



Intel® Core™ vPro™ Processors Common- Use Guide

For RealVNC VNC Viewer Plus*

Introduction

Common Uses for VNC Viewer Plus* from RealVNC and Intel® Core™ vPro™ Processors

IT professionals are often required to make costly on-site visits to diagnose and repair problems with PCs. RealVNC VNC Viewer Plus* allows IT to remotely access the problem PC, which removes the need for most on-site visits. Even when the problems prevent access to the operating system (OS), IT can use RealVNC VNC Viewer Plus to repair or reinstall as necessary.

Intel® Core™ vPro™ processors extend the management capabilities of RealVNC VNC Viewer Plus to enable enhanced management of IT devices, even in powered-off states. These capabilities can drive lower overhead for IT professionals and help allow IT professionals to more effectively meet higher service level agreements (SLAs).

This paper illustrates how to use RealVNC VNC Viewer Plus in conjunction with Microsoft Windows 7* PCs equipped with Intel Core vPro processors in several scenarios you face every day. When you manage these scenarios with the Intel and RealVNC solution, you can reduce administrative overhead, increase IT efficiency, and improve your ability to deliver IT services. Two computers are involved in the use of RealVNC Viewer Plus—the VNC server (PC you access) and the VNC viewer (PC you use VNC from).

WHITE PAPER
Intel® vPro™ Technology
RealVNC VNC Viewer Plus



Table of Contents

Introduction	4
Setup and Assumptions	4
Common Use Cases Covered in this Guide	4
Use Case 1: Scan for Malware Outside the OS	5
Step 1: Connect to the Remote PC	5
Step 2: Mount and Boot a Windows PE Boot Disc Image	5
Step 3: Scan and Clean the Hard Disk	6
Use Case 2: Repair a Damaged Windows 7 Boot Manager	6
Step 1: Connect to the Remote PC	6
Step 2: Mount and Boot a Windows RE Boot Disc Image	7
Step 3: Repair Boot Record	7
Use Case 3: Create and Restore a Drive Image with Microsoft ImageX*	7
Step 1: Connect to the Remote PC	8
Step 2: Mount and Boot a Windows RE Disc Image	8
Step 3: Create an Image with Microsoft ImageX	8
Step 4: Restore to an Image	9
Use Case 4: Recover Files from a BitLocker-encrypted Hard Drive	9
Step 1: Connect to the Remote PC	10
Step 2: Establish Drive Protection	10
Step 3: Unlock the Drive	11
Use Case 5: Modify BIOS Settings with KVM	12
Step 1: Connect to the Remote PC	12
Step 2: Access the PC's BIOS	12
Use Case 6: Troubleshoot Windows Issues with Windows Safe Mode	13
Step 1: Connect to the Remote PC	13
Step 2: Start in Safe Mode	14
Conclusion	14
Related links	15

Setup and Assumptions

Software	RealVNC VNC Viewer Plus* 1.1
Hardware	At least one PC built with an Intel® Core™ i5 vPro™ or Intel® Core™ i7 vPro™ processor (must have Intel Active Management Technology version 6.0 or greater)
Basic Assumptions	<ol style="list-style-type: none"> 1. You have activated Intel vPro technology on the PCs through configuration of the Management Engine BIOS extension (MEBx).¹ 2. You have installed and configured VNC Viewer Plus for your environment.² 3. You have created a Windows RE disc image and/or Windows PE disc image with the following tools: Microsoft Windows Malicious Software Removal Tool*, Bootrec.exe, and Microsoft ImageX*.

Common Use Cases Covered in this Guide

- Scan for malware outside the OS
- Repair a damaged Windows 7 boot manager
- Create and restore a drive image with Microsoft ImageX*
- Recover files from a BitLocker-encrypted hard drive
- Modify BIOS settings with KVM
- Troubleshoot Windows issues with Windows Safe Mode

Use Case 1: Scan for Malware Outside the OS

The vast majority of malware remains dormant until the PC's OS initiates. IT administrators can combat such malware with a pre-boot scan and clean. Such pre-boot attacks have previously required on-site visits from IT, but Intel Core vPro processors and VNC Viewer Plus enable easy access to remote PCs without active OSs. This allows IT to remotely scan and clean disks without allowing the malware a chance to defend itself.

