

# **Integrating Intel® vPro™ Technology with LANDesk® Management Products**

Information in this document is provided in connection with LANDesk Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted by this document. Except as provided in LANDesk's terms and conditions for the license of such products, LANDesk Software assumes no liability whatsoever, and LANDesk Software disclaims any express or implied warranty, relating to sale and/or use of LANDesk Software products including, but not limited to, liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright or other intellectual property right. LANDesk Software products are not intended for use in medical, life saving, or life sustaining applications. The reader is advised that third parties can have intellectual property rights that can be relevant to this document and the technologies discussed herein, and is advised to seek the advice of competent legal counsel, without obligation of LANDesk Software.

LANDesk Software retains the right to make changes to this document or related product specifications and descriptions, at any time, without notice. LANDesk Software makes no warranty for the use of this document and assumes no responsibility for any errors that can appear in the document nor does it make a commitment to update the information contained herein.

Copyright © 2006 LANDesk Software Ltd. or its affiliated companies. All rights reserved.

LANDesk is either a registered trademark or trademark of LANDesk Software Ltd. or its affiliated companies in the United States and/or other countries. Avocent is a registered trademark of Avocent Corporation or its affiliates. Intel and Intel vPro are registered trademarks or trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

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

Information regarding third-party products is provided solely for educational purposes. LANDesk is not responsible for the performance or support of third-party products and does not make any representations or warranties whatsoever regarding the quality, reliability, functionality or compatibility of these products.

Document version 8.70.5 10/13/06

# Contents

Document overview.....	4
Overview of Intel® vPro™ technology.....	5
Intel vPro technology device setup.....	6
Enterprise vs. Small-business mode.....	6
Configuration in TLS vs. non-TLS mode.....	6
Setup and configuration server.....	7
Setting up, configuring and managing Intel AMT devices in Enterprise mode.....	8
Managing Intel® AMT devices with LANDesk® software.....	12
Version support summary.....	12
Setting up and configuring Intel AMT devices.....	12
Running the Configure Services utility (step 2).....	13
Configuring Intel AMT devices (steps 3-9).....	13
Un-provisioning Intel AMT devices.....	13
Intel AMT BIOS settings.....	13
Automatic discovery and configuration with a setup and configuration server (steps 10-11).....	14
Managing devices from the administrative console.....	15
Intel AMT inventory summary.....	16
Updating the Intel AMT inventory.....	16
Intel AMT event log (step 17).....	16
Power options (step 18).....	16
SOL.....	17
IDE-R boot options.....	17
Other reboot options.....	18
Multi-device boot options.....	18
Changing Intel AMT credentials for managed devices (steps 19-20).....	19
System Defense (step 21).....	19
Agent Presence (step 22).....	21
LANDesk® Out-of-band monitor (AMTMON) features.....	22
Tips.....	23
Tips for Intel® UPSD Desktop Q965 Express motherboard-based systems.....	24
Tips for using static IP addresses.....	25
Log file troubleshooting tips.....	26
Known issues.....	28
Appendix: Previous versions of Intel AMT and LANDesk products.....	32
Setting up, configuring, and managing Intel AMT release 1.0 devices.....	32
Notes on configuring Intel AMT release 1.0 devices.....	34
Notes on discovering Intel AMT release 1.0 devices.....	34
Known issues: Intel AMT release 1.0.....	35
Tips for Lenovo™ systems containing Intel® AMT release 1.0 features.....	35
Tips for Intel UPSD D945G motherboard-based systems.....	36

## Document overview

---

This document describes the use of Intel® vPro™ technology by LANDesk management software, including LANDesk® System Manager, LANDesk® Server Manager, and LANDesk® Management Suite. It documents the practical issues of setting up new devices equipped with Intel® AMT (Active Management Technology) and then discovering and managing those devices using LANDesk products.

The following is a general outline of this document, with a brief description of each section.

- **Overview of Intel vPro Technology:** briefly describes the uses of Intel vPro Technology, specifically Intel Active Management Technology (AMT), and describes the different components of Intel AMT functionality
- **Setting up, configuring, and managing Intel AMT devices:** a procedural outline of the steps required to set up, configure, and manage Intel AMT devices
- **Managing Intel AMT devices with LANDesk software:** procedural instructions for discovering and managing devices equipped with Intel AMT, and notes on using Intel AMT features from a LANDesk product console
- **Tips:** user tips for managing Intel AMT devices with LANDesk products
- **Known issues:** list of current issues with, when possible, workarounds
- **Appendix:** information about using LANDesk version 8.6.x products, and differences in managing Intel AMT release 1.0 devices

**Note on terminology:** Intel AMT is available for desktop PCs and tethered notebooks (it is not supported on wireless connections at this time). These computers are collectively referred to as “devices” in this document to simplify the terms used.

# Overview of Intel® vPro™ technology

---

Intel® vPro™ technology simplifies the management of desktop and notebook computers with built-in management and security features. Key capabilities of Intel vPro technology include remote management, remote problem resolution, and hardware-enhanced security.

Intel® AMT is a key component of Intel vPro technology that provides customers with manageability and security features built into the hardware and which is only fully exposed by third-party management applications like LANDesk® software. Intel AMT hardware features include:

- Non-volatile memory where system information can be secured and stored
- A communication channel that runs separately from the OS, so communication is available even when the device is powered off or the OS is unavailable
- Configurable hardware-based network filters that can be set to quarantine, rate-limit traffic, or send an alert when security threats are recognized

This document describes how LANDesk software implements the features of Intel AMT release 2.0. Intel AMT release 2.0 is supported in LANDesk version 8.70 products. (For information about LANDesk version 8.6.x software and Intel AMT Release 1.0 devices, see the appendix.)

Intel AMT is designed to help IT staff “discover, heal, and protect” managed devices:

- Discover: The Intel AMT device notifies a management server on the network that it is up and ready to be managed. Intel AMT also provides functions that let remote software (such as LANDesk products) query for basic inventory information.
- Heal: Intel AMT features include Serial-over-LAN (SOL) and IDE-Redirection (IDE-R). SOL lets you remote control the boot process of an Intel AMT device and can let you change BIOS settings or run diagnostic programs. IDE-R configures the remote Intel AMT device to boot to a remote media device such as a floppy, CD, or a network-based boot image, allowing you to run a diagnostic program from the management console. Also, management applications can register to receive hardware and system events as they are generated on the Intel AMT device.
- Protect: New Intel AMT protection features are System Defense and Agent Presence.
  - The System Defense feature enables the LANDesk® management console (MC) to configure the Intel AMT device to monitor network packets transmitted to/from the host operating system. The MC configures Intel AMT with policies which, when applied, inspect packets and can take actions such as dropping or limiting the rate of the packets from being transmitted/received and sending an alert to the MC.
  - The Agent Presence feature enables the MC to configure the Intel AMT device to monitor for state changes of a local agent process running on an Intel vPro-based PC. Automatic actions can be taken for specific state changes such as unexpected shutdown or non-startup of a local agent.

The available actions are sending an alert to the MC and automatic application of a System Defense policy.

## Intel vPro technology device setup

Unless pre-arranged with your OEM, Intel AMT functionality is turned off by default. Refer to your OEM setup documentation for information about your hardware.

In order to activate Intel AMT functionality, specific BIOS settings are required. These settings and menu options may vary between OEMs. The procedural instructions in this document describe Intel vPro systems manufactured without any customization. For more detailed information, go to

[http://www.intel.com/business/vpro/pdfs/deployment\\_guide.pdf](http://www.intel.com/business/vpro/pdfs/deployment_guide.pdf).

Once Intel AMT is enabled in the ME BIOS, but before the device has been fully set up and configured (provisioned), the device is considered to be in a pre-provisioned state. While in this state, the various configuration options in the Intel AMT BIOS can be changed. Once the device has been provisioned, most of these options can't be changed until the device is un-provisioned, which resets the Intel AMT settings and puts the device back in the pre-provisioned state.

## Enterprise vs. Small-business mode

Within the Intel AMT BIOS, two modes of operation can be selected: Enterprise and Small-business mode. The main difference between these two modes is that the more secure TLS communication protocol is not available in Small-business mode. This document describes the use of Enterprise mode in examples, and LANDesk recommends using it.

## Configuration in TLS vs. non-TLS mode

LANDesk software communicates with Intel AMT devices using HTTP or HTTPS protocol. It uses SOAP calls provided by the Intel AMT SDK to make HTTP requests for data or to issue commands.

Intel AMT devices can be configured using Transport Layer Security (TLS), which uses HTTPS and certificates to provide stronger security for communication with the LANDesk core server. To use TLS, you must first ensure that Enterprise mode is selected (Intel AMT default) in the BIOS. However, the device does not actually use TLS communication until after it has been configured by your LANDesk software.

When LANDesk configures the device in TLS mode, it creates two certificates. One is saved in the Intel AMT non-volatile memory storage area, the other is put in the `ManagementSuite\AMTProv\CertGenerator\SecScripts\rootCA` folder on the core server. Because HTTPS and certificates are used from then on to communicate with the device, other Intel AMT-enabled third-party applications or even other LANDesk core servers will be unable to talk to the device unless they get a copy of the certificate (from the `rootCA` folder) that was created during the configuration process. If you don't have the certificate, you must fully un-provision and then re-provision the Intel AMT device in order to clear the certificate and generate a new one.

