



Intel® vPro™ Technology Common-Use Guide

For the Kaseya IT Automation Platform

White Paper

Intel® vPro™ Technology
Kaseya IT Automation
Platform

Introduction

Common Uses for the Kaseya IT Automation Platform + Intel® vPro™ Technology

Intel® Core™2 processors with vPro™ technology and Intel® Centrino®2 with vPro™ technology extend the management capabilities of the Kaseya IT Automation Platform to enable enhanced discovery and to analyze and monitor IT devices, even in powered-off states. These extended remote management capabilities translate into lower overhead for IT professionals as well as higher service level agreements (SLAs) that IT professionals can offer their users.

This paper illustrates how to use Kaseya's IT Automation solution with Intel® vPro™ technology in several common scenarios. In doing so, this paper shows IT professionals how to lower administrative overhead and increase the level of service they can offer.



Table of Contents

- Introduction** 1
- Setup and Assumptions** 3
- Common Uses Covered in this Guide** 3
- Use Case 1: Improved Device Discovery and Intel vPro Technology Status** 3
- 1.1: Initial and Ongoing Client System Enumeration** 3
- 1.2: Initial and Ongoing System Analysis** 4
- Use Case 2: Optimization of Ongoing Maintenance & Management** 5
- 2.1: Automated Mass Power On / Off** 5
- 2.2: Routine Maintenance of Desktops: Install Patches / Software after Hours** 6
- 2.3: Use Case: Application Deployment using the Kaseya Application Deployment Wizard** . 7
- Conclusion** 9
- Related Links** 9

Setup and Assumptions

Software	<ul style="list-style-type: none"> ▪ Kaseya 2008 (v5.0) or higher
Hardware	<ul style="list-style-type: none"> ▪ Motherboard with Intel vPro Technology, which includes Intel Active Management Technology (Intel AMT)
Basic Assumptions	<ol style="list-style-type: none"> 1. You have configured the Intel AMT BIOS extensions of all client computer systems. 2. You have installed the Kaseya server software. 3. You have installed the Kaseya agent software on the monitored computers.

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 or 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.

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 user devices. In addition, the Intel Active Management Technology (Intel AMT), upon which vPro relies, requires an administrator password that helps prevent unauthorized access to network devices. This 24/7 access provides faster and more accurate discovery of systems, thus reducing the number of on-site visits, lowering administrative overhead, and allowing IT professionals to provide higher levels of service with existing staff.

Kaseya provides a complete, integrated IT automation solution to centrally monitor and manage IT infrastructure from a single, Web-based platform.

1.1: Initial and Ongoing Client System Enumeration

Establishing and maintaining a computer system inventory is a core IT service. Whether it is the initial inventory for a new user that establishes a baseline, or a regular monthly inventory to track changes, getting an accurate count of computers is a central component of IT management.

When combined with Intel vPro technology, Kaseya 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 going on site, thus saving time and money. This remote accuracy also means that more frequent inventory assessments are possible without increased costs. The end result is greater levels of service at lower cost.

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

Step 1: Connect To Your Network

1. Log on to the Kaseya console.

Step 2: Add Devices to the LAN Watch List

LAN Watch uses an existing agent on a managed machine to periodically scan the local area network for any and all new devices connected to that LAN since the last time LAN Watch was run. These new devices can be workstations and servers without agents or SNMP devices. Optionally, the Virtual System Administrator (VSA) can send an alert when LAN Watch discovers any new device. LAN Watch

effectively uses the agent as a proxy to scan a LAN behind a firewall that might not be accessible from a remote server.

You can discover new machines and devices by scheduling a LAN Watch scan.

To set a schedule for discovering new machines and devices on LANs:

1. In the Kaseya console, click the **Monitor** link at the top of the page.
2. On the **Monitor** page, in the **Function list** column on the left side of the page, click the **LAN Watch** entry that sits below the **SNMP Monitoring** section.
3. Using the drop-down lists to the right of the **Schedule** button, set the date and time to run the first discovery job.
4. Select the **Run recurring every** checkbox and then enter the values you want for how often you want the job to repeat.
5. Select the **Enable vPro** checkbox. Enter the **Username**, **Password**, and **Confirm** password information.
6. Select the checkboxes next to the machines for which you want **vPro** discovery enabled.
7. Click the **Schedule** button.

Step 3: View the Detailed Asset Report

You can use Kaseya to create several useful reports. To get a detailed asset inventory that includes the information gained from vPro-enabled machines, you can use the **Machine Summary** report, which produces a detailed report for each machine ID matching the Machine ID / Group ID filter. You can also use the **Machine Summary** report to generate comprehensive reports for individual machines. The **Machine Summary** report is configurable, allowing you to select which system data and application data will be included in the report. The Audit > Machine Summary page displays similar information.