This use case demonstrates the steps required to scan and clean a PC that may be infected, using Microsoft Windows Malicious Software Removal Tool*.

Step 1: Connect to the Remote PC

1. From the VNC Viewer Plus home screen, enter the IP Address of the **AMT Server**, the PC you're connecting to.
2. From the **Connection Mode** drop-down list select **Intel® AMT KVM**.
3. From the **Encryption** drop-down list select **None**.
4. Click **Options**.
5. On the **Display** tab, select **Scale to window size**, or set scaling as desired.
6. Select **Enable toolbar**.
7. On the **AMT Server** tab, clear **Always connect using FQDN**.
8. Click **OK**.
9. Click **Connect**.
10. Enter a valid username and password in the **Username** and **Password** fields.
Note: These are the Username and Password you configured when you activated Intel vPro technology on the remote PC.

11. Click **OK**.

Step 2: Mount and Boot a Windows PE Boot Disc Image

1. Click the **Mount Disk Images** icon on the drop-down set of tools at the top center of the VNC Viewer Plus display.
2. Click **Browse** next to the CD/DVD field.
3. Locate the disc image on the network, select it, and then click **Open**.
4. Click **Mount**.
5. If the target computer is on, power it down. Click the Windows Start button, and then click **Shut down**.
Note: This step might cause your VNC Viewer Plus session to disconnect. If this happens simply reconnect as you did in Step 1.
6. Once the computer is powered-off, click the **Power** icon on the drop-down set of tools at the top center of the VNC Viewer Plus display.
7. Click **Power On**.

8. From the **Choose a boot option** drop-down list, select **Boot to CD/DVD**.
9. Click **Power On**.
10. When prompted to press any key to boot from CD, press **Enter**. The computer will boot from the Windows PE image to a command prompt.

Step 3: Scan and Clean the Hard Disk

1. When the computer boots from the Windows PE disc image, type at the command prompt **cd**[file path to your malicious software removal tool] (for example, cd\tools).
2. Type **windows-kb890830-v3.13.exe** (or similar, if using a different version).

3. Select **Accept all terms of the preceding license agreement**, and then click **Next**.
4. Click **Next**.
5. Select **Full scan**, and then click **Next**. Windows Malicious Software Removal Tool scans the entire PC for malicious software.
6. When the scan completes click **Finish**.
7. Click the **Mount Disk Images** icon on the drop-down set of tools at the top center of the VNC Viewer Plus display.
8. Click **Remove**, and then click **Close**.
9. Type **Exit** at the command prompt to reboot the PC to Windows.

End of Use Case 1

Use Case 2: Repair a Damaged Windows 7 Boot Manager

Intel Core vPro processors and VNC Viewer Plus enable administrators to access remote PCs on a network, even those in a powered-off state or with an inoperable OS. Remote access is secured through the use of an administrator password, which is required to initiate a remote access session. This secure remote access to PCs means fewer on-site visits, lower administrative overhead, and faster diagnosis and repair of Windows 7 PCs.

This use case demonstrates the steps required to access and repair a PC that experiences boot errors (for example, errors finding bootmgr).

Step 1: Connect to the Remote PC

1. From the VNC Viewer Plus home screen, enter the IP Address of the **AMT Server**, the PC you're connecting to.
2. From the **Connection Mode** drop-down list select **Intel® AMT KVM**.
3. From the **Encryption** drop-down list select **None**.
4. Click **Options**.
5. On the **Display** tab, select **Scale to window size**, or set scaling as desired.
6. Select **Enable toolbar**.
7. On the **AMT Server** tab, clear **Always connect using FQDN**.
8. Click **OK**.
9. Click **Connect**.
10. Enter a valid username and password in the **Username** and **Password** fields.
Note: These are the Username and Password you configured when you activated Intel vPro technology on the remote PC.
11. Click **OK**.