Intel added the PID/PPS mechanism in Intel AMT release 2.0 to secure the certificate transmission process. The PID (provisioning ID) is simply an ID number and the PPS (provisioning passphrase) is an alphanumeric string used for encrypting the communication channel. These two strings work together to verify in a secure way that the device is being configured by an authorized management console.

The process for creating PID/PPS pairs and using them is as follows. The admin creates one or more PID/PPS pairs using the LANDesk administration console. The pairs that are generated are saved in the database, and the admin prints a list of the pairs. The admin then enters a PID and PPS manually on each Intel AMT device.

After the admin exits the AMT BIOS, the Intel AMT device sends a “hello” packet, containing only the PID, to the setup and configuration server (the LANDesk core server). The LANDesk product looks up the PID in the database to find the PPS, and then begins the configuration process. The PPS is used to encrypt the communication channel between the LANDesk core server and the Intel AMT device. With the encrypted communication channel, the TLS certificate is transmitted to the Intel AMT device and secure TLS communications are enabled.

## Setup and configuration server

Intel vPro devices running Intel AMT in Enterprise mode require a setup and configuration server to be available on the network. A setup and configuration server has an application running which listens for “hello” packets from Intel AMT devices. Beginning with version 8.70 LANDesk products, core servers include a setup and configuration server.

When you set up a device, you can identify the setup and configuration server by entering the setup and configuration server’s IP address (the IP address of your core server) and port 9971 in the Provisioning Server section of the Intel AMT BIOS.

After the LANDesk core server receives the “hello” packet it immediately configures the device and puts it in the AMT section of the LANDesk Unmanaged device discovery (UDD) table in the database.

For more information about the discovery and configuration process, see “Managing Intel AMT devices with LANDesk software” later in this document.

# Setting up, configuring and managing Intel® AMT devices in Enterprise mode

---

This section contains a procedural list that outlines the basic steps to follow in setting up, configuring, and managing devices with Intel® AMT running in Enterprise mode and using TLS security. Details and tips about individual steps can be found in the following section, “Managing Intel AMT devices with LANDesk software.”

These instructions are written for users of LANDesk® System Manager. The procedure is the same for LANDesk® Server Manager. Most steps are similar for LANDesk® Management Suite, although there are differences when using the Win32 console to manage devices.

This example uses an Intel® BIOS. Details of how the BIOS screens are accessed and the specific UI choices in the BIOS may vary between different manufacturers.

## Configuring and discovering the device

1. Install the LANDesk software. Activate the core server by running the Core Server Activation utility (**Start | All Programs | LANDesk | LANDesk Core Server Activation**).
2. At the LANDesk System Manager console, open the Configure Services Utility (**Start | All Programs | LANDesk | Configure Services**). Click the **Intel AMT Configuration** tab. Under **Current Intel AMT Credentials**, enter the username and password you will be using when you set up the new Intel AMT devices in the Intel AMT BIOS. If you want to use a different set of credentials to access the device after setup is complete, enter a username and password under **Provision with new Intel AMT Credentials**. Click **Provision in TLS mode**, then click **OK**.

**Note:** While you could manage devices in Enterprise mode and select non-TLS security, it is not recommended that you do so.

3. Open the LSM console (**Start | All Programs | LANDesk | LANDesk System Manager**). Click **Hardware Configuration | AMT | Provisioning | Generate AMT ID**, and generate one or more PID/PPS pairs. When they are generated, print the list of key pairs for use in setting up the device (see step 8).
4. On the Intel AMT device, start the ME BIOS (press F2 as the device boots). Change the password to a strong password. In the ME BIOS, set the Manageability Feature to Intel AMT. This allows the display of Intel AMT options from the ME BIOS main menu.
5. If the device has been previously managed or its previous state is unknown, then fully un-provision it.
6. Ensure that **Enterprise mode** is selected as the Provisioning Model (this is the default Intel AMT setting).
7. For the Provisioning Server details, enter the IP address of the LSM core server and port 9971.

8. Enter a PID/PPS pair from the list that you printed. (Be sure that you use a unique PID/PPS pair for each device.)
9. Choose the **Save and Exit** option in the AMT BIOS.
10. Open the LSM console and find the device in the **Intel AMT** group in the top pane of the **Device discovery** page. Right-click the device and select **Target**. In the lower pane, click the **Manage** tab, select **Move targeted devices**, and click **Move**. The device is then moved from **Device discovery** to **My devices**.
11. To verify that the process worked, double-click the device in the **My devices** page (to open the Server information console for that device) and select the **AMT | Intel AMT options** page. You should see inventory data for the device.

### Installing agents on the device

At this point, the Intel AMT device can be managed with some, but not all, Intel AMT features. Other features require a LANDesk agent to be installed on the device. The Agent Presence feature requires a LANDesk agent, as do the amtmon.exe features (disabling the network, enabling the network, and scheduling a vulnerability scan on the next reboot).

Before you install the LANDesk agent, two Intel drivers and a Microsoft patch must be applied to the device. You can then install agents using the “pull” or “push” method, as explained in the following steps.

12. To install these drivers, you must have the ME enabled in the ME BIOS and Windows must be running.
13. Install the Intel® Management Engine Interface driver. The ME Interface driver is required by LANDesk agents to communicate with the local Intel AMT storage area. Make sure this driver is the latest version (currently the version number is 1081). If you update this driver, verify that the version was actually updated by checking the driver’s properties under **System Devices** in the Windows® Device Manager. If it did not update correctly, redo the update from the Device Manager – System Devices list: right-click the driver, select **Properties**, click the **Driver** tab, and click **Update Driver**.
14. Install the Intel Active Management Technology – SOL (COM3) driver. This driver is not actively used, but is installed as a placeholder so you don’t get an “Unknown hardware” error in the System Devices list.
15. Ensure that the Microsoft® Cumulative Security Update for Internet Explorer MS05-014 is installed. This update contains a Microsoft patch required by Intel AMT. Although Microsoft Knowledge Base article 889388 says that the patch applies to Windows Server® 2003, we have found that it is also needed for Windows® XP. The patch fixes an issue in an HTTP Service module and prevents the LANDesk agents from crashing when calling into the Intel AMT API.
16. The quickest and easiest way to install the LANDesk agent on a single managed device is to “pull” the agent. At the Intel AMT device, map a drive to the core server and attach to the **ldlogon** share. Run **wscfg32.exe** to install the LSM and LDMS agents, or run **ServerConfig.exe** to install the LDSM agents. Make sure Monitoring is selected in the agent configuration.

or

“Push” the LANDesk agent to one or more devices from the LANDesk console.

- a) If the credentials you are using on the console are different from those you use on the managed device, open the Configure Services utility (**Start | All Programs | LANDesk | Configure Services**). Click the **Scheduler** tab and click **Change Login**. Change the **Service Login** to the credentials for your LANDesk console, and add the credentials for the managed device to the **Alternate credentials** list. (This allows the scheduler to remotely log in on the managed devices to install the agent.)
- b) In the LANDesk console, click **My devices**. Select the Intel AMT devices you want to install the agent to and click **Target**.
- c) Click **Agent configuration** and select a standard Windows agent configuration. Or click **New** to create a new configuration with the agents that you want to install (the Monitoring agent must be included in any agent configuration installed on an Intel AMT device).
- d) With the configuration selected, click **Schedule task** on the toolbar. Click **Targeted devices | Add target list**, then click **Schedule task | Start now**. Click **Save**. The agent configuration package is built and installed on the targeted devices. It may take several minutes before there is any activity on the devices as the package is built. You can watch the progress of the agent installation by clicking the **Configuration tasks** tab on the lower pane of the console. The Intel AMT device does not need to be rebooted after the agent package is installed.

## Managing devices

The following Intel AMT features can be accessed after you have configured, discovered, and installed agents on your Intel AMT device.

17. To view the Intel AMT event log, double-click the device in the **My devices** list, then click **System information | Logs | Intel AMT log**.
18. To select power options such as reboot, Serial-over-LAN and IDE-R options, double-click the Intel AMT device in the **My devices** page, then click **Power options** in the left navigation pane.
19. To change the Intel AMT credentials for one device, double-click that device in the **My devices** page, then click **Hardware configuration | AMT | Provisioning | Configuration**.
20. To change the Intel AMT credentials for multiple devices, open the LSM console and click **Hardware configuration | AMT | Provisioning | Configuration**.
21. To select a System Defense configuration, open the LSM console and click **Hardware configuration**. In the console that opens, click **AMT | System Defense**. The **System Defense policies** page lets you apply System Defense policies to the Intel AMT devices you have targeted. The **System Defense remediation** pages lets you restore network access to devices whose traffic filter has tripped an applied policy and are currently quarantined.

To test this feature, target a device and apply the “BlockFtpSrvr” policy to it.

On that device, open a command prompt window and enter `ping -t <core server address>`. Open a second command prompt window and enter `ftp <core server address>`. This should trigger the SD policy and send an alert to the core server, which can be seen in the LSM alert log (click **Log** in the LSM console). Double-click the alert to see a detailed description. The pings should also stop responding. To resolve the issue, click **AMT | System Defense | Remediation** in the LSM console, select the computer, and click **Apply**. The pings should now resume.

