src/Dst" option only appears on the Ditto x86.

PASSWORD AND ENCRYPTION MANAGEMENT WITH DISK EDIT

Disk Edit allows you to add or remove BIOS passwords or OPAL encryption.

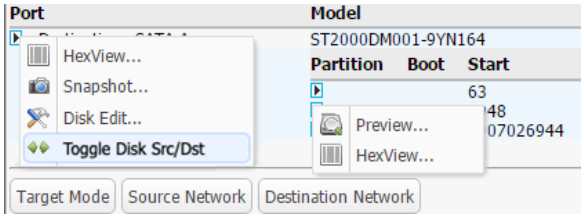


The "Disk Edit" window.

> **NOTE**
> Not all drives support disk passwords and encryption.

To open Disk Edit, follow these steps:

1. Navigate to the **Home screen** and scroll down to the **Disks panel**.
2. Click on the disk's name under the "Port" column and select **Disk Edit...**. The "Disk Edit" window will open.



Drop-down menus for a disk (left) and a disk's partition (right).

LOCK / UNLOCK DISKS

The "Lock / Unlock" tab allows you to view current settings and add or remove BIOS passwords for an attached disk.

> **NOTE**
> If the attached drive is self-encrypting and encryption is set on the drive, this tab will be greyed out.

CURRENT SETTINGS

- **Security Lock Enabled:** Indicates whether a security lock exists on the disk. The available statuses are "True" and "False".
- **Security Frozen:** Indicates whether the disk allows changes to the security state or not. The available statuses are "True" and "False".
- **Master Password Revision:** Displays the master password revision code which tells you if the disk's master password has been changed or if it is the factory default password.
- **Security Locked:** Indicates whether the disk allows any data input/output. The available statuses are "True" and "False".
- **Password Lockout:** Indicates whether the disk has been locked due to the user password being entered incorrectly too many times. The available statues are "True" and "False". To reset this, power cycle the disk.
- **Security Level:** Indicates the disk's current security level. The available levels are "Maximum" and "High".

CHANGE SETTINGS

ADD A DISK LOCK/BIOS PASSWORD

1. Ensure that the disk you want to run "Disk Edit" on is connected as a Destination Disk.
2. Open the "Disk Edit" window. See Section : Password and Encryption Management with Disk Edit, page 33.
3. Click on the "Lock / Unlock" tab if it's not already selected.

4. In the "Change Settings" section, choose the type of password you wish to add from the "Security Settings" drop-down box. The available types are **User** or **Master**.
5. If you selected "User" in the step above, choose the desired security level from the "Security Level" drop-down box. If you selected "Master", the "Security Level" drop-down box doesn't show and you may continue on to the next step.
6. Choose the password's format from the "Password" drop-down box. Choose **text** if you will be adding a typical ASCII text password. Choose **hex** if you will be adding a password written as hexadecimal digits.
7. Enter your desired password into the "Password" field. You can optionally toggle the **Show Password checkbox** if you want to show the password in plain text.

NOTE
If you are entering a hex password, you must enter an even number of ASCII characters representing hexadecimal digits (e.g. "17a64F").

8. You may optionally toggle the **Log password change to System Log checkbox** to record the password in plain text to the System Log.
9. Click the **Add Disk Lock button**.
10. On the confirmation dialog box that pops up, click **Yes** to confirm the addition of a user password.

NOTE
If you are setting a Master password, confirming will set a user password with a "High" security level, which is required to add a master password. To add a master password, continue on to the next steps.

11. If you are setting a user password, you are finished and your user password has been added. If you are adding a master password, continue on to the next step.
12. Click the **Set Password button**.
13. Click **Yes** to confirm the addition of a master password.

HOW TO UNLOCK A DISK

1. In the "Lock / Unlock" tab of the "Disk Edit" window, choose the type of password you wish to unlock from the "Security Settings" drop-down box. The available types are **User** or **Master**.
2. If you selected "User" in the step above, leave the "Security Level" drop-down box alone and continue on to the next step. If you selected "Master", the "Security Level" drop-down box doesn't show and you may continue on to the next step.
3. Enter the password into the "Password" field. You can optionally toggle the **Show Password checkbox** if you want to show the password in plain text.
4. Choose the password's format. If the password is in ASCII text, choose **text** from the "Password" drop-down box. If the password is hex, choose **hex** from the "Password" drop-down box.
5. Ignore the **Log password change to System Log checkbox** as it is not considered during this operation.

6. Click the **Unlock Disk button**.

The disk will now unlock if you have entered the password correctly. If it fails, the Ditto will display an error window and you should check your password and its format and try again.

REMOVE A DISK LOCK/BIOS PASSWORD

1. Ensure that the disk you want to run "Disk Edit" on is connected as a Destination Disk.
2. In the "Lock / Unlock" tab of the "Disk Edit" window, choose the type of password you wish to remove from the "Security Settings" drop-down box. The available types are **User** or **Master**.
3. If you selected "User" in the step above, leave the "Security Level" drop-down box alone and continue on to the next step. If you selected "Master", the "Security Level" drop-down box doesn't show and you may continue on to the next step.
4. Enter the password into the "Password" field. You can optionally toggle the **Show Password checkbox** if you want to show the password in plain text.
5. Choose the password's format. If the password is in ASCII text, choose **text** from the "Password" drop-down box. If the password is hex, choose **hex** from the "Password" drop-down box.
6. Ignore the **Log password change to System Log checkbox** as it is not considered during this operation.
7. Click the **Remove Disk Lock button**.

The disk lock will be removed if you have entered the password correctly. If it fails, the Ditto will display an error window and you should check your password and its format and try again.

POWER CYCLE DISK

You can power cycle an attached disk at any time in the "Disk Edit" window. For example, you may do so to engage a disk lock or BIOS password that you just added to a disk.

In the "Change Settings" section, click the **Power Cycle Disk button** to power cycle the disk.

NOTE

"Power Cycle Disk" is only available for attached eSATA disks on the Ditto Forensic FieldStation and Ditto DX Forensic FieldStation.

NOTE

If you are still planning to work in "Disk Edit" after power cycling a disk, you should close and reopen the "Disk Edit" window so it reflects the change of state.

ENCRYPTION / OPAL

The "Encryption / OPAL" tab allows you to view current settings and add or remove an encryption password for an attached self-encrypting drive.

NOTE

Not all drives are self-encrypting. If the attached drive is not self-encrypting or a standard disk lock is set on the drive, this tab will be greyed out.

NOTE

The drive must be attached as a Destination disk to add or remove disk encryption.

CURRENT SETTINGS

- **Encryption Enabled:** Indicates whether encryption exists on the disk. The available statuses are "True" and "False".
- **MBR Done:** Indicates whether the drive's regular MBR is visible or not. The available statuses are "True" and "False".
- **Password Lockout:** Indicates whether the disk has been locked due to the user password being entered incorrectly too many times. The available statuses are "True" and "False". To reset this, power cycle the disk.
- **MBR Enabled:** Indicates whether the drive's Shadow MBR is enabled or not. The available statuses are "True" and "False".

CHANGE SETTINGS

ADD DISK ENCRYPTION

1. Ensure that the disk you want to run "Disk Edit" on is connected as a Destination Disk.
2. Open the "Disk Edit" window. See Section : Password and Encryption Management with Disk Edit, page 33.
3. Click on the "Encryption / OPAL" tab if it's not already selected.
4. In the "Change Settings" section, choose the password's format from the "Password" drop-down box. Choose **text** if you will be adding a typical ASCII text password. Choose **hex** if you will be adding a password written as hexadecimal digits.
5. Enter your desired password into the "Password" field. You can optionally toggle the **Show Password checkbox** if you want to show the password in plain text.

NOTE
If you are entering a hex password, you must enter an even number of ASCII characters representing hexadecimal digits (e.g. "17a64F").

6. Click the **Add Disk Encryption button**.
7. On the confirmation dialog box that pops up, click **Yes** to confirm the addition of a user password.

You have successfully added disk encryption! You may optionally press the **Power Cycle button** to enable it.

HOW TO UNLOCK DISK ENCRYPTION

1. In the "Encryption / OPAL" tab of the "Disk Edit" window, enter the password into the "Password" field. You can optionally toggle the **Show Password checkbox** if you want to show the password in plain text.
2. Choose the password's format. If the password is in ASCII text, choose **text** from the "Password" drop-down box. If the password is hex, choose **hex** from the "Password" drop-down box.
3. Ignore the **Log password change to System Log checkbox** as it is not considered during this operation.
4. Click the **Unlock Disk Encryption button**.

The disk's encryption will now unlock if you have entered the password correctly. If it fails, the Ditto will display an error window and you should check your password and its format and try again.

REMOVE DISK ENCRYPTION

1. Ensure that the disk you want to run "Disk Edit" on is connected as a Destination Disk.
2. In the "Encryption / OPAL" tab of the "Disk Edit" window, enter the password into the "Password" field. You can optionally toggle the **Show Password checkbox** if you want to show the password in plain text.
3. Choose the password's format. If the password is in ASCII text, choose **text** from the "Password" drop-down box. If the password is hex, choose **hex** from the "Password" drop-down box.
4. Ignore the **Log password change to System Log checkbox** as it is not considered during this operation.
5. Click the **Remove Disk Encryption button**.

The disk encryption will be removed if you have entered the password correctly. If it fails, the Ditto will display an error window and you should check your password and its format and try again.

POWER CYCLE DISK

You can power cycle an attached disk at any time in the "Disk Edit" window. For example, you may do so to engage a disk lock or BIOS password that you just added to a disk.

In the "Change Settings" section, click the **Power Cycle Disk button** to power cycle the disk.

NOTE
"Power Cycle Disk" is only available for attached eSATA disks on the Ditto Forensic FieldStation and Ditto DX Forensic FieldStation.

NOTE
If you are still planning to work in "Disk Edit" after power cycling a disk, you should close and reopen the "Disk Edit" window so it reflects the change of state.

TOGGLE A USB DISK BETWEEN SOURCE AND DESTINATION

NOTE
This feature is only available on the Ditto x86.

The Ditto x86 does not come with physical Source Side or Destination Side data ports on the unit, so a software toggle has been built into the Ditto GUI to allow you to change whether disks connected to the host system via USB should be treated as Source Disks or Destination Disks.

Source Disks are treated as read-only and any changes to them are prevented to preserve their contents as evidence. Destination Disks can be read and written to as normal.

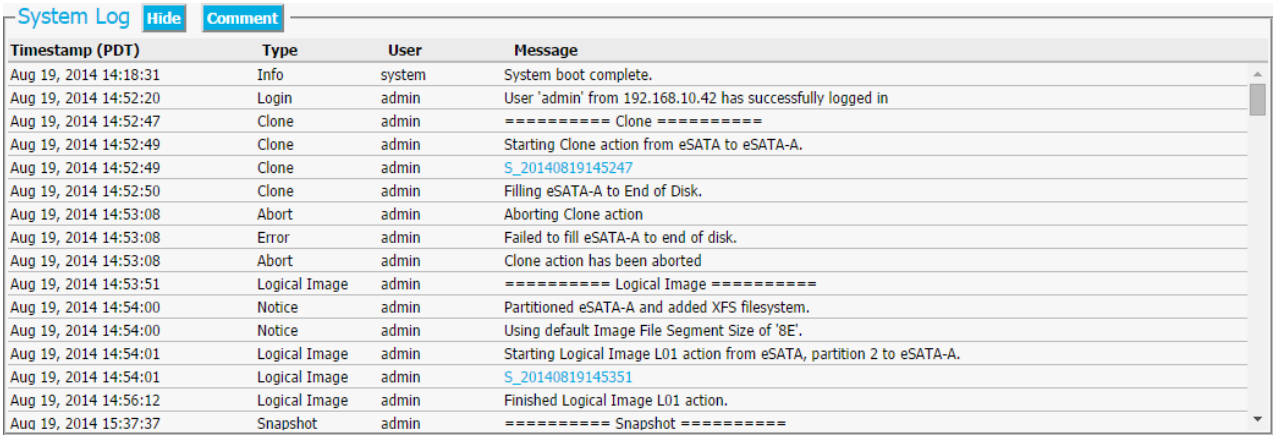
To toggle a USB disk between Source or Destination, click on the disk name under the "Port" column and then select **Toggle Disk Src/Dst**.

NOTE
To choose whether an iSCSI volume is treated as a Source Disk or Destination Disk, see Section 4.2.1: How to Access an iSCSI Device, page 79.

IMPORTANT
Please note that all other types of disks connected to the host system are treated as Source Disks by the Ditto x86 and will be read-only to preserve their contents as evidence.

2.2.6. SYSTEM LOG

Shows the actions that the Ditto has performed.



Timestamp (PDT)	Type	User	Message
Aug 19, 2014 14:18:31	Info	system	System boot complete.
Aug 19, 2014 14:52:20	Login	admin	User 'admin' from 192.168.10.42 has successfully logged in
Aug 19, 2014 14:52:47	Clone	admin	========== Clone ==========
Aug 19, 2014 14:52:49	Clone	admin	Starting Clone action from eSATA to eSATA-A.
Aug 19, 2014 14:52:49	Clone	admin	S_20140819145247
Aug 19, 2014 14:52:50	Clone	admin	Filling eSATA-A to End of Disk.
Aug 19, 2014 14:53:08	Abort	admin	Aborting Clone action
Aug 19, 2014 14:53:08	Error	admin	Failed to fill eSATA-A to end of disk.
Aug 19, 2014 14:53:08	Abort	admin	Clone action has been aborted
Aug 19, 2014 14:53:51	Logical Image	admin	========== Logical Image ==========
Aug 19, 2014 14:54:00	Notice	admin	Partitioned eSATA-A and added XFS filesystem.
Aug 19, 2014 14:54:00	Notice	admin	Using default Image File Segment Size of '8E'.
Aug 19, 2014 14:54:01	Logical Image	admin	Starting Logical Image L01 action from eSATA, partition 2 to eSATA-A.
Aug 19, 2014 14:54:01	Logical Image	admin	S_20140819145351
Aug 19, 2014 14:56:12	Logical Image	admin	Finished Logical Image L01 action.
Aug 19, 2014 15:37:37	Snapshot	admin	========== Snapshot ==========

The “System Log” panel on the “Home” screen.

The “Hide” button allows you to minimize the panel. The “Comment” button allows you to write a note that is appended to the System log.

To view the log details of a particular action, click on the link under the “Message” column. which will be denoted by a filename with a date/timestamp format: “S_yyyymmddhhmmss”. Alternatively, you can click on the **Logs button** from the top menu bar.

You can then click on the **Short Report button** to generate a short report. See Section 2.5.2: Generate Short Report, page 64 for more information.

For details on where action log files are located and how they are saved, see Section 1.2: "Ditto Logs" Storage Location and Behavior, page 8.

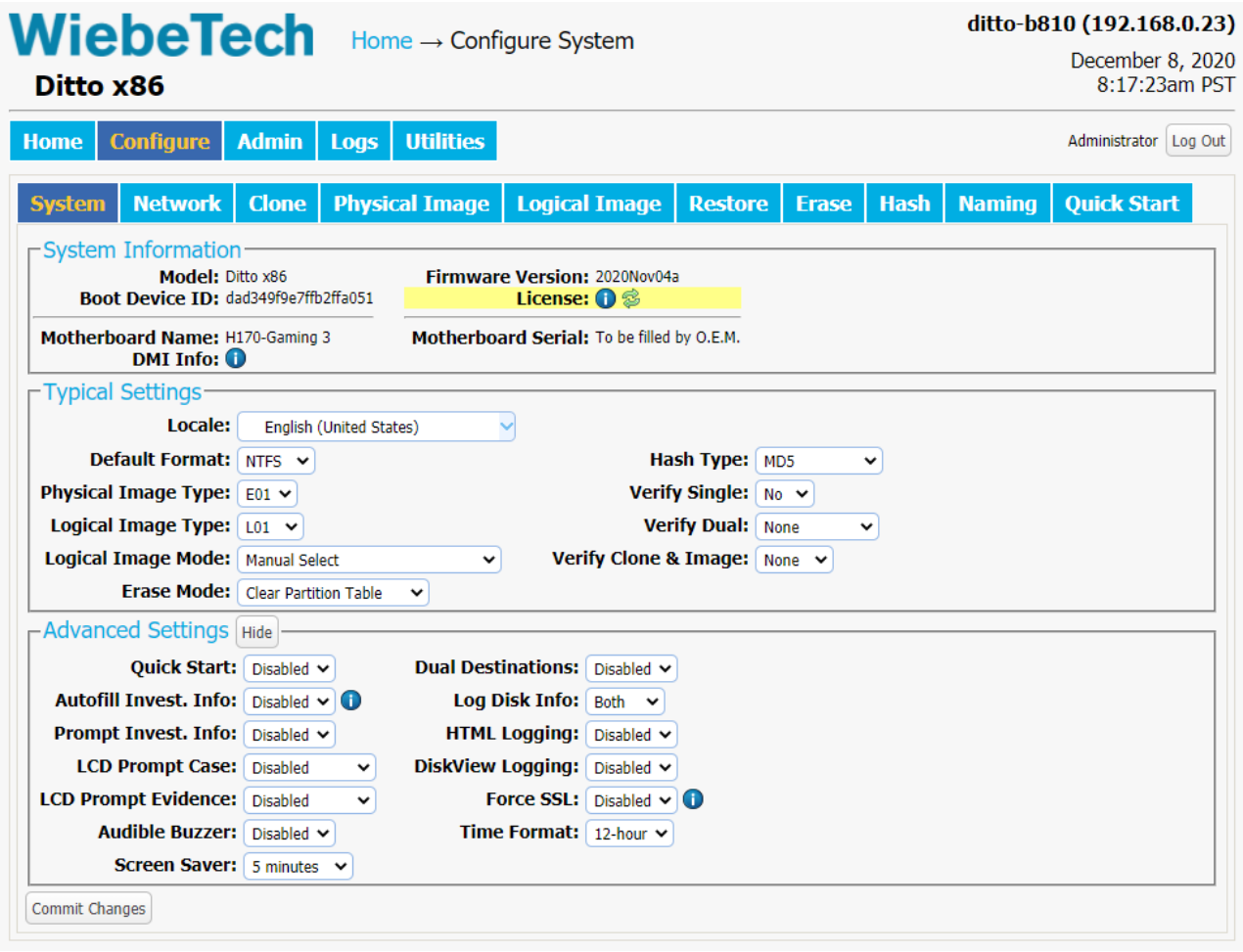
NOTE

Ditto Forensic FieldStation and Ditto DX Forensic FieldStation users: An SD card is **required** to be inserted into the Ditto in order to save logs.

