MANAGING STORAGE

on HP devices using HP Web Jetadmin

CONTENTS

OVERVIEW

HP Web Jetadmin provides several options for managing storage media in HP devices. Device lists display all storage media types and properties/contents. Hard disks can be initialized or securely erased using different levels of data overwrite. Fonts, forms, and macros can viewed, added, deleted, and remotely printed on devices. Print jobs that have been stored on the printer through the job retention feature of the printer driver (disk jobs) can be viewed, deleted, and remotely printed.

STORAGE COLUMNS

HP Web Jetadmin offers several columns to view various types of storage media and their contents that are present on devices (see Figure 1). Columns can be enabled to determine whether devices contain hard disks, RAM disks, or flash disks. The contents of disks can be displayed by hovering over the column values for **Resident Fonts** or **Fonts and Macros**. Methods for overwriting data during erase operations can be viewed by enabling **Secure File Erase Mode** or **Secure Disk Encryption Mode**. It can be determined which devices have a file system password set by enabling **File System Password**. **File System External Access** allows for determining whether NFS, PJL, etc. are enabled or disabled on devices.

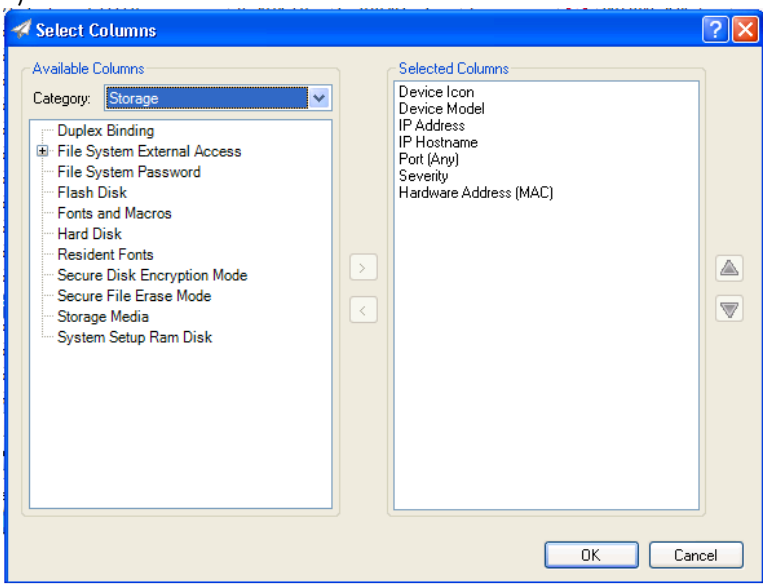

Figure 1 – Storage Columns

STORAGE TAB

Storage media can be managed on a device in HP Web Jetadmin by selecting the **Storage** tab while viewing a device or multiple devices (see Figure 2). Clicking on the **View** drop-down menu displays a list of media types or files upon which actions can be performed:

- Media
- Fonts and Macros
- Resident Fonts
- Disk Jobs

Figure 2 – Storage Tab View Drop-down Menu

MEDIA

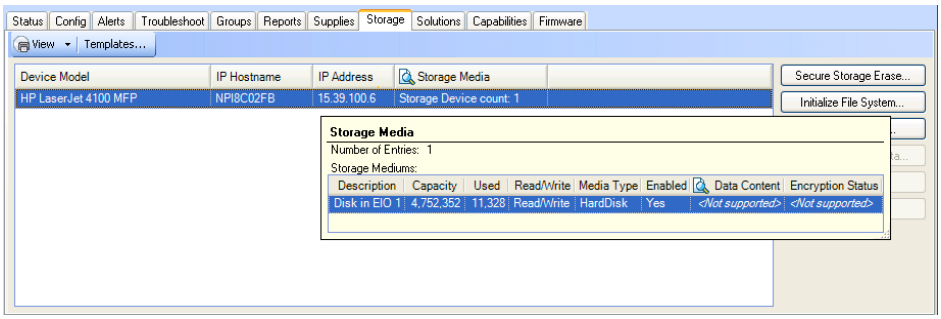

FIGURE 3 – STORAGE MEDIA PROPERTIES

Once the **Media** item has been selected from the **View** drop-down menu, a **Storage Media** column is visible that contains a list of all storage media installed on the device. If the **Storage Device** count is 1 or greater, the mouse-over tool tip displays a table of all the storage media on the device. The table contains the properties of the media such as **Description** and **Size** (see Figure 3). Once a device model is highlighted, the following actions are available by clicking on their respective boxes on the right hand side of the screen depending upon what is supported by the particular model:

