SyAM Software™

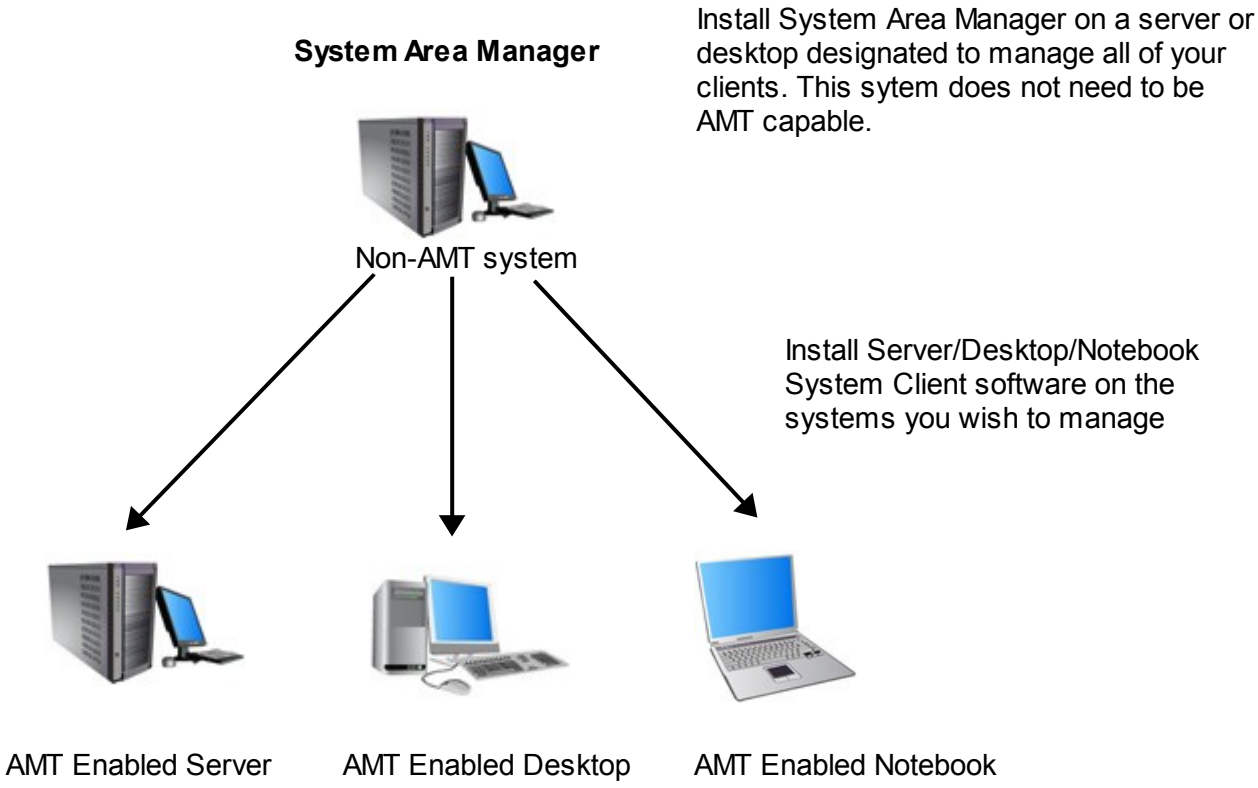
Overview of Managing Intel vPro Platforms using SyAM Software

Revision D

April 2007

Table of Contents

SyAM Software Products



Procedures to installation of SyAM Software:

1. Configure the AMT settings in the BIOS of the Intel vPro platforms.
2. Install SyAM Software System Client products (Server, Desktop and Notebook) on the systems to be managed.
3. Install System Area Manager on the system designated to be the central manager (IP must be static).
4. Browse to the System Area Manager and add the IP addresses of the System Client systems.
5. Configure the Central Alert Matrix.

Configuring AMT BIOS Settings

In order to use the AMT functionality on Intel vPro platforms you must enter the Bios of that particular system and enable it. All Intel vPro platforms are shipped with default settings which must be changed in order to use the AMT functions.

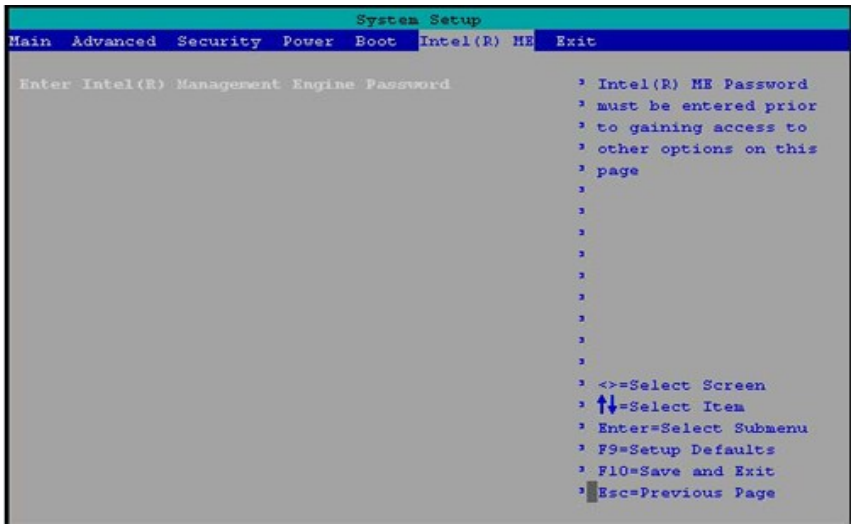
Below are the Bios configurations you need to select for the AMT system to function properly.

AMT 1	AMT 2
Small – Medium Business Provisioning	Small – Medium Business Provisioning
Managability Feature – Intel AMT	Capability - Intel AMT Generation 2.0
Enable SOL and IDER	Managability Feature – Intel AMT
AMT IP Address can be DHCP or Static	Enable SOL and IDER
	AMT IP Address can be DHCP or Static

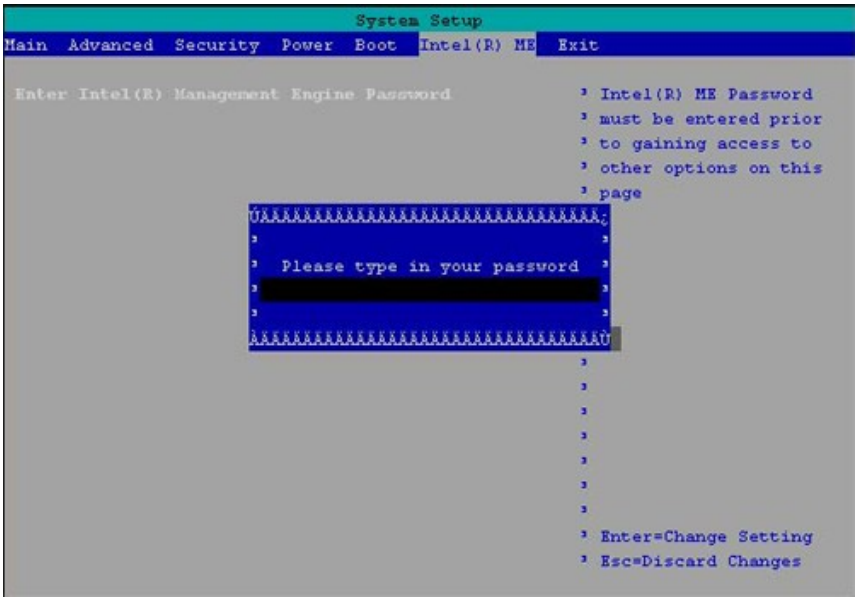
Below is a list of Intel motherboards and their BIOS levels that have been validated by SyAM Software.