Ditto x86 users: Logs are only saved when you use the Text Interface or the standard Ditto GUI (called "Ditto x86" and "Ditto x86 - Kiosk" in the boot menu, respectively). They are **not** saved when you choose the "Ditto x86 - Kiosk Non-persistent" option, or if you remove the Ditto x86 hardware from the host computer.

2.3. CONFIGURE SCREEN

The “Configure” screen allows you to modify the way the Ditto drive imager functions to suit your specific needs. Click on the **Configure tab** to access the “Configure” screen.



The "Configure" screen, showing the "System" tab on a Ditto x86. Not all options seen here are available on all models, and some available on other models are not seen here.

2.3.1. SYSTEM

The "System" tab allows you to view and customize the following settings. This information is also displayed in the "System Settings" panel on the "Home" screen. When you are finished modifying settings, click the **Commit Changes button** to save the changes.

SYSTEM INFORMATION

- **Model:** Displays the product model of Ditto hardware you are using.
- **Serial Number:** Displays your product's unique serial number. This is only visible on the Ditto Forensic FieldStation and the Ditto DX Forensic FieldStation.
- **Boot Device ID:** Displays your product's unique device ID number. This is only visible on the Ditto x86.
- **Firmware Version:** Displays the current version of firmware your Ditto is running.
- **License:** This displays a color bar if your software license is near expiration or is expired. It is only visible on products like the Ditto x86 that operate on a subscription-based model. The bar is yellow if the

license is within 30 days of expiration, and orange if it is within a week of expiration. The bar turns red once the license expires or if no license is found. See Section 6: Licensing and Subscriptions, page 97 for more information. Click the **Information icon** to learn how to renew your subscription.

- **Motherboard Name:** Displays the host machine's motherboard name. This is only visible on the Ditto x86.
- **DMI Info:** This is only visible on the Ditto x86. It displays Desktop Management Interface information about the host machine, including BIOS, motherboard, chassis, product info, system, CPU, and RAM.
- **Motherboard Serial:** Displays the serial number of the host computer's motherboard. This is only visible on the Ditto x86.

TYPICAL SETTINGS

- **Locale:** This lets you choose the location you are using Ditto. Currently, the only settings available are "English (United States)" and "English (Test)".
- **Default Format:** This is the default file system that will be used to format destination disks when they are used in actions that the Ditto performs. The available formats are HFS+, FAT32, exFAT, NTFS, EXT2, EXT3, EXT4, and XFS.
- **Physical Image Type:** Sets the default physical image type for all actions that create a physical image. The image types available are E01 or DD.
- **Logical Image Type:** Sets the default logical image type for the “Logical Image Source Disk” action. The logical image types available are L01, TAR, ZIP, and LIST.
- **Logical Image Mode:** Sets the default logical image profile. The logical image profiles available are All Files and Dirs, All Except Windows, All Except Windows Programs, Windows Registry Files, All Users - Windows, All Temporary - Windows, All Except Swap and Hibernate, All Media Files, All Office Files, and All Financial Files. See Section : Logical Image Profiles, page 16 for a description of each mode.
- **Erase Mode:** Sets the default erase mode that will be used for all actions that require erasing disks. The available modes are Clear Partition Table, Quick Erase, LBA/Offset Pattern, Custom Erase, Secure Erase Normal, Secure Erase Enhanced, DOD Clear, DOD Sanitize, NIST800-88 Clear, and NIST800-88 Purge.
- **Hash Type:** Sets the default hash algorithm that will be used for disk verification and the “Hash Disk” action. The available algorithms are None, MD5, SHA-1, SHA-256, MD5 & SHA-1, or MD5 & SHA-256.
- **Verify Single:** Determines whether individual destination disks are hashed and compared to the hash value of the source disk. The available options are Yes and No.
- **Verify Dual:** Requires that the “Dual Destinations” option in the Advanced Settings is enabled (see Section : Advanced Settings, page 42). Compares the hash value of both destinations to the hash value of the source. You can choose to verify Destination 1 or Destination 2 individually, both, or none. Destination 1 and Destination 2 are selected from the “Action” section of the “Home” screen.
- **Verify Clone & Image:** Determines whether cloned and imaged disks are hashed and compared to the hash value of the source disk’s hash value during a “Clone & Image Source Disk” action. You can choose to verify the clone, the image, both, or none.

ADVANCED SETTINGS

- **Lightbar Mode:** Enables or disables the light bar on the face of the Ditto DX Forensic FieldStation. The available settings are "Off" and "Color". This setting is only visible when using the Ditto DX Forensic FieldStation.

- **Quick Start:** Enables the “Quick Start” screen on the Text Interface that appears after you boot or reboot your Ditto hardware. The settings for this mode may be modified in the “Quick Start” tab (see Section 2.3.11: Quick Start, page 60).
- **Autofill Invest. Info:** Automatically inserts the user account's full name into the Investigator name field located in "Investigation Info" on the "Home" screen (see Section 2.2.2: Investigation Info, page 28).
- **Prompt Invest. Info:** Opens a “Configure Investigation Info” window after the user has hit the “Start” button in the “Action” section on the “Home” screen. This allows the user to customize the Investigator, Case Number, Evidence Number, Description, Notes, Base Directory Name prefix, and the Base File Name prefix fields prior to performing the requested action.
- **LCD Prompt Case:** Determines how the "Case Number" field in the "Investigation Info" section of the System Log is handled when using the Text Interface. Five options may be chosen. “Disabled” leaves the case number as it is. “Inc/Dec” allows you to manually increment the case number up or down using the Up or Down arrows while using the Text Interface. “AutoInc” automatically increments the case number, and “AutoInc/Pause” automatically increments the case number, but displays a confirmation prompt on the Text Interface before beginning the requested action.

  NOTE
  This setting requires you to enter a number into the "Case Number" field specified in the "Investigation Info” section on the "Home" screen in order to enable it (see Section 2.2.2: Investigation Info, page 28).

- **LCD Prompt Evidence:** Determines how the "Evidence Number" field in the "Investigation Info" section of the System Log is handled when using the Text Interface. Five options may be chosen. “Disabled” leaves the evidence number as it is. “Inc/Dec” allows you to manually increment the evidence number up or down using the Up or Down arrows while using the Text Interface. “AutoInc” automatically increments the evidence number, and “AutoInc/Pause” automatically increments the evidence number, but displays a confirmation prompt on the Text Interface before beginning the requested action.

  NOTE
  This setting requires you to enter a number into the "Evidence Number" field specified in the “Investigation Info” section on the "Home" screen in order to enable it (see Section 2.2.2: Investigation Info, page 28).

- **LCD/LED Brightness:** Sets the relative brightness of the LCD's and LED's on the Ditto Forensic FieldStation or the DX Forensic FieldStation on a scale of 0 to 6. Setting a value of “0” will turn off all LCD's and LED's on the unit. This setting has no effect on a Ditto x86.
- **Stealth Mode:** Turns off all LED's and LCD's on the Ditto Forensic FieldStation and the Ditto DX Forensic FieldStation. The physical “Stealth Mode” Switch on these Ditto products serves the same purpose (see your Ditto's specific hardware documentation). This setting is only visible when using the Ditto Forensic FieldStation and the Ditto DX Forensic FieldStation.

  TIP
  If Stealth Mode is enabled from the Ditto GUI, the physical switch cannot override it.

- **Audible Buzzer:** Alerts the user to various actions that occur when using the Ditto.

NOTE

Ditto x86 users: The Ditto x86 uses the host system's audible buzzer, so this feature will not function if the host system doesn't have one.

- **Screen Saver:** Sets the time interval that must pass before the Ditto x86 turns off the computer's monitors. This setting is only available on the Ditto x86. The available settings are "Disabled", "5 minutes", "15 minutes", "30 minutes", "1 hours", and 2 hours".
- **CPU Speed:** Sets the speed of the Ditto DX Forensic FieldStation's CPU. The available settings from fastest to slowest are Turbo, Default, Economy, and Power Saver. This setting is only visible when using the Ditto DX Forensic FieldStation.
- **Dual Destinations:** Enables software mirroring mode to write the same data to two destinations at the same time. The available options are Enabled and Disabled.
- **Log Disk Info:** Determines whether S.M.A.R.T. and hdparm disk information is logged before running an action, after running an action, both, or not at all.

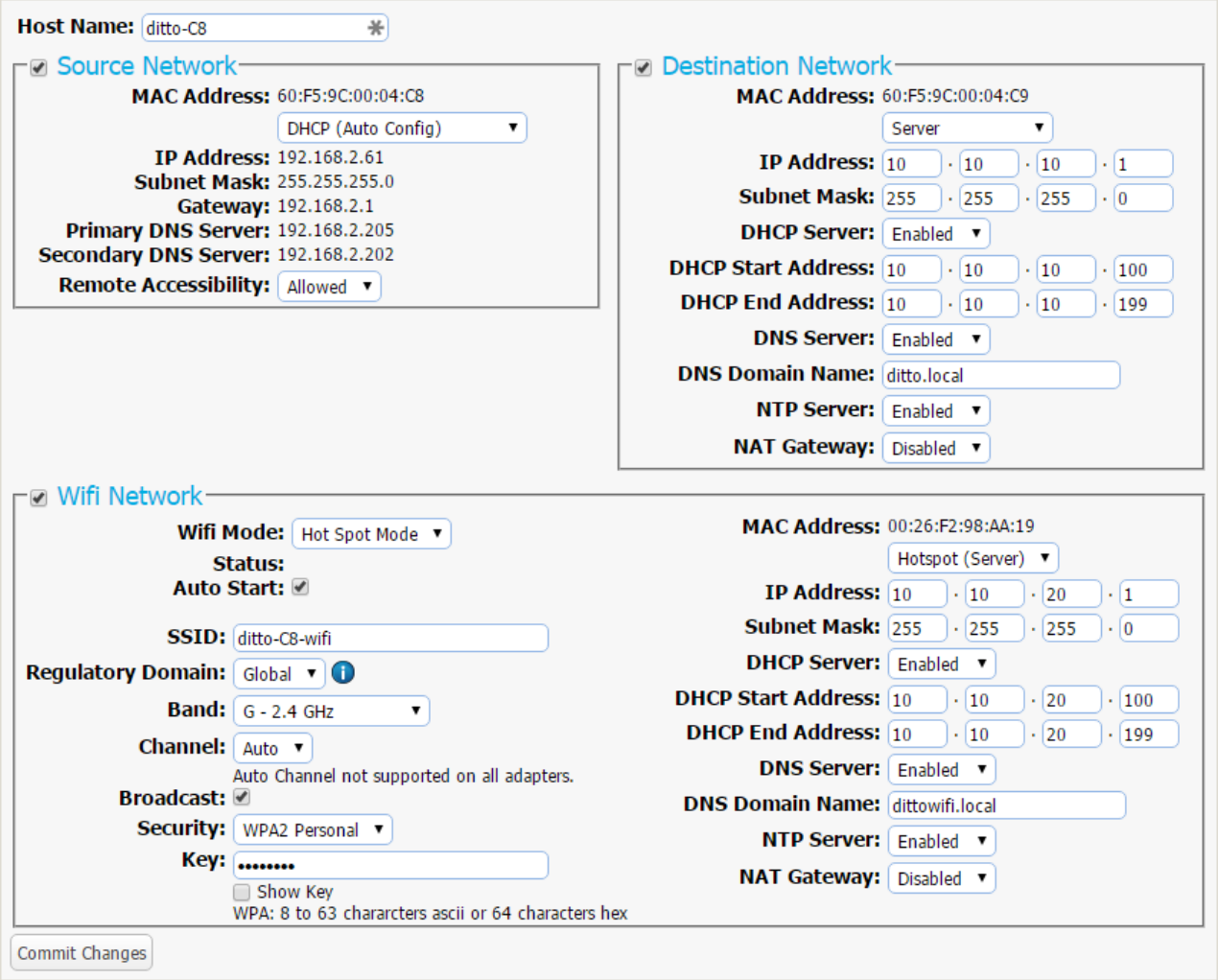
TIP

WiebeTech recommends that you log disk information both before and after an action to detect any disk problems that may have occurred during the action.

- **HTML Logging:** Logs are always saved in .XML format. This option causes your Ditto drive imager to save logs in HTML format as well. The available options are Off and On.
- **DiskView Logging:** Logs any action to preview a disk or actions performed while previewing a disk (i.e. starting or finishing a preview of a disk, starting or finishing a HexView action). The available options are Off and On.
- **Force SSL:** Forces a web browser to use Secure HTTPS to access the Ditto GUI.
- **Time Format:** Changes the time display in the top right corner of the Ditto GUI.

2.3.2. NETWORK

The "Network" tab allows you to view and customize the following settings. If you are unsure or have questions about changing your network settings, contact your network administrator. When you are finished modifying settings, click the **Commit Changes button** to save the changes.



The “Network” tab on the “Configure” screen, showing the “Source Network”, “Destination Network”, “Control Network” and “Wifi Network” settings. The "Control Network" and “Wifi Network” sections are only available on the Ditto DX Forensic FieldStation. The "Wifi Network" section only appears when a USB wireless network adapter has been detected by a Ditto DX Forensic FieldStation or a Ditto x86".

HOST NAME

Allows you to change what name for the Ditto will be displayed on a network. Host names are not case sensitive, but must begin with any letter “A-Z”. They can contain the the letters A-Z, numbers 0-9, underscore “_”, and dash “-” characters. Host names must also be limited to 64 characters.

SOURCE NETWORK

On the Ditto Forensic FieldStation and Ditto DX Forensic FieldStation, the “Source Network” section displays the Source Side Ethernet port’s MAC Address as well as its network mode. On the Ditto x86, it displays the host machine's Ethernet MAC address as well as its network mode.

You can enable or disable the Source Network adapter using the check box.

To set the network mode, choose either “DHCP (Auto Config)” or “Static IP (Manual Settings)” from the top drop-down box. If you choose "Static IP (Manual Settings)" you will also have to input the relevant network information into the text boxes that appear.

The “Remote Accessibility” drop-down box allows you to choose whether or not the Ditto responds to any network traffic via the source Ethernet port.

NOTE

Ditto x86 users: If your host computer has more than one Ethernet port then the "first" port is considered the Source Network port. It's not always obvious what the "first" port is since the order depends on how they are seen from the kernel point of view. You may have to do some trial and error to determine which port is which. Better support for this situation is planned for a future firmware upgrade.

TIP

Connecting a Ditto to a Source Network with access to the Internet will allow a user who isn't on site to remotely connect to the Ditto. Just type in the IP Address of the Ditto into a web browser and press **Enter**.

DESTINATION NETWORK

On the Ditto Forensic FieldStation and Ditto DX Forensic FieldStation, the “Destination Network” section displays the Destination Side Ethernet port’s MAC Address as well as its network mode. On the Ditto x86, it displays the host machine's secondary Ethernet port's MAC address as well as its network mode.

NOTE

In order for the Ditto x86 to connect to a Destination Network it must be attached to a host machine with two connected Ethernet ports.

You can enable or disable the Destination Network adapter using the check box.

To set the network mode, choose either “Server”, “Client (DHCP)”, or “Client (Static IP)” from the dropdown box. If you choose "Client (Static IP)" you will also have to input the relevant network information into the text boxes that appear.

SERVER

The “Server” option in the drop-down box allows you to configure the Ditto for use as a server. This can be helpful if you are connecting an iSCSI device to the Destination Ethernet port on your Ditto Forensic FieldStation or Ditto DX Forensic FieldStation (see Section 4.2.2: Directly Connect an iSCSI Device, page 80),

or you are connecting the Ditto Forensic FieldStation or Ditto DX Forensic FieldStation directly to your computer instead of through your office network.

NOTE
Ditto x86 users: WiebeTech does not recommend using the Ditto x86 as a server. The Ditto x86 also does not currently support connections to iSCSI devices.

The default settings below will work for most environments. This is an advanced option, so do not customize the default server configuration below unless directed to do so by your network administrator.

