Intel® vPro™ Technology
Common-Use Guide
For Level Platforms Managed Workplace* 2012

Introduction

Common Uses for Level Platforms Managed Workplace* 2012 + Intel® vPro™ Technology

The Intel® Core™ vPro™ Processor Family extends the management capabilities of Level Platforms Managed Workplace 2012 to enable it to better discover, analyze, and monitor managed-service providers' (MSPs’) customer desktops, even when they are powered off. These extended remote management capabilities translate into lower overhead for MSPs as well as a higher service level agreement (SLA) that MSPs can offer their current and potential customers.

This paper illustrates how to use Level Platforms’ Managed Workplace remote management software with Intel vPro technology in several common scenarios. In doing so, this paper shows MSPs how to lower administrative overhead and increase the level of service they can offer their customers.
# Table of Contents

**Introduction**

Setup and Assumptions

Common Uses Covered in This Guide

**Use Case 1: Improved Device Discovery and Intel vPro Technology Status**

1.1: Initial and Ongoing Client System Inventory

1.2: Initial and Ongoing System Analysis

1.3: Alerts for Computers That Are Down or Missing from the Network

**Use Case 2: Optimization of Ongoing Maintenance and Management**

2.1: Routine Maintenance of Desktops: Install Patches and Software without a Desk Side Visit

2.2: BIOS Edit

**Use Case 3: Remote Diagnosis and Repair of Client Systems**

3.1: Use Remote Control to Troubleshoot a Problem

3.2: Remotely Diagnose a Problem Before an Onsite Visit

3.3: Remotely Restore an OS Image from a Hidden Partition

**Conclusion**

**Related Links**
Setup and Assumptions

<table>
<thead>
<tr>
<th>Software</th>
<th>Level Platforms Managed Workplace 2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware</td>
<td>Motherboard with Intel® Active Management Technology (Intel® AMT) ¹</td>
</tr>
</tbody>
</table>
| Basic Assumptions   | 1. You have configured the Intel AMT BIOS extensions of all client computer systems.  
2. You have installed Onsite Manager on an existing Windows Device at each customer site.  
3. You have installed the Service Center at your MSP site |

Common Uses Covered in This Guide

- Improved device discovery and Intel vPro technology status
- Optimization of ongoing maintenance and management
- Remote diagnosis and repair of client systems

Use Case 1: Improved Device Discovery and Intel vPro Technology Status

The power-off computer-detection capabilities of Intel vPro technology allow for the most comprehensive remote view possible of MSP customer hardware. In addition, Intel Active Management Technology (Intel AMT) requires an administrator password that protects the SMB customer from unauthorized access to their network devices. This 24/7 access provides faster and more accurate discovery of MSP customer systems, resulting in fewer onsite visits and lower administrative overhead, and allows MSPs to serve more customers with existing staff.

Level Platforms Managed Workplace gives solution providers a complete, integrated solution to centrally monitor and manage SMB customers from a single, Web-based platform. Managed Workplace consists of two components:

- The **Onsite Manager** is a lightweight application that is installed on an existing Windows Device at each customer site or as an appliance, depending on the MSP business model. The Onsite Manager includes a Web console that is hosted on Microsoft IIS and uses Microsoft SQL Server on the back end.

- The **Service Center** is installed on a Windows Server located at the MSP site or at a hosting location. The Service Center Web console is hosted on Microsoft IIS and also uses Microsoft SQL Server on the back end. You can integrate the Service Center with Microsoft Windows Server Update Services (WSUS) to provide patch management services.

Multiple Onsite Managers can connect to the Service Center using a secure SSL connection to provide SOAP/XML Web services over HTTPS.

1.1: Initial and Ongoing Client System Inventory

Whether you need the initial inventory for a new customer that establishes a baseline, or a regular monthly inventory to track changes, getting an accurate count of customer computers is a central component of managing customer contracts.

When combined with Intel vPro technology, Level Platforms Managed Workplace can monitor the availability of virtually any IP-enabled device, whether it is powered on or not. The ability to monitor both powered up and powered down machines helps to ensure inventory accuracy without an onsite visit. This remote accuracy also means that more frequent inventory assessments are possible without increased costs. The end result is a higher level of service at a lower cost.

This use case walks you through the steps required to discover customer assets, both initially and on an ongoing basis.

