License Server
Process Automation and Imaging

Version 11 User Guide

Extreme Protocol Solutions

www.enterprisedataerasure.com

Contents

Figures

General Information

i. Icons And Buttons Used Throughout License Server

The icons in the following tables can be found throughout **License Server**.

License Server Features (Main Window)						
Feature Icons		Feature's Activity Icons				
	Licensing	 Licensing	 DHCP	 Remote Control	 XView IP Monitoring	
	PXE Profiles	 Profiles	 System Condition	 Device Grading	 User Fields	 Database Scripts
	BurnIn Test					
	Imaging	 Imaging Models	 Post Imaging			
	Device Drivers					
	Database Services					
	Reporting	 Report Templates	 Label Templates	 QR Templates	 Previous Reports	 Create Reports

Table 1 The Icons For The Features In License Server

Action Buttons			
Common		XErase	
	Save/Update		Login User
	Save As		Display / View Sectors
	Add Element		Start Erasure
	Remove Element		Stop Erasure
	Build Report(s)		
	Settings (License Server) Erasure Methods (XErase)	License Server	
	Refresh Information (LC) Rescan Devices (XErase)		Set Profile as The Default
	Configure Setting (LC) Edit User Fields (XErase)		Scale View Up (+) or Down (-)

Table 2 Action Icons / Buttons Found Throughout License Server

ii. Conventions

These conventions are used throughout this guide to enhance its readability.

"double quotes" = used as minimally as possible to improve readability and used to clarify usage where required or to denote specific/literal/special meaning. May also appear in bold font.

Normal bold font = **ABC Company names, names of sections and licensed products, fields in License Server and its features and options.**

Normal bold underlined = **titles of documents/other guides**, **new sections** or **steps to follow**

Bold italicised font = typed input/responses, mouse clicks, key presses.

***Bold Italicized and Underlined font** = **important, take close/special note**.*

Normal Blue Underlined = Links to URLs and different places within this document or to other documents related to erasures (c:\XERASwin\PDF)

ADWBDITG = **A**cronyms **W**ill **B**e **D**efined **I**n **T**he **G**lossary at the end of this document. The acronym will appear in bold underlined blue font representing a link to the acronym in the glossary for the first occurrence only (e.g., click ADWBDITG which is the main header for the Glossary Of Acronyms).

iii. Introduction

Welcome to **License Server** by **Extreme Protocol Solutions**, the highly customizable solution designed simplify the ITAD/ITAM process. This solution eliminates the need for several steps, as well as stations, in your current processes by consolidating data erasure, component testing, system re-imaging and reporting into a single customizable automated process. It also supports whatever sanitization standard you or your customer may require whether it be DoD, NAVSO, NIST (etc.) and can be easily adapted to accommodate any future standard for data erasure or disk sanitization.

Component testing is provided through **PassMark's BurnInTest™** which has been completely integrated and automated. If re-imaging systems is part of your refurbishment process, the customization and automation aspects of the Imaging feature will prove to be a step up from current methods. Additionally, features such as dynamic driver and program injection will also significantly increase the efficiency of the refurbishment process.

There is no other software product on the market today with the capabilities and controls that are found in **EPS License Server**.

Figure 1 License Server's Main Window

> **Note**: There is a wide variety of devices that can be processed by **License Server**. This document was written using a HP Elite Book laptop.

Refer to the table of main icons for a cross reference of each feature and its customization/activity bar.

Features At A Glance

Erasure

License Server features all the power and functionality of our industry leading erasure software, **XErase Enterprise Data Erasure**, in an integrated platform.

Component Testing

Under license from **Passmark, EPS** has integrated the industry leading capabilities of their **BurnInTest™** (**BIT**) software into **License Server**. This feature enables the testing of most of the major components built into devices such as laptops (i.e., processor, memory, keyboard, etc.) according to accepted industry and refurbisher standards.

Imaging

EPS has developed a superior methodology for implementing the principals of the Microsoft Refurbisher program. What was a two or three step process has been automated to become a single network based process that saves time and reduces cost as well as manpower needs.

Device Drivers

This feature is part of the **Imaging** process. Once configured, it includes all the drivers provided by Microsoft as part of their Refurbisher Program. The feature must be configured prior to attempting to install an image onto a device after it has been processed.

Database Services

Included with **XErase** is the ability to interface to a standalone database or to various **ERP** databases with information related to assets and the results of their erasure and/or testing. Additional licensing as well as predefined credentials and privileges on the respective ERP environment may be required.

Reporting

In addition to viewing reports that were previously generated, new reports can also be generated for completed erasures in various formats (i.e., **PDF**, **HTML**, **CSV**, etc.). Sample report templates are provided from which customized reports can be created according to your requirements.

Remote Control And XView IP Monitoring Tool

XView provides a consolidated view of all the successfully booted clients. The minimized view will show the status (i.e., running erasures, BIT, etc.) of a client. Accessing a client in this view is a simple double click away. It is a convenient way to manage multiple clients without having to physically touch the client.

Preparation

Licensing

The following table contains a list of all the available licenses (as of this document) for the features within **License Server**. Ensure that an active license is available for the desired features.

Feature	License		Type	Use
	Name	Number (min.)		
License Server	XELTWin	1	Required	PXE Server
XErase Light				XErase on the client
Burn In Test	XEBITwin	1	Optional	Testing internal components
Reimaging	XEIMGwin	1	Optional	Reimaging the client with its operating system
Verification	3RDVFYwin	1	Optional	3rd Party Verification

Table 3 Cross Reference Of Licenses To Features

Refer licensing questions to sales@extremeprotocol.com.

Windows Requirements

Ensure the correct version of Windows is installed for the workload (i.e., the number of clients that will be connected concurrently) to be handled by the system that will be running **License Server**.

- Systems running Windows 10 can handle a maximum of up to 20 clients.
- Windows Server has no **PXE** limitations and can boot up to 250 IP addresses (clients) per port. Many systems designed to act as a server have multiple ethernet ports which can be used to expand the PXE network's capability. Contact your local IT team(s) for further details.

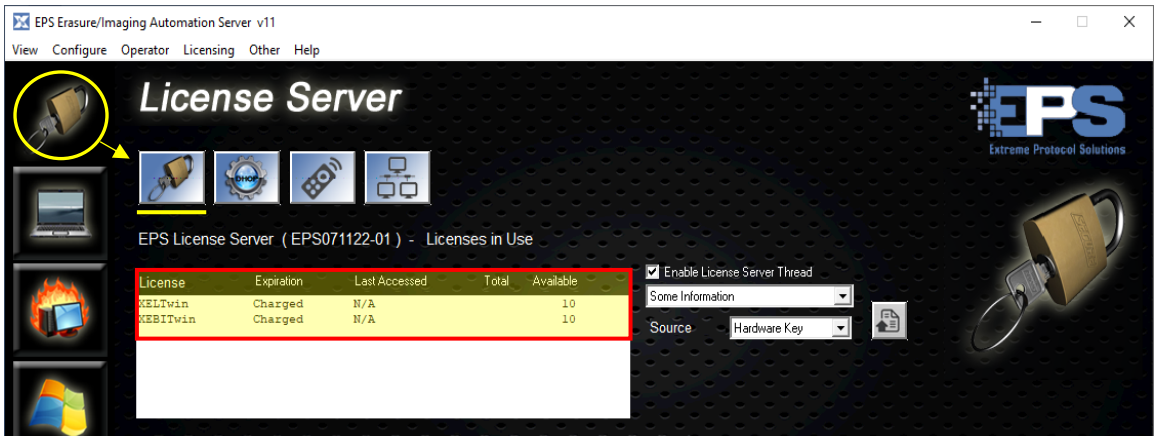


Figure 2 Displaying The Licensing Information

Network Requirements

Access the interface to be used for the PXE network using **Control Panel** and confirm its properties are set as described in the following table. It is also highly recommended that the configuration include an unmanaged switch in the initial topology.

Settings Location (->Tab)	Attribute	Setting
Properties	QoS	Disable
	IPv6	Disable
Configure -> Power Management	Allow the computer to turn off this device to save power	Disable
Configure -> Advanced	Interrupt Moderation (if present)	Disable
	Priority & QoS	Disable
Network -> Firewall	All network related	Turn off/disable
TCPv4	Properties: - Obtain an IP address automatically - Obtain DNS server address automatically	 Select/enable Optional/select

Table 4 Recommended Network Attributes For The PXE Ethernet Interface

The default network addresses that will be assigned to/by DHCP are:

Network: **10.100.1.1**
Server (License Server): **10.100.1.2**
First Client: **10.100.1.10**
Range For All Possible Clients: **10.100.1.10 – 10.100.1.254**

Contact your local IT team for technical assistance as/if necessary.

Note: Many systems will have an ethernet IPMI port. Do not use this dedicated single purpose port. It is not designed to be used for normal TCPIP traffic.

Licensing - General Configuration And Management Tools

It is assumed that **License Server** is already installed. If the software is not installed, complete the steps in Appendix A – Installing License Server then return here and continue with setting up DHCP**.**

DHCP

License Server requires a reliable ethernet network to communicate with remote clients connected to the same network segment. Once a client is recognized on the PXE network, DHCP will assign it a unique address. Systems that are currently shipped by **EPS** should already have DHCP configured for the (physical) ethernet port labeled, **PXE,** above it. Connect one end of a working ethernet cable into that port on the system and the other end into a port (by convention for unmanaged switches, the first port) on the switch, then click  .

Otherwise, or if the status is not as displayed below, follow the steps in for reconfiguring DHCP.

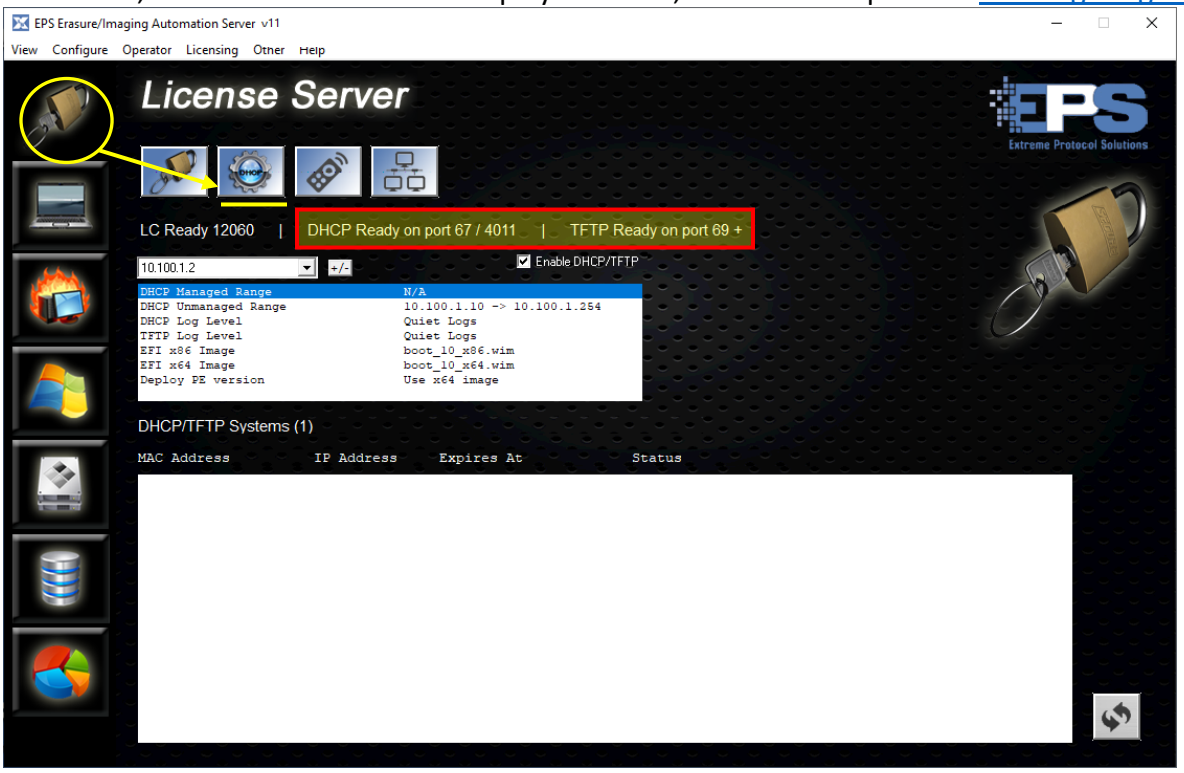


Figure 3 General Configuration - DHCP

To reduce the risk of losing the configuration (and having to reconfigure it), do not use this port for anything other than operations related to **License Server**. While the configuration supplied with the system can be changed, doing so will require a degree of networking skill and understanding of how DHCP works. Consult with your local networking team if further assistance is required.

Once configured, any (connected) clients that are being booted will be displayed in the lower information portion of the DHCP window during its PXE boot process.

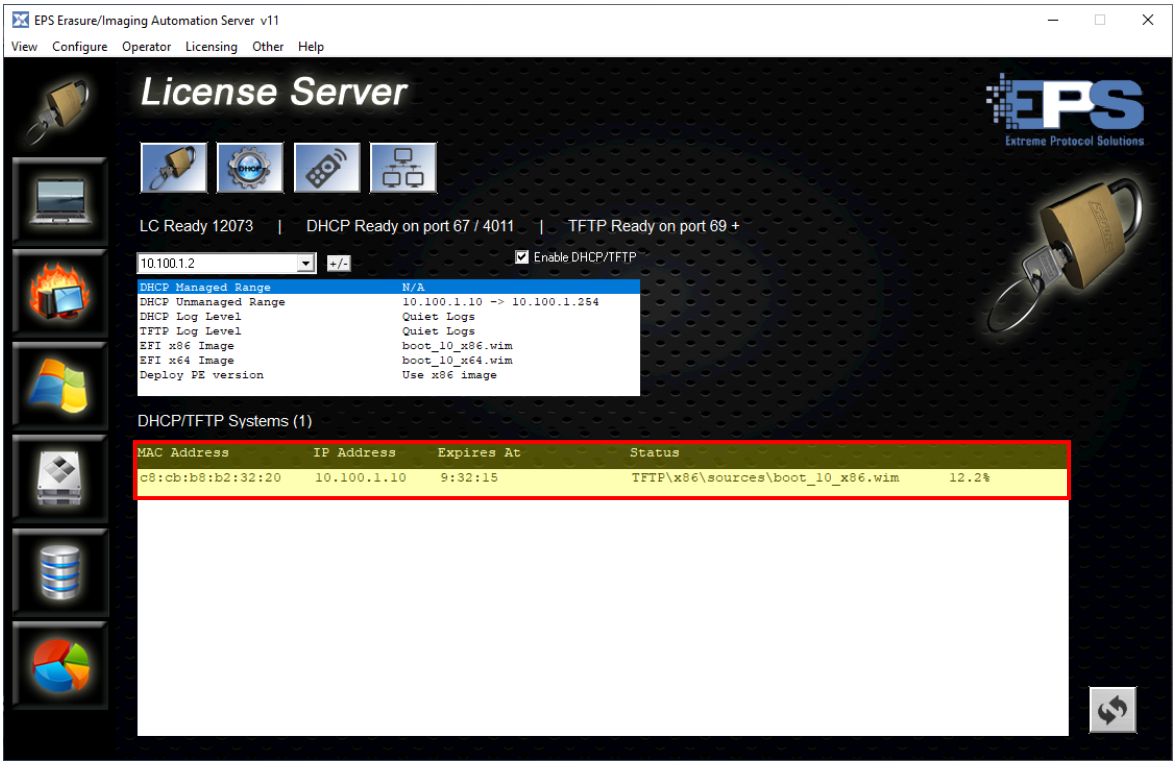


Figure 4 General Configuration - Displaying Network Connected Clients

> **Note**: Each client has its own method of starting PXE boot. On many laptops, pressing the F12 key while it is powering on will invoke PXE boot.

If a new configuration is desired, refer to the **Reconfigure DHCP** portion of **Appendix A**.

Remote Control

Remote Control ( ) is a convenient way of managing a client over the network just like it was physically present and is especially useful as the number of clients increases. The client's network information will be displayed in the DHCP window (Figure 4) as it boots and, after it reaches a certain point in the boot process, it can be accessed with **Remote Control**.

Unless a profile that automates further actions is in use (see XErase PXE Profiles), once the client finishes booting, the **XErase** window will appear. At this point, the client, along with **XErase**, can be managed using the controls available on the respective window.

Sessions that are opened too soon will result in only the bootloader being displayed.

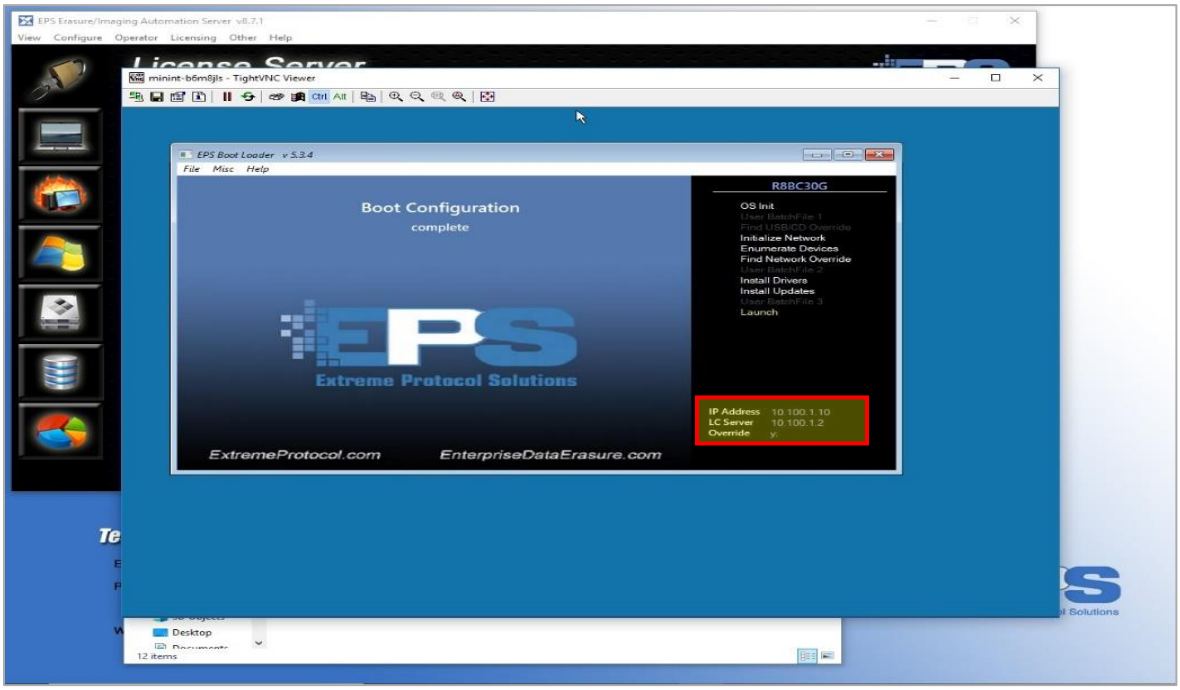


Figure 5 Remote Control - Viewing The Client's Boot Screen

Just allow the bootloader to finish at which time the activity configured in your profile will be started. The profile used below was configured to just launche **XErase** with the drives selected. Once you are more comfortable with **License Server**, you can either modify one of the included profiles or create a totally custom profile specific to your organization's requirements.

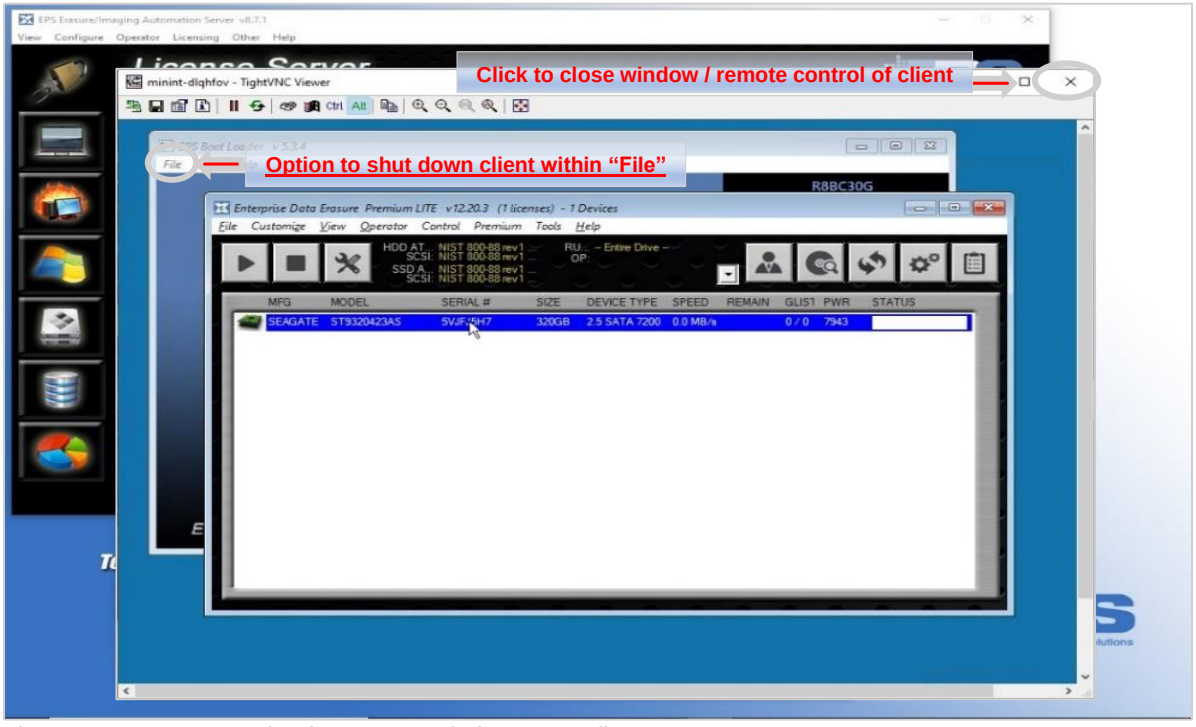


Figure 6 Remote Control - The XErase Window On A Client

XView IP Monitoring Tool

The **XView IP Monitoring Tool** ( ) is a convenient way of obtaining a "single pane of glass" to the potentially hundreds of clients that could be connected to **License Server**. It can be opened at any time after a client has been powered on and is connected on the network to monitor the progress of a client while it is booting. It is also another way to access Remote Control of the client.

A new layout must be created during the initial launch of **XView**.

1. In the **XView** window, click the under **Interface Configuration Files**, provide a (file) name when prompted and save it. The name will appear in the field as soon as it is saved.
2. Update the **System Group** with the geometry desired, the label (name) that will represent this grouping in the window, along with the addresses for the server and the address of the first address (**StartIP**) to assign to the first client in this group.

> **Note**: If this is the first group, use the defaults unless there is reason to do otherwise (i.e., multiple PXE networks).

3. Add the new group into the window/view with .
4. Adjust the view as desired with the + – located under **Scale Group** until the new group is visible in the desired size.

   If additional groupings (i.e., networks) are needed, ensure DHCP has been configured to recognize the network/client addresses, then repeat the process and supply a new name for the configuration file as well as the label for the **System Group**.

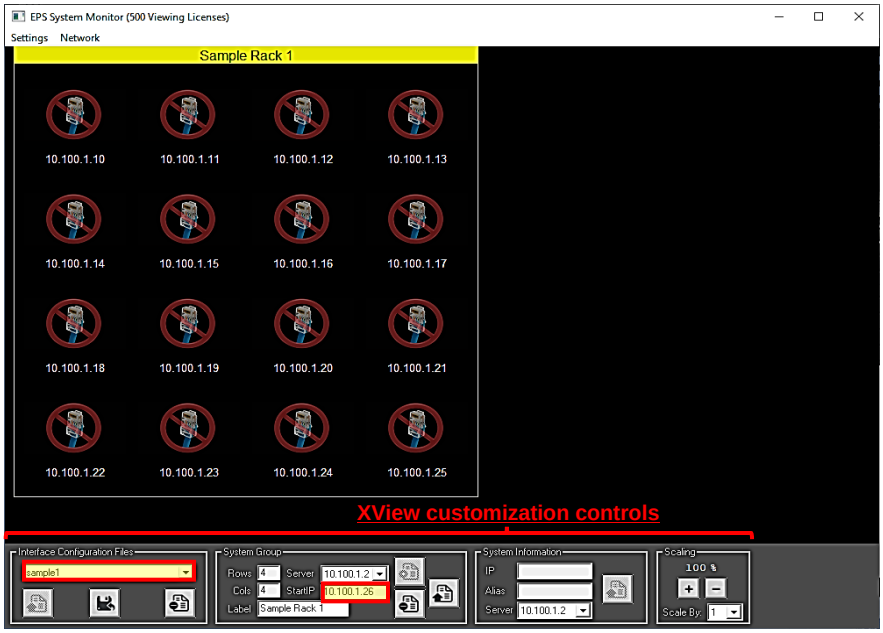


Figure 7 XView IP Monitoring – Adding A New Group

From this point on, any clients that are included in the defined range of addresses will appear displaying the progress of their PXE boot process –  when started,  as the boot process continues,  as Windows (WIM) is loading and configured, then lastly, a miniature view of the client once the configured profile is activated. Access the client (**Remote Control**) by double clicking the client.

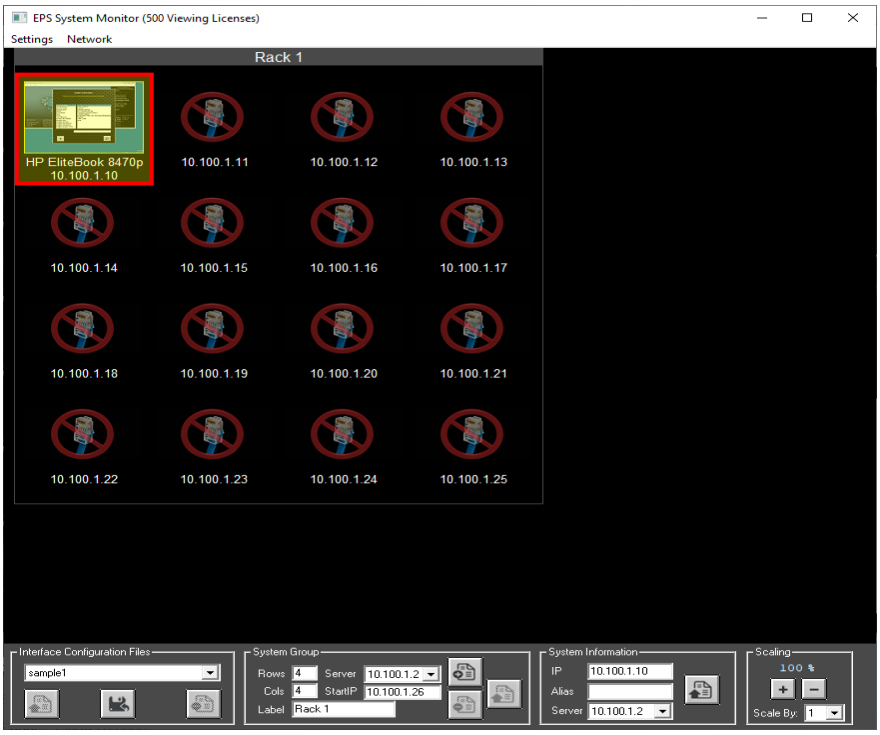


Figure 8 XView Minimized Display Of A Booted Client

Configuring PXE And XErase

Each of the remaining features can be used independently or configured to automate the complete stream of activity related to processing a device.