IP Address: 10.10.10.1
Subnet Mask: 255.255.255.0
DHCP Server: Enabled
DHCP Start Address: 10.10.10.100
DHCP End Address: 10.10.10.199
DNS Server: Enabled
DNS Domain Name: ditto.local
NTP Server: Enabled
NAT Gateway: Disabled

WARNING
Do not connect the Ditto Forensic FieldStation or Ditto DX Forensic FieldStation to another network while it is configured as a server. Doing so will cause network conflicts and may disrupt network traffic.

CLIENT (DHCP)

This option automatically configures the Destination Ethernet port to connect to the attached network.

CLIENT (STATIC IP)

This option allows you to manually configure the Destination Ethernet port to connect to the attached network.

CONTROL NETWORK

The “Control Network” section is only available on the Ditto DX Forensic FieldStation. This section displays the Control Side Ethernet port’s MAC Address as well as its network mode.

You can enable or disable it using the check box.

To set the network mode, choose either “Server”, “Client (DHCP)”, or “Client (Static IP)” from the dropdown-box. If you choose "Client (Static IP)" you will also have to input the relevant network information into the text boxes that appear.

TIP
Connecting a Ditto DX Forensic FieldStation to a Control Network with access to the Internet will allow a user to connect remotely to the Ditto DX. Just type in the IP Address of the Ditto DX into a web browser and press **Enter**.

SERVER
"Server" allows you to configure the Ditto for use as a server so that you can connect it directly to your computer instead of through your office network.

NOTE
Ditto x86 users: WiebeTech does not recommend using the Ditto x86 as a server. The Ditto x86 also does not currently support connections to iSCSI devices.

The default settings below will work for most environments. This is an advanced option, so do not customize the default server configuration below unless directed to do so by your network administrator.

IP Address: 10.10.10.1
Subnet Mask: 255.255.255.0
DHCP Server: Enabled
DHCP Start Address: 10.10.10.100
DHCP End Address: 10.10.10.199
DNS Server: Enabled
DNS Domain Name: dittoctl.local
NTP Server: Enabled
NAT Gateway: Disabled

WARNING
Do not connect the Ditto to another network while it is configured as a server. Doing so will cause network conflicts and may disrupt network traffic.

CLIENT (DHCP)
This option automatically configures the Destination Ethernet port to connect to the attached network.

CLIENT (STATIC IP)
This option allows you to manually configure the Destination Ethernet port to connect to the attached network.

WIFI NETWORK

This section allows you to configure a third party USB Wifi network adapter that's been plugged into one of the "Control Interface" USB ports on the Ditto DX Forensic FieldStation, or a wifi adapter on the target computer for a Ditto x86.

NOTE

The "Wifi Network" section is only available on the Ditto DX Forensic FieldStation and Ditto x86.

You can enable or disable the Wifi network adapter using the check box.

Adapters with an Atheros chipset and some adapters with Realtek chipsets are compatible.

"Wifi Mode" allows you to determine whether the Ditto DX Forensic FieldStation or Ditto x86 connects to a wifi network or acts as a wifi hot spot itself.

"Hot Spot Mode" is helpful if you are working in a separate location from the Ditto that is still within range of a wireless network, or if there is no hardwired network available in the location.

Choose "Client Mode" to connect to an existing wifi network or "Hot Spot Mode" to make the Ditto into a Wifi hot spot and act as a server.

NOTE

Ditto x86 users: Your host computer's Wifi adapter compatibility with the Ditto x86 is not guaranteed due to limited driver support.

CLIENT MODE

To connect to a wifi network, see Section : Connect to a Wifi Network, page 49.

Click the **Disconnect button** to disconnect from a Wifi network.

Check the **Auto Start box** if you want the Ditto to automatically connect to a Wifi network you've previously connected to whenever it is detected.

To select the client mode's networking mode, you can choose either "Client (DHCP)" or "Client (Static IP) from the drop-down box underneath the MAC Address. "Client (DHCP)" automatically configures the USB wifi network adapter to connect to a wifi network. "Client (Static IP)" allows you to manually configure the connection.

CONNECT TO A WIFI NETWORK

CHOOSE FROM A LIST OF AVAILABLE WIFI NETWORKS

1. Navigate to the "Network" tab on the "Configure" screen if you aren't there already.
2. If the box next to "Wifi Network" is not checked, check it to enable the Wifi network. Otherwise continue onto the next step.
3. Click the **Connect... button**. A new window will open. After a short time a list of available wifi networks will be displayed.
4. Choose the wifi network you wish to connect to and click **Connect**.
5. In the new window that opens, type in the network's key, or password.
6. Click **OK**. These credentials will be saved to the Ditto.

The Ditto will connect to the network. If it does not connect, double check your key and try again.

MANUALLY CONNECT TO A WIFI NETWORK

1. Navigate to the "Network" tab on the "Configure" screen if you aren't there already.
2. If the box next to "Wifi Network" is not checked, check it to enable the Wifi network. Otherwise continue onto the next step.
3. Click the **Manual Connect... button**. A new window will open.
4. Input the relevant network information into the window. Each network has an SSID, Security mode, and key.
5. Click **OK**. These credentials will be saved to the Ditto.

The Ditto will connect to the network. If it does not connect, double check your network information and try again.

HOT SPOT MODE

Check the **Auto Start box** if you want the Ditto to begin broadcasting as a hot spot automatically whenever a wifi adapter is detected.

The default settings below will work for most environments, with several exceptions.

WARNING

Do not connect the Ditto to a wired network while it is configured as a hotspot. Doing so will cause network conflicts and may disrupt network traffic.

SSID: {Host Name}-wifi
Regulatory Domain: Global
Band: G - 2.4 GHz
Channel: Auto
SSID Broadcast: Checked
Security: WPA2 Personal

Key: ditto123
Show Key: Unchecked
IP Address: 10.10.10.1
Subnet Mask: 255.255.255.0
DHCP Server: Enabled
DHCP Start Address: 10.10.20.100
DHCP End Address: 10.10.20.199
DNS Server: Enabled
DNS Domain Name: dittowifi.local
NTP Server: Enabled
NAT Gateway: Disabled

TIP
Input your own Key to ensure that your Ditto remains secure.

NOTICE
You may be required to conform to your country's laws and regulations regarding wireless radio frequency usage. Select your two-digit country code from the "Regulatory Domain" drop down list, and the Ditto will limit the frequencies it may broadcast on to only those in the permitted range(s).

2.3.3. CLONE

The "Clone" tab allows you to view and customize the following settings for disk cloning actions, including the "Clone & Image Source Disk" action. When you are finished, click the **Commit Changes button** to save the changes.

TYPICAL SETTINGS

- **Source HPA/DCO:** Sets whether the cloning action should indicate in the log that there is an HPA (host protected area) or DCO (device configuration overlay) present, temporarily bypass the HPA, permanently unhide the HPA, or permanently unhide both the HPA and DCO.
- **Fill to End of Disk:** Check this box to enable zeroes to be written to the end of the disk.
- **Reset After Fill:** Choose whether an HPA or DCO is set on the destination disk so that the capacity of the destination disk becomes identical to the capacity on the source disk.

ADVANCED SETTINGS

The advanced settings may be hidden. Click the **Show button** to reveal them.

- **Buffer Size:** Sets the the buffer size used by the Ditto during a cloning action. The minimum size is 512B (bytes). The default size of 1M (megabyte) works best for most uses.

- **Exit when a bad sector is encountered:** Aborts the cloning action if the Ditto encounters a bad sector on the source disk.

2.3.4. PHYSICAL IMAGE

The “Physical Image” tab allows you to view and customize the following settings for physical imaging actions, including the “Clone & Image Source Disk” action. There are separate options available for both the “E01” and “DD” image types. When you are finished, click the **Commit Changes button** to save the changes.

E01

Click on the **E01 tab** to reveal the E01 image settings.

TYPICAL SETTINGS

- **Image File Segment Size:** Allows you to specify the size in bytes that image file segments should be. The minimum size is 1M (megabyte). If this field is left blank, the maximum size will be used. Click the Information icon for more information.
- **Source HPA/DCO:** Sets whether the physical image action should indicate in the log that there is an HPA (host protected area) or DCO (device configuration overlay) present, temporarilybypass the HPA, permanently unhide the HPA, or permanently unhide both the HPA and DCO.
- **Compression Type:** Sets whether the action should use empty block compression or no compression.
- **EWF File Format:** Choose which EnCase image file format should be used during E01 physical images. WiebeTech recommends using “encase6” for most acquisitions.

ADVANCED SETTINGS

The advanced settings may be hidden. Click the **Show button** to reveal them.

- **Buffer Size:** Sets the the buffer size used by the Ditto during an E01 physical image action. The minimum size is 512B (bytes). The default size of 1M (megabyte) works best for most uses.
- **Acquire Offset:** Specifies the byte offset on the disk at which to begin an image.
- **Error Granularity:** Determines how many sectors are ignored on a read error. The minimum size is 512 bytes. The default size is the Buffer Size.
- **Acquire Length:** Specifies the length in bytes that you want to capture.
- **Read Error Retries:** Specifies the number of tries the Ditto will try to read a sector before moving on to the next sector.
- **Swap Byte Pairs of the Media Data (endian conversion):** Check this box if you need to convert from big-endian to little-endian or vice-versa, which may be necessary for disks used in older x86 or PowerPC-based systems.
- **Wipe Sectors on Read Error (mimic EnCase-like behavior):** If a read error is encountered during an E01 physical image action, the Ditto will write out zeroes to fill the sector.

DD

Click on the **DD tab** to reveal the DD image settings.

TYPICAL SETTINGS

- **Image File Segment Size:** Allows you to specify the size in bytes that image file segments should be. The minimum size is 1M (megabyte). If this field is left blank, the maximum size will be used. Click the Information icon for more information.
- **Source HPA/DCO:** Sets whether the physical image action should indicate that there is an HPA (host protected area) or DCO (device configuration overlay) present, temporarily bypass the HPA, permanently unhide the HPA, or permanently unhide both the HPA and DCO.
- **Auto Span Destination:** Check this box to span an image across multiple drives if the Destination drives are smaller than the Source drive.

ADVANCED SETTINGS

- **Buffer Size:** Sets the the buffer size used by the Ditto during a Physical Image DD action. The minimum size is 512B (bytes). The default size of 1M (megabyte) works best for most uses.
- **Acquire Offset:** Specifies the byte offset on the disk at which to begin an image.
- **Acquire Length:** Specifies the length in bytes that you want to capture.
- **Exit when a bad sector is encountered:** Aborts the Physical Image DD action if the Ditto encounters a bad sector on the source disk.

2.3.5. LOGICAL IMAGE

The “Logical Image” tab allows you to view and customize the following settings for the “Logical Image Source Disk” action. There are different options available for each of the L01, ZIP, TAR, and LIST file types. When you are finished, click the **Commit Changes button** to save the changes.

L01 SETTINGS

Click on the **L01 tab** to configure the L01 image settings.

TYPICAL SETTINGS

- **Image File Segment Size:** Allows you to specify the size in bytes that image file segments should be. The minimum size is 1M (megabyte). The maximum size is limited by the target file system. If this field is left blank, the maximum size will be used. Click the Information icon for more information.
- **Log File Access/Modify/Change Times:** Check this box to log the access, modify, and change time-stamps of files and directories during an L01 logical image action.
- **Compression Type:** Sets whether the action should use empty block compression or no compression.
- **Per File Hash Type:** Sets the default hash algorithm that will be used for individual file verification. The available algorithms are MD5 or SHA-1. The default setting is “None”

ADVANCED SETTINGS

- **Buffer Size:** Sets the the buffer size used by the Ditto during an L01 logical image action. The minimum size is 512B (bytes). The default size of 1M (megabyte) works best for most uses.
- **Read Error Retries:** Specifies the number of tries the Ditto will try to read a sector before moving on to the next sector.

ZIP SETTINGS

Click on the **ZIP tab** to configure the following ZIP image setting.

- **Log File Access/Modify/Change Times:** Check this box to log the access, modify, and change timestamps of files and directories during the logical image action. This setting is format-dependent.

TAR SETTINGS

Click on the **TAR tab** to configure the following TAR image setting.

- **Log File Access/Modify/Change Times:** Check this box to log the access, modify, and change timestamps of files and directories during the logical image action. This setting is format-dependent.

LIST SETTINGS

Click on the **LIST tab** to configure the following LIST image settings.

- **Log File Access/Modify/Change Times:** Check this box to log the access, modify, and change timestamps of files and directories during the logical image action. This setting is format-dependent.
- **Validate File Extensions:** Uses MIME to make sure that the file headers of the files within the newly created logical image list match their file extensions. Any questionable files are highlighted in the Logical Image Report.

2.3.6. RESTORE

The “Restore” tab allows you to view and customize the following settings for the “Restore Physical Image” action. When you are finished, click the **Commit Changes button** to save the changes.

TYPICAL SETTINGS

- **Fill to End of Disk:** Check this box to enable zeroes to be written to the end of the disk.
- **Reset After Fill:** Choose whether an HPA or DCO is set on the destination disk so that the capacity of the destination disk becomes identical to the capacity on the source disk.

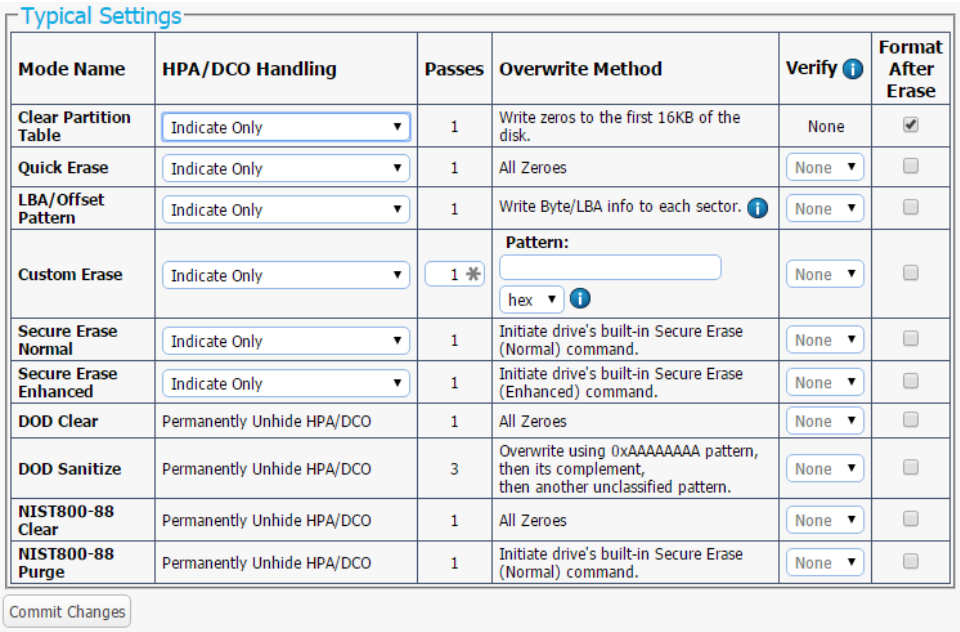
ADVANCED SETTINGS

The advanced settings may be hidden. Click the **Show button** to reveal them.

- **Buffer Size:** Sets the the buffer size used by the Ditto during a restore action. The minimum size is 512B (bytes). The default size of 1M (megabyte) works best for most uses.

2.3.7. ERASE

The "Erase tab" allows you to customize settings for how the Ditto erases disks.



The "Erase" tab on the "Configure" screen, showing all available erase modes and their customizable settings.

AVAILABLE ERASE MODES

ERASE MODE	EXPLANATION
Clear Partition Table	Removes the partition table on the disk.
Quick Erase	Performs a single pass writing all zeroes.
LBA/Offset Pattern	Writes byte/LBA info to each sector. Each sector is written with: B_XXXXXXXXXXXXXX L_DDDDDDDDDDD 'XXXXXXXXXXXXX' is the Byte offset as a hexadecimal string, and DDDDDDDDDDD' is the LBA number as a decimal string. The remainder of the sector is filled with zero.
Custom Erase	Performs 1-99 passes, overwriting the disk with zeroes or a user-selected pattern.
Secure Erase Normal	Initiates the disk's built-in Secure Erase Normal function.
Secure Erase Enhanced	Initiates the disk's built-in Secure Erase Enhanced function.
DOD Clear	Performs the U.S. Department of Defense "Clear" standard by writing all zeroes to the disk in one pass.
DOD Sanitize	Performs the U.S. Department of Defense "Sanitize" standard by using a 0xAAAAAAA pattern, then its complement, and then another unclassified pattern.

ERASE MODE	EXPLANATION
NIST800-88 Clear	Performs the “Clear” standard defined by NIST special publication 800-88 by writing all zeroes to the drive.
NIST800-88 Purge	Performs the “Purge” standard defined by NIST special publication 800-88. by initiating the drive’s built-in Secure Erase (Normal) command.

CUSTOMIZABLE SETTINGS

Some Erase Modes require several of the following settings to be configured a certain way as part of their standard. In these cases, the settings cannot be modified.