---

¹ Intel® Active Management Technology (Intel® AMT) requires the computer system to have an Intel® AMT-enabled chipset, network hardware and software, as well as connection with a power source and a corporate network connection. Setup requires configuration by the purchaser and may require scripting with the management console or further integration into existing security frameworks to enable certain functionality. It may also require modifications of implementation of new business processes. With regard to notebooks, Intel AMT may not be available or certain capabilities may be limited over a host OS-based VPN or when connecting wirelessly, on battery power, sleeping, hibernating or powered off. For more information, see www.intel.com/technology/platform-technology/intel-amt/.
Step 1: Intel Active Management Technology Automatic Discovery

1. Log on to the Managed Workplace Service Center console.
2. Expand Status in the left navigation bar, and then click Central Dashboard.
3. Click the site with which you want to work, and click on the cog icon at the end of the “Site Installation” line. Then select the Network Discovery tab.
4. Click Modify.
5. Under Intel vPro Credentials, click Change Password and enter the credentials that were used to configure Intel AMT.
6. Under SNMP V1/V2 Community String, click Add and enter the community string. If you have not changed the default in your network devices, enter “public” for the community string.
7. Under Scan Settings, click Add.
8. In the Add or Modify Scan Settings window, click Range and enter the range of IP addresses you want to scan.
9. Click Save.
10. Click Save on the Modify Network Scan Settings.
11. Click Scan now.

Managed Workplace 2012 discovers all devices in the network and lists them in the Device Management tab. It can take several minutes for information discovered during the scan to be displayed in the Managed Workplace Service Center console.

Step 2: View Intel AMT Status and Device Information

After you complete the device discovery procedure, Intel vPro technology lets you see detailed information about each device it is enabled on, even if the device is powered off.

1. Expand Configuration in the left navigation bar and click Intel vPro to see devices that have Intel vPro technology enabled.

   The Intel vPro Device Configuration page opens, showing all of the Intel vPro technology-enabled devices that belong to the network.

2. In the devices list, click the Device name/Alias of the device for which you want to see detailed information.

   The Device Management window opens and displays device information organized in tabs.

3. Click the Intel AMT link located under the “Monitoring” section on the right hand side.

   This page displays information about the device and the Intel AMT firmware installed on it. Under Intel AMT Status, you can power the device on or off, cycle the device’s power, or power reset the device.

4. Click the Hardware Inventory tab. This tab displays detailed information about the device’s hardware, including:
   - System information
   - Baseboard
   - BIOS
   - Processor Information
   - Memory Information
   - Disk Information

1.2: Initial and Ongoing System Analysis

Another core function of every MSP is to regularly monitor the attributes of the customer’s computer systems. MSPs should be able to drill down into individual customer computers to see a detailed hardware profile, including processor, memory, video cards, and other types of hardware information. This drill-down capability should also apply to software, giving the MSP visibility into operating system type, version, and patch level, in addition to installed applications, such as antivirus software and Microsoft Office suites. In addition, the security state of individual computers should be transparent so that configuration issues can be addressed.

A common challenge that MSPs face is keeping this asset information up to date given the fact that daily computer use and administration invariably lead to changes. By applying the capabilities of Intel vPro technology, Level Platforms Managed Workplace enables MSPs to gather customer computer asset information with real-time accuracy, even when managed computers are in low-power and powered-off states.

By continually monitoring these assets in real time, an MSP can increase the number of first-call resolutions. Furthermore, when onsite trips are necessary, such high-quality asset monitoring can reduce the cost of onsite visits by empowering the technician with complete and accurate information about the problem systems.

This visibility can be particularly helpful when planning for significant upgrades. For example, knowing the exact type and amount of memory in a customer computer would be very useful when planning an upgrade to Windows 7*. Arriving onsite with inaccurate memory information could result in a wasted onsite visit, adding to overhead and reducing service quality.

This use case walks you through the steps required to gather up-to-the-minute information from customer computers monitored with Managed Workplace. It is based on the assumption that you have completed the steps outlined in section 1.1 above to discover and import computer systems.

