

# Intel® vPro™ Technology Use Case Reference Design

Remote Drive Erase

---

Revision 1.0  
March, 2011  
Document ID: 1083

# Revision History

Revision	Revision History	Date
1.0	Initial release.	March, 2011

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS ARE NOT DESIGNED NOR INTENDED FOR ANY APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The Intel® Active Management Technology may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.

Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or by visiting Intel's Web Site.

Intel® Active Management Technology requires the computer system to have an Intel(R) AMT-enabled chipset, network hardware and software, as well as connection with a power source and a corporate network connection. Setup requires configuration by the purchaser and may require scripting with the management console or further integration into existing security frameworks to enable certain functionality. It may also require modifications of implementation of new business processes. With regard to notebooks, Intel AMT may not be available or certain capabilities may be limited over a host OS-based VPN or when connecting wirelessly, on battery power, sleeping, hibernating or powered off. For more information, see [www.intel.com/technology/platform-technology/intel-amt/](http://www.intel.com/technology/platform-technology/intel-amt/)

Throughout this document Intel ME refers to Intel® Management Engine and Intel® AMT refers to Intel® Active Management Technology.

Intel, the Intel logo, Intel® AMT, and Intel® vPro™ are trademarks or registered trademarks of Intel Corporation in the United States and other countries.

\*Other names and brands may be claimed as the property of others.

Copyright © 2011 Intel Corporation. All rights reserved.

# Contents

---

<b>1</b>	<b>Preface .....</b>	<b>5</b>
1.1	Document Scope .....	5
1.2	Intended Audience .....	5
1.3	Related Documentation and Software .....	5
<b>2</b>	<b>Introduction .....</b>	<b>6</b>
2.1	Example Usage Illustrated in This Document .....	6
2.2	Process Overview .....	7
<b>3</b>	<b>Detailed Steps .....</b>	<b>8</b>
3.1	Customize the ISO .....	8
3.2	Set Up the Console and Connect to the Managed Client Using SOL/IDER .....	10
3.3	Connect Using KVM Remote Control .....	13
3.4	Reboot the Managed Client to the Remote Linux* ISO .....	14
3.5	Remotely Erasing the Managed Client's Hard Drive .....	19
<b>4</b>	<b>Building the ISO .....</b>	<b>25</b>
4.1	Build System Requirements .....	25
4.2	Reference Links .....	25
<b>5</b>	<b>Appendix A: Architectural Considerations for the Included ISO File .....</b>	<b>27</b>
<b>6</b>	<b>Appendix B: Remote Drive Erase Error Messages .....</b>	<b>28</b>
<b>Figures</b>		
Figure 1:	The Remote Drive Erase ISO Builder Main Screen .....	9
Figure 2:	Connect and Control Panel, Connected to Selected Computer .....	11
Figure 3:	Remote Control Settings .....	12
Figure 4:	Serial-over-LAN Shows Connected .....	12
Figure 5:	Terminal Tool Redirection Menu .....	14
Figure 6:	The VNC* Viewer Plus IDE-Redirection Menu Icon .....	14
Figure 7:	Terminal Tool Information Panel at Bottom .....	15
Figure 8:	Remote Reboot to Redirect CD Menu .....	15
Figure 9:	The VNC Viewer Plus Power Menu Icon .....	16
Figure 10:	Press 'c' to Continue .....	16
Figure 11:	The Main Remote Drive Erase Menu .....	17
Figure 12:	Client with Multiple Hard Disk Drives .....	18
Figure 13:	Client with One Hard Disk Drive .....	19
Figure 14:	Menu to Select Erase Level (Low/Medium/High) .....	20
Figure 15:	Test email .....	21
Figure 16:	Error log file .....	22
Figure 17:	Remote Drive Erase Uses the Shred Utility .....	23
Figure 18:	The Erase Completes Successfully .....	24



# 1 Preface

---

Intel® vPro™ technology gives the Information Technology (IT) professional the capability to remotely erase the hard disk on a managed client with Intel vPro technology. The procedure described in this document boots a small Linux\* OS (an ISO file) on the remote managed client and then allows the IT professional to erase the client's hard drive. The ISO can be configured to send the IT professional an email containing the remote client's serial number and other identifying information so that a record exists of the remote disk wipe. This can be useful in the event a remote PC (say, in the field) must be physically shipped to the company's IT department—the PC's data can be completely removed before the PC is shipped.

## 1.1 Document Scope

This document does not include local language files.

The procedure in this document and its accompanying software are supported only on computers with Intel vPro technology. See section 2.1 for specific requirements.

## 1.2 Intended Audience

This document is intended for IT professionals who need out of band access to the hard drive data on a computer with Intel vPro technology, with the intent of completely erasing that hard drive's data. Readers should have a good working familiarity with Intel vPro Technology, including configuration and use of Intel AMT for out-of-band management. Readers should also be familiar with the basics of IT infrastructure, especially networked environments and their component technologies.

## 1.3 Related Documentation and Software

The download package for this Use Case Reference Design, including the Remote Drive Share software and supporting files referenced in this document, can be found at the following link:

<http://communities.intel.com/docs/DOC-4785>

Also of interest:

<http://communities.intel.com/docs/DOC-4910> (contains information on using RealVNC's VNC\* Viewer Plus with KVM Remote Control)

## 2 Introduction

---

This Use Case Reference Design demonstrates how managed clients with Intel vPro technology can be remotely booted to a small Linux ISO in order to remotely erase all data on their hard drives.

The document provides a high-level summary of the process, a detailed step-by-step example, an overview of the included Linux ISO, and steps to rebuild the ISO. The detailed steps in this document are intended to be used as a reference or example, so that readers can adapt them to their own process tailored to their specific needs.

### 2.1 Example Usage Illustrated in This Document

This document focuses on sharing the hard drive of a managed client with Intel vPro technology and has the following requirements:

1. Managed Client(s) with Intel vPro technology, supporting SOL/IDER or KVM Remote Control:
  - Configured for use with Intel vPro technology
  - Wired network connection
  - No Software Disk Encryption - Software Disk Encrypted hard drives cannot currently be accessed remotely
2. Management Console Application supporting Intel vPro technology's SOL/IDER feature
  - The document example uses Intel's Manageability Commander Tool

Other types of deployments, consoles, Intel AMT states, etc. are beyond the scope of this document.

## 2.2 Process Overview

The following is a high level overview of the remote client hard drive access and erasure process, to give you a general idea of what you will be doing in the step-by-step procedures in the remainder of the document. The steps in the overview table correspond to the major subsections of Chapter 3.

