Table of Contents

Enterprise Data Erasure - Chapter 1 Introduction ................................................................. 1

1.1 Certification .......................................................................................................................... 2
1.2 Standards ............................................................................................................................. 2

Enterprise Data Erasure - Chapter 2 Erasing Devices ............................................................. 3

2.1 – Interface and Features ...................................................................................................... 3
2.2 - Configuring Erasure Type by Protocol ............................................................................ 3
2.4 - Erasing on Device Discovery ............................................................................................ 5
2.5 - Restarting Erasures .......................................................................................................... 5
2.6 - Force Failure/Results Utility ............................................................................................. 6
2.7 - Viewing Device Log ........................................................................................................... 8
2.8 - Viewing the Media ............................................................................................................ 8
2.9 – Log Monitor and Analysis Tool ......................................................................................... 10

Enterprise Data Erasure - Chapter 3 Device Reports ............................................................... 12

3.1 – Device Report Generation ............................................................................................... 12
   Field Defines: .......................................................................................................................... 13
   Value Defines: ......................................................................................................................... 13
   Creating a User-Defined Field: ............................................................................................. 14
   Modifying a User-Defined Field: .......................................................................................... 14
   Deleting a User-Defined Field: ............................................................................................. 14
   Requiring User Input: ............................................................................................................. 14
   Loading and Saving Report Templates: .................................................................................. 14

3.4 – QR Code Customization .................................................................................................. 15

3.4 - Report Samples ................................................................................................................ 16
   PDF Example: ........................................................................................................................ 16
   HTML Example: ..................................................................................................................... 17
   XML Example: ....................................................................................................................... 18
   CSV Example: ....................................................................................................................... 19
   CSV Database Export Example: ............................................................................................ 20
   Text Example: ......................................................................................................................... 21

Enterprise Data Erasure – Chapter 4 Interface Customization .................................................. 22
8.1 Enabling Grading Feature...........................................................................................................43
8.2 Creating Grading Profiles ............................................................................................................44
**Table of Figures:**

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Example of the Physical Interface</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>List View and Interface icons</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>Selecting an Erasure Method</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>Online Device, Start Arrow and Erasure Method</td>
<td>5</td>
</tr>
<tr>
<td>5</td>
<td>Restarting Erasure icon and indicators</td>
<td>6</td>
</tr>
<tr>
<td>6</td>
<td>Force Erasure Results dialogue</td>
<td>7</td>
</tr>
<tr>
<td>7</td>
<td>Enabling Bulk Add feature</td>
<td>7</td>
</tr>
<tr>
<td>8</td>
<td>Erasure log folder path in Windows Explorer</td>
<td>8</td>
</tr>
<tr>
<td>9</td>
<td>The View Media button</td>
<td>8</td>
</tr>
<tr>
<td>10</td>
<td>Media Viewer (data)</td>
<td>9</td>
</tr>
<tr>
<td>11</td>
<td>Viewing hash with Media Viewer and log file with reference hash</td>
<td>9</td>
</tr>
<tr>
<td>12</td>
<td>Viewing hash with Media Viewer and log file with invalid hash</td>
<td>10</td>
</tr>
<tr>
<td>13</td>
<td>Log Monitor and Analysis Tool with records displayed</td>
<td>11</td>
</tr>
<tr>
<td>14</td>
<td>Report Generator with records displayed</td>
<td>12</td>
</tr>
<tr>
<td>15</td>
<td>Report Customization window</td>
<td>13</td>
</tr>
<tr>
<td>16</td>
<td>Label Customization window</td>
<td>15</td>
</tr>
<tr>
<td>17</td>
<td>QR Code Creator</td>
<td>15</td>
</tr>
<tr>
<td>18</td>
<td>Example PDF Report</td>
<td>16</td>
</tr>
<tr>
<td>19</td>
<td>Example HTML Report</td>
<td>17</td>
</tr>
<tr>
<td>20</td>
<td>Example XML Report</td>
<td>18</td>
</tr>
<tr>
<td>21</td>
<td>Example CSV Report</td>
<td>19</td>
</tr>
<tr>
<td>22</td>
<td>Example of a database report exported to a CSV file</td>
<td>20</td>
</tr>
<tr>
<td>23</td>
<td>Example of a report exported to text file</td>
<td>21</td>
</tr>
<tr>
<td>24</td>
<td>Customizing the Device List</td>
<td>21</td>
</tr>
<tr>
<td>25</td>
<td>Interface Customization Window</td>
<td>22</td>
</tr>
<tr>
<td>26</td>
<td>Creating an Adapter Alias</td>
<td>23</td>
</tr>
<tr>
<td>27</td>
<td>Working with Program Settings</td>
<td>23</td>
</tr>
<tr>
<td>28</td>
<td>Modifying Recycler Mode</td>
<td>24</td>
</tr>
<tr>
<td>29</td>
<td>Working with Startup Events</td>
<td>25</td>
</tr>
<tr>
<td>30</td>
<td>Selecting Pressure Events</td>
<td>25</td>
</tr>
<tr>
<td>31</td>
<td>Enable, disable or modify Erasure Settings</td>
<td>26</td>
</tr>
<tr>
<td>32</td>
<td>Automating NIST methodology</td>
<td>27</td>
</tr>
<tr>
<td>33</td>
<td>Enabling Post Erasure Events</td>
<td>27</td>
</tr>
<tr>
<td>34</td>
<td>Setting the default locations for logs and reports</td>
<td>28</td>
</tr>
<tr>
<td>35</td>
<td>Working with Network Options</td>
<td>28</td>
</tr>
<tr>
<td>36</td>
<td>Turning Report Options on or off</td>
<td>29</td>
</tr>
<tr>
<td>37</td>
<td>Options in the Advanced 1 menu</td>
<td>29</td>
</tr>
<tr>
<td>38</td>
<td>Creating Profiles</td>
<td>30</td>
</tr>
<tr>
<td>39</td>
<td>Creating a new profile</td>
<td>31</td>
</tr>
<tr>
<td>40</td>
<td>Saving a profile</td>
<td>31</td>
</tr>
<tr>
<td>41</td>
<td>Selecting a profile</td>
<td>32</td>
</tr>
<tr>
<td>42</td>
<td>Determining the active profile</td>
<td>32</td>
</tr>
<tr>
<td>43</td>
<td>The Physical Interface</td>
<td>33</td>
</tr>
<tr>
<td>44</td>
<td>Accessing Design Physical Interface</td>
<td>36</td>
</tr>
<tr>
<td>45</td>
<td>Designing a Physical Interface</td>
<td>36</td>
</tr>
<tr>
<td>46</td>
<td>Configuring operator logins</td>
<td>38</td>
</tr>
<tr>
<td>Figure</td>
<td>Description</td>
<td>Page</td>
</tr>
<tr>
<td>--------</td>
<td>--------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>47</td>
<td>Create Privilege Group</td>
<td>39</td>
</tr>
<tr>
<td>48</td>
<td>Assigning Privilege Group to user</td>
<td>40</td>
</tr>
<tr>
<td>49</td>
<td>Database Integration Mapping</td>
<td>41</td>
</tr>
<tr>
<td>50</td>
<td>Adding offline database entries</td>
<td>42</td>
</tr>
<tr>
<td>51</td>
<td>Enabling Grading Feature</td>
<td>43</td>
</tr>
<tr>
<td>52</td>
<td>Accessing Grading Profile Creator</td>
<td>44</td>
</tr>
<tr>
<td>53</td>
<td>Configuring Drive Grading</td>
<td>44</td>
</tr>
</tbody>
</table>
Welcome to XErase™ Enterprise Data Erasure, the quickest most efficient means of securely erasing data.