Step 1: Connect To Your Customer’s Network

1. Log on to the Managed Workplace Service Center console.
2. Expand Status in the left navigation bar, and then click Devices.
Step 2: View Asset Details of a Computer

1. On the Devices page, a list of devices that belong to the site appears. If necessary, select the Service Group option and select a Site Group from the drop-down list.
2. Click on the name of the device you want to view.
3. The Device Management page displays detailed information about the device. Tabs on the page provide the following types of information:
   a. Hardware: CPUs, disk drives, NICs, video and sound cards, CD drives, and monitors
   b. Software: OS and version, installed software, and patch history
   c. Windows Events: Discovered Windows events that meet the parameters you specify in the drop down list boxes
   d. Performance Counters: Graphs for the performance counters that the Onsite Manager scan discovers on a device
   e. Windows Services: A list of Windows services discovered on the device
   f. Network Services: A list of network services being monitored on the discovered device
   g. MBSA: An overview of the results of the MBSA (Microsoft Baseline Security Analyzer) scan that the Onsite Manager performed on the device
   h. Intel AMT: A list of events, a detailed hardware inventory, and AMT status
      The Intel AMT tab is present for devices that contain Intel vPro technology. In the Intel® AMT Status section, you can power on, power off, and reset a device remotely. You can also see at a glance the BIOS-level events for any AMT-enabled device, such as Power Off and Reset events. In addition, the Hardware Inventory tab displays detailed information about the device’s hardware profile.
   i. Attributes: Allows you to record information about a device that is not collected during the device scan

1.3: Alerts for Computers That Are Down or Missing from the Network

Level Platforms Managed Workplace uses Intel vPro technology to enable proactive inventory monitoring for all computer assets. Because Intel vPro technology can detect systems that are powered off or are in low-power states, it enables Managed Workplace to determine when a desktop or other stationary computer asset has been removed from the network. This capability can enable the MSP to respond to such situations the moment they happen, rather than discovering them later during a physical, onsite count.

This use case walks you through the steps required to set up automatic notification for computers that become disconnected from the network.

Step 1: Connect To Your Customer’s Network

1. Log on to the Managed Workplace Service Center console.
2. Expand Status in the left navigation bar, and then click Central Dashboard.
3. Click the site with which you want to work.

Step 2: Create an AMT Monitoring and Alert Rule

1. Expand the Configuration section in the left navigation bar, and then click Monitor & Alert Rules.
2. Select the device you want to monitor from the Device drop-down list.
3. Click Add Monitor.
4. Select AMT Events from the Choose the type of monitor to add drop-down list, and then click Add Monitor.
5. Select the Monitor tab.
6. Enter a Title and Description in the Monitoring Rule section.
7. In the AMT Event Rule section:
   a. Select the All check box next to the “Source” section, unless you want to monitor events only from a specific source.
   b. Specify the level of severity that will trigger the rule from the Severity drop-down list.
   c. Enter a search string that is unique to that alert if you are monitoring for an explicit alert in the Details Search Text field.
8. Select the Alerts tab, and then click Add Alert Configuration.
9. Enter a Title and Description.
10. Click Add Alert Rule.
11. In the AMT Event Alert Rule Parameter dialog, select the source for the event, alert severity required, and/or a search string that is unique to that alert, if you are monitoring for an explicit alert, and then click Save.
12. Select Alert when any rule conditions are met or Alert when all rule conditions are met.
13. In the Alert Categories, Actions and Notifications section, select the notification options you prefer. Depending upon the options you select, you might need to configure additional parameters.
14. Click Save.
15. Click Save in the Add AMT Events Monitor window. The new monitoring and alert rule appears in the Monitors list.
Use Case 2: Optimization of Ongoing Maintenance and Management

The remote power-management functionality of Intel vPro technology allows MSPs to ensure that tasks requiring a reboot are completed and confirmed—all from remote locations, without a desk side visit. Using the remote power-on/power-off functionality of Intel vPro Technology, administrators can complete and confirm such tasks as software updates and patches, anti-virus and firewall definition updates, software installation, and any troubleshooting tasks that require a reboot. This functionality opens up new services that MSPs can offer customers (such as power management) and makes some tasks possible remotely (such as applying BIOS updates) that were previously only possible with an onsite visit.

2.1: Routine Maintenance of Desktops: Install Patches and Software without a Desk Side Visit

MSPs often need to deploy patches or software packages to computers on the customer’s network. A common practice is to install these after normal business hours so that workers are not interrupted. In these scenarios, powered off computers can prevent MSPs from successfully completing the installations. By taking advantage of the power on and power off capabilities of Intel vPro technology, Level Platforms Managed Workplace can enable MSPs to remove this obstacle from patch and software installation tasks, ensuring that the task is completed the first time. This approach reduces overhead costs and increases customer satisfaction.