The features have been organized in the main window to, as much as possible, mirror that work flow and documented in the same manner. If used independently, a specific profile for the specific feature must (still) be configured.

The default profile used after a client is booted will launch whatever activity it was configured for. At minimum it should at least launch **XErase**. While all the default settings (i.e., erasure methods, rules, logs, etc.) can be used, you will likely want to customize a profile to perform certain actions, for example, selecting drives and starting an erasure once the client is booted and **XErase** is started. A profile can be customized to the degree of automation desired – minimal, which requires manual intervention, to fully automated requiring little-to-no intervention.

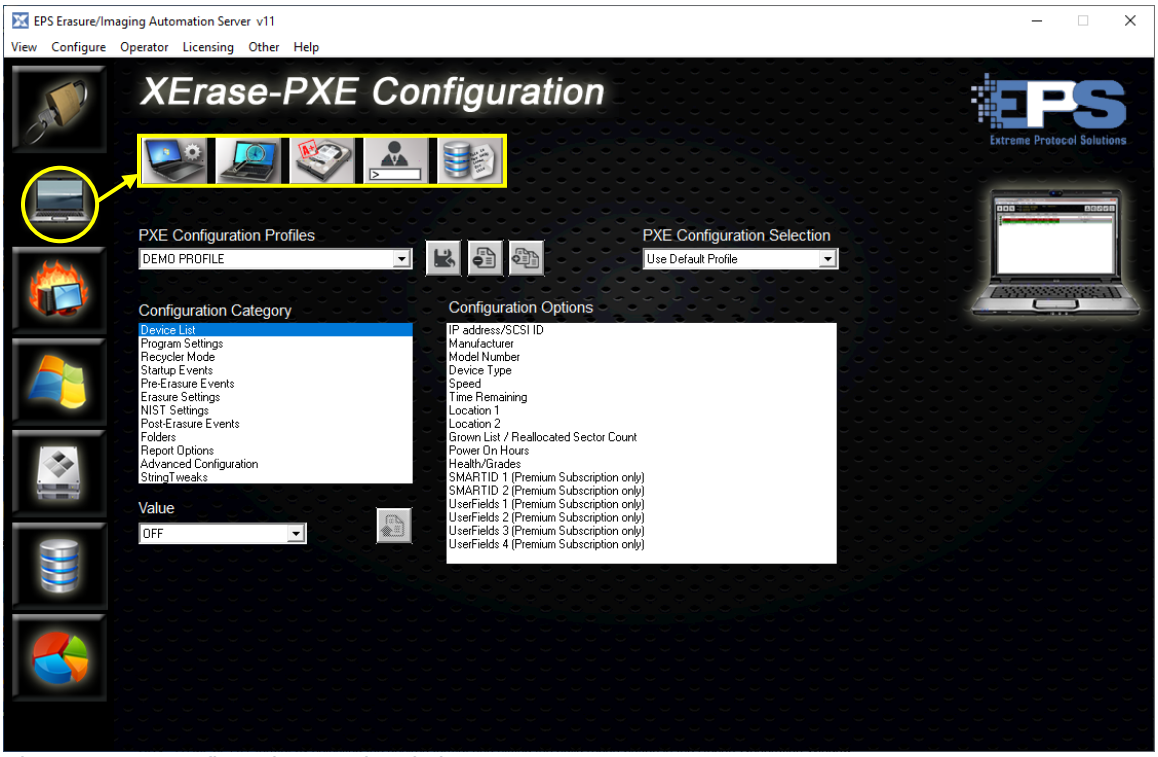


Figure 9 PXE Configuration – Main Window

Create / Edit PXE Configuration Profiles

The PXE profiles establish how the client will behave once the bootloader finishes. While any of the sample profiles can be used without further modification, if any changes are made to them, it is recommended they be saved using a different filename in case the default samples are needed as a ("baseline") reference. Modeling your specific requirements based on the included samples might be a good way to get started.

In summary, the profile is defining how **XErase** (and/or other features) behaves once the client is booted. It can be configured to be automated to the degree desired.

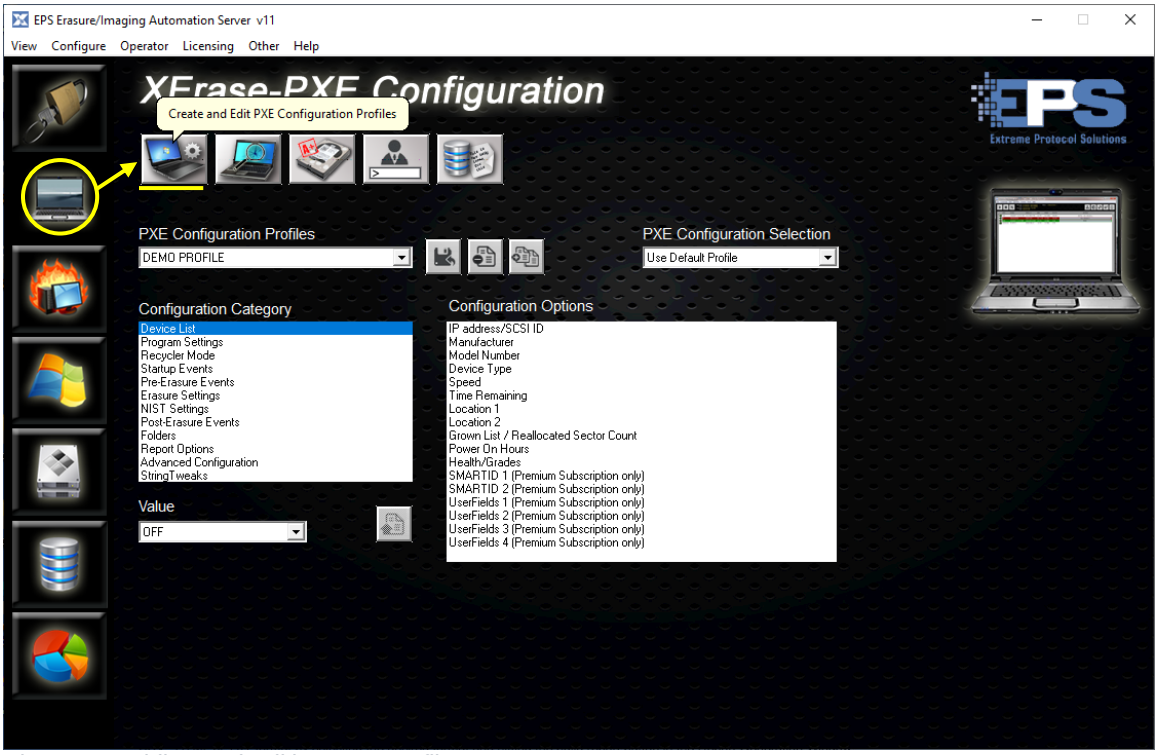


Figure 10 Adding And Editing PXE Profiles

The following steps will create a new profile called "documentation" based on the sample, **1X NIST Erase** profile. A few options will be changed to demonstrate the process. Modify the steps to include/exclude items as desired to fit your requirements.

> **Note:** The **License Server Quick Start Guide** uses the "DEMO PROFILE" (requires manual input/intervention after the client is booted) which can be used as a quick and easy way of getting introduced to the purpose of a PXE profile.

1. Click the dropdown arrow beneath ***PXE Configuration Profiles*** and select ***Sample 5. 1X NIST Erase***.

Figure 11 Selecting A Sample Profile

2. Click  , then provide a filename for the new profile and save it. If it doesn't appear under **PXE Configuration Profiles**, select it from the dropdown.

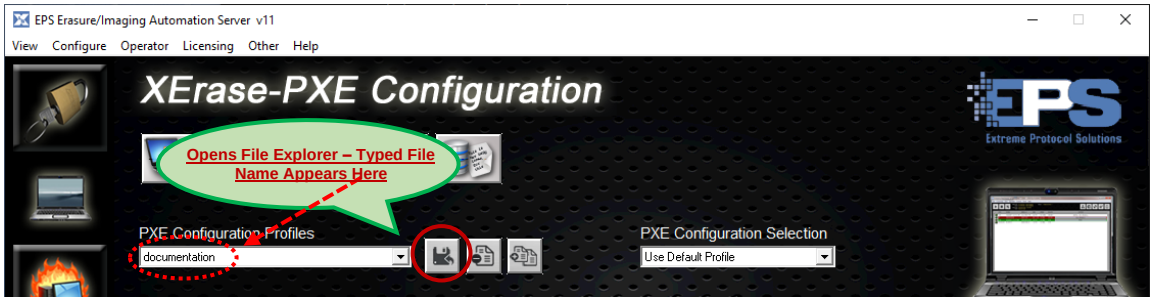


Figure 12 Creating A New PXE Profile Based On A Sample

3. Update the desired **Configuration Category** and its option(s). Remember to save the update with  ***each time*** a change is made that needs to be retained for each of the **Configuration Options**. This example will turn ***Recycler Mode*** from the default, **OFF** to ***Warn***.

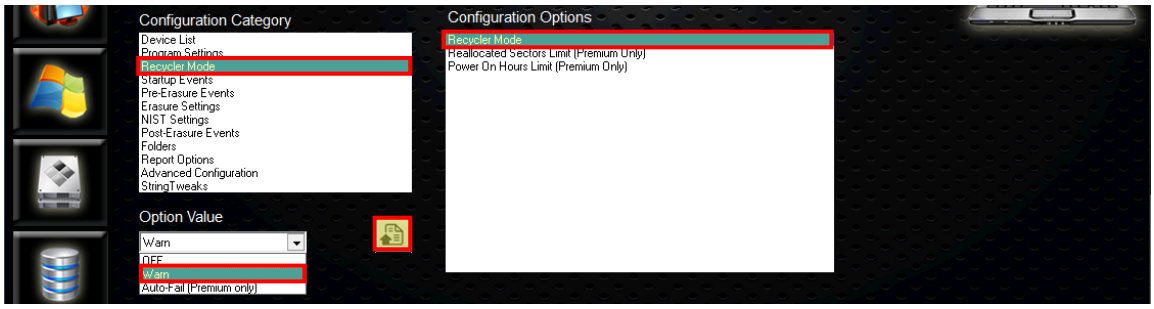


Figure 13 Setting An Option Using Recycler Mode

Review the other options and/or **Configuration Category** and their options and update them at this time. Remember, anything modified here will determine how **XErase** will behave and the way erasures will be run once they are started.

4. Confirm the desired profile is showing, and whether that will be the default when **XErase** starts with  .

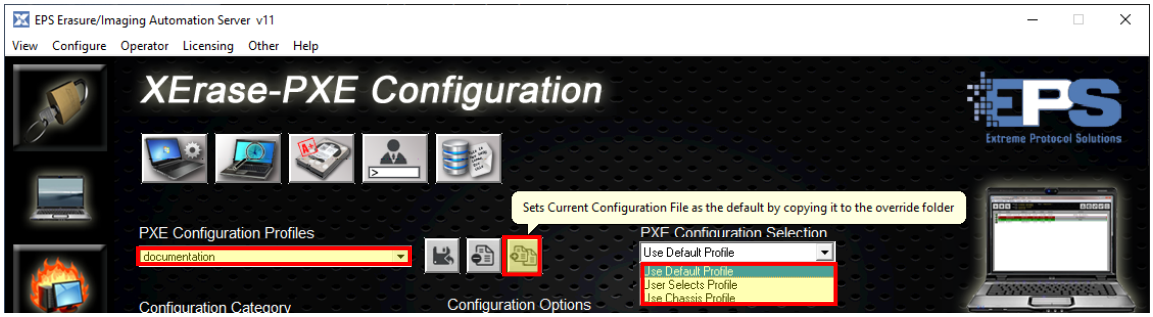


Figure 14 Setting The New Profile As The Default

PXE Configuration Selection	Action When Called (After The Client Is Booted)
Use Default Profile	Whatever is defined in the listed profile
User Selects Profile	Operator sees a menu of profiles to select from when the client is booted.
Chassis Profile	Predefined set of activities specific to the client (i.e., laptop, system, network switch)

Table 5 Summary Matrix Of Profiles To Configurable Actions

A general description of each of the items under the **Configuration Category** follows. Given the large number of options available for each category, they will not be discussed in detail here. Most are on/off toggles which can be set according to your requirements.

> **Note**: Support for NVMe storage is dependent on the system XErase is running on. Some systems and interfaces will mount NVMe drives as basic SCSI storage disks, some will use Microsoft StorNVMe which can erase disks with a low level utility in a desktop system but may not be able to in a the **License Server** PXE environment.

Device List – Sets which fields are displayed in the **XErase List Interface** view on the client after it has been booted up and **XErase** is started. Two optional labels have been added in the below figure to help illustrate the use of this list. The positions cannot be changed and there is limited space so take care that the name(s) do not "crowd" each other out and become unreadable.

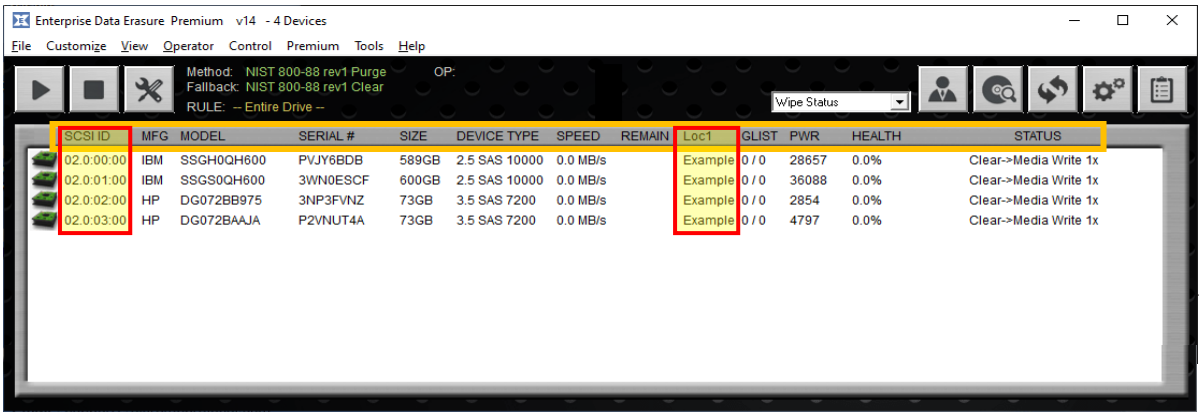


Figure 15 Configuration Category - Device List

Program Settings – Sets the options that control **XErase** when it is launched. A few of the more common options that can be set include loading previous logs (allows for resumption of an erasure), disabling **PUIS** for drives that came from devices such as set top boxes or game consoles (etc.) and may have been left in standby when they were last powered down, as well as setting the default interface to either **List** or **System Interface** view. This is also where the option to enable **EraseSURE Verify Mode** (separate licensing may be required) can be found. Once enabled, it can verify erasure methods for hundreds of devices (i.e., disks, laptop, desktops, servers, storage arrays, etc.) simultaneously.

Recycler Mode – Set these options to help reflect the accessibility and usability of a drive based on its condition. Setting the **Recycler Mode** to **Warn** will greatly improve the stability of the system when dealing with drives that may not be in good working order. Additionally, devices that exceed the specified thresholds or don't meet the configured grading standards will automatically display a warning or failure which helps to quickly determine whether to scrap a drive without attempting an erasure on it.

Startup Events – The options in this category are related to the actions that need to be performed when **XErase** is started. Items such as **Execution of System Condition Prompts**, **Keyboard Testing** and **BurnInTest** (etc.) can all be found here and enabled or disabled.

Pre-Erasure Events – As the name suggests, these options control what will be performed after **XErase** is started but prior to the start of the erasure. Enabling device grading and pre-validation of opcodes (i.e., confirms that the drive understands the commands that will be sent to it) are a couple of items that can be set with this category. This is also where the option to enable the execution of database parsing scripts (i.e., files containing commands to run) at the end of an erasure can be found.

Erasure Settings – Establishes what activities **XErase** performs when an erasure begins. This is where the **Primary** and **Fallback Erasure Methods** are set. The defaults are **NIST 800-88 rev1 Purge** and **NIST 800-88 rev1 Clear** respectively. While the defaults should work for most drives, if any are changed, consider performing a test erasure on a few devices to ensure the performance or the results of the erasure are not impacted.

> **Warning**: There is a potential for performance problems, as well as other unexpected/undesired results, if **Use Override storage for DiskErase** is modified. Only update the option when directed to do so by **EPS** support.

NIST Settings – These settings configure the NIST SP800-88 erasure methods for **Purge**, **Cryptographic Erasure** and **Clear**. Further details can be found in **c:\LCServer\PDF\Erasure Process.PDF** and **c:\LCServer\PDF\NIST.SP.800-88R1.PDF**. Use the **Open SECURE Filter window to Enable/Disable/Change Order** option to access to some of the new security features that are included in current drives.

Appendix D contains additional information related to the NIST standards and how XErase implements them.

Post Erasure Events – Controls activities that occur after the erasure has completed. Write stamping of block zero and imaging are examples of controls that can be run at that time. Health and grading can be done either before or after the erasure.

Folders – Sets the locations of where items such as logs and reports are stored as they are generated. This is also where the location for the **Override Folder**, which is related to overriding the USB boot settings at the time of booting the client(s), can be found.

As of this document, the  which is used to configure the folders for logs and reports is not active. To modify the path and add prompting, modify the existing path under **Folder Name**.

For example, to add two levels (folders) beneath the existing "**logs\<YEAR>"** folder asking for the customer name (**<PROMPT1>**) and job number (**<PROMPT2>**), update the field to include this:

logs\<PROMPT1:Customer><PROMPT2:Job Number>

Remember to click  to save the update.

Report Options – Controls the creation of custom device labels and entries for manifests upon completion or failure of an erasure. Included in these options is the ability to specify custom report names as well as controlling the setup of page and label printers specific to **XErase**. The Generate Report/Device Labels, System Labels option can be found here. Customize the respective templates (if/as needed) first, then enable the desired option and select the respective template. Once enabled, the respect output will be generated as each device completes its erasure/process. The respective printer must be configured in Windows first.

Advanced Configuration – Many of the items included here are specific engineering level features that **EPS** support may ask to have enabled when troubleshooting software issues. Items such as modifying how the software performs a bus probe for devices, ignoring GLIST values, data transfer sizes, and the inclusion of USB devices, are all part of these options. Others may also be enabled to improve the discovery of a device and how it performs during erasure.

String Tweaks - The options in this category are all on/off toggles that make minor modifications to the way certain information is displayed/stored/used. The modifications are internal to **XErase** and will appear in various places as required to help make the text/information that is displayed clearer and/or more visible (easier to read).

System Condition Files

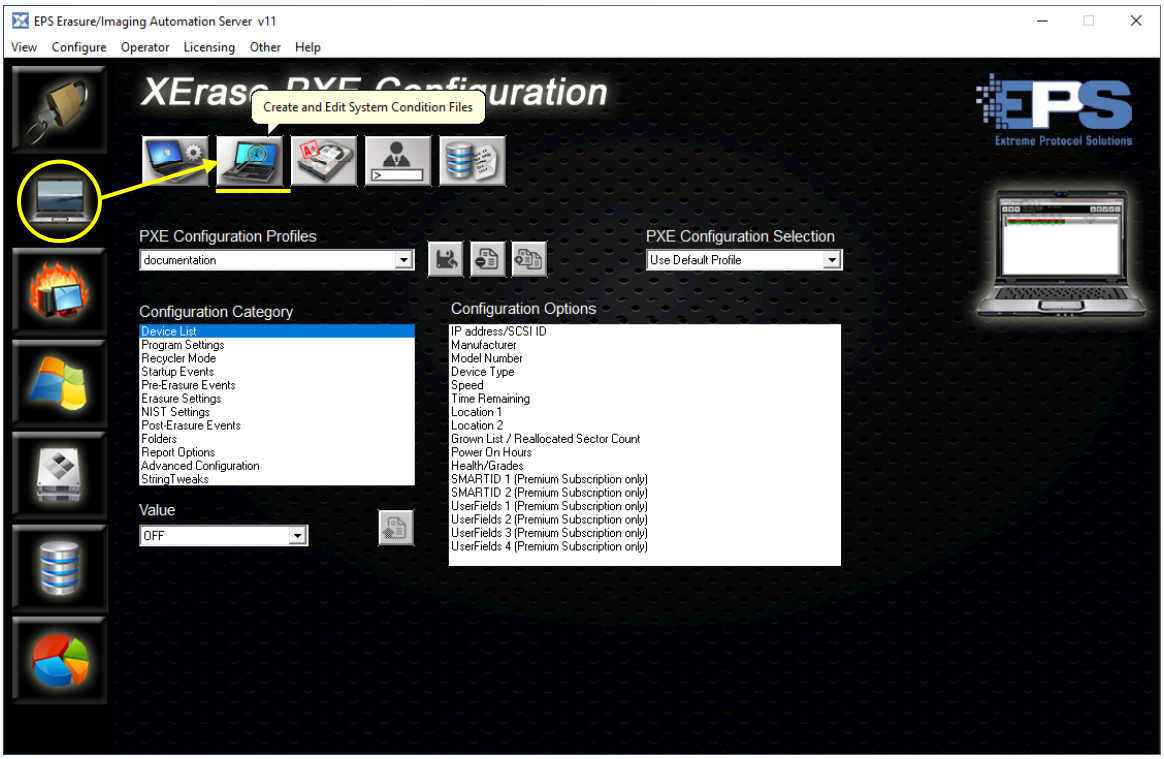


Figure 16 Accessing The System Condition Files

Auditing and documenting assets as they are being processed are key aspects of the revenue recovery cycle and an integral part of the ITAD and ITAM business. Using **System Condition Files** enhances this process and reduces the amount of manual intervention required by building condition statements to match the needs of your operation. Once they are customized, the operator is prompted to select specific condition information about the asset they are processing. All of the data is preformatted which greatly reduces the risks associated with discrepancies during entry (i.e., typos and duplicated entries, etc.) when the data is analyzed.

For the following steps, the file, **SystemCondition_SAMPLE**, included with **License Server**, will be used as the basis for the new condition file. As with **PXE Profiles**, the defaults can be used, at least until you become more familiar with what the **System Condition File** was designed to do.

Ensure **SystemCondition_SAMPLE** is displayed under **System Condition File** and all its categories and options are displayed. If the options field is blank, clicking anywhere in the **Configuration Category** field or reselecting the **SystemCondition_SAMPLE** should populate the respective fields.

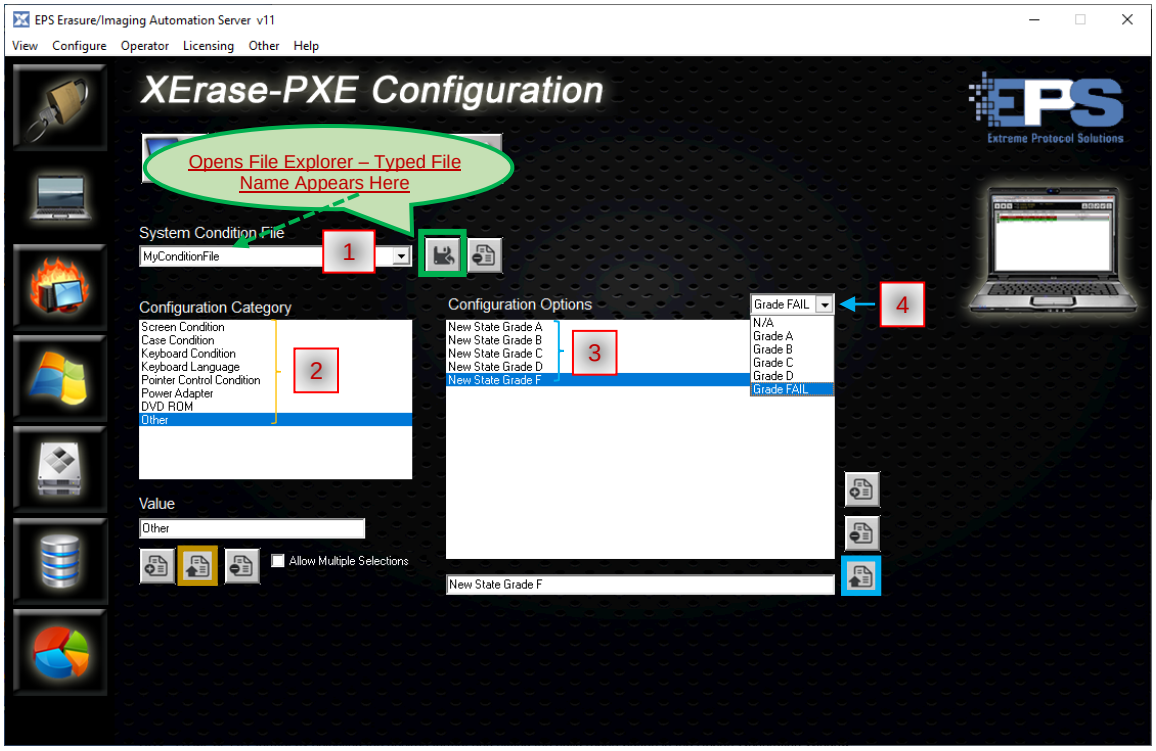


Figure 17 The Sequence Of Steps To Add A System Condition File

1. Click , provide a name for the configuration file, and save it. The new name should appear in the **System Condition File** field. Select it from the dropdown if it doesn't.
2. Select an item (component) in the field under **Configuration Category**.
3. For that component, select a **Configuration Option**.
4. In the dropdown immediately above and to the right, select the corresponding grade for the option. Remember to save ( ) after the updates have been made.

   Repeat for each option. Once done, selecting a specific option should now also display the assigned grade when the option is chosen (look in the upper right part of this section). Customize the options to meet your requirements (i.e., change grades, add/remove, etc.).

   Repeat steps **2 – 4** for each **Configuration Category**.

5. If there are **Configuration Categories** (components) that need to be added:
   a) Type the name of the new category in the space provided beneath **Value** then add the new option(s) with and save it with .
   b) Select the new category, then add **Configuration Options** by typing the desired option in the space beneath and add it with .
   c) Select the new option and assign a grade for it.
   Repeat steps **a** – **c** until all the desired categories and options have been added and grades (or **N/A**) are assigned. The grade assigned will appear in the drop down ("c" in the following figure) for each **Configuration Option** when it is selected.

d) Once all the options have been added and their grades are assigned, save the options with .