Step 2: Mount and Boot a Windows RE Boot Disc Image

1. Click the **Mount Disk Images** icon on the drop-down set of tools at the top center of the VNC Viewer Plus display.
2. Click **Browse** next to the CD/DVD field.
3. Locate the disc image on the network, select it, and then click **Open**.
4. Click **Mount**.
5. If the target computer is on, power it down. Click the Windows Start button, and then click **Shut down**.
Note: This step might cause your VNC Viewer Plus session to disconnect. If this happens simply reconnect as you did in Step 1.
6. Once the computer is powered-off, click the **Power** icon on the drop-down set of tools at the top center of the VNC Viewer Plus display.
7. Click **Power On**.
8. From the **Choose a boot option** drop-down list, select **Boot to CD/DVD**.
9. Click **Power On**.

10. When prompted to press any key to boot from CD, press **Enter**. The computer will boot from the Windows RE disc image.
11. When the computer boots from the Windows RE disc image, select **US** from the **Select a keyboard input method** drop-down list, and then click **Next**.
12. In the **System Recovery Options** window select **Use recovery tools that can help fix problems starting Windows**, and then select **Windows 7**.
13. Click **Next**.
14. Click **Command Prompt**.

Step 3: Repair Boot Record

1. At the command prompt (opened in Step 2), type **bootrec /fixboot**, and then press **Enter**.
2. Type **exit**, and then press **Enter**.
3. Alternately, at the System Recovery Options window click **Startup Repair**.
4. Once the PC is done scanning click **Finish**.
5. Click the **Mount Disk Images** icon on the drop-down set of tools at the top center of the VNC Viewer Plus display.
6. Click **Remove**, and then click **Close**.
7. Click **Restart** to reboot to Windows.

End of Use Case 2

Use Case 3: Create and Restore a Drive Image with Microsoft ImageX*

VNC Viewer Plus allows IT administrators to mount remote disc images, which can enable repair and reinstallation of a faulty OS from an image of the PC's hard drive without the need for an on-site visit.

This use case demonstrates how to create and mount a boot CD image and then use Microsoft ImageX* to restore a hard drive backup image that is stored on a separate partition.

Step 1: Connect to the Remote PC

1. From the VNC Viewer Plus home screen, enter the IP Address of the **AMT Server**, the PC you're connecting to.
2. From the **Connection Mode** drop-down list select **Intel® AMT KVM**.
3. From the **Encryption** drop-down list select **None**.
4. Click **Options**.
5. On the **Display** tab, select **Scale to window size**, or set scaling as desired.
6. Select **Enable toolbar**.
7. On the **AMT Server** tab, clear **Always connect using FQDN**.
8. Click **OK**.
9. Click **Connect**.
10. Enter a valid username and password in the **Username** and **Password** fields.
Note: These are the Username and Password you configured when you activated Intel vPro technology on the remote PC.
11. Click **OK**.

Step 2: Mount and Boot a Windows PE Disc Image

1. Click the **Mount Disk Images** icon on the drop-down set of tools at the top center of the VNC Viewer Plus display.

2. Click **Browse** next to the CD/DVD field.
3. Locate the disc image on the network, select it, and then click **Open**.
4. Click **Mount**.
5. If the target computer is on, power it down. Click the Windows Start button, and then click **Shut down**.
Note: This step might cause your VNC Viewer Plus session to disconnect. If this happens simply reconnect as you did in Step 1.
6. Once the computer is powered-off, click the **Power** icon on the drop-down set of tools at the top center of the VNC Viewer Plus display.
7. Click **Power On**.
8. From the **Choose a boot option** drop-down list, select **Boot to CD/DVD**.
9. Click **Power On**.

When prompted to press any key to boot from CD, press **Enter**. The computer will boot from the Windows PE disc to a command-line tool.

Note: For this Use Case we use a Windows PE disc image, but a Windows RE disc image can work just as well (assuming it contains ImageX). If you prefer to use Windows RE, follow the steps in Use Case 2: Step 2.

Step 3: Create an Image with Microsoft ImageX

1. Once the computer has booted, type **gimagex.exe** at the command prompt, and then press **Enter**. The GImageX control panel will open.
Note: If ImageX is located in a different directory on your disc image, type **cd\[file path to ImageX]**, and then repeat the step 1.
2. On the **Capture** tab, click **Browse** next to the Source field.
3. Select the disk you wish to image, and then click **OK**.
4. On the **Capture** tab, click **Browse** next to the Destination field.
5. Select the partition or network location where you wish to store your image.
6. Type a name for the image in the **File name** field, and then click **Save**.
7. If desired, fill in the **Name** and **Description** fields.
8. Click **Create**. ImageX creates an image of the healthy disk. This might take a while.
9. Once ImageX has finished creating the image, click **Close**.

