

Intel i5 and i7 Processors in the Industrial World

Intel first released the Core i7 processor at the end of 2008; the original platform based on the new 'Nehalem' architecture was aimed at the high end / enthusiast sector. Since then, successive models have been released; code named 'Lynnfield' and 'Clarkdale', still with cutting edge performance the i7 brand with 7 year Intel supported availability is ideal for the industrial sector.

Based on new 32nm lithography, Amplicon's Ventrax and Impact-R rackmount industrial systems equipped with Intel i5 and i7 processor offer a range of new performance enhancements and features to greatly benefit the industrial user.

Performance

As with all subsequent generations of processors, a significant performance improvement is to be expected, and in this respect the comparison between the i5, i7 class processors when compared to their Core 2 predecessors represents an exceptional leap.

For the industrial user the increase in performance may simply be desired for improved responsiveness of a given application, or to reduce the processing time for intensive applications such as data encoding, or encryption. However, the new platform also gives scope for several older systems to be replaced and merged within a single system.

Fig. 1 - Passmark Performance Test Benchmarks

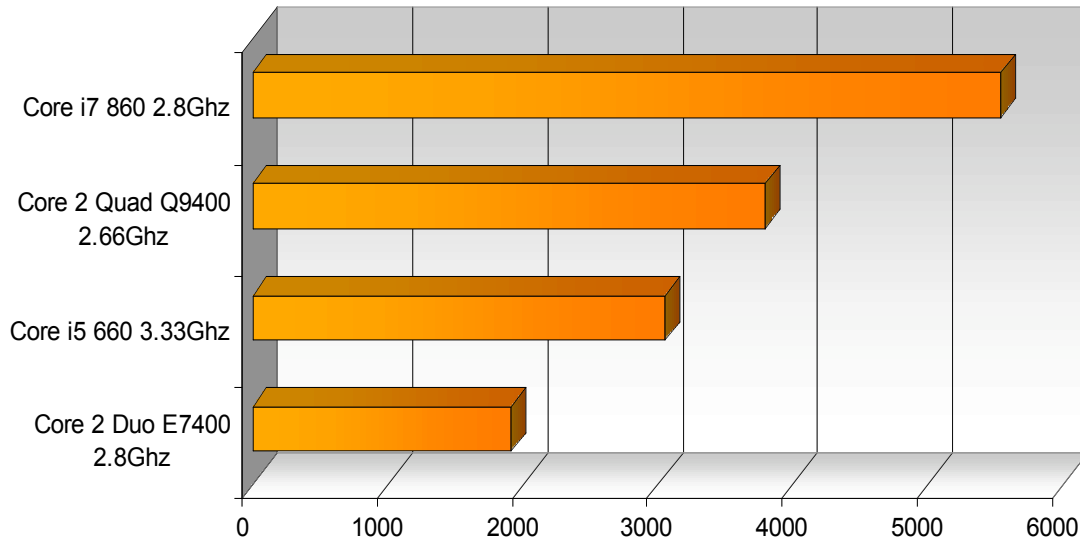


Figure 1 shows the comparison between key models of older 'Conroe' Intel Core 2 models, and newer 'Clarkdale' i5, 'Lynnfield' i7 processors, based on a synthetic benchmark generated with Passmark Performance Test.

Whilst the performance benefits in real world applications will of course vary dependant on various factors, such as software implementation, and the number of cores used, the illustration is representative of comparative performance between the different generations of processor.

Scalable Performance

The Core i5 and i7 processors feature intelligent and scalable processing, dependant on workload enabling the processors to offer both optimised performance and power consumption.

Turboboost

Intel Turbo Boost Technology is one of the many exciting features that Intel has built into latest-generation Intel micro-architecture codename Nehalem. It automatically allows processor cores to run faster than the base operating frequency if it's operating below power, current, and temperature specification limits.

For Industrial applications this feature is particularly beneficial, as it provides a performance benefit to even older industrial software applications which are seldom re-written to make use of additional cores, which have become the norm in desktop processing over the last decade, despite in many cases having a desire for additional performance from the application.

Intel Turbo Boost Technology is activated when the Operating System (OS) requests the highest processor performance state (P0). The maximum frequency of Intel Turbo Boost Technology is dependent on the number of active cores. The amount of time the processor spends in the Intel Turbo Boost Technology state depends on the workload and operating environment.

Any of the following can set the upper limit of Intel Turbo Boost Technology on a given workload:

- Number of active cores
- Estimated current consumption
- Estimated power consumption
- Processor temperature

When the processor is operating below these limits and the user's workload demands additional performance, the processor frequency will dynamically increase by 133 MHz on short and regular intervals until the upper limit is met or the maximum possible upside for the number of active cores is reached.