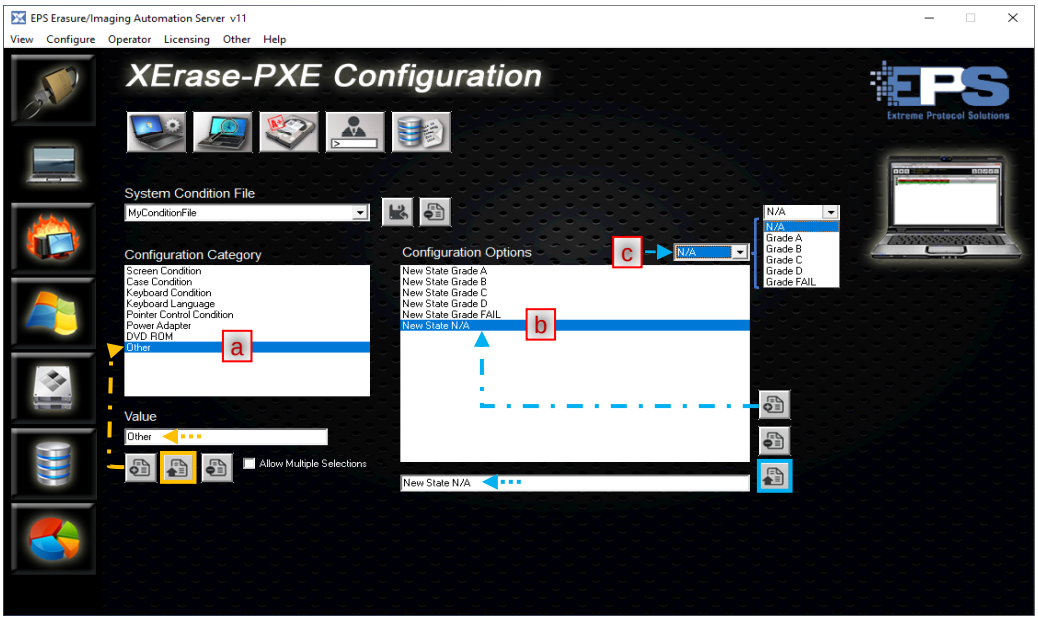


Figure 18 Mapped Steps To Adding An Configuration Option And Grade

Device Grading

Device health and grading is another tool designed to help reduce the chances of **RMAs** and ensure inventory to be resold is of a known good quality. Grades can be set for each type of drive that **XErase** recognizes according to your organization's guidelines and policies. When establishing the grade, determine which parameter to use, the constraint ("threshold") for the parameter and the grade to classify it to.

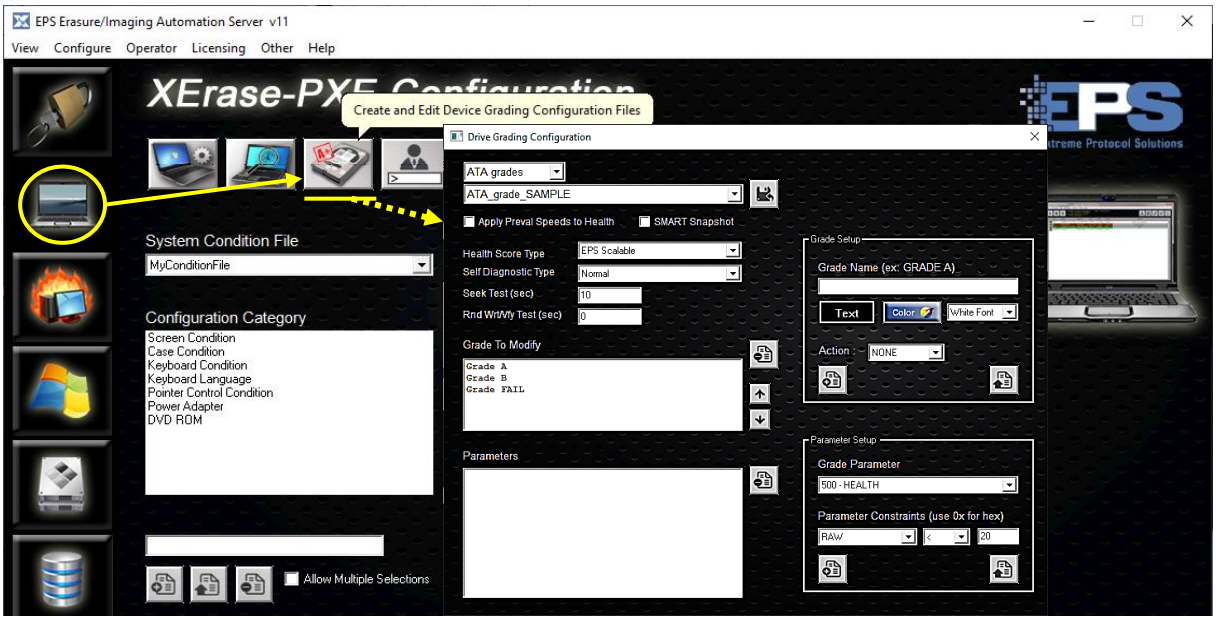


Figure 19 The Device Grading Files

Once the parameters are set, provide a name for the classification and save it. While any name can be used (i.e., good, better, best, etc.), grading by letter (i.e., **Grade A**, **Grade B**, **Grade C**, etc.) may be the most intuitive. Further customization can be made by setting colors for the grade, for example, **A**, **B**, and **C**. A grade must be set for each type of drive individually. Remember to save each update as it is made.

Note: This grading is for drives and, while similar in concept, is unrelated to the grading in the **System Condition Files** section.

In order to see the grading, it must be enabled in the respective PXE profile and will appear as disks are being erased providing for a quick and easily identifiable means of sorting disks for further processing.

User Field Templates

These templates contain customizable fields that allow data to be captured in the log file for each device that is erased or otherwise processed by **License Server**. The fields can be added to reports and either be system generated (aka, "normal" from the log files) or entered by the operator when prompted.

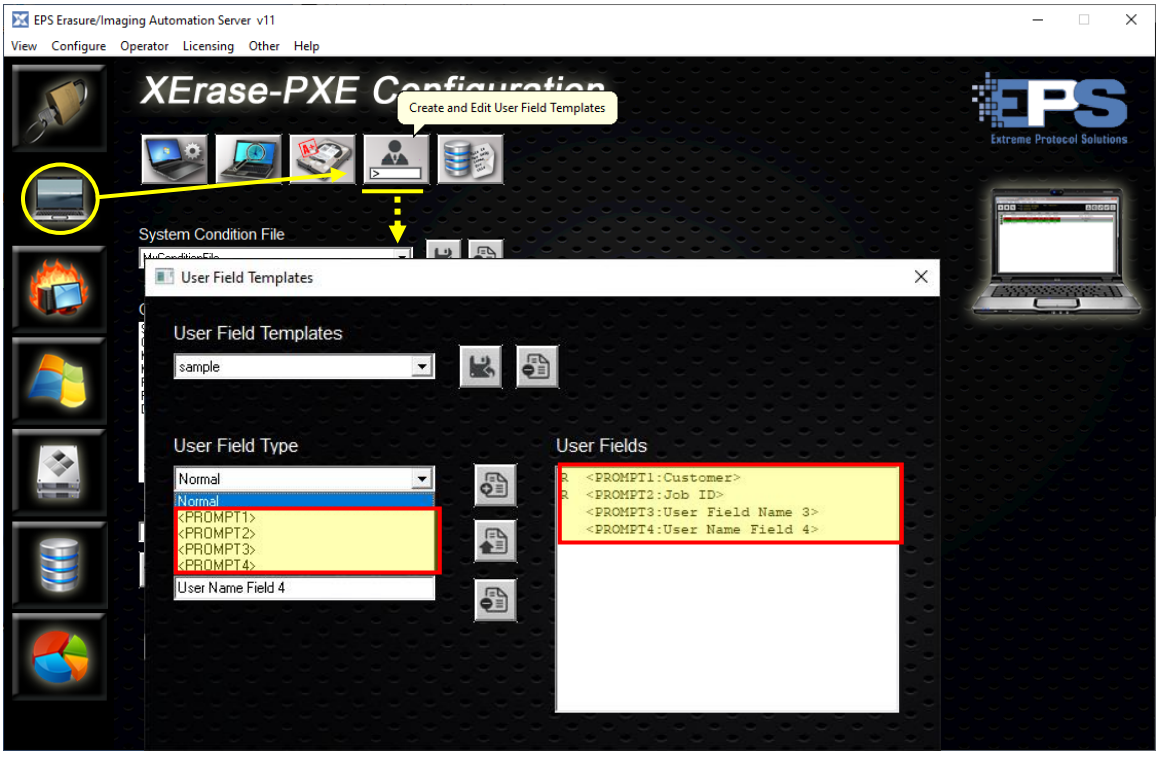


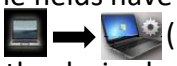
Figure 20 The User Field Templates

To create a **User Field Template**:

1. Click  which will open the template creation window.
2. Name and save the template with  .

3. Select one of the choices in the dropdown selections of **User Field Type** and enter a name for the field under **User Field Name**.
4. Specify if the field is required/mandatory.
5. Click  to add the field to the template; it will appear on the right side under **User Fields**.

   Repeat steps **3**, **4** and **5** for each desired field. Once all the fields have been added, click  to include them in the template (file).

6. After all the fields have been added and saved, enable the template.
   a. Go to  (**PXE Configuration Profiles**).
   b. Select the desired profile, then **Program Settings** (under **Configuration Category**) and **User Defined Fields** (under **Configuration Options**).
   c. Set the option value "**ON**", then select the name specified in step **2** for the **User Fields Template**, click  (update/save).

Database Scripts

Use this feature to update existing database tables with "one time" entries needed after a device has been processed. The script should be written and tested by an experienced database administrator before being placed into production.

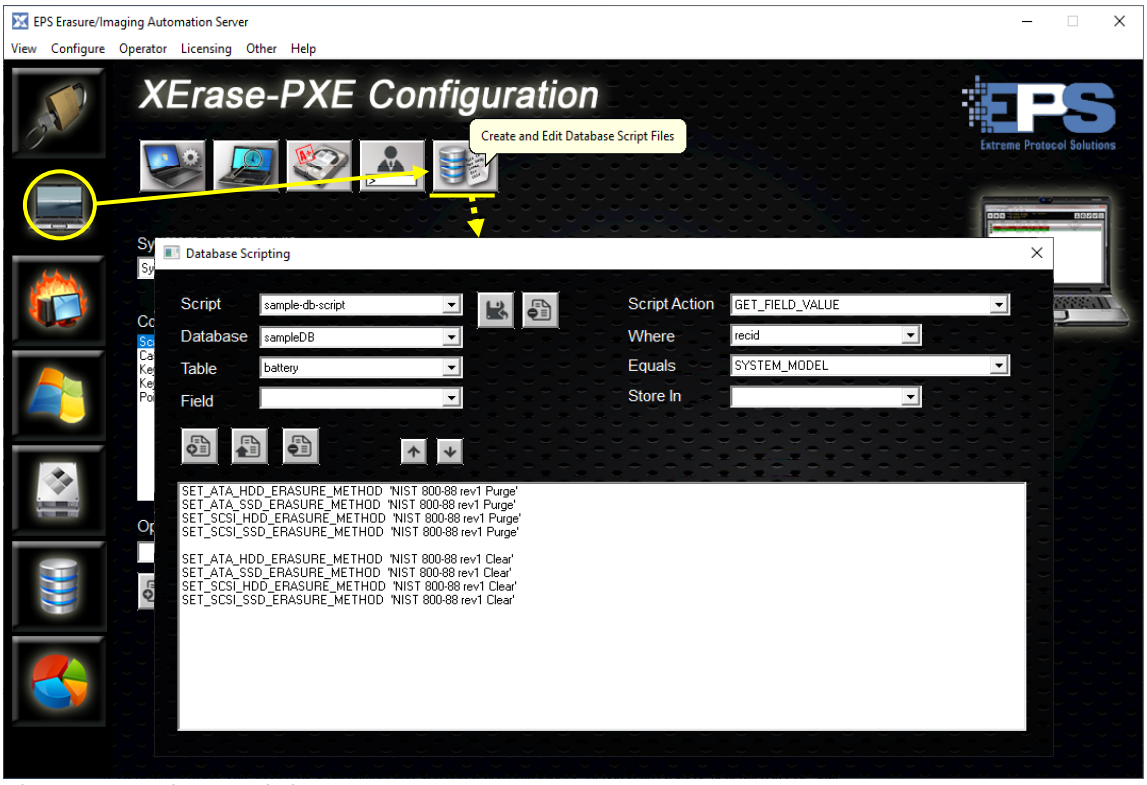


Figure 21 Database Scripting

After creation remember to enable the script:  (**Run File/Database Parsing Script**).

Burn In Test

EPS has incorporated the functionality of PassMark Software's, BurnInTest (BIT*),* into **License Server**. Having BIT integrated into License Server enables access to custom testing options for most onboard components of the devices that could be processed by License Server. The main benefit to this integration is the consolidation of separate testing and erasure stations into one.

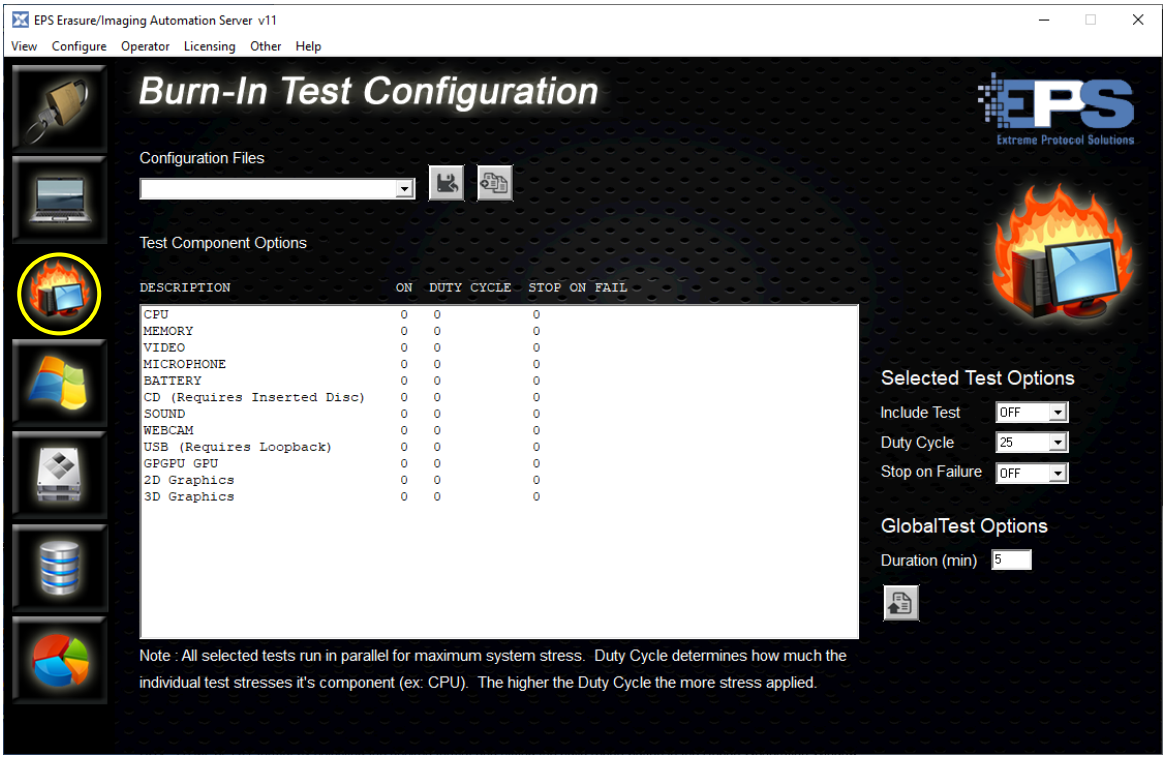


Figure 22 The BurnInTest Configuration Window

To create a new **BurnInTest** profile:

1. Click which will create the file within which the selections from the following steps will be stored.
2. Select the desired component to be tested.
3. Under **Selected Test Options**, enable the test, specify the desired cycle and what to do on failure, then click to add/update the settings to the profile.

   Repeat steps **2** and **3** for each component to be tested.
4. Set a **Global Test Option** to limit the overall duration of the test in its entirety, then click again.

5. If the profile is to be the default, click  .

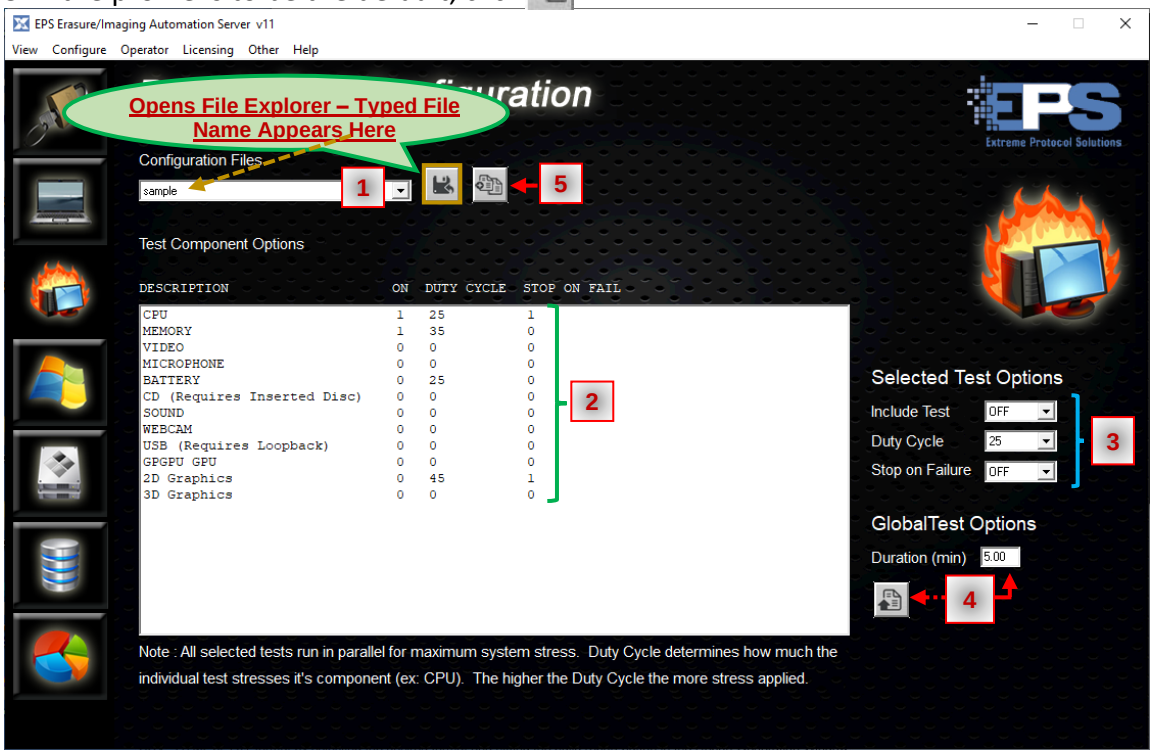


Figure 23 A Mapped Steps To A Configure BurnInTest

5. Finally, go to  ➡  , select the desired profile and, for **Startup Events** (under **Configuration Category**), enable the option, **Execute System Burn-In Test,** as well as the **Burn-In Test File** name. Remember to save the update with  .

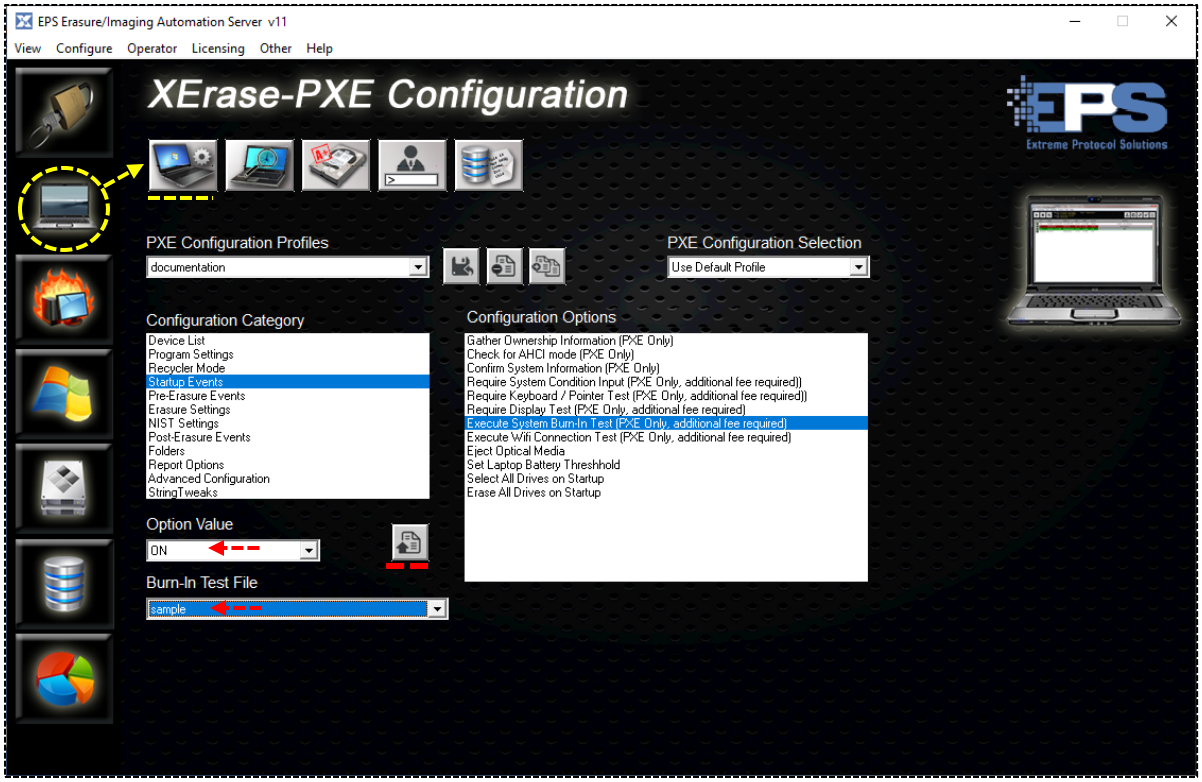
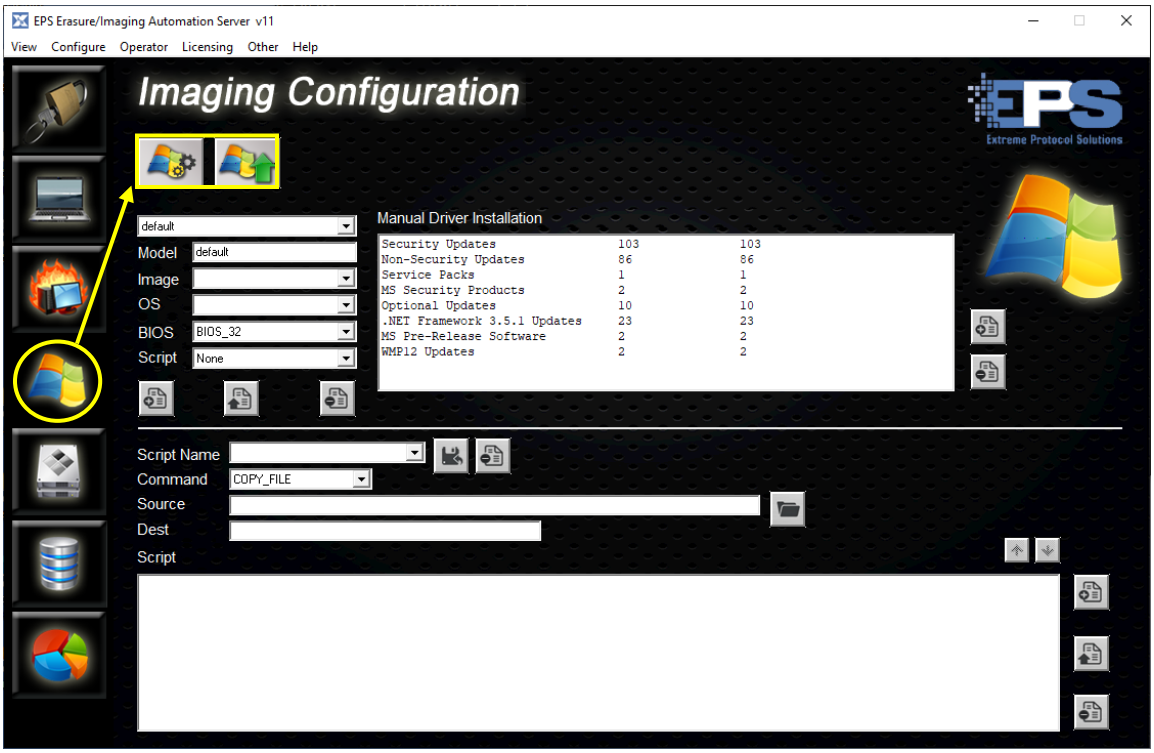


Figure 24 Confirming BIT Is Enabled In The PXE Profile

Imaging

Another feature that has been incorporated into **License Server** is the ability to reinstall an operating system onto a device. The **EPS** implementation is based on the principles of the **Microsoft Refurbisher Program** and, while not a requirement, is typically launched after the **BIT** and erasures have been completed. Windows and the operating system for Apple devices are currently the two supported operating systems.



Model Files

License Server includes a few models designed to help make reinstalling the operating system on a newly processed device faster and easier to set up. The "default" model will be used as the basis for the following steps. As with the other samples, leaving the default unmodified in case it is needed as a reference is recommended.

For the basic installation, only the fields in the upper half (shaded portion above the white line in the previous figure) are required and discussed in the following steps. The lower half can be used to further customize the imaging process and reduce the intervention required after the operation system has been installed.

Note: There is minimal support for this feature. It may be removed from future releases of License Server.

Prerequisites:

- If applicable, review/configure **Device Driver Configuration** ( ) and ensure the required drivers exist.
- The images **WIMs** to be used must be in **c:\XERAS_override\WIM\images**.