Step 4: Restore to an Image

1. To restore an image, click the **Apply** tab of the GImageX control panel opened in Step 3.
2. Click **Browse** next to the Source field.
3. Select the healthy image created in Step 3 of this Use Case, and then click **Open**.
4. Click **Browse** next to the Destination field.
5. Select the unhealthy disk, and then click **OK**.
6. Click **Apply**. ImageX applies the image to the disk.
7. Once the image is applied, click **Close**.
8. Exit ImageX by clicking the close button at the top right.
9. Click the **Mount Disk Images** icon on the drop-down set of tools at the top center of the VNC Viewer Plus display.
10. Click **Remove**.
11. Click **Close**.
12. Type **exit** at the command prompt, and then press **Enter**. The computer will restart into Windows using the newly imaged disc.

End of Use Case 3

Use Case 4: Recover Files from a BitLocker-encrypted Hard Drive

Microsoft BitLocker allows the encryption of hard drives to prevent unauthorized access. It is designed to secure all or part of a hard drive or an external storage device—a capability available as of Windows 7. This encryption strengthens security, but can become problematic if the password and recovery key are lost. Through the establishment of a Data Recovery Agent (DRA) IT can assure that all secured devices can be recovered even if the passwords are forgotten or lost. BitLocker DRA uses certificates to establish identity and trust.

This use case demonstrates how to regain access to a BitLocker-encrypted hard drive on a remote PC if the password is unavailable. This use case assumes that an IT administrator has set up DRA for BitLocker.

Step 1: Connect to the Remote PC

1. From the VNC Viewer Plus home screen, enter the IP Address of the **AMT Server**, the PC you're connecting to.
2. From the **Connection Mode** drop-down list select **Intel® AMT KVM**.
3. From the **Encryption** drop-down list select **None**.
4. Click **Options**.
5. On the **Display** tab, select **Scale to window size**, or set scaling as desired.
6. Select **Enable toolbar**.
7. On the **AMT Server** tab, clear **Always connect using FQDN**.
8. Click **OK**.
9. Click **Connect**.

10. Enter a valid username and password in the **Username** and **Password** fields.
Note: These are the Username and Password you configured when you activated Intel vPro technology on the remote PC.
11. Click **OK**.

Step 2: Establish Drive Protection

If the target computer is powered off:

1. Once the computer is powered-off, click the **Power** icon on the drop-down set of tools at the top center of the VNC Viewer Plus display.
2. Click **Power On**.
3. From the **Choose a boot option** drop-down list, select **Boot to OS**.

4. Click **Power On**.

Once powered on, complete the following steps to determine the protection status of the desired BitLocker protected drive:

1. Click **Start**.
2. Type **cmd.exe** in the search field.
3. In the results list, right-click **cmd** and click **Run as administrator**. If asked to confirm, do so. This opens a command-line tool.
4. At the command prompt type **manage-bde -status [drive]** (for example, **manage-bde -status F:**), and then press **Enter**. The tool will present the status and general information of the requested drive.
5. To determine the precise protection of the drive, type **manage-bde -protectors -get [drive]** (for example, **manage-bde -protectors -get F:**), and then press **Enter**. This command will display the various protection methods in use on the drive. If a Data Recovery Agent was assigned in the encryption process, then the command-line tool will present the certificate thumbprint(s) usable to unlock the drive.

Note: If you have access to the password or recovery key, you can unlock the drive simply by using them (either through Windows Explorer and the unlock-agent accessed by double-clicking, or by unlocking directly from the command-line tool with **manage-bde -unlock [drive]**). For this use case it is assumed you do not have access to these tools, and must thus make use of the DRA.

Step 3: Unlock the Drive

Once you have determined what certificate(s) BitLocker requires to unlock the desired drive, you must locate that certificate.

1. To check for the certificate on the remote PC itself, type **certmgr.msc** at the command prompt, and then press **Enter**.
2. In the window that opens, click **Action**, and then click **Find Certificates**.