22. To select an Agent Presence configuration, open the LSM console and click **Hardware configuration**. In the console that opens, click **AMT | Agent Presence | Configuration**. Agent Presence is a global configuration. It will apply the selected configuration to all Intel AMT R2.0 devices that have a LANDesk agent installed on them.

To test this feature, open the Agent Presence Configuration page and set the **Heartbeat** times to 30 seconds and the **Startup** times to 60 seconds, then click **Apply**. On a managed Intel AMT device, open the Windows® Task Manager and kill the **collector.exe** process. Within 30 seconds, an Agent Presence alert should show up in the LSM alert log. Double-click the alert to get more detailed information. Return to the managed Intel AMT device, and from the LDClient directory run **restartmon.exe** to restart the collector. Within 30 seconds another Agent Presence alert should appear in the LSM alert log indicating that the LANDesk Monitoring service is started.

# Managing Intel® AMT devices with LANDesk® software

---

This section describes in detail how Intel® AMT devices are discovered and managed using LANDesk® software products. It gives details about some of the procedural steps outlined in the previous section. This section also contains information about using Intel AMT features with LANDesk software products.

## Version support summary

Intel AMT release 2.0 features are supported in LDSM and LSM 8.70. They are not supported in LDMS except when LSM or LDSM is also installed on the same server as LDMS. Either of these products can be selected for installation during the LDMS installation, or they can be installed standalone.

When a management agent is installed from the LDMS console onto an Intel AMT device, using the Client configuration tool, the System Manager agent option can be selected in the agent configuration. This installs the LSM features that enable Intel AMT on the managed device.

**Note:** When installing LDMS with LSM or LDSM, you do not need to check the Web console checkbox on the page where LSM is selected. The Web console check-box on that page is for installing the LDMS Web console, not the LSM or LDSM web console.

LSM and LDSM 8.70 support four features that are new in Intel AMT release 2.0:

- Agent Presence, which monitors LANDesk agents running on the managed device.
- A very basic implementation of System Defense, which monitors network traffic patterns.
- The use of PID/PPS pairs for additional configuration security.
- A setup and configuration server, which monitors network traffic for Intel AMT devices. The devices send a discovery packet to the setup and configuration server and, in response, the setup and configuration server automatically configures the devices (although there are some manual steps that must be performed on the Intel AMT device before the discovery packet can be sent).

## Setting up and configuring Intel AMT devices

The setup and configuration process described in this document is based on the Intel implementation of Intel AMT. As other manufacturers implement this standard, their hardware and firmware may differ from what is described here.

Parts of setup and configuration are done in the BIOS screens of the Intel AMT devices. Other tasks are done by LANDesk software products. For example, the initial credentials (username and password) used to enable Intel AMT features are entered in the BIOS screen of the device. For Intel AMT release 2.0 devices in Enterprise mode, configuration can only be completed by the setup and configuration server (LANDesk core server) that communicates with the device via a secure TLS connection.

## Running the Configure Services utility (step 2)

The first configuration task for Intel AMT devices is to run the LANDesk Configure Services utility and (on the **Intel AMT configuration** tab) enter the same username and password that will be entered in the AMT BIOS. If you want the credentials to be changed when the device is configured, enter a second set of credentials. The scenario for this is that the IT person who receives the Intel AMT devices and gets them all configured can do this using a potentially less-secure password or at least one that is different from what the final administrator wants to use. When LANDesk **[INSERT management software]** initially configures the devices it will automatically change the AMT username and password to the new username and password if you have entered both sets of credentials in the Configure Services utility.

## Configuring Intel AMT devices (steps 3-9)

With Intel AMT there are two BIOS screens used for setup and configuration. The first is the ME (Manageability Engine) BIOS extension screen, and the second is the AMT BIOS extension screen. Intel AMT functionality is enabled or disabled on the ME BIOS, and the AMT BIOS can only be accessed after you enter the ME BIOS and enable Intel AMT. (If you are unable to enter the AMT BIOS, make sure Intel AMT is enabled in the ME BIOS.)

The first task in configuring Intel AMT is set the ME password to a strong password. The default ME password is "admin". There is no interface to change the ME password programmatically, so it can't be changed via LANDesk software. If you change the ME password and subsequently forget it, you will be unable to enter the ME or AMT BIOS and will need to reflash the firmware. When you change the ME password, that ME password also sets the Intel AMT password. There is no separate option to explicitly set the Intel AMT password in the BIOS, but in reality they are two separate credentials. The Intel AMT credentials have a programmatic interface and, after you change the ME password to a strong password, you can change the Intel AMT credentials via the LANDesk console or during the configuration process.

## Un-provisioning Intel AMT devices

The AMT BIOS includes options to fully or partially un-provision the Intel AMT device, which reverses the changes made during setup and configuration. It is always a good idea to un-provision the device before configuration, as there is no accurate way to determine what state the Intel AMT device is currently in. A full un-provision resets most of the Intel AMT settings back to their defaults, and removes any existing certificates. If there is an existing certificate on the device that was not generated by the existing LANDesk core server, then LANDesk **management software** will not be able to talk to Intel AMT. A partial un-provision is used when you want a previously configured device to start re-sending "hello" packets, because it was either deleted from the LANDesk console or there was some unrecoverable error during the discovery or management process. While none of the Intel AMT settings are reset during a partial un-provision and no existing certificate is cleared, you can change some of the Intel AMT fields, such as the Host name and Provisioning Server address.

## Intel AMT BIOS settings

Various settings in the AMT BIOS screen are described below.

**Host name:** The host name set in the Intel AMT BIOS is independent of the Windows computer name.

If the Intel AMT device is going to be added to a Windows Domain, fill in the **Domain** field; otherwise, leave it blank.

In the **Provisioning Server** address field, enter the LANDesk core server IP address. The port is 9971. If you forget this port number, it can be found in the text on the **Intel AMT Configuration** tab in the Configure Services utility.

(There is another option for identifying the setup and configuration server. You can manually create a new DNS entry called "ProvisioningServer" and give it the same IP address as the core server. If you don't enter a Provisioning Server address in the AMT BIOS, then Intel AMT will send out a packet to server ProvisioningServer, which should resolve to the core server address if you have added the DNS entry.)

We recommend that the Enterprise and TLS modes be used for additional security benefits. In order for AMT "hello" packets to be sent to the setup and configuration server, Enterprise mode must be selected. Selecting Enterprise mode does not require that TLS communication mode be used; non-TLS may still be selected in the LANDesk Configure Services tool.

When Enterprise mode is selected, a PID/PPS must be entered as well. The PID/PPS is created in the LANDesk console using the Hardware Configuration tool. The PID prefix is simply an arbitrary identifying character sequence. The Batch name is a label that lets you identify various PID/PPS batches that you generate. These PID/PPS pairs can be printed out to better facilitate entering them on the various Intel AMT devices, but for security purposes the print-out should be destroyed when configuration is complete. When entering the PID/PPS, include the dashes; letters can be upper- or lower-case. A unique PID/PPS pair should be used for each device – do not use the same key for multiple devices.

Make sure SOL and IDE-R are enabled if you plan to use those features.

## Automatic discovery and configuration with a setup and configuration server (steps 10-11)

After you exit the AMT BIOS screen, a "hello" packet is sent to the address entered in the **Provisioning Server** field. A service on the LANDesk core server listens for the "hello" packet and once it is received, the LANDesk product configures the Intel AMT device in either TLS or non-TLS mode and puts the device into the **Intel AMT** group in the **Unmanaged** list on the **Device discovery** page.

When the device is configured, if you entered a secondary username and password in the Configure Services utility, the credentials of the Intel AMT device are changed to the new ones as part of the configuration process.

If the device does not show up in the **Unmanaged** devices list, try the following troubleshooting options:

- Check the Event Log in the LANDesk console for a possible problem.
- Make sure the credentials entered in Configure Services are the same as those entered in the ME BIOS on the Intel AMT device.
- Make sure the Intel AMT device was fully un-provisioned, and not partially un-provisioned, unless you know it was previously configured by this core server.

The “hello” packet is initially sent every minute the first five minutes, then once every ten minutes for the next hour, then once every hour for the next day, then the “hello” packet stops being sent except once every time the device starts up after a reboot. However, as soon as the device is successfully configured, the “hello” packet stops being sent until the device is either partially un-provisioned, or is fully un-provisioned and re-configured.

Once the Intel AMT device is found in the discovered devices list, manage the device by selecting it and using the **Manage** tab options under **Device discovery**. The process may take a couple of minutes as the LANDesk product gathers the inventory to populate the database and completes further configuration of the Intel AMT device. You can watch the progress of the move by clicking the **Move status** tab; if the device fails to be managed this tab will show possible failure explanations. After the device is successfully managed, it can be found in the **My devices** list. Click the **Refresh** button on the toolbar if the display doesn't auto-refresh.