<b>Description</b>	The IT Professional ensures prerequisites are met and remotely accesses and erases the Managed Client's hard drive.
<b>Prerequisites</b>	<ul style="list-style-type: none"> <li>• SOL/IDER or KVM Remote Control must be enabled in Intel AMT on the Managed Client(s).</li> <li>• The Managed Client must be provisioned.</li> <li>• If using SOL/IDER to remotely connect to the client, a management console application capable of SOL/IDER functionality must be installed on a Management Console System.</li> <li>• If using KVM Remote Control to connect, a KVM Remote Control console such as RealVNC's VNC* Viewer Plus must be installed on the Management Console System</li> <li>• The Linux* ISO file included with this Use Case Reference Design (rde.iso) must be copied to a file location that is accessible by the Management Console System (for example, the Management Console System's hard drive).</li> </ul>
<b>Process flow</b>	<ol style="list-style-type: none"> <li>1. Customize the ISO file that will be used to reboot the Managed Client.</li> <li>2. Identify the Managed Client whose hard drive you need to erase.</li> <li>3. From the Management Console, establish a SOL/IDER session or KVM Remote Control session with the Managed Client.</li> <li>4. Remotely reboot the Managed Client to the specified Linux ISO (rde.iso).</li> <li>5. Confirm erasure of the Managed Client's hard drive.</li> </ol>
<b>Expected outcome</b>	The remote Managed Client's hard drive is completely erased.

## 3 Detailed Steps

---

This chapter and its subsections provide detailed, step-by-step procedures to remotely erase your Managed Client's hard drive using Out of Band (OOB) access from a Management Console system. Section 3.2 applies to using SOL/IDER to connect to the managed client. Section 3.3 applies to using KVM Remote Control to connect to the managed client. Other sections are applicable to either connection method, with any exceptions noted in the actual steps.

### 3.1 Customize the ISO

Included with this Use Case Reference Design is an application called "ISO Builder" (**iso\_builder.hta**) which is used to customize the ISO file (**rde.iso**) that the remote client will boot. The resulting customized ISO file will contain the following information:

<b>Take input from</b>	Will you use SOL terminal or KVM Remote Control session?
<b>Server</b>	OPTIONAL: FQDN name of the SMTP Mail Server to use for sending email status messages to Recipient (see Recipient below).
<b>Port</b>	Port number for SMTP Server; 25 for no encryption, 465 for SSL, 587 for TLS. Needed only if a server address is entered.
<b>Encryption</b>	Encryption method for SMTP Server: None, SSL, or TLS.
<b>Authentication</b>	Yes or No. Is a user name and password required for accessing the SMTP server.
<b>Username</b>	The user name that has permission for encryption access to the SMTP Server. Field is displayed only if "Yes" is then selected for <b>Authentication</b> .
<b>Password</b>	The password for the specified user name. If Server is selected, field is displayed only if "Yes" is then selected for <b>Authentication</b> .
<b>Recipient</b>	OPTIONAL: Email address to send status messages to.
<b>Sender</b>	OPTIONAL: Email address to appear in "from" field of status email messages to "Recipient".
<b>Subject</b>	OPTIONAL: Subject line to appear in status email.

The ISO Builder application asks you to enter the above information, which will be used to build the ISO. If you leave a field blank, the ISO will prompt for that information once it is booted on the managed client.

Follow the steps below to use ISO Builder to customize the ISO file.

1. Open the UCRD download .zip file and extract the ISO Builder application file, `iso_buider.hta`, to the console system.
2. Double-click **iso\_builder.hta** to run the ISO Builder application. The following screen is displayed.

**Remote Drive Erase ISO Builder**

Take input from: **Choose at boot** Will you be using a SOL terminal, a KVM session, or will you choose when the image loads?

Server: **192.168.11.2** Enter FQDN name of SMTP Mail Server

Port: **25** Enter port number for SMTP Server  
Generally 25 for no encryption, 465 for SSL or 587 for TLS

Encryption: **None** Choose encryption method for SMTP Server

Authentication: **No** Is authentication required for SMTP Server

Recipient: **user@intel.com** Recipient email address that status messages will go to

Sender: **remote\_erase@intel.com** Sender email address that will appear in Reply to: field of email

Subject: **RDE** Subject line for status email

**Build ISO** **Close**

**Figure 1: The Remote Drive Erase ISO Builder Main Screen**

3. Enter the appropriate information for each field, as desired. Remember, the ISO will prompt for whatever information you do not enter here once it boots on the managed client.



#### NOTE

*To test the email notification without starting a remote erase, see section 3.5, step 2 on page 20, and enter "test" at the prompt, as instructed for testing.*

4. Click **Build ISO**. The ISO Builder creates the file **rde.iso** in whatever folder you launched ISO Builder.

## 3.2 Set Up the Console and Connect to the Managed Client Using SOL/IDER

Follow the steps in this section if you are planning to use SOL/IDER to connect to your managed client.



### NOTE

*The procedure described below for using SOL/IDER uses Intel's Manageability Commander Tool, included in the Intel AMT SDK available at the link below, as the management console application. However, the concept should be applicable to other management console applications. The intent is to provide a detailed example of how the remote OOB hard drive access process can be accomplished with the Manageability Commander Tool, which readers can then apply to their specific IT environment and whatever management console application they are using.*

*The Manageability Commander Tool is available here:*

*<http://software.intel.com/en-us/articles/download-the-latest-version-of-manageability-developer-tool-kit/>*

*If you wish to use Intel's Manageability Commander Tool, install the Manager Developer Toolkit and ensure that you select to install the Manageability Commander Tool during the installation process. Otherwise, adapt the following procedures to your particular management console application.*

The first step is to set up your Management Console Application to perform SOL/IDER and connect to the Managed Client. The acronym SOL stands for Serial over LAN and IDER stands for IDE redirection. The SOL session connects the Management Console Application to a terminal on the Managed Client. IDER directs the Managed Client to boot from a location other than the internal hard drive. Follow the steps below to connect to an Intel vPro technology based client using the Manageability Commander Tool. The steps below assume that the Manageability Commander Tool has been installed on the Management Console System.

1. On the Management Console System, launch the Manageability Commander Tool by clicking **Start -> All Programs -> Manageability Toolkit -> Manageability Commander Tool**.
2. In the tool, select **File -> Add -> Add Intel AMT Computer....** Enter the requested information in the Add Intel AMT Computer window.

3. In the left-hand pane, right-click on the computer you just added and select **Connect** from the pop-up menu. The **Connect** button in the right-hand pane changes briefly to **Abort Connect**, then after a minute or so it changes again to **Disconnect** once the connection is established.