3. From the **Find in** drop-down list, select **All certificate stores**.

4. In the **Contains** field, enter a certificate thumbprint obtained in the Step 2.
5. From the **Look in field** drop-down list, select **SHA1 Hash**.
6. Click **Find Now**.

Note: If multiple certificates are able to unlock the desired drive, repeat the above steps with each thumbprint until one is found.

7. If a usable certificate is found on the PC, open the command-line tool and type **manage-bde -unlock [drive] -cert -ct [certificate thumbprint]**, then press **Enter**.
8. If no usable certificate is available on the local system, you must locate one elsewhere on the network—presumably in a localized DRA storage.
9. If the remote PC can access the DRA storage location where a usable certificate is located, open the command-line tool and type **manage-bde -unlock [drive] -cn [name of computer with the certificate] -cert -ct [certificate thumbprint]**, and then press **Enter**.
10. If the remote PC cannot access the DRA storage location, copy the certificate to a location where the remote PC can access it locally or on the network.
11. Open the command-line tool, type **manage-bde -unlock [drive] -cert -cf [file path, including file name]**, and then press **Enter**.
12. Once you have located a usable certificate and entered the correct command to unlock the drive, the message “The certificate successfully unlocked volume [drive]” displays. You can now access the drive, as well as the options to set a new password, save or print the recovery key again, or even remove BitLocker protection altogether.

End of Use Case 4

Use Case 5: Modify BIOS Settings with KVM

IT staff members can use a computer's BIOS to diagnose and fix various problems, restore default settings, or change boot order. Access to the BIOS requires action before the OS boots, and so this valuable tool has historically been unavailable remotely. With Intel Core vPro processors and VNC Viewer Plus, access to the remote PC's BIOS is simple. Through these technologies, IT administrators can remotely access a computer's BIOS to diagnose and repair a variety of problems, and also determine if an on-site visit is necessary to replace faulty hardware.

This use case describes the steps required to remotely access a PC's BIOS.

Step 1: Connect to the Remote PC

1. From the VNC Viewer Plus home screen, enter the IP Address of the **AMT Server**, the PC you're connecting to.
2. From the **Connection Mode** drop-down list select **Intel® AMT KVM**.
3. From the **Encryption** drop-down list select **None**.
4. Click **Options**.
5. On the **Display** tab, select **Scale to window size**, or set scaling as desired.
6. Select **Enable toolbar**.
7. On the **AMT Server** tab, clear **Always connect using FQDN**.
8. Click **OK**.
9. Click **Connect**.
10. Enter a valid username and password in the **Username** and **Password** fields.
Note: These are the Username and Password you configured when you activated Intel vPro technology on the remote PC.
11. Click **OK**.

Step 2: Access the PC's BIOS

If the target computer is powered on:

1. Click **Start**.
2. From the sleep options list, select **Restart**.
3. Once the pre-boot screen appears, press the key that accesses the BIOS.

Use Case 6: Troubleshoot Windows Issues with Windows Safe Mode

Some issues in Windows, such as driver incompatibilities and other common problems, can be diagnosed and solved with Windows Safe Mode. Starting in Safe Mode requires action before the OS boots, which has previously required an on-site visit from IT personnel. However, with VNC Viewer Plus and Intel Core vPro processors, restarting a computer in safe mode is simple.

This use case describes the steps necessary to access the remote PC's safe mode, where you can diagnose and repair as if you were sitting at the computer itself.

Note: The key required to enter the BIOS settings differs among PC manufacturers and BIOS providers. Use the key that is appropriate to the specific PC.

4. The remote PC enters the BIOS settings. From here you can diagnose and repair issues as with the client PC.
5. When finished, save any changes you have made and exit the BIOS settings.

If the target computer is powered off:

1. Once the computer is powered-off, click the **Power** icon on the drop-down set of tools at the top center of the VNC Viewer Plus display.
2. Click **Power On**.
3. From the **Choose a boot option** drop-down list, select **Boot to OS**.
4. Click **Power On**.
5. Once the pre-boot screen appears, press the key that accesses the BIOS.
Note: The key required to enter the BIOS settings differs among PC manufacturers and BIOS providers. Use the key that is appropriate to the specific PC.
6. The remote PC enters the BIOS settings. From here you can diagnose and repair issues as with the client PC.
7. When finished, save any changes you have made and exit the BIOS settings.