This use case walks you through the steps required to deploy a software package to all computers in a customer’s network—even those that are powered off.

Step 1: Power On the Target Computer

1. Log on to the Managed Workplace Service Center console.
2. Expand Status in the left navigation bar, and then click Central Dashboard.
3. Click the site with which you want to work.
4. Under Summary in right hand navigation bar, click Devices.
5. Click on the device you wish to power on.
6. Click the Intel AMT link in the right hand navigation bar under the Monitoring section.
7. Click the Power On link under the Intel AMT Status section.

Step 2: Create a Patch Management Policy

To use the patch management functions of Managed Workplace, Windows Server Update Services must be installed and configured.

A patch management policy consists of four parts:

- Synchronization options
- Automatic approval options
- Windows update agent policies
- Approval groups

To modify synchronization options

1. Expand Patch Management in the left navigation bar, and then click Settings.
2. Click Synchronization Options.
3. Under Products and Classifications, click the Change button under the Products section.
4. Select only the products you want to patch manage, and then click Save.
5. Under Classifications, click the Change button.
6. Select only the classifications you want to patch manage, and then click Save.
7. Select the site you wish to configure from the Site drop-down list.
8. Select Store patch files locally on the Onsite Manager, or deselect if you do not want to store patch files locally.
9. Choose Download updates in all languages, including new languages or Download updates only in the selected languages, checking the corresponding checkbox for each language.

Level Platforms, Inc. recommends specifying the subset of update languages your clients or organization uses, as downloading all updates in all languages will require a significantly greater disk space footprint.
10. Click Save.

To modify automatic approval options

1. Expand Patch Management in the left navigation bar, and then click Settings.
2. Click Automatic Approval Options.
3. In the Approve for Installation section, select Automatically approve updates for installation by using the following rule, or deselect to prevent automatic approval for installation.
4. Click Add/Remove Classification.
5. Check each patch classification to approve for installation, and then click Save.
6. Click Add/Remove Computer Groups.
7. Check each Approval Group for which installation will be automatically approved, and then click Save.

8. In the Revisions of Patches section, select Automatically approve the latest revision of the patch (with the same approval of the initial patch) or Continue using the older revision and manually approve the new patch version.

9. Select Automatically decline patches when a new revision causes them to expire, or deselect it to prevent automatically declining expired patches.

10. In the WSUS Patches section, select Automatically approve WSUS patches for installation, or deselect it to prevent automatic approval of WSUS patches.

11. Click Save.

To create a Windows update agent policy:

1. Expand Patch Management in the left navigation bar, and then click Settings.

2. Click Windows Update Agent Policies.

3. Click Add Agent Policy.

4. In the Agent Policy Identification section, enter a name and description for the policy, and then click Save.

5. Click the Policy tab.

6. In the Detection Frequency section, select how often the devices check for new patches.

7. In the Automatic Updates Options section:
   a. Select one of the following radio buttons:
      • Notify for download and notify for install
         Local users will be notified in the System Tray that updates are ready to be downloaded/installed.
      • Auto Download and notify for install
         Updates will be automatically downloaded and local users will be notified in the System Tray that updates are ready to be installed.
      • Auto download and auto install
         Updates will be automatically downloaded and installed based on the Auto Install Settings.
      • Automatic updates options configurable on client
         Local users may adjust the update settings in Windows.
   b. If you have selected Auto download and auto install:
      • In the Auto Install Settings section, use the drop-down lists to choose when installations occur.
      • Select wait X minutes after the next system startup to install, entering a value for X in minutes between 1 and 60, or select wait until next scheduled time to install to define how missed installations are handled.
   c. Select Immediately install minor updates to have updates installed immediately when they do not interrupt Windows services or require a restart.
   d. Select Allow non-administrative users to approve/disapprove updates to allow regular users to select which updates to install.

8. In the Auto Reboot After Installation section:
   a. Select Auto reboot after installation to cause a reboot prompt to appear on devices.
   b. Choose when the prompt will appear for the first time from the Reboot prompt drop-down list.
   c. Choose how often the prompt will appear thereafter from the Consecutive prompts after drop-down list.