Whether you need to erase entire frames, drive enclosures or individual drives, this data erasure software can provide a cost effective, fully automated solution to save you time, money and give you and your customers the peace of mind that comes from an industry leader.

This solution supports whatever sanitization standard you or your customer may require whether it is DoD, NAVSO, NIST etc. The software can easily adapt to accommodate any future data erasure or disk sanitization standards.

Our Industry Unique Physical Interface below along with our List Interface provide the operator with a direct view into the system and erasure status of each drive in an intuitive manner. All devices that are online and accessible are displayed with key data points. No other software currently available today has the features or functionality of Enterprise Data Erasure!

![Figure 1 - Example of the Physical Interface](image-url)
1.1 Certification

XErase has been certified by ADISA to conform to the standards for data security and recycling of disk drives prior to their disposal or reuse. The latest certificate can be viewed at http://adisa.global/wp-content/uploads/2018/02/ADISA_Extreme-Protocol-Solutions_ADPC0033.pdf

1.2 Standards

The standards XErase uses to sanitize disks are:

- NIST SP800-88R1 (https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-88r1.pdf)
**Enterprise Data Erasure - Chapter 2 Erasing Devices**

**2.1 – Interface and Features**

On open Enterprise Data Erasure defaults to the standard list interface and control set which provide access to all the software features and customizations. Any devices connected to the software will display drive data in list format as shown below.

In addition to standard file menu controls users have access to icon-based controls and feature selectors, as well as visibility into the erasure methods and rules directly through this interface.

![Figure 2 – List View and Interface icons](image)

**Interface Icon Descriptions (left to right)**

**Left Group**
- Start Erasure
- Stop Erasure
- Erasure Method Configuration

**Right Group**
- Device Field Selector Dropdown
- Operator Login and Administration
- View Media
- Rescan Devices
- User Fields and Configuration
- Report Generation

**2.2 - Configuring Erasure Type by Protocol**

As mentioned in the Interface and Features Section above the user has total control over their erasure method of choice. Later in this document, we will outline how the system administrator can control the available erasure methods by operator login.

By clicking the Wrench/Screwdriver Icon a window of available erasure methods will appear. This interface provides control over which erasure method will be used based on the protocol (ATA, SCSI) of the device (HDD, SSD) being erased.
Simply select from the available options and set your default erasure types by protocol and click the update Icon at the bottom of the box and close the window. Once selected, the erasure methods will appear in the center section of the list interface giving the operator visibility into the selected method in use.

**Figure 3 – Selecting an Erasure Method**
2.3 - Manually Starting an Erasure

To start an erasure manually...

1. Select the desired devices from the device list. Multiple devices may be selected using the shift or control keys in combination with the left mouse button or by using the Control menu to select or deselect all devices.
2. Ensure the desired erasure method is selected for each protocol type.
3. Click the Start Button and the erasure process will start.

2.4 - Erasing on Device Discovery

You may configure the software to automatically begin the specified erasure method once a device is detected by the software. By default, this feature is not enabled, and the operator must enable it. To do so, simply open the Customize menu then select Interface / Erasure Settings and highlight “Start Erasure on Device Discovery”. Then at the bottom select ON from the option value dropdown and click the “Update” button. This will enable the feature and each time a new device is detected by the software the device will be probed, added to the list and the appropriate erasure method (by protocol) will be launched on the device.

Whether executed manually or on device discovery, each device will show a percent bar with a description and number of the pass currently being executed. (Please refer to Figure 1 for an example.)

2.5 - Restarting Erasures

There are several instances where you will potentially need to restart erasure on a drive that has already begun to process. For example, the erasure was started with the wrong erasure method selected or the erasure was aborted, and you want to restart erasure from the beginning and not resume from current location, etc. To do this you must tell XErase that the erasure restart is allowed. Below are the steps to perform this action.

1. Click the “Select Erasure Method / Rule Icon” (Screwdriver and Wrench).
2. Select the desired erasure method or keep the currently selected method.
3. Check the “Restart Erasure” check box and then click the update Icon.
You will then notice that “RESTART ERASURE” appears in the upper center of the XErase screen indicating that restart is active and that you have chosen to restart erasure from the beginning.

![Image of XErase screen showing the Restart Erasure feature.](image)

**Figure 5 - Restarting Erasure icon and indicators**

### 2.6 - Force Failure/Results Utility

Another Industry Unique feature within Enterprise Data Erasure, is the Force Failure utility. This tool allows the user to add device logs for drives that are below grade or designated for destruction. This feature then allows these nonfunctional or below grade drives, to be reported with drives that have been processed and erased.