End of Use Case 5

Step 1: Connect to the Remote PC

1. From the VNC Viewer Plus home screen, enter the IP Address of the **AMT Server**, the PC you're connecting to.
2. From the **Connection Mode** drop-down list select **Intel® AMT KVM**.
3. From the **Encryption** drop-down list select **None**.
4. Click **Options**.
5. On the **Display** tab, select **Scale to window size**, or set scaling as desired.
6. Select **Enable toolbar**.
7. On the **AMT Server** tab, clear **Always connect using FQDN**.
8. On the **Inputs** tab, select the desired key from the **Menu Key** drop-down list (any key other than the key necessary for Safe Mode access—typically F8).
9. Click **OK**.
10. Click **Connect**.
11. Enter a valid username and password in the **Username** and **Password** fields.
Note: These are the Username and Password you configured when you activated Intel vPro technology on the remote PC.
12. Click **OK**.

Step 2: Start in Safe Mode

If the target computer is powered on:

1. Click **Start**.
2. From the sleep options list, select **Restart**.
3. After the initial boot screen, but before Windows starts, press **F8** (or if your remote PC requires another key for safe mode access, press that).

Conclusion

Intel Core vPro processors allow greater remote access and interactivity with remote PCs than has previously been possible. RealVNC VNC Viewer Plus takes advantage of this technology to allow IT professionals greater access to KVM-enabled remote PCs, including the ability to access elements of the PC outside of the OS, as well as access to powered-off PCs. This extended capability means lower operating costs, greater efficiency, and faster diagnosis and repair of problem PCs. As the use cases in this document demonstrate, IT can use this technology to remotely diagnose and repair a variety of computer problems that would previously have required on-site visits. And, in the case that an on-site visit remains necessary, Intel Core vPro processors and RealVNC VNC Viewer Plus provide IT enough access to determine the problem and be prepared to deal with it ahead of time, substantially reducing the time needed for the on-site visit.

Note: If Windows starts as normal without entering safe mode repeat the above steps to try again.

4. Use the arrow keys to scroll to **Safe Mode**.
5. Press **Enter**.
6. The remote PC now boots into safe mode. From here you can diagnose and troubleshoot as if you were in safe mode on your own PC.

If the target computer is powered off:

1. Once the computer is powered-off, click the **Power** icon on the drop-down set of tools at the top center of the VNC Viewer Plus display.
2. Click **Power On**.
3. From the **Choose a boot option** drop-down list, select **Boot to OS**.
4. Click **Power On**.
5. After the initial boot screen, but before Windows starts, press **F8** (or if your remote PC requires another key for safe mode access, press that).

Note: If Windows starts as normal without entering safe mode follow the steps for If the target computer is powered on to try again.

6. Use the arrow keys to scroll to **Safe Mode**.
7. Press **Enter**.
8. The remote PC now boots into safe mode. From here you can diagnose and troubleshoot as if you were in safe mode on your own PC.

End of Use Case 6

Related Links

- For more information about Intel Core vPro processors, visit:
http://www.intel.com/itcenter/products/core/core_vpro/index.htm
- For more information about Intel vPro technology, visit:
<http://www.intel.com/itcenter/tool/vpro/index.htm>
- For more information about RealVNC and VNC Viewer Plus, visit:
<http://www.realvnc.com/products/viewerplus/index.html>

Endnotes

1. For more information on how to activate Intel vPro technology, visit
<http://www.intel.com/itcenter/tool/vpro/index.htm>
2. For more information on how to install and configure VNC Viewer Plus, visit <http://www.realvnc.com/products/viewerplus/1.1/docs/ad1026169.html>

Disclaimers

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 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 by visiting Intel's Web site at www.intel.com.

Copyright © 2010 Intel Corporation. All rights reserved. Intel, the Intel logo, Xeon, Xeon inside, Intel Core, and Intel vPro are trademarks of Intel Corporation in the U.S. and other countries.

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

Printed in USA

1110/AD/PRW/PDF

Please Recycle

324742-001 US