## Managing devices from the administrative console

When a device is moved from the **Unmanaged** devices list to the **My devices** list, an inventory mini-scan file is created using the inventory data that is queried from the Intel AMT device at this time. This .scn file saved in the ManagementSuite\LDScans directory where it is consumed by the inventory service. Once consumed, the inventory service removes the computer from the unmanaged device discovery tables and inserts the data into the main LANDesk database tables. Information about the newly managed Intel AMT device can be found in either the **Intel AMT Summary** page or by viewing the **Inventory** and expanding the **AMT\_Info** table.

In addition, a couple of Intel AMT configuration functions are called at this time, like the registration of all ASF alerts to be sent to the core. Because multiple Intel AMT devices may be moved at the same time, and the process can take more than a few seconds for each device, this operation is done in a separate process to avoid tying up the LANDesk product console.

At this time a copy of the encrypted Intel AMT credentials, found in the **Intel AMT Configuration** page of the Configure Services utility, is saved into the database. This is done to allow each Intel AMT device to have a unique and independently managed set of credentials.

Some Intel AMT features do not require LANDesk agents to be installed, and can operate in what is called out-of-band (OOB) mode. Sometimes “out-of-band” means no agents are installed and sometimes it means the device is powered off but still plugged in. For these features, OOB has both meanings.

LSM and LDSM use a Web console for their interface. Most of the Intel AMT features in these two products can be found by either double-clicking the device (which brings up the Server information console and shows the Intel AMT summary and boot options) or by clicking **Hardware Configuration** in the left navigation pane (which contains most of the Intel AMT-specific features). If you are using the LDMS Win32 console, some features are accessed by right-clicking an Intel AMT device in the **My devices** list and selecting options from the context menu. You can also switch to the LDSM or LSM console that you have installed to use these features.

## Intel AMT inventory summary

The inventory summary is a display of a subset of the inventory information queried from the Intel AMT device, such as the device manufacturer, BIOS version and date, and the Intel AMT version. When you open the **Inventory summary** window, the data is queried real-time from the device, not read from the database, so the dialog may take a moment to display.

A good method to determine whether a device is configured in TLS or non-TLS mode is to open the inventory summary and verify the protocol type – HTTP for non-TLS mode and HTTPS for TLS mode.

To open the inventory summary, double-click the device in the **My devices** list, then click **System information | AMT | Intel AMT options**.

## Updating the Intel AMT inventory

In LSM and LDSM you can manually update the Intel AMT inventory data that is stored in the database. To do this, double-click the device in the **My devices** list, then click **System information | AMT | Intel AMT options | Update inventory**. (In the LDMS Win32 console you can select multiple devices and update all of their inventories at the same time.)

If you install the LANDesk agent on a device and the IP address of the device changes (for example, because DHCP gave it a new address or the device was moved to a different subnet), the Inventory scanner will automatically update the IP address in the database on the next inventory scan. However, if you do not have the agent installed, the only way to update the IP address in the database is to run this Update Inventory operation.

## Intel AMT event log (step 17)

The Intel AMT event log is a log that is maintained and stored on the Intel AMT device by Intel AMT. The events it records are independent of and do not necessarily correspond to the ASF events sent from the device. LANDesk products record all Intel AMT ASF events in the Alert log, but it does not query the Intel AMT event log and retrieve those events to put in the Alert log. The only way to view the Intel AMT log events is to open the **Intel AMT Log** page, or to view it in the Intel AMT Web console.

To view the **Intel AMT log** page, double-click the device in the **My devices** list, then click **System information | Logs | Intel AMT log**.

The log can be cleared, refreshed, and exported to a CSV file.

## Power options (step 18)

You can send various power option commands to managed Intel AMT devices. They are grouped under **Power options** in the Server information console (double-click the device in the **My devices** list, then click **Power options**).

Various boot options may be used together. For example, you can do a reboot and enable Serial-over-LAN (SOL) and IDE-Redirection together. Or you can send a power-on command, start SOL, and then enter the BIOS.

## SOL

Serial-over-LAN (SOL) is a technology that can pass text output data over the network to be displayed on a remote computer. It allows an admin to remotely view and control the boot process of the Intel AMT device up to the point of a non-DOS based OS starting – for example, you can view system boot messages, BIOS access, or DOS.

SOL only passes through text-based data, not true graphics. While in DOS, various applications can be viewed as long as they output text data.

LANDesk uses its regular remote control (RC) viewer for Intel AMT SOL. When an SOL boot request is made from the console, the RC viewer is launched. The viewer communicates with a service on the LANDesk core server through which all the SOL data is routed through from the Intel AMT device to the RC viewer. The service opens the SOL session with the AMT device.

The session is closed when either the viewer is closed or Windows starts up. If the LANDesk agents are installed, including the Remote Control agent, then when the Intel AMT device boots into Windows, the Remote Control viewer will automatically start remote controlling the OS. If the agents are not installed or if you have no wish to continue remote controlling the device, close the Remote Control window. Also if you plan to re-attempt a new SOL session on the same device, you should still close the SOL viewer.

## IDE-R boot options

IDE-Redirection (IDE-R) is a technology that allows the Intel AMT device to redirect its disk IDE interface to boot from bootable media on a LANDesk core server instead of its local hard drive. The connection can be redirected to a physical floppy or CD drive or it can point to a bootable floppy or CD image file.

This is accomplished by initially setting up an IDE-R session via Intel AMT. This session allows the two devices to stay connected while the Intel AMT device is rebooted, in addition to transmitting the data. LANDesk software only initiates the session – it does not manually send any of the IDE-R data; that is handled by the Intel AMT SDK code that is linked into LANDesk software and the Intel AMT firmware and BIOS on the remote Intel AMT device.

When LANDesk management software opens the session, it gives Intel AMT the paths to the CD and floppy media. These paths may be drive letters that have a bootable CD or floppy in them, or they may be paths to image files that are .ISO files of bootable CDs and/or .IMG files of bootable floppies. After the session is opened an Intel AMT boot or reboot command is sent to the Intel AMT device, and this command tells it whether to boot from the CD or floppy image.

An Intel AMT device can have only one IDE-R session open to it at one time, but the console can have IDE-R sessions open to multiple Intel AMT devices at the same time.

In setting up IDE-R, the admin can select whether to boot from a floppy or CD. Although this selection can obviously only be one or the other, we have seen some Intel AMT devices require the user to provide both floppy *and* CD media. Even if you never plan to use a floppy for IDE-R booting, a floppy drive or image file is required. This requirement is based on the fact that we provide the boot media info when setting up the IDE-R session before and independent of issuing an Intel AMT command to reboot and boot to the CD or floppy drive. Even though the user knows what option they are selecting before the session is created, Intel AMT doesn't.

Because IDE-R only works when booting up an Intel AMT device, the media should be bootable media, otherwise nothing will happen and the Intel AMT device will instead boot up to its local OS.

Floppy image files must be in .img format. CD image files must be in .iso format. There are numerous shareware applications out on the web for converting your boot disks to these and other formats.

At this time Intel AMT is not able to redirect the IDE connection from the Intel AMT device to a image on the remote networked drive. The media must be local to the Win32 console if using the Win32 console, or local to the LANDesk core server if using the Web console (because the Web console's back-end code is actually running on the core server).

In order to provide a more simple experience to the customer, LANDesk management software doesn't expose the concept of the IDE-R session. When an IDE-R boot is issued and we create the session, neither Intel AMT nor LANDesk knows when the user finishes the task they are doing with IDE-R, so the session is kept open for six hours, at which point it is automatically closed. This period of time should be adequate for operations typically performed, such as re-imaging a device or installing an OS.

## Other reboot options

The reboot options on the **Power options** page are described below.

**Enter BIOS setup on power on:** This option forces Intel AMT to go into the BIOS setup when the device boots. This option is useful if you want to go into the BIOS setup but the hotkey is unknown or does not work, or if the bootup is so fast you can't press the hotkey in time.

**Show console redirection window:** Check this box to enable SOL and open a console window that displays the device's boot process.

**Normal Boot:** This option boots the device normally.

**Boot from local CD/DVD drive:** This option overrides whatever the boot order is as defined in the BIOS and tries to boot the device to the local CD first. If there is no bootable CD or DVD then it boots up the local OS.

**Boot from local hard drive:** This option overrides whatever the boot order is as defined in the BIOS and tries to boot the device to the local primary hard disk first.

**PXE boot:** If the Intel AMT device has PXE booting enabled in the BIOS, this option forces the device to try PXE booting first. If it is unable to find a PXE server to boot from, it boots up the local OS.

**IDE-R options:** Select **IDER boot** from the boot method list, then select the source of the boot media and specify the location of the media.

## Multi-device boot options

While some of the Intel AMT boot options don't lend themselves to multi-device operations, such as SOL and IDE-R, the normal power off, power on, and reboot commands do. In the LSM and LDSM consoles (and the LDMS Web console), these power commands can be found as a group options tab in the lower pane. After all the devices you want to perform the operation on have been selected or targeted, then select the **Power options** section and chose which command to execute.

In the LDMS Win32 console, there are now three additional right-click menu options for these three commands. Because the Win32 console currently does not let you access sub-menus if multiple devices are selected, that's why they are not sub-items of the Intel AMT options sub-menu.