To access this utility, click the “File” Menu and select “Force Erasure Results” The utility dialogue box will display as shown below. Complete the fields needed to meet your reporting requirements and save the results.

The tool also automates drive lookup by Model number. Simply type or scan in the model number, and if present in our database, the drives demographics will auto-populate. If not simply type them in. Once saved that device will not be present in your database for future usage.

User fields can be created and used within the tool as well. This will allow for customizations such as Job or Lot ID, as examples. These will then be saved to the log file for reporting.

A Bulk add feature is also provided. Simply click the “Bulk Serial Numbers” radio box. You can now type or scan multiples of the same item in and save each as a separate log file. This is handy in situations where you have many of the same item as it eliminates the need to complete separate entries for each device.
Figure 6 - Force Erasure Results dialogue

Figure 7 – Enabling Bulk Add feature
2.7 - Viewing Device Log

Each device creates and adds to its own data erasure log. This log is placed in the logs subfolder in the XErase install folder and is named using the serial number of the device c:\XERASwin\logs \[Year\] \[Month\] \[Serial Number\].txt. You may access the log files direct in Windows by following the path noted and by “Right” clicking on the device in the physical or list interface and selecting “View Logs”.

To view erasure log for one or more devices simply click on the desired device(s) and click the View Logs button and the log file will open in the operating system’s default text viewer.

![Figure 8 - Erasure log folder path in Windows Explorer](image)

2.8 - Viewing the Media

XErase has a media viewer that allows for the viewing of any logical block address on the selected device. To view the media on a device, simply select the device and click the View Media button.

![Figure 9 - The View Media button](image)

Depending on your configuration you may have two options (View Data and View Hash). The View Data option displays the actual data on the specified LBA (Logical Block Address). The “View Hash” option displays a hashed representation of the data. This option is the more secure of the two options and may be the only option available in your configuration.

This window also includes a bad blocks list (if any exist) for the currently selected device. You may click on a block in that list to view its contents and verify the over write. Please refer to the Figure 6 for clarification.
Figure 10 - Media Viewer (data)

Figure 11 – Viewing hash with Media Viewer and log file with reference hash
2.9 – Log Monitor and Analysis Tool

As part of the audit process it is important to know which drives were erased, when and by whom. The Log Monitor and Analysis utility within Enterprise Data Erasure, provides a searchable database that contains all erasure data by month and year and is searchable by Date Range, Folder, and Serial Number. The tool automatically provides a summary table of the records displayed, providing an immediate pass/fail report at a glance. The utility allows for record sortation with two drop down sort filters that allow for detailed analysis of the data.

Logs may be viewed within the tool as well. Labels may be generated, and a Zip file of selected records created for outside analysis or communicated to a customer.

The tool also allows customers utilizing Enterprise Data Erasure database functionality, to manually upload records to their connected database. This is extremely handy when records from other devices, or those handled offsite, need to be uploaded and reported out of a single source.
Figure 13 - Log Monitor and Analysis Tool with records displayed
Enterprise Data Erasure - Chapter 3 Device Reports

3.1 – Device Report Generation

Once devices have been erased, reports can be created that combine several devices together. These reports are available in several different formats depending on your software’s configuration. These formats are Secure PDF, HTML, XML, Text and CSV format. In addition, device report information can be placed in a table (with or without grid borders) or a list. To create a report simply select devices from the report device list, select the Report Format, the Device Format and click the Build Report button.

3.2 - Device Report Customization

XErase Enterprise Data Erasure allows the user to customize their reports format and data to fit the customer’s needs by accessing the Customize / Reports menu option. From this window you can create a customized report including logo’s, titles, and any desired device/system/erasure specific fields. The figure below provides an overview of this function and specific fields that can be customized.

<table>
<thead>
<tr>
<th>Start Date</th>
<th>Serial Number</th>
<th>Model</th>
<th>Size</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>05/24/2016</td>
<td>607010123</td>
<td>ST1000DM001</td>
<td>2.00 TB</td>
<td>2.7 hrs</td>
</tr>
<tr>
<td>05/25/2016</td>
<td>14423000000</td>
<td>CRUCIAL</td>
<td>256.00 GB</td>
<td>6 min</td>
</tr>
<tr>
<td>05/24/2016</td>
<td>9H95590112</td>
<td>SEAGATE</td>
<td>2.00 TB</td>
<td>2.7 hrs</td>
</tr>
<tr>
<td>05/24/2016</td>
<td>9H95590113</td>
<td>SEAGATE</td>
<td>2.00 TB</td>
<td>2.7 hrs</td>
</tr>
<tr>
<td>05/24/2016</td>
<td>9H95590114</td>
<td>SEAGATE</td>
<td>2.00 TB</td>
<td>2.7 hrs</td>
</tr>
<tr>
<td>05/24/2016</td>
<td>9H95590115</td>
<td>SEAGATE</td>
<td>2.00 TB</td>
<td>2.7 hrs</td>
</tr>
<tr>
<td>05/24/2016</td>
<td>9H95590116</td>
<td>SEAGATE</td>
<td>2.00 TB</td>
<td>2.7 hrs</td>
</tr>
<tr>
<td>05/24/2016</td>
<td>9H95590117</td>
<td>SEAGATE</td>
<td>2.00 TB</td>
<td>2.7 hrs</td>
</tr>
<tr>
<td>05/24/2016</td>
<td>9H95590118</td>
<td>SEAGATE</td>
<td>2.00 TB</td>
<td>2.7 hrs</td>
</tr>
</tbody>
</table>

Figure 14 - Report Generator with records displayed
Field Defines:
The following can be found in the Formatting Fields drop down list.
1. `<TITLE>` This is the first line of your report title.
2. `<TITLE2>` This is the second line of your report title
3. `<TITLE3>` This is the third line of your report title
4. `<IMAGE TOP_LEFT>` The image you wish to display in the top left corner of PDF or HTML reports.
5. `<IMAGE TOP_RIGHT>` The image you wish to display in the top right corner of PDF or HTML reports.
6. `<FILE>` A text file that you wish to include in the report header.
7. `<ERASURE_STATISTICS>`
8. `<DEVICE_FIELD>`
9. `<DEVICE_LOGS>`
10. `<INSERT_SYSINFO>`
11. User Defined

Value Defines:
The following can be found in the Defined Values drop down list.
1. `<OPERATOR>` Inserts the currently logged in operator name as a value.
2. `<DATE>` Inserts the date as a value.
3. `<TIME>` Inserts the time as a value.
Creating a User-Defined Field:
To create a user-defined field, simply type the field name and value (if desired) and click new. If you wish the field value prompted for at the time of report creation, simply leave the field value blank. If the field value is a filename such as an image or text file to include, simply click the browse button and locate the desired file.