9. In the Enable Patch Management section, select Enable Patch Management to enable the agent, or unselect it to disable the agent.

10. Click Save.

11. Select the Apply Policy tab.

12. To apply the Agent Policy to individual devices:
   a. Select the Devices tab and click Apply to Other Devices.
   b. Use the filters to narrow the choices as required, and check each device to which the Agent Policy should be applied. Click Add.

13. To apply the Agent Policy to groups of devices:
   a. Select the Groups tab and click Apply to Other Groups.
   b. Use the filters to narrow the choices as required, and check each group to which the Agent Policy should be applied. Click Add.

To create an approval group:

1. Expand Patch Management in the left navigation bar, and then click Settings.

2. Click Approval Groups.

3. Click Add. Enter a name for the Approval Group in the field that appears. Click Add to the right of the field.

4. Select All Computers from the Approval Group drop-down list to display all devices reporting into Patch Management (those added to the Windows Update Agents Policies that have been created).

5. Check each device to add to the Approval Group and click Move selected devices.

6. Choose the group from the drop-down list to move the devices into, and then click OK.
2.2: BIOS Edit

MSPs occasionally need to access and edit the BIOS settings on remote computers to diagnose, repair, or enable additional functionality in customer computers.

For example, Windows 7 can run legacy Windows XP applications from within its Start menu using Windows XP Mode. However, Windows XP Mode requires hardware-assisted virtualization, such as Intel Virtualization Technology (VT). Computers equipped with Intel vPro technology are capable of running Windows XP Mode, but Intel VT must first be enabled in the BIOS settings.

MSP support staff can remotely access BIOS settings and enable Intel VT from within Managed Workplace, allowing customers to take advantage of Windows XP Mode.

Step 1: Verify the BIOS Capabilities

First, confirm that the BIOS version of the computer you are running supports hardware-assisted virtualization.

1. Log into Managed Workplace Service Center.
2. In the left navigation bar, expand the Status section and click Central Dashboard. Select the customer site you wish to work in. Then click Devices under the Summary section in the right hand navigation bar.
3. Click on the Device Name of the system whose BIOS settings you want to access.
4. Click on the Intel AMT link under the Monitoring section in the right hand navigation bar.
5. Click the Hardware Inventory tab confirm that the data is populated with valid information (This information can take 5-10 minutes to populate after discovering the client)

Step 2: Edit BIOS to Enable Intel Virtual Technology

Now you need to establish a remote connection with the computer so that you can edit its BIOS settings.

1. From the right hand channel bar, click on the Remote Control link under the Management section.
2. In the Remote Services section, select Intel® AMT under the Service drop down menu.
3. Under the Intel AMT Configuration section, select the Emulation Type that your client supports (refer to the BIOS is need be).
4. In the Intel AMT Configuration section, select Boot to BIOS and click Connect.
5. BIOS menus and navigation vary widely between manufacturers. Locate and enable the Intel VT setting. In our environment, we selected Config > CPU Intel Virtualization Technology > Enabled.
6. Save the changes and exit the BIOS Setup Utility.
7. The computer should power down and restart. If it does not, restart it manually. When the computer reboots, Intel VT will be enabled and ready for Windows XP Mode.
Use Case 3: Remote Diagnosis and Repair of Client Systems

An MSP’s profitability is directly related to the efficiency of its support personnel. MSPs can best leverage support personnel by focusing on preventing support incidents from occurring in the first place. However, while this focus on preventative maintenance will reduce the number of support incidents, it will not eliminate them altogether. Support incidents will still occur, and when they do, the MSP can further improve efficiency by focusing on the percentage of support incidents that are handled remotely during the first call for support.

While Managed Workplace is designed to help MSPs achieve a high first-call resolution rate, by coupling Managed Workplace with the capabilities of Intel vPro technology, MSPs can dramatically improve first-call resolution rates, resulting in lower overhead and improved service levels.

The remote diagnostic and repair capabilities that Intel vPro technology adds to Managed Workplace, particularly for computers that are powered off or in low-power states, lets MSPs resolve more customer support issues remotely. Furthermore, when onsite visits are required, it enables MSP technicians to go prepared with the right tools and hardware to correct the problem. This approach can reduce the number of onsite visits required to solve the problem.