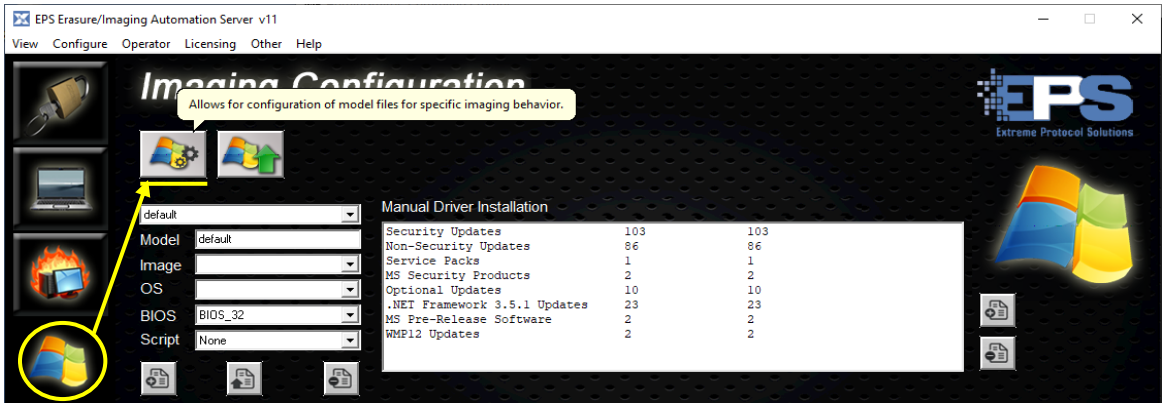


Figure 25 Imaging Configuration Models

1. If it is not already displayed, click the first field and select **default**.
2. Provide the name of the **Model** (file name) the customizations will be saved as in the **Model** field, then save it with - the name will change from "default" to the one that was just provided.
3. Click the **Image** field and select the image that is to be provisioned to the client. These reflect the WIMs that should have been copied into **c:\XERAS_override\WIM\images**.
4. Select the name and version of operating system for the image from the previous step.
5. Then select the architecture of the **BIOS** which is specific to the model of the device on which the operating system is being installed.

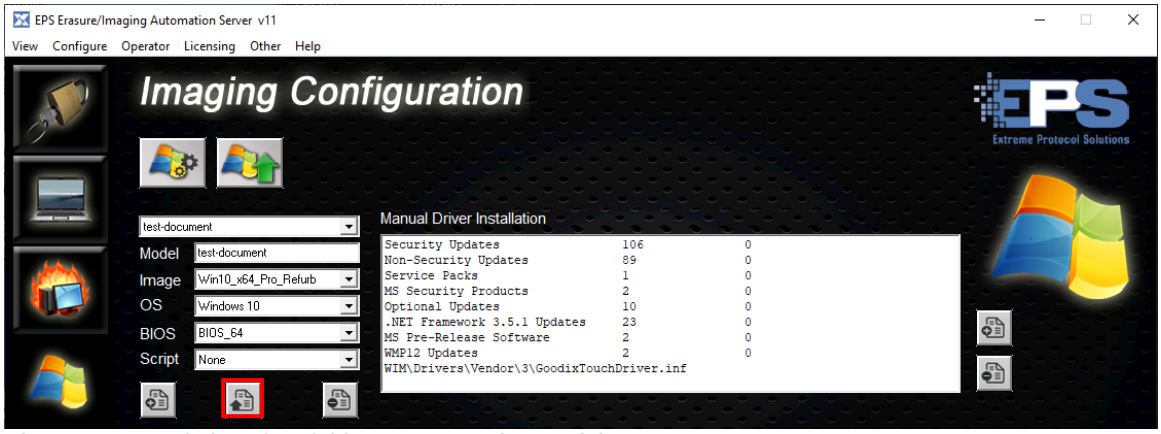


Figure 26 Completing The Fields For An Imaging Model

Notes:

1. Refer to the vendor's documentation for the device being reimaged to confirm the correct architecture is being used.
2. The BIOS for most current devices should be 64 bit - **BIOS_64 will not work** on a x32 (32 bit) machine but **BIOS_32** may work on a x64 (64 bit) machine.

6. If there are device drivers that need to be installed during the installation (refer to Device Driver), add them by clicking the (to the right of the field) under **Manual Driver Installation**, navigate to the respective "inf" file and save it.
7. Finally, remember to save any updates with .

Optional: If there is a post installation script, select it from the dropdown next to **Script**. Note that in order for it to be recognized in this window, the default location for any prewritten scripts should be **c:\XERAS_override\WIM\scripts** and should have a file extension of ".scr". Once found, its contents will also appear in the lower half of the window.

In addition to modifying existing scripts, this is also where new scripts can be added. It is highly recommended that any modifications to existing scripts or newly written scripts be tested external to **License Server** before being integrated into this feature.

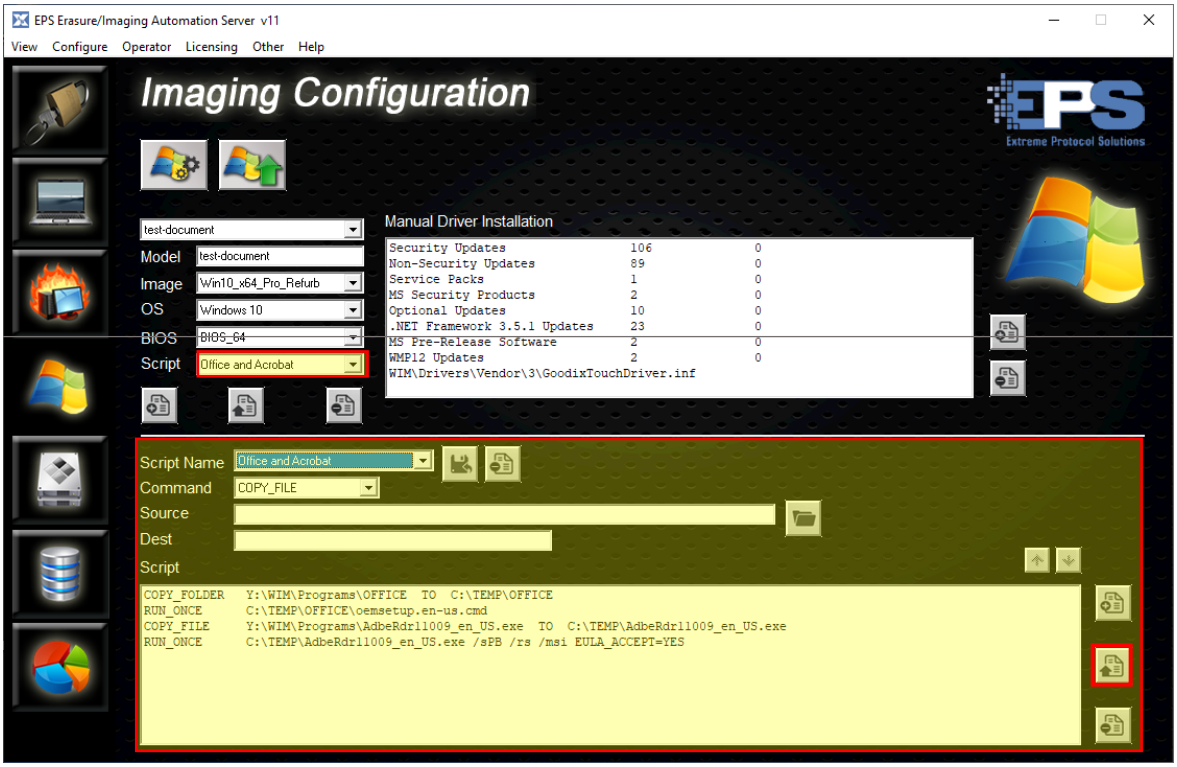


Figure 27 Customizing A Script To Run During Imaging

Remember to save any updates with the in this section of the window.

Post Imaging Steps

Once Windows has been reinstalled, there will usually be additional customizations that need to be performed to ensure the device conforms to your organization's requirements. Using this activity, customizations can now be automated and performed in "cookie cutter" fashion on multiple devices.

Figure 28 Configuring Windows Updates For Post Installation

Device Driver Configuration

A device driver is software that represents a hardware component (i.e., processor, memory, disk drive, USB, COM ports, adapters, etc.) that allows the operating system to recognize what it is and its functionality. Drivers are loaded when the client is booted. Without them, the hardware component it represents will not be accessible or usable.

Most device drivers are included with the operating system. This feature was designed to assist in configuring the ones that are not. Once configured, the drivers will be injected (installed) while the operating system is being installed if it's needed.

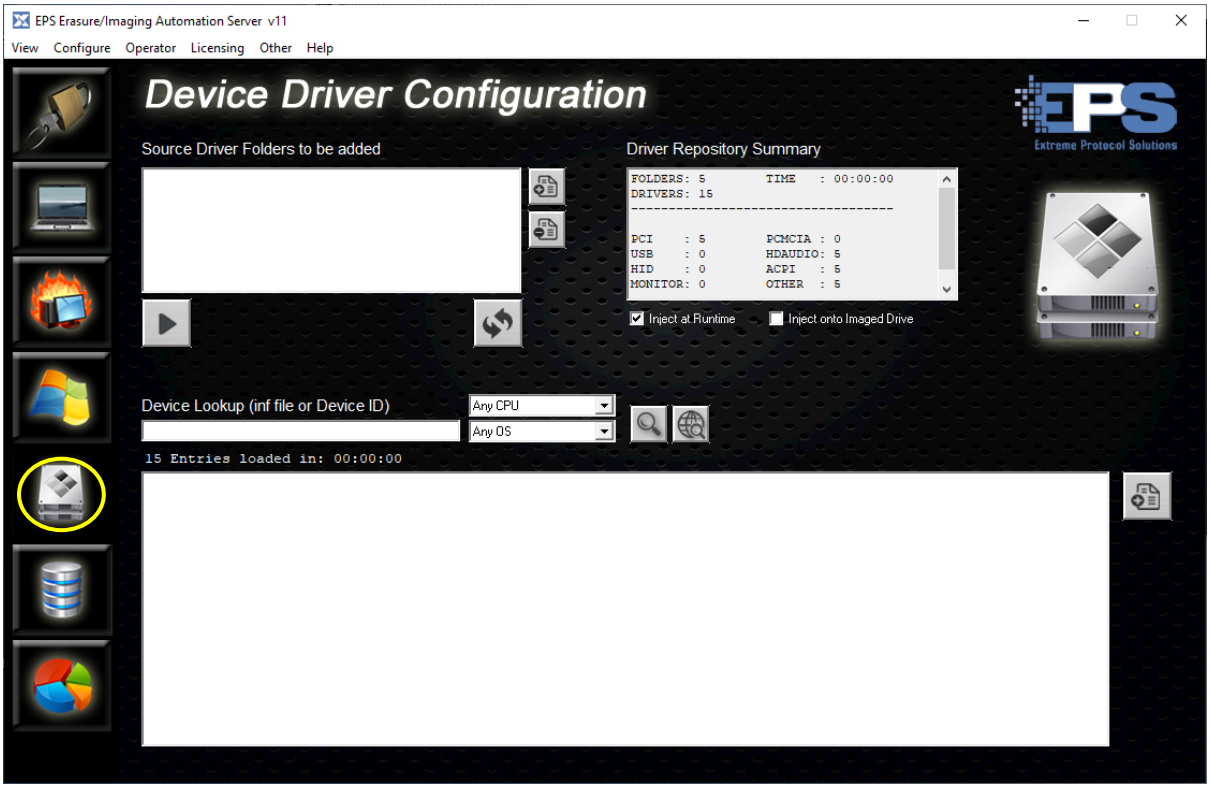


Figure 29 The Device Driver Configuration Feature

Prerequisites:

- Drivers from the **Microsoft Refurbisher Program** must be available in **c:\XERAS_override\drivers**.
- Connection to the internet.

For the following steps, the source folder for the drivers is **c:\documentation\test** and will end up in **c:\XERAS_override\WIM\Drivers**.

1. Click  next to the field for **Source Driver Folders to be added**. Once **File**

Explorer appears, navigate to the desired folder and save the location. The selected path will appear in the referenced field.

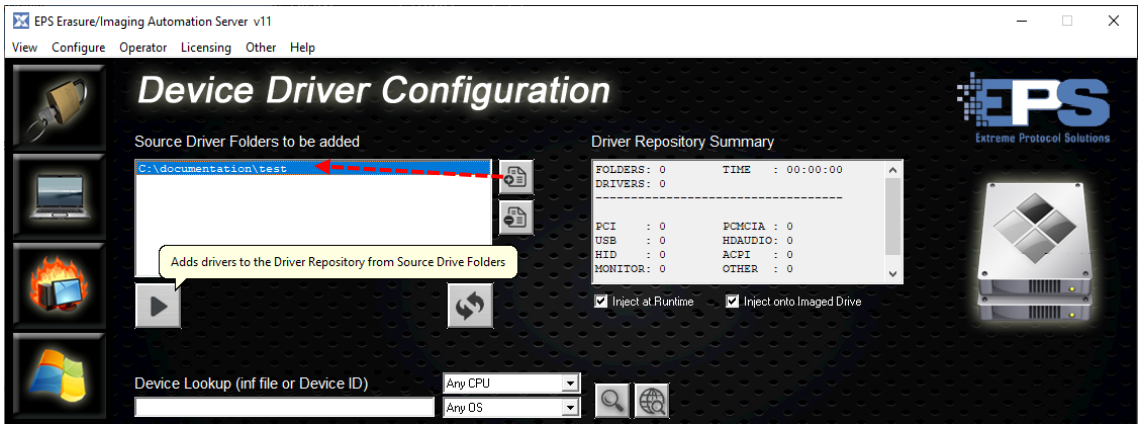


Figure 30 Adding The Source For The Drivers

2. Click ▶ to add and index the drivers to the required location(s) as well as when and where the drivers will be injected. The statistics related to indexing the drivers will be displayed.

   Optional: If needed, the lower half of the window provides the ability to do an online lookup for a device driver assuming valid information for the device is provided. To search the driver repository within **License Server** use 🔍 and 🌐 to search the catalog at Microsoft's website.

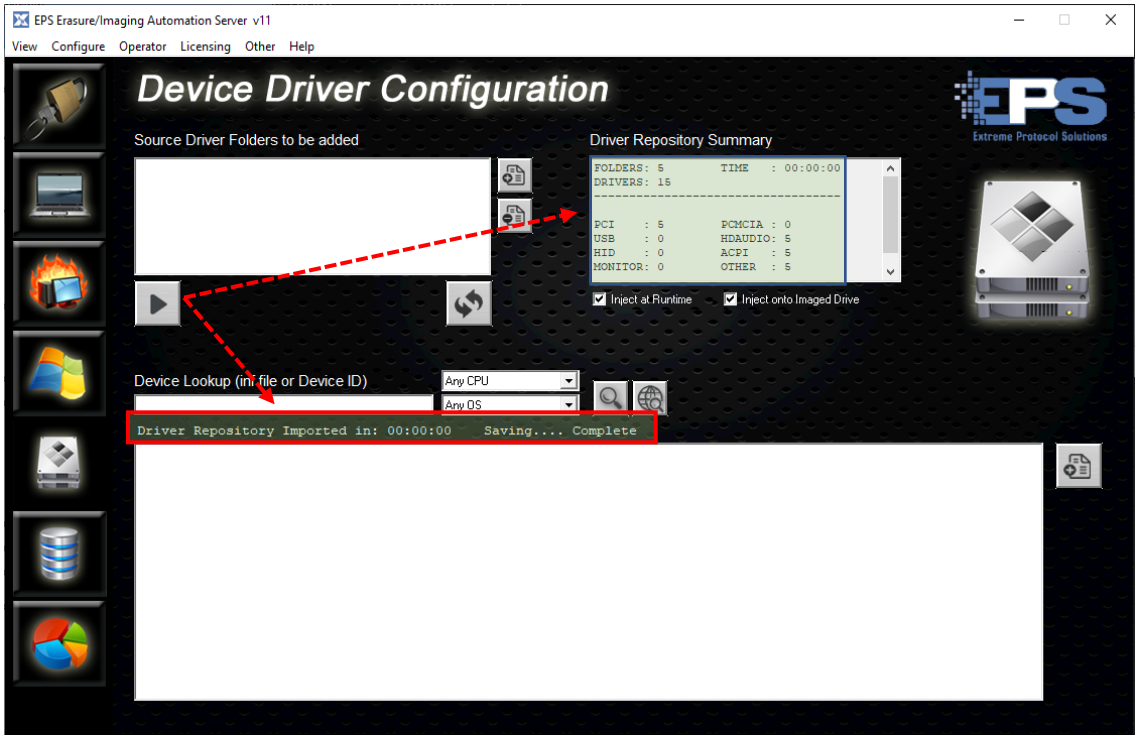


Figure 31 Integrating The Drivers Into The Configuration

Database Configuration

Included with the **Premium** license of **XErase,** is a powerful means to interact directly with a (local or remote) database which makes uploading information related to the devices processed by **License Server** a smooth, effortless and automatic process. If it doesn't already exist, a database and related tables can be quickly established by using one of the sample scripts included with **License Server** in the folder, **c:\LCServer\Database**. Once created, the fields from **License Server's** features will need to be mapped (i.e., cross referenced) to the fields of the tables.

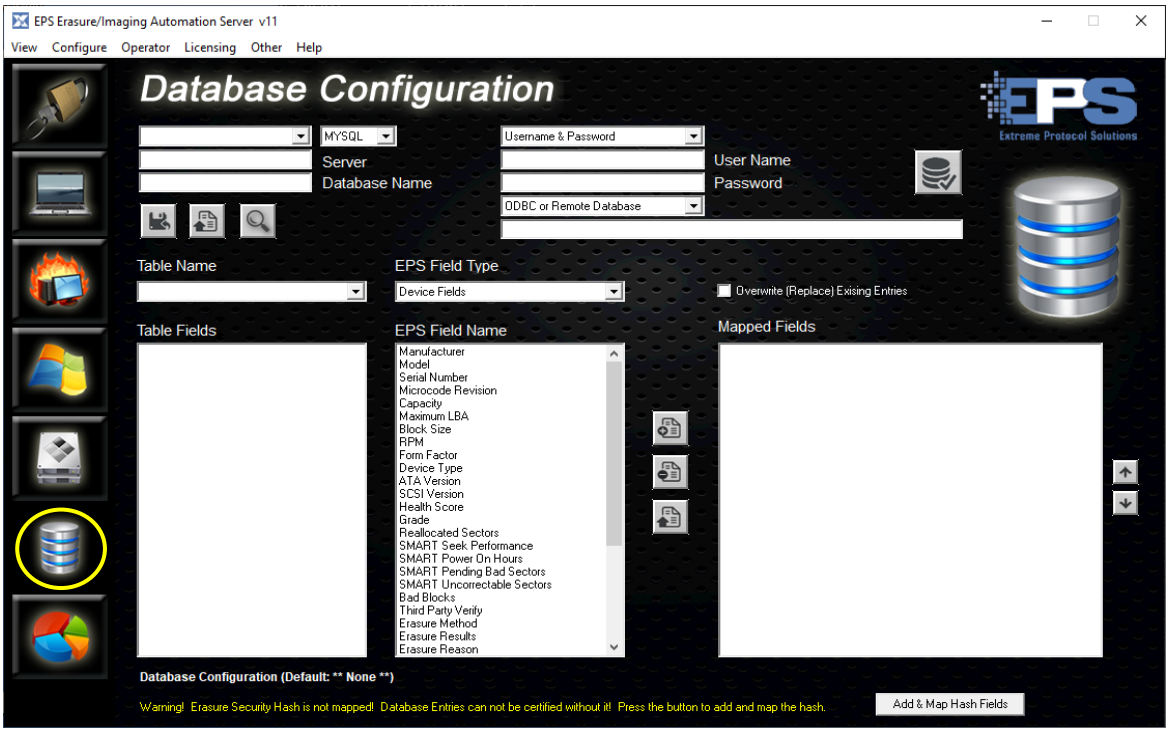


Figure 32 The Database Feature

Prerequisites:

- If the **DB** is running remotely (i.e., on a system other than where **License Server** is running), confirm the hostname of the system as well as the name of the DB to connect to.
- Ensure the DB network connection between **License Server** and the system where the database is running is not being blocked by any network related security settings.
- Verify the account conducting the transaction(s) has an account and password (if required) defined, as well as authorization to access, the database. If one doesn't exist, have one created and the authorizations enabled.
- Ensure that any required **ODBC** related to the client side have been installed. A 32 bit and 64 bit ODBC driver should be included with Windows 10 or higher. Before attempting to connect, ***confirm the connection using the tools included with the ODBC*** package/driver.

- The database and tables must exist before this feature can be used for the first time. If this is a new database, one of the scripts in **c:\LCServer\database** can be used to quickly create the DB and tables.

> **Note**: If your organization uses an ERP system, the database and mappings may already be established. Refer to Appendix C - Databases for further information.

Refer any questions/issues to your database administrator and/or network security team.

Once the database has been created, map the desired fields for the features within **License Server** to the records in the tables into which data will be loaded.

1. Establish the connection to the database.

   a. Choose the type of database (**MySQL** or **SQL**) from the dropdown.

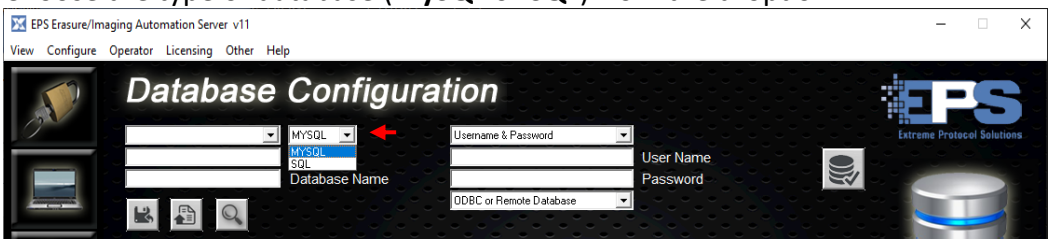


Figure 33 Selecting The Type Of Database To Use

   b. Select which credentials to use when connecting to the database.

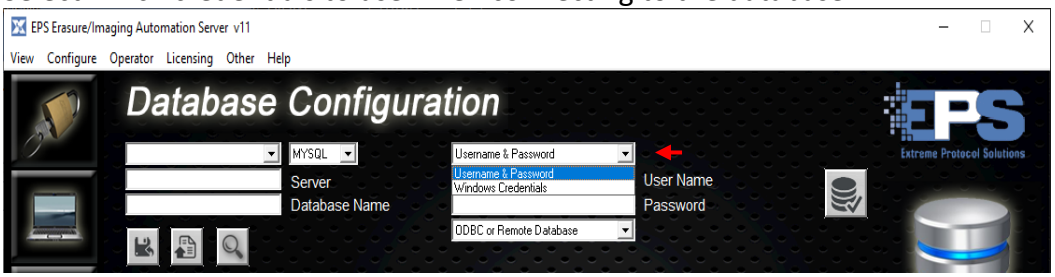


Figure 34 Configuring An Account's Access To A Database

   c. Fill in the user credentials as well as the type of connection (local or remote).

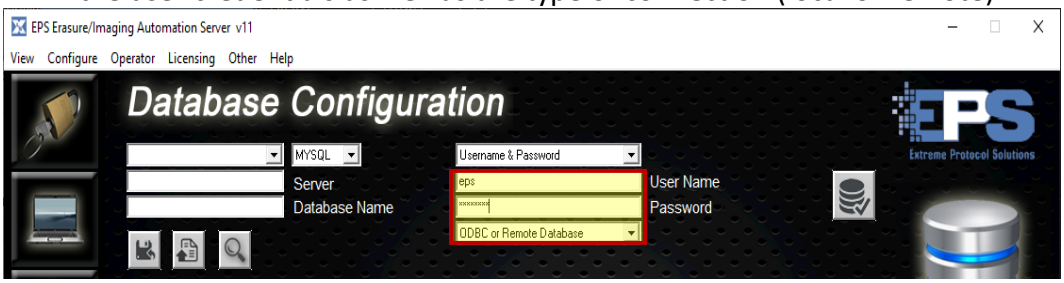


Figure 35 Setting The Account's Credentials

d. Enter the hostname or IP address (as used in this example) of the system where the database is running along with the name of the database.

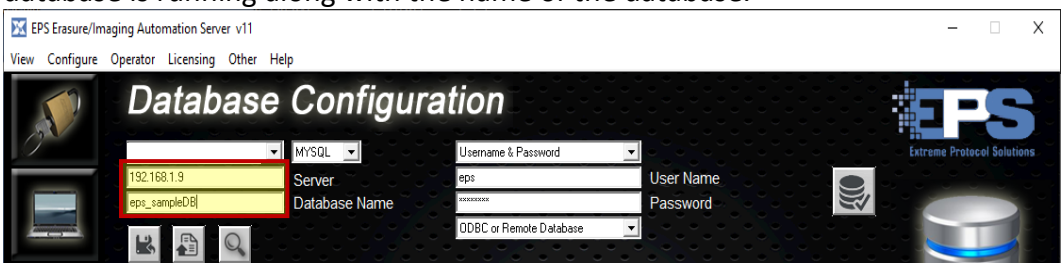


Figure 36 Setting Where The Database Is Running

e. Click  and provide a name for the profile. Once saved, the name will appear in the field to the left of where the type of database was first selected; the default table and its fields should remain.

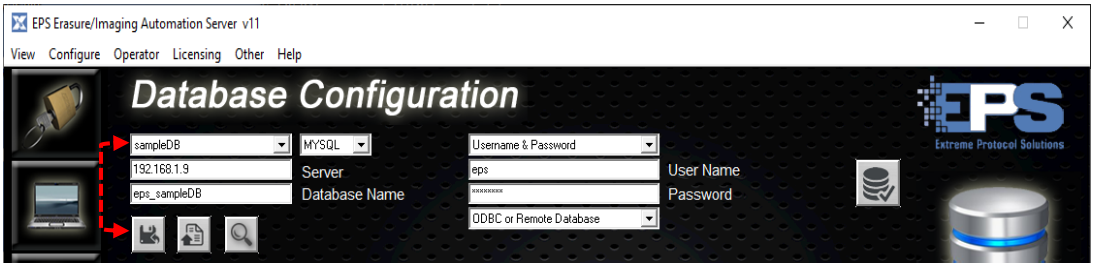


Figure 37 Saving The Database Configuration

2. Map the fields and hash keys.

a. Select the table whose fields are to be mapped.