Modifying a User-Defined Field:
To modify a user-defined field, simply select the field from the field list, change the field name or value if desired and click update. You can also modify the position of the field in the report by clicking the up or down arrow buttons.

Deleting a User-Defined Field:
To delete a user-defined field, simply select the field from the field list and click the Delete Button.

Requiring User Input:
During the report generation process it may be necessary to obtain user input. For example, if devices are erased for different customers you may want to have your operator type in the name of the customer that they are generating the report for. To accommodate this requirement, the Custom Field Entry window has a Non-Savable Value checkbox. This checkbox can be used during field creation or after the fact by selecting the desired field, checking the box and hitting the update button. Once a field is marked as non-savable the operator will be prompted to enter a value for that field each time a report is generated.

Loading and Saving Report Templates:
Since you may have different report field requirements for different customers the Custom Field Entry window provides a means of loading and saving all report fields into a template. Templates can then be loaded and saved as desired with the last template accessed used as the default.

3.3 – Label Customization
XErase allows the user to design and customize labels for device or system use by accessing the Customize / Label menu option. From this window you can create a customized label including logo’s, barcodes, QR codes, and any desired device/system/erasure specific fields. The following figure provides an overview of this function and specific fields that can be customized.
XErase also allows the user to design their own QR code for use on device and system labels. To do so, access the Customize / QR Code menu option. From this window you can create a customized QR code including any desired device/system/erasure specific fields. The figure below provides an overview of this function and specific fields that can be customized.
3.4 - Report Samples

PDF Example:

![Image of XErase Data Erasure Certificate of Erasure]

**Erasure Description**

This Erasure conforms to the NIST 800-88 rev1 standard, if possible, by determining methods that your drive is capable of performing and executing one that conforms to the specification.

Current methods include the following, and chosen in the order below if visible for this disk. Details are found on pages 32/33 for Hard Disk Drives (HDD), and pages 36/37 for Solid State Drives (SSD) in this document: [http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf](http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf)

1) **SECURE ERASE** - Zeros to all blocks (usually ATA SSD only)

2) **SCSI Format** - Zeros to the media (usually SCSI SSD only). At least as good as an overwrite pass. Probably erases unallocated blocks also (firmware dependent.)

3) **Overwrite** - 1x or 3x write passes (usually 1x for HDD and 3x for SSD)

After the Clear is complete, a Seeded Verify test will be performed if the Secure Erase or Format was performed. In addition a minimum 2500 block spot verify is always performed unless the user specifically chooses a full media verify or a NIST Shc verify option for more coverage.

**METHODS**

1) NIST 800-88 rev1 Clear - SecureErase, SpotVerify 1000

4) NIST 800-88 rev1 Clear - Write Over, SpotVerify 1000

---

**Figure 18 - Example PDF Report**
### HTML Example:

**XErase Data Erasure**

**Certificate of Erasure**

**Erasure Results Summary**

<table>
<thead>
<tr>
<th>Capacity</th>
<th>Passed</th>
<th>Failed</th>
<th>Error</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>2TB</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
</tbody>
</table>

**Erasure Description**

This Erasure conforms to the NIST 800-88 rev. 1 standard, if possible, by determining methods that your drive is capable of performing and executing one that conforms to the specification.

Current methods include the following, and shown in the order below if viable for this disk:

1. Secure Erase - Zeros out all blocks (usually ATA SSD only)
2. Sanitize - Zeros out the media (usually SATA & SAS drives only) At least as good as any-erase pass. Probably more secure_erase_blocks also. (Vendor dependent)
3. Overwrite - Takes the media passes (usually ATA or FDE and In the SSD)

After the Clean is complete, a Seeded Verify test will be performed if the Secure Erase or Fastest was performed. In addition a Seeded Clean (Bolt clean verify or Always performed unless the user specifically chooses a Full media verify or a NIST 800-88 verify option for more coverage.

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Device ID</th>
<th>Media Serial</th>
<th>Capacity</th>
<th>Date</th>
<th>Status</th>
<th>Health</th>
<th>Size</th>
<th>Free Space</th>
</tr>
</thead>
</table>
| STT2000600NSX20 | TN20010600CLI | 5X9DB000000 | 2TB | 2014-02-20 | 30720 | 0.0 | Pass | 0 | 100%