- **Secure Storage Erase**: Starts the secure storage erase action on the device. Various secure modes can be set for the storage erase action to dictate how many levels of overwrite will occur to secure the erase operation.
- **Initialize File System**: Causes the device user directory structure to initialize. The file system will vary depending on device or storage type. This feature can be scheduled as a one-time or recurring operation.
- **Write Protection**: Enables or disables write functionality on the selected storage facility.
- **Erase Customer Data**: Starts the Erase Customer Data wizard for the selected devices. Various secure modes can be set for the storage erase action to dictate how many levels of overwrite will occur to secure the erase operation. This operation will remove any stored job information from the device. Device configuration settings will not be erased.
- **Use Drive**: If a device has more than one drive installed, this allows for selecting the drive where configuration files, stored jobs, and temporary files are stored and for moving existing customer data to that drive.
- **Erase Drive**: Completely erases a drive. This process does not preserve any data. The Secure Erase option selects the most secure erase method available for the selected drive. The Cryptographically Erase option is performed only on secure drives. This option resets the encryption key, prevents access to the data, turns the drive off and then on, and re-encrypts the drive with new keys.

Secure Storage Erase

Normally when a file is deleted from a hard disk drive, the file name entry is erased from the disk's file allocation table, removing the file's presence. The file's data still exists in the disk's individual sectors and is overwritten only when that sector is allocated for a different file. HP Secure Storage Erase technology overwrites a deleted file's data from the individual sectors with random data using either a one pass or three pass overwrite which conform to current US Government specifications. The Secure Erase Mode feature controls how temporary job files are erased at the completion of print, copy, fax, or digital send jobs as well as how disks are erased using Secure Storage Erase. The Secure Erase Mode for deleting temporary files can be set under **Configuration, File System**. Temporary job files include:

- Temporary data for print jobs
- Temporary data for copy, fax, e-mail, and send to network folder jobs

The HP Secure Erase feature will not impact data stored on:

- Flash-based non-volatile RAM that is used to store default printer settings, page counts, etc.
- A system RAM disk (if utilized)
- The flash-based system boot RAM

Changing the erase mode (Secure Sanitizing Erase, Secure Fast Erase, or Non-secure Fast Erase) does not overwrite previously stored data on the disk, nor does it immediately perform a full Secure Storage Erase. Changing the erase mode dictates how the MFP erases data after the erase security mode has been changed. To enable Secure Storage Erase, select **Secure Storage Erase** on the right hand side of the screen after highlighting the printer from the **Media** selection on the **View** drop-down menu (see Figure 4). The following Secure Erase Mode options are available for selection:

- **Non-secure Fast Erase mode**: Performs standard file system delete only (does not overwrite file data)
- **Secure Fast Erase mode**: Performs a one pass overwrite of all data
- **Secure Sanitizing Erase mode**: Performs a three pass overwrite of all data

A device File System Password is required to be set on the device before a Secure Erase Mode operation can be set. If a File System Password exists on the device and if it is not captured in HP Web Jetadmin's credential store, the user will be prompted for the password when attempting to set the Secure Erase Mode. Device File System Passwords can be configured on the devices from HP Web Jetadmin. When these are configured, they are also placed into the credential store. Global file system credentials can be added to HP Web Jetadmin through **Tools > Options > Shared > Credentials > Device > File System (File System Password).** These are used when no password exists in the store and one is required by the device.