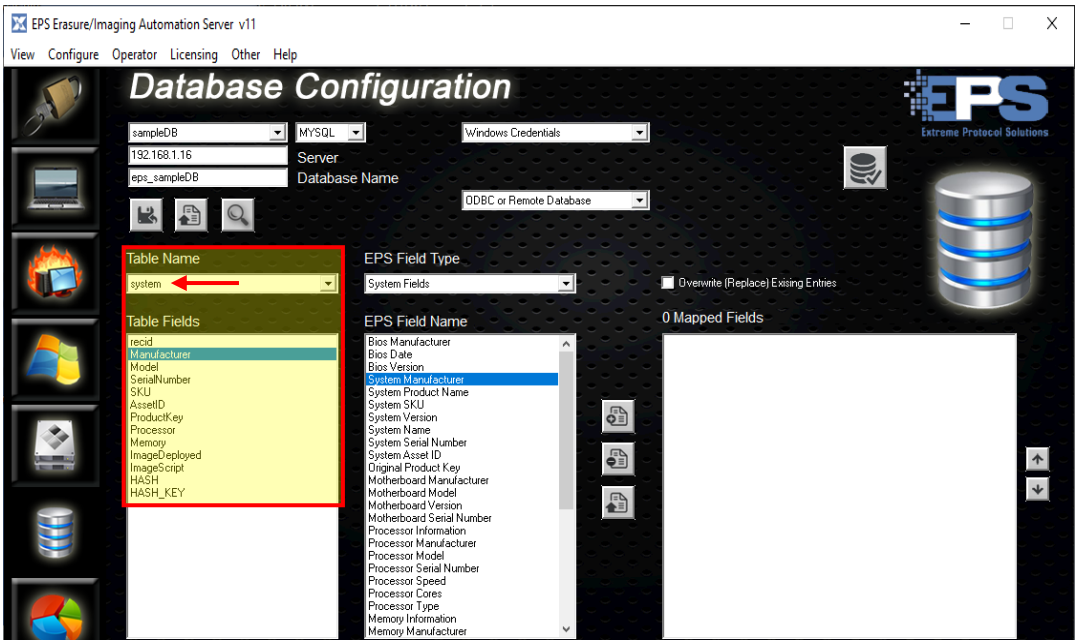


Figure 38 Mapping The EPS Fields To Database Tables

b. Select the **EPS Field Type** from the choices in the dropdown, along with the corresponding **EPS Field Name**, then click to add the field to the **Mapped Fields**. Last, select the newly added field and (circled in red below) to save the individual mapping.

Repeat steps **a** and **b** until the maps for the fields of the current table, as well as fields for any other desired table, have been mapped.

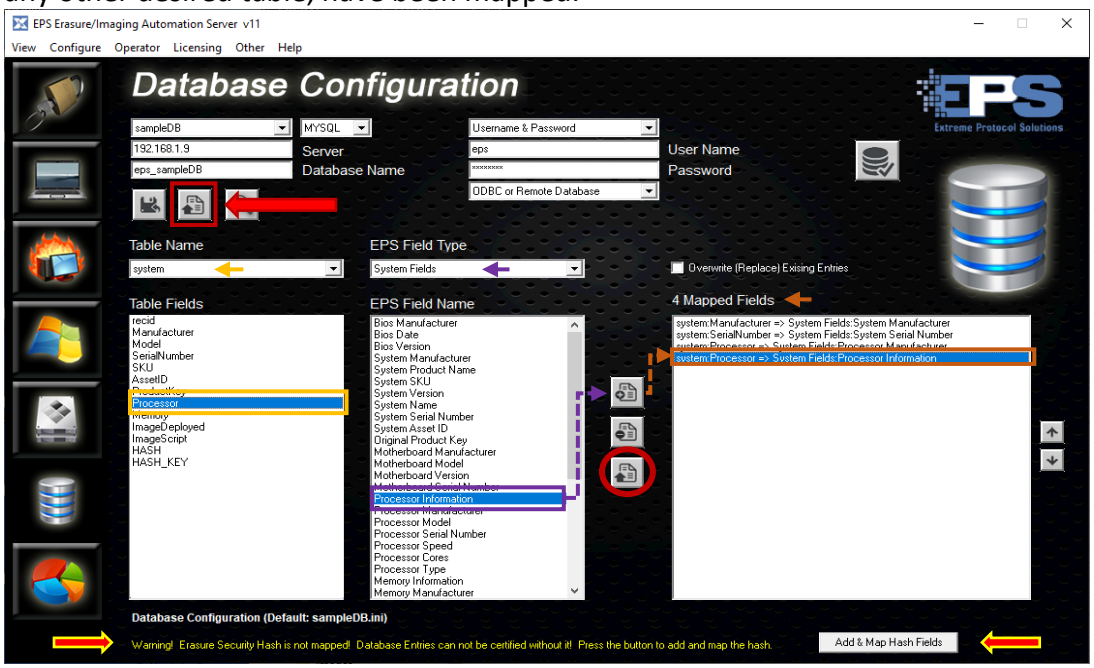


Figure 39 The Steps Required To Map EPS Fields

c. **Optional** - Map the hash and hash key for the storage device table.
Once the hash fields have been mapped and saved, refresh the DB by clicking the name of the profile - the warning at the bottom of the screen (refer to Figure TBD) should not be displayed any longer.

3. Confirm that all the requirements for the DB related to both current and (potential) future updates to **XErase** are met with and remediate any notices that are displayed, especially the ones marked, "**REQUIRED**". Refer to Appendix C – Database Notifications for a sample of the possible warnings.

For example, if this notice was displayed.

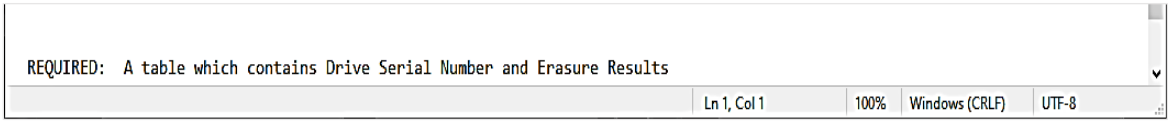


Figure 40 An Example Of A Notice When Checking The DB Requirements

These mappings would need to be added to remediate the notice.

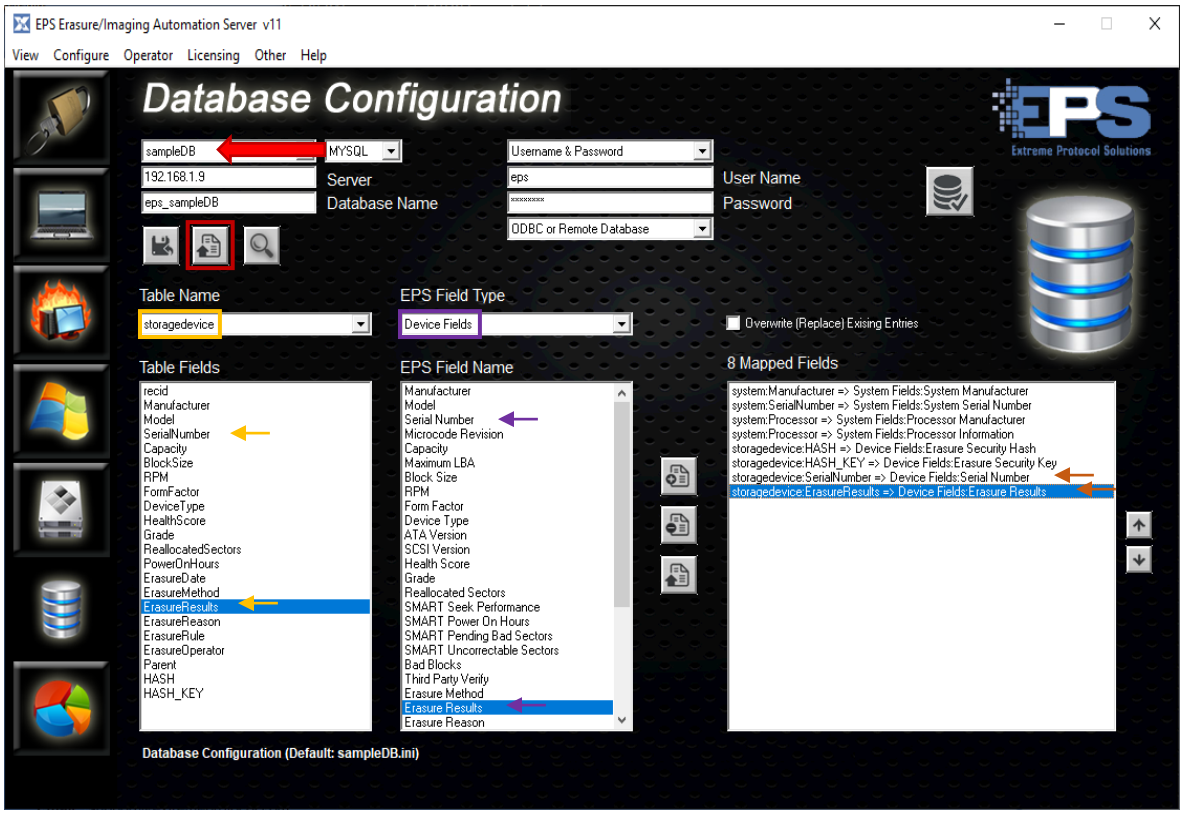


Figure 41 Remediating A "Required" Notice

Once added, confirm by clicking again and ensure no "**REQUIRED**" notices are displayed.

4. Save all the updates to the database profile with the located just beneath the name of the DB. To view all the mappings for any of the table fields that have been mapped, refresh the DB by clicking the name of the database profile, then select the **Table Name** from the listing in the dropdown.

5. Finally, enable the options in the respective **XErase-PXE Configuration** profile.

   Click → and select the desired profile, then ensure the **Configuration Categories** and their options are set as depicted in the following figures using your values.

To automatically "inject" the data into a DB once the erasure finishes, **Configuration Category: Program Settings, Database Injection**.

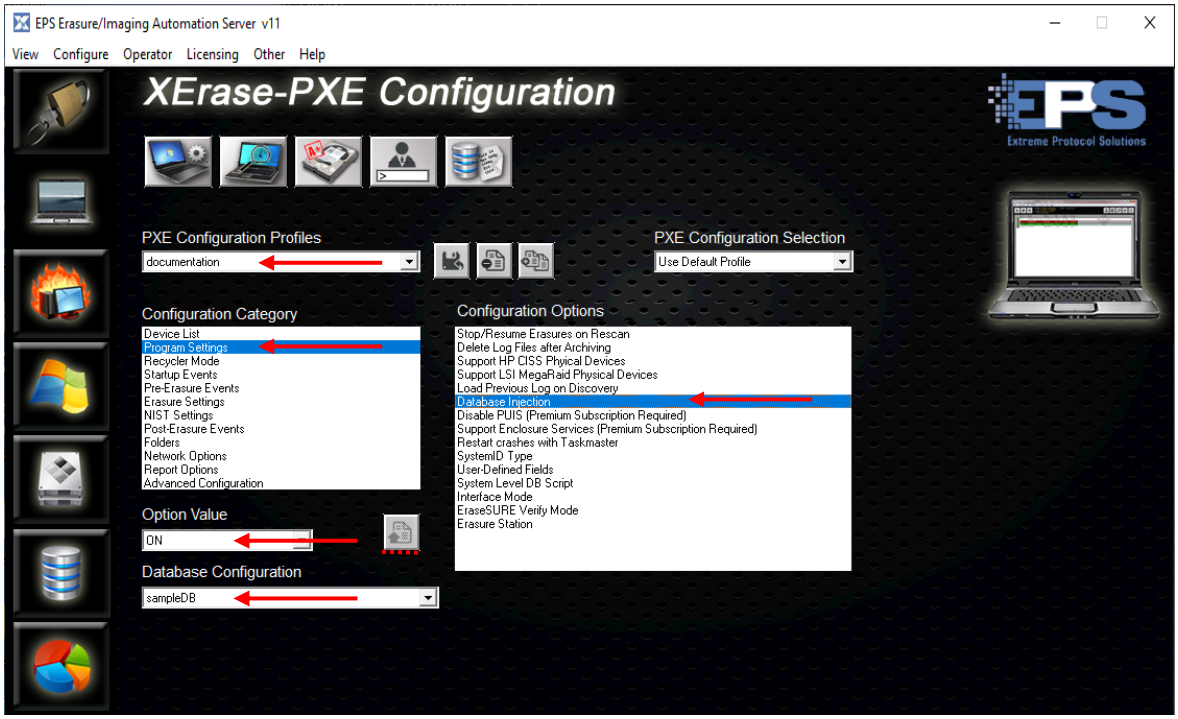


Figure 42 Enabling The Database In The PXE Profile

Optionally, if generating exports for the DB is desired when the erasure completes, **Configuration Category: Report Options, Generate Report**.

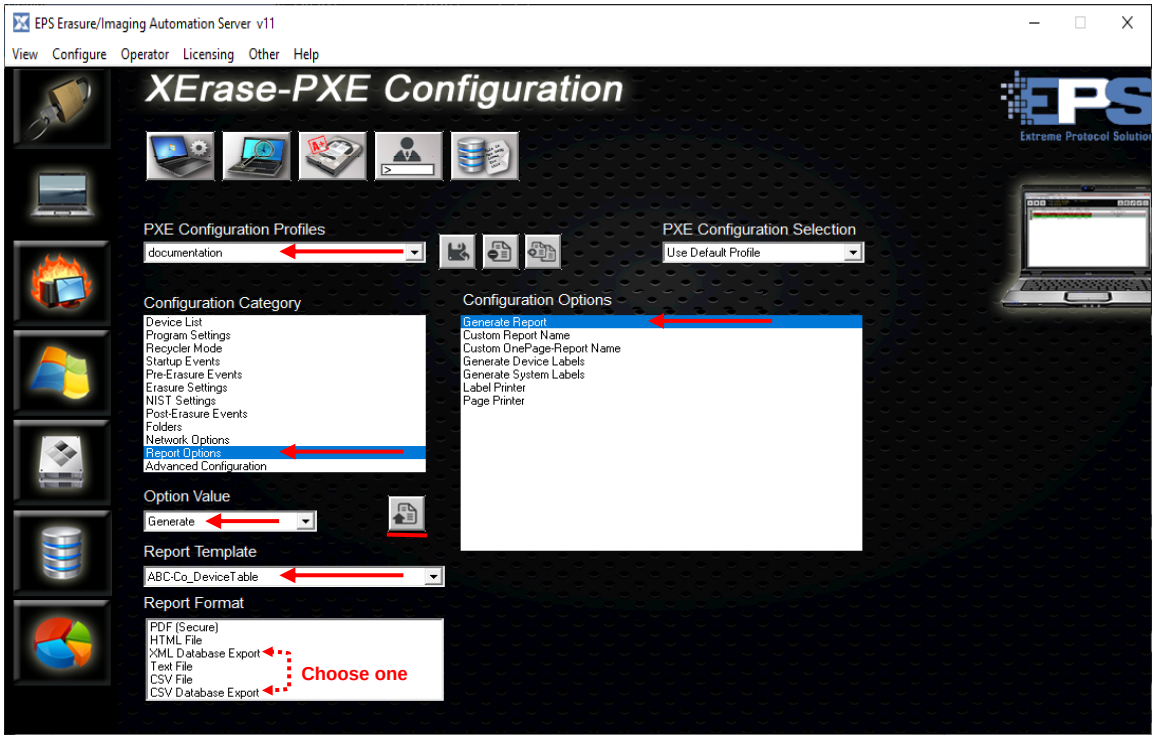


Figure 43 Enabling The Automatic Export Of Data

Reporting

Once devices have been erased, reports can be created in a variety of types and layouts. Reports can be generated in many of the common formats such as, **Secure PDF**, **HTML**, **Text** (viewable in Notepad or Wordpad), **XML** and **CSV**.

Figure 44 The Reporting Feature

Report Templates

A company logo will be added to a template as a simple illustration of updating the **DriveOnePage** (drives on one page) sample template and saved to a template called, "***MyCompanyOneDrive***". The only prerequisite for this example is to confirm that the desired image is in the required location (**c:\XERAS_override\images**) and that it is in **JPEG** format.

1. Click  .
2. Select a template from the drop down next to **Template** (or one of your choosing), then  and provide a name when prompted.
3. Click in the field/drop down arrow to the right of **Type** in the **Report Element** section and select **<IMAGE_TOP_RIGHT>**.
4. Click  and navigate to where the image is stored (it should open to the correct location by default), select the desired image and click **Open**.
5. Add it to the list of elements with  . A preview with the new logo should appear in the upper right.

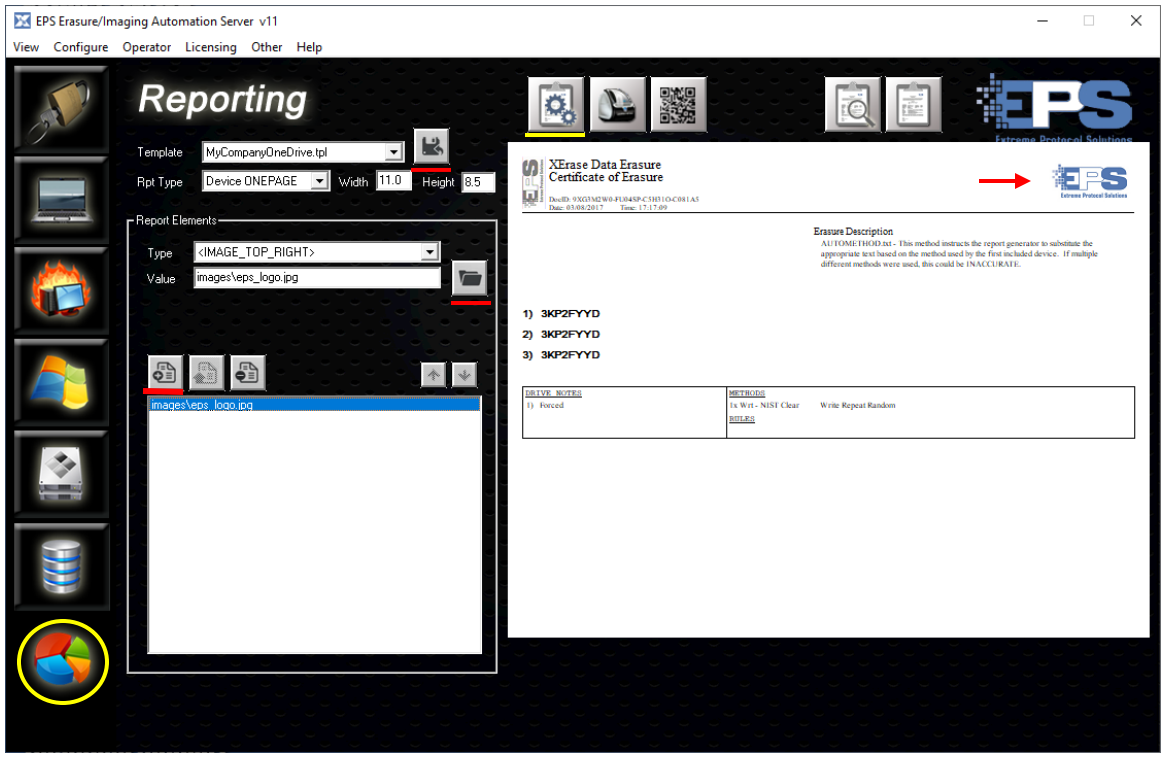


Figure 45 A Report Template In Landscape Mode

If other elements need to be included in (or removed from) the template, repeat steps **1** and **3** for each element that needs to be added to (or removed from) the template. Each will appear within the preview as it is added (or disappear if removed). To change the order an element appears in the list/preview, select it, then / to move it up/down in the list/preview. Elements like, "<**IMAGE_TOP_RIGHT**>" will remain in the preview as the name implies regardless of where it is in the list. Commit the element to the template with .

6. Use to save the template providing a filename for it when prompted.

Label Templates

The **Label Templates** are very similar to the report templates but have a limited amount of space available within which to include information. While labels can be generated for any device processed, they are most commonly generated when a disk drive has been erased.

Customizing these templates is nearly identical to the report templates using the buttons and elements to set the information to be displayed in the two columns.

When setting elements, monitor the preview to ensure the font remains readable (fonts will become smaller as more elements are added) and that the columns are not

truncated (cutoff). Just like the report templates, whatever is in the **Rpt Type** field will become the default type of report whenever a label is printed.

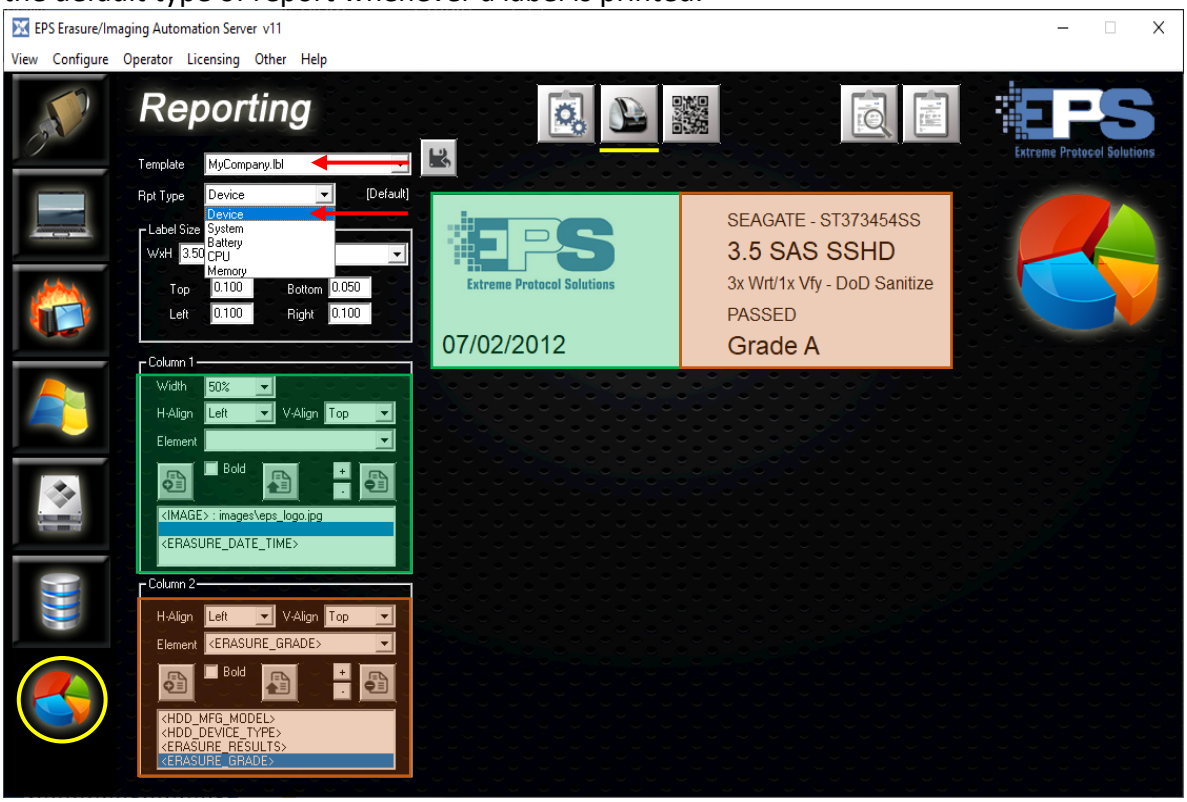


Figure 46 A Label Template With A Company Logo

If QR codes need to be added, the code must be generated first.

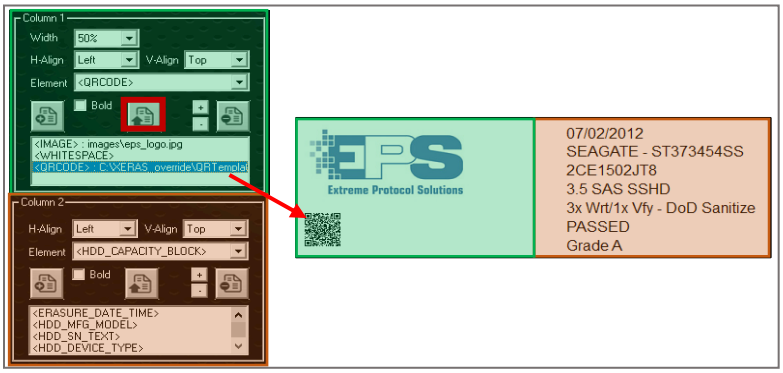


Figure 47 A Label Template With A QR Code Added

Then, add the "**<QRCODE>"** element to the respective **Label Template**.

1. Click  .
2. Navigate to ***c:\XERAS_override\QRTemplates*** and select the desired file (it will have an extension of "**.qrt**"), click ***Open***. That element can be added to either column.
3. Make the desired adjustments (if any), then  .

Finally, in order to print a label, the name of the label template to use as well as its option value must be set:  ➡  ➡ **Report Options** ➡**Generate Device** (and/or **System Labels)**.

For each **Configuration Option**, set the desired **Option Value** specific to the results of the activity that was performed and select the template to use. The label will be generated only for devices that meet the **Option Value** (i.e., Pass, Fail, etc.) that is set here.

While in the configuration options, remember to select a default **Label Printer**. Note that the printer must already been added to Windows.

QR Templates

QR templates are configured the same way as the report and label templates. There are just fewer fields – **Rpt Type** and for the **QR Elements** section, **Format** and **Element**. After any modifications are saved, confirm the code by either reading it back from the screen or printing a label and reading it back from there.

Figure 48 Generating A QR Template

1. Select a template to use as a model and save it using a new name.
2. Select the desired option for ***Rpt Type*** and optionally, the ***Format*** if it needs to be anything other than (the default) **Text**.
3. Choose the elements to be included from the list in the drop down next to ***Element*** and add them with  .

Generating Reports

Use this feature to view/print reports that have been previously generated or to compile reports for activity that has not been reported on yet. Depending on your requirements, reports can be generated in a variety of formats including, secure **PDF**, **HTML** or **Text**, as well as **XML** and **CSV Database Export**. The XML and CSV formats are a convenient way to add data to a predefined database (refer to Database script and Database Configuration) or import the information into a spreadsheet.

View Previously Generated Reports

Reports are stored in the locations configured in **PXE Profiles** ➡ **Folders** once they are generated and can be viewed either directly from that location or using this tool.

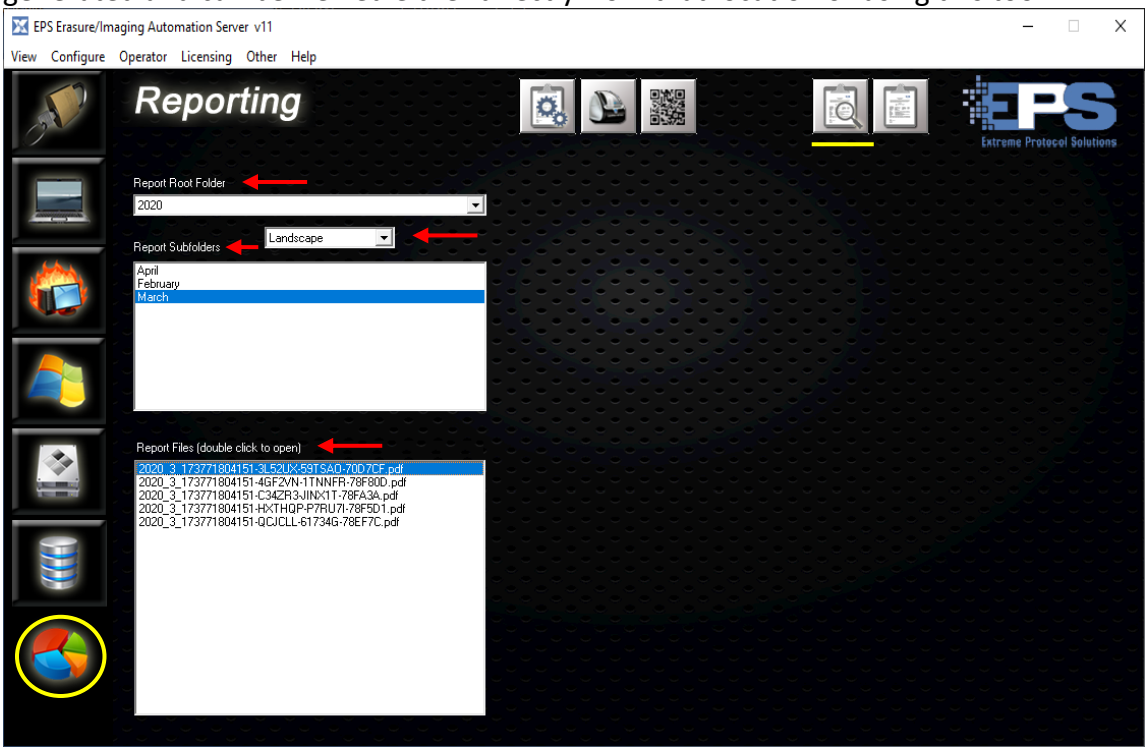


Figure 49 Report9ing - Viewing Previously Generated Reports

To view a previously generated report:

1. Click .
2. Select the desired folder from the **Report Root Folder.**
3. Choose the orientation (**Landscape** or P**ortrait**).
4. Select a folder from **Report Subfolders.**
5. Open one of the files under **Report Files (double click to open)**.