**Figure 19 - Example HTML Report**
XML Example:

```xml
<xml version="1.0" encoding="ISO-8859-1"/>

<REPORT>
  <ReportInfo>
    <DeviceID>00:00:00:00:00:00:00:00</DeviceID>
    <date>07/25/2018</date>
    <time>10:15:48</time>
  </ReportInfo>
  <caseFile>
    This Erase conforms to the NIST 800-88 rev1 standard, if possible, by determining methods that your drive is capable of performing and executing one that conforms to the specification. Current methods include the following, and choose the order below if viable for this disk. Details are found on pages 32/33 for Hard Disk Drives (HDD), and pages 36/37 for Solid State Drives (SSD) in this document:
    1) Secure Erase - Erase to all blocks (usually A1A 650 only)
    2) Hcci Format - Erase to the media (usually HCCI SSD only)
    At least as good as an overwrite pass. Probably crosses unmapped blocks also (firmware dependent)
    3) Overwrite - 1x or 3x write passes (usually 1x for HDD and 3x for SSD) After the Clear is complete, a Sendel Verify test will be performed if the Secure Erase or Format was performed. In addition a minimum 2000 block spot verify is always performed unless the user specifically chooses a full media verify or a HCCI Verify option for more coverage.
  </caseFile>
  <caseNotes>
    <summary>
      <xml group total="3" other="0" passed="3" size="250 GB">
        <xml group total="0" other="0" passed="0" size="21 MB"/>
        <xml group total="0" other="0" passed="0" size="Total"/>
      </summary>
    <number>2</number>
    <type>SATA</type>
    <MODEL>ST32000648AS</MODEL>
    <DEVICE_TYPE>3.5 SATA 7200</DEVICE_TYPE>
    <SERIAL_NUMBER>WNN22932</SERIAL_NUMBER>
    <CAPACITY>2.00 TB</CAPACITY>
    <DATE>05/25/2014</DATE>
    <MINUTES>0:0:0:0</MINUTES>
    <total_MINUTES>0:0:0:0</total_MINUTES>
    <STATUS>PASSED</STATUS>
    <PASS>958321-01-100-0701</PASS>
    <drive_notes_ref>drive_notes_ref</drive_notes_ref>
  </caseNotes>
  <caseNotes>
    <summary>
      <xml group total="3" other="0" passed="3" size="250 GB">
        <xml group total="0" other="0" passed="0" size="21 MB"/>
        <xml group total="0" other="0" passed="0" size="Total"/>
      </summary>
    <number>3</number>
    <type>SATA</type>
    <MODEL>ST32000648AS</MODEL>
    <DEVICE_TYPE>3.5 SATA 7200</DEVICE_TYPE>
    <SERIAL_NUMBER>WNN189V1</SERIAL_NUMBER>
    <CAPACITY>2.00 TB</CAPACITY>
    <DATE>05/25/2014</DATE>
    <MINUTES>0:0:0:0</MINUTES>
    <total_MINUTES>0:0:0:0</total_MINUTES>
    <STATUS>PASSED</STATUS>
    <PASS>958321-01-100-0701</PASS>
    <drive_notes_ref>drive_notes_ref</drive_notes_ref>
  </caseNotes>
  <caseNotes>
    <summary>
      <xml group total="3" other="0" passed="3" size="250 GB">
        <xml group total="0" other="0" passed="0" size="21 MB"/>
        <xml group total="0" other="0" passed="0" size="Total"/>
      </summary>
    <number>4</number>
    <type>SATA</type>
    <MODEL>ST32000648AS</MODEL>
    <DEVICE_TYPE>3.5 SATA 7200</DEVICE_TYPE>
    <SERIAL_NUMBER>WNN189V1</SERIAL_NUMBER>
    <CAPACITY>2.00 TB</CAPACITY>
    <DATE>05/25/2014</DATE>
    <MINUTES>0:0:0:0</MINUTES>
    <total_MINUTES>0:0:0:0</total_MINUTES>
    <STATUS>PASSED</STATUS>
    <PASS>958321-01-100-0701</PASS>
    <drive_notes_ref>drive_notes_ref</drive_notes_ref>
  </caseNotes>
</REPORT>
```

Figure 20 - Example XML Report
CSV Example:

```
<table>
<thead>
<tr>
<th>Model,DEVICE TYPE, SERIALNUM, CAPACITY, DATE, HOURS, HEALTH, STATUS, NOTES, Rack</th>
</tr>
</thead>
<tbody>
<tr>
<td>ST3200064405, 3.5 SATA 7200, 9W457002, 2.00 TB, 05/25/18, 583578, 0, PASSED, PHX02-01-100-0702</td>
</tr>
<tr>
<td>ST3200064405, 3.5 SATA 7200, 9W457002, 2.00 TB, 05/25/18, 583578, 0, PASSED, PHX02-01-100-0702</td>
</tr>
<tr>
<td>ST3200064405, 3.5 SATA 7200, 9W457002, 2.00 TB, 05/25/18, 583578, 0, PASSED, PHX02-01-100-0702</td>
</tr>
<tr>
<td>WD2502ABYS-188766, 3.5 SATA 7200, UCAT1377630, 250.00 GB, 05/25/18, 555850, 0, PASSED, PHX02-01-100-0703</td>
</tr>
<tr>
<td>WD2502ABYS-188766, 3.5 SATA 7200, UCAT1377630, 250.00 GB, 05/25/18, 555850, 0, PASSED, PHX02-01-100-0703</td>
</tr>
<tr>
<td>WD2502ABYS-188766, 3.5 SATA 7200, UCAT1377630, 250.00 GB, 05/25/18, 555850, 0, PASSED, PHX02-01-100-0703</td>
</tr>
<tr>
<td>WD2502ABYS-188766, 3.5 SATA 7200, UCAT1377630, 250.00 GB, 05/25/18, 555850, 0, PASSED, PHX02-01-100-0703</td>
</tr>
</tbody>
</table>
```

Figure 21 - Example CSV Report
CSV Database Export Example:

```
Figure 22 – Example of a database report exported to a CSV file
```
Text Example:

Figure 23 - Example of a report exported to text file
Enterprise Data Erasure – Chapter 4 Interface Customization

4.1 – Device List

To more effectively use the device list space a certain level of customization is provided that allows the user to turn ON or OFF certain fields in the list. This conserves space or provides more elaborate device information depending on the user’s preference. To access the device list customization, simply select Interface from the Customize menu and click the Device List category. To modify the list options, simply click on the desired option and use the drop-down list to select either ON or OFF. Once you have completed your change, click the Update button and the device list will dynamically modify to accommodate your changes.