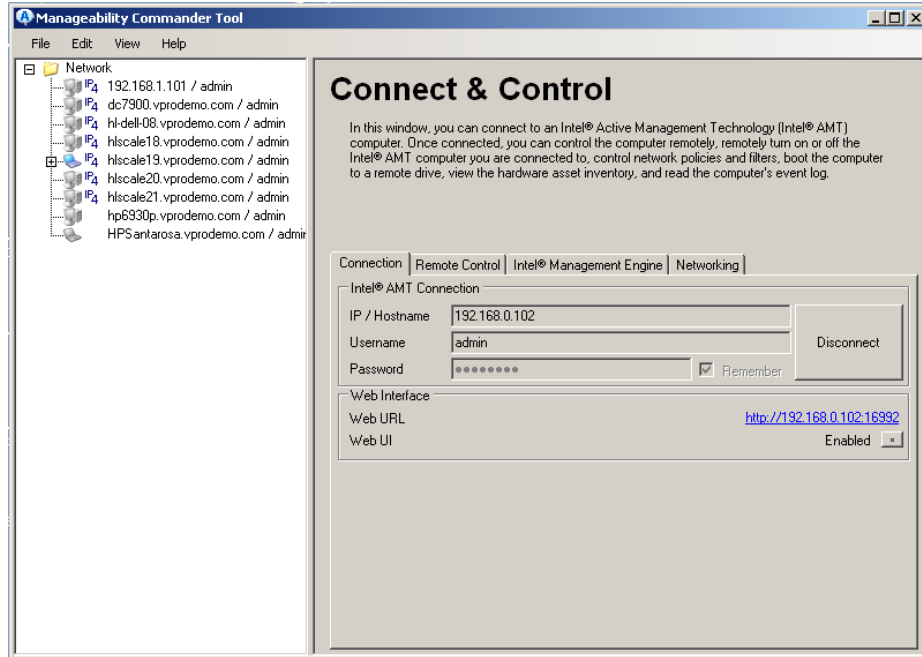
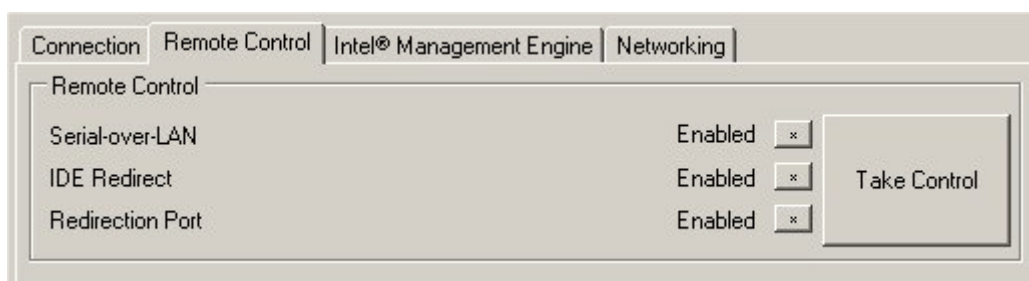


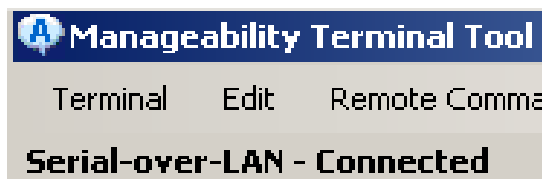
Figure 2: Connect and Control Panel, Connected to Selected Computer

- In the Connect and Control panel, click the Remote Control tab. Verify that **Serial over LAN**, **IDE Redirect**, and **Redirection Port** are **Enabled**, as shown below. If any of the items are **Disabled**, click on the \* button to enable the item. If the item is still not enabled, you may need to enable the item in Intel AMT by rebooting the Managed Client and entering the Intel® Manageability Engine BIOS Extension (Intel® MEBX) to enable the item manually. See Intel MEBX documentation for details.



**Figure 3: Remote Control Settings**

- On the Remote Control tab, click the **Take Control** button. Verify that the Manageability Terminal Window opens (as shown below) and that **Serial-over-LAN** is shown as **Connected**.



**Figure 4: Serial-over-LAN Shows Connected**

You are now ready to initiate a SOL/IDER session with the Managed Client. Using the SOL/IDER session, you will reboot the Managed Client to the specified Linux ISO, which will enable you to share the Managed Client's hard drive on your Intranet and access the hard drive's data from your Management Console System.



## NOTES

- If the Managed Client has been fully powered off, and it has a hard drive password enabled, instruct the client's owner to power it up and enter the hard drive password locally. At that point, you are ready to remotely reboot the Managed Client from the Management Console as described in the following section.*
- Software Disk Encrypted hard drives can be erased.*

### 3.3 Connect Using KVM Remote Control

Follow the steps below:

1. Click **Start -> Programs -> RealVNC -> VNC Viewer Plus**.
2. On the New Connection screen, set the following (the order is important):
  - For **Connection Mode** select **Intel AMT KVM**.
  - For **AMT Server** enter the IP address of the remote PC.
  - For **Encryption** select **None**.
3. Click **Connect**.
4. Enter your Intel AMT credentials. The document example uses **admin, P@ssw0rd**.  
**Note:** these credentials must have administrative rights to Intel AMT.
5. Click **OK**.
6. The KVM Remote Control session starts. Depending on how KVM Remote Control was configured you will either be prompted for user consent or be at the remote client's desktop. If the latter, you are done with these steps. Proceed to the conclusion paragraphs after these steps.
  - For more details on User Consent, refer to the UCRD document *Quick KVM Remote Control for Brand New 2010 Intel® Core™ vPro™ Processor Based PCs*, section 6, available at the link below.  
<http://communities.intel.com/docs/DOC-4795>
7. On the Managed Client screen a sprite is displayed with a consent code. Enter this code into the viewer window on the console. **Note:** Do not use the number pad.  
Once the code is entered you will have remote keyboard, video, and mouse control of the remote client.

At this point it is almost as if you are sitting in front of the remote client. You can do many of the same things allowed by a VNC or RDP server such as walk the user through a set of steps, type in the user's recovery passphrase, or install/uninstall software for the user. This reference design will only cover benefits of a KVM Remote Control session with Intel AMT over the current in band services mentioned above.

## 3.4 Reboot the Managed Client to the Remote Linux\* ISO

The next step is to remotely reboot the Managed Client to the **rde.iso** file. In the following steps we will use the Management Console Application to remotely reboot the Managed Client to **rde.iso**.

1. If you have not already done so, copy the Linux ISO file **rde.iso** (which you customized in section 3.1) to a location that is accessible to the Management Console System, such as the Management Console System's hard drive.
2. In the Manageability Terminal Tool, select **Disk Redirect** from the menu bar at top, then select **Change Target CD-ROM > Redirect to Image File**, as shown in Figure 5 below. If using KVM Remote Control, click the IDE-Redirection menu icon, shown in Figure 6 below.