## Changing Intel AMT credentials for managed devices (steps 19-20)

Most IT shops have policies of changing passwords on a regular basis. To allow the administrator to change the Intel AMT password on all of the managed Intel AMT devices, there is a common page in the LANDesk console at **Hardware configuration | AMT | Provisioning | Configuration**. You can target all of the Intel AMT devices you want updated and set a new username and password for them. This password must be a strong password. When you do this, the credentials are changed in both the database and on the Intel AMT devices.

To change the username and password on a single device, there is an equivalent page in the Server information console that you can use to change the credentials for that specific device. Double-click the device in the **My devices** list, then click **Hardware configuration | AMT | Provisioning | Configuration**.

If at some point the credentials are changed in Configure Services, then Intel AMT operations will still work for all managed devices because the credentials are saved per device.

Remember that only the Intel AMT credentials have a programmatic method to change them, but the ME credentials do not. The only way to change the ME credentials is by entering the ME BIOS on each device. If the ME credentials are forgotten, the only way to enter the ME or AMT BIOS again is to reflash the BIOS and firmware.

## System Defense (step 21)

System Defense is a technology that allows the LANDesk management console to configure policies on an Intel AMT device that will filter, identify, and control certain types of network packets being transmitted or received. These policies describe network traffic that could be a possible virus or worm attack.

The following steps describe the System Defense process for controlling network traffic:

1. The management console calls the System Defense (SD) configuration utility to configure an Intel AMT device with a SD policy.
2. An external attack occurs – a virus, worm or other attack vector that matches one of the filters in the current policy.
3. An SD filter is triggered, causing the Intel AMT SD hardware to transmit an alert to the console informing it of the attack.
4. The management console accepts the alert and requests the filter name from the corresponding Intel AMT device. With the alert information an alert handler is called to adjust the SD policy, terminating most network communications to and from the Intel AMT device. All adjustments done to an Intel AMT device are done through the System Defense configuration utility.

5. After the issue has been resolved, the System Defense configuration utility called by the console restores network connectivity by restoring the original policy on the AMT node.

All System Defense filters fall into one of five types of filters: Statistics Pass, Statistics Drop, Rate Limit, Pass and Drop.

- A statistics filter counts all of the packets that match the filter and either permit them to pass through or be dropped by System Defense. Statistics filters are used to gather information and could be used to do a post mortem on an attack.
- A rate limit filter only allows so many packets per minute. Once the limit has been reached no other packets matching the filter will be permitted to pass. This type of filter is used to stop packet flood attacks. The LANDesk UDP flood and Block FTP policies are examples of this type filter.
- A pass filter allows all packets matching the filter to pass through. This type of filter allows packets that match the filter to pass through when the default transmit/receive filters are true. This type of filter is used by the kill all NICs policy. This policy is used to allow the LANDesk, DHCP and DNS ports to be open while all other network traffic is dropped.
- A drop filter allows all packets matching the filter to pass through. This type of filter allows packets that match the filter to pass through when the default transmit/receive filters are false.

SD filters have three possible actions that can be taken when they are triggered:

- Drop the matching packet
- Rate limit the matching packets, and once the threshold has been met, drop all subsequent matching packets
- Send an alert to the management console, allowing the console to decide what is to be done (all LANDesk filters send an alert)

The System Defense technology is capable of filtering denial of service attacks, internet worms and viruses that attack ports in a very consistent manner. System administrators may find that System Defense may allow them to control some forms of undesirable Internet user behavior by blocking certain ports.

System Defense does not require any agents to be installed on the Intel AMT device. System Defense policies may be configured on a per-device basis. To define System Defense policies and apply them to targeted Intel AMT devices, open the LSM console and click **Hardware configuration**. In the console that opens, click **AMT | System Defense | Policies**.

There are four pre-defined System Defense policies in LANDesk products:

- An FTP access policy which will trip SD if an FTP access is made either to or from the Intel AMT device.
- A UDP flood policy which will trip SD if Intel AMT sees at least 20000 UDP packets per minute and is supposed to monitor for a denial-of-service attack.
- An SYN flood policy which will trip SD if Intel AMT sees at least 20000 IP packets per minute and is supposed to monitor for a denial-of-service attack.
- A Kill All NICs policy which will immediately trip SD.

In LANDesk 8.70 products there is no interface to create or modify System Defense filters or policies. We are investigating additional functionality for the System Defense features to be delivered at a later date.

Once System Defense filter is tripped, an alert will show up in the Alert log. The LANDesk product, through Intel AMT features, limits network access by applying the Kill All Nics policy when System Defense trips. The device is also placed in the Remediation queue, which is found in **Hardware configuration | AMT | System Defense | Remediation**. When the device is remediated, then the Kill All NICs policy is removed and the previous policy is applied. It is up to the administrator to manually do the actual remediation of removing the virus or spyware, or fixing whatever else was the cause of the System Defense trip, using whatever tools they want to use, including LANDesk® Remote Control, LANDesk® Virus Protect, LANDesk® Vulnerability Scanner, and so on.

The Kill All NICs policy drops all packets except for DNS, DHCP, LANDesk, and Intel AMT communication.

## Agent Presence (step 22)

Agent Presence provides a method to monitor on Intel AMT devices whether an application is running or not at the hardware level. What this technology provides that other application monitoring programs don't is the security that the user can't stop or kill the application monitoring program itself and thereby get around restrictions or avoid detection.

Installing a LANDesk agent on the managed device is required for Agent Presence to work. During the agent install, a program on the core configures the Intel AMT device with the applications it should monitor and how often they should send a heartbeat to Intel AMT. Once the agent is installed it registers with Intel AMT and starts sending heartbeats. Because the agent is notifying the local Intel AMT system, these heartbeats do not generate network traffic.

There are two time values associated with Agent Presence. One is the startup time, which is the delay between the OS starting up and the agent sending the first heartbeat. This delay allows enough time for the OS and applications to start without generating false alerts. The second value is the time to allow between heartbeats. If Intel AMT fails to get a heartbeat after this period of time, it generates an ASF alert notifying the core server.

LANDesk has extended Agent Presence so that the LANDesk agent can monitor other applications as well as itself. The single agent sends distinct heartbeats for each of the applications it is monitoring. In version 8.70 products, LANDesk provides monitoring of three pre-defined applications. These other applications are required LANDesk agents for monitoring all other services provided by the LANDesk service monitoring feature.

The agent gets its list of applications from an XML file stored in the Intel AMT non-volatile memory storage area, where a program on the core stores it and updates it if any changes are made. It is kept in this storage area so that it can be updated even if the device is turned off.

Agent Presence is configured automatically when LANDesk agents are installed. However, to select additional configuration options, open the LSM console and click **Hardware Configuration**. In the console that opens, click **AMT | Agent Presence | Configuration**.

Agent Presence is an all or nothing feature. It is either on for all managed Intel AMT devices or off for all devices, and is controlled by the **Enable Agent Presence monitoring** check-box.

By default Agent Presence monitors three processes on the managed device. They are the Agent Presence agent itself (LDAMT.EXE), the LANDesk Management Agent (RESIDENTAGENT.EXE), and the LANDesk Monitoring Service (COLLECTOR.EXE). The reason the LANDesk Management Agent is monitored is because much of the Client/Server communication between LANDesk agents and the LANDesk core server is through this application. The reason the LANDesk Monitoring Service is monitored is because it is the heart of the LANDesk monitoring system, which include monitoring service; so if these applications are running then you can monitor any other service on the device using the LANDesk service monitoring tool. These applications and descriptions are defined in AGENTPRESENCE.XML which is sent down to the Intel AMT non-volatile memory storage area on the Intel AMT device, and which is subsequently read by the LANDesk agent to determine what it should monitor.

The startup time is the time between the bootup of Windows and commencement of Agent Presence monitoring. The default value is six minutes. The Heartbeat value is the time Intel AMT expects between heartbeats. The default value is two minutes.

One step in verifying Agent Presence is working correctly on the device is to open the Windows Task Manager and make sure LDAMT.EXE is running.

Once the startup time has passed, then the way to generate an Agent Presence alert is to either kill the COLLECTOR.EXE process or stop the LANDesk Management Agent service. If the COLLECTOR.EXE process is killed, the way to start it up again is to run RESTARTMON.EXE which is located in the LDCLIENT folder on the client.

You should see Agent Presence start and stop alerts in the LANDesk Alert log (not the AMT Event Log).

## LANDesk Out-of-band monitor (AMTMON) features


Starting with version 8.6.0, LANDesk products have the ability to disable the network at the OS level on Intel AMT devices. This was not done through the Intel AMT System Defense feature, but rather it was done through LANDesk agents and communicating via the Intel AMT non-volatile memory (NVM) area. When the user chooses to disable the network, a value is written to a location in the NVM that a service called LANDesk Out-of-band Monitor (AMTMON.EXE) on the client is monitoring. If the service sees the flag to disable the network, it does so. If it sees the flag to enable the network, it does that. And if it sees the flag to run the vulnerability scan on the next reboot, it sets that up. A message box pops up on the managed device notifying the user when any of the three operations is performed.

To use these monitoring features, double-click the device in the **My devices** list, then click **System information | AMT | Intel AMT options**. Under **Configuration options**, click **Enable**, **Disable**, or **Scan**.

Note: Do not ping the Intel AMT device to test if the network is disabled, as Intel AMT may still respond to pings.