- **Mode Name:** The name of the erase mode.
- **HPA/DCO Handling:** Sets how erase actions using the specified erase mode should handle HPAs and DCOs. It can indicate in the log that there is an HPA (host protected area) or DCO (device configuration overlay) present, temporarily bypass the HPA, permanently unhide the HPA, or permanently unhide both the HPA and DCO.
- **Passes:** For the “Custom Erase” setting only, this allows you to specify the number of passes the disk is overwritten during the erase action. You can specify between 1 and 99 passes.
- **Overwrite Method:** For the “Custom Erase” setting only, you can specify a pattern for the disk to write repeatedly across the entire disk. If “text” is selected from the drop-down box, the “Pattern” field must contain one or more ASCII characters. If “hex” is selected, the “Pattern” field must contain an even number of ASCII characters representing hexadecimal digits (e.g. 17a64F). Leaving the “Pattern” field blank tells the Ditto to use zeroes.
- **Verify:** This is a planned feature that is not currently implemented. The “Verify” drop-down box will allow you to verify the erased disk after it has been fully erased. If “Quick” is selected, the beginning, middle, and end of the disk will be read to ensure that the last pattern was actually written. If “Full” is selected, the entire disk will be read to ensure that the last pattern was actually written. If “None” is selected, no verification will be performed.
- **Format After Erase:** Check this box to format the disk with the default format. The default format can be set in the “System” tab on the “Configure” screen (see Section 2.3.1: System, page 41).

2.3.8. HASH

The “Hash” tab allows you to view and customize the following settings for all hash actions. When you are finished, click the **Commit Changes button** to save the changes.

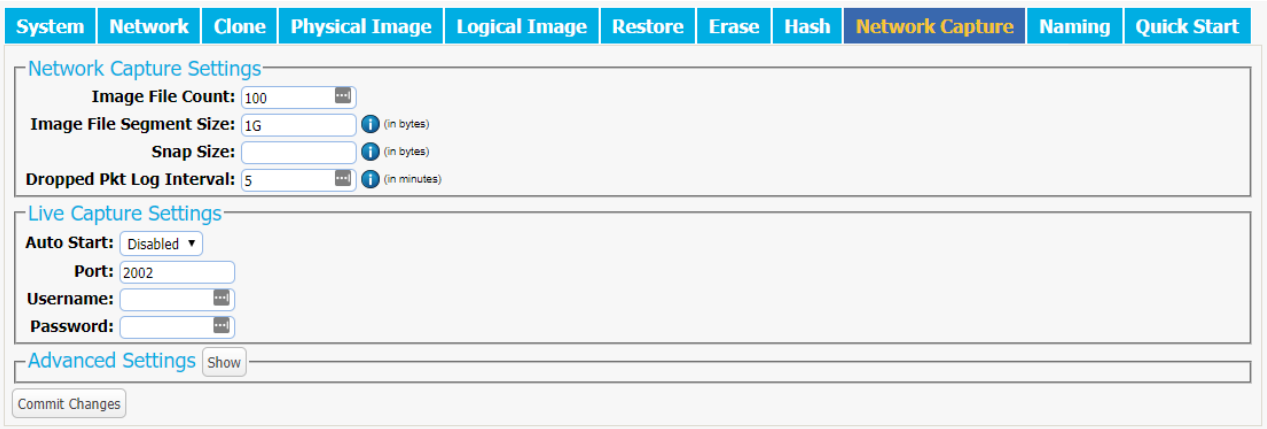
ADVANCED SETTINGS

- **Buffer Size:** Sets the the buffer size used by the Ditto during a hash action. The minimum size is 512B (bytes). The default size of 1M (megabyte) works best for most uses.
- **Exit when a bad sector is encountered:** Aborts the hash disk action if the Ditto encounters a bad sector on the target disk.

2.3.9. NETWORK CAPTURE

> **NOTE**
> This tab is only available on the Ditto Shark or when the Ditto Network Tap Module is being used with the Ditto Forensic FieldStation or Ditto DX Forensic FieldStation.

The "Network Capture" tab allows you to view and customize the following settings for all network capture actions. When you are finished, click the **Commit Changes button** to save the changes.



The "Network Capture" tab on the "Configure" screen.

NETWORK CAPTURE SETTINGS

- **Image File Count:** Specifies the maximum number of image files (based on image file segment size, see Section : Network Capture Settings, page 57) that are created on the Destination disk. When the number is reached, the Ditto will begin overwriting the oldest file on the disk for each new file that is created. Set this to **0** to fill the disk until it reaches capacity.
- **Image File Segment Size:** Allows you to specify the size in bytes that each image file should be. The minimum size is 1M (megabyte). If this field is left blank, the maximum size will be used. When the specified size is reached, a new image file is created. Click the **Information icon** for more information.
- **Snap Size:** Allows you to capture up to the specified amount of bytes of each packet of data. Click the **Information icon** for more information.
- **Dropped Pkt Log Interval:** Allows you to specify the time interval in minutes of how often the Ditto writes its accumulated dropped packet information to the Action log. Setting this value to '0' disables packet loss reporting. Click the **Information icon** for more information.

LIVE CAPTURE SETTINGS

When enabled, this service runs continuously in the background and streams captured data in real-time over the network to a remote monitor using the third-party Wireshark network protocol analyzer. See Section : Network Capture, page 22 for more information.

- **Auto Start:** Set this value to 'Enabled' to turn on live capture as soon as the Ditto is powered on. Set this value to 'Disabled' if you want the user to choose when to start the live capture service in the Ditto GUI.
- **Port:** This is the port that the Network Tap Module uses to talk to the third-party network protocol analyzer software. The default port is '2002'.
- **Username:** The username used by the third-party network protocol analyzer software.
- **Password:** The password used by the third-party network protocol analyzer software.

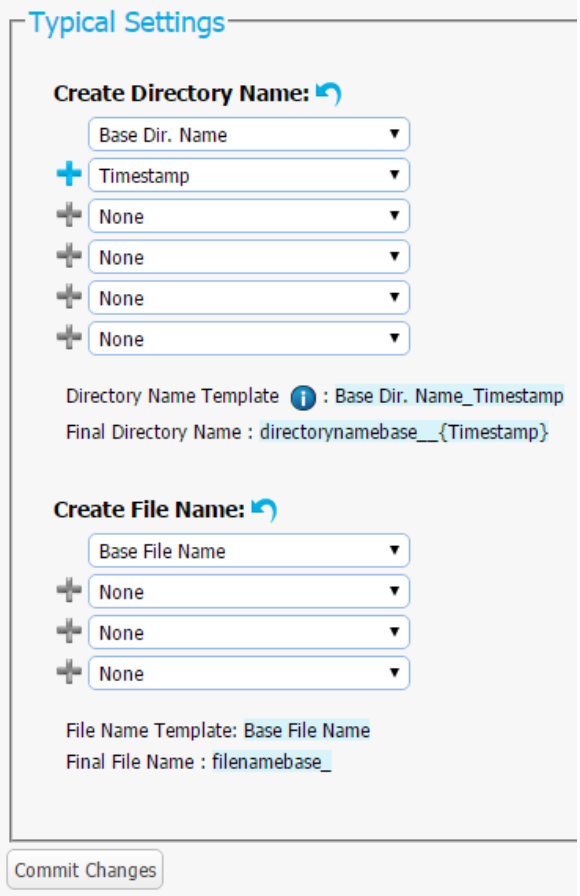
ADVANCED SETTINGS

- **Buffer Size:** Sets the the buffer size used by the Network Tap Module during a network capture action. The minimum size is 512B (bytes). The default size of 16M (megabyte) works best for most use cases. Click the **Information icon** for more information.
- **MTU:** If you are using the Network Tap Module on a network that's configured to a non-standard maximum transmission unit size (e.g. it uses jumbo frames), then set this field to match that value. Most Ethernet LANs will use the standard MTU of 1500. The commonly accepted range for a valid MTU is 68 to 65,535 as defined in RFC 791. Click the **Information icon** for more information.
- **Link Speed:** Allows you to set the Ethernet connection speed throughput. In most cases, "Auto Negotiate" will work. If you experience problems staying connected, you may need to change the speed to match what your network's capabilities are.

2.3.10. NAMING

The "Naming" tab allows you to customize how the Ditto names directories and files during imaging actions. When you are finished, click the **Commit Changes button** to save the changes.

As shown in the image below, the file directory used in imaging actions can be a name that contains up to six user-selectable fields, and the file name used in imaging actions can contain up to four user-selectable fields. As you customize these fields, the "Directory Name Template", "Final Directory Name", "File Name Template", and "Final File Name" fields will update. The template fields show the order of variables will appear in the name, whereas the final name fields display the directory or file name using the actual information from the "Investigation Info" panel on the "Home" screen and the source disk.



The "Naming" tab on the "Configure" screen.

VARIABLES

To modify the any of the user-customizable variables, navigate to the "Investigation Info" section on the "Home" screen (see Section 2.2.2: Investigation Info, page 28).

- **Timestamp/{Timestamp}:** Displays the timestamp. The timestamp is required to be included in all directory names, but it is optional for file names.
- **Base Filename:** Displays the base file name. This option is the default first variable for file names, but may be changed. User customizable.
- **Case Number:** Displays the case number. User customizable.
- **Description:** Displays the description field. User customizable.
- **Evidence Number:** Displays the evidence number. User customizable.
- **Investigator:** Displays the investigator. User customizable.
- **Source Drive Model Type:** Displays the model number of the source disk.
- **Source Drive Unique ID:** Displays the unique ID number of the source disk.

2.3.11. QUICK START

The “Quick Start” tab allows you to customize the quick start mode that appears in the Text Interface when the “Quick Start” option is enabled in the “System” tab.

NOTE

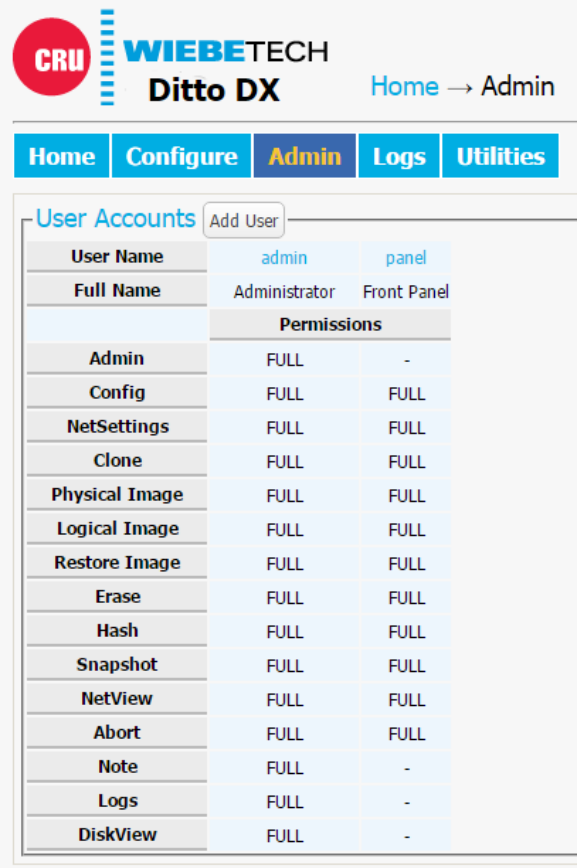
Many of the settings on the next page are visible only when certain types of actions are selected in the “Action to perform” drop-down box. For example, choosing "Clone Source Disk" from the drop-down box will reveal several different options than are visible when choosing "Physical Image Source Disk."

QUICK START SETTINGS

- **Action to perform:** Sets the action that is performed by the quick start mode.
- **Allowed Sources:** Place a check mark next to each source where you want the Ditto to search for a connected source.
- **Allowed Targets:** Place a check mark next to each target where you want the Ditto to search for a connected target.
- **Clone Destination:** For the “Clone Source Disk” and “Clone & Image Source Disk” actions only. Specifies the target destination where the source disk will be cloned.
- **Source Partition:** Determines which partition(s) will be imaged from the source disk. Choose **All** to image the entire source disk.
- **Image Destination:** Specifies the target destination where the image will be placed.
- **Image Partition:** Specifies the partition on the target destination where the image will be placed.
- **Action Target:** For the “Erase Destination Disk” action only. Specifies which target volume will be erased.

2.4. ADMIN SCREEN

The “Admin” screen allows the administrator to manage user accounts and assign permission levels for each user. Click on the **Admin tab** to access the “Admin” screen from the Ditto GUI.



The "Admin" screen.

2.4.1. USER ACCOUNTS

The Ditto contains two permanent accounts; "admin" and "panel". The "admin" account is the Administrator account, and only the Full Name and password may be modified. The "panel" account modifies access permissions for functionality that can be accessed through the Text Interface on all Ditto drive imagers.

2.4.2. PERMISSIONS

PERMISSION LEVELS

Permission levels in the Ditto GUI are displayed as "FULL", "AUTH", or as a hyphen, and as "Full Access, "Must Authenticate", and "None", respectively, when editing or creating a user.

- **FULL/Full Access:** The user has complete access to the features governed by that permission and is not required to enter a password.
- **AUTH/Must Authenticate:** The user must authenticate their credentials with a password in order to change a setting or perform an action that that permission governs.
- **A hyphen/None:** The user does not have access to the features governed by that permission.

CONFIGURABLE PERMISSIONS

The following list of permissions specifies what each controls, and can be configured when adding or editing a user account. Some permissions for the Administrator and Front Panel accounts will be greyed out by default.

- **Admin:** “None” allows access to modify the User Name and Full Name of the Administrator, Front Panel, and the user’s own account, and allows the user to change his or her own password, but blocks the user from viewing any account’s permission levels. “Modify Users” enables the user to be able to modify user accounts, passwords, and permissions (except for the “Admin” permission). “Full Access” additionally enables the ability to create and delete users and assign the “Admin” permission.
- **Configure:** Governs all non-network configuration settings, including those found in the “System Settings” panel on the “Home” screen and on all tabs on the “Configure” screen.
- **Network Settings:** Controls access to the network settings on the “Configure” screen.
- **Clone:** Controls access to the “Clone Source Disk” and “Clone & Image Source Disk” actions.
- **Physical Image:** Controls access to the “Physical Image Source Disk” and “Clone & Image Source Disk” actions.
- **Logical Image:** Controls access to the “Logical Image Source Disk” action.
- **Restore Image:** Controls access to the “Restore Physical Image” action.
- **Resume Image:** Controls access to the "Resume Image" action.
- **Erase:** Controls access to the “Erase Destination Disk” action.
- **Hash:** Controls access to the “Hash Disk” action.
- **Snapshot:** Controls access to the “Snapshot Disk” action.
- **Network Capture:** Controls access to the "Network Capture" action, which is only visible when you are using a Ditto Shark or have a Network Tap Module attached to your Ditto Forensic FieldStation or Ditto DX Forensic FieldStation.
- **NetView Scan:** Controls access to the “Netview Scan” action.
- **Pause:** Controls access to the ability to pause actions in progress.
- **Abort:** Controls access to the ability to abort actions in progress.
- **Note:** Controls access to the “Comment” buttons in the “Action” and “System Log” panels on the “Home” screen.
- **Logs:** Controls the ability to delete log files from the “Logs” screen. •
- **Disk View:** Controls the ability to preview and download files from the suspect drive via the “Disks” panel on the “Home” screen.
- **Disk Edit:** Controls access to the "Disk Edit" feature available via the "Disks" panel on the "Home" screen, which allows you to add or remove BIOS passwords or OPAL encryption.

2.4.3. ADDING A NEW USER

To add a new user, click the **Add User button**, enter the user’s information, and set the permission levels. When finished, click on the **Commit Add button**.

2.4.4. EDITING AN EXISTING USER

To update a user’s name, password, or permissions, click on the user account under the “User Name” column, update the information, and then click the **Commit Edits button**.

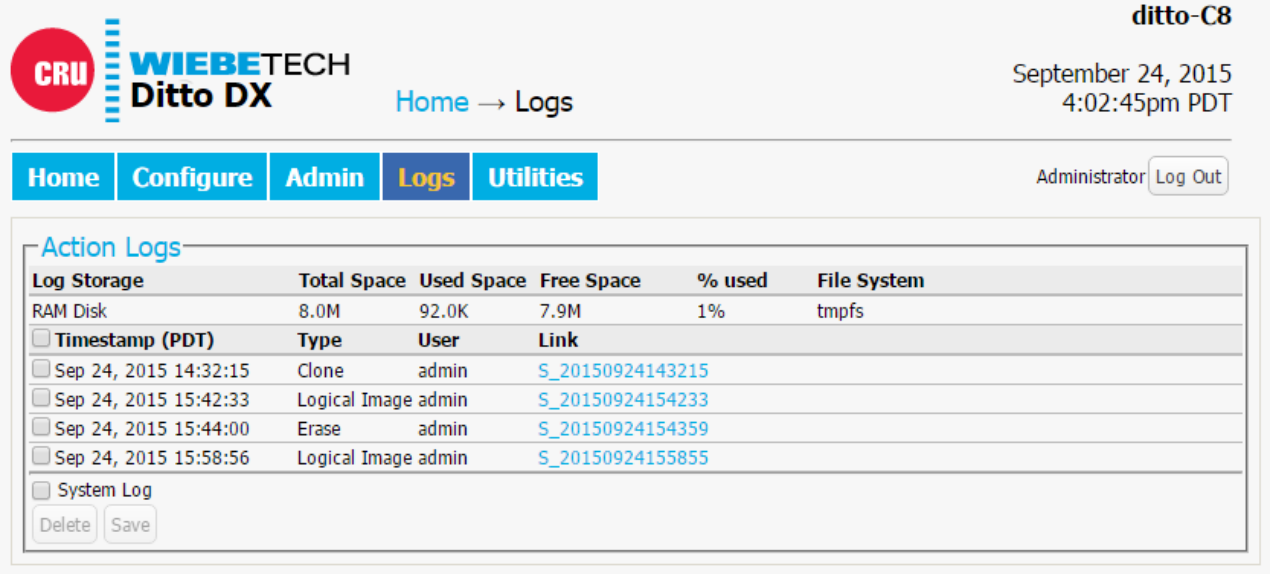
2.4.5. DELETING A USER

To delete a user, click on the user account under the “User Name” column and click on the **Delete User button**.