### NOTE

*Older versions of the Manageability Commander Tool may require you to specify a floppy image as well. If your version requires this, you can specify rde.iso as the floppy image, but keep in mind that it is the CD ROM image that will be used for the redirected boot.*

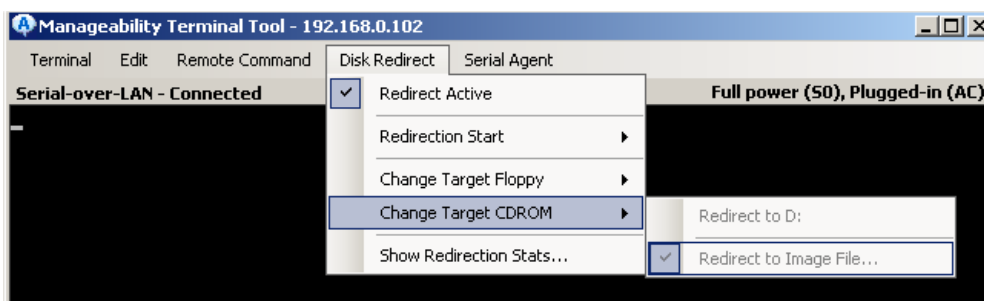


Figure 5: Terminal Tool Redirection Menu



Figure 6: The VNC\* Viewer Plus IDE-Redirection Menu Icon

3. Browse to the location where you copied the **rde.iso** file. Select the desired file and click **Open**. In Commander, the filename appears in the **CDROM** value displayed at bottom (as shown in Figure 7 below). For KVM Remote Control, be sure to click **Share** in the VNC Viewer Plus IDE-Redirection window (to share the ISO with the remote client), then skip to step 7.
4. In Commander, from the menu bar, select **Disk Redirect > Redirect Active**. The message **IDE Redirect Active** appears at bottom (as shown below).



Figure 7: Terminal Tool Information Panel at Bottom

5. From the menu bar, select **Remote Command > Remote Reboot to Redirect CD**.

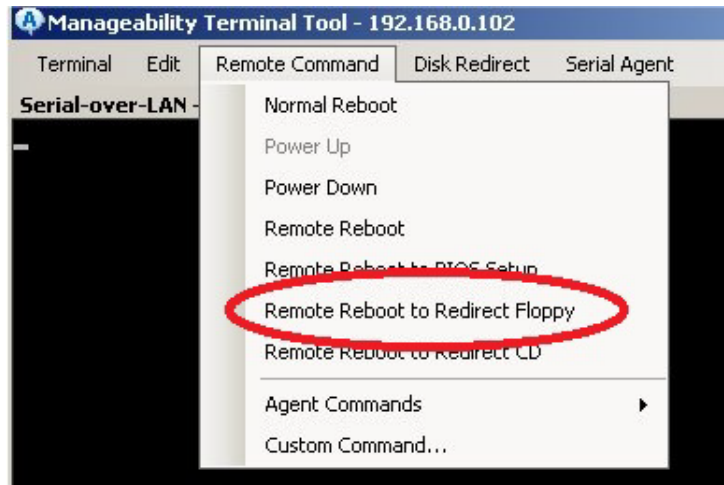


Figure 8: Remote Reboot to Redirect CD Menu

6. Click **Yes** in the **Reboot Computer to Remoted CDROM?** dialog. Wait for the Managed Client to finish rebooting and for the Remote Drive Erase “continue” screen to appear in the SOL window (shown in Figure 10 below).
7. For KVM Remote Control, in the session window, click **Start > Shutdown > Restart** (on the remote client) to restart the client and boot it to the ISO image you previously shared. If Windows is not running on the remote client, then click the **Power** button as shown in Figure 9 below:



Figure 9: The VNC Viewer Plus Power Menu Icon

8. Press 'c' to continue.

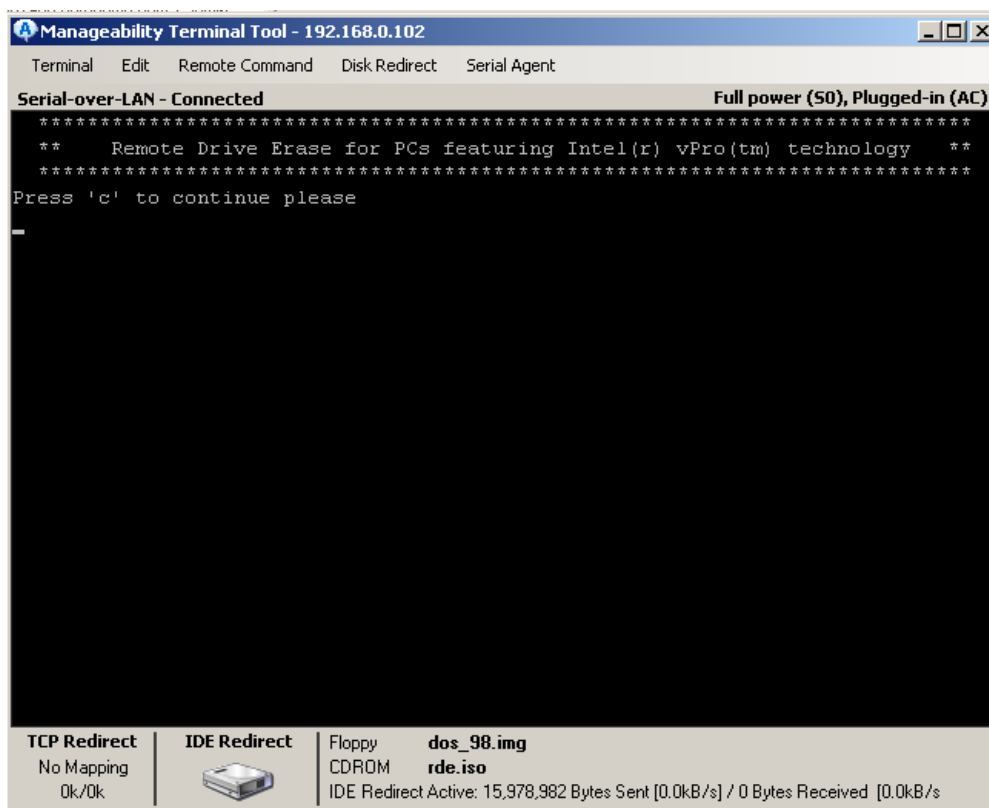


Figure 10: Press 'c' to Continue

All hard drive partitions found on the Managed Client are listed using Linux device nomenclature. Boot drives are designated by an asterisk (\*). Figure 11 shows the Commander SOL/IDER window, but the same content should appear in the KVM Remote Control session window.