## Tips

---

- Intel® AMT will not work through a proxy server. Make sure there is no proxy configured on the managed device in **Internet Explorer | Tools | Internet Options | Connections | LAN Settings | Proxy Server**.
- Get the latest BIOS and firmware from your manufacturer's or Intel's web site.
- The Alpha and Beta Intel AMT release 2.0 devices have many known issues – too many to list here. If something doesn't work as expected there's an equal chance the problem is a platform, LANDesk® software, or user error. Because the final Intel AMT SDK was not available until after the 8.70 LANDesk products were released, LANDesk will be releasing patches built from that SDK with whatever issues we may have found. Final BIOS's will also not be available until August **[IS AUGUST CORRECT?]**. Please have patience and report any issues to the proper authorities, but realize everything will not be perfect.
- LANDesk 8.70 does not support configuring the PID/PPS on an Intel AMT device via a USB drive.
- It is strongly recommended to not use static IP addresses on the Intel AMT device unless you know exactly what the issues are and know what you are doing. See "Tips for using static IP addresses" later in this section for more information.
- The Intel AMT Web Console can be accessed by either "http://<machine name or IP address>:16992" for non-TLS mode devices, or "https://<machine name or IP address>:16993" for TLS mode devices.
- Intel AMT devices in Enterprise mode do not enable the Intel AMT Web Console until it is successfully configured.
- Serial-over-LAN (SOL) is a technology that only supports text data – true graphical data will not pass through nor be shown in the SOL viewer.
- Unless you have a copy of the certificate that was used to initially configure an Intel AMT device in TLS mode, LANDesk will be unable to talk to the device until it is fully un-provisioned. Because of this, it is highly recommended you always un-provision an Intel AMT device before using it with any LANDesk product for the first time.
- To reset the Intel AMT password on a Cortez or Tappen device because you've forgotten it or don't know it for some reason:
  1. Move jumper J6F1 to pins 2-3. This is located near the large power connector, right next to the piezo speaker.
  2. Short the manufacturing jumper with a metal object. It looks like two flat metal rectangles next to two holes on the motherboard.
  3. While shorted, reboot the device. It should come up in Maintenance Mode, and automatically boot to the BIOS.
  4. Select "Reset AMT Defaults" and press Enter. It may take a minute or so to finish resetting.

5. Press F10 to exit the BIOS and save changes, and it will tell you to power off the device.
  6. After powering off, remove the short and put the jumper back to pins 1-2.
  7. Boot back up, enter the Intel AMT BIOS, and the password should now be reset back to admin.
- The default Domain field in the HP Intel AMT BIOS is "intel.com". It is recommended to change this to your working domain or delete it if you are not using a domain.
  - Many Beta Intel AMT release 2.0 devices have identical Intel AMT GUIDs. LANDesk **management software** uses the GUID to uniquely identify the device in the database. After one device is successfully managed and then a second device with an identical GUID is moved, the Inventory service thinks that that device is already in the database, so a new record is not created. We use the GUID because the machine name and IP address can be easily changed.
  - If you did manage multiple devices with the same GUID, it is recommended that you reset your database. In the ManagementSuite directory on the core server, run CoreDBUtil.exe, and click the **Reset** button. Reset will delete all of the data in the database and rebuilds the tables. The **Build** button rebuilds tables, but does not delete existing data. After resetting, you need to re-activate the core and re-enter the Intel AMT credentials using the Configure Services utility.
  - During the installation of the LANDesk agents, you may see a Windows exception caused by the AMT Configuration Helper. This is caused by the core server changing addresses since the time the LANDesk product was installed – most likely because the core server was installed while connected on one network, and then the server was moved somewhere else where it connects to a different network and changes addresses. In a corporate environment, the core server is a *server class device* and is expected to have a static IP address. To work around this problem, edit the ServerConfig.ini and DefaultServer.ini files. (Or edit a custom .ini file if you have created a custom client configuration setting.) Change the core IP addresses located on several different lines (search for the address in the file), and replace with the new IP address. Do not replace the IP address with the core server name. Uninstall the agents by mapping a drive from the client to the core server and attach to the LDMAIN share (the ManagementSuite directory), then run UninstallWinClient.exe. There are no dialogs, but you can see it running in Task Manager. After a few minutes the device will automatically reboot. Re-run the client configuration.
  - The link to the LANDesk Support Knowledge Base article where Intel AMT patches for the 8.7 products can be downloaded is:  
<http://kb.landesk.com/display/4/kb/article.asp?aid=3550>

## Tips for Intel® UPSD Desktop Q965 Express motherboard-based systems

Intel UPSD manufactures the Intel® Desktop Q965 Express motherboard which is the Intel® vPro™ platform that contains support for Intel AMT release 2.0. On systems based on this motherboard, the BIOS is uniquely different from BIOS's or platforms from other vendors.

First, the ME and AMT BIOS screens are integrated into the main UPSD BIOS screens as opposed to accessing them separately via Ctrl+P.

Second, there is no “Un-provision” command located in the UPSD BIOS. To un-provision the device, you have to turn it off, unplug it, change a jumper from pins 1 and 2 to pins 2 and 3 (a yellowish jumper located near the rear USB ports on the devices LANDesk has, it may be different on different models), boot the device, and now located on the first page of the BIOS is an option to reset the Intel AMT settings. After choosing this, the device may flicker once after a second or so, and now you should exit the BIOS and then power down the device, unplug it, set the jumper back, and power it back on.

Third, after making changes in the Intel ME, you must select the **Save and Continue** menu option located in the UPSD BIOS to save the settings. Pressing **F10** to exit and save the BIOS settings will *not* save the Intel AMT settings.

## Tips for using static IP addresses

Because Intel AMT devices have two components that are assigned an IP address – the Intel AMT chip and the device’s operating system – you can potentially have two entries in your list of discovered devices for the same Intel AMT device. This happens only if you want to use a static IP address rather than using DHCP.

To use static IP addresses with Intel AMT devices, the Intel AMT firmware should be configured with its own MAC address. The Intel AMT R1.0 Aspenhill board is the only one that ships with this second MAC address already configured. For instructions on how to re-install the firmware and configure it properly, please contact Intel.

Once configured, the Intel AMT device will have a different MAC address, IP address, and host name than the device OS. To be able to manage Intel AMT devices correctly, you need to use the following settings for DHCP and static IP addresses:

- DHCP: Both the OS and Intel AMT use DHCP and the host names are the same.
- Static IP: Both the OS and Intel AMT are set to use static addresses and they are different from each other, the MAC addresses are different, and the host names are also different.

If an Intel AMT R2.0 machine is put in Enterprise mode, the only way to talk to it is via the “hello” packet being sent to the setup and configuration server. After the machine is managed by LANDesk software, Intel AMT operations may be performed on it like normal. What you should *not* do is discover and manage the OS IP address; otherwise you will have two computer entries that represent the same computer. Because the only common identifier between the two devices is the AMT GUID, and because the AMT GUID can not be found remotely for the OS device, the two entries cannot be merged.

If you want to install the LANDesk agents, you cannot push the agents, because the only IP address in the database is the Intel AMT IP address, and the push utility needs access to the OS. So the agents need to be pulled (from the managed Intel AMT device) by mapping a drive to LDLOGON on the core server and running ServerConfig.exe.

Before pulling the agents, we recommend changing a setting in the Configure Services utility. Click **Start | All Programs | LANDesk | LANDesk Configure Services**. On the **Inventory** tab, click **Device IDs** to manage duplicate records. In the **Attributes List**, scroll about half way down and move the **AMT GUID** attribute to the **Identity Attributes** list. This will force the AMT GUID to be one of the attributes that can uniquely identify a computer.

Now when the Inventory scan from the managed Intel AMT device is imported into the database, the Inventory service matches the Intel AMT GUID from the device that's already in the database with the OS information in the scan file.

## Log file troubleshooting tips

The log files created by LANDesk products will not likely help the casual user of LANDesk management products. They are intended as a help to developers in determining where problems are occurring. The following log files are useful to help debug issues and may be requested by Support or Development team members.

**AMTConfigDll.Log.** This is the primary LANDesk AMT log file and can be found in either Windows\Temp or Documents and Settings\<logged-in user>\Local Settings\Temp. If a service or the Win32 console logged the data, then it will be in the Windows\Temp file. If a Web service or the Web console logged the data, then it will put in Documents and Settings file. The reason the file is in the temp directory is because the code is common between all contexts, and that directory is accessible to the Web services and all other contexts.

**AMTProvMgr.Log.** This log is the Intel AMT release 1.0 provisioning program's log and is found in the ManagementSuite directory. If a device fails to move to the LANDesk database, then this log may help determine the source of the problem.

**AMTProvMgr2.Log.** This log is the Intel AMT release 2.0 provisioning program's log and is found in the ManagementSuite\AMTProv directory. If a device fails to show up in the UDD table after the "Hello" packet should have been sent, then this log could be useful in determining where a problem has occurred.

**AMTDiscService.Log.** This log is from the service that listens for "Hello" packets and is found in the ManagementSuite directory. If a device fails to show up in the UDD table after the "Hello" packet should have been sent, then this log could help find the source of the problem.