Fig 2. - Maximum Turboboost Core Speed Increase

i5 660 3.33Ghz Processor	Dual Core Standard Speed 3.33Ghz	Maximum Turbo-boosted clock speed 3.6Ghz
i7 860 2.8Ghz Processor	Quad Core Standard Speed 2.8Ghz	Maximum Turbo-boosted Clock speed 3.46Ghz

Hyper Threading

Today's Intel Hyper-Threading Technology (Intel HT Technology) delivers thread-level parallelism on each processor resulting in more efficient use of processor resources higher processing throughput—and improved performance on multi-threaded software.

In simple terms, the technology doubles the number of processing cores, allowing the performance of single core to be simultaneously shared between two active threads, thus increasing the number of transactions that be processed simultaneously.

An Intel processor and chipset combined with an OS and BIOS supporting Intel HT Technology allows you to run demanding applications simultaneously whilst always maintaining system responsiveness, important for industrial applications where an application is monitored in real time and user interaction maybe required.

Intel intelligent power technology

Coupled with the new scalable performance, Core i5 and i7 processors, has a number of power optimisations built in, meaning the system's power consumption does not increase from the older generation despite the performance gains. This is particularly important for industrial applications where power budgets are often limited, defined by existing power schemes, or even environmental targets for reductions in overall power consumption.

This also means the processors have the same Thermal Design Power (TDP) as the previous range of Conroe processors. Both of which simplify the selection of new systems featuring the new processor, without needing to re-review power budgets, or thermal design for when replacing existing systems.

Integrated power gates allowing individual idling cores to be reduced to near zero power, independent of other operating cores reducing idle power consumption to 10 watts when compared to 16-50 watts in prior generations of Intel quad core processors.

Automated low power states automatically put processor and memory into the lowest available power states that will meet the requirement of the current workload. Because processors are enhanced with more and lower CPU power states and memory and I/O controllers have new power management features the degree to which power can be minimised and is now greatly enhanced.

Migration to PCI Express

Many industrial grade systems have long been based on PICMG 1.0 technology which is derived from SBC (Single Board Computer) and Backplane technology. In more recent years PICMG 1.3 has been adopted, introducing the PCI Express bus into backplane based systems, at the cost of the much older ISA bus.

With the i5 and i7 systems and their heavy reliance on PCI Express technology, PICMG 1.3 is the only compatible option for the new platforms, meaning the ISA bus is no longer available. Configurations with large numbers of standard PCI slots are still possible, and are available within Amplicon's Ventrax series.

Intel Active Management Technology and Remote Management



A major barrier to IT efficiency has been lowered by Intel Active Management Technology (Intel AMT), a feature of Intel Core processors.

Systems equipped with i5 and i7 processors can make use of built-in platform capabilities and popular third-party remote management and security applications, meaning Intel AMT allows systems to easily remotely maintained, and monitored.

Extensive surveys of numerous IT organizations - including Intel's - laid the groundwork for defining and designing Intel AMT. Three of the top IT needs revealed by this research included better asset management, reduced downtime, and minimized desk-side visits. Intel design teams determined that these issues were best addressed through platform architectural enhancements, resulting in the following features for supporting those needs.

Features and benefits

Intel Active Management Technology (Intel® AMT)

Out-of-band system access

Discover. With built-in manageability, Intel AMT allows IT to discover assets even while PCs are powered off.¹ Plus, remote consoles don't rely on local software agents, helping to avoid accidental data loss.

Remote troubleshooting and recovery

Diagnose. Providing out-of-band management capabilities, Intel AMT allows IT to remotely isolate and recover systems after OS failures while alerting and event logging helps reduce downtime.

Hardware-based agent presence checking

Verify. Ensuring better protection for your enterprise, hardware-based agent presence checking proactively detects that software agents are running while missing agents are automatically detected and alerts are sent to the management console.

Proactive alerting

Isolate. Proactively blocking incoming threats, Intel AMT System Defense contains infected clients before they impact the network while alerting IT when critical software agents are removed.

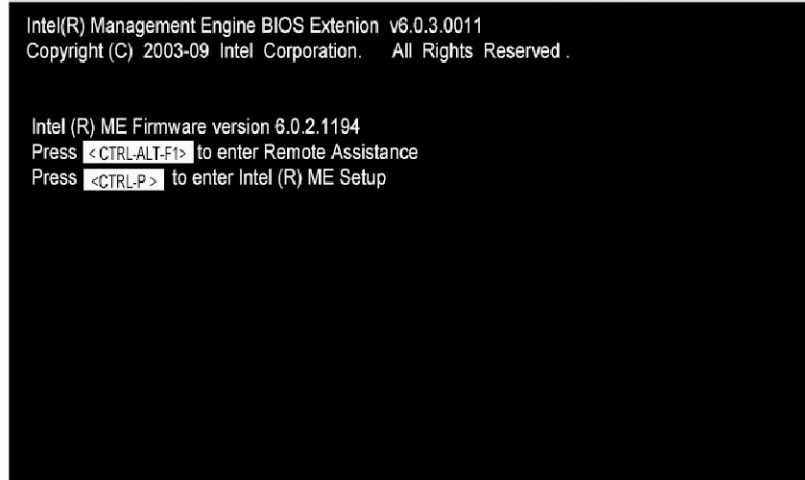
Remote hardware and software asset tracking