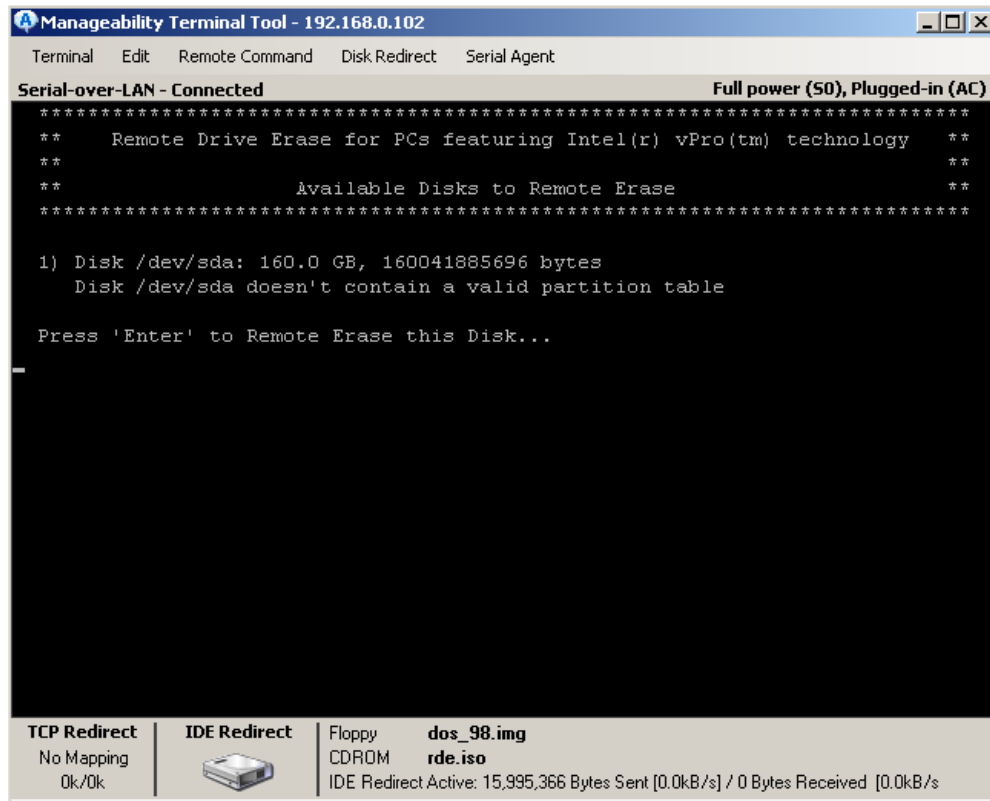
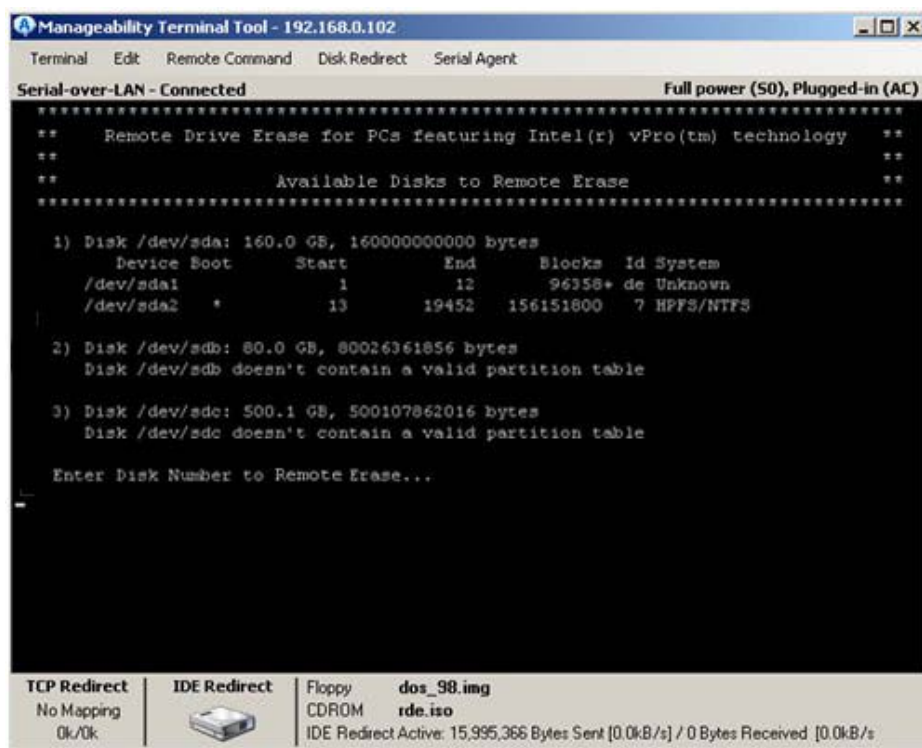


Figure 11: The Main Remote Drive Erase Menu

**NOTE**

The screen in Figure 12 below shows a system with three hard disk drives (two have already been erased and thus display the message “doesn't contain a valid partition table”). If you are connected to a system with multiple hard drives, enter the number of the drive you wish to erase.

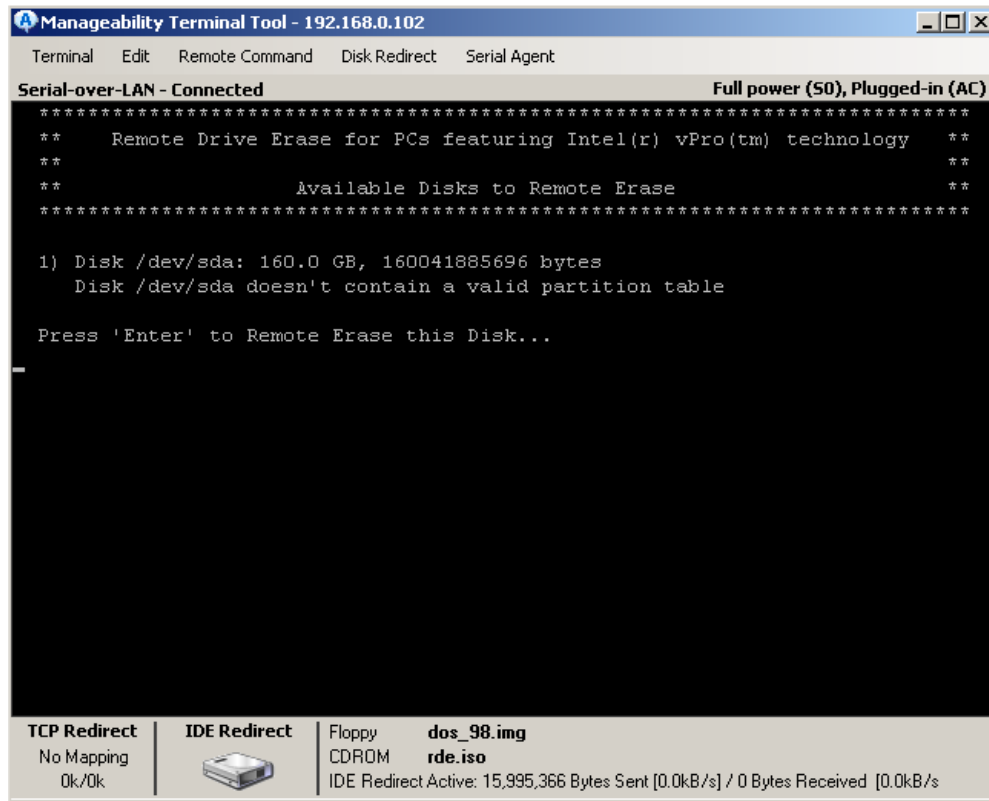


**Figure 12: Client with Multiple Hard Disk Drives**

At this point you are ready to erase the Managed Client's hard drive from the Management Console System. Proceed to the next section.