> **WARNING**
> **There is no delete confirmation dialog box!** Do **not** click this button unless you are absolutely certain you wish to delete the account.

2.5. LOGS SCREEN

The “Logs” screen provides information about the Ditto’s actions. Click on the **Logs tab** to access the “Logs” screen. For information about log storage and how to access them, see Log Storage Location and Behavior.



The “Logs” screen.

2.5.1. VIEWING ACTION LOGS

Action logs show the timestamp, the type of action performed, the user who performed the action, and a link to the “Action Log” screen that provides more information about the performed action.

To view a log of a particular action, find and click on the link for that action located in the "Link" column, which will be denoted by a filename with a date/timestamp format: “S_yyyymmddhhmmss”.

You can then click on the **Short Report button** to generate a short report. See Section 2.5.2: Generate Short Report, page 64 for more information.

SETTINGS
Displays the settings of the Ditto that were used when the particular action was performed.

USER PERMISSIONS
Displays the permissions of the user that were in place when the particular action was performed.

EXTENDED DISK INFO
This report displays the information of the disk used in the action (which is identified in the title of this report). The information captured includes information from both before the action was performed as well as information after the action was performed.

The information presented includes the interface, model, serial number, capacity, the presence of HPAs (host protected areas) or DCOs (device configuration overlays), partition information, hdparm information, and S.M.A.R.T information.

If multiple disks are used in the action, then multiple reports are created.

LOGICAL IMAGE REPORT
This report appears in action logs of “Logical Image Source Disk” actions and displays each directory and file that was imaged, along with their size and any error messages that were generated. If “Validate File Extensions” is enabled for LIST logical images in the “Configure” screen, it will also log any files in LIST logical images that have a mismatched file header and extension (see Section : LIST Settings, page 54).

Click on the **Export button** to save a copy of the log as an Excel spreadsheet.

Click on the **Export Suspects button** to save a copy of all of the suspect files where there is a mismatch between the file’s MIME type and file extension.

NETVIEW REPORT
This report appears in action logs of “Netview Scan” actions and displays summaries of the discovered hosts, including the IP address, MAC address, and the manufacturer associated with the MAC address if that information can be determined.

NOTE
The “Hostname” will be blank if a DNS lookup could not associate the host’s IP address to a name.

2.5.2. GENERATE SHORT REPORT
You can generate a report of a particular action and then print or save it as an HTML document.

To do so from the "Logs" screen, find and click on the link for that action located in the "Generate Short Report" column, which will be denoted by a filename with a date/timestamp format: “SR_S_yyyymmddhhmmss”.

When viewing a log from the "Action Log" screen, you can simply click on the **Short Report button** in the top right corner of the screen to generate a short report.

Click the **Save button** to save a copy of the report in HTML.

- **Ditto x86:** Saves the report to the "download" folder in the "Ditto Logs" storage location.
- **Remote connection to a Ditto x86:** Opens your computer OS's "Save As..." dialog box and you can choose the location to save the report to.
- **All other Ditto hardware:** Opens your computer OS's "Save As..." dialog box and you can choose the location to save the report to.

Click the **Print button** to open up your computer's "Print" dialog box and print a copy of the report.

NOTE
The "Print" button is not available when using a Ditto x86 directly in "Kiosk" mode from its host computer.

2.6. UTILITIES SCREEN

The “Utilities” screen allows you to perform various miscellaneous functions, including the ability to upgrade firmware, import customized configurations, remotely reboot the Ditto, modify date and time settings, and perform a factory reset. Click on the **Utilities tab** to access the “Utilities” screen from the Ditto GUI.

2.6.1. SYSTEM MAINTENANCE

FIRMWARE UPGRADE

For information on how to upgrade the firmware, see Section 5: Upgrading Firmware, page 94.

CONFIGURATION

You can save and load configurations for the Ditto that can be used on any Ditto drive imager hardware. The file generated saves a copy of every customizable setting available.

SAVE CONFIGURATION

To save a configuration, click on the **Save Config button**. Name the file, and then click **Continue** to open a Save As dialog box and save the file to your computer.

LOAD CONFIGURATION

1. Click on the **Load Config button**, browse to the .xml configuration file you want to load, highlight it, and click **Open**.

2. The “Confirm Import” window will open. Place a check next to each setting you want to load, and then click **Continue**. By selecting these settings, you will be overwriting the existing settings, so be sure to save the current configuration first.
3. The Ditto will import the configuration settings. Click **OK** when it’s finished.

OTHER BUTTONS

- **Reboot:** Opens a confirmation dialog box to reboot the Ditto.
- **Power Off:** Opens a confirmation to turn the Ditto x86 off. This option is only visible on Ditto x86 products.
- **Date & Time:** Allows you to set the current date, time, and timezone. Click the **Synchronize button** to sync these settings to your computer OS's date, time, and time zone.

NOTE
The "Synchronize" button is not available when using a Ditto x86 directly in "Kiosk" mode from its host computer.

- **Factory Reset:** Opens a confirmation dialog to return the Ditto to factory settings. Check the **Purge Ditto SDCard log files box** or the **Purge Ditto Log files box** (depending on your Ditto model) to remove all log files from the logs storage location. You can also use the Text Interface to perform a factory reset. See Section 3.3: Factory Reset, page 77.
- **System Verify:** Verifies that the Ditto's operating system files have not been modified and places a statement in the system log. If the verification fails, the details can be viewed by exporting the System Diagnostics.
- **Diagnostics:** Exports a diagnostics log file in HTML format. The diagnostics log contains information about the Ditto’s current configuration, including user accounts, kernel messages, logs, process information, disks, PHP errors, and system verify results.

2.6.2. UPGRADE LOG MESSAGES

This section displays the status log of firmware upgrades and is only visible after a firmware upgrade has been performed.

2.6.3. IMPORT LOG MESSAGES

This section displays the status log of configuration file exports and imports and is only visible after a configuration file has been loaded.

3. TEXT INTERFACE

The Text Interface is the non-graphical text-based user interface available on all Ditto drive imager models.

Ditto Forensic FieldStation and Ditto DX Forensic FieldStation users: The Text Interface must be used when using your Ditto as a standalone device. No additional computer required, which can be useful when working with evidence disks in the field. You can access it through these devices' front panels.

Ditto x86 users: You can load into the Text Interface from the boot menu by choosing the **Ditto x86 option**. Use this interface if you are using your Ditto x86 with an older PC with graphical issues (e.g. an old MacBook® with AMD Radeon™ graphics), or if you prefer using a non-graphical text-based user interface instead of the Ditto GUI.

NOTE
The Ditto x86 may also be accessed remotely via a web browser when booted into the Text Interface. Remote users will see the Ditto GUI.

The Text Interface allows you to clone, physically image, perform a logical image using a Logical Image Mode, simultaneously clone and image, erase, hash a disk, or perform a snapshot of a disk. You can also adjust settings, view information about attached disks, or check on the Ditto's operational status.

TIP
The administrator account can assign access permissions to the Text Interface's actions and settings using the Ditto GUI and editing the 'panel' user account (see Section 2.4.1: User Accounts, page 61).

3.1. HOW TO NAVIGATE

3.1.1. USING A KEYBOARD

All Ditto drive imagers support a PC USB Keyboard.

Ditto Forensic FieldStation and Ditto DX Forensic FieldStation users: Plug a PC USB keyboard into a USB port on the side of your Ditto. It will automatically be detected.

TIP
Ditto DX users can plug their keyboard into the "Control" side of the Ditto DX to preserve the USB ports on the "Source" and "Destination" sides for drives.

Ditto x86 users: Use a keyboard connected to the computer you are using to boot your Ditto x86 with.

Here is a table of common keyboard commands:

KEY	COMMAND
Left	Backs out of a menu or setting and returns to the previous screen.
Right	Selects a menu option.
Up/Down	Navigates through the available screens and menu options.
Enter	Selects a menu option.
Escape	Cancels an edit when typing in a text field. Also exits Quick Start Mode if it is enabled.
Delete	Deletes the character currently highlighted by the cursor when editing a text field.
Backspace	Deletes the character immediately behind the cursor when editing a text field.
NumLock	Forces the numbered arrow keys to type numbers when pressed.
CapsLock	Forces all letter keys to type capital letters.

NOTE
If multiple keyboards are connected to the Ditto, keystrokes from all keyboards will be processed.

3.1.2. USING THE FRONT PANEL ON DITTO HARDWARE

If you are using the Ditto Forensic FieldStation or the Ditto DX Forensic FieldStation, you will use the navigation buttons on the front of the Ditto to navigate through the menu.

Use **Up** and **Down** to scroll through the available options in the Text Interface.

Use **Right** to select an option.

Use **Left** to go back to the previous screen.

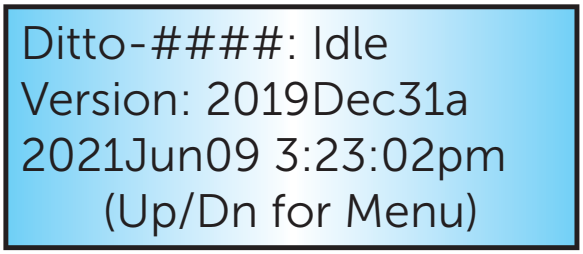
If Quick Start Mode is enabled, press **Left** to exit it.

3.2. MENU SCREENS

The Text Interface menu consists of the following screens:

3.2.1. STATUS SCREEN

The "Status" screen is the default screen. It shows the progress of any current processes. When the Ditto is “Idle”, the current firmware of the unit is also listed on this screen.



The “Status” screen on the Text Interface.

3.2.2. PERFORM ACTION SCREEN

The "Perform Action" screen is where you start, abort, and document the following actions:

- **Clone Disk:** Makes an exact duplicate of the source disk on one or two destination disks.
- **Physical Image Disk:** Creates an E01 or DD image of the source disk on one or two destination disks.
- **Logical Image Disk:** Creates an L01, ZIP, TAR, or LIST file containing selected types of files from the source disk on one or two destination disks. You can select from all available Logical Image Profiles except "Manual Select". See Section : Logical Image Profiles, page 16 for a list.
- **Clone & Image Disk:** Simultaneously creates a clone of the source disk on one destination disk and creates an image on a second destination disk.
- **Erase Disk:** The Ditto drive imager erases the destination disk using your preferred Erase Mode. The Erase Modes available are Clear Partition Table, Quick Erase, LBA/Offset Pattern, Custom Erase, Secure Erase Normal, Secure Erase Enhanced, DOD Clear, DOD Sanitize, NIST800-88 Clear, and NIST800-88 Purge.
- **Hash Disk:** Hashes the selected source or a destination disk using your preferred algorithm. Hash values are saved in the System Log. The available algorithms are MD5, SHA-1, SHA-256, MD5 & SHA-1, or MD5 & SHA-256.
- **Snapshot Disk:** Captures extended disk information about the selected target disk. This includes S.M.A.R.T., hdparm, USB, and SED information. What information is reported depends on the disk interface and disk capabilities.

PERFORMING ACTIONS WITH THE TEXT INTERFACE

1. Adjust the Ditto's settings to your requirements. See Section 3.2.4: Settings Screen, page 70.
2. Navigate to the "Perform Action" screen if you are not there already.
3. On the “Perform Action” screen, press **Up** and **Down** to cycle through the available actions. Press **Right** to select the one you want.
4. Cycle through the available settings for the action. Press **Right** if you wish to modify them.
5. When you are finished modifying settings, scroll down to option that asks you to start the action (ex. “Start Physical Image?”). Press **Right** to begin.

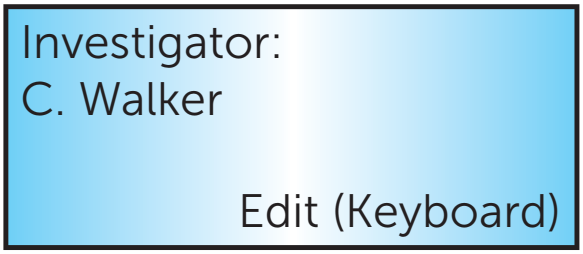
The status and remaining time will be displayed on the screen as the Ditto performs the action.

To abort an action, press **Left** at any time. The Ditto will ask if you wish to abort the action. Press **Right** to confirm, or **Left** to cancel the abort request.

3.2.3. INVESTIGATION INFO SCREEN

The “Investigation Info” screen groups related information that may also be used in creating custom directories and file names (see Section 2.3.10: Naming, page 58).

NOTE
To modify this Investigator Info from the Text Interface, you must have a keyboard attached.



The “Investigator” field in the “Investigation Info” screen on the Text Interface, when a USB keyboard is attached to the Ditto.

Each field is filtered to block non-printable ASCII characters. Any characters at the file system level that may not be safe for a directory name or file name will be filtered out and replaced with an underscore. Only printable ASCII characters are currently allowed for directory and filenames. Multiple underscores will also be reduced to a single underscore per naming item.

The Ditto will generate an error message if you enter a non-printable ASCII character or if your message exceeds the 58 character limit. Additionally, when the final directory or filename that uses any of these fields is created, another level of filtering is applied.

NOTE
Strings longer than 20 characters are displayed with an ellipses character (...) at the right side of the string.

To modify these settings from the Ditto GUI, see Section 2.2.2: Investigation Info, page 28.

3.2.4. SETTINGS SCREEN

The “Settings” screen allows you to view and customize the following settings, which are grouped into five subsections. These settings will be the default settings used in any actions performed.

NOTE

The settings accessible from the "Settings" screen cannot be modified if the "panel" user account does not have full access to the “Configure” permission. See Section 2.4: Admin Screen, page 60 for information on how to customize the "panel" user account.

SYSTEM SETTINGS

- **Default Format:** This is the default file system that will be used to format destination disks when they are used in actions that the Ditto performs. The available formats are HFS+, FAT32, exFAT, NTFS, EXT2, EXT3, EXT4, and XFS.
- **Physical Image Type:** Sets the default physical image type for all actions that create a physical image. The image types available are E01 or DD.
- **Logical Image Type:** Sets the default logical image type for the “Logical Image Source Disk” action. The logical image types available are L01, TAR, ZIP, and LIST.
- **Logical Image Mode:** Sets the default logical image profile. The logical image profiles available are All Files and Dirs, All Except Windows, All Except Windows Programs (abbreviated as “All Except... Programs”), Windows Registry Files (abbreviated as "Windows Re...try Files"), All Users - Windows, All Temporary - Windows (abbreviated as "All Tempor... - Windows"), All Except Swap and Hibernate (abbreviated as “All Except...Hibernate”), All Media Files, All Office Files, and All Financial Files. See Section : Logical Image Profiles, page 16 at the end of this subsection for information on what each profile does. See Section 4.4: AutoSelect Logical Image Profiles, page 84 for information on how to create your own profiles.
- **Hash Type:** Sets the default hash algorithm that will be used for disk verification and the “Hash Disk” action. The available algorithms are None, MD5, SHA-1, SHA-256, MD5 & SHA-1, or MD5 & SHA-256.
- **Erase Mode:** Sets the default erase mode that will be used for all actions that require erasing disks. The available modes are Clear Partition Table, Quick Erase, LBA/Offset Pattern, Custom Erase, Secure Erase Normal, Secure Erase Enhanced, DOD Clear, DOD Sanitize, NIST800-88 Clear, and NIST800-88 Purge.
- **Verify Single:** Determines whether individual destination disks are hashed and compared to the hash value of the source disk. The available options are Yes and No.
- **Verify Dual:** Requires that the “Dual Destinations” option below is enabled. Determines whether mirrored destination disks are hashed and compared to the hash value of the source disk’s hash value(s). You can choose to verify Destination 1 or Destination 2 individually, both disks, or none. Destination 1 and Destination 2 are selected when setting up the action to be performed.
- **Verify Clone & Image:** Determines whether cloned and imaged disks are hashed and compared to the hash value of the source disk’s hash value during a “Clone & Image Source Disk” action. You can choose to verify the clone, the image, both, or none.
- **Quick Start:** Enables the “Quick Start” screen on the Text Interface that appears after you boot or reboot your Ditto hardware. The settings for this mode may be modified in the “Quick Start” tab (see Section 2.3.11: Quick Start, page 60).
- **Autofill Inv. Info:** Automatically inserts the user account's full name into the Investigator name field located in the "Investigation Info" section of the "Home" screen (see Section 2.2.2: Investigation Info, page 28).

- **Prompt Invest. Info:** Prompts you to customize the following fields with a keyboard after you start an action (but before the action begins); Investigator, Case Number, Evidence Number, Description, Notes, Base Directory Name prefix, and the Base File Name prefix.
- **Prompt Case:** Determines how the "Case Number" field in the "Investigation Info" screen is handled when using the Text Interface. Five options may be chosen. “Disabled” leaves the case number as it is. “Inc/Dec” allows you to manually increment the case number up or down using the Up or Down arrows while using the Text Interface. “AutoInc” automatically increments the case number, and “AutoInc/Pause” automatically increments the case number, but displays a confirmation prompt on the Text Interface before beginning the requested action.

  NOTE
  This setting requires you to enter a number into the "Case Number" field specified in the "Investigation Info” screen in order to enable it (see Section 2.2.2: Investigation Info, page 28).

- **Prompt Evidence:** Determines how the "Evidence Number" field in the "Investigation Info" screen is handled when using the Text Interface. Five options may be chosen. “Disabled” leaves the evidence number as it is. “Inc/Dec” allows you to manually increment the evidence number up or down using the Up or Down arrows while using the Text Interface. “AutoInc” automatically increments the evidence number, and “AutoInc/Pause” automatically increments the evidence number, but displays a confirmation prompt on the Text Interface before beginning the requested action.

  NOTE
  This setting requires you to enter a number into the "Evidence Number" field specified in the “Investigation Info” screen in order to enable it (see Section 2.2.2: Investigation Info, page 28).

- **Lightbar Mode:** Enables or disables the light bar on the face of the Ditto DX Forensic FieldStation. The available settings are "Off" and "Color". This setting is only visible when using the Ditto DX Forensic FieldStation.
- **LCD/LED Brightness:** Sets the relative brightness of the LCD's and LED's on the Ditto Forensic FieldStation or the DX Forensic FieldStation on a scale of 0 to 6. Setting a value of “0” will turn off all LCD's and LED's on the unit. This setting has no effect on a Ditto x86.
- **Buzzer:** Alerts the user to various actions that occur when using the Ditto.

  NOTE
  Ditto x86 users: The Ditto x86 uses the host system's audible buzzer, so this feature will not function if the host system doesn't have one.

- **CPU Speed:** Sets the speed of the Ditto DX Forensic FieldStation’s CPU. The available settings from fastest to slowest are Turbo, Default, Economy, and Power Saver. This setting is only visible when using the Ditto DX Forensic FieldStation.
- **Dual Destinations:** Enables software mirroring mode to write the same data to two destinations at the same time. The available options are Enabled and Disabled.
- **Log Disk Info:** Determines whether S.M.A.R.T. and hdparm disk information is logged before running an action, after running an action, both, or not at all.

TIP
WiebeTech recommends that you log disk information both before and after an action to detect any disk problems that may have occurred during the action.

- **HTML Logging:** Logs are always saved in .XML format. This option causes your Ditto drive imager to save logs in HTML format as well. The available options are Off and On.
- **DiskView Logging:** Logs any action to preview a disk or actions performed while previewing a disk (i.e. starting or finishing a preview of a disk, starting or finishing a HexView action). The available options are Off and On.
- **Force SSL:** Forces a web browser to use Secure HTTPS to access the Ditto GUI.
- **Time Format:** Changes the time display in the top right corner of the Ditto GUI.

SRC (SOURCE) NETWORK SETTINGS

NOTE
The following settings cannot be modified if the "panel" user account does not have access to the “Network Settings” permission. See Section 2.4.4: Editing an Existing User, page 62 for information on how to customize the "panel" user account.

- **Src Network:** Enable or disable the Source Network Ethernet connection.

NOTE
This setting must be enabled in order to view the remaining settings in this section.

- **Src MAC Address:** Displays the Source Ethernet port’s MAC address.
- **Src IP Assignment:** Displays the Source Ethernet port’s IP assignment method. The available options are DHCP or Static. An IP address can be manually configured in the Ditto GUI (see Section : Source Network, page 45).
- **Src Network Access:** Allows you to choose whether or not the Ditto responds to any network traffic via the Source Ethernet port.
- **Src IP Address:** Displays the IP address assigned to the Source Ethernet port.
- **Src Subnet Mask:** Displays the subnet mask address assigned to the Source Ethernet port. It is only visible if the “Src IP Assignment” is set to “Static”.

DST (DESTINATION) NETWORK SETTINGS

NOTE
The following settings cannot be modified if the "panel" user account does not have access to the “Network Settings” permission. See Section 2.4.4: Editing an Existing User, page 62 for information on how to customize the "panel" user account.

- **Dst Network:** Enable or disable the Destination Network Ethernet connection.

NOTE
This setting must be enabled in order to view the remaining settings in this section.

- **Dst MAC Address:** Displays the Destination Ethernet port’s MAC address.
- **Dst Network Mode:** Displays the Destination Ethernet port’s networking mode. The available options are Server, Client (DHCP), or Client (Static IP). “Server” allows you to connect the Ditto directly to a computer without the use of an intermediary network. The network mode can be further configured in the Ditto GUI (see Section : Destination Network, page 46).
- **Dst IP Address:** Displays the IP address assigned to the Destination Ethernet port.
- **Dst Subnet Mask:** Displays the subnet mask address assigned to the Destination Ethernet port. It is only visible if “Dst Network Mode” is set to “Client (Static IP)” or “Server”.

CTL (CONTROL) NETWORK SETTINGS

NOTE
This menu option is only visible if you are using a Ditto DX Forensic FieldStation.

NOTE
The following settings cannot be modified if the "panel" user account does not have access to the “Network Settings” permission. See Section 2.4.4: Editing an Existing User, page 62 for information on how to customize the "panel" user account.

- **Ctl Network:** Enable or disable the Control Network Ethernet connection.

NOTE
This setting must be enabled in order to view the remaining settings in this section.

- **Ctl MAC Address:** Displays the Control Ethernet port's MAC address.
- **Ctl Network Mode:** Displays the Control Ethernet port's networking mode. The available options are Server, Client (DHCP), or Client (Static IP). "Server" allows you to connect the Ditto DX Forensic FieldStation directly to a computer without the use of an intermediary network. The network mode can be further configured in the Ditto GUI (see Section : Control Network, page 47).
- **Ctl IP Address:** Displays the IP address assigned to the Control Ethernet port.
- **Ctl Subnet Mask:** Displays the subnet mask address assigned to the Control Ethernet port. It is only visible if "Ctl Network Mode" is set to "Client (Static IP)" or "Server".

NETCAP SETTINGS

NOTE
This screen is only available on the Ditto Shark or when the Ditto Network Tap Module is being used with the Ditto Forensic FieldStation or Ditto DX Forensic FieldStation.

The "NetCap Settings" screen allows you to modify the settings that govern network capture actions.

- **NetCap Filter:** Sets the default network capture filter for the "Network Capture" action. The available filters are All, HTTP, E-Mail, SSH, or any available custom filter that you have saved onto the currently installed SD card. To create your own custom filter, see Section 4.5: Network Capture Filters, page 85.
- **NetCap File Count:** Specifies the maximum number of image files (based on image file segment size, see Section : Network Capture Settings, page 57) that are created on the Destination disk. When the number is reached, the Ditto will begin overwriting the oldest file on the disk for each new file that is created. Set this to '0' to fill the disk until it reaches capacity.
- **NetCap Snap Size:** Allows you to capture up to the specified amount of bytes of each packet of data.
- **NetCap Pkt Log Inter:** Allows you to specify the time interval in minutes of how often the Ditto writes its accumulated dropped packet information to the Action log. Setting this value to '0' disables packet loss reporting.
- **Live Capture:** Enable this service and it will run continuously in the background and stream captured data in real-time over the network to a remote monitor using the third-party Wireshark network protocol analyzer.
- **LiveCap Auto Start:** Set this value to 'Enabled' to turn on live capture as soon as the Ditto is powered on. Set this value to 'Disabled' if you want the user to choose when to start the live capture service in the Ditto GUI.
- **NetCap MTU:** If you are using the Network Tap Module on a network that's configured to a non-standard maximum transmission unit size (e.g. it uses jumbo frames), then set this field to match that value. Most Ethernet LANs will use the standard MTU of 1500. The commonly accepted range for a valid MTU is 68 to 65,535 as defined in RFC 791.

- **NetCap Link Speed:** Allows you to set the Ethernet connection speed throughput. In most cases, 'Auto Negotiate' will work. If you experience problems staying connected, you may need to change the speed to match what your network's capabilities are.

DATE & TIME

- **Date:** Displays the date and allows you to change it.
- **Time:** Displays the time and allows you to change it.
- **Timezone:** Displays the time zone and allows you to change it.

3.2.5. UTILITIES SCREEN

The "Utilities" screen allows you to reboot the Ditto.

- **Reboot:** Reboots the Ditto. Select this option, then select **Continue** to reboot the DItto.
- **Power Off:** Opens a confirmation to turn the Ditto x86 off. This option is only visible on Ditto x86 products.

3.2.6. DISK INFO SCREEN

The "Disk Info" screen shows all available Source Disks and Destination Disks. Ports are only displayed if a disk is connected there.

The "Disk Info" screen on the Text Interface.

Press **Right** to view Details, and then **Up** or **Down** to scroll through the partitions available on the disk.

The following information is displayed about each connected disk:

• Physical Port Location
• Model Number
• Capacity and File System

Press **Right** on a Disk to view Details, and then **Up** or **Down** to scroll through the partitions available on the disk. The following information is displayed about each partition:

• Port and Partition Number
• Used Capacity
• Available Capacity
• File System

NOTE
Disk details are only available on disks that have the capability to provide them when queried by the Ditto.

3.2.7. WEB INTERFACE

Select this menu item to boot into the Ditto GUI.

CAUTION
There are no submenu screens and no confirmation screen. Selecting this option will cause you to load immediately into the Ditto GUI.

NOTE
This setting is only available on the Ditto x86.

3.3. FACTORY RESET

To reset a Ditto Forensic FieldStation's or a Ditto DX Forensic FieldStation's settings back to their factory defaults using the Text Interface, follow these steps:

1. Press and hold the **Up**, **Right**, and **Down** navigation buttons on the Front Panel while powering the unit on. The Ditto will start up and then display the text, “Preparing Factory Reset”.
2. On the confirmation screen that appears soon after, press **Right** to continue or **Left** to cancel.

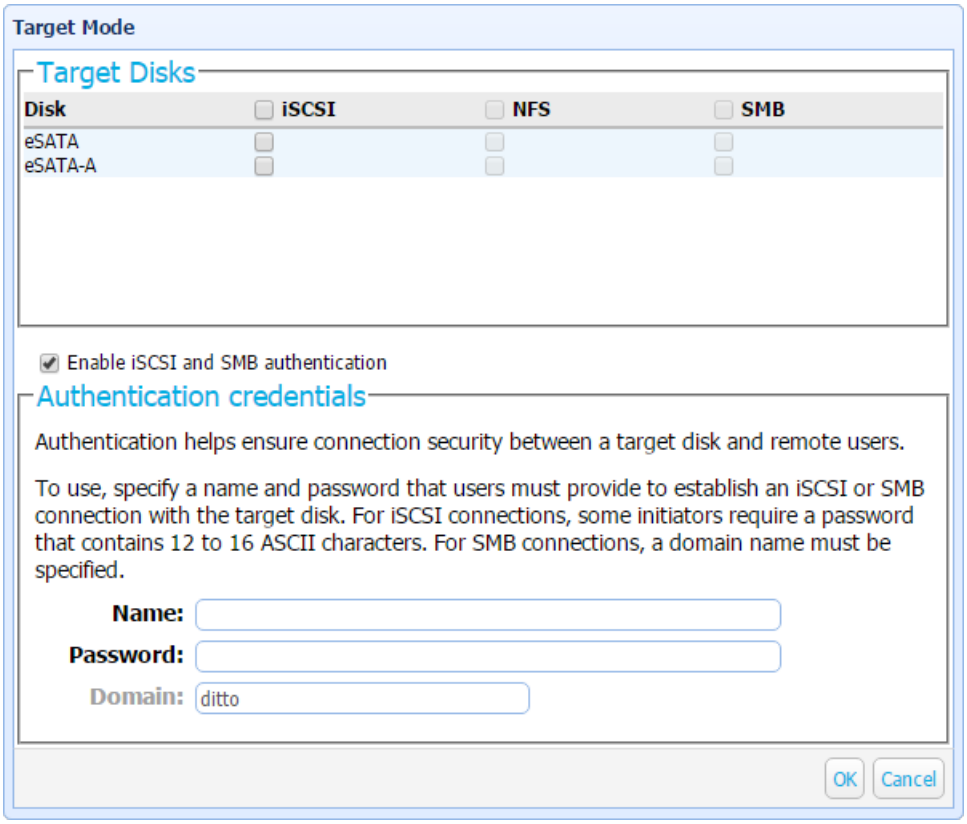
NOTE
This procedure is only possible on the Ditto Forensic FieldStation and Ditto DX Forensic FieldStation. Ditto x86 users can factory reset their unit from the Ditto GUI which is available on all Ditto products. See , [66].

4. ADVANCED FEATURES AND FUNCTIONS

4.1. TARGET MODE: REMOTELY ACCESS DISKS ATTACHED TO THE DITTO WITH THIRD PARTY SOFTWARE

NOTE
This feature is not yet available on the Ditto x86.

You can use third party data acquisition software to remotely connect to iSCSI disks that are connected to the Ditto. The machine this software is installed on does not have to be physically connected to any Ditto hardware. Instead, the software can be run remotely from a separate location within the same network.



The "Target Mode" window is used to allow computers and third party software to remotely connect via iSCSI to disks connected to Ditto.

Follow these steps to put the Ditto into Target Mode:

1. On the “Home” Screen, navigate down to the bottom of the “Disks” panel and select the **Target Mode button**.
2. Check the boxes in the iSCSI column next to the disk(s) that you wish to mount on your computer as iSCSI device(s).
3. Check **Enable iSCSI and SMB authentication** if you wish to require authentication in order for iSCSI initiator software to connect to the selected disk(s). Then input your desired credentials.
4. Press the **OK button**.
5. Input the Ditto’s IP address into your iSCSI initiator software in order to attach to it. Initiators can vary, but typically you’ll add the IP address to the “Discovery” section of your initiator software.

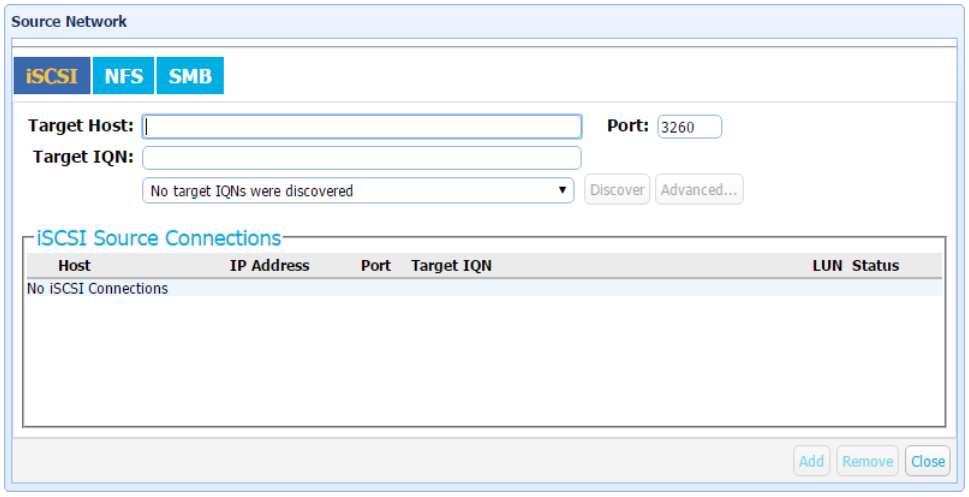
4.2. USING ISCSI DEVICES

4.2.1. HOW TO ACCESS AN ISCSI DEVICE

NOTE
This feature is not yet available on the Ditto x86.

These directions work regardless of whether you are connecting to an iSCSI device on the network or one physically attached to your Ditto.

1. Ensure that the Ethernet port through which the Ditto is connected to your network is properly configured for use with your network (see Section 2.3.2: Network, page 44). Unless you have manually configured the Ditto’s network settings before, you most likely do not have to change anything. If you are directly connecting the iSCSI device to the Ditto, then follow the directions in Section 4.2.2: Directly Connect an iSCSI Device, page 80 before continuing.
2. On the Ditto GUI, ensure you are on the “Home” Screen and navigate down to the bottom of the “Disks” panel.
3. Click the **Source Network button** if you want to attach the iSCSI device to the Ditto as a write-blocked source device, or click the **Destination Network button** if you want to attach the iSCSI device as a read/write-enabled destination.



The "Source Network" window's iSCSI tab allows you to connect iSCSI devices to the Ditto via the Source Side Ethernet port. The "Destination Network" tab looks similar and does the same via the Destination Side Ethernet port.

4. Click on the **iSCSI tab** if it is not already selected.
5. Type the iSCSI device's IP address into the "Target Host" text field.
6. Type in the port number of the target iSCSI volume into the "Port" text field if the number is different than the default value of '3260'. If you don't know the port number, leave it as the default value.
7. Click the **Discover button**. The Ditto will detect any IQNs (iSCSI Qualified Names) attached to the IP address.
8. Select the IQN you wish to attach to the Ditto from the drop-down box.
9. If authentication is required to connect to the IQN, click the **Advanced... button** and input the appropriate credentials, including the user name, password, and domain. Otherwise, continue to the next step.
10. Click the **Add button**. The IQN will now appear in the list below.
11. Repeat steps E through J to add more IQNs. When you are finished, click **Close**.

The iSCSI disk(s) have now been added to the list of Disks, allowing you to perform actions on them like you would any other disk.

4.2.2. DIRECTLY CONNECT AN ISCSI DEVICE

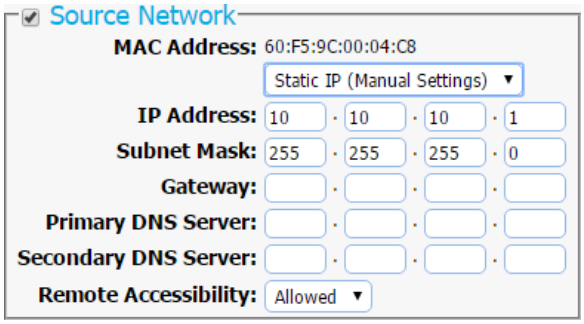
If you do not wish to connect an iSCSI device to your network (for example, it may be a suspect device with unknown properties), you can directly connect the device to the Ditto and isolate it from the rest of your network. There are two methods for doing so. Once you have connected the device, continue down to the third subsection, "Adding an iSCSI Disk to the 'Disks' Panel"

CONNECT VIA THE SOURCE SIDE ETHERNET PORT

NOTE
This feature is **only** supported by the Ditto Forensic FieldStation and the Ditto DX Forensic FieldStation. It is not available on the Ditto x86.

Follow these instructions if the iSCSI device you are attaching to the Ditto is a suspect device. You'll need to connect the iSCSI device to the Source Side Ethernet port and manually configure the IP address of both the Ditto and the iSCSI device.

1. Manually set the Ditto's IP address.
   a. On the Ditto GUI, click on the **Configure tab** at the top of the screen, and then select the **Network tab**.
   b. In the "Source Network" section, select **Static IP** from the drop-down box underneath the MAC address



The "Source Network" section on the "Configure" screen's "Network" tab, set to "Static IP".

   c. Type in the desired IP address and subnet mask into the appropriate fields. Do **not** fill in the Gateway, Primary DNS Server, or Secondary DNS Server unless directed to do so by your network administrator.
   d. Click **Commit Changes**.
2. Manually set the iSCSI device's IP address.The first three octets of the IP address must be identical to the first three octets of the Ditto's IP address. The fourth octet must be different, and must be any other number between 1 and 254.
3. Set the iSCSI device's subnet mask. It must be identical to the Ditto's subnet mask.
4. Set the iSCSI device's gateway. It must be identical to the Ditto's IP address.

NOTE
Based on the IP address configuration of a Ditto that's displayed in the figure above, a valid configuration for an iSCSI device would be as follows:

IP address: 10.10.10.100
Subnet mask: 255.255.255.0
Gateway: 10.10.10.1

5. Ensure that the iSCSI device is connected to the Source Side Ethernet port.
6. Continue to Section 4.2.1: How to Access an iSCSI Device, page 79 to access the iSCSI device from the Ditto GUI.

CONNECT VIA THE DESTINATION SIDE ETHERNET PORT

NOTE
This feature is **only** supported by the Ditto Forensic FieldStation and the Ditto DX Forensic FieldStation. It is not available on the Ditto x86.

Follow these instructions if you will be transferring evidence or other data to the iSCSI device:

1. Ensure that the Destination Side Ethernet port is configured to act as a server (see Section : Server, page 46).
2. Click on the **Configure tab** at the top of the page, and then select the **Network tab**.
3. In the "Destination Network" section, select **Server** from the drop-down box underneath the MAC address. Do not customize the default server configuration unless directed to do so by your network administrator.
4. Click **Commit Changes**.
5. Connect the iSCSI Device to the Destination Side Ethernet port. The iSCSI device will be assigned a new IP address if the iSCSI device is configured to obtain a new IP address from DHCP, which will the case for most devices. If no IP address is assigned, you will need to configure the iSCSI device to use DHCP. If that is not possible, contact your network administrator.
6. Once the iSCSI device is assigned an IP address, continue to Section 4.2.1: How to Access an iSCSI Device, page 79 to access the iSCSI device from the Ditto GUI.

4.2.3. REMOVE AN ISCSI DEVICE

This process prevents timeout issues where the Ditto will attempt to connect to iSCSI volumes that are no longer connected to it.

1. On the "Home" Screen of the Ditto GUI, navigate down to the bottom of the "Disks" panel.

2. Click the **Source Network button** if your iSCSI device is connected via the Source Side Ethernet port, or click the **Destination Network button** if your iSCSI device is connected via the Destination Side Ethernet port.
3. Click on the **iSCSI tab** if it is not already selected.
4. Under the “iSCSI Source Connections” or the “iSCSI Destination Connections” section, check the boxes next to the IQN(s) you want to remove and click the **Remove button**.
5. Physically disconnect the iSCSI device from the Ditto.

4.3. USING NFS AND SMB (SAMBA) SHARES

4.3.1. CONNECT TO NFS AND SMB NETWORK SHARES

1. Ensure that you are connected to the network that hosts the share you wish to connect to.
   - **Ditto Forensic FieldStation or Ditto DX Forensic FieldStation users:** Ensure that the network is physically connected to the appropriate Ethernet port on your Ditto. Use the Source Side Ethernet port to connect to a network share you wish to examine. Use the Destination Side Ethernet port to connect to a network share you wish to copy files to.
   - **Ditto x86 users:** Ensure that the host computer is connected to the network you wish to connect to.
2. On the Ditto GUI, ensure you are on the “Home” Screen and navigate down to the bottom of the “Disks” panel.
3. Click the **Source Network button** to connect to a network share you wish to examine. Click the **Destination Network button** to connect to a network share you wish to copy files to.

NOTE
Ditto Forensic FieldStation and Ditto DX Forensic FieldStation users: The Source Network button only displays network paths physically attached to the Source Side Ethernet port and the Destination Network button only displays networks physically attached to the Destination Side Ethernet port.

4. Click on the **NFS tab** or the **SMB tab**, depending on which type of share you are connecting to.
5. Type the server name into the "Server" text field.
6. If you are connecting to an SMB share, select the appropriate protocol from the **Protocol drop-down box**. If you don’t know the correct protocol, leave it as the default value of **SMBv1**.
7. Click the **Show Shares button**. The Ditto will detect any shares attached to the server.
8. Select the share you wish to attach to the Ditto from the drop-down box.
9. If you are connecting to an SMB share and authentication is required, click the **Advanced... button** and input the appropriate credentials, including the user name, password, and domain. If the SMB share does not require authentication or you are connecting to an NFS share, continue to the next step.
10. Click the **Add button**. The share will now appear in the list below.
11. Repeat steps C through I to add more shares. When you are finished, click **Close**.

The share(s) have now been added to the list of Disks, allowing you to perform actions on them like you would any other disk.

4.3.2. REMOVE AN NFS OR SMB (SAMBA) SHARE

1. On the Ditto GUI, ensure you are on the “Home” Screen and navigate down to the bottom of the “Disks” panel.
2. Click the **Source Network button** to disconnect a network attached as a Source, or click the **Destination Network button** to disconnect a network attached as a Destination.
3. Click on the **NFS tab** or **SMB tab**, depending on the which type of share you are removing.
4. Under the “iSCSI Source Connections” or the “iSCSI Destination Connections” section, check the boxes next to the share(s) you want to remove and then click the **Remove button**.

4.4. AUTOSELECT LOGICAL IMAGE PROFILES

AutoSelect is a feature that allows you to search during a logical image action only for those file types of interest to you.

4.4.1. CREATING A PROFILE

AutoSelect profiles are XML files that follow the structure detailed below. Below the code structure are also a series of additional considerations you should take into account when writing your own profiles.

```
<?xml version=”1.0” encoding=”UTF-8”?>
<!-- All attributes must be in single quotes if they contain double quotes.
-->
<DittoAutoSelect
xmlns:xsi=”http://www.w3.org/2001/XMLSchema-instance”
xsi:noNamespaceSchemaLocation=”autoSelect.xsd”
>
<select title=”Example Title”>
<include path=”*”>
<name>*.jpeg</name>
<name>*.jpg</name>
<name>*.m4*</name> <!-- .m4a, .m4v, etc -->
</include>
<exclude path=”Windows”/>
</select>
</DittoAutoSelect>
```

The name of the auto select XML file can be any legal file name with a .xml file extension. Each AutoSelect XML file may contain one or more <select title=”...”> blocks. The select block’s title will appear at the bottom of the “Logical Image Mode” selection list prepended with “SDCard/” followed by the subdirectory’s name, if any.

Each select block may contain one or more <include path=”...”> and/or <exclude path=”...”> blocks. The include/exclude block’s path (case-insensitive) may contain wildcard characters and will be included in or excluded from the auto selection, respectively.

Each include block may contain zero or more <name>...</name> blocks, which specify a file name to be included in the auto selection. File names are case-insensitive and may contain wildcard characters to specify a set of file names. Exclude blocks cannot contain name blocks.

NOTE
You cannot remove the pre-made profiles from the Logical Image Mode list.

DOWNLOAD AN XML SCHEMA FOR VALIDATION

Ditto Forensic FieldStation and Ditto DX Forensic FieldStation users: Type the following into the address bar of an Internet browser, where <IP Address> is the IP address of your Ditto hardware: **http://<IP Address>/data/DittoAutoSelect/autoSelect.xsd**. Then press **Enter**. You can then save the XSD file to the location of your choice.

Ditto x86 users: Type the following into the address bar of the Ditto GUI: **localhost/data/DittoAutoSelect/autoSelect.xsd**. Then press **Enter**. The XSD file will automatically download to the "download" folder in the "Ditto Logs" storage location.

4.4.2. ADD A NEW PROFILE TO DITTO

1. Access the "Ditto Logs" storage location.
   - **Ditto Forensic FieldStation and Ditto DX Forensic FieldStation users:** Remove the SD card from your Ditto hardware and open it on your computer.
   - **Ditto x86 users:** Connect the Ditto x86 to your computer and access the "Ditto Logs" volume from your computer.
2. Create a directory named **DittoAutoSelect** in the root of the "Ditto Logs" storage location and open it.
3. Place your AutoSelect logical image profile XML file(s) into the directory.
4. If you are a Ditto Forensic FieldStation or Ditto DX Forensic FieldStation user, reinsert the SD Card into your Ditto hardware.

Your custom AutoSelect profiles will now be available in the Ditto GUI. Navigate to the "Home" screen and choose the "Logical Image Source Disk" action in the "Action" panel. Your custom AutoSelect profiles can be found in the “Logical Image Mode” drop-down box.

4.5. NETWORK CAPTURE FILTERS

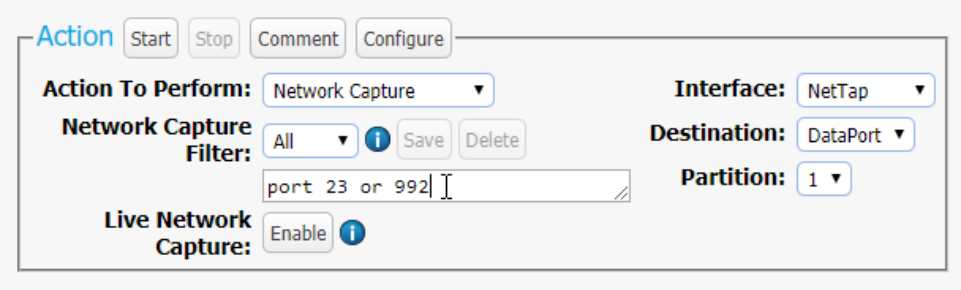
NOTE
This feature is only available for use with the Ditto Shark or when the Ditto Network Tap Module is being used with the Ditto Forensic FieldStation or Ditto DX Forensic FieldStation.

Insert the SD Card containing your network capture filter(s) into the your Ditto Forensic FieldStation or Ditto DX Forensic FieldStation and your custom network capture filters will become available in the “Network Capture Filter” drop-down box when configuring a “Network Capture” action. You may also add sub-directories that contain one or more network capture filter XML files to the DittoNetCapFilter directory.

Choose the way to add or edit your own network capture filter that works best for your usage scenario.

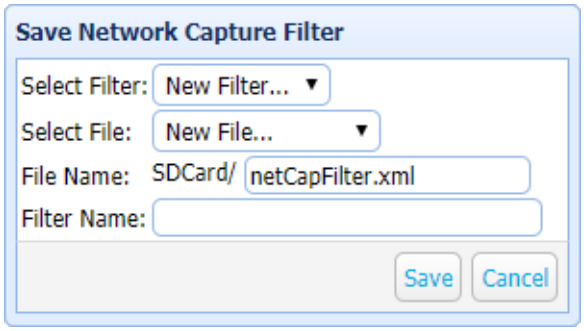
4.5.1. CREATING FILTERS WITH A WEB BROWSER AND THE DITTO GUI

1. If you are using a Ditto Forensic FieldStation or Ditto DX Forensic FieldStation, insert the SD card containing your network capture filter(s) into your Ditto. If you are using a Ditto x86, continue on to the next step.
2. Using the Ditto GUI, select **Network Capture** from the “Action to Perform” drop-down box.
3. If you are editing an existing network capture filter that you created, select it from the “Network Capture Filter” drop-down box. If you are creating a new filter, continue on to the next step.
4. Type in the ports you wish to capture in your network capture filter in the text box directly below the “Network Capture Filter” drop-down box (see image below). Use the word ‘or’ to separate each port.



The “Action” panel, showing where to type in the ports that you wish to capture with the “Network Capture” action.

5. Click the **Save button**. The “Save Network Capture Filter” dialog box will pop up (see image below).



The “Save Network Capture Filter” dialog box lets you save custom network capture filters.

6. Use the “Select Filter...” drop-down box and select **New Filter...** to create a new filter or select an existing filter to overwrite it.
7. Use the “Select File...” drop-down box and select **New File...** to create a new XML file, or select an existing file to add your network capture filter to the file.

8. Type the desired filename into the “File Name” text box.
9. Type the desired name of the filter into the “Filter Name” text box.
10. Click the **Save button** to save the filter.

4.5.2. MANUAL FILTER CREATION

You can manually create a network capture filter by using the XML code structure below. Below the code structure are a series of additional considerations you should take into account when creating your own filters.

```
<?xml version=”1.0” encoding=”UTF-8”?>
<!-- All attributes must be in single quotes if they contain double quotes.
-->
<dittoNetCapFilter
xmlns:xsi=”http://www.w3.org/2001/XMLSchema-instance”
xsi:noNamespaceSchemaLocation=”netCapFilter.xsd”
>
<filter title=”All”>insert port numbers here, separated by the word‘or’</
filter>
</dittoNetCapFilter>
```

The name of the network capture filter XML file can be any legal file name with an XML file extension. Each XML file may contain one or more <filter title=”...”> blocks. The filter block’s title will appear at the bottom of the “Network Capture Filter” selection list prepended with “SDCard/” followed by the subdirectory’s name, if any.

NOTE
You cannot remove existing selections from the Network Capture Filter list.

Click the **Information icon** for a link to a site that describes the syntax supported by network capture filters.

DOWNLOAD AN XML SCHEMA FOR VALIDATION

Ditto Forensic FieldStation and Ditto DX Forensic FieldStation users: Type the following into the address bar of an Internet browser, where <IP Address> is the IP address of your Ditto hardware: **http://<IP Address>/data/DittoNetCapFilter/netCapFilter.xsd**. Then press **Enter**. You can then save the XSD file to the location of your choice.

Ditto x86 users: Type the following into the address bar of the Ditto GUI: **localhost/data/DittoNetCapFilter/netCapFilter.xsd**. Then press **Enter**. The XSD file will automatically download to the "download" folder in your Ditto Logs partition.

MANUALLY ADD A NEW FILTER TO DITTO

1. Access the "Ditto Logs" storage location.

- **Ditto Forensic FieldStation and Ditto DX Forensic FieldStation users:** Remove the SD card from your Ditto hardware and open it on your computer.
- **Ditto x86 users:** Connect the Ditto x86 to your computer and access the "Ditto Logs" volume from your computer.

2. Create a directory named **DittoNetCapFilter** and open it.
3. Place your network capture filter XML file(s) into the directory.
4. If you are a Ditto Forensic FieldStation or Ditto DX Forensic FieldStation user, reinsert the SD Card into your Ditto hardware.

Your network capture filters will now be available in the Ditto GUI. Navigate to the "Home" screen and choose the "Network Capture" action in the "Action" panel. Your custom filters can be found in the “Network Capture Filter” drop-down box.