> **Note**: The default location for the reports is set in the **Folder Name** field of the active profile in **PXE Configuration Profiles** ➡ **Folders** ➡ **Default Report Folders**.

Create A New Report

Reports can be generated at any time after an erasure completes as long as the logs exist. The logs can be in their original locations, on a network share or on other removable media and:

- ✓ ***Must*** have been generated by **XErase** during an erasure.
- ✓ ***Must not*** have been edited in any way by anything other than **XErase** in a single threaded (i.e., only one connection to the disk) session.

Any that do not comply with those two requirements will be reported as "***Modified***" and the respective disk(s) considered "***NoCert***" (uncertified).

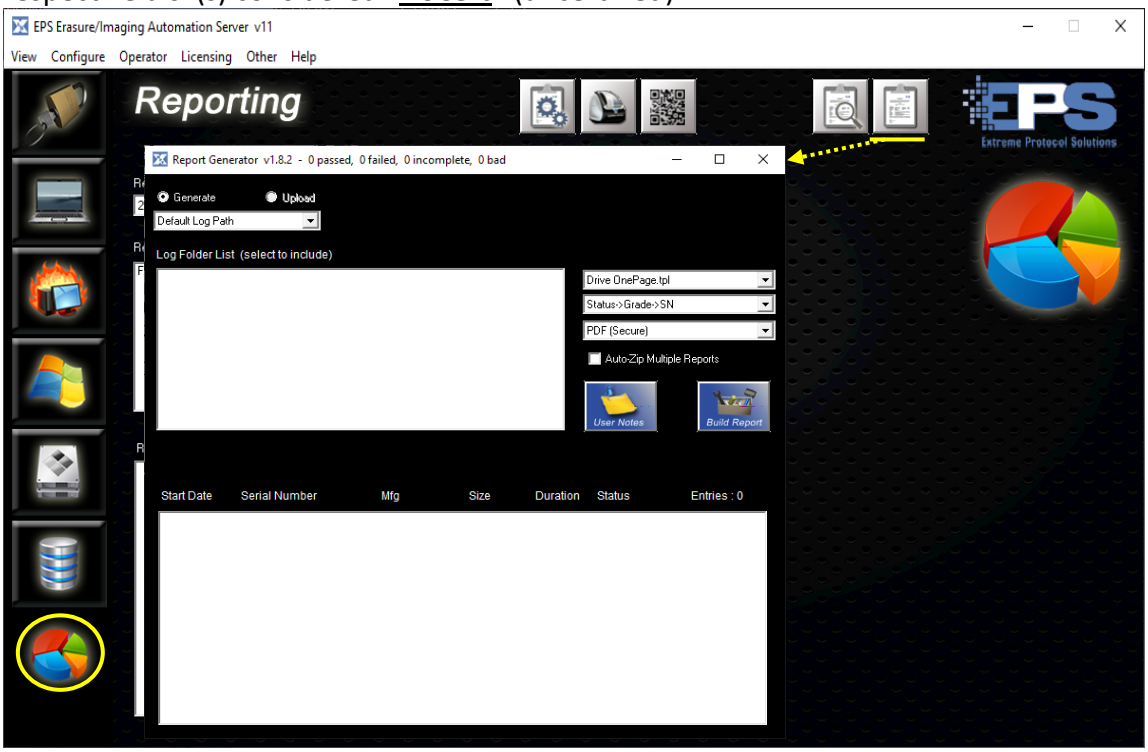


Figure 50 Creating A Report

Notes:

1. The default location for the logs is set in the **Folder Name** field of the active profile in ➡ ➡ **Folders** ➡ **Default Log Folder**.

2. If **Program Settings** ➡ **User Defined Fields** ➡ **Option Value** is **ON,** the path will include what is set in **User Fields Templates**.

The following sections describe the three methods of selecting the folders that contain logs. The default path is set to, "**log\<YEAR>\<MONTH_STR>**" where, "**<YEAR>" =** 2020 and "**<MONTH_STR>**" = April.

A. Selected SubFolders And Saved Sources

1. Click  .
2. In the dropdown selections under **Generate**, select either **Selected SubFolders** or **Saved Sources**, then click  .
3. The top level folder (for this example, 2020) will appear in the main field. If the logs are stored in a location not displayed in the main field, double click **UP**, follow the prompt to "**Double Click a Folder**…" navigate to the respective drive (double click a selection) under **Shortcuts**, then the double click a folder that appears in the main field until the desired folder is displayed in the main field.

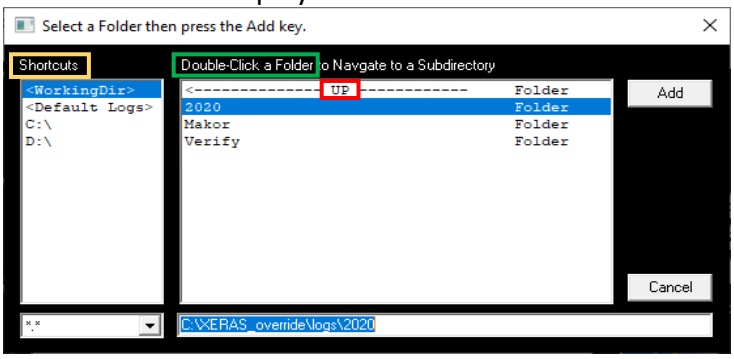


Figure 51 Choosing The Directory Containing The Logs

4. Click  .
5. In the subsequent window, all the logs found (including those in any subfolders) will be preselected. Deselect the logs to exclude, if any, from the report (the Windows ***select all*** key/mouse combination is enabled).

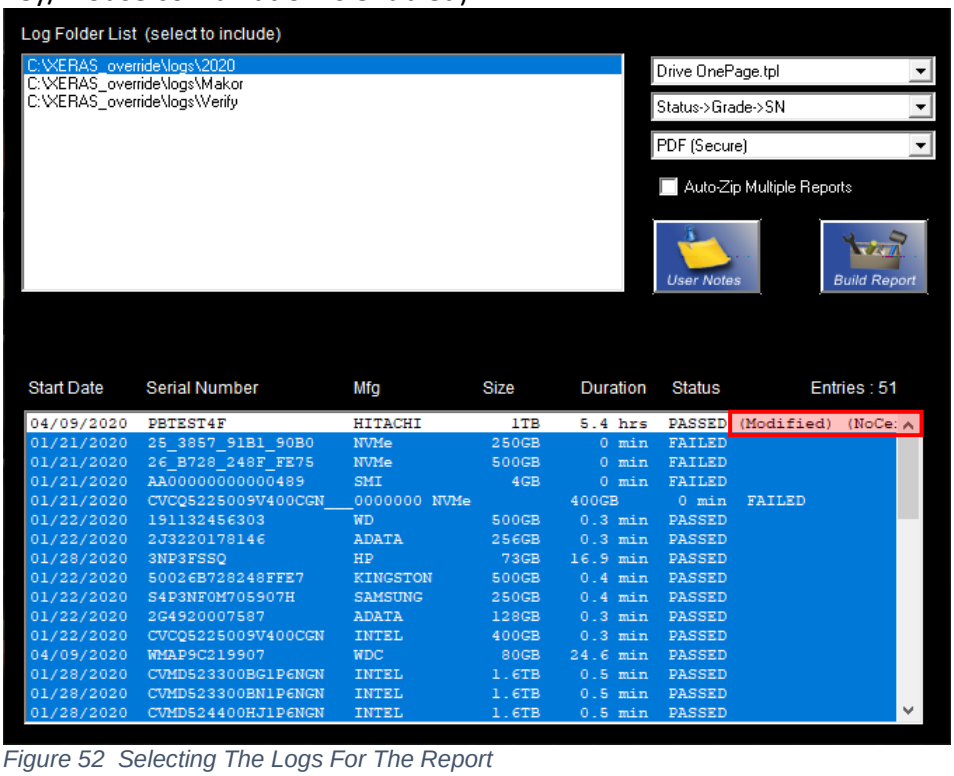


Figure 52 Selecting The Logs For The Report

Note that the logs included in the previous figure are from multiple periods (unsorted) since in this example, there were four folders (January, February, March, April) under the specified **Log Folder List**. To get a more specific period/range, either continue opening any subsequent subfolders (until there are no more) or use **Filter Logs by Criteria** (next section).

6. Once the desired logs are selected, create the report with 

.

B. Filter Logs by Criteria

1. Select **Filter Logs by Criteria**.
2. Fill in the criteria for the logs to include in the report.

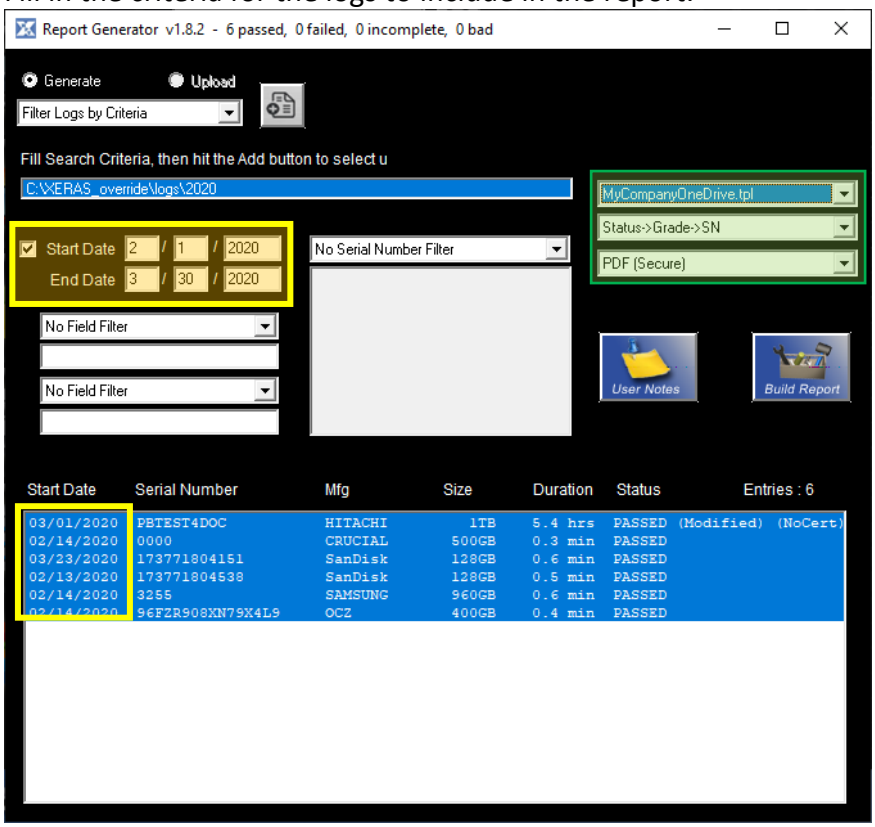


Figure 53 Choosing The Criteria For The Report

To search using different criteria:

a) Select and update the respective fields (**EXAMPLE**: Start/End Date).
b) Click  and select the same (or search for a different) folder.

3. Select the type of report, category and format for the report in the fields on the right side.
4. Create the report with 

.

The (Main) Menu Bar

In addition to providing an alternative path to accessing the main features, the controls in this portion of the main window are used to manage and access supplemental parts of **License Server**. Many of the subitems are self explanatory (i.e., Licensing, Logoff, etc.) and will not be described in this guide.

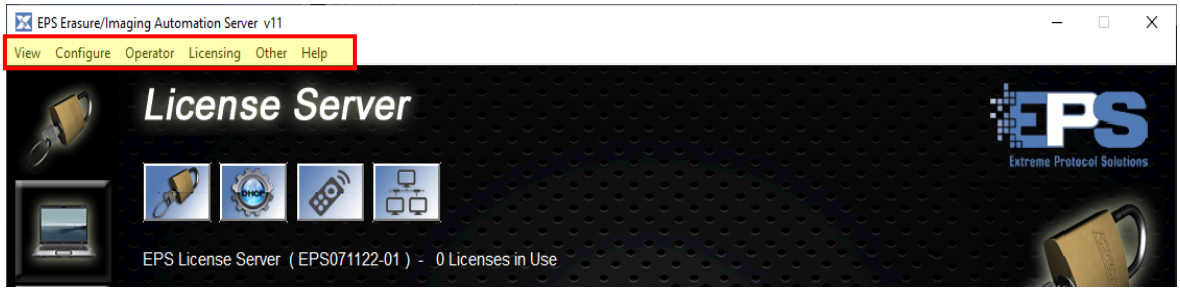


Figure 54 The (Main) Menu Bar

View

The subitems under this selection provide an alternate path to accessing the features included with **License Server** as well as exiting the program. Selecting the feature from the list will call up the first (by default) or the last accessed action of the selected feature if there are multiple activities available. Features that do not have an active license will be greyed out and will not be accessible.

The following table provides a cross reference of the features to their activities.

Listed Feature	Feature's Activities
License Server	Licensing, DHCP, Remote Control, XView
PXE Configuration	PXE Profiles, System Condition, Device Grading, User Fields, DB Scripts
Data Base Configuration	Set Up Database Access
Device Driver Configuration	Device Driver Injection
Burn-In Test Configuration	PassMark's BurnInTest
Imaging Configuration	Model An Operating System, Post Imaging Scripts / Steps
Reporting	Configure Report, Label, QR Code Templates, Create Reports
Exit	Exit (Close) License Server

Table 6 Cross Reference Of The Features In The Menu Bar

Configure

Items under this control are related to additional configurations not directly related to the features described so far. Many are self-explanatory and will not be described in great detail.

Check for updates

Contacts **EPS** and installs available updates to **License Server**. To avoid any issues or incompatibilities, any running activity (i.e., erasures, **BurnInTests**, etc.) should be stopped prior

to installing the updates. Ensure the system **License Server** is running on has an active/stable connection to the internet and that any Windows and/or network security filters are disabled. They can be enabled once the update is completed.

Set Location Data

Presents a window into which identifying information specific to the system License Server is running on is recorded, namely, the **System name**, **System Location1**, **System Location 2**. Once provided, the information will be included wherever that information is required based upon the underlying software framework (i.e., templates, reporting, etc.). This information is independent of the options in **PXE Profiles ➡ Device List**.

Set Client Prompt Values

Presents a window with fields into which four prompts can be provided.

ERP Settings

Integrated into License Server is the ability to interact with some of the more common ERP environments that support the ITAD/ITAM business process. To use this capability, simply select the ERP Interface and supply the information specific to the respective choice when the main window appears.

The following screenshots of the predefined ERP interfaces are provided as a preview of the information that will be required for each interface. Note that the **Erasure Method Check** field may have multiple options specific to the environment and has not been expanded to ensure all the fields of the main interface are properly displayed.

Figure 55 The ERP Environments Included In XErase

Marketplace Settings

This item interfaces to online stores and displays the pricing for selected components. It is a convenient means to find comparative pricing of similar components that have been processed by **License Server**. Additional licensing may be required.

To take full advantage of this tool, ensure the system running **License Server** is connected to the internet and that System Condition Files as well as Device Grading profiles have been set and enabled.

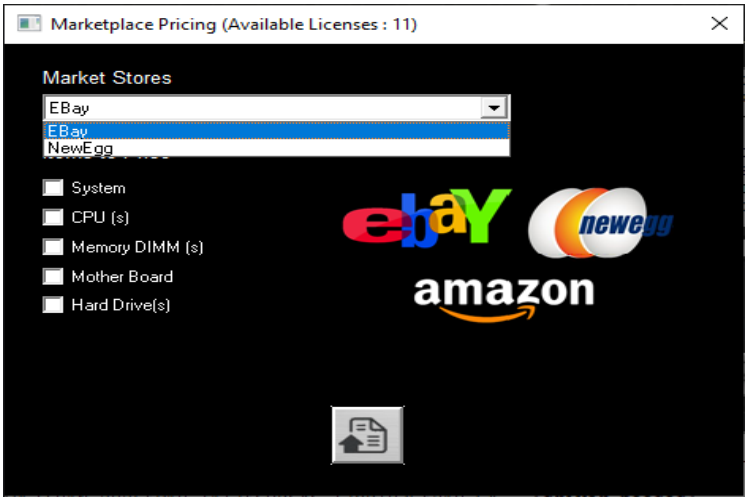


Figure 56 Selecting A Marketplace For Pricing Information

Erasure Method Mapping

The ERP environments illustrated in the previous section all have the erasure mappings included in their databases. **Erasure Method Mapping** is a convenient means to quickly add a new mapping to the ERP database table.

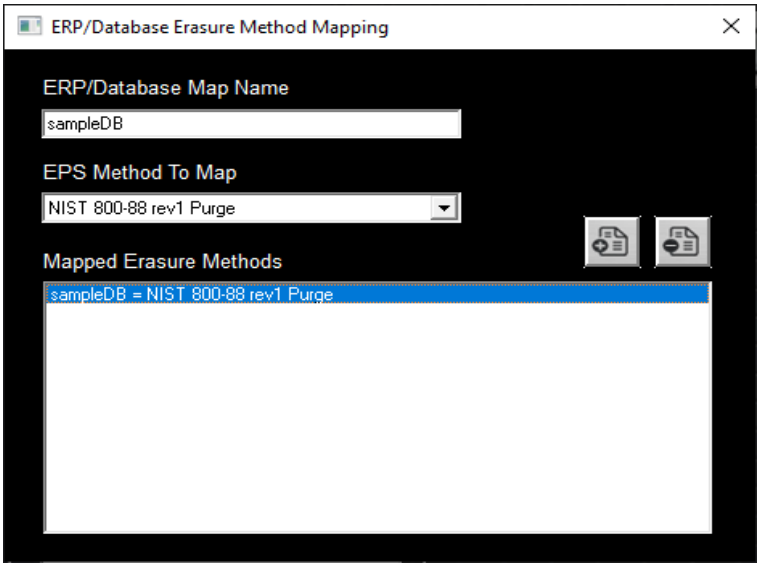


Figure 57 Mapping An EPS Method To An ERP Database

Launch Executable on Startup

Reserved for future use.

Service

Reserved for future use.

Operator

This control item can be used to create or manage accounts and their associated privileges to **License Server**. Once an operator is logged in using their account, their name is attached to each device for any activity performed including reporting. If **Erasure Manifests** are turned on, then operator names are searchable as well making it easy to determine which devices were erased by a specific operator over a certain period.

Login

This control logs a user in and gives them access to the various features and activities within **License Server** based on the privileges their account has been configured for. The only account that exists after installation is, "**Administrator**" with no enabled privileges. New accounts and groups (as well as any updates) must be created with the **Administrator** account. Since this account should have the highest level of privileges, it is highly recommended that the first group to be created be for this account.

A. Creating **Privilege Groups** is a means of classifying ("grouping") accounts to specific sets of features and activities. This is especially useful if adding accounts for a large number of users who will be performing the same activities with the same privileges. Much like templates for reports and labels, they can be viewed as a template of privileges for accounts/users.

> **Note**: There are different ways of creating privilege groups. Using the steps outlined here will ensure the proper privileges are assigned to the correct/desired groups in the most efficient manner possible.

1) Log in as **Administrator** using the default password, **epspw** (all lower case - this is ***case sensitive***). Remember to change this at some point and share it only with select individuals according to your organization's security requirements.
2) The first group to be created should be for the **Administrator** account with all the **Available Privileges** enabled.

Select **Privilege Group** from the dropdown under **Operator Login**.

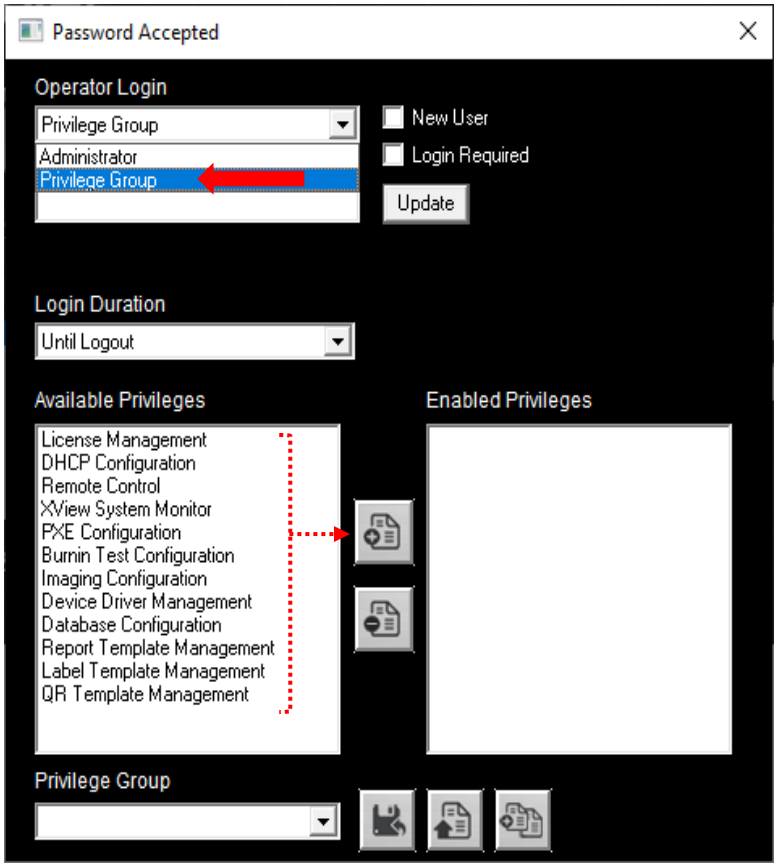


Figure 58 Adding The Admin Privilege Group

3) Starting with **License Management** under **Available Privileges**:
   - Select it.
   - Add it to the **Enabled Privileges** with  .
   - Repeat for the next **Available Privilege** until all the privileges are enabled.

> **Note**: There is no "select all". Each privilege must be selected and added to **Enabled Privileges** individually.

4) Save the privilege group with  and provide a name (**EXAMPLE**: since this is for the **Administrator** account, "**admin**") when prompted - the new name will appear in the field under **Privilege Group** once it has been saved.

5) Assign the group to the **Administrator** account with  .

   All the privileges should still be displayed under **Enabled Privileges** as a result of adding the **admin** privilege group. If they aren't, refresh the list by selecting **Privilege Group** under **Operator Login** and an existing group that has all the privileges enabled (**EXAMPLE**: "admin").

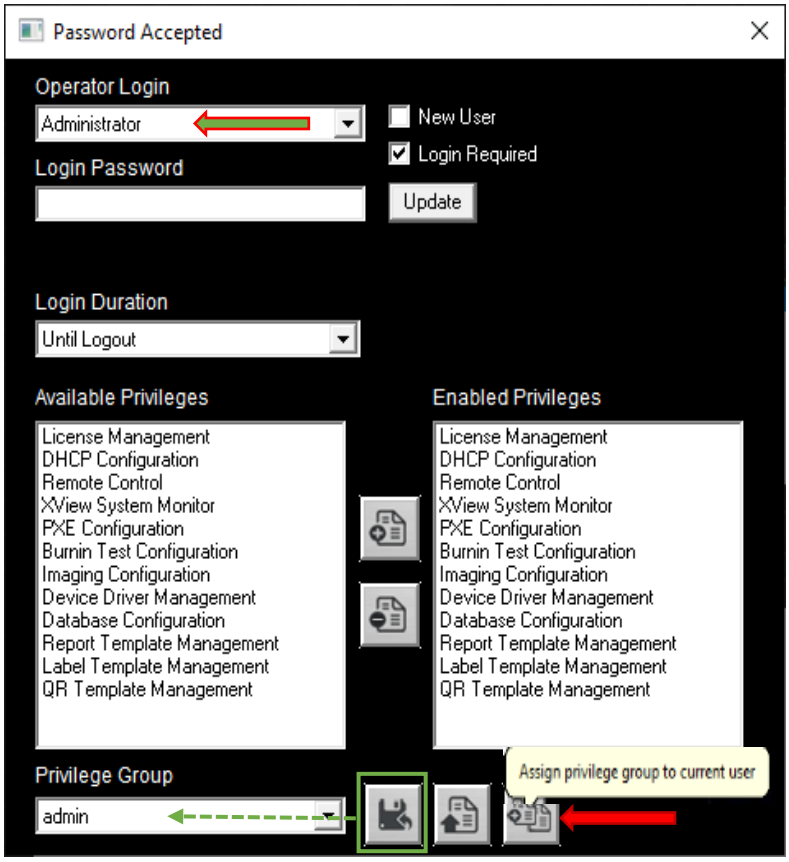


Figure 59 Assigning A Privilege Group To The Adminstrator Account

   If this is to be the only group, close the window. Otherwise, continue.

6) Start the creation of the new/next group by clicking  and providing the name of the new group (**EXAMPLE**: the next group could be for the basic user/operator, "**baseoperator**").

7) Remove the unwanted privileges from the **Enabled Privileges** with  .

8) Once all the changes have been made, update the group's privileges with  .

> **Caution**: Before making or saving any modifications, check the name of the group under **Privilege Group** and ensure the correct group is being updated.

Repeat as often as needed until all the desired **Privilege Groups** with their respective **Enabled Privileges** have been created.

B. Creating An Account – if not already, log in as **Administrator** and provide the password when prompted.

1) Click the **New User** checkbox as well as whether logging is required.

> **Note**: Leaving **Login Required** unchecked allows the user to perform the activities without logging in.

2) Type the name of the account for the user in the **Operator Login** field.
3) Set the password for the account.

   Remember, this is ***case sensitive***. When notifying the user of their new account, advise them of the password **exactly** as it was set as well as that it is case sensitive.