### 3.5 Remotely Erasing the Managed Client's Hard Drive

Now that you have accessed the Managed Client's hard drive partitions from the Management Console System, you are ready to remotely and securely erase them.



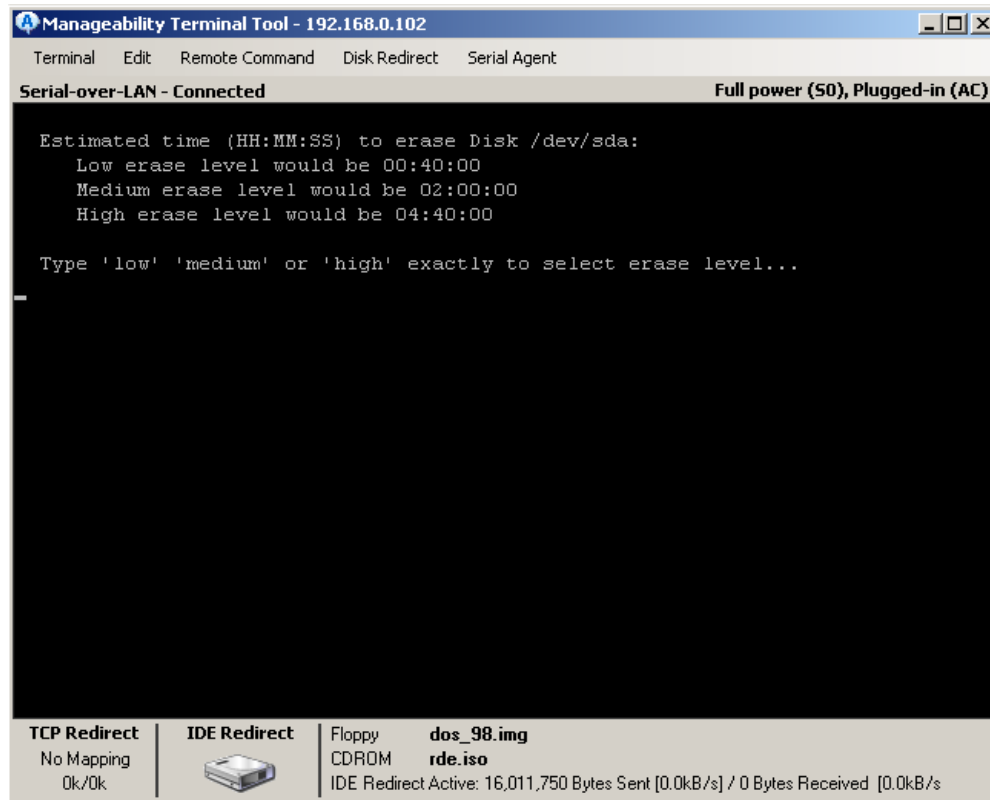
**Figure 13: Client with One Hard Disk Drive**

1. If you are connected to a system with only one hard disk drive (as shown in Figure 13 above), press the **Enter** key.

If you are connected to a system with multiple hard disk drives (as shown in Figure 12), enter the number of the drive you wish to erase and press the **Enter** key.

Note that when Remote Drive Erase finishes erasing that drive, it will return to this menu and you will have the opportunity to select the next drive to erase.

The Erase Level menu is displayed.



**Figure 14: Menu to Select Erase Level (Low/Medium/High)**

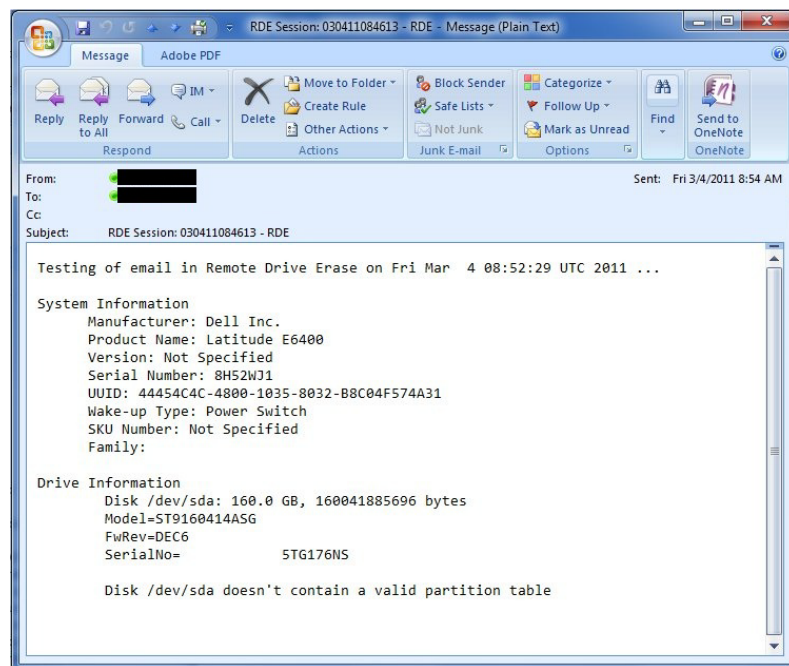
2. In the Erase Level menu (Figure 14) select the desired erase level. Low level makes a single pass, writing 0's to the hard drive. Medium level makes three passes: two passes writing random data (1's and 0's), then one pass writing 0's. High level makes seven passes: six writing random data and one writing 0's. Note that you must type the entire word exactly (i.e., "low" or "medium" or "high") and press the **Enter** key.