AMT Board	Bios Version
D945GTP	NT94510J.86A.3943.2006.0707.1405 NT94510J.86A.3996.2006.0908.1329
SE7230NH-1(NOBHILL2)	NH72310J.86B.1179.2006.0508.2328
DQ965CO	CO96510J.86A.4462.2006.0804.2059 CO96510J.86A.4713.2006.0828.1752 CO96510J.86A.5564.2006.1122.1346
DQ965GF	CO96510J.86A.4178.2006.0713.1823 CO96510J.86A.4462.2006.0804.2059 CO96510J.86A.4713.2006.0828.1752 CO96510J.86A.5564.2006.1122.1346
DQ965WC	CO96510J.86A.4861.2006.0905.1540
D945GCZ	NT94510J.86A.3943.2006.0707.1405 NT94510J.86A.3996.2006.0908.1329

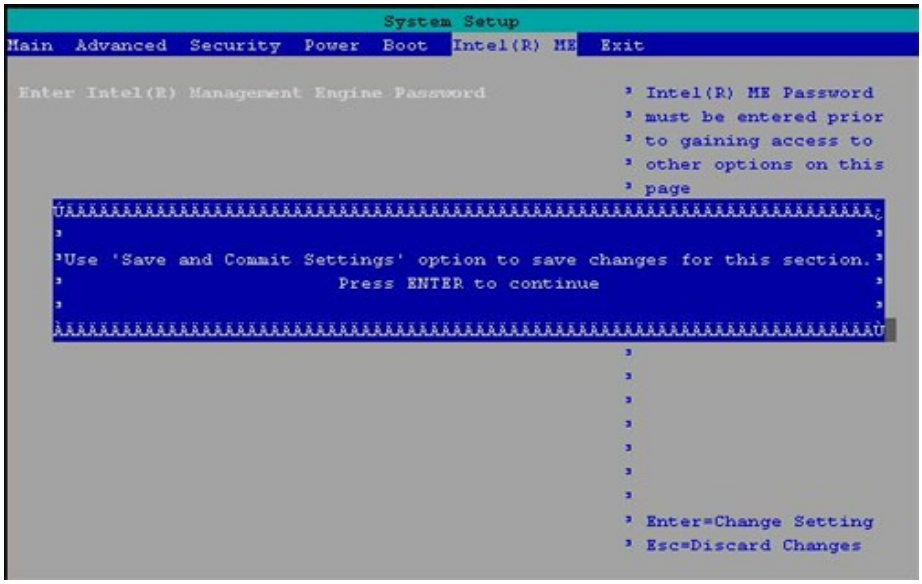
For more information please view our website: http://syamsoftware.com/main/products/validated_config.php



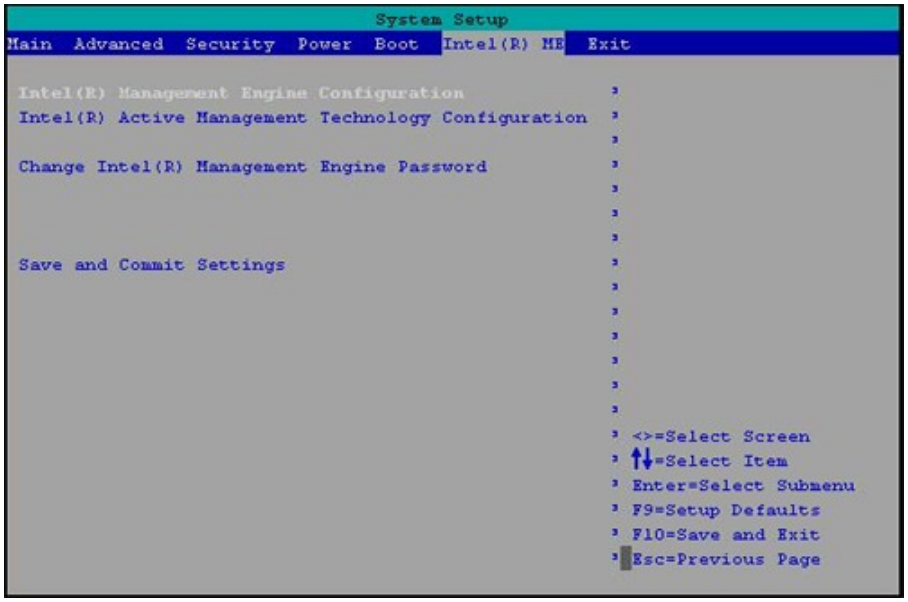
Once in the AMT system's bios, select the Intel tab.



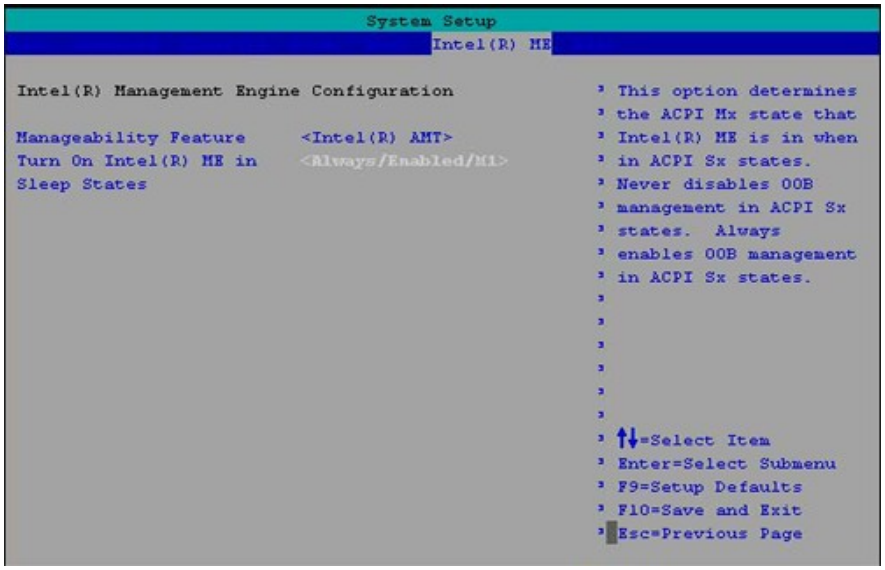
Enter in the AMT password for the system.



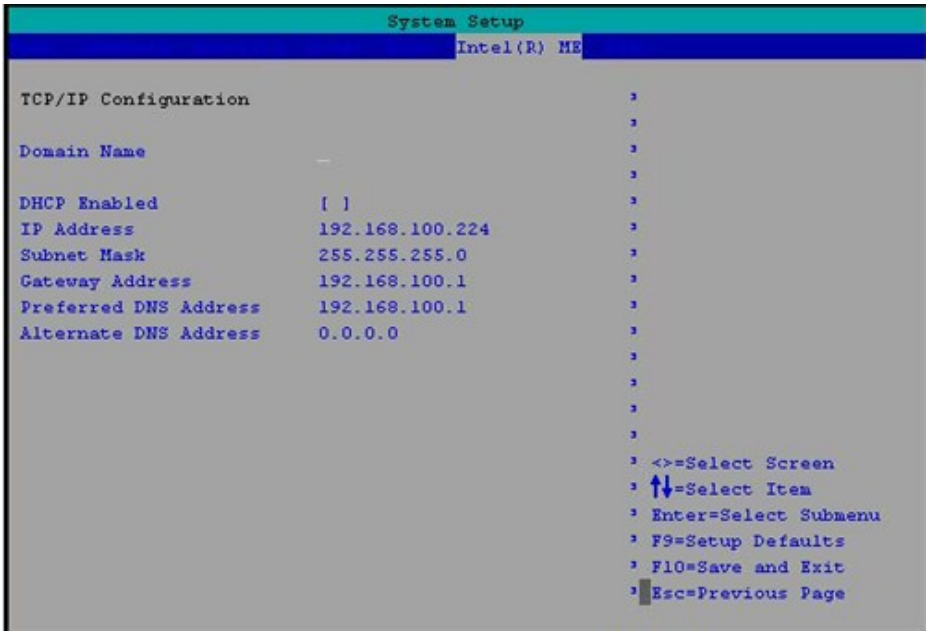
Press enter as directed to continue.