   Finally, create the account with [Add].
4)

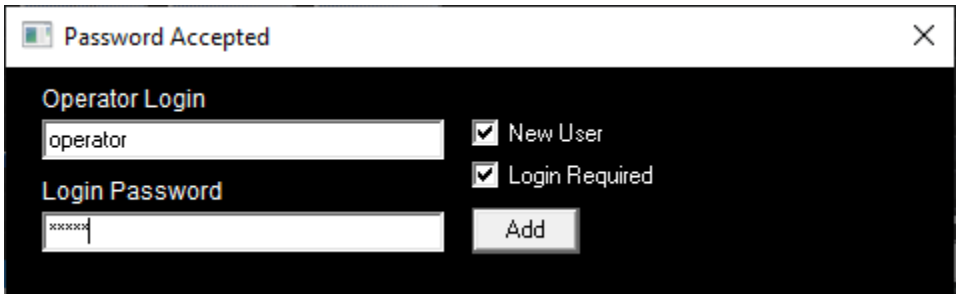


Figure 60 Setting An Account's Credentials

C. Updating The Account And Assigning A Privilege Group

1) Uncheck **New User** and select the newly added account from the dropdown under **Operator Login**.
2) Select the **Login Duration**.
   - Until Logout
   - Time Limit (enter time in minutes)
   - Drives Started (must enter quantity)

   If any changes are made, save them with [Update].
3) Select the group the account is to be a member of from the dropdown under **Privilege Group**, then assign the account to the group with  .

Logout

Logs a user off.

Licensing

Update License Key

Only use this item when directed to do so by **EPS** support.

Transfer Cloud Licenses

Once an account and password has been created on the **EPS** cloud, enables transferring any active licenses to/from a hardware dongle to the cloud and vice versa.

Contact **EPS** with any questions related to licensing.

Other

Upload Sys Info Database

Reserved for future use.

Upload Drive Info Database

Reserved for future use.

Get Beta XERASE for PXE

Use only when directed by **EPS** support.

Help

The version of **License Server** installed, links to documentation and support as well a means to access the error (aka, "debug") log can be found within this selection. A link to the documentation as well as new changes, new features and fixes to bugs will also be included whenever **License Server** is updated.

Here is a general description of each of the items.

Version N.x.y - Displays the version of **License Server** currently installed on the system. Version numbers ending with a suffix of "b" (i.e., 8.9.0**b**) are "beta" (not production yet) and should only be installed when directed to do so by **EPS**.

Open Documentation - Access the user guide (this document). Using **File Explorer**, look in **c:\LCServer\PDF**.

Open Notice - Reserved for future use.

Open LCserver Changes - Opens the latest updates to License Server.

Support Request - Connects to the **EPS** website and opens the form requesting support. Fill in the fields, then click ***send***.

Support can also be requested via:

Phone - (508) 278-3600

Email - support@extremeprotocol.com

Knowledge Base - Searches the EPS database for information related to bugs, tips on usage, technical specifications, etc.

Feature Request - Complete the form and submit it. The request will be reviewed and considered for inclusion in a future release or bug fix.

View Error Log - One of the ways of accessing the “debug” log (LCServer.log). Any requests for support should include this log to assist the EPS support team in determining if there is an issue and how to assist in resolving it.

Appendix A – Installing License Server

Use the following steps to perform a new installation (or reinstallation).

Launch The Installer

1. Download and launch the installer (http://enterprisedataerasure.com/software/setup.exe).
2. Once the installer is opened, confirm that **Web** is (pre)**selected**. If anything other than **Web** is preselected by default or the installer is all "grayed out", the system the installer is running on may not be connected to the network (aka, the internet). Close the installer and correct the issue before proceeding.

Figure 61 Selecting License Server In The Installer

3. Click in the field (or the dropdown arrow) to the right of **Product** and select **EPS License Server / PXE platform** from the choices.
4. Ensure **Version** is still defaulted to **Official Release**, then click Install. Watch the installer as it may update itself, then restart.
5. Close the installer once the desired product is installed using either **File -> Exit** or by clicking the **X** in the upper right corner of the window.

Start License Server

1. Start **License Server** either as specified in the installer or open File Explorer, navigate to **c:\LCServer** and double click LCServer.

   During startup, **License Server** checks to see if updates are available. If any exist, a window labeled, **Product Updates Are Available**, will appear.

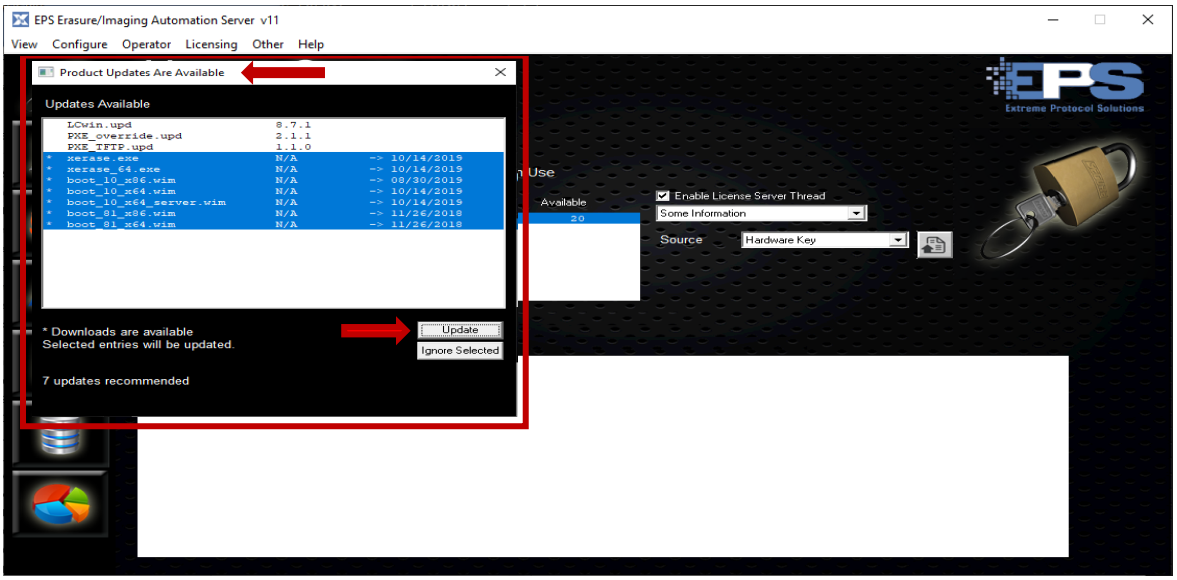


Figure 62 Installing Updates

2. Click Update and allow the update to complete. The window will close itself once it is done.
3. Confirm the source for the license. If it needs to be changed, select the correct source from the list in the drop down next to **Source**, then, before clicking another action/icon or any other area of the window, remember to save ( ) the update.

> **Note**: Note the number of licenses. If the number under the "Available" column is "0", close **License Server** and review the licensing requirements. At least one license to "**XELTwin**" must be installed and available before erasures can be performed on the client. Refer to "Prerequisites" for further assistance.

Continue with setting up DHCP. If configuring DHCP "from scratch", continue with the following.

Reconfiguring DHCP

Prerequisites:

- Identify/note the interface, and its address, used by the system to connect to the infrastructure (i.e., "the internet"). Do ***not*** use the IPMI interface for the following steps.
- Identify/note the interface to be used by the system for the PXE network. An address is usually assigned a few seconds after a cable is connected to the port as well as the switch (i.e., output of the command, ***ipconfig***).

Additional hints and troubleshooting tips can be found in **Appendix A** of the **License Server, Quick Start Guide**.

To configure DHCP for the PXE network from scratch, perform these steps:

1. Close **License Server** and delete ***c:\LCServer\config\dhcp.ini***.
2. Open ***Windows Settings*** -> ***Network & Internet*** -> ***Ethernet*** -> ***Changer adapter options***.
3. For the respective PXE interface, ***right click*** -> ***Properties*** -> ***TCP/IPv4*** -> ***Properties*** then select:
   - ***Obtain an IP address automatically*** (the address and netmask should disappear)
   - ***Obtain DNS server address automatically*** (any existing addresses related to DNS should disappear)
4. Confirm the ethernet cable to be used for the PXE network is connected.
5. Start **License Server**, click  then  and respond to the prompt to autoconfigure.
6. Select the interface for the PXE network, then select ***Active*** from the drop down to the right, and ensure **Enable DHCP/TFTP** is checked/selected, then  .

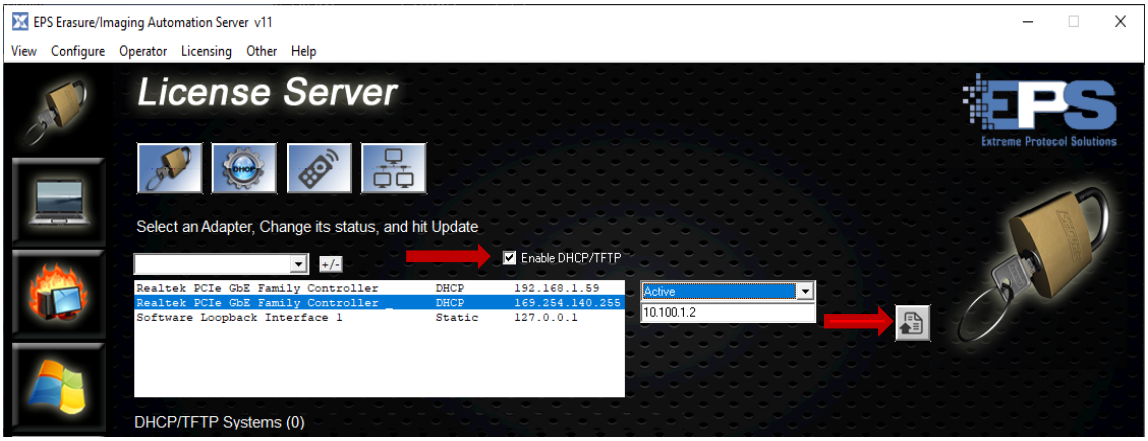


Figure 63 Reconfiguring DHCP - Selecting The Network

7. The results of the attempt will be displayed. Anything other than "**DHCP Ready**…**TFTP Ready**…" will require further research and repeating the steps from the beginning.

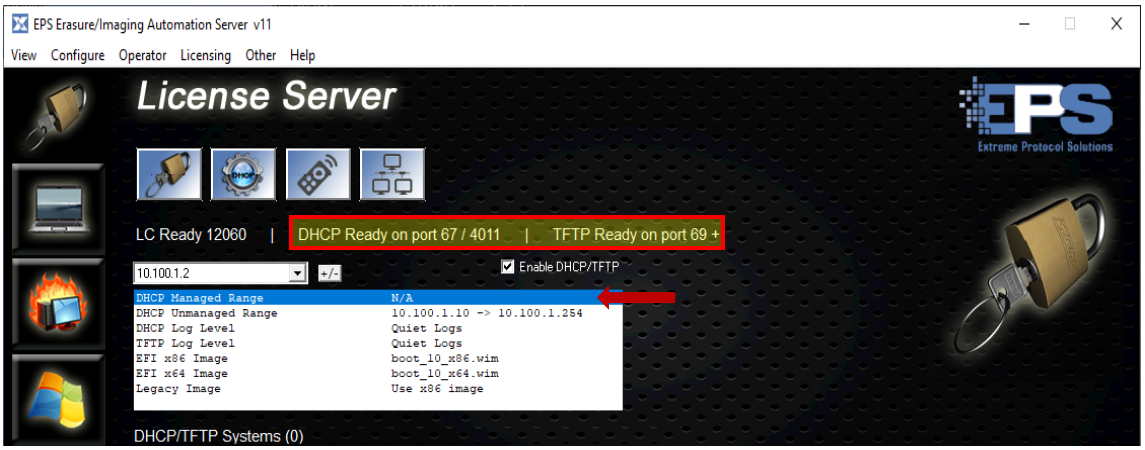


Figure 64 Confirming DHCP Is Configured And Active

Appendix B – HP ProCurve Managed Switches

General Information / Overview

When establishing a PXE network for the first time, the recommendation is to keep the configuration as simple as possible and expand it using additional switches as needed. In its simplest form, a network can be established using just a small unmanaged ("dumb") switch to connect the **License Server** to its clients. In this configuration, the maximum number of clients is restricted only by the number of ports available on the switch. Once the number of clients grows larger than available ports on the switch, the network can be expanded by adding additional (aka, "fanning out", a means of expansion) unmanaged switches or managed switches, the latter requiring some additional knowledge and skills to configure.

All managed switches are expected to be either directly connected to the host port or connected via an unmanaged switch acting as a fanout hub if multiple managed switches are required. Using the unmanaged switch scheme simplifies connectivity for startup.

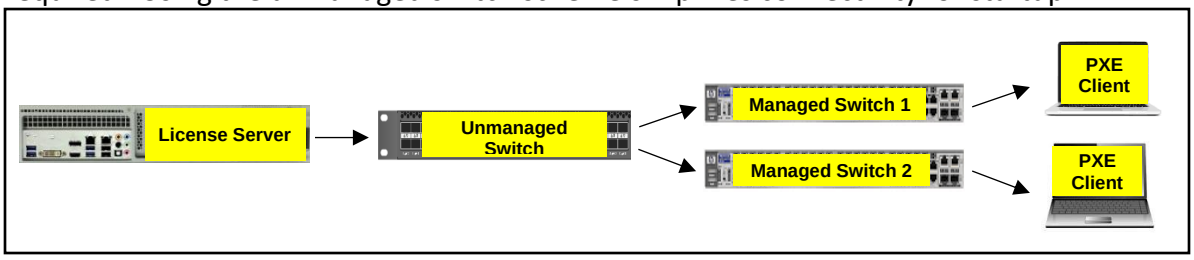


Figure 65 A Network With Multiple Switches

The port that connects the managed switch to the host/unmanaged switch should be the **last** port on the switch to simplify client addressing. For example, if using a 48 port switch, use port 48 to uplink to the **License Server** port and ports 1 through 47 for PXE clients. Adding a second managed switch would repeat that process of connecting the last port of the managed switch to any of the ports on the **un**managed switch.

Although it is **not recommended**, if daisy chaining the managed switch(es) becomes **necessary**, plug one end of the cable that will be used to connect the next managed switch into port 47 of the existing switch and the other end into port 48 of the new/next managed switch. This will require manually editing **c:\LCserver\config\dhcp.ini** and the switch definition file to reduce the number of clients. Contact support@extremeprotocol.com for further assistance.

There are two modes of network operation, both of which are in IPv4 format – "big network" which uses the format **10.Y**.x.x, giving a maximum of 65525 clients on that port, and the older "smaller network" format of **10.100.Y**.x with a maximum of 245 clients. "Y" is unique per **License Server** port, while "x" indicates a possible client address. Even though it's possible to have huge numbers of clients on a "big network", it is not practical due to memory usage and other overhead associated with tracking all of them.

Sample addressing schemes in the two formats follow.

Format	Port#	Default Port IP address	Client Range
Small	1	**10.100.1.**2	**10.100.1.**10 – **10.100.1.**254
Small	2	**10.100.2.**2	**10.100.2.**10 – **10.100.2.**254
Small	3	**10.100.3.**2	**10.100.3.**10 – **10.100.3.**254

Format	Port#	Default Port IP address	Client Range
Big*	1	**10.100.**0.2	**10.100.**0.10 – **10.100.**1.254
Big*	2	**10.101.**0.2	**10.101.**0.10 – **10.100.**1.254
Big*	3	**10.102.**0.2	**10.102.**0.10 – **10.100.**1.254

***** - Big is still under development.

Figure 66 Examples Of A Small And Big Network Addressing Scheme

In the following instructions, replace any references to 10.100.1.2 with the appropriate IP address of the PXE port of the system running **License Server**. If using an **un**managed switch to fan out to managed switches, confirm the following prerequisite steps are are completed.

1. Disconnect any/all ethernet cables in the ethernet port(s) to any managed switch(es). Any network connections should be ***only*** to the ***un***managed switch(es).
2. Configure the **EPS** monitor (see **XView**).
3. Ensure **License Server** is running and that DHCP and TFTP are active/enabled.
4. Open **XView** and configure it (6 rows x 10 columns to start with), make any other adjustments desired, then click  to display the grid.
5. Click the  beneath **Interface Configuration Files** to save the configuration.
6. Plug in the ethernet cable from the unmanaged switch to port 48 of the managed switch.
7. Wait a couple of minutes for all DHCP requests to be satisfied as the switch is being recognized (represented by the hour glass).
8. Right click over the DHCP (hourglass) entry and choose, "Mark as **un**managed switch", which will move the switch(es) into a hidden IP address range and immediately display a confirmation message containing the relevant information.

Guidelines For Connecting To And Setting Up The HP Procurve Switch

A. Reset The ProCurve To Factory Defaults: A factory reset will flush out any configuration set within the switch when it was last used. Two paper clips (or similar small thin objects) that have been straightened will be required in order reset the switch back to factory defaults. Some models may have small raised buttons and may not require the use of the paperclips.

1) Do not have the network port attached to the **ProCurve** yet.
2) Insert the end of one paper clip into the opening labeled **reset**.
3) Insert the end of the second paper clip into the opening labeled **clear.**
4) Gently push **both** in simultaneously.
   - If the LEDS all light up, the reset is in progress.
   - If the LEDs do not light, repeat steps 2 and 3 ensuring both buttons are pushed in ***at the same time***.
5) Release the **reset** button while still holding down the **clear** button.

6) The **Aux/PS/Tmp/Fan/Test** LEDs should turn orange, after which the **Test** LED should start blinking.
7) Release the **clear** button and wait while the switch performs a self-test.
8) The self-test will be complete when the LEDs for the ports along with the **Test** LED turn off. The self-test will take approximately two minutes to complete.

   Refer to the abstract or the complete guide for the switch on the HP's support website (https://support.hpe.com) for further details.

B. Configure And Connect The System's Serial Port: Review the system running **License Server** you will be connecting to the switch from and confirm a "serial/RS232" (aka COM) port is available. Many systems (i.e., desktop workstations, servers, non-laptop) will have an onboard 9 pin serial port similar to "**1**" below. Alternatively, any system can use of a USB adapter ("**3**" or "**5**" of figure TBD). The Procurve referenced for the following was connected using the RJ45-to-USB ("**5**") serial cable.

1) Identify and note the correct "COM" port within the operating system (i.e., on Windows, via **Device Manager**) to use, especially if there are multiple ports (COM1, COM2, etc.) available.
2) Acquire a suitable serial cable similar to one of the examples in the following figure and connect one end to the system/**License Server** being used as the console. Connect the other end to the port labeled, "Console" on the **ProCurve**.

Figure 67 Pictures Of RS232/Serial Connectors And Cables

3) Download and install **PuTTY** from the website.

4) Open **PuTTY** and configure these required settings.

- Expand the **Connection** tree, select **Serial** and confirm that the settings for the COM port (from **step 1)** to be used are set as follows.

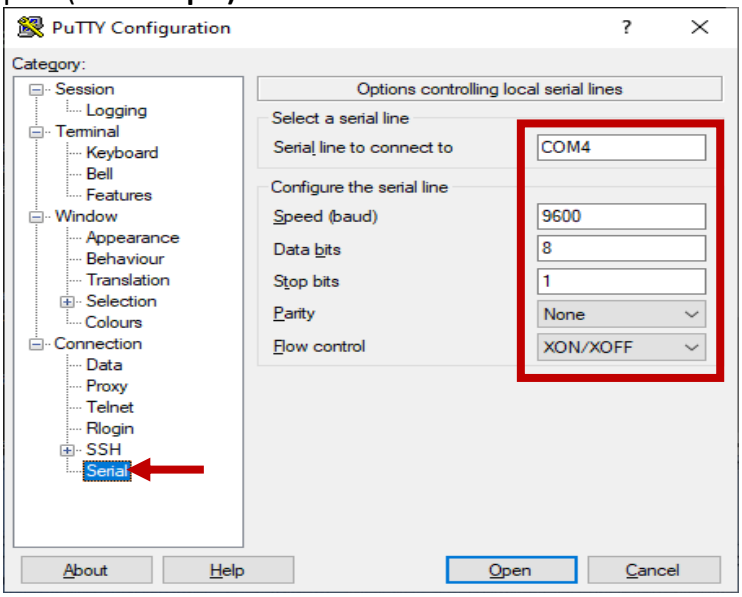


Figure 68 Configuring The PuTTY Connection

- Change the terminal's keyboard type to **VT100+**
- Select **Serial** as the session's **Connection Type**. The **Serial Line** as well as the speed should be automatically set to the one defined previously.

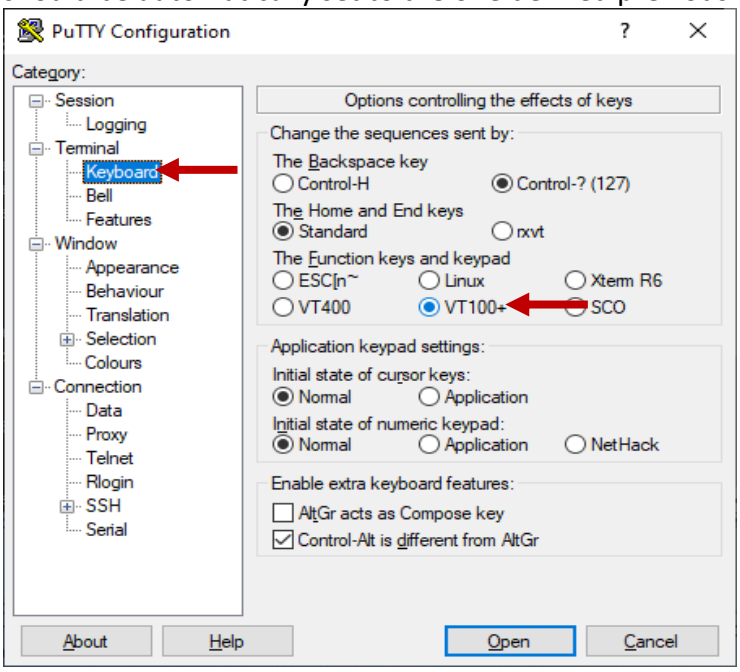


Figure 69 Selecting The Keyboard For The PuTTY Session

– Click **Open**.

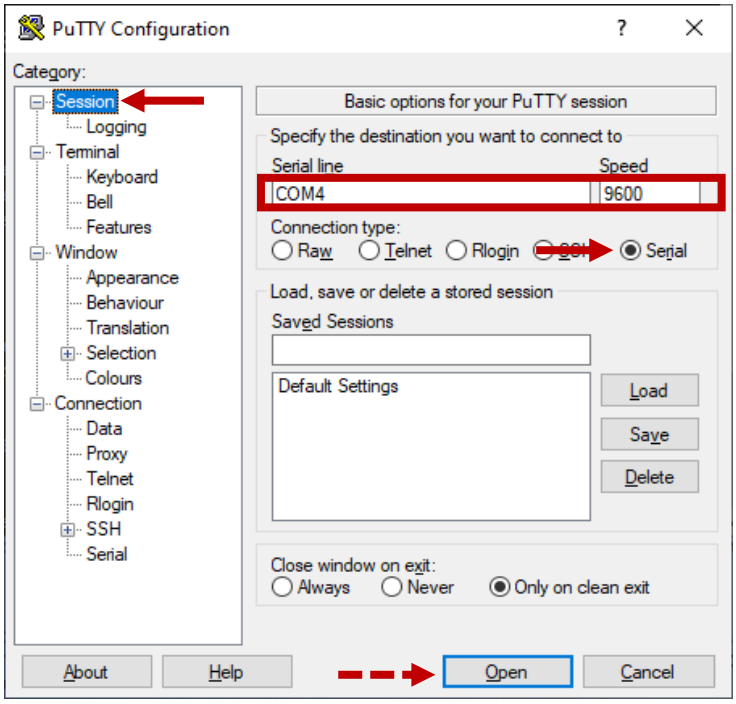


Figure 70 Opening The PuTTY Connection

5) Wait a few seconds, then press ***ENTER*** two or three times until a message showing the baud rate (**Speed** in the above) is displayed. Continue to press the ***ENTER*** key occasionally until the banner appears, then follow the prompt ("…press any key…") until ***ProCurve Switch 6600ml-48G-4XG#,*** or similar output representing the model of your switch, appears on the console (window).

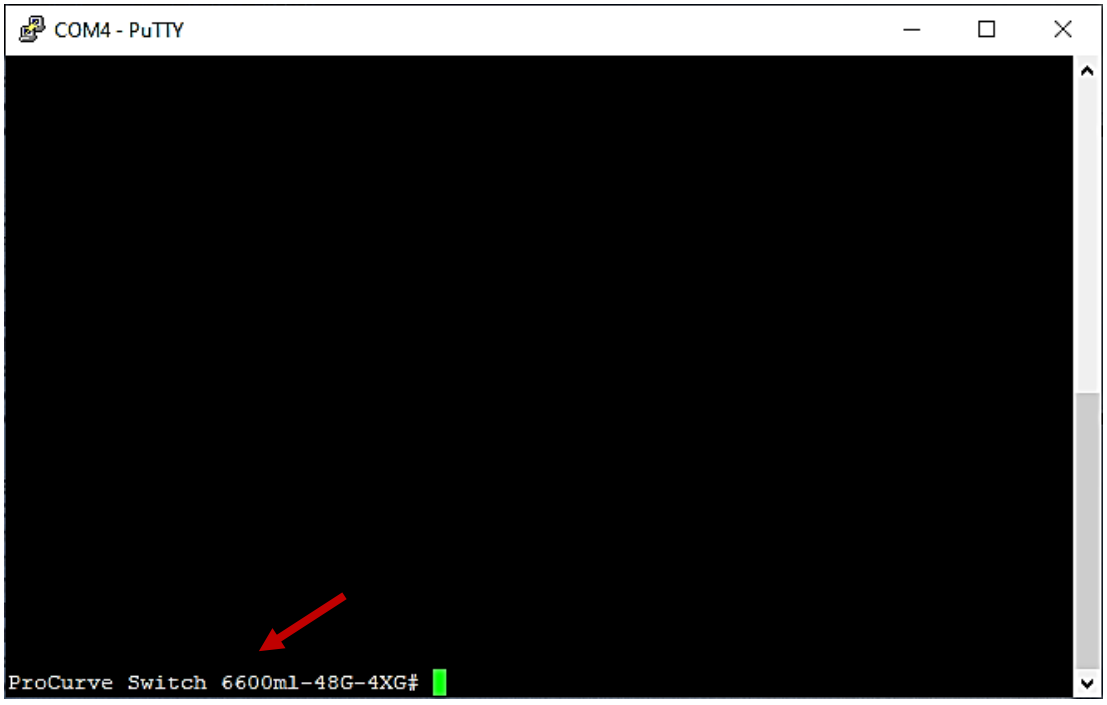


Figure 71 The Console Window/Session To The ProCurve Switch

C. Configure The ProCurve Switch: Most serial console sessions are not capable of displaying graphical GUI (**g**raphical **u**ser **i**nterface) output and will usually have an ASCII (aka, "text") version of the output. Since they will not recognize the existence of a mouse either, navigation is accomplished with either the ***tab*** key or the ***up, down, left, right arrows*** keys on the keyboard.

Once the console window appears:

1) Type ***setup*** and press ***ENTER***.
2) Go to the **System Name** field and change it to ***Procurve1*** or a name unique to the switch which will help identify it once in use, especially if there are other similar switches in use.
3) Go to the **Manage Password** field and type in, ***EPSpw1234!*** (exactly as displayed; note case sensitivity).
4) In the **Confirm Password** field, type in the same password (***EPSpw1234!***).
5) Review the **IP Config** field and confirm it is set to **DHCP/Bootp** so **License Server** can detect and configure that protocol. If it isn't, navigate to it and change it to **DHCP/Bootp**.
6) Follow the prompt at the bottom of the screen to **go to Actions**, then right arrow to **Save**. Once the setup is saved, the menu is exited and the command prompt will return.

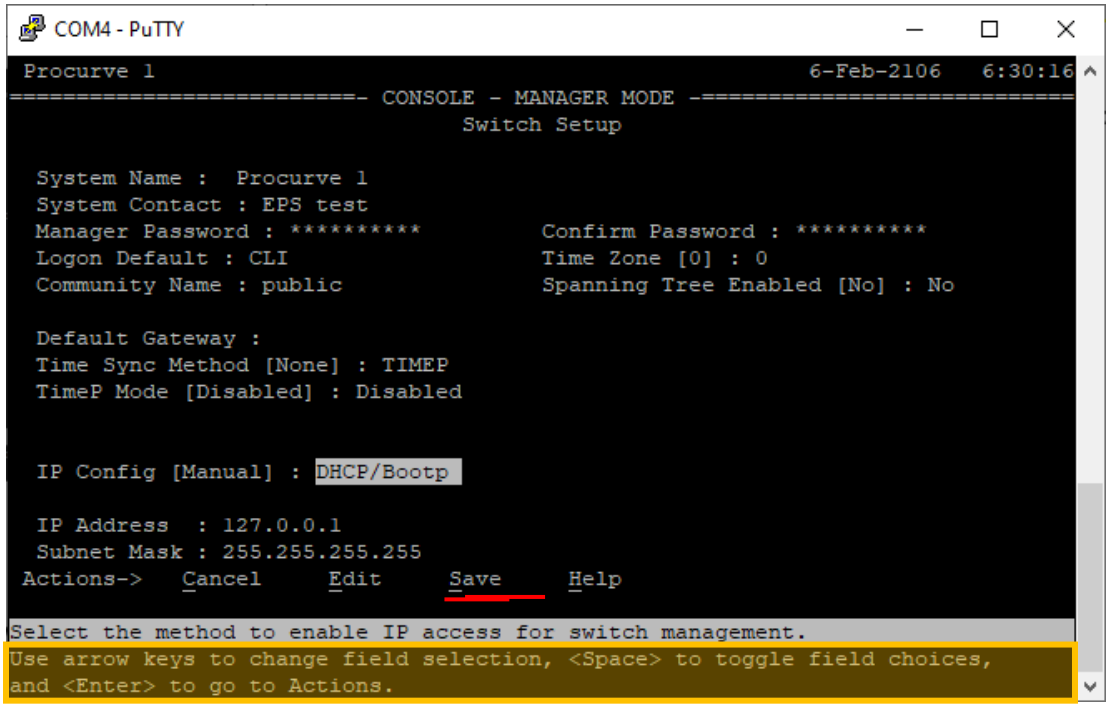


Figure 72 Saving The ProCurve's DHCP Settings

7) Configure the switch - type ***configure***, press ***ENTER***.

The prompt will change to 

8) Set up the snmp server – type the following:
   - ***snmp-server enable*** press ***ENTER***.

- ***snmp-server response-source 10.100.1.2*** press ***ENTER***.

> **Note**: Ignore the error message, "Warning: Specified IP address is not configured on any VLAN."

9) Display the configuration and confirm the above information was set correctly with, ***show snmp-server*** press ***ENTER***.

10) Follow the instructions displayed at the bottom of the page for going to the next page and confirm the settings for **Snmp Response Pdu Source-IP Information** are set as displayed in the following figure.

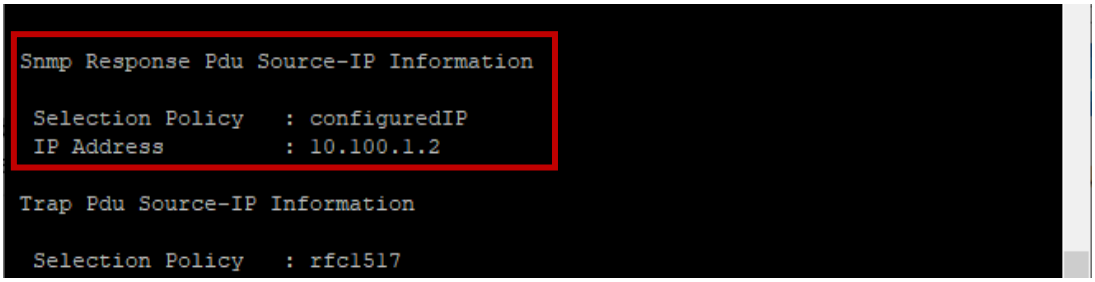


Figure 73 Viewing The ProCurve SNMP Response Settings

11) Type, ***ip authorized-managers 10.100.1.2,*** press ***ENTER***.

12) Type ***show config*** press ***ENTER*** and confirm the settings are set as required.

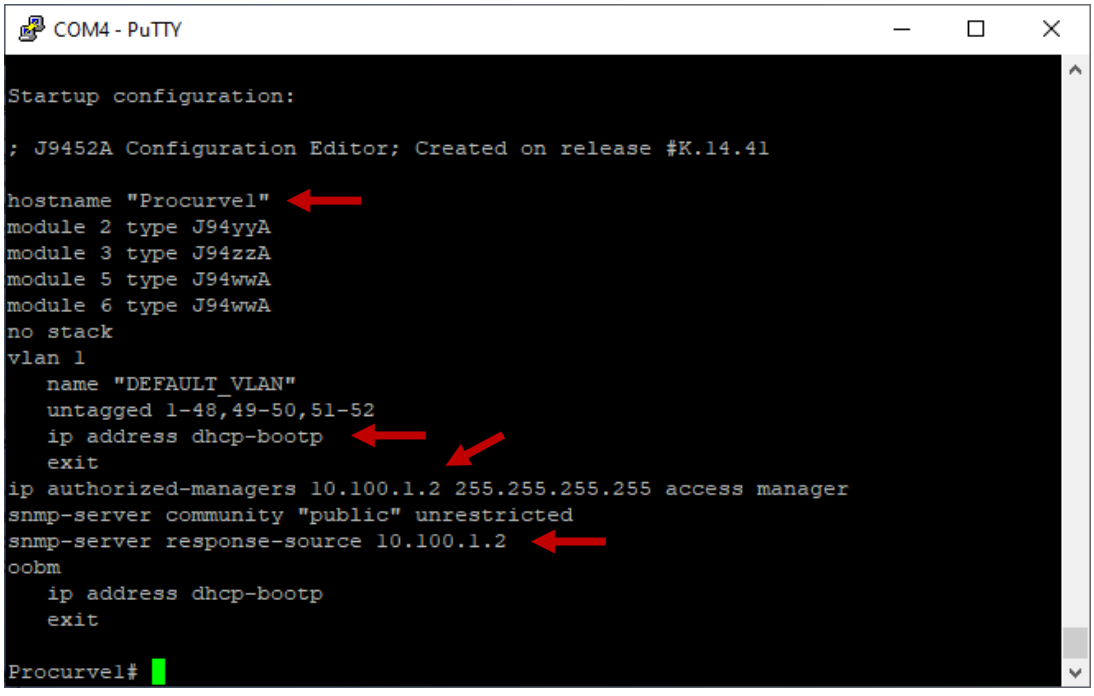


Figure 74 Viewing The ProCurve Configuration

D. Converting The DHCP Client To A Managed Switch

1) In the system monitor (**XView**) window, the ProCurve should have requested an IP address and been given the first available client address (10.100.1.10).
2) Right click over the hourglass representing the switch, then select ***MARK as Managed Switch***. A message confirming the managed switch, **Procurve1**, was added as a managed switch should be displayed.

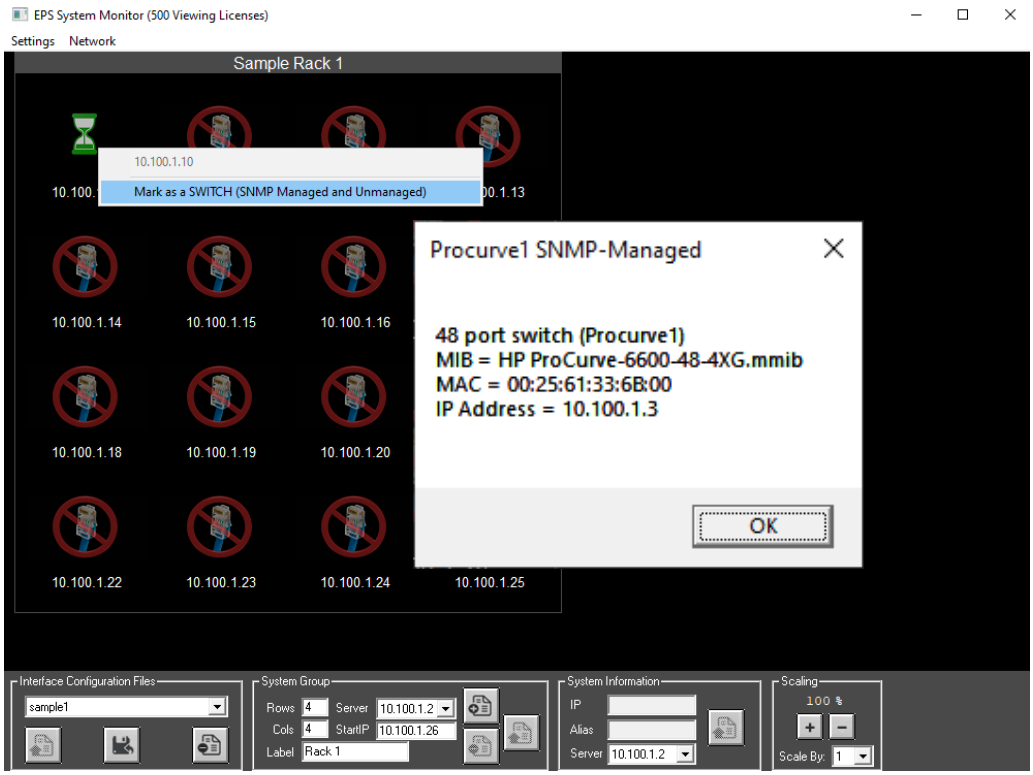


Figure 75 Adding The ProCurve Switch To XView

3) Return to the PuTTY console window and type ***setup***.
4) Set **IP Config** to **Disabled** by pressing the ***space bar*** twice.
5) Press ***ENTER*** then navigate with the ***right arrow*** to ***Save*** and press ***ENTER***.
6) Return to the **XView** window. Within 10 seconds (or so), go to **Network Menu** and select **Switch Summary**. It should indicate that 10.100.1.3 is **UP** along with its configuration.

```
Network Port 10.100.1.2 (MAC) <- License Server
--------------------------------------------------------------------------------
UP  10.100.1.3  00:25:61:33:6B:00 (Model)  10.100.1.10-10.100.1.57 (Hostname)
```

Figure 76 Displaying The Network Information

Note: Because of the volume of output, the actual model and hostname in the above figure was removed to ensure the figure is readable).

Optional – Changing To A Static Address: The switch (in DHCP mode) requires **License Server** to be running in order for it to get its IP address and configure its subnet. If the switch powers up, or renews an IP address while **License Server** is not running/responding, the switch could have issues.

Setting the switch to a static IP after the **License Server** has been configured will decouple them. However, the switch should always work no matter the state of **License Server**. Use the following steps to disabled DHCP and assign static addresses.

Open **PuTTY** and connect to the switch via the console serial port.

1) Press ***ENTER*** and when prompted for the password, ***EPSpw1234!***
2) Type ***setup***.
3) Navigate to **DHCP/BootP** and press the ***space bar/key*** to toggle/change the entry to **Disabled**.
4) Press ***ENTER*** then navigate with the ***right arrow*** to ***Save*** and press ***ENTER***.
5) Type ***setup***.
6) Navigate to DHCP/BootP and press the *Space key* to change the entry to Manual.
7) Type the IP address that you pinged earlier (also in server_0_switchlist.txt), type the subnet (255.255.255.0 for small, and 255.255.0.0 for big).
8) Press the *Enter key*.
9) Navigate to Save and press ***ENTER*** *key*
10) Logout by closing the PuTTY window.

Repeat the process as necessary if adding additional managed switches.

Appendix C – Databases

Database Notifications

When setting up the database, once all the desired fields have been mapped, verify that the current and (potential) future requirements for **XErase** have been mapped with  and remediate any notices that are displayed. The "REQUIRED" notices ***must*** be resolved before using the database.

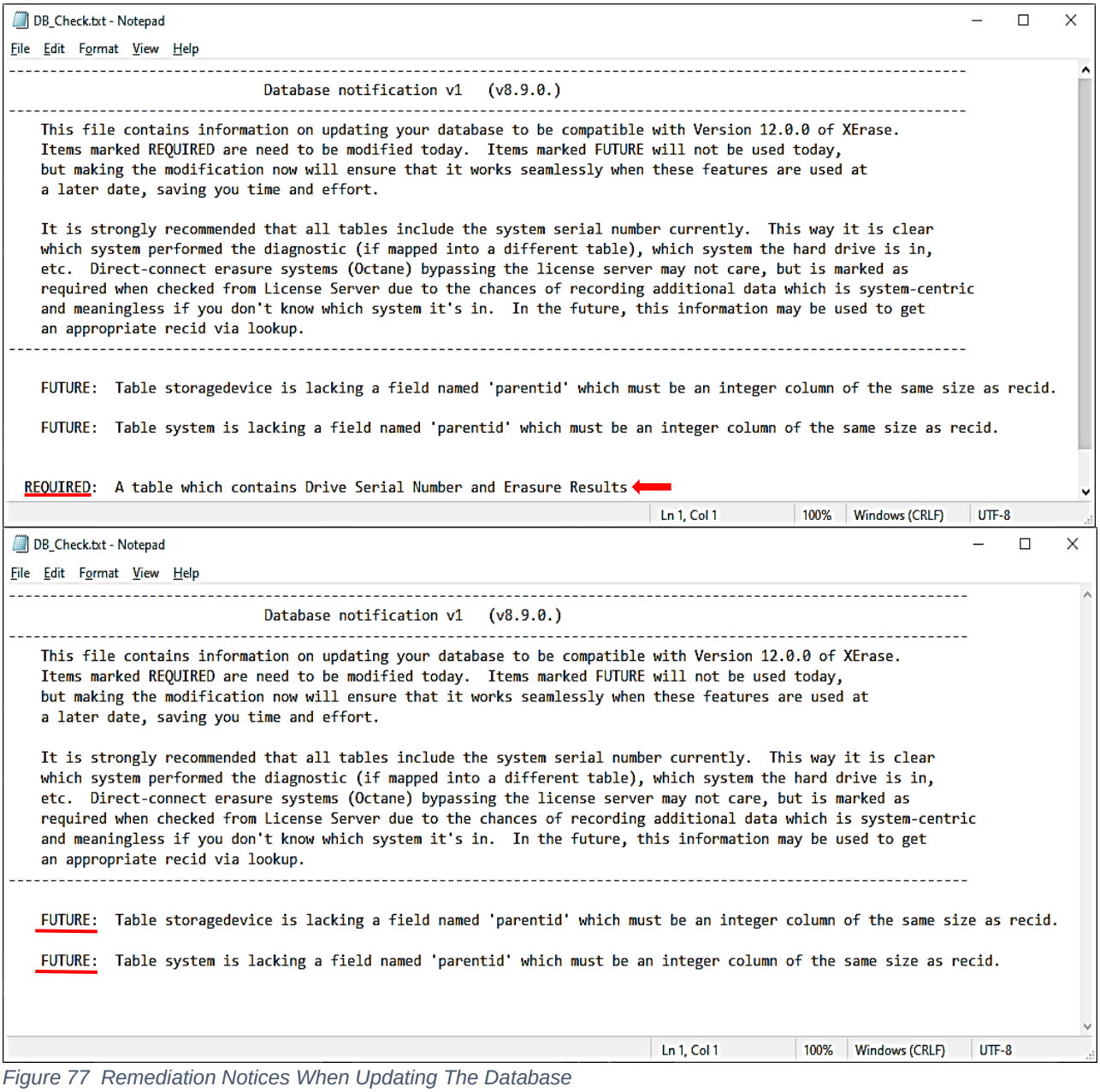


Figure 77 Remediation Notices When Updating The Database

Appendix D – NIST Erasure Methods And Standards

The following table provides a brief summary of the different actions included in the options of the **Secure Filter** depending on the type of drive. This information may also be displayed on the report based on the type of method used to erase the drive(s) and if that element is included in the report.

NIST Purge Filter	Action Performed
Sanitize Blockerase - SSD	All blocks ereased, including currently unmapped blocks.
Sanitize Overwrite – HDD	One or three passes of repeating data to the entire media. Number of passes is dictated by the Clear, 3x Overwrite setting.
Sanitize Cryptographic Erase	Changes the encryption key on the device. A device may also choose to blockerase over overwrite the media afterwards so that nonrandom data is visible on the disk.
Secure Erase (Enhanced) – HDD	Drive erases all blocks on the media
NVMe Format / Crypto	NVMe drive erases itself either by clearing the data, changing the cryptographic key or both.
Note: After the purge is complete, a seeded verify test will be performed in addition to a minimum 2500 block spot verify unless the user specifically chooses a full media verify or a NIST Slice verify option for more coverage.	

Extreme Protocol Solution's **Enterprise Data Erasure** software is an engine that will perform the actions defined by a wipe method, which can be easily defined and expanded as needed. As a result, the list below is only a starting point to what the software can be configured to do.

All storage erasures listed below will include some level of verification which takes place after all erasure passes that is controlled by software settings unless specifically shown in a method. Firmware based erasure methods are verified by validating against known data in a random selection of blocks to ensure that the storage device did implement the method, which is in addition to the verification mentioned above. For example, a NIST 800-88 rev1 Purge would implement the following: 1 Seed + 1 FW (Purge) + 1 SeedVfy + 1 Verify.

Firmware Based Erasure	(All firmware erasures pre-seed known data and verify change in addition to other verification methods)
NIST 800-88 rev1 Purge	One of Sanitize Overwrite, BlockErase, Cryptoscramble, SE Enh (hard disks), NVMe Format or Opal Revert
NIST 800-88 rev1 Clear	One of Secure Erase/SCSI Format or 1x/3x manual overwrite as configured
Secure Auto	One Firmware Erasure
BSI-GS	One Aperiodic Random + one Firmware Erasure
BSI-GSE	Two Aperiodic Random + one Firmware Erasure
Secure Auto + 1x DoD	One Firmware Erasure + 1x manual overwrite (CB)
Secure Auto + 3x DoD	One Firmware Erasure +3x manual overwrite (EB/14/repeating random)

Manual Overwrite	
1x Wrt/Vfy - NIST Clear/Verify	1x write (repeating random)
1x Wrt/Vfy - DoD Clear/Verify	1x write (5C)
3x Wrt/Vfy - DoD Sanitize	3x write (EB/14/repeating random)
4x Wrt/Vfy - DoD 5220.22M+	4x write (EB/14/repeating random/repeating random)
DoD 5220.22-M 3X Sanitize	3x write (repeating random/FF/00)
DoD 5220.22-M 5X Sanitize	5x write (repeating random/EB/14/FF/00)
DoD 5220.22-M 7X Sanitize	7x write (repeating random/4C/B3/EB/14/FF/00)
3x Wrt/Vfy - NAVSO Purge No Format	3x write (FFFFFFFF/27FFFFFF/repeating random)
1x HMG CCITSEC	1x write (00)
3x HMG CCITSEC	3x write (00/FF/repeating random)
HMG Infosec 1X	1x write (00)
HMG Infosec 3X	3x write (00/FF/repeating random)
1x Write - GOST R 50739-95	1x write (repeating random)
2x Write - GOST R 50739.95	2x write (00/repeating random)
1x Write - ISM 6.2.92	1x write (repeating random)
3x Write - ISM 6.2.92	3x write (repeating random/repeating random/repeating random)
1x Write - NZSIT 402	1x write (repeating random)
3x Write - VSITR	3x write (00/11/repeating random)
7x Write - VSITR	7x write (00/11/00/11/00/11/repeating random)
7x Write - RCMP TSSIT OPS-II	7x write (00/11/00/11/00/11/repeating random)
BSI-2011-VS	1x write (FF) + Verify + 1x write (00) + Verify
1X Zero Drive	1x write (00)
2x Random	2x write (repeating random/repeating random)
3x Random	3x write (repeating random/inverse repeating random/repeating random)
5x Wrt/Vfy	5x write (00/FF/EB/14/repeating random)
7x Wrt/Vfy	7x write (00/FF/EB/14/AA/55/repeating random)
Verification Methods	
Verify Disk Fully	Verifies every block on the disk regardless of settings
Verify Disk	Verifies the disk based on software configuration settings (NIST/Spot/Full)
NIST 800-88 Verify 10 pcnt	Verifies 10% of the media using the NIST 800-88 Slice process

NIST 800-88 Verify 5 pcnt	Verifies 5% of the media using the NIST 800-88 Slice process
NIST 800-88 Verify1 pcnt	Verifies 1% of the media using the NIST 800-88 Slice process
NIST FF Verify 5 pcnt	Verifies 5% of the media using the NIST 800-88 Slice process against a pattern of FF
NIST ZERO Verify 5 pcnt	Verifies 5% of the media using the NIST 800-88 Slice process against a pattern of 00
Other	
Secure Lock	Uses the Secure spec to Lock a compliant ATA disk for transport
Switches	
NIST 800-88 rev1 Purge	Manufacturer dependent
NIST 800-88 rev1 Clear	Manufacturer dependent
Cisco Secure Erase	For vendors enrolled in the Cisco program, erases the switches thoroughly for reprocessing

Glossary Of Acronyms

Credits: Most of the meanings for the following are taken either directly or indirectly (reworded) from Wikipedia and applicable web sites.

AWBDITG - **A**cronyms **W**ill **B**e **D**efined **I**n **T**he **G**lossary: this page

AHCI - **A**dvanced **H**ost **C**ontroller **I**nterface: A general technical standard defined by Intel that defines how Serial ATA controllers should work.

BIOS - **B**asic **I**nput **O**utput **S**ystem: Preinstalled software that controls how hardware is initialized and interfaces to the operating system.

CSV - **C**omma **S**eparated **V**alues: A file containing comma separated values to deliminate data. The contents are commonly imported into databases. It can also be opened with a spreadsheet application in which case, the commas become the borders of the cells.

DB - **D**ata**b**ase: A software "container" that contains information ("data") organized by tables, inside of which the data is held.

DHCP - **D**ynamic **H**ost **C**onfiguration **P**rotocol: A means of automatically assigning IP addresses to clients as they join/are connected to a network.

DoD - **D**epartment **o**f **D**efense: The governmental body that originally established the (rigorous) standards for sanitizing their own drives which were then adopted by the private sector.

DNS - **D**omain **N**ame **S**erver: The TCPIP method of mapping human recognizable names (i.e., websites, hostnames, etc.) into their IP addresses/numbers.

ERP - **E**nterprise **R**esource **P**lanning: An integrated set of (usually software) tools that helps an organization plan, implement, document and project a forecast for their business, among other uses/objectives.

HTML - **H**yper **T**ext **M**arkup **L**anguage: Text that is written between a set of "<TAG>" (open) and </TAG>" (close) that formats/determines how a web page looks in a web browser.

IP - Short for TCP**IP**: The set of rules that allows computers to connect to and communicate with each other.

IPMI - **I**ntelligent **P**latform **M**anagement **I**nterface: An integrated interface (looks like an ethernet port) dedicated to the management and monitoring of the computer. It is not the same, and cannot be used, as a regular ethernet port.

IPv6 - **I**nternet **P**rotocol **v**ersion **6** (aka, TCPv6): The newest way of assigning TCPIP addresses since IPv4 is running out of assignable addresses (numbers).

ITAD - **I**nformation **T**echnology **A**sset **D**isposal: The processes used to properly dispose of the physical equipment and components used in today's electronics equipment.

ITAM - **I**nformation **T**echnology **A**sset **M**anagement: A framework intended to oversee the best practices and processes for managing IT (Information Technology) assets.

JPEG/JPG - **J**oint **P**hotographic **E**xperts **G**roup: A technology used to compress (the size of) digital images that minimizes the loss of the quality of the image.

NAVSO - **Nav**al **S**taff **O**ffice: A set of publications written by the U. S. Navy which establishes the guidelines for all of its operations including the handling of information (IT) systems and their security throughout its lifecycle from installation to disposal.

NIST - **N**ational **I**nstitute of **S**tandards and **T**echnology: A part of the US Department of Commerce whose goal, according to Wikipedia, is to, "…promote innovation and industrial competitiveness…From 1901-1988, the agency was named the Nation Bureau of Standards".

ODBC - **O**pen **D**ata**b**ase **C**onnectivity: Software that configures how a system connects to a database. In a client-server model, the ODBC is typically configured (required) on the client side.

PDF - **P**ortable **D**ocument **F**ormat: A standard that establishes how to display text and images in a document that is independent of the computer hardware and the operating system.

PUIS - **P**ower **U**p **I**n **S**tandby (Mode): Firmware built into disk drives, commonly found in appliances like (cable) set top boxes, that causes the drive to not start spinning when power is first applied. The drive only spins up ("powers up") when it is accessed, thus extending the life of the drive.

PXE - **P**reboot E**x**ecution **E**nvironment: The primary means of booting x86 / x64 based systems over a network.

QoS - **Q**uality **o**f **S**ervice: The measurement of the overall performance of the network.

RMA - **R**eturn **M**erchandise **A**uthorization: Part of the process for sending back a product either for reimbursement, repair or replacement.

TCPv4 - (aka, IPv4):

TFTP - **T**rivial **F**ile **T**ransfer **P**rotocol: The basic means of transferring small files from one system to another commonly used as the first steps to booting a system over the network.

WIM - **W**indows **I**maging **F**ormat: A file based version of Windows containing enough of the basics to get a system booted.

XML - E**x**tensible **M**arkup **L**anguage: Similar to HTML, it is text inside of a file with "tags" enclosed by a set of "< >" that defines a set of rules typically used to store, transport and manipulate data.