**NOTE**

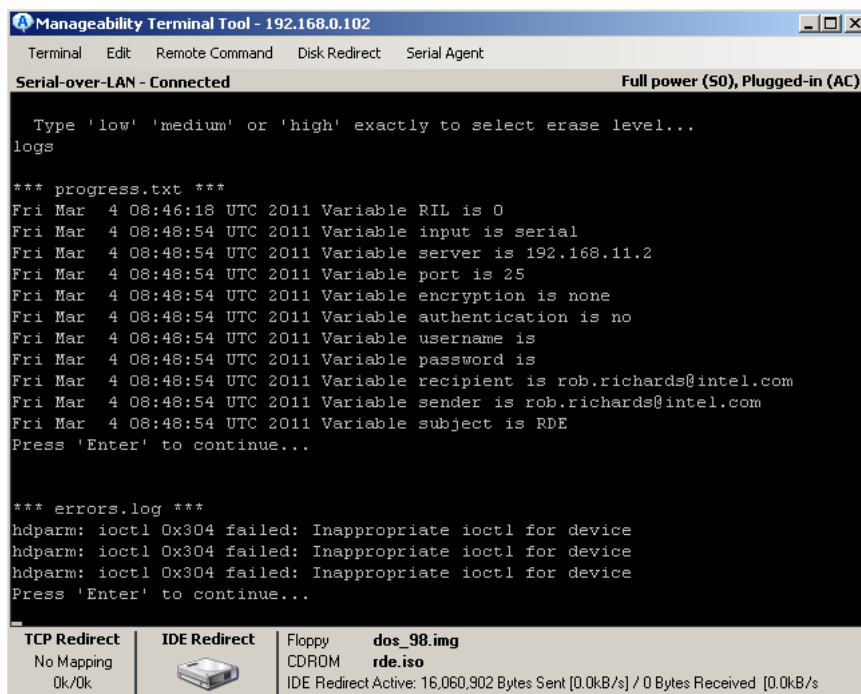
To test email notification **without erasing the remote client's hard disk drive**, you can type "test" at the prompt to send a test email to the account specified in ISO Builder when you created the ISO (see section 3.1, step 3 on page 9). An example email is shown in Figure 15 below.

Also, you can enter "logs" at the prompt to view an error log (shown in Figure 16 below) in case the test email did not work as expected.

Note that you must still connect to the remote client (section 3.2 or 3.3) and reboot it to your ISO (section 3.4) in order to test the email notification as described in this note.



**Figure 15: Test email**

**Figure 16: Error log file**

*Note that the “hdparm” errors listed toward the end of the logfile are normal and not a cause for concern. One “hdparm” error will be shown for each partition on the drive being erased.*

Remote Drive Erase begins erasing the specified disk, using the Linux “shred” utility, as shown in Figure 17. In addition, if you specified an SMTP mail server and recipient email address, the ISO sends a status email message stating that the secure erase has begun.

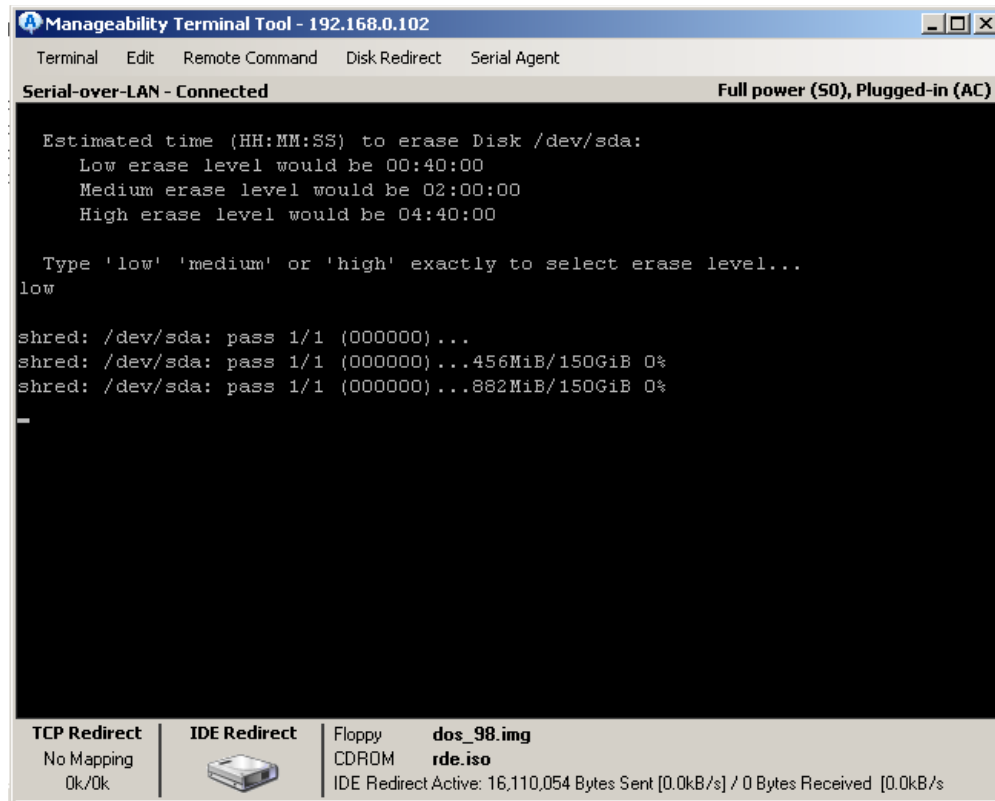
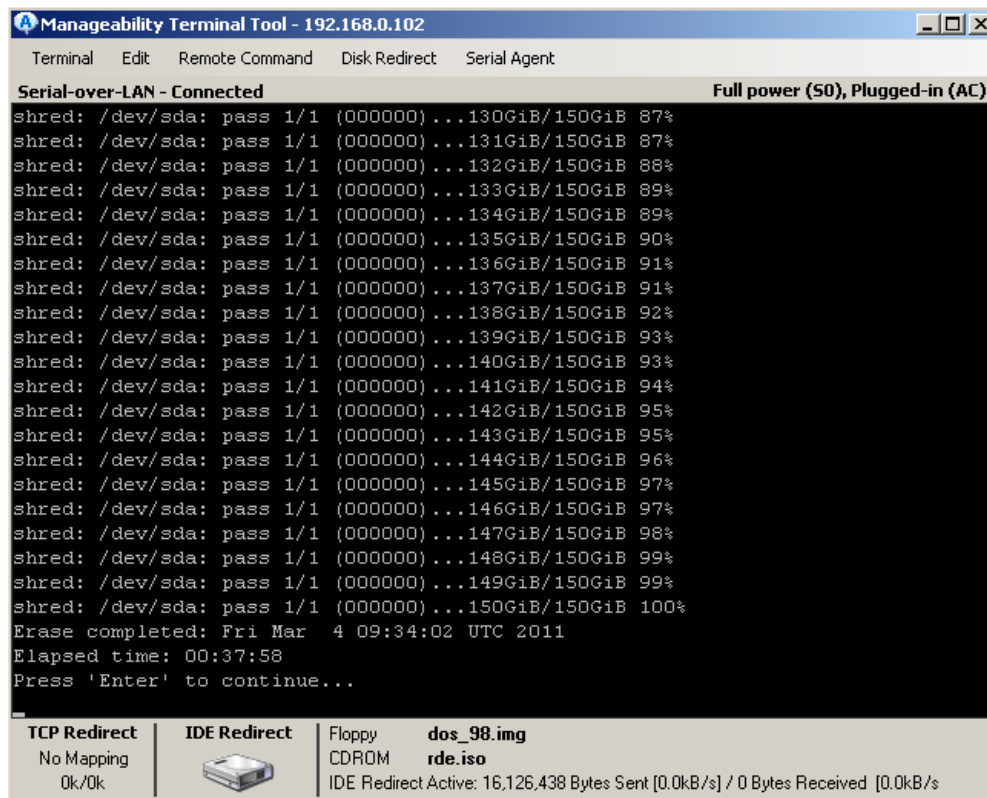