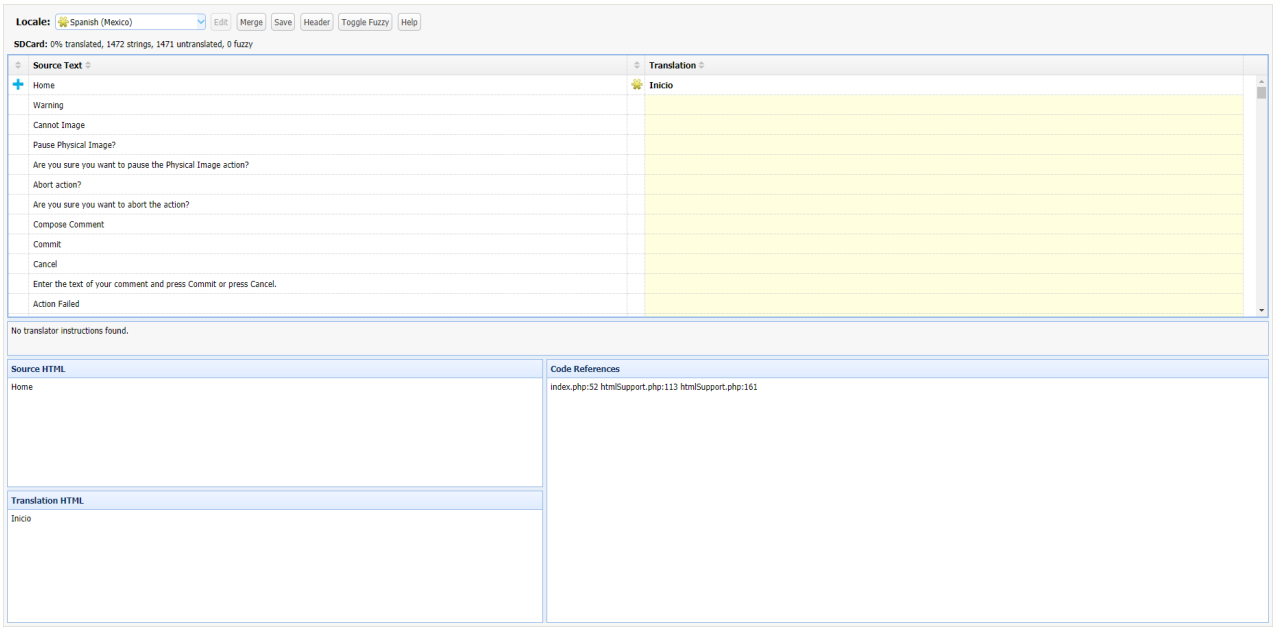
4.6. LOCALIZATION AND TRANSLATION

4.6.1. LOGGING INTO THE I18N TRANSLATE SCREEN

1. While using the Ditto GUI, type the following URL into the browser, where <IP Address> is your Ditto unit's IP address: **http://<IP Address>/I18N.php**. Then press **Enter**.
2. Log into the Ditto GUI's "I18N Translate" screen with your username and password.
3. Click on the **Locale drop-down box** and choose the language you'd like to view.

4.6.2. I18N TRANSLATE SCREEN OVERVIEW

The "I18N Translate" Screen is where you can view, manage, and edit the translations stored in the "Ditto Logs" storage location.



The "I18N Translate" Screen, showing the toolbar, the "Source Text" and "Translation" tables, and the "Translator Instructions", "Code References", "Source HTML", and "Translation HTML" text boxes.

TOOLBAR

- **Locale:** Click on this to select a translation to view. An Asterisk symbol in this column indicates that the translation file is located in the logs storage location (the SD card in the Ditto Forensic FieldStation and Ditto DX Forensic FieldStation, or the Ditto Logs partition on the Ditto x86). It also indicates that the file is either overriding the built-in locale or is providing a new translation. A Star symbol indicates that the translation file is stored on the Ditto's built-in non-accessible storage and is fully supported by WiebeTech.
- **Edit:** Allows you to edit the selected translation.
- **Merge:** Use this button when you want to update the locale files that exist on the SD card with message changes that may have been introduced in the last firmware upgrade. This button is only enabled when the necessary locale files for the selected locale exist in the 'Locale' directory.
- **Save:** Saves the translation. This button is only enabled when changes have been made to a translation or the PO file header.
- **Header:** Allows the translator to modify some of the translation PO file's header information.
- **Toggle Fuzzy:** Toggles the Fuzzy symbol for the selected row. Once saved, fuzzy translations will not appear on the Ditto GUI or Text Interface.

  NOTE
  'Fuzzy' means that the text string was modified since the last firmware upgrade or is new and very similar to one of the old text strings.

- **Help:** Opens the "Help" dialog box for the "Translate Page".

STATUS BAR

The status bar indicates the location that the currently selected translation is saved, the percentage of text strings that have been translated, the total number of text strings available, the total number of untranslated strings, and how many strings are marked as fuzzy.

The location is marked in **bold** and indicates that the translation file is stored on the Ditto's built-in non-accessible storage ("Built-in") or in the "locale" directory on the SD card ("SD card").

NOTE

Ditto x86 users: When the status reads "SD Card," the locale file is actually stored in the "Ditto Logs" partition on the Ditto x86.

TRANSLATION SECTION

The columns in the translation table are defined from left to right:

- **Source Status:** A + Modified symbol appears after the text string has been translated during the current session.
- **Source Text:** The English version of the text to be translated.
- **Translation Status:** A Fuzzy symbol appears if the translated text string was modified since the last firmware upgrade or is new and very similar to one of the old text strings. You can manually toggle this status on or off by clicking on the text in the "Translation" column and then clicking on the **Toggle Fuzzy button**.

  NOTE

  Translated text strings marked as 'fuzzy' **will not** appear on the Ditto GUI or Text Interface.

- **Translation:** Contains the localized version of the text string. It is blank if no translated text string has been provided. This field may be edited.

The remaining four text boxes are defined from top to bottom, left to right:

- **Translator Instructions:** Displays instructions to the translator, if any, about the context and usage of the currently selected text string in the translation table.
- **Source HTML:** Shows the English raw HTML of the currently selected text string in the translation table.
- **Code References:** Shows each PHP page and line on the page where the currently selected text string is used.
- **Translation HTML:** Shows the translated raw HTML of the currently text string in the translation table. This field may be edited.

4.6.3. HOW TO TRANSLATE

You can localize your Ditto to any language by following the directions below.

IMPORTANT
Ditto Forensic FieldStation and Ditto DX Forensic FieldStation users: Ensure that an SD card is inserted into the Ditto. An SD Card is **required** since that is where the translation files are stored for these devices.

1. Log into the "I18N Translate" page. See Section 4.6.1: Logging into the I18N Translate Screen, page 88.
2. Choose the desired language from the **Locale drop-down box** and wait for the page to load the translation file and refresh the page.
3. Once the page reloads, click the **Edit button** to enable editing. There may be a short pause as the Ditto writes the translation file in the logs storage location.
4. Click on the desired text string in the "Translate" column in the translate table. You may then modify or write new text there. When finished, press **Enter**.
5. You can optionally modify the HTML for the selected text string by clicking into the "Translation HTML" text box at the bottom of the page.
6. Continue modifying rows until finished.
7. Click the **Save button** to save your translation. Saved translations are located in the the logs storage location (the SD card in the Ditto Forensic FieldStation and Ditto DX Forensic FieldStation, or the Ditto Logs partition on the Ditto x86).

TIP
Be sure to save occassionally by clicking on the **Save button**!

OTHER CONSIDERATIONS

- You can quickly find "fuzzy" translations by clicking the header of the "Translation status" column (the third column) to sort it to show fuzzy translations first. You can also sort for messages that need a translation by clicking the header of the "Translation" column.

  NOTE
  'Fuzzy' means that the text string was modified since the last firmware upgrade or is new and very similar to one of the old text strings.

- Translated text strings marked as 'fuzzy' **will not** appear on the Ditto GUI or Text Interface.
- Be sure to pay attention to whether there are any translator instructions in the "Translator instruction" text box, located directly below the translation table. These instructions can provide valuable context as to how the selected text string is used by the Ditto.
- The "Code References" text box can also provide additional context because it calls out on which screens the currently selected text string is used.

4.6.4. COPYING TRANSLATIONS TO OTHER DITTOS

Follow these instructions to copy the translations to other Dittos:

1. Connect the media containing your translation files to a computer while it's already booted.
   - **Ditto Forensic FieldStation and Ditto DX Forensic FieldStation users:** Remove the SD card from your Ditto and connect it to a computer.
   - **Ditto x86 users:** Connect your Ditto x86 to a computer while it's booted.
2. Open the media volume you just connected.
   - **Ditto Forensic FieldStation and Ditto DX Forensic FieldStation users:** Open the SD card volume and navigate to the "locale" folder.
   - **Ditto x86 users:** Open the "Ditto Logs" volume and navigate to the "locale" folder.
3. Copy the folders for each translation you want to your computer.
   - To copy individual translations, open the "locale" folder and select the individual translation folders and copy them to your computer.
   - To copy all translations, copy the entire "locale" folder to your computer.
4. Connect the media to which you want to copy your translation files to your computer.
   - **Ditto Forensic FieldStation and Ditto DX Forensic FieldStation users:** Remove the SD card from your Ditto and connect it to a computer.
   - **Ditto x86 users:** Connect your Ditto x86 to a computer while it's booted.
5. Open the "Ditto Logs" storage location. See Section 1.2: "Ditto Logs" Storage Location and Behavior, page 8.
6. If you are copying individual translations, create a folder named "locale" in the root of your media and open. Otherwise, continue onto the next step.
7. Copy the translation files from your computer to your media.
   - If you are copying individual translations, copy them into the "locale" folder you just created.
   - If you are copying the "locale" folder, copy it into the root of the media.
8. **Ditto Forensic FieldStation and Ditto DX Forensic FieldStation users:** Return the SD card to your Ditto.

You've successfully copied your translation files! Repeat these steps for each Ditto you want to put your translations onto.

4.6.5. MERGING TRANSLATIONS INTO NEW FIRMWARE UPDATES

Follow these instructions

IMPORTANT

Ditto Forensic FieldStation and Ditto DX Forensic FieldStation users: Ensure that the SD card containing the translations is inserted into the Ditto. This SD Card is **required** since that is where the translation files are stored for these devices.

1. Log into the "I18N Translate" screen. See Section 4.6.1: Logging into the I18N Translate Screen, page 88.

2. Select the translated language you want to merge from the **Locale drop-down box**.
3. Click on the **Merge button**. This will merge any POT file updates with the translation files where they are stored and also open up Edit Mode.
4. Click the header of the "Translation status" column (the third column) to sort it to show fuzzy translations first. This will bring the new strings that need re-translated up to the top of the list.
5. Translate the text strings that need translated. See Section 4.6.3: How to Translate, page 90.
6. When you are finished, click the **Save button** to save your translation.

4.6.6. DELETING TRANSLATIONS

Follow these instructions to delete a translation from a Ditto:

1. Log into the "I18N Translate" screen. See Section 4.6.1: Logging into the I18N Translate Screen, page 88.
2. Select the language you want to delete from the **Locale drop-down box**.
3. Click on the **Header button**.
4. On the window that pops up, note the text under the "Language" section. This is the name of the folder that you will need to delete later on. (e.g. "es_MX")
5. Connect the media containing your translation files to a computer while it's already booted.
   - **Ditto Forensic FieldStation and Ditto DX Forensic FieldStation users:** Remove the SD card from your Ditto and connect it to a computer.
   - **Ditto x86 users:** Connect your Ditto x86 to a computer while it's booted.
6. Open the media volume you just connected.
   - **Ditto Forensic FieldStation and Ditto DX Forensic FieldStation users:** Open the SD card volume and navigate to the "locale" folder.
   - **Ditto x86 users:** Open the "Ditto Logs" volume and navigate to the "locale" folder.
7. Find the folder with the same text you noted down in the Header window (e.g. "es_MX") and delete it.

You've successfully deleted the translation! Repeat these steps for any other translations you wish to delete.

5. UPGRADING FIRMWARE

Firmware upgrades are made available on CRU and WiebeTech's website at www.cru-inc.com/support/software-downloads/ditto/

There are three methods to upgrade your Ditto's firmware.

5.1. METHOD 1: MANUALLY ENTER A DOWNLOAD LINK

NOTE
This method requires the Ditto to have an Internet connection.

1. Ensure that the Ditto is connected to a network with Internet access.
2. Go to the firmware updates webpage and choose your Ditto product.
3. Scroll down to the table of available firmware downloads. Copy or write down the URL of the firmware you wish to use from the "Download (or right click to copy to clipboard)" column.
4. Log into your Ditto's Ditto GUI and navigate to the "Utilities" screen.
5. Type or paste the link into the top text field and click the **Firmware Upgrade button**.
6. When it asks you to confirm the retrieval of the upgrade file, click **Continue**.
7. The Ditto will download the file and install it. After the upgrade is finished, click **OK**.
8. A dialog box will appear asking you to reboot. Click the **Reboot button** to reboot or **Continue** to use the Ditto without rebooting.

NOTE
You must reboot for the firmware to take effect.

5.2. METHOD 2: DOWNLOAD TO YOUR COMPUTER

NOTE
This method works with the Ditto Forensic FieldStation and the Ditto DX Forensic FieldStation, as well as when using the Ditto x86 remotely. It does **not** work when you are using the Ditto x86 directly.

1. Go to the firmware updates webpage and choose your Ditto product.

2. Scroll down to the table of available firmware downloads. Click on the firmware you wish to use from the "Download (or right click to copy to clipboard)" column. A "Save As" dialog box will appear. Save the file in a convenient location.
3. Log into your Ditto's Ditto GUI and navigate to the “Utilities” screen.
4. Click on the **Upload... button**.
5. Locate the firmware file you just downloaded, select it, and click **Open**.
6. Click on the **Firmware Upgrade button**.
7. When it asks you to confirm the retrieval of the upgrade file, click **Continue**.
8. The Ditto will copy the file over to itself and install it. After the upgrade is finished, click **OK**.
9. A dialog box will appear asking you to reboot. Click the **Reboot button** to reboot or **Continue** to use the Ditto without rebooting.

NOTE
You must reboot for the firmware to take effect.

5.3. METHOD 3: UPLOAD VIA A USB THUMB DRIVE

1. Go to the firmware updates webpage and choose your Ditto product.
2. Scroll down to the table of available firmware downloads. Click on the firmware you wish to use from the "Download (or right click to copy to clipboard)" column. A "Save As" dialog box will appear. Save the file to a USB thumb drive.
3. Connect the thumb drive.
   - **Ditto Forensic FieldStation and Ditto DX Forensic FieldStation users:** Insert the thumb drive into the Source Side USB port.
   - **Ditto x86 users:** Plug the thumb drive into your host computer.
4. The Ditto will immediately scan the thumb drive and display a list of all firmware files found on the drive.
   - **Ditto Forensic FieldStation and Ditto DX Forensic FieldStation:** The list can be found on the Front Panel of your Ditto. Use the **Up** and **Down** arrows to move the cursor to the firmware that you wish to use and then press **Right**.

     CAUTION
     No confirmation dialog box will appear after you press Right. Doing so will immediately update your device's firmware.

   - **Ditto x86 Text Interface:** Use the **Up** and **Down** arrows to move the cursor to the firmware that you wish to use and then press **Right**.

     CAUTION
     No confirmation dialog box will appear after you press Right. Doing so will immediately update your device's firmware.

- **Ditto x86 Ditto GUI (Kiosk Mode):** A "USB Upgrade" window will appear after a moment. Select the firmware you wish to use than the click the **Upgrade button**. Then click **OK** on the confirmation dialog box that appears.

5. The Ditto's firmware will be upgraded. The Ditto will ask you to reboot. You may choose to do so now or continue using the Ditto without rebooting.

NOTE
You must reboot for the firmware to take effect.

6. LICENSING AND SUBSCRIPTIONS

Users of the Ditto x86 require a software license in order to use the product. Each brand new Ditto x86 comes with a year-long license subscription, after which the subscription can be renewed.

Users of the Ditto Forensic FieldStation, Ditto DX Forensic FieldStation, and Ditto Shark do not need a software license subscription to use each product.

6.1. SUBSCRIPTION STATUS

On the "Home" screen of the Ditto GUI, you can look at the "License" indicator in the "System Settings" panel to see the status of your subscription at a glance. The following table lists the different statuses:

STATUS	DESCRIPTION
No Indication	Your subscription is active.
Yellow bar	Your subscription is active but is within 30 days of expiring.
Orange bar	Your subscription is active but is within 7 days of expiring.
Red bar	Your subscription has expired and needs to be renewed, or it is missing and needs to be re-validated. To renew, see Section 6.2: Renewing a Subscription, page 97. To re-validate, see Section 6.3: Validating a Subscription, page 97.

To see more detail about your subscription status, click the **Information icon** next to the License indicator. It will display the following information:

- **License Status:** Displays whether your license is valid or expired.
- **Device ID:** Displays your product's unique device ID number.
- **Device Model:** Displays your base product model.
- **Device Serial:** Displays your product's unique serial number.
- **Feature:** Displays which subscription level you have.
- **Expiration:** Displays your expiration date.

6.2. RENEWING A SUBSCRIPTION

To renew your license subscription, please contact WiebeTech Sales. We are available Monday through Friday, from 8AM to 5PM Pacific.

- United States: 1-800-260-9800, Option 2
- International: +1-360-816-1800, Option 2

After you renew your subscription, you may have to re-validate it. See Section 6.3: Validating a Subscription, page 97.

6.3. VALIDATING A SUBSCRIPTION

Every Ditto x86 comes with a year-long subscription and does not need to be validated to use. However, sometimes there are cases when validating a subscription is necessary.

The Ditto x86 will need an active Internet connection to connect to the licensing server and validate your license. See Section : Source Network, page 45 when using the Ditto GUI or Section : Src (Source) Network Settings, page 73 when using the Text Interface to connect to the Internet.

To validate your subscription, click on the Refresh icon next to the "License" indicator, located in the "System Settings" panel on the "Home" screen, as well as on the "System" tab on the "Configure" screen.

Once validated, you should not need to reconnect to the Internet to validate your subscription again until you renew it.

NOTE

If you unplug the Ditto x86 from the host computer, your license will no longer be detected and you will lose functionality. Plug the Ditto x86 back in and refresh the page if you are using the Ditto GUI. If you are using the Text Interface, plug the Ditto x86 back in and reboot it. The license will reactivate after a moment, even without an Internet connection.

7. PRODUCT SUPPORT

Your investment in CRU and WiebeTech products is backed up by our free technical support for the lifetime of the product. Contact us through our website, cru-inc.com/support or call us at 1-800-260-9800 or +1-360-816-1800.

This page is intentionally left blank.