Update. Helping to keep software and virus protection up-to-date across the enterprise, Intel AMT also enable third-party software to store version numbers or policy data in non-volatile memory for off-hours retrieval or updates.

Using iAMT with Amplicon Systems

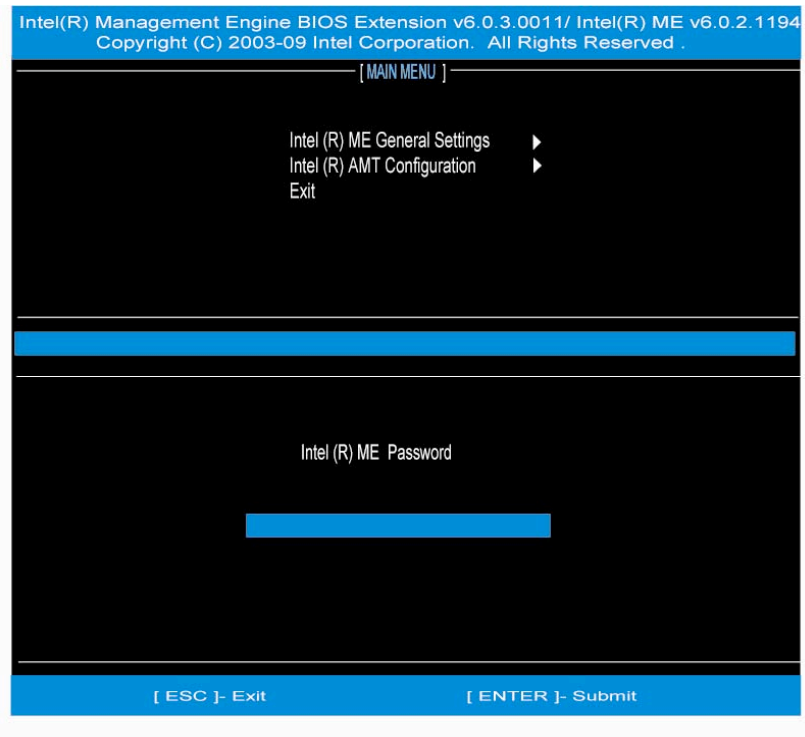
- 1 Enter system BIOS to enable Intel iAMT function.
- 2 Exit from BIOS after starting Intel iAMT, and press Ctrl+P to enter MEBx Setting.

 It is better to press Ctrl+P before the screen popping out.



Set & Change Password

1. You will be asked to set a password when first log in. The default password is 'admin'.



3. Create a new password for the first time.

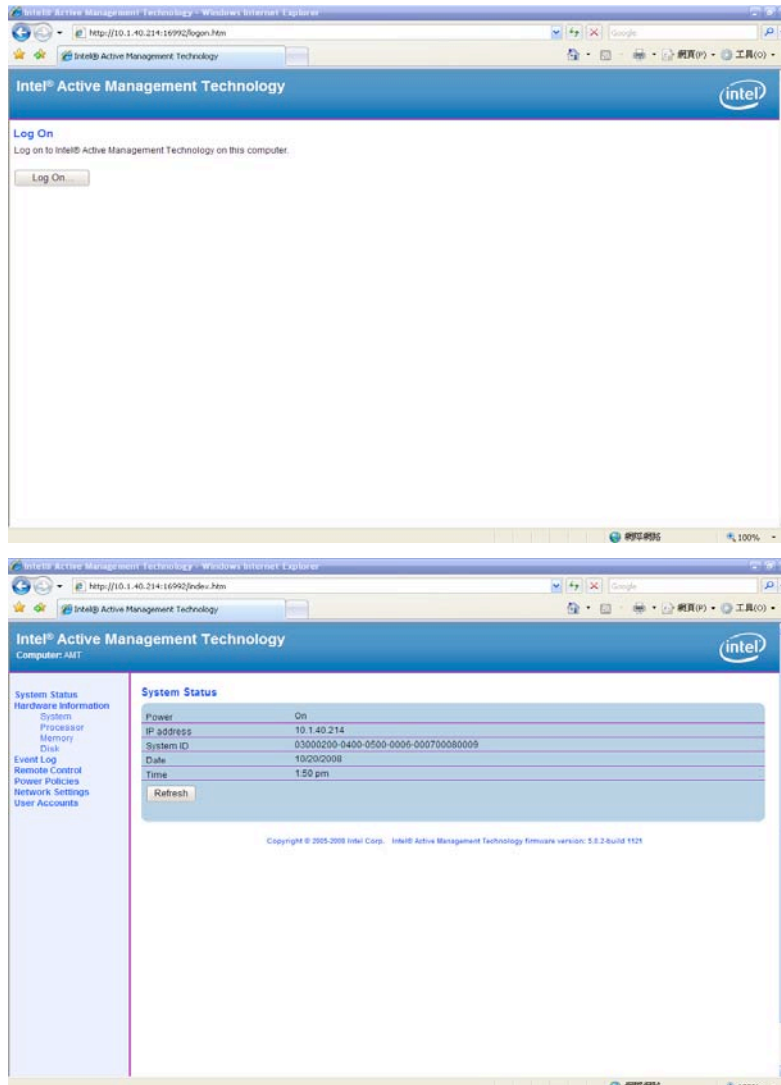
The new password must contain: (example:!!11qqQQ) (default value), eight characters, one upper case character, one lower case character, one number, one symbol such as ! \ ` ; ' \$

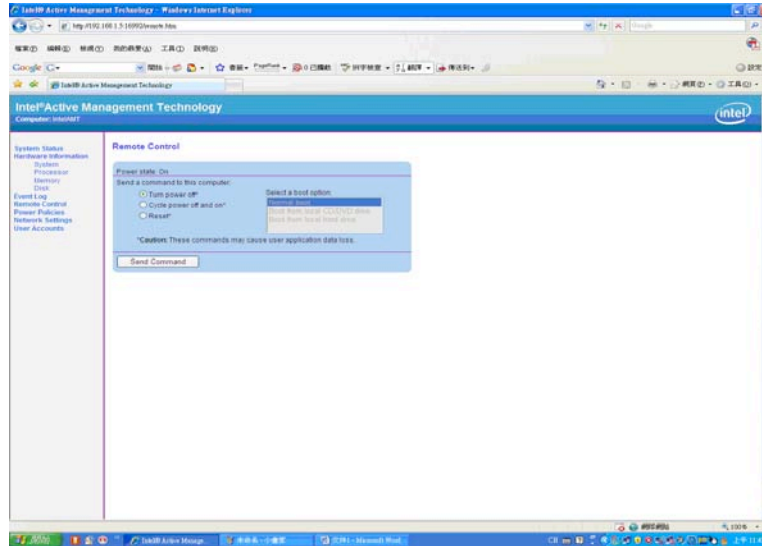
4. Configure an IP address within the iAMT console to suit the network the system is connected to. Once configured, the system can be accessed through a web browser.

Using the Intel iAMT Web Console

The web console is available on all models of i5 and i7 systems, and allows the system to be powered on, off, rebooted, booted from a different boot device and hardware inventory to be viewed, even when the system is powered off.

1. From a web browser, please type `http ://(IP ADDRESS):16992`, which connects to Intel[®] iAMT Web. Example: <http://10.1.40.214:16992>
2. To log on, you will be required to type in username and password defined above (default user is 'admin').





Virtual KVM using Integrated VNC

Being able to access the PC through a web console is only the start of iAMT functionality. Amplicon's Intel Core i5 systems are equipped with a built-in out of band VNC server, meaning a VNC client can connect and view the system at any time, even when the system is powered off.

VNC provides remote access and control over any computer, whether on a local network or anywhere in the world. RealVNC's technology has played an integral role as part of today's connected world with hundreds of millions of users.

By using third party software from RealVNC, called [RealVNC Viewer Plus](#), this technology is taken to a new level by enabling industrial users to connect to a VNC Server embedded directly onto the 2010 Intel Core i5 / i7 Processor Family, providing built-in remote access. VNC Viewer Plus connects directly to the VNC Server embedded in the hardware - no additional software needs to be installed on the operating system for full graphical KVM out-of-band access. This unique solution enables users to remotely watch a full PC boot sequence, manipulate BIOS settings and re-install an operating system.

Amplicon Industrial systems with an Intel Core i5 processor allow remote hardware reset, power on/off and IDE redirection, providing users with the ability to boot from a remote CD or image. VNC Viewer Plus can help solve complex issues such as OS failures and boot problems without ever needing to be desk-side, particularly useful for industrial applications with very limited physical access, such as systems used within control panels.

Getting connected with VNC Viewer Plus on the client computer

Once VNC View Plus is fully installed. Start *VNC Viewer Plus* on the client computer by selecting **RealVNC > VNC Viewer Plus** from the **Start** menu. The **VNC Viewer Plus: New Connection** dialog opens:



Note: If the **Connection Mode** dropdown is not visible, *VNC Viewer Plus* is not licensed. You must enter a license key before you can connect to *AMT Server*. A 90 day trial version is available from www.realvnc.com.

Starting VNC Viewer Plus programmatically

For many industrial applications, it maybe preferable to built a script or webpage to allow a user to easily connect to each system with iAMT functionality, this can easily implemented by using the following URI scheme:

```
kvm://<username>:<password>@<host_computer>[/?<option>=<value>&...]
```

Note: *VNC Viewer Plus* must be installed and licensed on the computer on which the command runs.

An option/value pair can be any property from the **Expert** tab of the **VNC Viewer Plus Properties** dialog.

For example, you could enter the following at the command prompt:

```
C:\Program Files\RealVNC\VNCViewerPlus\vncviewer.exe -uri  
kvm://adminusr:Pa55w0rd!@amt.acme.org/?AmtUseFQDN=false&AmtRequireConsent=false
```

Or enter the following command in the address bar of a web browser:


```
kvm://adminusr:Acm31ncPwd*@amt2/?AmtUseFQDN=true
```

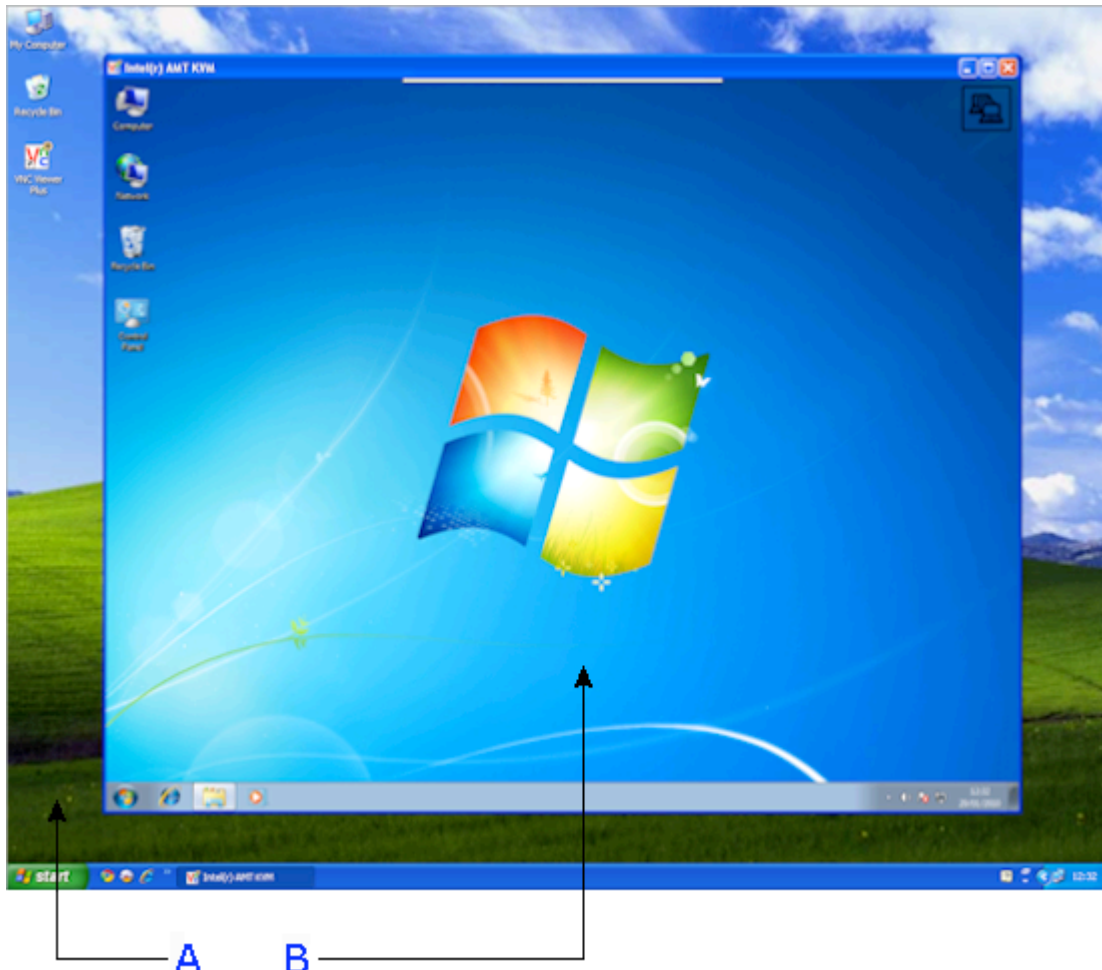
Or click a hyperlink in a web page constructed from the following HTML:

```
<a href="kvm://stdusr:M1nPr1vs!@192.168.2.55/?ColourLevel=0">Connect!</a>
```



Once Connected - The VNC Viewer Plus user experience

When a connection is established, *VNC Viewer Plus* displays a new window on the client computer displaying video output from the host computer running *AMT Server*:

- If the host computer is powered off, or in hibernate mode, or has no functioning operating system, the screen will likely be black. To power the computer on, click the **Power**  *VNC Viewer Plus* toolbar button.
- If the host computer is powered on and has more than one monitor, a connection screen will likely be displayed prompting you to choose which monitor to remote. Press the F1 key to toggle between monitors, and then the ENTER key to continue (your mouse is disabled on this screen).
- If the host computer is powered on and an operating system is booted, the desktop of the host computer will likely be shown, or a login screen if no host computer user is currently logged on.



A. Desktop of a client computer running Windows XP. **B.** *VNC Viewer Plus* displaying the desktop of a host computer.

Note: The  graphic in the top right corner of the *VNC Viewer Plus* window flashes to indicate that a *VNC Viewer Plus* user is connected.

Controlling the host computer using your mouse

Your client computer's mouse is now shared with the host computer. This means that:

- Moving the mouse and clicking within the *VNC Viewer Plus* window affects the host computer and not the client.
- Moving the mouse and clicking outside the *VNC Viewer Plus* window, or on the *VNC Viewer Plus* title bar or window buttons (**Minimize**, **Maximize**, and **Close**), affects the client computer and not the host.

Note: If your mouse has no effect on the host computer, it may have been disabled.

Alternatively, it may be that the host computer is not currently accepting mouse input.

If client and host computers have different numbers of mouse buttons, you can configure *VNC Viewer Plus* to emulate those you do not have.

Controlling the host computer using your keyboard

Your client computer's keyboard is now shared with the host computer, with the exception of:

- The function key that opens the shortcut menu (F8 by default)
- The CTRL-ALT-DELETE key combination.

Note: If your keyboard has no effect on the host computer, it may have been disabled.

Keyboard behavior in Intel AMT 6.0

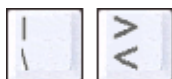
Note: The information in this section only applies to connections made to host computers running Intel AMT 6.0. The issues described have been fixed by Intel Corporation in Intel AMT 6.1 and later.

AMT Server interprets keyboard keys slightly differently to *VNC Server*. For a connection to *VNC Server*, *VNC Viewer Plus* reproduces what you type exactly. For a connection to *AMT Server*, however, it is first necessary to ensure that the keyboard language of the host computer is mapped to the type of keyboard attached to your client computer. For example, if your client computer has a UK keyboard, you should ensure that the host computer's keyboard language is set to English (United Kingdom).

Note: You can change the keyboard language of a host computer running Windows 7 by navigating to **Region and Language** in Control Panel. For other operating systems, consult the manufacturer's documentation.

Note also the following issues:

- If your client computer has a 102 key European-style keyboard, you cannot press the key next to the left SHIFT key. Depending on your keyboard, this may be one of the following keys:



Instead, to enter the characters on these keys, you must first change the host computer's keyboard language to English (United States), and then press the key on your keyboard corresponding to the key that you would press were your client computer to have a 101 key US-style keyboard. For example:

- If your client computer has a UK keyboard, press # and ~ (SHIFT-#) to enter the \ and | characters respectively.
- If your client computer has a French keyboard, press . (SHIFT-;) and / (SHIFT-:) to enter the < and > characters respectively.












Note that the last three of these keys are located either side of the space bar.

Using the VNC Viewer Plus toolbar

To see the toolbar, hover the mouse over the hot area at the top of the *VNC Viewer Plus* window:



The following table explains the effect of clicking each toolbar button.


Button name	Explanation
 New Connection	Opens the VNC Viewer Plus: New Connection dialog. You can start a new connection to <i>AMT Server</i> running on a different host computer, or to a VNC-compatible Server running on any computer.
 Save Connection	You can save the current connection so you can quickly reconnect in future without having to remember the <i>AMT Server</i> network address and any authentication credentials.
 Close Connection	Prompts you to close the current connection (and the <i>VNC Viewer Plus</i> window).
 Options	Opens the VNC Viewer Plus Properties dialog. You can configure most aspects of <i>VNC Viewer Plus</i> while the current connection is in progress.
 Full Screen Mode	Toggles full screen mode on and off.
 Send Ctrl-Alt-Del	Sends the CTRL-ALT-DELETE command to the host computer. (<i>Pressing</i> this key combination would be interpreted by your client computer.) You could alternatively press SHIFT-CTRL-ALT-DELETE.
 Mount Disk Images	Opens the Mount Disk Images dialog.
 Power	Opens the Power dialog to power the PC on or off.
 Connection Information	Opens a dialog displaying technical information about the current connection, such as the encryption method and compression format.
 encryption	The connection is encrypted/not encrypted (only one of these buttons is shown).
 connection speed/activity	Hovering over this toolbar button reveals the current connection speed.

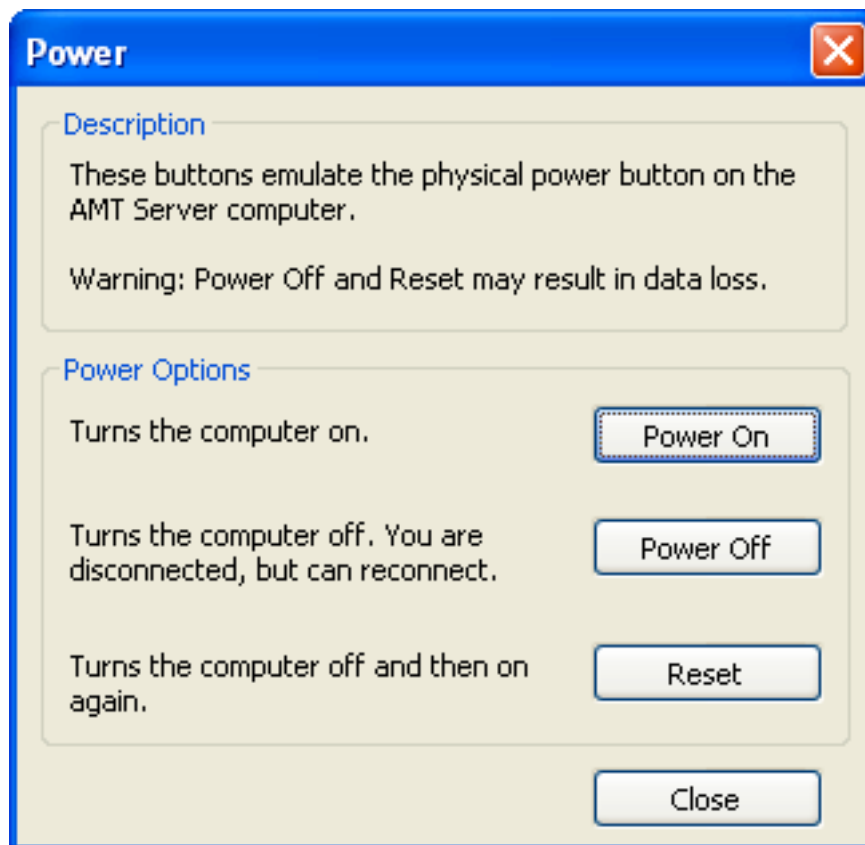
Powering the host computer on and off

You can use *VNC Viewer Plus* to power the host computer on, power it off, and power it off and then on again (that is, power cycle it).

Note: For power on and power cycle, you can choose to boot to BIOS configuration, to an operating system, or to a remotely-mounted image.

To perform these operations:

1. Click the **Power**  toolbar button. The Power dialog opens:

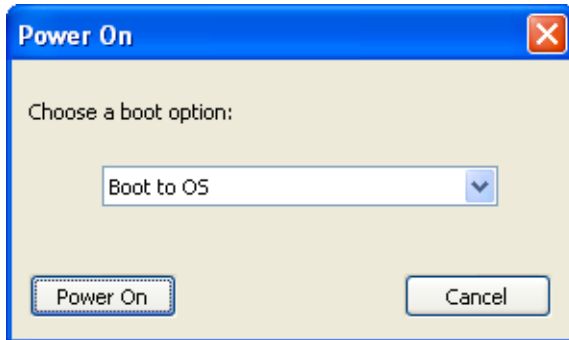


To:

- Power the host computer on, click **Power On**. Note this also wakes the host computer from hibernate, but not sleep, mode.
- Power the host computer off, click **Power Off**. Note that data may be lost if it has not been saved. You are disconnected, but are immediately prompted to reconnect without having to authenticate (actually *establishing* the connection, however, may take several moments).
- Power cycle the host computer, click **Reset**. Note that data may be lost if it has not been saved. You *should* remain connected. If not, configure *VNC Viewer Plus* for Wi-Fi and then reconnect.

Note: Power cycling is not the same as restarting an operating system. An operating system may subsequently complain that it was not shut down properly when the host computer powers back on.

3. For **Power On** or **Reset**, choose a boot option:



(This dialog is specific to the **Power On** command.)


Click the **Power On** button to perform this operation. Click the **Cancel** button to return to the **Power** dialog.

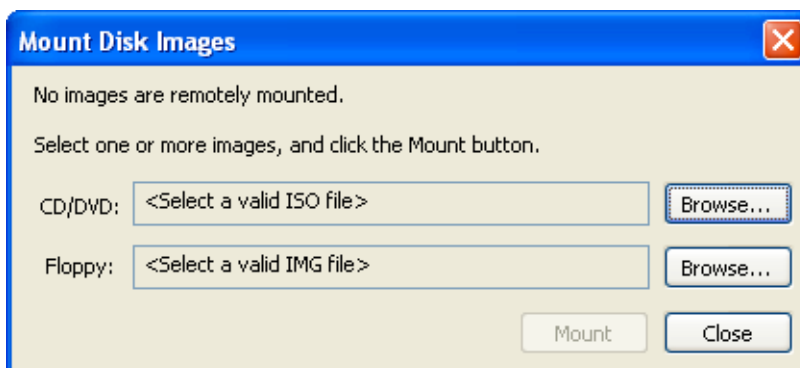
Remotely mounting an image on the host computer

You can use *VNC Viewer Plus* to remotely mount an image representing a CD/DVD or a floppy disk on the host computer. This means you can:

- Boot to that image, perhaps in order to install an operating system or a driver. Note if the image is not bootable it is ignored.
- Register the image as a drive, and navigate it using File Explorer or similar. Note the host computer must have an operating system.

To mount an image:

1. Click the **Mount Disk Images**  toolbar button. The **Mount Disk Images** dialog opens:





2. To mount a:


- CD/DVD image, browse to a valid .iso file.
- Floppy disk image, browse to a valid .img file.

3. Click the **Mount** button. Note the dialog automatically closes.

If you want to:

- Boot to the image, click the **Power**  toolbar button, either **Power On** or **Reset** (depending on the state of the host computer), and choose an appropriate boot option.
- Register the image as a drive, click the **Power**  toolbar button, either **Power On** or **Reset** (depending on the state of the host computer), and choose the **Boot to OS** option.

Note: You need only power cycle in order to register a drive the first time in a *VNC Viewer Plus* session. Subsequent times, you can remove the current image and mount a new one without having to power cycle. This means you can (for example) install a program that is distributed over multiple CDs. (You may need to use a program such as Device Manager (accessible from **System** in Control Panel under Windows 7) to scan for hardware changes in order to actually see the new drive in File Explorer or similar.)

An image remains mounted until you explicitly remove it. To do this, click the **Mount Disk Images**  toolbar button to open the **Mount Disk Images** dialog, and then click the **Remove** button.

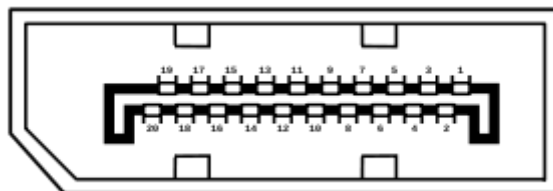
Note: If you disconnect (or are disconnected due to inactivity) and an image is still mounted, another newly-connected *VNC Viewer Plus* user cannot mount an image until you have acknowledged the disconnection warning dialog.

New Features of Amplicon Ventrix and Impact-R Core i5 & i7 Series

The new generation of Amplicon systems also has two new key features to provide more functionality for the industrial market.

Display Port

Amplicon's Impact-R systems feature display port, a modern display interface first released in 2008. Display port was designed to replace VGA, DVI and LVDS display interfaces, with high bandwidth support, to future proof systems for use with modern displays, which will make use of the high bandwidth with higher refresh rates and colour depths than current display standards.



The DisplayPort connector supports 1, 2, or 4 differential data pairs (lanes) in a Main Link, each with a total data rate of 1.62, 2.7, or 5.4 GBit/s, with self-clock running at 162, 270, or 540 MHz. Data is 8b/10b encoded, where each 8 bits of information are encoded with a 10 bit symbol, so the effective data rates after decoding are 1.296, 2.16, and 4.32 Gbit/s per lane (80% of the total).

Cable lengths supported are up to 15m at 1920×1080p60 at 24 bpp.

iTPM (Intel Trusted Platform Module)

For industrial applications requiring additional security functionality, Amplicon's Ventrax systems equipped with Intel i5 and i7 processors feature iTPM (Trusted Platform Module).

The Trusted Platform Module is a component on the desktop board that is specifically designed to enhance platform security above-and-beyond the capabilities of today's software by providing a protected space for key operations and other security critical tasks. Using both hardware and software, the TPM protects encryption and signature keys at their most vulnerable stages—operations when the keys are being used unencrypted in plain-text form. The TPM is specifically designed to shield unencrypted keys and platform authentication information from software-based attacks.