To Create a New Machine Summary Report:

1. Launch the **Service Center** Web console.
2. At the top of the **Kaseya** page, click the **Reports** link.
3. On the **Reports** page, in the **Run Reports** section, click the **Machine Summary** link on the left side of the page.
4. On the top of the page, select the machine group for which you want the report to apply.
5. In the **Select display settings** section, select the information from the **Not Displayed** group that you want to display in the report and click **Add**. If you want to remove some information from the report, select the appropriate headers in the **Displayed** section and click **Remove**.

6. Enter a title for the report in the **Enter title displayed on report header** section.
7. Click the **Run** button to run the report.
8. Click the link on the top of the report page for the machine name of interest.

1.2: Initial and Ongoing System Analysis

Another core responsibility of every IT professional is to regularly monitor the attributes of computer systems on the network. This includes drilling down into individual computers to identify hardware specifics, such as processor, memory, video card, and other types of hardware information. The task also applies to software, including operating system type, version, and patch level, in addition to installed software applications such as antivirus software and Microsoft Office suites. In addition, the security state of individual computers should be transparent so that security configuration issues can be identified and addressed as needed.

A common challenge faced by IT professionals is keeping this asset information up-to-date, as daily computer system usage and administration invariably leads to changes. By applying the capabilities of Intel vPro technology, Kaseya enables IT professionals to gather computer asset information with real-time accuracy, even in low-power and powered-off states.

The ability to continually monitor these assets in real time means that an IT professional can increase the number of first-call resolutions. When on-site trips are necessary, such high-quality asset monitoring can reduce the cost per visit by empowering the technician to arrive with complete and accurate information about the problem systems.

This can be particularly helpful when planning for significant upgrades. For example, knowing the exact type and amount of memory in a computer would be very useful when planning an upgrade to the Windows Vista® operating system. Arriving on-site with inaccurate memory information could result in a wasted visit, adding to overhead and reducing service quality.

The following use case walks you through the steps required to gather such up-to-the-minute information from computers monitored with Kaseya 2008 (v5.0 or higher). It assumes that you have completed the steps outlined in section 1.1 above to discover and import computer systems.

Step 1: Connect To Your Network

1. Log on to the Kaseya console.

Step 2: View Asset Details of a Computer

1. Click the **Audit** link at the top of the console page.
2. On the **Audit** page, in the **View Group Data** list, click the **System Info** link.
3. On the **System Info** page, select the machine group containing the system of interest from the **Select Machine Group** drop-down list.
4. From the list of machines that appear on the left, select the name of the machine for which you want to obtain detailed asset information. Detailed information about this machine, including information obtained from Intel vPro , is included on the asset information page.

End of Use Case 1

Use Case 2: Optimization of Ongoing Maintenance & Management

The remote power-on/power-off functionality of Intel vPro technology allows IT professionals to complete ongoing maintenance and management tasks from remote locations, without a desk-side visit. Tasks like software updates and patches, anti-virus and firewall definition updates, software installation, and any troubleshooting tasks that require a reboot can all be completed and confirmed via the remote power-on/power-off functionality of Intel vPro Technology. This broadens the range of services that IT professionals can provide (such as power management) and makes some tasks possible remotely (such as applying BIOS updates) that were previously only possible with an on-site visit.

2.1: Automated Mass Power On/Off – Green Computing Scenario

Intel vPro technology enables Kaseya to remotely power on or off one or more machines on the managed network. The ability to initiate and schedule a mass power-on using Intel vPro technology enables IT professionals to save money on infrastructure power costs. A mass power-off can be initiated in the evening, and then a mass power-on can take place before workers reach their desks.

In the following use case, we will see how to use the Kaseya mass power-on feature, enabled by Intel vPro technology, to power on machines before users get to the desktops in the morning.

Step 1: Connect To Your Network

1. Log on to the Kaseya console.

Step 2: Schedule Shutdown of Target Computers at Night

1. Click the **Scripts** link on the top of the console page.

2. In the **Function List**, navigate to the **Public Scripts\Sample Scripts\System Mgmt** tree list. Find and select the **Shutdown** script.
3. On the schedule page, select the machine group from the **Select Machine Group** list to which you want to apply the mass shutdown.
4. Select the **Year/Month, Date, Hour, and Minutes** for when you want the shutdown event to take place. Make sure to schedule a time far enough in the future so that the patch installation can complete.
5. Select the **Run recurrent every X hour/day/month** check box if you want the scheduled event to recur.
6. From the machine list, select the check boxes next to the machines that you want to shut down during the scheduled event. If desired, you can use the **Select All** link to select all the machines in the group.
7. Click the **Schedule** button.