4.2 - Adapter Properties

To more descriptively enhance your erasure reports, Enterprise Data Erasure provides the ability to assign alias names to each adapter. This provides you with a more detailed description of the position of the drive that was erased. For example Octane, Slot 4 instead of just 03.0:04:00 (HA.BUS:TID:LUN). To assign an alias, simply click on the adapter entry in the Options list. Type in or modify the Alias Name field and click the update button. Any reports generated after this modification will contain the alias information in addition to the HA.BUS:TID:LUN position description. In addition to aliases, this option also allows you to force adapter RESETs during rescan. This is useful if you have an array enclosure that does not properly identify targets without a RESET. Lastly, this option has a Manual Auto Detection Required option for non-plug-and-play protocols such as U320 SCSI and below. If this option is selected on an adapter the software will query the adapter every ten seconds to see if any new devices have been added or removed.
4.3 – Program Settings

This option allows for direct control over how XErase utilizes various subset features available to the user. Control settings such as Disabling of PUIS (Power Up In Standby), Auto generation of database entries (if using XErase connected to a database), and Support for enclosure services, can all be accessed and enabled or disabled from this menu.

Figure 26 - Creating an Adapter Alias

Figure 27 – Working with Program Settings
4.4 – Recycler Mode

Recycler Mode is a new feature within XErase V12.0. This feature contains some optimizations within the software that greatly improve the stability of the system when dealing with drives that may not be in good health. Additionally, it allows the User to customize a few of the parameters used to determine a warning or failure. To do so, set the desired values for Reallocated Sectors limit and/or Power on Hours and hit the update button. Moving forward, devices that exceed those thresholds or don’t meet your grading standards will automatically produce a warning or failure based on your settings. This will allow you to not waste time on product you can’t resell.

4.5 – Startup Events

This option allows the user to control the various startup automation features within XErase when deployed via PXE. Items such as Execution of System Condition Prompts, Keyboard Testing, BurnIn Test etc. Can all be found here and enabled or disabled. Again, this pertains to XErase being deployed via PXE mode only.
4.6 – Pre-Erasure Events

Pre-Erasure Events are features that can be enabled to run prior to the start of an erasure. Device Grading, Pre-Validation of Opcode Testing (Pre-issuing of commands to drives for compatibility,) and ATA Resizing of HPA/DCO can all be enabled or disabled from this menu.
4.7 – Erasure Settings

The Erasure settings menu allows the User to enable/disable or modify some of the engineering functionality built into XErase. In this menu you can enable the default erasure methods available for SCSI and ATA devices on startup. Additionally, various automation features such as Auto failing of drives based on slow erasure speeds, Default Verification Settings, and Formatted Block size, are all accessible through this menu.

4.8 - NIST Settings

The NIST Settings Menu allows the user to configure how XErase automates the application of NIST SP800-88 Purge, Cryptographic Erasure and Clear methodology.

Controllable features are:

- **PURGE**: Prioritize Cryptographic Erasure Choices are: Always, Never, or Before Overwrites.
- **PURGE**: Action if Purge is Not Supported – The software provides three options and will automatically apply them based on the devices capabilities. Those options are: Perform a NIST Clear, Abort or Fail the erasure.
- **PURGE**: Overwrite if Random Data after Crypto. This allows the user to specify an overwrite if there is random data present after the cryptographic erasure. Some security policies may require a specific overwrite pattern after a crypto erasure.
- **CLEAR**: Use 3x Overwrite – This allows the user to specify the use of a 3x overwrite if the device does not support NIST Clear. Choices are Never, All drives, or on SSD’s only.
- **CLEAR**: Allow SCSI Format – This allows the user to specify the use of the SCSI Format command for SCSI devices that do not support NIST Clear. Choices are Never, All drives, or on SSD’s only.
- **CLEAR**: Allow ATA Secure Erase – This allows the user to specify the use of the Secure Erase command for ATA devices that do not support NIST Clear. Choices are Never, All drives, or on SSD’s only.
• NVME: Allow NVME format – This allows the user to specify an NVME format for NVME Devices that do not support any of the NIST Clear, Purge methods. It is a simple On or Off Functionality.

4.9 - Post Erasure Events
Post-Erasure Events are features that can be enabled to run once an erasure has completed. Device Grading, Re-imaging (PXE Only), Write Stamp of Block zero can all be enabled via this menu.

Figure 32 - Automating NIST methodology

Figure 33 - Enabling Post Erasure Events
4.10 - Folders

This option allows the user to set up the default locations for both log files and reports. It also contains the “Override Folder” which can be used for writing USB boot settings to override those that are created to RAM disk at the time of booting the system.

![User Customization](image)

Figure 34 - Setting the default locations for logs and reports

4.11 – Network Options

This feature allows XErase to work in Client or Master Mode. This can be used to integrate the remote-control features of XErase with the PXE Deployment of the software. The user can take advantage of the Physical Mapping features within XErase on PXE deployed devices via the network.

![User Customization](image)

Figure 35 - Working with Network Options
4.12 - Report Options

Report Options turn ON or OFF the creation of Custom Device Labels and Manifest Entries upon completion or failure of an erasure. It also allows the user to specify custom report names and it controls the setup of page and label printers within the software.

4.13 – Advanced 1 Menu

This menu contains some specific engineering level features that EPS Support may ask you to utilize 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 this sub menu.
5.0 – Profiles (*Premium Feature*)

Enterprise Data Erasure has many unique features that can be utilized to control and automate the erasure process. Although controlling the software’s features is straightforward, it can be time-consuming when making wholesale configuration changes. To simplify this, we have introduced another industry unique feature “Profiles”. You simply configure the software for a process then save it as a profile. These Profiles are available in our “Premium Subscription” package. This allows the user to switch back and forth on an as needed basis.

**Creating a Profile**

1. Select Customize then Method Rule Filter
2. In the Erasure Category Drop Down Select Profiles

![Figure 38 - Creating Profiles](image-url)
3. If Profile is new select the + Icon and say yes to prompt

4. In the dialogue box, name your profile and click Ok. The new Profile will now be in your list.
5. Highlight the new profile and click the Update Icon.
Changing Profiles
Profiles can be accessed and controlled via the Premium features menu. Simply select Change Profile and select the one you wish to use and then click the Update Icon.

You can also identify which profile is in use by glancing at the Message Bar at the top of the XErase window. It will tell you the Profile name currently in place.

The figures below will make this process cleared for the user.

![Figure 41 - Selecting a profile](image1)

![Figure 42 - Determining the active profile](image2)
Enterprise Data Erasure – Chapter 5 Physical Interface

5.1 - User Interface Layout

The Physical Interface was designed for static hardware configurations being used to erase drives. This interface gives a new level of usability to Extreme Manufacturing that allows for the complete graphical customization of the test GUI so that the software graphically mirrors the desired physical test setup. This new interface also provides the ability to integrate barcode scanning into your test process for better tracking and physical identification of devices. The Workspace of the Physical Interface is comprised of the following:

1. Disk Arrays that are a combination of graphical images and device layouts that describe the number of devices, rows, columns, sizes and spacing. Each Disk Array has a context menu associated with it.
2. Device Slots within the Disk Array that are attached to physical devices by serial number. Each slot has a context menu associated with it as well.
3. Erasure Method Options for ATA and SCSI based devices. These Erasure Methods either contain the standard 1X, 3X, 5X and 7X Overwrite Options or user-specified erasure options. This section also contains a Start on Discovery Checkbox that (if checked) automatically starts the appropriate erasure method on any newly discovered device.
4. Device Slot Customization drop down list that changes the contents of the Device Slot Text to one of the defined values: Wipe Status, Estimated Pass Time Left, Serial Number, Target ID, Capacity, Manufacturer, Model or SCSI/ATA Revision.
5. Zoom drop down list that expands or shrinks the GUI based on the selected value.
6. Device Information list box that contains all pertinent information for the selected device.
7. Serial Number Entry field for barcode scanning the Serial Number of the device into the selected slot. This section also has an Auto Tab checkbox that (when checked) automatically moves to the next device (left to right, top to bottom) once the return key (part of the barcode protocol) is detected after serial number entry.
8. Operator Login information that shows who is logged into the software and what their logout policy is. Policies can be set to auto logout after a specified amount of time, erasure launches or manual logout.

Figure 43 – The Physical Interface
5.2 - Global Context Menu

The Global Context Menu is triggered when the mouse is right clicked anywhere in the area surrounding the Disk Arrays. The menu options below are applied to all arrays simultaneously.

1. Start All - Starts the protocol specific erasure method indicated in the Erasure Method Options section.
2. Abort All - Aborts all active erasures.
4. Print Available Labels - Batch Prints all labels that have been generated by Completed or Failed devices.
5. Clear All Array Data - Removes any scanned in information as well as any slot / device associations.
6. Rescan All Arrays - Rescans each array to determine if any devices were added or removed. If any erasures are running this is a safe rescan that queries the adapters. If no erasures are running, then a full rescan is performed destroying and recreating the device list. The Disk Array Context Menu is triggered when the mouse is right clicked anywhere inside of a Disk Array. The menu options below are applied only to the array that was right clicked on. The name of that array appears as the title of the menu.

5.3 - Disk Array Context Menu

The Disk Array Context Menu is triggered when the mouse is right clicked anywhere inside the boundary area surrounding a specific array. The menu options below are applied the chosen array directly.

1. Start All - Starts the protocol specific erasure method indicated in the Erasure Method Options section.
2. Abort All - Aborts all active erasures on the Array.
4. Print Available Labels - Batch Prints all labels that have been generated by Completed or Failed devices in the Array.
5. Clear All Array Data - Removes any scanned in information as well as any slot / device associations.
6. Rescan Arrays - Rescans the array to determine if any devices were added or removed.
7. Assign Adapter to Array - Allows the user to define which adapter the Array is connected to. If a device is already assigned to a slot in the array, then this field then the value is automatically assigned. The Device Context Menu is triggered when the mouse is right clicked anywhere inside of an assigned device slot. The menu options below are applied only to the device that was right clicked on. The slot number and serial number of that device appears as the title of the menu along with the name of the array it is contained in.

5.4 - Device Context Menu

The Device Context Menu is triggered when the mouse is right clicked on a specific drive slot. The menu options below are applied directly to the chose drive/device.

1. Start - Starts the protocol specific erasure method indicated in the Erasure Method Options section.
2. Abort- Aborts the active erasures on the device.
3. View Log - Opens the log file for the device in the default text editor.
4. View Media - Opens the Media Viewer window (Section 2.5) displaying the contents of the media or hash data on the device.
5. Clear Device Assignment - Removes any scanned in information as well as any slot / device associations.
6. Report Label - Contains submenus that allow viewing and printing of the device label that was generated by Erasure Completion or Failure.
7. Force Fail Device - Creates a Device Report Label as well as a Device Log / Erasure Report entry failing the device. This is useful in instances where a device that was inserted is not coming online or has ceased functioning. The Slot Context Menu is triggered when the mouse is right clicked anywhere inside of an unassigned slot. The menu options below are applied only to the slot that was right clicked on. These options allow the user to manually assign the slot to either an existing serial number (if you forgot to scan it before inserting) or to a hardcoded Target ID which is only useful for protocols such as Parallel SCSI in which the Target IDs are physical and static.
5.6 - Visual Feedback

While an Erasure is running there are several means of visual feedback that provide both basic and extensive information about the erasure process. Inside of each assigned slot is color, text and percent bar to indicate status. As shown below the device slot contains a color associated with the device’s state.

**Color Scheme:**
- **Dead/Locked**    Black
- **Offline Wait**   Yellow
- **Bad Drive Data** Orange
- **Idle and not selected** White
- **Selected**       Dark Blue
- **Running**        Light Blue
- **Running with Errors** Red
- **Complete/Passed** Green
- **Failed**         Maroon

**Legacy replacements:**
- **Running**        Green
- **Complete/Passed** Light Grey

And as always, if Complete and a Grade is assigned, the Grade color replaced the stock color.

