

# Intel® vPro™ Technology Use Case Reference Design

Remote Drive Mounting

---

Revision 1.1

March 2014

Document ID: 1101

# Revision History

Revision	Revision History	Date
1.0	Initial release.	August 2011
1.1	Updated for Intel ME 9.	March 2014

By using this document, in addition to any agreements you have with Intel, you accept the terms set forth below.

You may not use or facilitate the use of this document in connection with any infringement or other legal analysis concerning Intel products described herein. You agree to grant Intel a non-exclusive, royalty-free license to any patent claim thereafter drafted which includes subject matter disclosed herein.

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.

A "Mission Critical Application" is any application in which failure of the Intel Product could result, directly or indirectly, in personal injury or death. SHOULD YOU PURCHASE OR USE INTEL'S PRODUCTS FOR ANY SUCH MISSION CRITICAL APPLICATION, YOU SHALL INDEMNIFY AND HOLD INTEL AND ITS SUBSIDIARIES, SUBCONTRACTORS AND AFFILIATES, AND THE DIRECTORS, OFFICERS, AND EMPLOYEES OF EACH, HARMLESS AGAINST ALL CLAIMS COSTS, DAMAGES, AND EXPENSES AND REASONABLE ATTORNEYS' FEES ARISING OUT OF, DIRECTLY OR INDIRECTLY, ANY CLAIM OF PRODUCT LIABILITY, PERSONAL INJURY, OR DEATH ARISING IN ANY WAY OUT OF SUCH MISSION CRITICAL APPLICATION, WHETHER OR NOT INTEL OR ITS SUBCONTRACTOR WAS NEGLIGENT IN THE DESIGN, MANUFACTURE, OR WARNING OF THE INTEL PRODUCT OR ANY OF ITS PARTS.

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 products described in this document 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 go to:  
<http://www.intel.com/design/literature.htm>

Intel® vPro™ Technology is sophisticated and requires setup and activation. Availability of features and results will depend upon the setup and configuration of your hardware, software and IT environment. To learn more visit: <http://www.intel.com/technology/vpro>.

Intel® Active Management Technology Requires activation and a system with a corporate network connection, an Intel® AMT-enabled chipset, network hardware and software. For notebooks, Intel AMT may be unavailable or limited over a host OS-based VPN, when connecting wirelessly, on battery power, sleeping, hibernating or powered off. Results dependent upon hardware, setup and configuration. For more information, visit [Intel® Active Management Technology](#).

KVM Remote Control (Keyboard, Video, Mouse) is only available with Intel® Core™ i5 vPro™ and Core™ i7 vPro™ processors with Intel® Active Management technology activated and configured and with integrated graphics active. Discrete graphics are not supported.

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

Intel, the Intel logo, Core, 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 © 2011-2014 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	Remote ISO Launcher .....	8
3.1.1	Setup .....	8
3.1.2	Perform Remote Drive Mount .....	10
3.2	KVM Remote Control .....	12
3.3	Serial Over LAN .....	16
<b>A</b>	<b>Appendix: Building the ISO .....</b>	<b>23</b>
A.1	Build System Requirements .....	23
A.2	Building the ISO .....	24
<b>B</b>	<b>Appendix: Remote Drive Mounting Error Messages .....</b>	<b>25</b>



# 1 Preface

---

Intel® vPro™ technology gives the Information Technology (IT) professional the capability to remotely boot a managed client with Intel vPro technology to a remote ISO image file. The procedure described in this document remotely boots a small Linux\* OS on the remote managed client and then exports the drive as an iSCSI target to a remote system. Once booted on the client, the ISO passes a Challenge Handshake Authentication Protocol (CHAP) username and random password back to the management console over the secured SOL session. Using iSCSI Initiator, the remote client's shared hard drive can then be mounted at the block level to the management console's file system as if it were physically located in the console system. This allows the IT professional to perform low level actions on the remote client's hard drive from the console system, such as reformatting or imaging the remote client's hard drive. This process works regardless of the state of the remote client's operating system.

## 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 to remotely perform low level disk actions on a computer with Intel vPro technology. 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

- Remote ISO Launcher (RIL)  
<http://communities.intel.com/docs/DOC-5943>

## 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 enable remote mounting of the client hard drive at the block level. This capability could be useful in remotely reformatting a client hard drive, as well as remotely retrieving data from a system who's OS will not boot.

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 and remotely mounting 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:
  - Configured for use with Intel vPro technology
  - Wired network connection
2. Management Console Application supporting Intel vPro technology's SOL/IDER feature

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

## 2.2 Process Overview

The following table provides a high level overview of the remote client hard drive sharing and mounting 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.



### NOTE

*As part of this process, system credential information (including a user name and randomly generated password) for the Managed Client is passed to the Management Console's SOL window, for use in mounting the client's hard drive. If the Managed Client has not been configured to use TLS or MTLS security for Serial over LAN (SOL) connections (for example, if the client was provisioned in SMB mode), this username and password will be passed as clear text. Also, if you are using KVM Remote Control with port 5900, it may be possible for a "sniffer" to read the data.*

<b>Description</b>	The IT Professional ensures prerequisites are met and remotely accesses the Managed Client's hard drive.
<b>Prerequisites</b>	<ul style="list-style-type: none"> <li>• SOL/IDER must be enabled in Intel AMT on the Managed Client(s).</li> <li>• The Managed Client must be configured.</li> <li>• The Linux* ISO file included with this Use Case Reference Design (remotedrivemount.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> <li>• When 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>• An iSCSI initiator must be on the Management Console. Windows 7 and Windows Server 2008 have an iSCSI initiator included. If you are using Windows XP, you must download and install an iSCSI initiator.</li> </ul>
<b>Process flow</b>	<ol style="list-style-type: none"> <li>1. Identify the Managed Client whose hard drive you need to access.</li> <li>2. From the Management Console, either:               <ol style="list-style-type: none"> <li>a) Use KVM initiate connection reboot to selected ISO with IDER</li> <li>b) Use SOL initiate connection reboot to selected ISO with IDER</li> <li>c) Use RIL for automated iSCSI connection run Remote ISO Launcher</li> </ol> </li> <li>3. The Managed Client will boot the specified Linux ISO</li> <li>4. Create an iSCSI session to the client's hard drive.</li> </ol>
<b>Expected outcome</b>	The Managed Client's hard drive is mounted to the Management Console's file system as if it were physically in the console system.

## 3 Detailed Steps

---

Establishing an iSCSI connection to the Managed Client's hard drive may be performed using one of three remote control methods:

- Remote ISO Launcher (RIL)  
RIL automates much of the process and is therefore the recommended method whenever possible.
- KVM Remote Control  
Any Intel AMT enabled KVM Remote Control console that also supports IDE Redirection can be used. This document outlines using RealVNC VNC Viewer Plus.
- Serial Over LAN (SOL)  
Any Intel AMT enabled console that supports SOL and IDE Redirection can be used. This document outlines using Manageability Commander.

### 3.1 Remote ISO Launcher

To obtain Remote ISO Launcher, download and open the Use Case Reference Design *Remote ISO Launcher (RIL)*, available from the following website:

<http://communities.intel.com/docs/DOC-5943>

To use Remote ISO Launcher to reboot the Managed Client and automatically mount its hard drive, perform the steps in the following subsections.

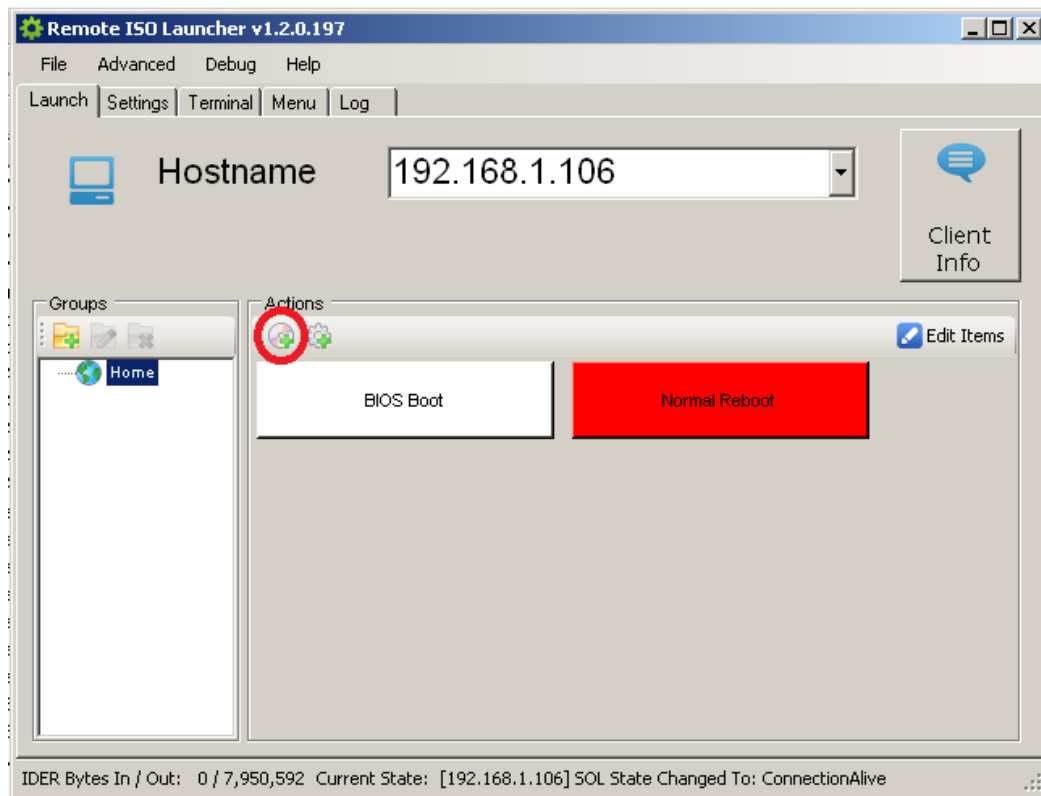
#### 3.1.1 Setup

Do the following one time to set up Remote ISO Launcher:

1. If you haven't already done so, download and extract the Remote ISO Launcher (RIL) app from <http://communities.intel.com/docs/DOC-5943>.
2. If you have not already done so, copy the Linux ISO file **remotedrivemount.iso** (included in this Use Case Reference Design's download .zip file) to a location that is accessible to the Management Console System, such as the Management Console System's hard drive.



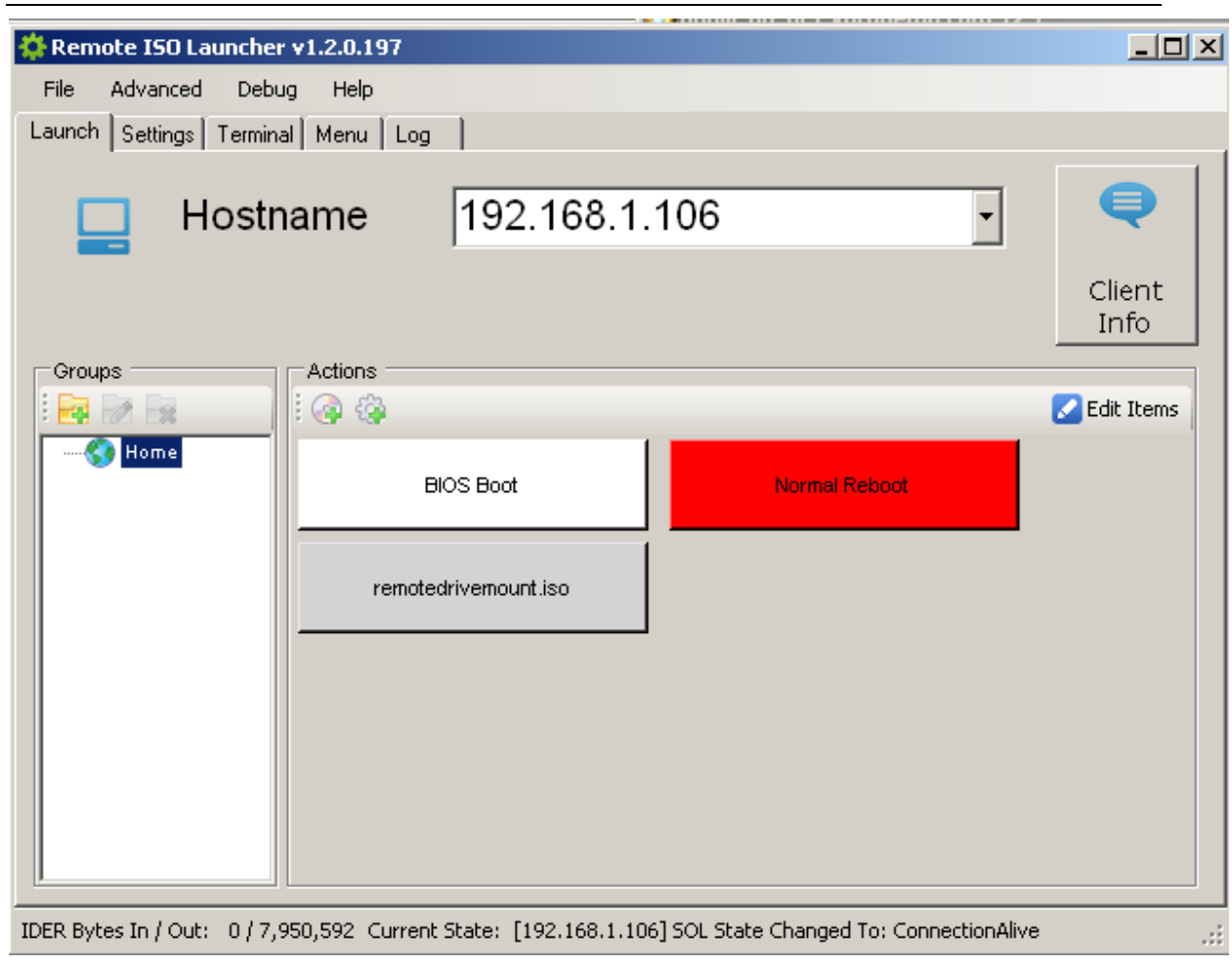
3. In the RIL app folder, double-click **RemoteISOLauncher.exe** to launch the RIL app.



**Figure 1: Remote ISO Launcher**

4. To create a Boot Image button for remotedrивemount.iso, click the CD+ icon circled above.
5. In the Manage ISO Images dialog, enter **REMOTEDRIVEMOUNT.ISO** for the Friendly Name and click **Browse** to browse to the location of the remotedrивemount.iso file.
6. Click **Add**. The friendly name "REMOTEDRIVEMOUNT.ISO" appears in the lower pane, along with the path you selected.

7. Click **Done**. The Manage ISO Images dialog closes, and now the button **REMOTEDRIVEMOUNT.ISO** appears in the Boot Images pane of the Launch tab.  
Note



**Figure 2: New Boot Image Button Added**

8. Click **File -> Save**.

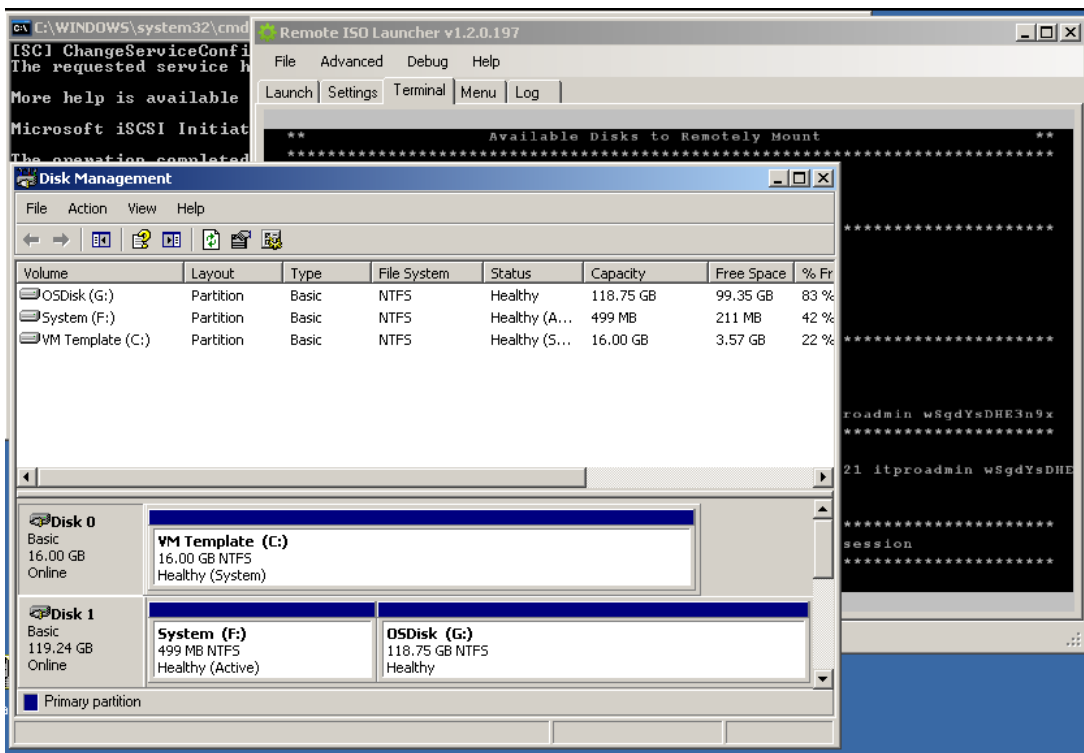
### 3.1.2 Perform Remote Drive Mount

Do the following each time you want to perform a remote drive mount:

1. On the Launch tab, enter the IP Address of the Managed Client that you want to reboot to remotedrivemount.iso and automatically mount its hard drive.
2. If desired, click **Client Info** to ensure that RIL can communicate with this Managed Client.
3. Click the Settings tab and enter the Intel AMT username and password. Adjust any other settings as required by Intel AMT's configuration.

4. Click the Launch tab.
5. Click your new **REMOTEDRIVEMOUNT.ISO** button in the Boot Images section to reboot the Managed Client and automatically mount its hard drive. When the blue checkmark appears in the corner of the **REMOTEDRIVEMOUNT.ISO** button, the ISO has initiated the IDer channel.

At this point, remotedrивemount.iso has already run the batch file iSCSI.bat (included with Remote ISO Launcher under the batch folder) and mounted the Managed Client's hard drive to the Management Console file system. It will also open Disk Manager so you can verify the drive connection.



**Figure 3: The Managed Client's Hard Drive is Automatically Mounted**

Perform any desired work on the remote drive. When finished, close the session as follows:

1. Close Disk Manager.
2. In Remote ISO Launcher, select the terminal tab and press **Enter**.

## 3.2 KVM Remote Control

Follow the steps below:



### NOTE

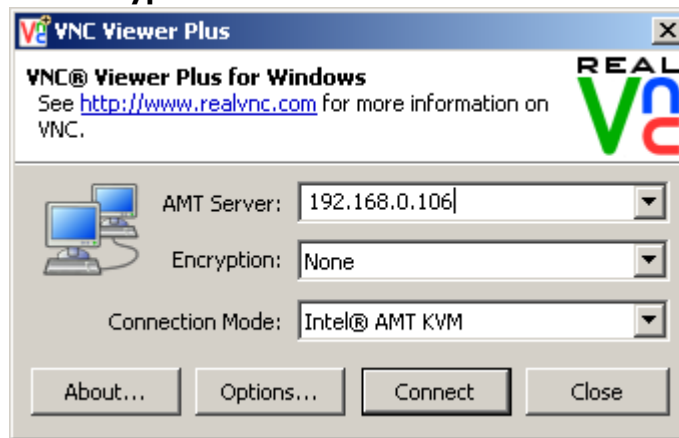
*The procedure described below uses RealVNC VNC Viewer Plus, provided at the link below, as the management console application. However, the concept should be applicable to other management console applications. The intent is to provide a detailed example of how the remote OOB hard drive access process can be accomplished with the KVM Remote Control, which readers can then apply to their specific IT environment and whatever management console application they are using.*

*RealVNC VNC Viewer Plus is available here:*

<https://www.realvnc.com/products/viewerplus/>

*If you wish to use RealVNC VNC Viewer Plus, download and install it now.*

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.
8. If you have not already done so, copy the Linux ISO file **remotedrivemount.iso** (included in this Use Case Reference Design's download .zip file) to a location that is accessible to the Management Console System, such as the Management Console System's hard drive.
9. Click the IDE-Redirection menu icon, shown in Figure 4 below.



**Figure 4: The VNC\* Viewer Plus IDE-Redirection Menu Icon**

10. Browse to the location where you copied the remotedrivemount.iso file. Select the desired file and click **Open**. Click **Mount**.
11. Click the **Power** button as shown in Figure 5 below. Then click **Reset**.

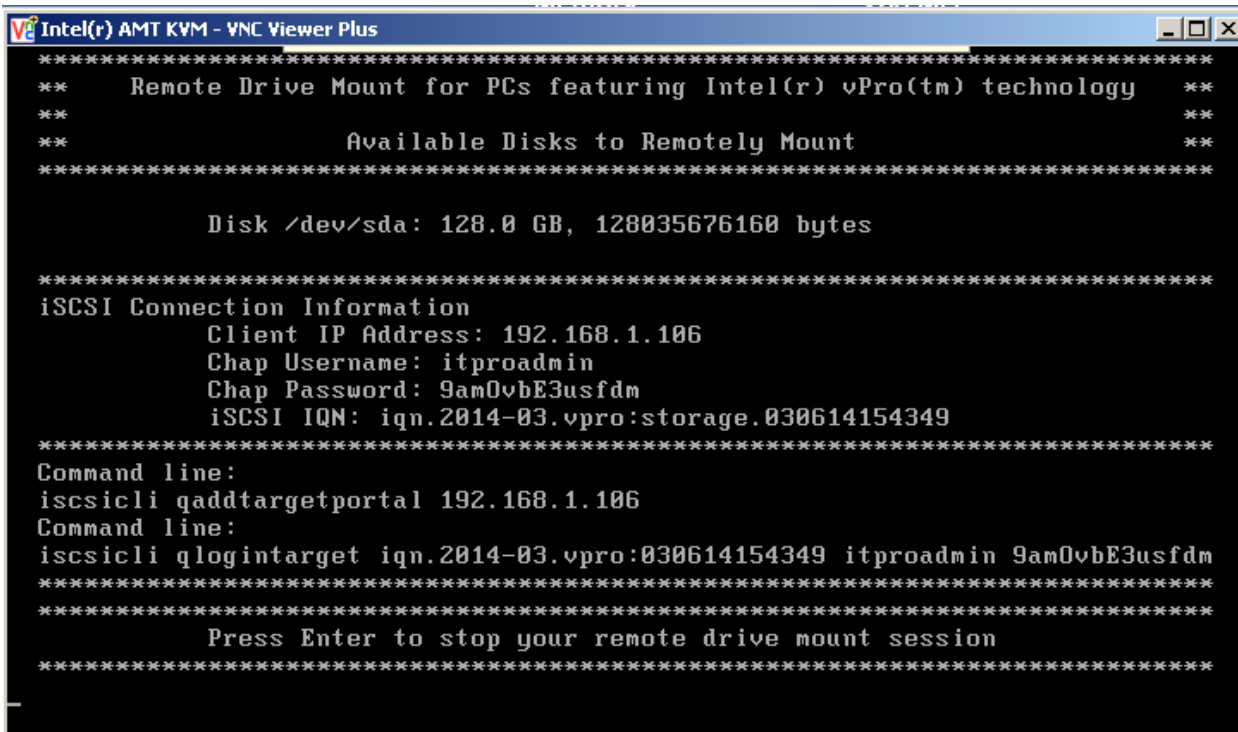


**Figure 5: The VNC Viewer Plus Power Menu Icon**

12. Choose **Boot to CD/DVD** and click **Reset**. If prompted to perform a non-graceful reset, click **Yes**.
13. After the Managed Client reboots and the Linux operating system loads, you will be prompted to press "c" to continue. Press "c" in your KVM session.  
 The purpose of pressing "c" is to determine where screen output will be delivered. Screen output includes the Managed Client's IP Address and username/password to access the iSCSI target.

All hard drive partitions found on the Managed Client are listed using Linux device nomenclature. iSCSI connection information is displayed, which you will use in the following section to mount the client's hard drive. In addition, command lines are displayed which can be used from Windows command prompt.

Figure 6 shows the Commander SOL/IDER window, but the same content should appear in the KVM Remote Control session window.



```

Intel(r) AMT KVM - VNC Viewer Plus
*****
Remote Drive Mount for PCs featuring Intel(r) vPro(tm) technology
*****
Available Disks to Remotely Mount
*****
Disk /dev/sda: 128.0 GB, 128035676160 bytes

*****
iSCSI Connection Information
Client IP Address: 192.168.1.106
Chap Username: itproadmin
Chap Password: 9am0vbE3usfdm
iSCSI IQN: iqn.2014-03.vpro:storage.030614154349
*****
Command line:
iscsicli qaddtargetportal 192.168.1.106
Command line:
iscsicli qlogintarget iqn.2014-03.vpro:030614154349 itproadmin 9am0vbE3usfdm
*****
Press Enter to stop your remote drive mount session
*****

```

**Figure 6: Remote Drive Mounting Main Screen**



#### NOTE

*The password for the CHAP user name and target name is randomly generated by the Remote Drive Mounting software.*

Now that you have created an iSCSI target of the Managed Client's hard drive on your Intranet, you are ready to mount it to the Management Console. This can be done using either of two methods:

- Run an iSCSI initiator on the Management Console and use the provided iSCSI connection information, including a CHAP user name and password.
- Open a command prompt on the Management Console and enter the provided command lines if you are using Microsoft Windows and the Microsoft iSCSI initiator.

The steps below are for the command line method. You can open a command prompt on the Management Console and enter the iscsicli command lines provided on the Remote Drive Mounting Main Screen in the SOL window (see Figure 7 below). The command lines are only applicable to a Microsoft Windows console that is using the Microsoft iSCSI initiator.

```

Intel(r) AMT KVM - VNC Viewer Plus
*****
Remote Drive Mount for PCs featuring Intel(r) vPro(tm) technology
*****
Available Disks to Remotely Mount
*****
Disk /dev/sda: 128.0 GB, 128035676160 bytes
*****
iSCSI Connection Information
Client IP Address: 192.168.1.106
Chap Username: itproadmin
Chap Password: 9am0vbE3usfdm
iSCSI IQN: iqn.2014-03.vpro:storage.030614154349
*****
Command line:
iscsicli qaddtargetportal 192.168.1.106
Command line:
iscsicli qlogintarget iqn.2014-03.vpro:030614154349 itproadmin 9am0vbE3usfdm
*****
Press Enter to stop your remote drive mount session
*****

```

**Figure 7: KVM Window Showing iSCSI Command Lines**

1. On the Management Console System, open a command prompt window and enter the first iscsicli command line in the KVM window (note that Figure 7 above is just an example, and that you should use the command line provided on the actual Remote Drive Mounting main screen in your active KVM Remote Control session). This command adds the Managed Client's hard drive to iSCSI target portal list.
2. Once the first command completes, enter the second iscsicli command from the Remote Drive Mounting main screen to log in to the target portal (which results in mounting the Managed Client's hard drive).

Once the second iscsicli command completes, the Managed Client's hard drive will be mounted to the Management Console. It can be viewed under My Computer or under Disk Manager.

Perform any desired tasks on the remote hard drive. When finished, disconnect it as follows:

1. Close My Computer, Disk Manager, and / or any open files on the remote hard disk.
2. In the KVM session, press **Enter**.
3. Reboot the Managed Client.

## 3.3 Serial Over LAN

Follow the steps below.



### NOTE

*The procedure described below uses Intel's Manageability Commander Tool, provided 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 Serial Over LAN, 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:*

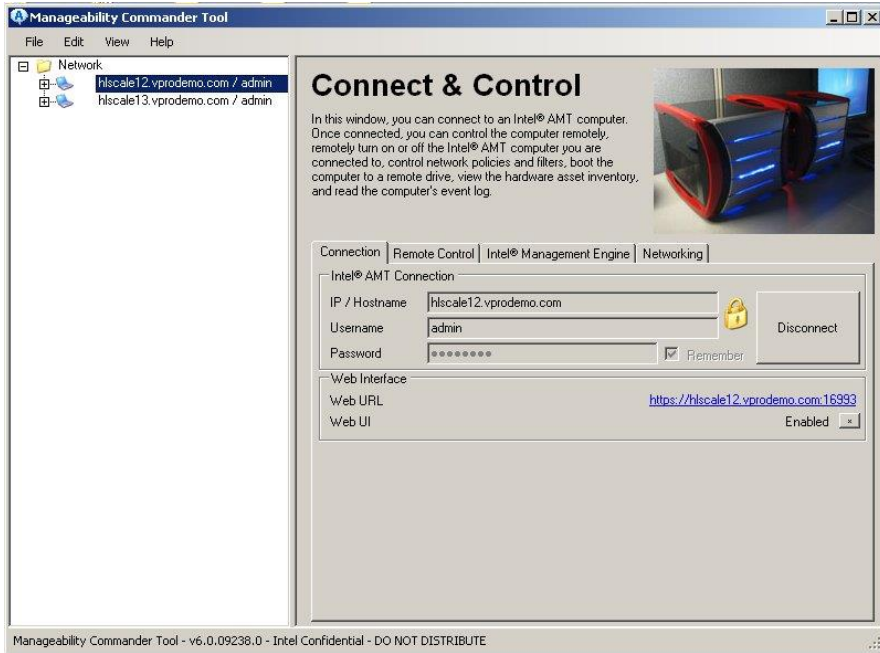
*<http://software.intel.com/en-us/articles/download-the-latest-version-of-manageability-developer-tool-kit/>*

*If you wish to use Intel's Manageability Commander Tool, install the Manager Developer Toolkit now 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.*

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.

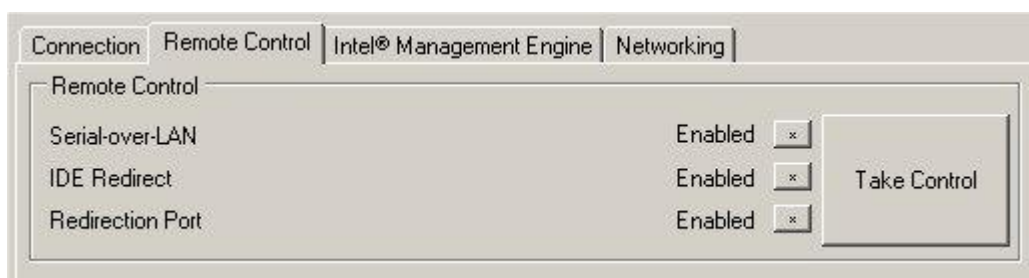


3. In the left-hand pane, right-click on the computer you just added and select **Connect** from the pop-up menu. The **Connect** button in the right-hand pane changes briefly to **Abort Connect**, then after a minute or so it changes again to **Disconnect** once the connection is established.



**Figure 8: 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 9: 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 10: 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.



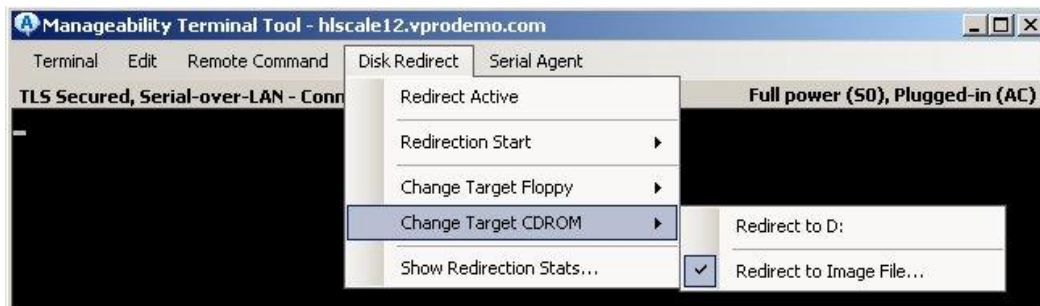
#### **NOTE**

*If the client's hard drive is Software Disk Encrypted, the appropriate decryption agent must be running on the management console. When prompted for the client's Software Disk Encryption password, have the client's owner supply his or her password.*

6. If you have not already done so, copy the Linux ISO file **remotedrivemount.iso** (included in this Use Case Reference Design's download .zip file) to a location that is accessible to the Management Console System, such as the Management Console System's hard drive.
7. 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 11 below.

**NOTE**

*Some versions of the Manageability Commander Tool may require you to specify a floppy image as well. If your version requires this, you can specify remotedrivemount.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 11: Terminal Tool Redirection Menu**

8. Browse to the location where you copied the remotedrivemount.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 12 below).
9. In Commander, from the menu bar, select **Disk Redirect > Redirect Active**. The message **IDE Redirect Active** appears at bottom (as shown below).

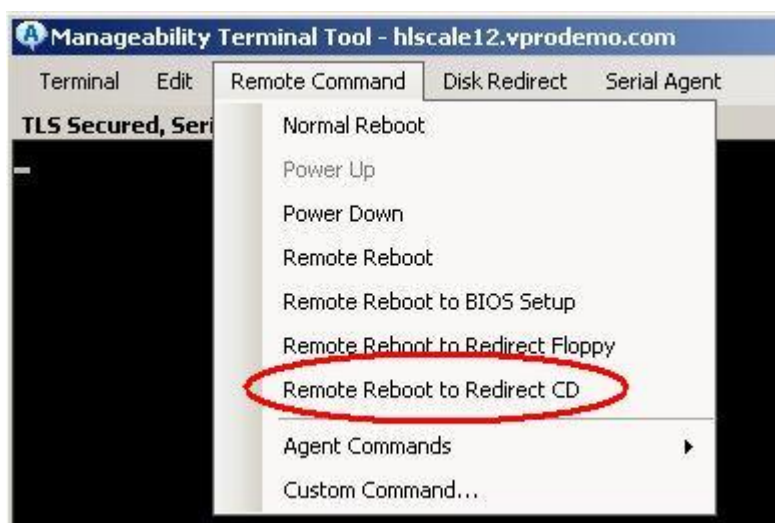


**Figure 12: Terminal Tool Information Panel at Bottom**

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

**NOTE**

*If the Managed AMT Client has not been configured to use TLS or MTLS security for SOL connections (for example, if the client was provisioned in SMB mode), be aware that a user name and randomly generated password for the Managed Client hard drive will be passed as clear text to the Management Console's SOL window upon completing this step. Also, if you are using KVM Remote Control with port 5900, it may be possible for a "sniffer" to read the data.*

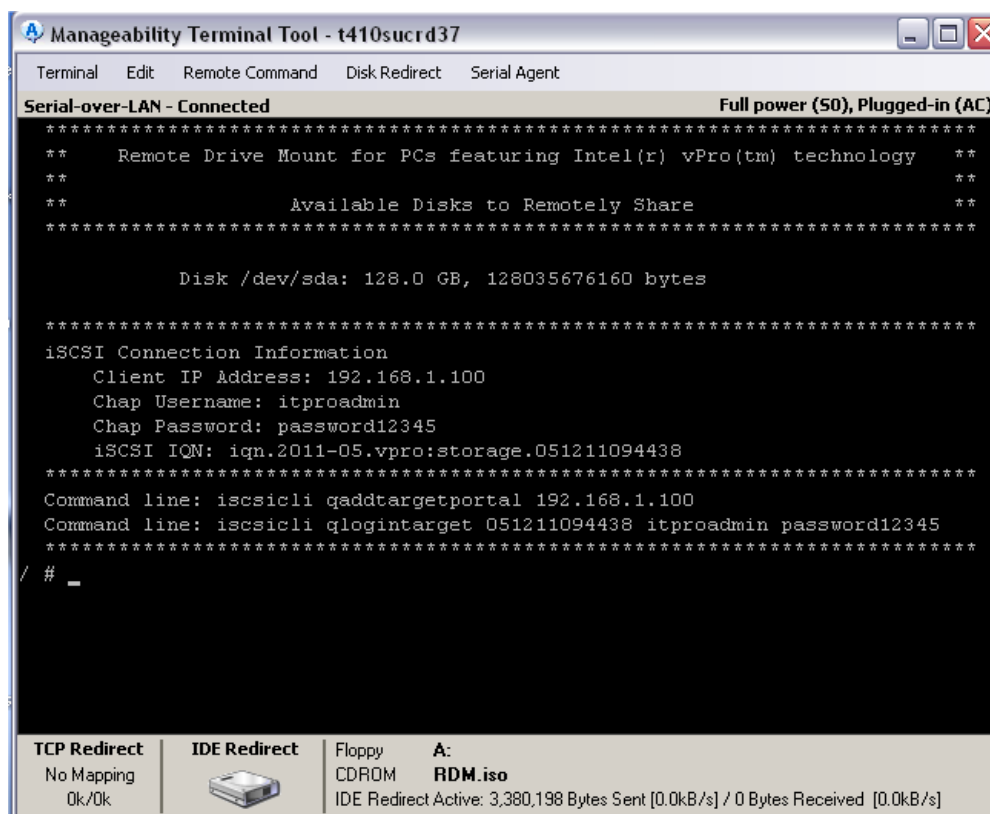


**Figure 13: Remote Reboot to Redirect CD Menu**

- Click **Yes** in the **Reboot Computer to Remoted CDROM?** dialog. Wait for the Managed Client to finish rebooting and for the Remote Drive Mounting main screen, which contains credential information for the Managed Client, to appear in the SOL window (shown in Figure 14 below).
- After the Managed Client reboots and the Linux operating system loads, you will be prompted to press "c" to continue. Press "c" either in the SOL KVM session.  
The purpose of pressing "c" is to determine where screen output will be delivered. Screen output includes the Managed Client's IP Address and username/password to access the iSCSI target.

All hard drive partitions found on the Managed Client are listed using Linux device nomenclature. iSCSI connection information is displayed, which you will use in the following section to mount the client's hard drive. In addition, command lines are displayed which can be used from Windows command prompt.

Figure 14 shows the Commander SOL/IDER window, but the same content should appear in the KVM Remote Control session window.



**Figure 14: Remote Drive Mounting Main Screen**



#### NOTE

*The password for the CHAP user name and target name is randomly generated by the Remote Drive Mounting software.*

Now that you have created an iSCSI target of the Managed Client's hard drive on your Intranet, you are ready to mount it to the Management Console. This can be done using either of two methods:

- Run an iSCSI initiator on the Management Console and use the provided iSCSI connection information, including a CHAP user name and password.
- Open a command prompt on the Management Console and enter the provided command lines if you are using Microsoft Windows and the Microsoft iSCSI initiator.

Steps below are for the command line method. You can open a command prompt on the Management Console and enter the iscsicli command lines provided on the Remote Drive Mounting Main Screen in the SOL window (see Figure 15 below). The command

lines are only applicable to a Microsoft Windows console that is using the Microsoft iSCSI initiator.

```

Manageability Terminal Tool - t410sucrd37
Terminal Edit Remote Command Disk Redirect Serial Agent

Serial-over-LAN - Connected Full power (S0), Plugged-in (AC)
*****
** Remote Drive Mount for PCs featuring Intel(r) vPro(tm) technology **
**
** Available Disks to Remotely Share **
*****

Disk /dev/sda: 128.0 GB, 128035676160 bytes

*****
iSCSI Connection Information
Client IP Address: 192.168.1.100
Chap Username: itproadmin
Chap Password: password12345
iSCSI IQN: iqn.2011-05.urn:ietf:params:scsi:target:051211094438
*****
Command line: iscsicli qaddtargetportal 192.168.1.100
Command line: iscsicli qlogin target 051211094438 itproadmin password12345
*****
/ # _

TCP Redirect IDE Redirect Floppy A:
No Mapping No Mapping RDM.iso
0k/0k IDE Redirect Active: 3,380,198 Bytes Sent [0.0kB/s] / 0 Bytes Received [0.0kB/s]

```

**Figure 15: SOL Window Showing iSCSI Command Lines**

13. On the Management Console System, open a command prompt window and enter the first iscsicli command line in the SOL window (note that Figure 15 above is just an example, and that you should use the command line provided on the actual Remote Drive Mounting main screen in your active SOL Remote Control session). This command adds the Managed Client's hard drive to iSCSI target portal list.
14. Once the first command completes, enter the second iscsicli command from the Remote Drive Mounting main screen to log in to the target portal (which results in mounting the Managed Client's hard drive).

Once the second iscsicli command completes, the Managed Client's hard drive will be mounted to the Management Console. It can be viewed under My Computer or under Disk Manager.

Perform any desired tasks on the remote hard drive. When finished, disconnect it as follows:

1. Close my Computer, Disk Manager, and / or any open files on the remote hard disk.
2. In the SOL session, press enter.
3. Reboot the Managed Client.

## A Appendix: Building the ISO

---

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

### A.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 rdm.iso.

Prepare your system as follows:

1. Install Ubuntu 12.04LTS on an x86\_64 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 python`
  - `sudo apt-get install libgirepository1.0-dev`
  - `sudo apt-get install gperf`
  - `sudo apt-get install libgudev-1.0-dev`
  - `sudo apt-get install libqtglib-2.0-0`
  - `sudo apt-get install libblkid-dev`
  - `sudo apt-get install upx-ucl`
  - `sudo apt-get install build-essential`
  - `sudo apt-get install zlib1g-dev`
  - `sudo apt-get install libncurses5-dev`
  - `sudo apt-get install nasm`
  - `sudo apt-get install cdc`
  - `sudo apt-get install libssl-dev`
  - `sudo apt-get install upx`
  - `sudo apt-get install libnl-3-dev`
  - `sudo apt-get install libglib2.0-dev`
  - `sudo apt-get install bison`
  - `sudo apt-get install flex`

## A.2 Building the ISO

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

1. Extract the remotedrивemount.tar.gz file onto your Ubuntu 12.04 or higher Linux system in any directory. The .tar is extracted to create a directory structure with the root directory "remotedrivemount".



### 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 remotedrивemount directory.
3. Type "sudo make" and wait for the remotedrивemount.iso file to build.

Upon build completion, the remotedrивemount.iso file is built.

The remotedrивemount 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.
- iSCSI Enterprise Target – iSCSI target support kernel module for the Linux kernel



## B Appendix: Remote Drive Mounting Error Messages

---

```
*****
** Remote Drive Mount for PCs featuring Intel(r) vPro(tm) technology **
**
** A remote serial connection was not found on this system. **
** Remote Drive Mount 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 remotedrivemount.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 remotedrivemount.iso, this message should not be displayed.

```
*****
** Remote Drive Mount for PCs featuring Intel(r) vPro(tm) technology **
**
** No available Device/Partitions were found on this system. **
** Remote Drive Mount 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.