Figure 17: Remote Drive Erase Uses the Shred Utility

- When the erase completes, the message “Erase completed” is displayed, as shown in Figure 18. Press the **Enter** key to return to the main Remote Drive Erase menu. If a mail server and recipient address were specified, a status email message is sent stating that the disk was erased successfully.



**Figure 18: The Erase Completes Successfully**

- If you are connected to a system with multiple hard disk drives, select the next hard disk to erase and repeat steps 2 - 3 above. Otherwise, if all drives on the system have been erased (as indicated by the message “does not contain a valid partition table”), end the SOL session and disconnect from the remote system (in the Manageability Commander tool this is done by clicking **Terminal > Exit**).

## 4 Building the ISO

---

The components needed to rebuild the ISO file have been included in this Use Case Reference Design download package.

### 4.1 Build System Requirements

The ISO must be built using a Linux system. We have included the necessary components and files to rebuild the included ISO file rde.iso.

Prepare your system as follows:

1. Install Ubuntu 10.10 on an x86 based system.
2. Verify that your system is connected to the Internet.
3. Launch a terminal and type the following commands to install required packages:
  - `sudo apt-get install build-essential`
  - `sudo apt-get install zlib1g-dev`
  - `sudo apt-get install libncurses5-dev`
  - `sudo apt-get install upx`
  - `sudo apt-get install nasm`

### 4.2 Reference Links

The following components were included in the Use Case Reference Design download package and do NOT need to be downloaded. They are included here for your reference. If you need to update one of these packages, you will need to edit the makefile to include the new .tar file name.

- Busybox 1.16.2:  
<http://www.busybox.net/downloads/busybox-1.16.2.tar.bz2>
- Linux Kernel 2.6.33.2:  
<http://www.kernel.org/pub/linux/kernel/v2.6/linux-2.6.33.2.tar.bz2>
- SAMBA 3.4.1:  
<http://samba.org/samba/ftp/stable/samba-3.4.1.tar.gz>
- Syslinux 3.84:  
<http://www.kernel.org/pub/linux/utils/boot/syslinux/syslinux-3.84.tar.gz>
- Zlib 1.2.3:  
<http://www.zlib.net/zlib-1.2.3.tar.gz>
- NTFS-3G 2010.3.6:  
<http://tuxera.com/opensource/ntfs-3g-2010.3.6.tgz>

## 4.3 Building the ISO

Perform the following steps to build the ISO file rde.iso.

1. Extract the rde.tar.gz file onto your Ubuntu 10.04 or higher Linux system in any directory. The .tar is extracted to create a directory structure with the root directory "rde".



### NOTE

*Do not extract the .tar file on a Windows system and open the .txt files. Windows adds control characters to the files which will corrupt the build process.*

2. Open a terminal session and navigate to the rde directory.
3. Type "sudo make" and wait for the rde.iso file and iso\_root directory to build.
4. In your ISO Builder directory replace 'iso\_root' with the new 'iso\_root' directory in the Linux build. This will allow you to customize your rde.iso file (see section 3.1)

Upon build completion, the rde.iso file is built, which erases hard drives using a SOL/IDER connection or KVM Remote Control connection.

## 5 Appendix A: Architectural Considerations for the Included ISO File

---

The remote share ISO was developed to be as small as possible in order to facilitate quick SOL/IDER sessions. The Managed Client must transfer the entire ISO to memory over the network before booting. The small size was made possible by only including components in the Linux ISO that were necessary for remote share functionality.

The major components are:

- Linux Kernel – Provides core OS features. Compiled with minimal driver and module support
- Busybox – Shell support and drive mounting. Configured with default configuration options.
- shred – a Linux utility that erases hard drives.

## 6 Appendix B: Remote Drive Erase Error Messages

---

```
*****
** Remote Drive Erase for PCs featuring Intel(r) vPro(tm) technology **
**                                                                    **
** A remote serial connection was not found on this system.          **
** Remote Drive Erase requires this connection and will now halt.    **
*****
```

This message is only displayed on the client screen. It will appear if the system being booted is not an Intel vPro technology based system or Intel AMT is not enabled on the system. One possible reason for this message to be displayed is if the rde.iso image has been burned to a CD and then used to boot a system that does not have Intel vPro technology. If you establish a SOL/IDER connection to an Intel vPro technology based client and then boot the client with rde.iso, this message should not be displayed.

```
*****
** Remote Drive Erase for PCs featuring Intel(r) vPro(tm) technology **
**                                                                    **
** An appropriate Intel network adapter was not found on this system. **
** Remote Drive Erase requires this adapter and will now halt.        **
*****
```

This message is displayed on both the client screen and the SOL terminal. It will be displayed if the client system does not have an Intel LAN adapter installed. If the client system is an Intel vPro technology based system, this message should never be displayed.

However, it might be displayed if the managed client has a non Intel LAN adapter installed or if the managed client has been booted with a CD of the rde.iso image and does not have an Intel LAN adapter. However, in that case the previous message would be displayed and Remote Drive Share would likely exit before displaying this message.

```
*****
**   Remote Drive Erase for PCs featuring Intel(r) vPro(tm) technology   **
**                                                                    **
**       No available Device/Partitions were found on this system.       **
**   Remote Drive Erase requires an available device and will now halt.   **
*****
```

This message is displayed on both the client screen and the SOL terminal. This message occurs if there are no SATA drives installed in the system. It also might occur if the hard drive has completely failed or lost power and is no longer recognized by the client system.

```
*****
**   Remote Drive Erase for PCs featuring Intel(r) vPro(tm) technology   **
**                                                                    **
**       A working DHCP server was not found on this network.           **
**   Remote Drive Erase requires a valid IP address and will now halt.   **
*****
```

This message is displayed on both the client screen and the SOL terminal. This message can occur if there is no DHCP server for Remote Drive Share to use. This should be a rare case since the SOL/IDER connection also needs the DHCP server to be running. This message might be displayed in the event that a system without a network connection was booted from a CD with rde.iso.