**IPMIRedirectionService.Log.** This log is from the SOL redirection service and is found in the ManagementSuite directory. Despite the name it is also used for Intel AMT and routes all display data from the Remote Control viewer to and from AMT. We have had trouble with this service crashing, so if you are unable to perform an SOL operation, especially if you get an error in the RC console that it's not able to talk to the core, then make sure this service is running. The service name is LANDesk® Console Redirection Service.

**Console.exe.Log.** This log is from the Win32 console. If some AMT operation fails that was executed from the Win32 console, then there is a small chance the data in this log would be helpful in figuring out the problem.

**Amtmon.Log.** This log file is found on the AMT client in the LANDesk\LDClient directory. It contains a good indicator of whether the LANDesk AMT agents can talk to the non-volatile memory area.

**AmtSessionMgrSvc.Log.** This log file is generated by the program that manages all of the IDE-R sessions, and indicates what drives or image files were selected among other things.

**AmtSessionMgr.Log.** This log file is generated by the program that sends IDE-R information to the AmtSessionMgrSvc.Log

## System Defense logs

The following four logs are for help in debugging System Defense problems. The CBConfig.log, CBState.log, and CBAlerHandler.logs are created after adding the following registry values:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\LANDesk\ManagementSuite\CircuitBreaker]
"CBParseLog"=dword:00000003
"CBLog"=dword:00000003
```

**CBConfig.Log.** This log file is generated when a System Defense policy is applied to an Intel AMT R2.0 machine.

**CBState.Log.** This log file is generated when a System Defense alert is received from an Intel AMT R2.0 machine and gives information about the System Defense state.

**CBAlerHandler.Log.** This log file is generated when a System Defense alert is received from an Intel AMT R2.0 machine and provides information about the alert and how it was handled. For example, a log entry is added when the KillAllINics policy is successfully applied.

**AlertService.Log.** This log file is generated by the service that processes the LANDesk alerts.

## Known issues

The following are known issues with managing Intel® AMT devices, with workarounds and fixes (if available).

Issue	Workaround	Fix
<b>LANDesk® product issues</b>		
If the Intel AMT device is put into Small-Business mode and the communication type is left as TLS in Configure Services, LANDesk management software will fail to talk to the device. Once the device has been managed incorrectly, there is no way to correctly manage it in non-TLS mode until you reinstall the product or apply the patch.	Either put the Intel AMT device in Enterprise mode and select TLS, or put the device in Small-Business mode and select non-TLS in the Configure Services tool.	Patch available upon request.
On a Japanese core server, the Remote Control window immediately closes after doing a SOL boot of an Intel AMT device.	None.	Patch available upon request.
After doing an SOL boot of an Intel AMT device that has the LANDesk agents installed, and the device boots into Windows®, the Remote Control console brings up a dialog to enter your credentials rather than just automatically remote controlling Windows.	None.	Patch available upon request.
In the Web Console, after clicking Update Inventory on the Intel AMT Summary page, the inventory data disappears. Also the link to the Intel AMT Web console on that page also now fails to connect properly, and the AMT Boot Options page now fails to get the current boot state of the Intel AMT device.	None.	Patch available upon request.
When doing a SOL boot, the LANDesk® Remote Control viewer displays the error "Communication to the core failed". This usually happens because the LANDesk®Console Redirection Service crashed.	Restart the LANDesk Console Redirection Service.	None.
The SOL viewer does not pop up after issuing a SOL boot. The most likely cause was the AMT RemoteControl() call had an exception, which caused the LANDesk code to not launch the SOL viewer.	None.	Patch available upon request.
IDE-R fails to work. One of the problems is an old IMRSDK.DLL.	None.	Update to the AMT R2.0 Gold SDK version of IMRSDK.DLL.

Issue	Workaround	Fix
<p>When a System Defense filter trips the event is logged in the Intel AMT Event Log, but not in the LANDesk Event log, and the device is not "circuit broken." If you check the LANDesk@System Manager SNMP Message Relay Service, it is stopped. This problem appears to occur randomly.</p>	<p>None. Restarting the service will not fix it. The service is crashing when it receives the alert.</p>	<p>Patch available upon request.</p>
<p>Agent Presence is sometimes not automatically configured when the LANDesk agents are installed.</p>	<p>Go to the Agent Presence configuration page and click <b>Apply</b> after installing the agents.</p>	<p>None.</p>
<p>Sometimes the Agent Presence agent is not installed when the LANDesk agents are installed via WSCFG32.EXE rather than ServerConfig.exe.</p>	<p>Uninstall the agents by running UninstallWinClient.exe and reinstall using ServerConfig.exe.</p>	<p>Patch available upon request.</p>
<p>When using static IP addresses, either you ended up with two separate computer entries for the same computer – one with the OS information and one with the Intel AMT information – or there is one entry, but the Intel AMT features do not work.  (For information about using static IP addresses with Intel AMT devices, see "Tips for using static IP addresses" in the Tips section of this document.)</p>	<p>None.</p>	<p>Patch available upon request. Also, for this to work you must discover and manage the Intel AMT device and then pull the agents to it (map a drive and run ServerConfig.exe). If you discover and manage the OS "machine," then you will have two separate entries in the database, and you can't push the agents to the Intel AMT device because the Intel AMT IP and Hostname are not recognized by the client OS.</p>
<p>The feature to change the Intel AMT credentials does not work, either from the Server information console (for single devices) or from the console's Hardware configuration page (for multiple devices) – it may change the credentials on the Intel AMT device, but it will cause most of the Intel AMT functionality to stop working. This is caused by the database not being updated.</p>	<p>None.</p>	<p>Patch available upon request.</p>
<p>After a device is dropped off the network by the System Defense feature, some LANDesk tools that could be used to remediate the problem are not able to work, such as the Windows agent-based Remote Control.</p>	<p>None.</p>	<p>Patch available upon request.</p>

Issue	Workaround	Fix
If you choose to use the DNS "ProvisioningServer" entry method of identifying the setup and configuration server, you must still enter the port number 9971 in the AMT BIOS.	None.	Patch available upon request to let the user specify any port number to listen on by setting a Windows registry value. Note: While LANDesk previously used port 9982, beginning with version 8.71 port 9971 is used for the setup and configuration server.
Sometimes the Web console is unable to retrieve the power status of the Intel AMT device and all of the power options are grayed out.	If the problem is because of this defect, none.	Patch available upon request.
In the Web console, on the Power Options page in the Server Info view, the Refresh button fails to refresh the page.	Click <b>Power options</b> in the left-hand menu.	Patch available upon request.
After managing an Intel AMT device, the LANDesk alert log fills up with "Presence Heartbeat Restored (ASF)" events.	None.	Patch available upon request.
When issuing a SOL boot via the Web console, the SOL console can be too slow to open and it may miss displaying the BIOS post information.	None.	Patch available upon request.
Some devices do not support the Boot to BIOS option. If this is selected and the machine does not support it, the device is not rebooted and the administrator is not notified of the reason it failed.	Clear the Boot to BIOS boot option, select the SOL option and press the correct keystrokes to enter the BIOS as the BIOS is booting up.	None.
Black rectangles randomly show up in the Serial-over-LAN viewer when remote controlling the BIOS.	The black rectangles rarely seriously impede the ability to view and change settings in the BIOS.	None.
<b>Issues – Currently under investigation</b>		
After doing an IDE-R boot of an Intel AMT device, the AMTSessionMgrSvc.exe may experience a Buffer Overflow after six hours.	None.	None.
When doing a SOL boot, the LANDesk Remote Control viewer displays the error "The remote computer does not support console redirection". We see this occasionally and do not know the cause.	Retry.	None.
Sometimes the software-based System Defense feature does not work.	None.	None.
When viewing the AMT Event log, the string for Agent Presence alerts is incorrect.	None.	None.

Issue	Workaround	Fix
<p>When a device in the System Defense remediation queue is remediated, no alert is generated. This was not implemented.</p>	<p>None.</p>	<p>None.</p>
<p>When doing an IDE-R boot, the Intel AMT release 2.0 device displays the error: "Reboot and Select proper Boot device or Insert Boot Media in selected Boot device and press a key". We do not know why this error shows up.</p>	<p>There are two possible fixes for this problem: (1) Apply a new LANDesk patch that changes one of the flags being passed to Intel AMT when creating the IDE-R session. (2) Change the location of the boot image file if you are using an image file rather than a physical CD or floppy. Try putting the file in the root of the hard drive; if that works, try various locations to see which ones work. The issue may be related to directory rights access when issuing the IDE-R from the Web console.</p>	<p>A patch has been release that may resolve the issue.</p>

## Appendix: Previous versions of Intel® AMT and LANDesk® products

---

This section contains information about the differences in managing Intel® AMT release 1.0 devices, as well as information about differences in using LANDesk® version 8.6.x products. Intel AMT release 1.0 devices were built in 2005/06 with Intel's 945G chipset.

Devices with Intel AMT release 1.0 can be managed with versions 8.6.x and 8.70 of LANDesk® Management Suite (LDMS), LANDesk® Server Manager (LDSM), and LANDesk® System Manager (LSM).

If you are using Intel AMT release 1.0 devices we recommend that you get the latest BIOS and firmware from your OEM's or Intel's web site. There have been numerous and important fixes made compared to the BIOS shipped with most devices. The latest BIOS for Intel UPSD AMT release 1.0 boards, as of July 19, 2006, is build 3943.

### Setting up, configuring, and managing Intel AMT release 1.0 devices

The following is an overview of the process for setting up, configuring, and managing devices with Intel AMT release 1.0. These instructions are written for users of LANDesk System Manager 8.70. The procedure is the same for LANDesk Server Manager. Most steps are similar for LANDesk Management Suite, although there are differences when using the Win32 console to manage devices.

#### Configuring and discovering the device

1. Install the LANDesk software. Activate the core server by running the Core Server Activation utility (**Start | All Programs | LANDesk | LANDesk Core Server Activation**).
2. At the LANDesk System Manager console, open the Configure Services Utility (**Start | All Programs | LANDesk | Configure Services**). Click the **Intel AMT Configuration** tab. Under **Current Intel AMT Credentials**, enter the AMT username and password you will be using when you configure the new Intel AMT devices in the AMT BIOS. If you want to use a different set of credentials to access the device after configuration, enter a username and password under **Provision with new Intel AMT Credentials**. Click **Provision in TLS mode** or **Provision in non-TLS mode** depending on the security mode you want to use, then click **OK**.
3. On the Intel AMT device, start the AMT BIOS page and change the password to a strong password.
4. If the device has been previously managed or its previous state is unknown, then fully un-provision it.
5. Select **Enterprise** or **Small-business** mode.
6. With Intel AMT devices managed by LSM 8.70, you can enter the Provisioning Server information in the AMT BIOS to automatically discover the devices. If you want to use the Provisioning Server option, enter the IP address of the LSM core server and port 9971. (If you do not want to use the Provisioning

Server option, leave this information blank. You will need to complete step 8 below to discover the device.) (Note: the Provisioning Server option was not available in LANDesk 8.6.x products.)

7. Choose the **Save and Exit** option in the AMT BIOS.
8. If you did not use the Provisioning Server option described in step 6, complete this step. Open the LSM console and click **Device discovery** in the left navigation pane. In the lower pane, click the **Discovery configurations** tab and click **New**. Define a configuration, including the IP address of the Intel AMT device in the IP address range. Be sure to check **Discover Intel AMT 1.0 devices**. Click **OK**, then select the configuration and click **Schedule** on the **Discovery configurations** tab. Click **Schedule task | Start now | Save**. Depending on the number of devices in the IP address range you specified, discovery may take several minutes to complete.
9. When device discovery is complete, click the **Intel AMT** group in the top pane of the **Device discovery** page. Right-click the device and select **Target**. In the lower pane, click the **Manage** tab, select **Move targeted devices**, and click **Move**. The device is then moved from **Device discovery** to **My devices**.
10. To verify that the process worked, double-click the device in the **My devices** page (to open the Server information console for that device) and select the **AMT | Intel AMT options** page. You should see inventory data for the device.

## Installing agents on the device

At this point, the Intel AMT device can be managed with some, but not all, Intel AMT features. Other features require a LANDesk agent to be installed on the device. For Intel AMT devices, the amtmon.exe features (disabling the network, enabling the network, and scheduling a vulnerability scan on the next reboot) require a LANDesk agent.

11. The quickest and easiest way to install the LANDesk agent on a single managed device is to “pull” the agent. At the Intel AMT device, map a drive to the core server and attach to the **ldlogon** share. Run **wscfg32.exe** to install the LSM and LDMS agents, or run **ServerConfig.exe** to install the LDSM agents. Make sure Monitoring is selected in the agent configuration.

or

“Push” the LANDesk agent to one or more devices from the LANDesk console.

- a) If the credentials you are using on the console are different from those you use on the managed device, open the Configure Services utility (**Start | All Programs | LANDesk | Configure Services**). Click the **Scheduler** tab and click **Change Login**. Change the **Service Login** to the credentials for your LANDesk console, and add the credentials for the managed device to the **Alternate credentials** list. (This allows the scheduler to remotely log in on the managed devices to install the agent.)
- b) In the LANDesk console, click **My devices**. Select the Intel AMT devices you want to install the agent to and click **Target**.
- c) Click **Agent configuration** and select a standard Windows agent configuration. Or click **New** to create a new configuration with the agents that you want to install (Intel AMT is part of the Monitoring agent, which

must be included in any agent configuration installed on an Intel AMT device).

- d) With the configuration selected, click **Schedule task** on the toolbar. Click **Targeted devices | Add target list**, then click **Schedule task | Start now**. Click **Save**. The agent configuration package is built and installed on the managed device. It may take several minutes before there is any activity on the device as the package is built. You can watch the progress of the agent installation by clicking the **Configuration tasks** tab on the lower pane of the console. The Intel AMT device does not need to be rebooted after the agent package is installed.

## Managing devices

The following Intel AMT features can be accessed after you have configured, discovered, and installed agents on your Intel AMT device.

12. To view the Intel AMT event log, double-click the device in the **My devices** list, then click **System information | Logs | Intel AMT log**.
13. To select power options such as reboot, Serial-over-LAN and IDE-R options, double-click the Intel AMT device in the **My devices** page (this opens the Server information console for the device), then click **Power options** in the left navigation pane.
14. To change the Intel AMT credentials for one device, double-click that device in the **My devices** page, then click **Hardware configuration | AMT | Provisioning | Configuration**.

To change the Intel AMT credentials for multiple devices, open the LSM console and click **Hardware configuration | AMT | Provisioning | Configuration**.

## Notes on configuring Intel AMT release 1.0 devices

On Intel AMT release 1.0 devices, to turn on AMT functionality the user opens the AMT BIOS screen and changes the default **admin** password to a strong password.

**Host name:** Regardless of what name is entered in the Host name field in the AMT BIOS, as soon as Windows boots up, Intel AMT will sniff the wire and change the Intel AMT Host name to the Windows machine name if it is different.

**Security:** Intel recommends that you configure devices with Intel AMT release 1.0 only on a secure intranet. Intel AMT uses a non-TLS mode of communication until the certificate is created and the device is configured. Because secure communications can't be established until the certificate is installed on the Intel AMT device, the certificate is passed in-the-clear over the network when it is created. Thus it is not recommended to configure these devices except on a secure intranet.

**Power state:** Once the Intel AMT password has been set to a strong password in the AMT BIOS, the device may be discovered, managed, and operations performed on it, all while the device is powered off. This includes booting it up to a SOL/IDE-R session in order to install an OS on it for the first time.

## Notes on discovering Intel AMT release 1.0 devices

**Version 8.6.x:** In LANDesk version 8.6.x products, the only method of discovering any Intel AMT device is to use the LANDesk Unmanaged Device Discovery (UDD) tool and do

ping sweeps to discover and attempt to communicate via Intel AMT to each IP address. The option of discovering Intel AMT devices automatically with a setup and configuration server is not available in versions 8.6.x.

When an Intel AMT device is configured correctly and the credentials are entered in the Configure Services utility, run **Device discovery** from the console and Intel AMT devices are recognized as such. They are then added to the **Intel AMT** group in the **Discovered** devices page.

**Version 8.70:** With LANDesk 8.70 products, you can use the **Device discovery** tool to discover Intel AMT devices, or you can use an Intel AMT setup and configuration server to automatically discover the devices. To do this, add the IP address of the LANDesk core server (as the Provisioning Server), and specify port 9971, in the AMT BIOS page when setting up Intel AMT devices. This identifies the core server as the Intel AMT setup and configuration server on the network and allows that server to communicate with the device. The device, when configured correctly, sends a “hello” message to the setup and configuration server and is then discovered as an Intel AMT device.

## Known issues: Intel AMT release 1.0

Issue	Workaround	Fix
The LANDesk Inventory scanner fails to detect Lenovo™ Intel AMT release 1.0 devices as being Intel AMT devices.	None.	Patch available upon request.
IDE-R fails to boot to the remote image and boots into Windows.	Retry.	Update to BIOS 4861 or newer.

LANDesk 8.6.1 software has had a Service Pack release that contains several Intel AMT-related fixes. The Service Pack can be downloaded from: <http://kb.landesk.com/pf/12/webfiles/ServicePack/LD-861SP1.zip>. The Knowledgebase article about the Intel AMT patches is found here: <http://kb.landesk.com/article.asp?article=1954&p=5>

## Tips for Lenovo™ systems containing Intel® AMT release 1.0 features

- In order to configure Intel AMT TLS communications for Lenovo™ systems containing Intel® AMT release 1.0 features, you must manually connect to the Intel AMT web console and change the default password (which is “admin”) to a strong password. An Intel AMT strong password contains at least one lowercase and one uppercase letter, one number, and one special character, and the password must be at least 8 characters long.
- Lenovo systems containing Intel Intel AMT release 1.0 features do not support Serial-over-LAN.
- Lenovo systems containing Intel AMT release 1.0 features do not support IDE-R to a remote floppy device

## Tips for Intel® UPSD D945G motherboard-based systems

Intel UPSD manufactures the Intel® D945G motherboard which contains support for Intel AMT release 1.0. For these systems, make sure the “Wake on LAN from S5” option in the BIOS is set to “Power On”. If it is set to “Stay Off”, LANDesk will be unable to talk to the device while it is powered off and it will not be able to power it on or do IDE-R and SOL operations.