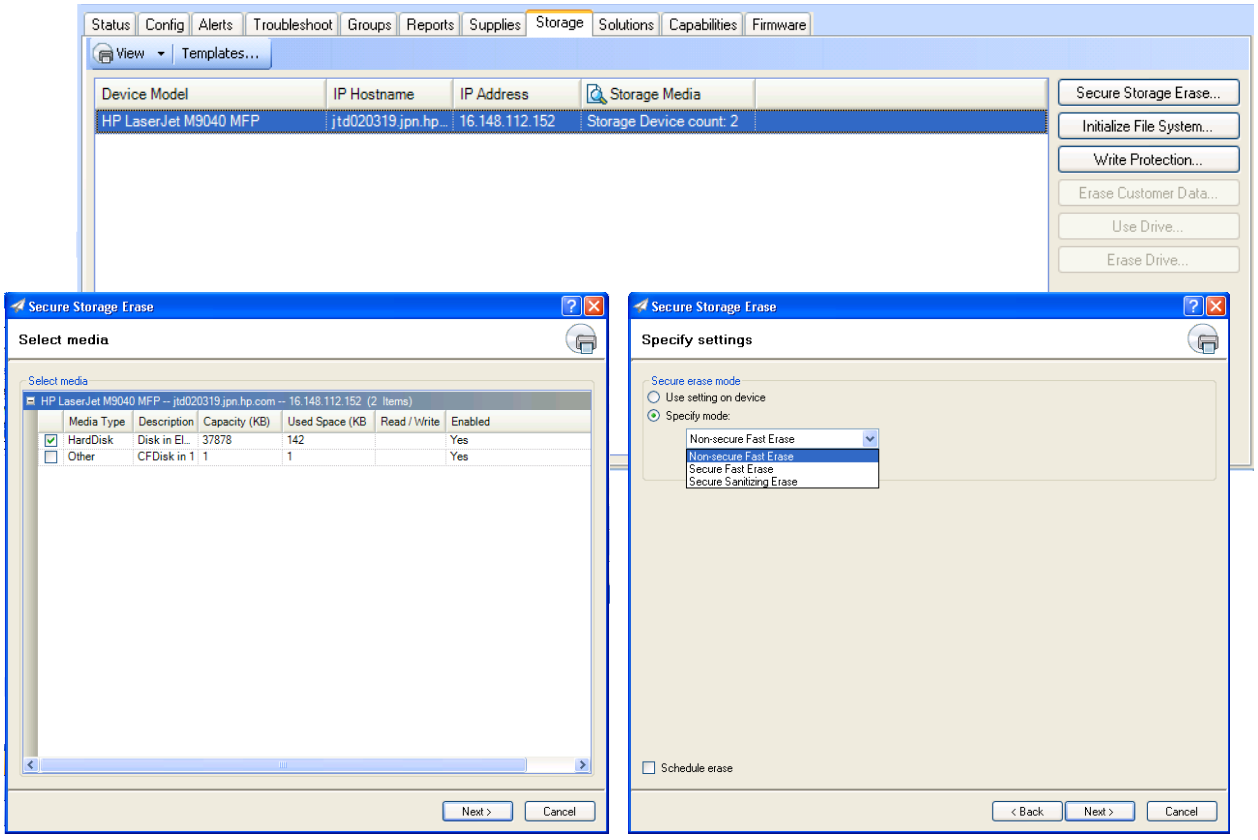

Figure 4 – Secure Storage Erase options

Erase Customer Data

Secure Storage Erase has traditionally referred to an erase operation that performed one of three erase behaviors over the entirety of a physical disk. Newer devices offer a different type of secure erase method, Erase Customer Data. Instead of erasing physical storage devices, the Erase Customer Data operation acts on the logical notion of customer data. The user cannot select a physical disk and request an erase. Instead, the user instructs the device to erase customer data with a Secure Fast Erase or Secure Sanitizing Erase mode (see Figure 5).

Erase Customer Data will erase and overwrite all job data files stored on the disk including:

- Temporary data for print jobs
- Temporary data for copy, fax, e-mail, and send to network folder jobs
- Stored Jobs, Stored Fax jobs

The File Erase Modes available are:

- **Non secure**
- **Secure Fast Erase**
- **Secure Sanitizing Erase**

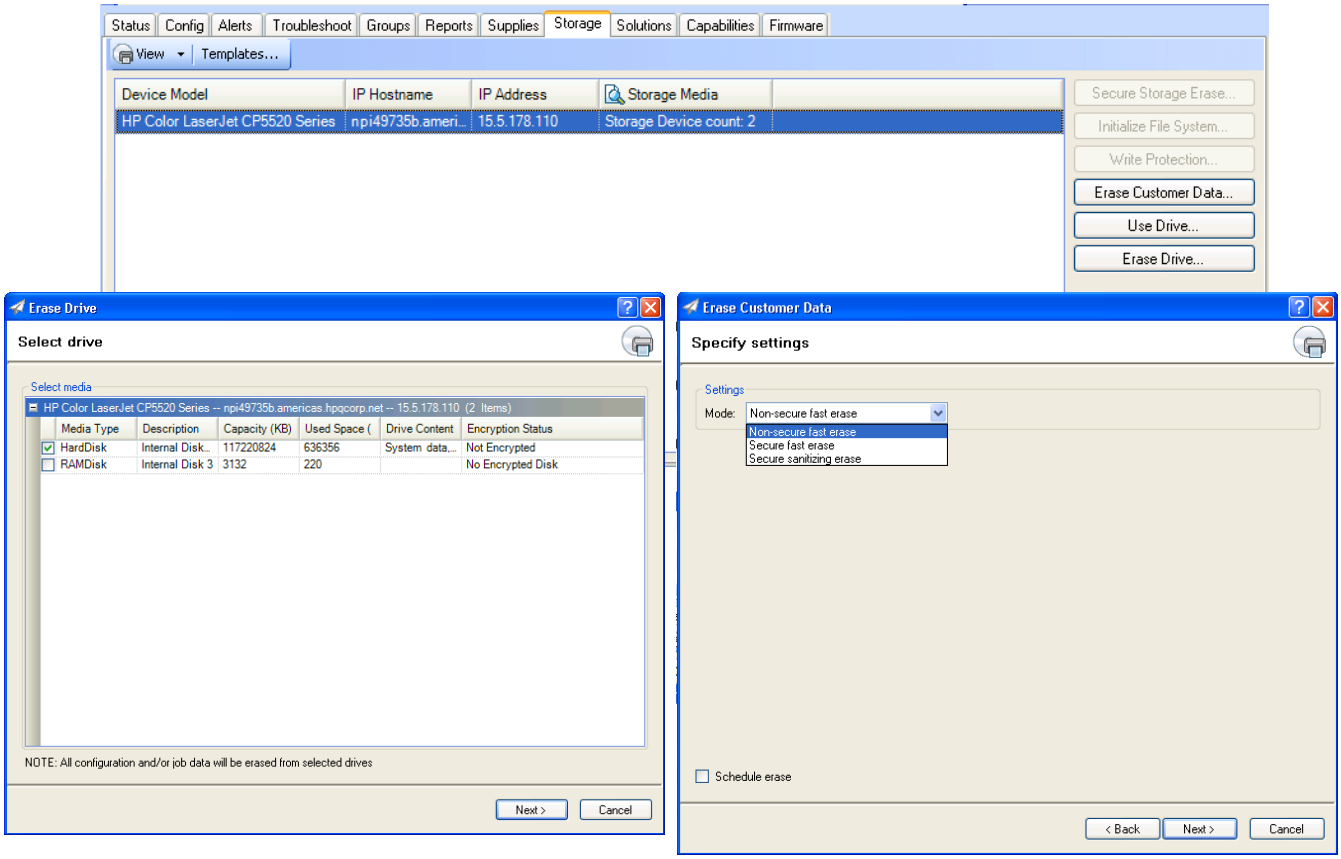

Figure 5 – Erase Customer Data Options

A File System Password is no longer required for the Erase Customer Data operation. Also, the File Erase Mode set under **Configuration** is only used for secure file erase of everyday temporary files. For storage erase, an erase mode is passed as a parameter to the erase method. Instead of the user-selected storage devices, the storage erase method will always erase all "customer data." To invoke the service, a client with correct web credentials makes a call to Erase Customer Data passing a valid erase mode. Internally, NVRAM flags are set and the device is rebooted.

Erase Drive

The HP High Performance Secure Hard Disk supports a special erase referred to as a “Crypto Erase”. The UI Storage tab contains a new **Erase Disk** button to be enabled for devices with the HP High Performance Secure Hard Disk. The new button launches a new wizard giving the user the option to select a disk from the list to erase. The button is only visible when a device that supports these new features is selected.

Selecting the erase option for one of these disks forces its encryption keys to be destroyed and new keys generated. This instantly renders all the encrypted data on the disk unreadable. There is no method to recover the encryption keys and no method to recover the encrypted data once the keys have been changed.

This erase mode is only accessible from the boot menus for the main system disk. It is available for accessory disks in EWS and HP Web Jetadmin. If the erased disk contained the system firmware, performing an erase will render the device inoperable. A new firmware image must be installed to the disk before the device can be used again.

The **Secure Erase Mode** selection by the user is simply a desired choice. The device will make a best effort attempt to perform the erase mode selected. If the selected option is not supported by the drive, the device will perform the closest match to the user's selection.

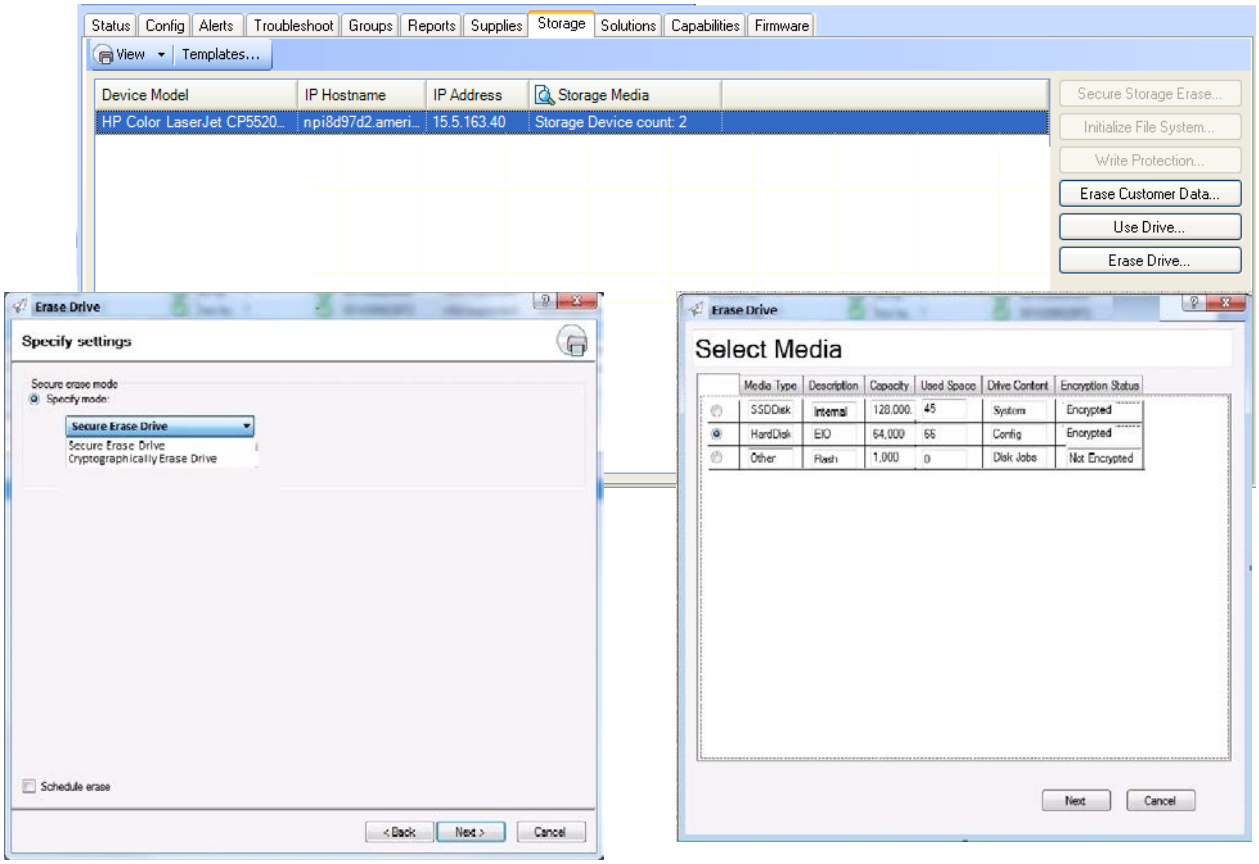

Figure 6 – Erase Drive

Initialize File System

The Initialize File System command acts directly on the disk partitions to provide troubleshooting and diagnostic tools. The manipulation of disk partitions is similar to formatting a hard disk and does not provide sector level overwrites of the disk space previously assigned to the removed partitions. These erase commands are not recommended for securely removing customer data.

When a disk initialization is performed on a device, Web Jetadmin sends an SNMP SET Request command on the file-system2-initialize-volume object. This object is defined I the MIB as such:

> Setting this object to eInitializing causes file system 2 to be initialized. The hrDeviceIndex value for the mass storage device is the same value that is used to index into the FILE-SYSTEM sub-tree. If the product supports up to 3 physical mass storage devices, the hrDeviceIndex for the mass storage devices will start at 2 if the mass storage device is installed, the FILE-SYSTEM2-INITIALIZE-VOLUME object will be the object that allows the mass storage device to be initialized that is the 1st device.

There are different techniques for initializing the file system including PJL commands such as FSINIT, but Web Jetadmin chose to use the SNMP object. This technique can be handy for erasing fonts, forms and stored print jobs where a secure erase is not necessarily needed.

FONTS AND MACROS

Selecting **Fonts and Macros** from the **View** drop-down menu displays a **Fonts and Macros** column with the number of fonts and macros installed on the device (see Figure 7). The mouse-over tool tip displays a table of all the fonts and macros installed on the device.

Highlight a printer and the following actions can be performed on the device by clicking their respective boxes on the right hand side of the screen:

- **Install**: Installs a font or macro on the selected device
- **Remove**: Removes the selected fonts and macros from the device, but does not remove them from the Storage Repository
- **Print Font/Macro**: Prints the selected fonts and macros on the selected device

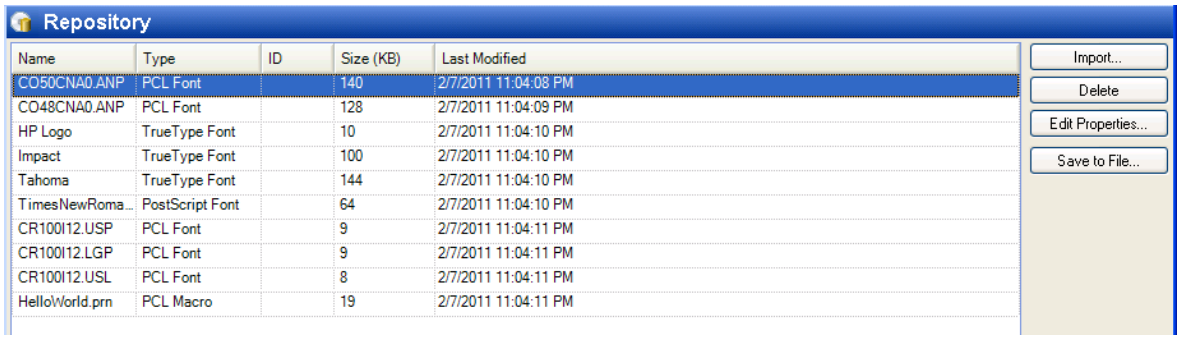

Figure 8 – Storage Repository

Before fonts and macros can be installed on devices, they must be imported into the storage repository (see Figure 8). Upon import, the files are converted into fonts or macros that the printer will understand and accept. This step calls into the FontConversion.dll and ImageMagick.dll files that were inherited from Web Jetadmin 8.1. They can ensure that page commands are stripped out and macro definition files are added. A pclResourceFile for each font/macro is also generated that acts as an index to inform the printer of which fonts and macros exist on the disk. The output from the .dll files is stored in a temp folder on the client.

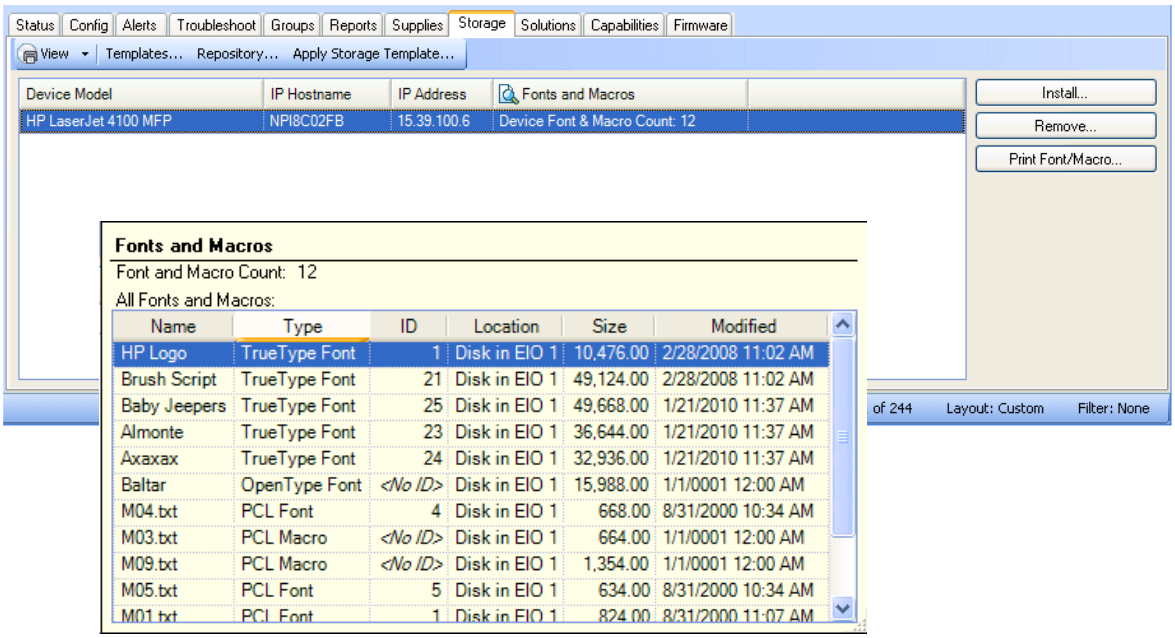

Figure 7 – Fonts and Macros

Fonts must be recognized as well known font types or they will fail to be imported into the repository. File extensions are irrelevant. The header of the font file is parsed for valid font definitions. The examples below are known file types that can be imported but the extensions are not restricted to these:

Fonts:
PostScript Type 1 - *.sfp
Binary - *.pfb
Open Type Font - *.otf
TrueType Font - *.ttf
PCL Font - *.anp

PCL Bitmap Fonts - *.LGP, *.USL, *.USP, *.R8L, *.R8P, *.L7L, *.L7P

Macros:
PostScript Macro - *.pfa, *.prn *.txt
Bitmap Image - *.bmp

Collections: - TrueType Collection file, *.ttc, contains a collection of TrueType Fonts in one packaged file. This file will be broken into its individual font files before it is sent to the FontConversion.dll for processing as FontConversion.dll cannot process collections on its own. If, during the file conversion process, there is no output from the .dlls, then the file was not recognized as a known type.

Once files have been imported, HP Web Jetadmin offers a user modifiable ID column that provides a Font ID upon which the font can be called. If a Resource ID is present inside an uploaded file, the ID will be preserved.

Files can be saved to file meaning a PJL file will be created on the pc that can be manually copied to a device later through any preferred print connection.

Install

Selecting the **Install** box will start the wizard that installs files from the repository onto the selected devices. Files and IDs provided by user will overwrite those on device. If the ID column is left blank, a new ID will be generated for the given font on the device during installation unless the device already contains the font and it has an ID.

A destination can be selected for the various media types. **Largest Free Space** is the default. Single device view will filter out media types not present, multi-device view will display all media types present or not.

An opportunity to provide validation for user to push fonts/macros and overwrite conflicting files/IDs on the device will be presented during the install. For files downloaded with no ID given, an ID is generated for it in the pclResourceFile.

PJL over port 9100 is the preferred mechanism for installing fonts and macros on devices. If PJL is disabled on the device, NFS will be used.

Storage templates can be created to download fonts/macros or delete fonts/macros. Templates can be selected when saving to file.

RESIDENT FONTS

Resident Fonts displays the number of fonts that came with the device out of the box. The mouse-over tool tip displays a table of all resident fonts on the device.

Resident fonts on USB drives that were installed by PJL scripts show up as **DIMM in Slot 4** for location. If multiple USB drives contain resident fonts, they will all be reported under the **Resident Fonts** view and the location will be reported as **DIMM in Slot 4** for all. This is due to how the printer reports these fonts. If multiple USB drives contain the same resident fonts and IDs, they will appear in the **Resident Fonts** view as repeats. The printer is reporting all the Resident Fonts on each USB drive with the same location.

The USB media drive will actually contain an "entities" directory in which resident fonts will exist as xxx.bin files where "xxx" is the name of the font. It is also possible to install non-resident fonts with WJA on a USB drive that already contains resident fonts if it shows up as a separate drive in the Media column. The fonts/macros installed will be placed in their respective directories on the USB drive (eg. /fonts, /pcl/macros, /Postscript) just as they would be on a hard disk and will show up in the Fonts And Macros view. Therefore, a USB drive may contain both resident fonts and installed fonts where resident fonts will be reported under the Resident Fonts view and installed fonts will be reported under the Fonts And Macros view.

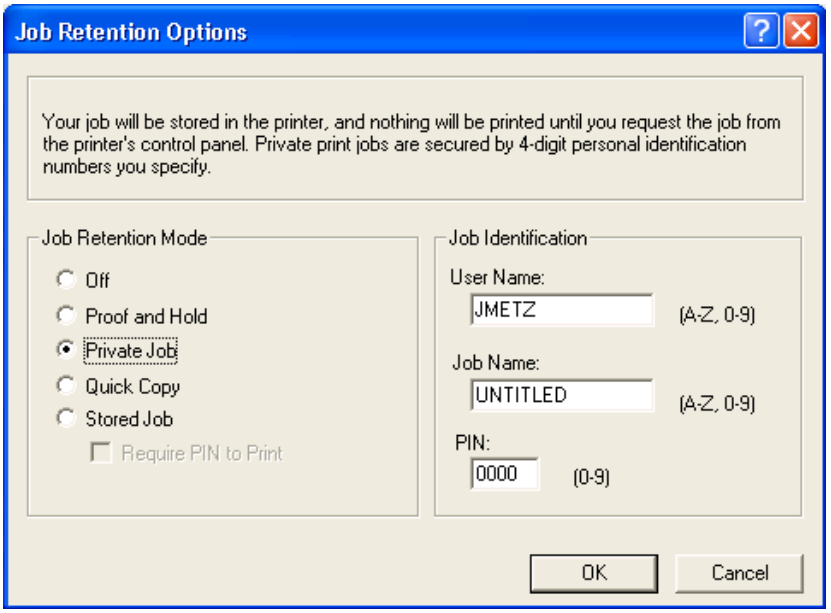

Figure 9 – Job Retention Options

DISK JOBS

Disk Jobs displays the number of stored jobs written to the device through the job retention feature of the printer driver. The mouse-over tool tip displays a table of the jobs on the device. The following options are available in this view:

- **Print Disk Job**: Prints the selected disk job. If the disk job is secured by a PIN, the correct PIN must be entered in order to print the job. If more than one PIN-protected job is selected to print and the jobs have different PIN values, only one can be printed as only one PIN can be entered.
- **Delete**: Deletes the selected disk job. PIN protected disk jobs can be deleted without a PIN being entered.

Viewing available disk jobs is an SNMP function and thus dependent on any SNMP credentials. Deleting disk jobs is a PJL function. Printing disk jobs is also a PJL function. PIN protected disk jobs cannot be deleted without a PIN while PIN protected disk jobs can be deleted without knowledge of the PIN. If multiple disk jobs are selected for printing the supplied PIN will be applied to all selected.

SUMMARY

HP Web Jetadmin provides numerous options for managing storage in HP devices. Secure storage erase options can be performed for properly decommissioning devices in secure environments. Fonts, forms and desk jobs can be manipulated to ensure devices have the proper files necessary for printing.

© Copyright 2015 HP Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.