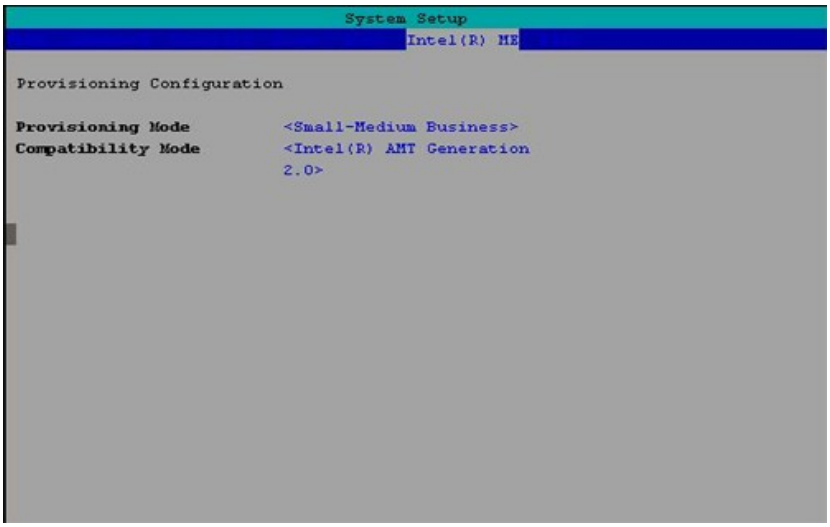
Select Intel Management Engine Configuration.



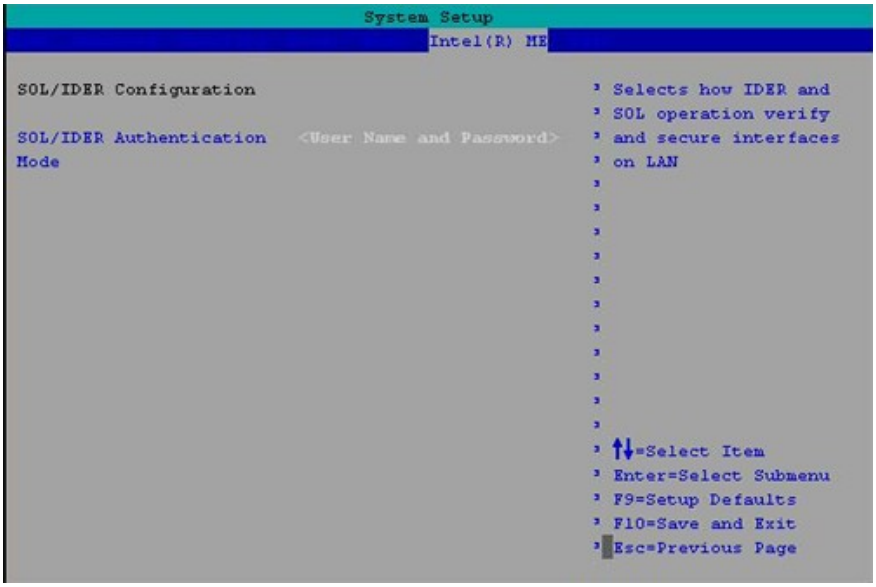
Switch the Managability Feature to Intel AMT, and Turn On Intel ME in to Always/Enabled/M1



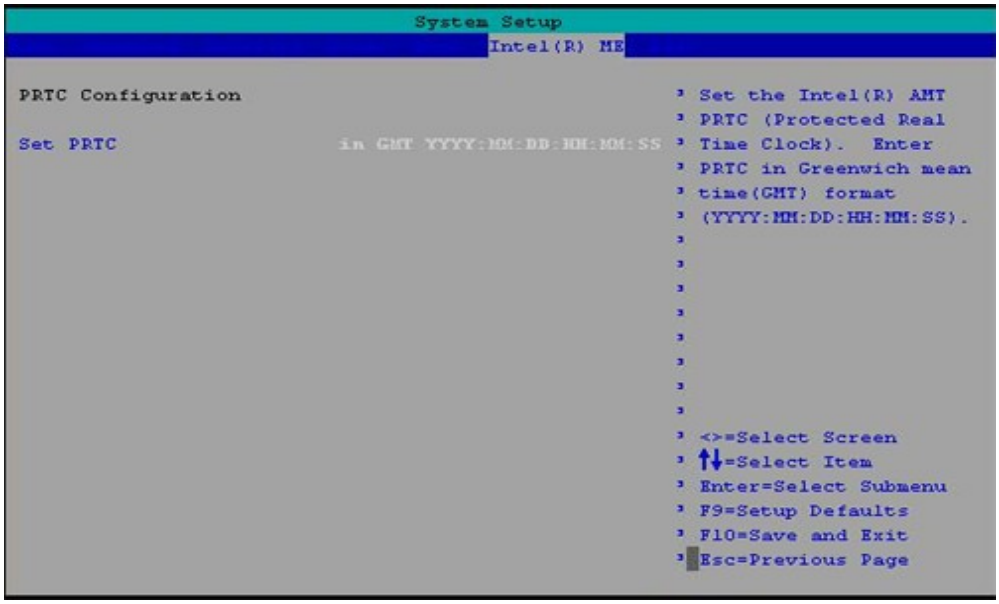
Next, go to TCP/IP configurationto configure the IP address of the system.



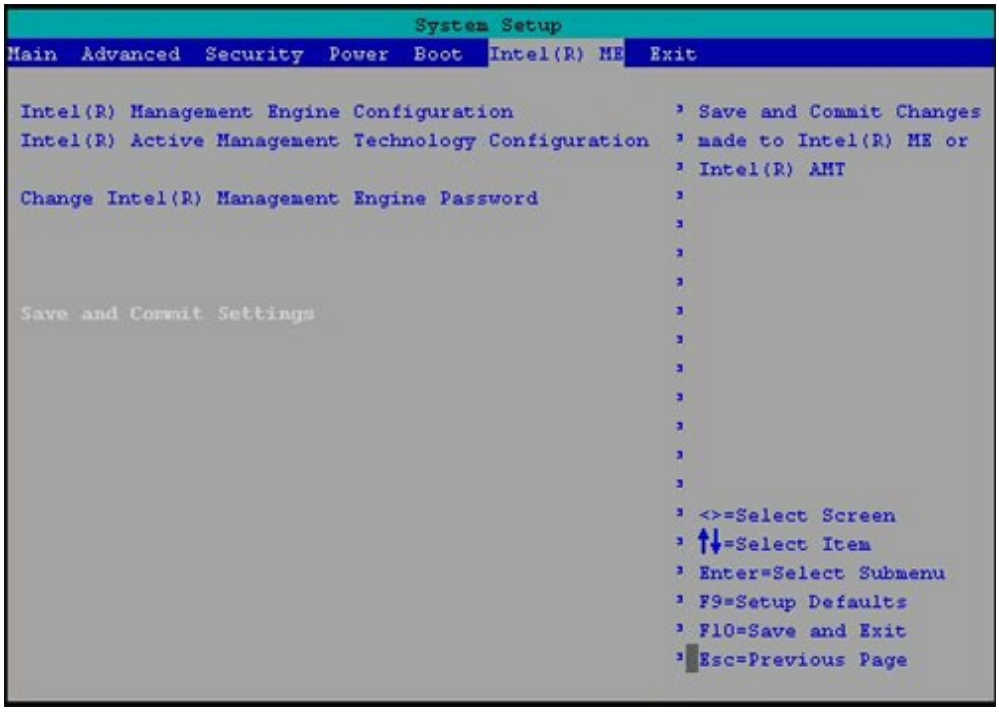
Switch Provisioning mode to Small-Medium Business and Compatibility Mode to Intel AMT Generation.



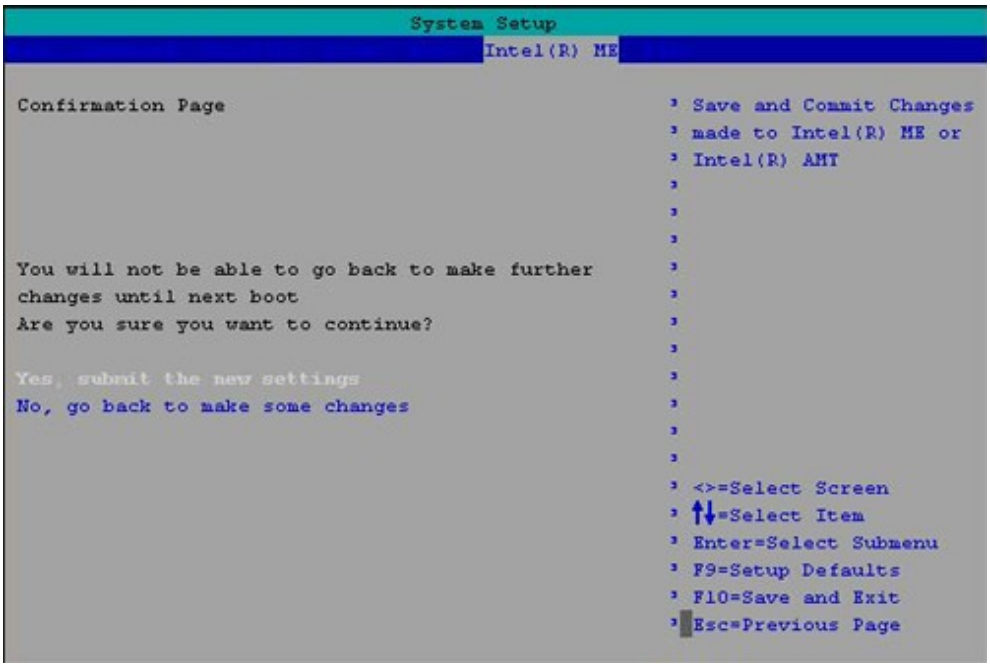
Under SOL/IDER Configuration make sure for authentication it says username and password.



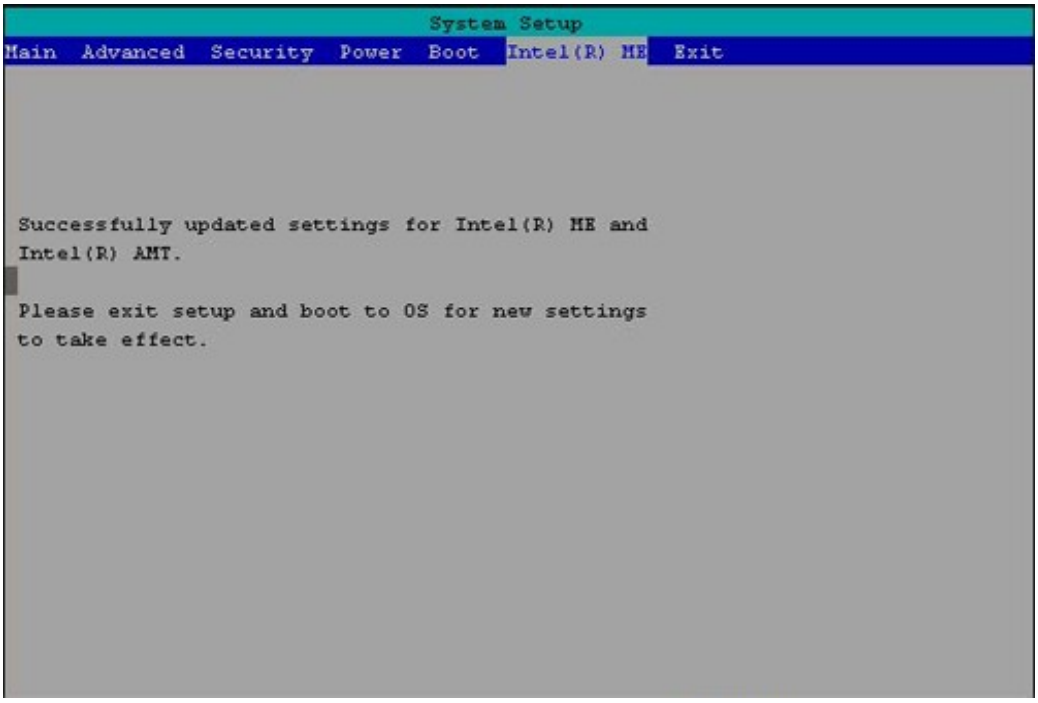
Set the Intel AMT PRTC clock in Greenwich mean time.



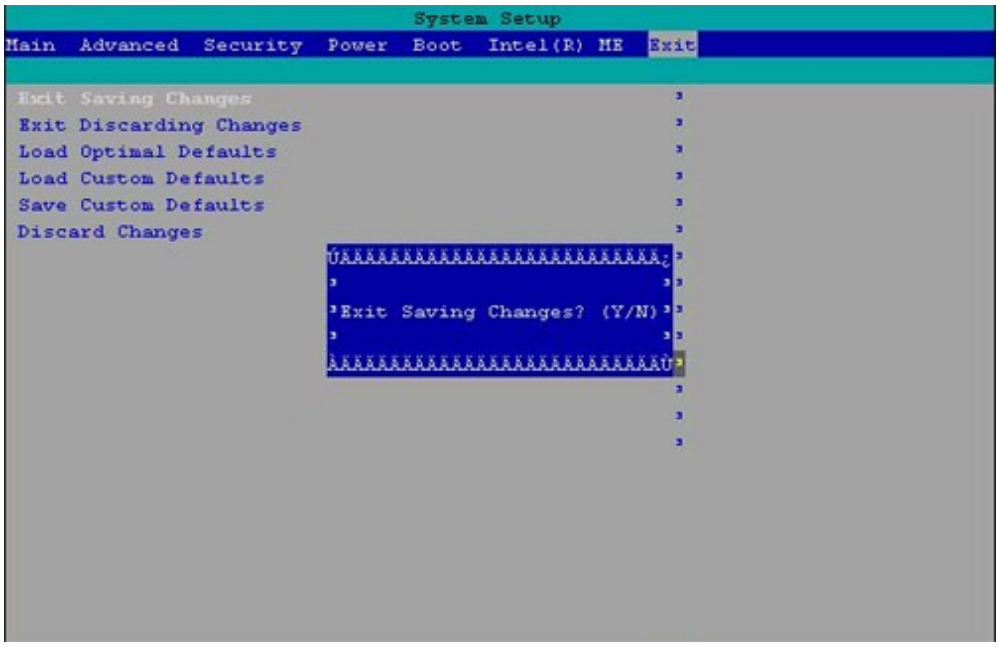
Save and Commit Settings.



Submit the new settings.



Exit the set up for the new settings to take effect.



Exit Bios saving your changes.

AMT Hardware Discovery

In order for the SyAM agent to identify the platform as AMT, the AMT local interface must be present. For AMT1 platforms this means the KCS driver must be loaded. For AMT2 platforms we will utilize the board string to identify that the Intel board is AMT capable. This allows the agent in Windows or Linux environment to identify AMT2 capable hardware.

Board Strings used for identifying AMT2 Capable Hardware :

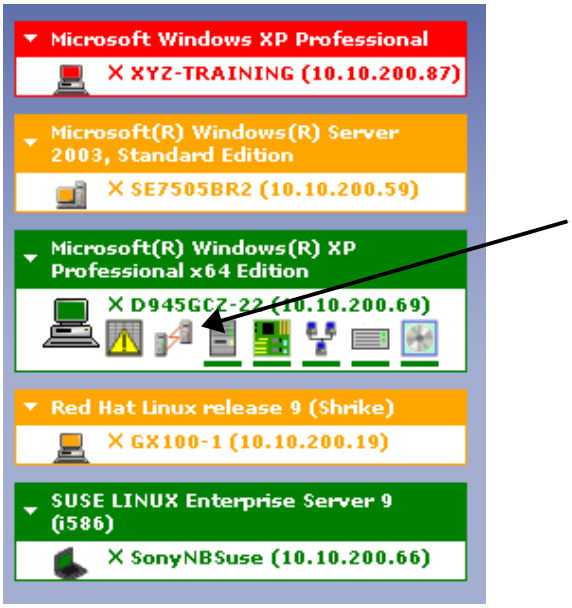
D945GCZ
D945GTP
SE7230NH-1
DQ965CO
DQ965GF
DQ965WC
Broadwater/ICH8

For Version 3.21 the discovery of AMT1 hardware presence will be restricted to Windows based operating systems only as it uses the KCS driver. In Version 3.2 AMT2 hardware identification through the Board string allows Windows and Linux agents to identify AMT2 presence.

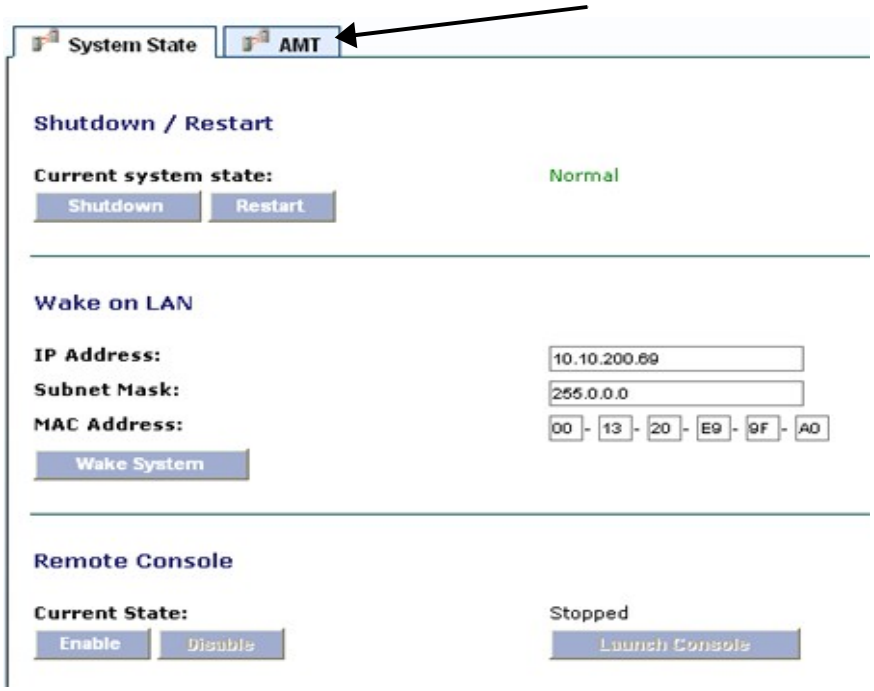
Note: AMT1 systems must install the Host interface driver and AMT2 systems must install the Hechi driver both provided by Intel.

Accessing AMT

You can access the AMT page by clicking on the Remote Management icon located in the system tree.



The AMT Tab will only appear on the Remote Management page if the system running the System Client software is identified as having Intel AMT technology onboard.

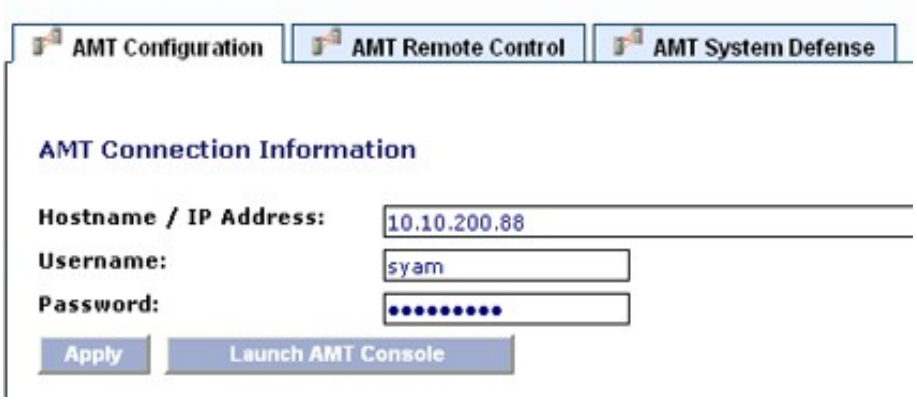


System Client can provide power management and AMT Console access when the system is in either an operating system-present or -absent state.

Please check http://syamsoftware.com/main/products/validated_config.php for validated AMT configurations.

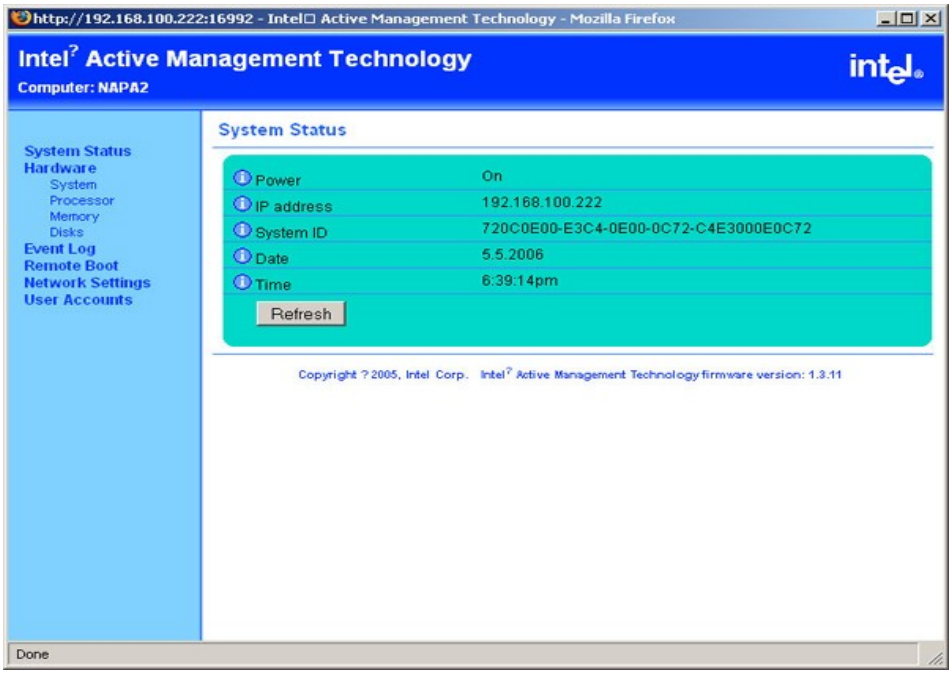
You must first configure the AMT Port IP address and Password using the vendor provided utilities (BIOS configuration) before you can utilize these AMT features.

Next select the AMT tab. On the AMT Configuration page, enter the user name, password and IP address of the AMT port for the managed system, then click on the apply button to save this data.



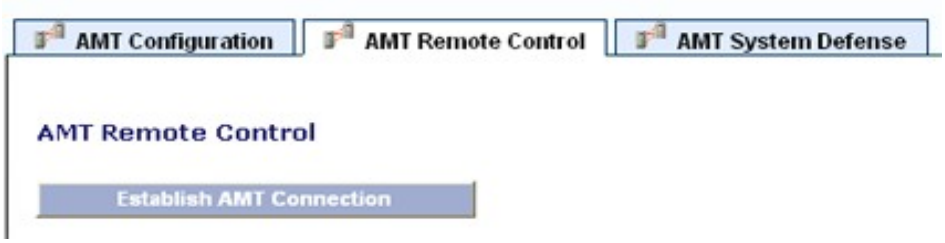
AMT Login Tab

Clicking on the Launch AMT Console will open up a new browser window which allows the user to login directly into the embedded AMT web server for configuration and informational purposes.



Launching the AMT Console

Once you have applied the user name, password and IP Address, click on the Establish AMT Connection button under the AMT Remote Control Tab to access the managed system's AMT Remote control features.



Establish AMT Connection

Power Functions

Once connected to the AMT system you can perform the following power options:

Power Off

This will perform a forced power off not a graceful shutdown.

Power On

This will perform a forced power on.

Power Reset

This will perform a power reset not a graceful reset.

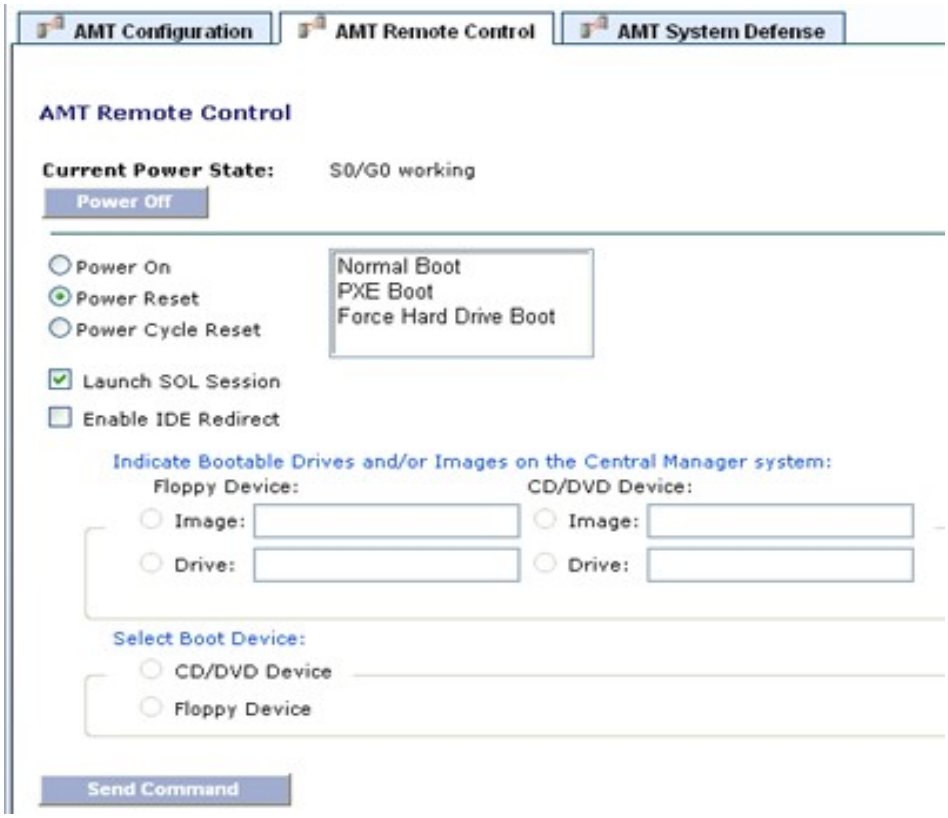
Power Cycle Reset

This will perform a power cycle reset.

Serial Over LAN (SOL)

Serial Over LAN enables a user to remotely reboot a system. When a user reboots with SOL enabled, the SOL session is presented in the user's browser allowing them to have full keyboard functionality with the rebooting system.

In order to create an SOL session, the user must first verify the current power status, then select either power on, power reset or power cycle reset. Next, click the 'Launch SOL Session' box, and then click on the 'Send Command' Button.



AMT Remote Control

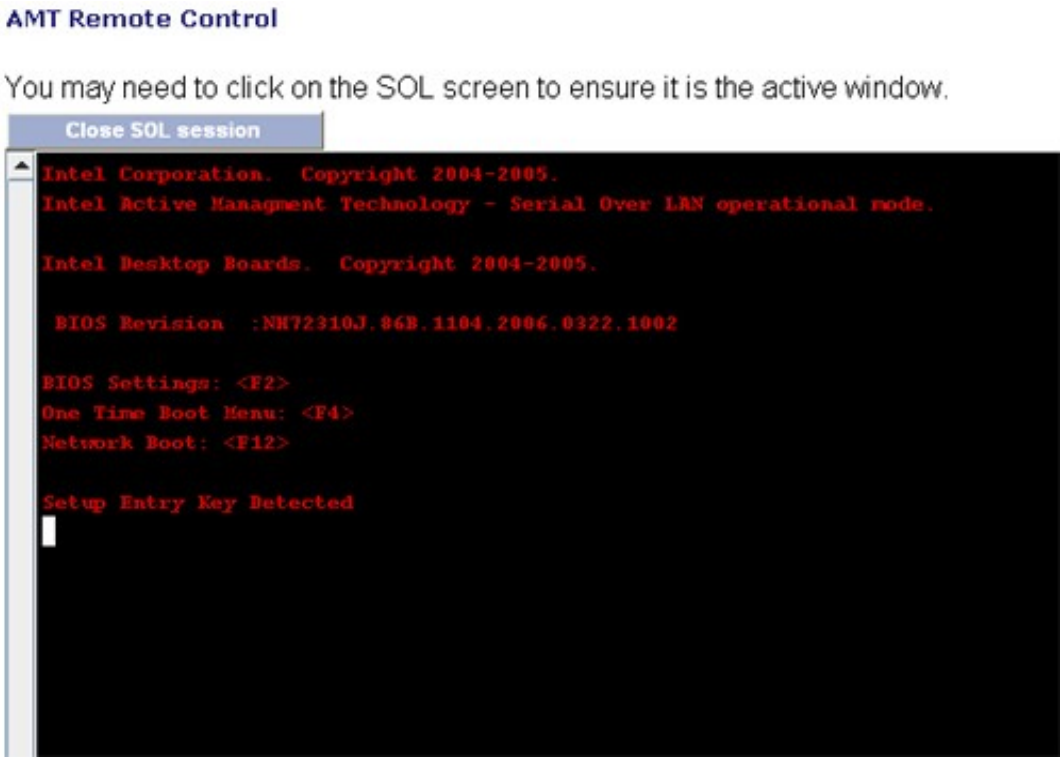
Please Note: When using an SOL session, you are only able to boot the system normally. You cannot specify special commands such as PXE.

Also,SOL and IDE-R only function with Power On and Power Reset Commands.

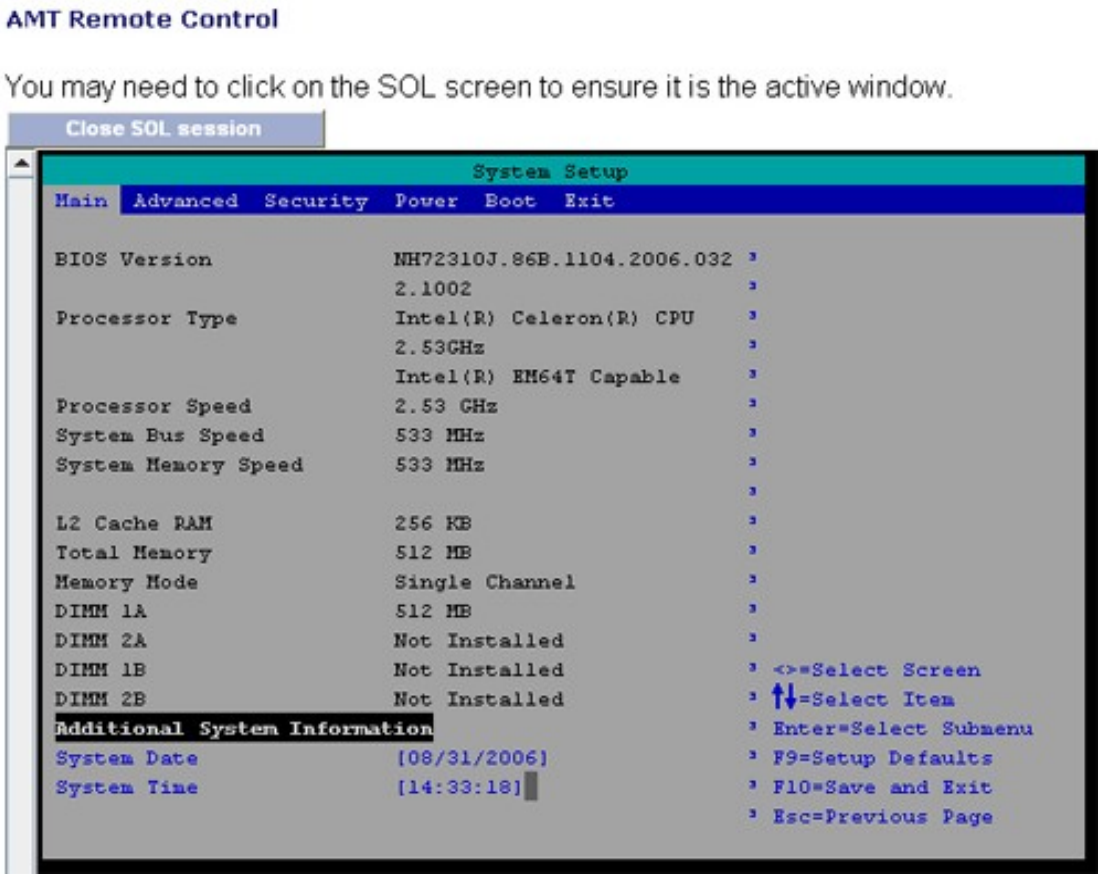
Once in the SOL session you will see the system booting remotely in your browser. It will say in the black screen the key to press in order to enter into the system's bios. First, click on the black screen, and then press that required key.

You must wait until the message to hit F2 appears, if you hit it prior to the message, the SOL session may hang and you will need to use the Close SOL session to exit the session cleanly. If you do not use the Close SOL session and just close the browser window the session will not be properly terminated.

Note*: After three sessions are closed incorrectly you will not be able to create another connection until the System Client Web Service is restarted. This can be done using the windows services manager.*



Serial Over LAN session



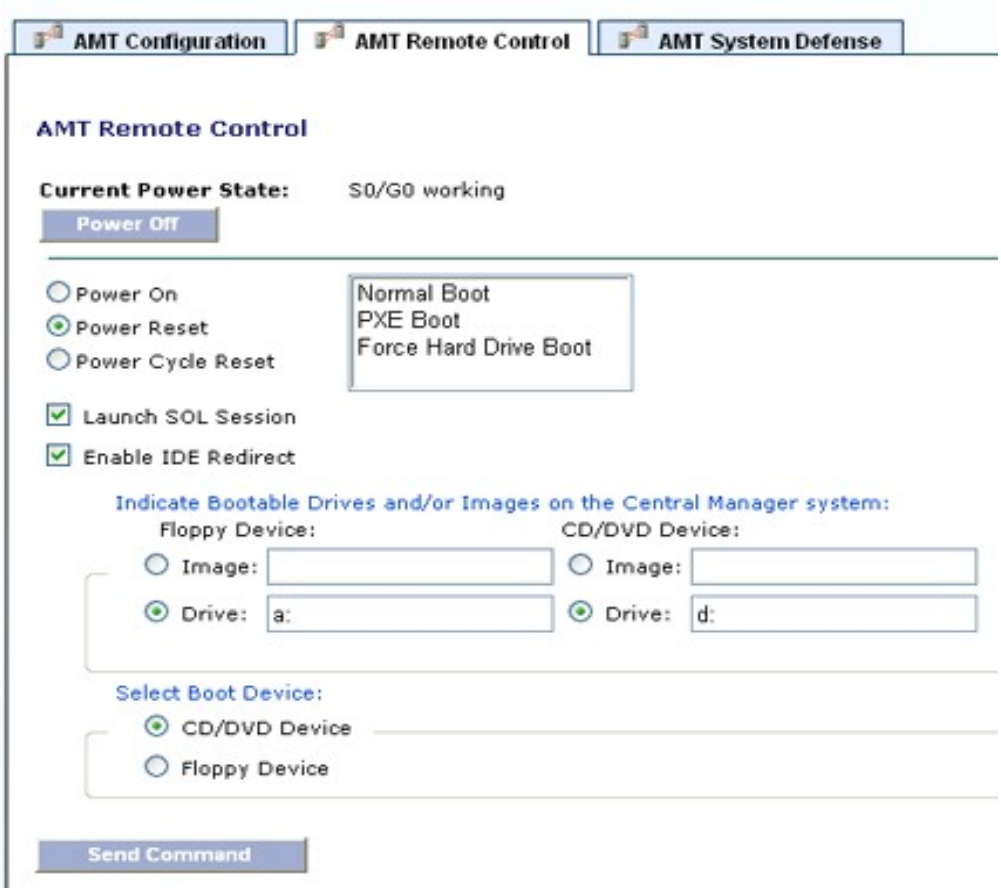
Serial Over LAN (In Use showing BIOS Re-configuration)

IDE-Redirect

IDE-Redirect allows an AMT managed system on a Central Management tree to boot from an image, floppy, CD or DVD device which is located in the system running System Area Manager. IDE-Redirect is only available when using SOL.

Part of the AMT IDE Redirect process is verifying a valid image or device. If you do not have a physical floppy device you must chose the image as the Floppy Device. Both a floppy drive or image, **AND** a CD/DVD drive or image, must be specified. **These drives or images are on the computer running System Area Manager, NOT on the computer running your web browser.**

To invoke the IDE Redirect click a power option and click in the SOL and IDE-R check boxes. Under image or drive, indicate which image or drive you want the system to boot from, then select the boot device, and click 'Send Command'.



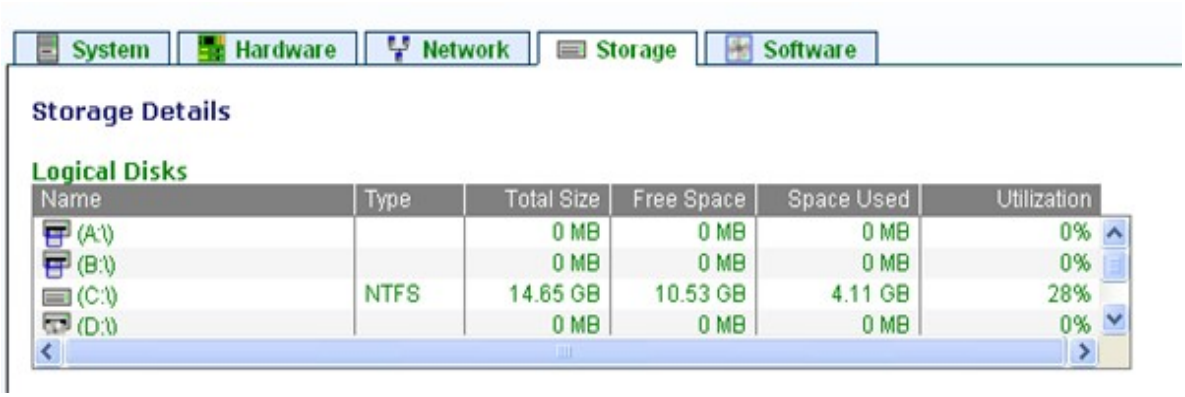
IDE-R on a Windows System Area Manager (Configured to boot off CD-Rom)

Windows/Linux Syntax

When using either a Windows or Linux System Area Manager you need to use the correct corresponding Windows or Linux syntax for the Floppy disk device and CD ROM device.

If you are unsure of the logical letter of the CD ROM device, simply browse to the Storage screen of the Windows System Area Manager.

If no floppy disk drive is present then you must select the bootable image.



Examples of IDE-R Drive and Image Syntax

System Area Manager running on a Windows Operating System

Floppy Device Drive **a:**

Floppy Device Image**c:\win98dos.img** or **c:\win98doscd.iso**

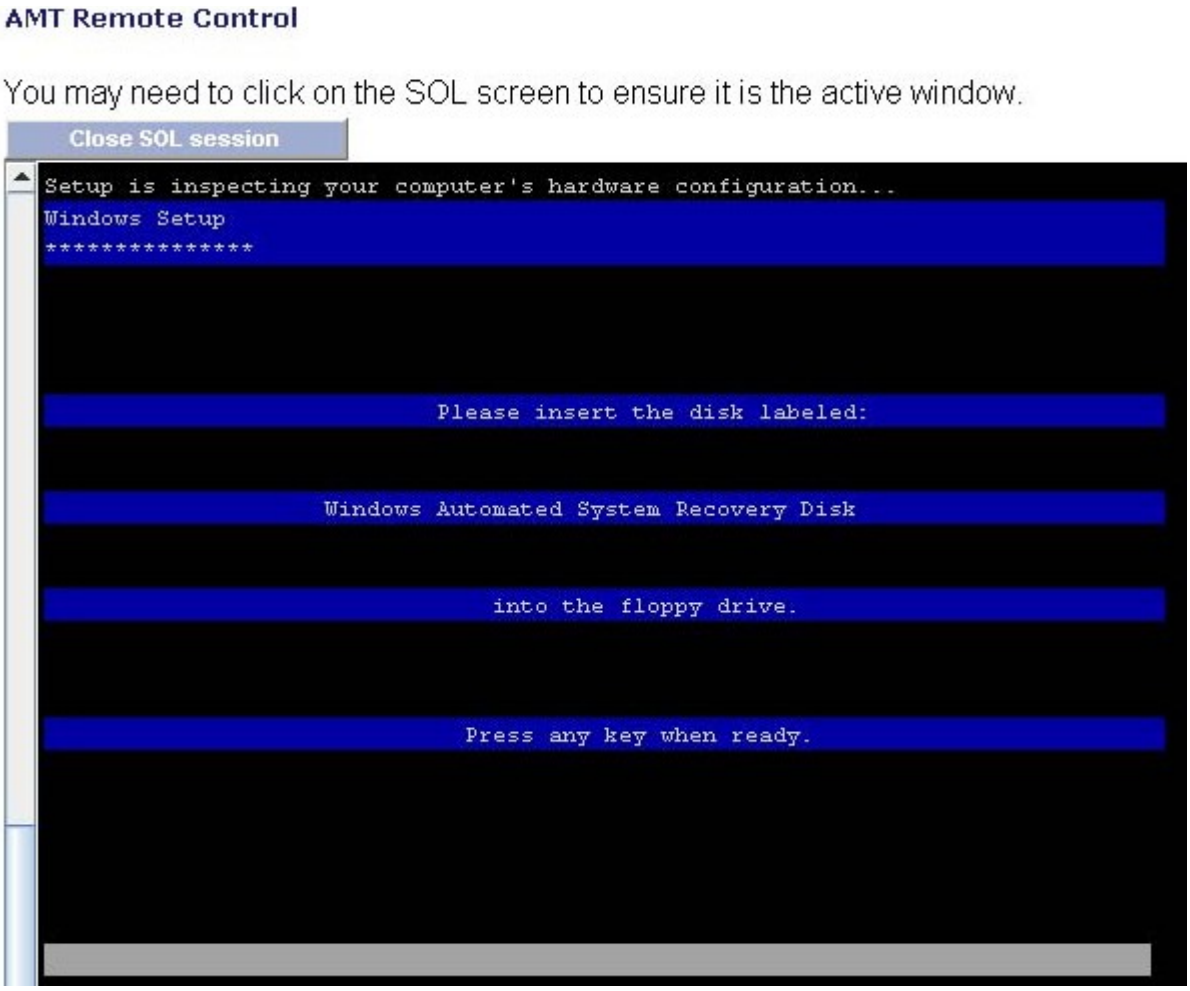
CD Rom Device Drive **d:**

CD Rom Device Image **c:\win98doscd.iso**

System Area Manager running on a Linux Operating System

Floppy Device Drive **/dev/fd0**

CD Rom Device Drive **/dev/hda**

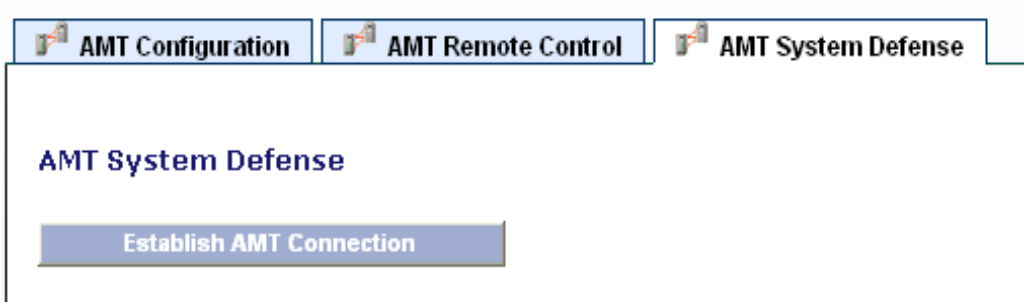


IDE-Redirect using a Windows CD-Rom device

System Defense

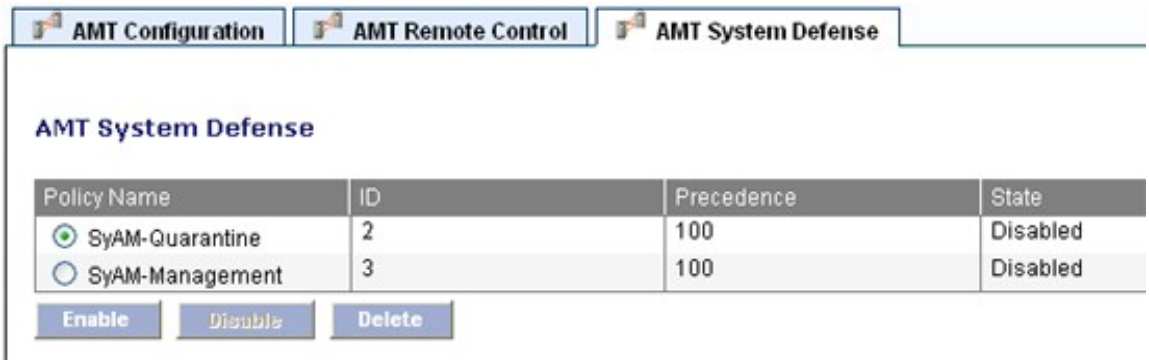
System Defense allows the System Area Manager to define and enforce network security policies. SyAM Software provides two preconfigured policies called SyAM-Management and SyAM-Quarantine.

In order to enable or disable these policies, click on the AMT System Defense tab, and then click on the Establish AMT Connection button.



Next, you will need to download the SyAM Policies by clicking on the Download button.

The Screen will refresh automatically and then the two SyAM-Management Policies policies will appear on the screen.



The “SyAM-Quarantine” policy causes the Intel AMT device to block all packets to/from the operating system running on the client.

The “SyAM-Management” policy causes the Intel AMT device to block all packets to/from the operating system running on the client, except those sent to and from SyAM’s management components. This allows the user to access the Intel AMT client system using SyAM System Client while the operating system is running, in order to inspect or repair the system, but without providing general access to/from the system.

At first, the two policies will appear as disabled. You can make a policy active by clicking on the enable button.There can only be one active policy at a time.
Please note that both SyAM Management polices must be deleted before you will be prompted again to download the policies.

Contact SyAM Software

For additional information, sales, or technical support, please contact SyAM Software:

SyAM Software, Inc.

Corporate Headquarters
1 Chestnut Street, Suite 3-I
Nashua, NH 03060
PH +1 603 598-9575
FX +1 603 598-9577
info@syamsoftware.com

888 UnifyMe (864-3963)

Sales Offices
US Sales 603 598-9575
South America +55 11 3641-3580
Mexico +52 55 8596-5078
Europe +49 (0) 8158 905933
www.syamsoftware.com

To download any of the SyAM Software products, please visit our website at:
www.syamsoftware.com/downloads