Step 3: Schedule a Mass Power-On Job

1. In the Kaseya console, click the **Remote Cntl** link at the top of the page.
2. On the **Remote Cntl** page, in the **Desktop Control** function list, click the **Power Mgmt** link.
3. Select the machine group that you want to manage from the **Select Machine Group** drop-down list.
4. Select individual hosts by selecting the checkbox to the left of each machine name. Alternately, you can select all machines in the group by selecting the check box to the left of the **Host Name** column header.
5. Select the **Power Up** option.
6. Click the **Schedule** button.
7. On the Schedule page, enter the **Date** and **Time** you want the power-on job to take place. Then select how often you want the job to recur: **Once**, **Hourly**, **Daily**, or **Monthly**. You can also select certain **execution** options, including **Skip if offline** and **Stagger by X minute(s)**.
8. Click the **Schedule** button.
9. In the **Recur Interval** column for the machine(s) selected for the power-on job, the recurrence interval for the scheduled job will be displayed.
3. On the **Remote Cntl** page, in the **Desktop Control Function** list, click the **Power Mgmt** link.
4. On the **Power Mgmt** page, select the machine group containing the machine you want to start from the **Select Machine Group** page.
5. Select the check box next to the machine you want to start.
6. Select the **Power Up** option.
7. Click the **Schedule** button.
8. On the **Schedule** page, enter the **Date** and **Time** you want the power on job to take place. Then select a **Recurrence** option. **Recurrence** options include **Once**, **Hourly**, **Daily**, and **Monthly**. You can also select an **Execution** option. **Execution** options include **Skip if offline** and **Stagger by X minute(s)**.
9. Click **Schedule** to save the schedule settings.
10. In the **Recur Interval** column for the machine(s) selected for the power-on job, the recurrence interval for the scheduled job will be displayed.

2.2: Routine Maintenance of Desktops: Install Patches/Software After Hours

Often, IT professionals need to deploy patches / software packages to computers on the network. A common practice is to install these after normal business hours, so that workers are not interrupted. In such scenarios, powered-off computers can keep installations from happening. By taking advantage of the power on / off capabilities of Intel vPro technology, Kaseya enables IT professionals to remove this obstacle from patches / software installation tasks, ensuring that the task is completed the first time. This reduces overhead costs and increases user satisfaction.

The following use case walks you through the steps required to deploy a patch to computers in a network—even those that may be powered off.

Step 1: Power on the Target Computers

1. Log on to the Kaseya console.
2. In the Kaseya console, click the **Remote Cntl** link at the top of the page.

Step 2: Deploy Patches to the Target Computer

1. Log on to the Kaseya console.
2. Click the **Patch Management** link on the top of the page.
3. On the **Patch Management** page, in the **Select Machine Group** drop-down list, select the group to which the machine you want to update belongs.
4. In the **Manage Updates** function list, click the **Machine Update** link.
5. On the **Machine Update** page, click the name of the server you wish to update.
6. On the patch update page, select the updates that you want to apply to the machine. You also have the option to **Select All** updates. Select the **Year/Month**, **Date**, **Hour**, and **Minutes** for when you want the update to take place.
7. Click the **Schedule** button.
8. The patches will show as **Pending** on the right side of the page.

Step 3: Schedule Shutdown of Target Computers after Updates Complete

1. Log on to the Kaseya console.
2. Click the **Scripts** link on the top of the console page.

3. On the **Scripts** page, in the **Function** list, navigate to the **Public Scripts\Sample Scripts\System Mgmt** tree list. Find and select the **Shutdown** script.
4. On the **Schedule** page, in the **Select Machine Group** drop-down list, select the machine group to which you want to apply the mass shutdown.
5. Select the **Year/Month, Date, Hour, and Minutes** for when you want the shutdown event to take place. Make sure to schedule a time far enough in the future so that the patch installation can complete.
6. Select the **Run recurrent every X hour/day/month** check box if you want the scheduled event to recur.
7. From the machine list, select the machines you want to shut down during the scheduled event. If desired, you can use the **Select All** link to select all the machines in the group.
8. Click the **Schedule** button.

Note:

After performing the use case described in section 2.2, the scheduled power down event overrides the scheduled event described in section 2.1. You will need to reschedule the power down event described in section 2.1 in order to maintain the green computing scenario.

2.3 Use Case: Application Deployment using the Kaseya Application Deployment Wizard

In addition to installing patches, IT professionals often need to deploy applications after hours. Kaseya's IT Automation Platform with Intel vPro support enables IT professionals to remotely power on devices so that they are available for automated application installation.

This use case walks you through the steps required to deploy an application to computers in a network—even those that may be powered off.