Managed Workplace provides several options for remote control; however, remotely controlling a customer computer that has not booted into Windows is only possible when the target computers are equipped with Intel vPro technology.

The following use case shows you how to take advantage of the remote diagnostic and repair capabilities of Intel vPro technology in situations commonly faced by MSPs today.
3.1: Use Remote Control to Troubleshoot a Problem

One scenario that front-line MSP support staff members commonly face is a Windows workstation that cannot boot. This condition can often be caused by a corrupt boot file. Remote control through Managed Workplace alone requires Windows to boot normally, which enables the Managed Workplace agent to run. Therefore, front-line support staff who face such situations without the benefits of Intel vPro technology cannot resolve this issue remotely. It must be promoted to a higher level of support, requiring an onsite visit.

However, if the MSP has successfully counseled the customer to acquire computer systems equipped with Intel vPro technology, Managed Workplace can interact with Intel vPro technology to let front-line support staff access a preboot environment for repair of this problem. This capability results in a first-call resolution for this common issue, reducing costs and increasing customer satisfaction.

This use case shows how Managed Workplace takes advantage of Intel vPro technology to provide first-call resolution for a customer reporting an “Operating System not found” or similar preboot error.

Step 1: Establish a Remote Connection

To repair the system on which Windows XP is broken or missing, you must first stage your preferred PE boot image within the SMB customer network. We are using Ultimate Boot CD for this example; you may use any pre-boot diagnostic tools that support a text-based UI. Store your image on the LP Onsite Manager at each customer location in the folder called C:\Program Files\Level Platforms\Onsite Manager\IDER Boot Images. The next step is to initiate a repair from a bootable image with repair utilities pre-installed. The image must be pre-deployed in the remote network, and it can be either a floppy image or CD image. The image file must be copied to the following folder on the computer hosting the Level Platforms Onsite Manager:

\c:\Program Files\Level Platforms\Onsite Manager\IDER Boot Images\.

1. Log into the Managed Workplace Service Center.
2. In the left navigation bar, expand the Status section and click Devices. Select the customer site from the drop-down list at the top of the main pane.
3. Click on the Device Name of the system that requires repair.
4. Click on the Remote Control link under Management in the right-hand channel bar.
5. In the Remote Services section, select Intel® AMT for the Service drop-down menu.
6. NOTE: this step is only required the first time you use Workplace Manager:
   a. In the AMT Configuration section, select “ANSI / Extended ASCII” for the Emulation type and “Normal Boot” so you can review the messages during POST; then click Save.
   b. In Internet Explorer:
      i. On the Tools menu, select Internet options.
      ii. Click the Security tab, and then click the Custom Level button.

3. NOTE: The first time you click Connect the following steps are required:
   a. Click Run in the LPI remote access framework client dialogue box.
   b. A Security Dialogue box appears. Click Install, and then click Run for the LP Workplace Tech Prep tool.
4. In the Remote Control Client window, click Yes to allow a normal reboot.
5. In this example the Master Boot Record has been corrupted, so during boot, you should see the Windows error message such as “Operating System not found.”

Step 3: Initiate Repair

The next step is to initiate a repair from a bootable image with repair utilities pre-installed. The image must be pre-deployed in the remote network, and it can be either a floppy image or CD image. The image file must be copied to the following folder on the computer hosting the Level Platforms Onsite Manager:

\c:\Program Files\Level Platforms\Onsite Manager\IDER Boot Images\

In this example, we are using Ultimate Boot CD with Ranish Partition Manager.

1. From within the Intel AMT Configuration section, put a check mark in the “IDE-Redirection” option.
2. Click the “Connect” button.
3. An IDER Image Selection window appears. Select the ISO you wish to boot to. Then click on the “Select Image” button.
4. A dialog box asks, Reboot Computer from CD Image? Select Yes. Press the Enter key when prompted to boot from CD image.
5. Based on the ISO you are booting, verify you can navigate through the UI via the Keyboard.
Step 4: Confirm That Repair Was Successful

Once the repair has finished, you must reboot the PC.

1. Click Remote Command in the menu bar, and select Normal Re-boot.

2. The Remote Control Client window opens and displays the message, Normal Reboot?; click Yes. If the repair was successful, you should see the POST messages of a normal reboot (image below).