5.7 - Interface Customization / Design

The Physical Interface is completely customizable and can include any number of pre-defined Disk Arrays or your own Array definitions and images. The Physical Interface Design options can be accessed by selecting the Design Physical Interface option from the Customize Menu. In this design mode, Drive Arrays can be added, deleted or re-ordered. Once you have completed your modifications re-select the Physical Interface from the View Menu. Type an Alias name if desired. The Alias will appear to the left of the Disk Array as shown below. Once selected, click the Add button to place it in the Array List and on the screen.
Figure 44 – Accessing Design Physical Interface

Figure 45 – Designing a Physical Interface
Adding Arrays:
To Add a Disk Array to the interface simply select the desired array from the drop-down list of Available Arrays. The click the (+) Plus button to add it to your Workspace.

Deleting Arrays:
To Delete a Disk Array from the interface simply select the desired array from the Array List. Once selected, click the (-) Minus button to remove it from the Array List and the screen.

Re-Ordering Arrays:
To Change the Order of a Disk Array in the interface simply select the desired array from the Array List. Once selected, click either the up or down arrow button to move it in the Array List and on the screen.
Enterprise Data Erasure – Chapter 6 Operator Management

6.1 - Operator Login Policy

Integrated into Enterprise Data Erasure is an operator management interface that provides a level of both security and accountability. An administrator account exists from which individual operator accounts and privilege groups may be created. Once created, the Administrator can set up a policy to require operators to log in as shown below.

Once an operator is logged in, their name is attached to each device they start, abort or build reports for. If Erasure Manifests (Section 2.6) 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.

The default Administrator Password is epspw. Passwords are case sensitive. It is recommended that you change the Administrator Password to something you can remember for security purposes. To log in as an operator, simply select the appropriate Operator Login name, type in the password and hit the Login button.

6.2 - Creating Operators and Logging In

To create a new operator...

1. Log in as Administrator
2. Check the New User checkbox
3. Type the name of the user in the Operator Login edit field
4. Type in the Operator password
5. Select Login Duration
   - Until Logout
   - Time Limit (enter time in minutes)
   - Drives Started (must enter quantity)
6. Click the Add button to create the new user.

Figure 46 - Configuring operator logins
6.3 - Privilege Groups

In XErase the Administrator can create Privilege Groups that can be assigned to each User. These privileges control what features each operator has access to while logged in. This allows for role-based access control and increased security.

To Create Privilege Groups:

1. Login as the Administrator
2. Select Privileges from the dropdown menu. (This will populate all the available features within XErase into the Enabled Privileges Menu.)
3. Adjust the Privileges Enabled by using the +/- Icons to set the enabled features.
4. Hit the Save Icon at the bottom of the screen and save your new privilege set.

![Figure 47 - Create Privilege Group]
Assigning Privilege Group to a user:

1. Login as an Administrator
2. Select the user to assign a privilege group to.
3. Select the appropriate roll-based privilege group and Hit the Plus Icon at the bottom of the screen to assign these privileges to the user. Privilege Groups will override any previously allowed permissions.

![Figure 48 - Assigning Privilege Group to user](image-url)
Enterprise Data Erasure – Chapter 7 SQL or MYSQL Database Integration (Premium Feature)

7.1 – Database Setup

XErase with the Premium License, contains an extremely powerful and simple interface for directly interacting with a local or remote MYSQL or SQL database. XErase can automatically upload device fields, system fields and user fields to any database that it can connect to.

The interface below shows how easy it is to map XErase fields to your fields.

1. First select enter the database IP, Name, Username and Password
2. Select the desired table to upload data to and its list of fields will appear
3. Click the Database Checker Icon for to identify any compatibility issues. These issues if present must be addressed prior to completing the database mapping below. Below is a mandatory required field that your database must have, ‘recid’ which must be a self-incrementing integer identity column.
4. Select the XErase field to map into the database field. You can choose from Device, System or User fields.
5. Now click the add button at the bottom of the screen and you have mapped your first field.
6. Repeat steps 2-4 and map all your fields
7. Un-Check the Overwrite (Replace) Existing Entries if you want a new entry created each time an asset is erased.

Figure 49 - Database Integration Mapping
7.2 – Automating Database Entries

Once you have set up your database you need to turn on automatic database entry generation. This can be done in the Customize / Interface / Program Settings menu option. Select Auto Generate Database Entries from the Program Settings list. Choose ON for the Option value and hit the update button. Every time an erasure is started a new entry will be created and each time the erasure finishes the entry will be updated.

7.3 – Adding Offline Database Entries

1. If you have erased systems or devices while not connected to your network whether on-site or in-house you can add all your entries to the database with the following process.
2. Connect to your network and verify that the connection is active
3. From the File Menu select Log Monitor and Archive
4. Select the devices to add or add all by clicking the select all button
5. Hit the Database Upload button

![Figure 50 - Adding offline database entries](image-url)
Enterprise Data Erasure – Chapter 8 Device Grading (Premium Feature)

Enterprise Data Erasure has another industry unique feature called “Device Grading”. Utilizing our protocol test and development background, we have given the user the ability to develop custom grading profiles that test and grade each device to their standards. This feature allows for complete control of your downstream materials, making your product more marketable and less susceptible to RMA.

8.1 Enabling Grading Feature

To use this feature, you must first have purchased a premium subscription, or an EPS Appliance maintained under an active support agreement. Additionally, Grading may be run Pre-Erasure, Post Erasure or both. To enable this feature, navigate to Customize, Interface, and select Pre or Post Erasure Event. Locate Health and Grading then enable by turning the feature on and selecting the update arrow.

The Figures below will provide guidance. The process is the same for either event, however, before the process is run you will need to create “Grading Profiles” for each drive protocol. (Refer to Section 8.2 for instruction on how to create these profiles.)

![User Customization](image)

Figure 51 - Enabling Grading Feature
8.2 Creating Grading Profiles

Enterprise Data Erasure comes with a basic set of grading profiles for ATA and SCSI Drives. These profiles are intended as examples. EPS recommends using them as a baseline, and then adjusting them to meet your processing needs and contractual requirements.

To access these profiles, Select the Premium Menu and then Device Grading.

Figure 52 - Accessing Grading Profile Creator

Figure 53 - Configuring Drive Grading