Step 1: Power on the Target Computers

1. Log on to the Kaseya console.
2. In the Kaseya console, click the **Remote Cntl** link at the top of the page.
3. On the **Remote Cntl** page, from the **Desktop Control Function** list, select the **Power Mgmt** link.
4. On the **Power Mgmt** page, from the **Select Machine Group** page, select the machine group containing the machine you want to start.
5. Select the checkbox(es) next to the machine(s) you want to start.

6. Select the **Power Up** option.
7. Click the **Run Now** button.

Step 2: Run the Application Deployment Wizard

1. In the Kaseya console, click the **Scripts** link at the top of the page.
2. On the **Scripts** page, in the **Installer Wizards** function list, click the **Application Deploy** link.
3. You need to tell the Application Deploy wizard if you want to send the installer from the VSA server to the remote machine and execute it locally or execute the installer from a file share on the same LAN as the remote machine. Note that pushing the application installation file to each machine from the VSA may be bandwidth-intensive. If you are installing to multiple machines on a LAN, no Internet bandwidth is needed to push out the application installation file: Each machine on the LAN can execute the application installation file directly from a common file share.
4. Select the application install file or specify the UNC path to the installer stored on the same LAN as the remote machine.
 - a. If you selected **Send the installer from the VSA server to the remote machine and execute it locally**, then the installer file must be on the VSA server. Select the file from the drop-down list. If the installer file does not appear in the list, then it is not on the VSA server. Click the **here** link to upload the file to the server.
 - b. If you selected **Execute the installer from a file share on the same LAN as the remote machine**, then the installer file must be on the remote file share prior to running the application deploy script. The specified path to the file must be in UNC format such as `\\computername\dir\`. **Note:** If the file is not already on the remote file share, you can put it there via FTP.

Click **Next**.

5. Next, the wizard needs to know what kind of installer was used by your software vendor to create the install package.
 - a. From the **Select the install package to send to the remote machine** drop-down list, select the appropriate entry. (The VSA provides a small utility to automatically identify all supported installer types. Supported installer types are: Windows Installer (MSI files), Wise Installer, InstallShield - Package for the Web, InstallShield - Multiple Files, Other.)
 - b. From the **What kind of install is this?** drop-down list, select the applicable type.

- c. Finally, enter any command line arguments you need in the **Specify command line** text box.

Click **Next**.

6. Enter a name for the script in the **Name the script to deploy this application** text box. Select the **Reboot the machine after installing the application** check box. Click **Create**.
7. From the **Machine.Group ID** list, select the check boxes next to the machines that you want to run installation script on. You can schedule the script to run at a specific time and date or run the installation script now. Select the **Year/Month, Date, Hour,** and **Minutes** for the scheduled time and date. Click the **Run Now** button to run the installation script now.

Step 3: Schedule Shutdown of Target Computers after Applications Install

1. Log on to the Kaseya console.
2. At the top of the console page, click the **Scripts** link.
3. On the **Scripts** page, in the **Function** list, navigate to the **Public Scripts\Sample Scripts\System Mgmt** tree list. Find and select the **Shutdown** script.
4. On the **Schedule** page, in the **Select Machine Group** drop-down list, select the machine group to which you want to apply the mass shutdown.
5. Select the machines you want to shut down during the scheduled event from the machine list. You can use the **Select All** link to select all the machines in the group.
6. Click the **Run Now** button.

End of Use Case 2

Conclusion

Intel Core 2 with vPro technology and Intel Centrino 2 with vPro technology extend the management capabilities of the Kaseya IT Automation Platform. Intel vPro technology enables Kaseya to better discover, analyze, maintain, and manage computer systems, particularly in low-power and powered-off states. For both public/private sector IT professionals and IT service providers, this extended functionality translates into the ability to better discover and enumerate computers, deal with computer problems with fewer on-site visits, and provide richer ongoing management and power optimization offerings to users. As the use cases outlined in this document illustrate, upgrading users to hardware running on processors enabled with Intel vPro technology can reduce operating costs, increase productivity, improve efficiency, and open new venues of IT service.

Related Links

- For more information about the Intel Core 2 processor with vPro technology and the Intel Centrino 2 with vPro technology, visit:
http://www.intel.com/technology/platform-technology/intel-amt/index.htm?iid=tech_pt+body_iamt
<http://softwarecommunity.intel.com/articles/eng/1034.htm>
- For more technical information on Intel vPro technology visit:
<http://www.intel.com/go/vproexpert>
- For more information about Kaseya, and to try it for free, visit:
<http://www.kaseya.com>

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS ARE NOT DESIGNED NOR INTENDED FOR ANY APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.

Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or by visiting Intel's Web Site: <http://www.intel.com>.

Intel® Active Management Technology 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.

Intel, Intel® Core™2 processor with vPro™ technology, Intel® Centrino® 2 with vPro™ technology, and Intel vPro are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

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

Copyright © 2008 Intel Corporation. All rights reserved.