3.2: Remotely Diagnose a Problem before an Onsite Visit

Even with the best remote control functionality provided by Intel vPro technology, some problems simply cannot be resolved remotely. Hardware failure, such as a hard disk failure, is one of those problems. However, by making the best use of Intel vPro technology, Managed Workplace can provide the onsite support staff with critical diagnostic information that helps ensure that the problem is solved with only one onsite visit.

In this use case, we will diagnose a failed hard disk drive before technicians go onsite to fix it.

Step 1: Establish a Remote Connection

1. Log into the Managed Workplace Service Center.

2. Expand Status in the left navigation bar and click Devices. Select the customer site from the drop-down list at the top of the main pane.
3. Click on the Device Name of the system that requires repair.

4. Under the Management section in the right hand channel bar, click on Remote Control.

5. In the Remote Services section, select Intel® AMT for the Service drop down menu.

6. Click the Connect button in the lower left corner.

7. A window briefly displays that says Verifying Application Requirements, this may take a few moments.

8. The Intel AMT Terminal window displays the message, Normal Reboot? Click Yes.

9. In this example the HDD has had a catastrophic failure, so a Boot error message should display during POST: 1962: No Operating System Found, press F1 to repeat boot sequence.

**Step 2: Check HDD Info in the BIOS**

1. In the Intel AMT Configuration section, select the Boot to BIOS option. Then click the Connect button.

2. A dialogue box asks: Reboot computer to Remoted BIOS? Click Yes.

3. Check the status of IDE Drive 0 in the BIOS System Summary menu. BIOS menus vary widely between manufacturers. In our environment, we used the arrow keys to select the BIOS System Summary menu and then pressed the Enter key. The menu shows None in the IDE Drive zero slot; this is where the OS is normally installed, so we have determined a catastrophic failure of the HDD and the technician can go to the site properly prepared.

**3.3: Remotely Restore an OS Image from a Hidden Partition**

Failure to boot is not always a failure of the hard disk or the MBR— the OS itself could become corrupt and fail to boot. This condition might normally require a desk side visit, but with Intel vPro technology and Managed Workplace, MSPs can remotely restore a default image stored in a hidden partition on the hard disk.

In this scenario, we will use Managed Workplace, Intel vPro technology, and TeraByte Image for DOS to replace a corrupt OS with a good image to restore the computer to working condition.

**Step 1: Establish a Remote Connection**

1. Log into the Managed Workplace Service Center.

2. Expand Status in the left navigation bar and click Devices. Select the customer site from the drop-down list at the top of the main pane.

3. Click on the Device Name of the system that requires repair.

4. Under the Management section in the right hand channel bar, click on Remote Control.

5. In the Remote Services section, select Intel® AMT for the Service drop down menu.

6. Select the IDE Redirection option.

7. Select the Terabyte for DOS boot image and click Yes to reboot.

8. Press the Enter key when prompted.

**Step 2: Restore a Backup Image**

1. Select Restore from the Terabyte Image for DOS main menu, and then select Next.

2. Select Automatic, and then select Next.

3. Select File (Direct), and then select Next.

4. Select BIOS (Direct), and then select Next.

5. Select the hard drive that contains the backup image, and then select Next.

6. Select the partition that contains the backup image, and then select Next.

7. Select the backup image to restore from, and then select Next.

8. Select the partitions you want to restore, and then select Next.

9. Select Yes to confirm.

10. Select Start to begin the restore process.

11. When the restoration process completes, select OK and press Enter.

12. Access the Intel AMT console and reboot the computer.
Conclusion

Intel vPro technology extends the management capabilities of Level Platforms Managed Workplace. It enables Managed Workplace to better discover, analyze, maintain and manage computer systems, particularly in low-power and power-off states. For managed-service providers, this extended functionality translates into better discovery and inventory of customer computers, more effective resolution of customer computer problems with fewer onsite visits, and allows them to provide richer ongoing management and power optimization offerings to clients. As the use cases outlined in this document illustrate, upgrading customers to hardware running on Intel vPro technology-enabled processors can reduce MSP operating costs and open new, profitable venues of customer service.

Related Links

For more information about Intel Active Management Technology (Intel AMT), a feature of the all new 2012 Intel Core vPro Processor Family with cost-saving manageability, visit:

For more information about Level Platforms Managed Workplace, and to try it for free, visit:

For more information on how Level Platforms Managed Workplace leverages Intel vPro technology, visit: