INTEL® CLIENT MANAGEABILITY ADD-ON FOR MICROSOFT SMS 2003 USE CASE GUIDE

Table of Contents

Introduction

Common Uses Covered in This Guide

Intel® vPro™ technology, in conjunction with the Intel® Client Manageability Add-on for Microsoft* SMS 2003, improves system management capabilities of Microsoft* Systems Management Server 2003 and enables endpoints management even in power-off states. It also allows better power saving, security, support and diagnostics. This document presents the following use cases which demonstrate these enhancements and is intended for those who will be implementing Intel vPro technologies in a Microsoft SMS management infrastructure:

- Asset Inventory
- Imaging and Re-imaging
- Power saving
- Remote diagnostic and repair
- Enforced administrative isolation off the network
- Automatic isolation off the network
- Patch Management isolation off the network

Setup and Assumptions

Software	• Management server and console: Microsoft Windows 2003 Server R2 SP2; Microsoft SMS 2003 v3.6; Intel Client Manageability Add-on for Microsoft SMS 2003. • Managed Intel vPro-enabled client with Microsoft Vista SP1
Hardware	• PC with Intel vPro technology[1]. Firmware version 3.2.1 under test is DELL 755 Optiplex, although the same results should be observed with machines from other OEM's.
Basic assumptions	1. Intel Client Manageability Add-on for Microsoft SMS 2003 and vPro-enabled endpoint are operating in Microsoft infrastructure with Domain Controller and Active Directory 2. Intel® SCS has been installed and configured according to the Intel® SCS Installation and User Manual 3. Intel® vPro™ – enabled client machines were provisioned before the use cases described below have been tested.

[1] Intel® Active Management Technology requires the computer system to have an Intel(R) 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/.

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

Asset Inventory Use Case

ACTORS:

1. **Asset Inventory Team** is responsible for tracking assets.
2. **Field Service Team** is responsible for repairing, maintaining and upgrading systems.

SCENARIO:

Asset Inventories are conducted using software tools that sweep an enterprise network. The success of this has traditionally been dependent on multiple factors.

1. Installed operating system
2. Installed management tool agent
3. System is powered on

Failures to meet any of the above criteria lead to inaccuracies in asset reporting and require substantial effort to remedy.

Examples are:

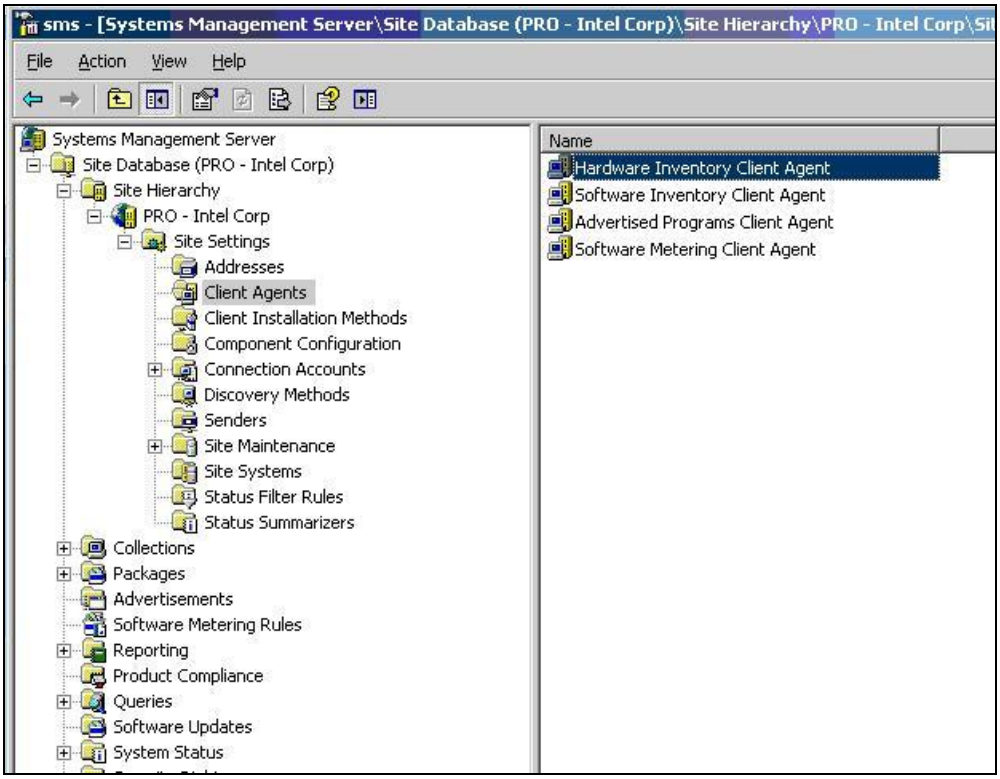
- Systems that tend to be powered off for extended periods of time such as those located in remote or infrequently occupied locations can end up in a "lost" status by dropping off the inventories because they are not available during the automatic inventory sweeps.
- Verification of specific hardware configurations, such as what slot contains a stick of memory and what type it contains requires an accurate and current inventory based on the above criteria or a desk-side visit.

SOLUTION:

PCs with Intel® vPro™ technology can be utilized to collect hardware inventories, verify service tags or serial numbers and check hardware configurations without interrupting the end-user or visiting desk-side.

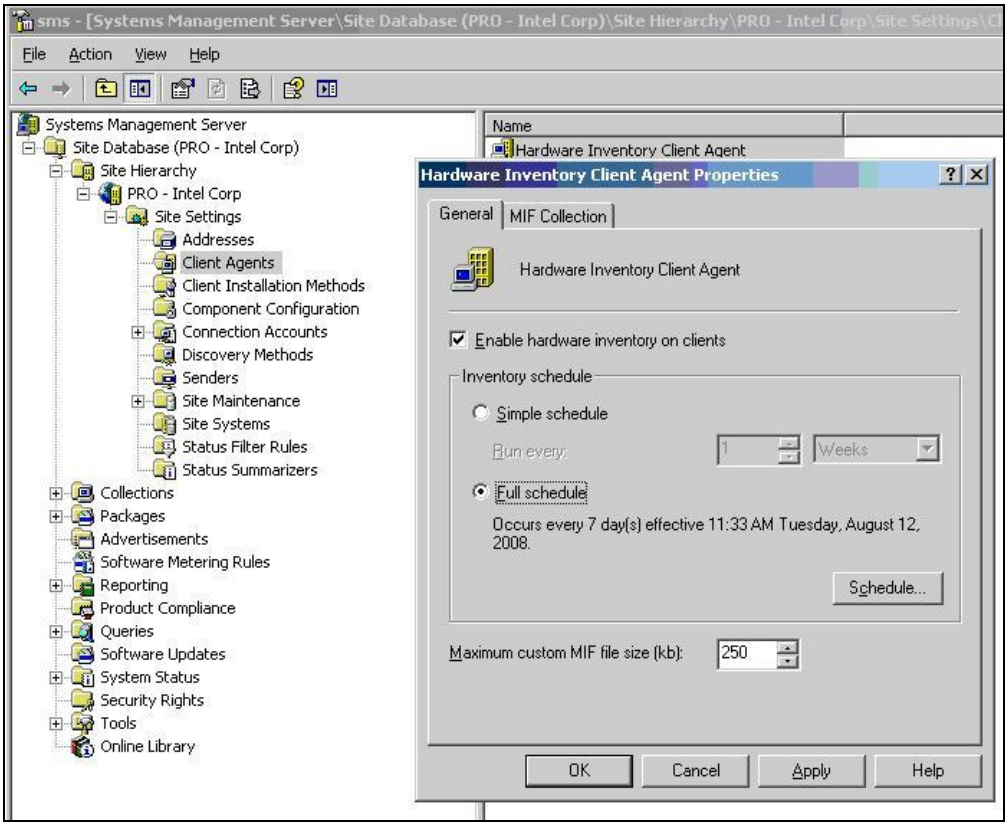
1. From the **System Management Server Administrative Console**, navigate to **Systems Management Server → Site Database → Site Hierarchy → <site code> - <site name> → Site Settings → Client Agents.**

   In the **right** pane, right-click **Hardware Inventory Client Agent**, and select **Properties**

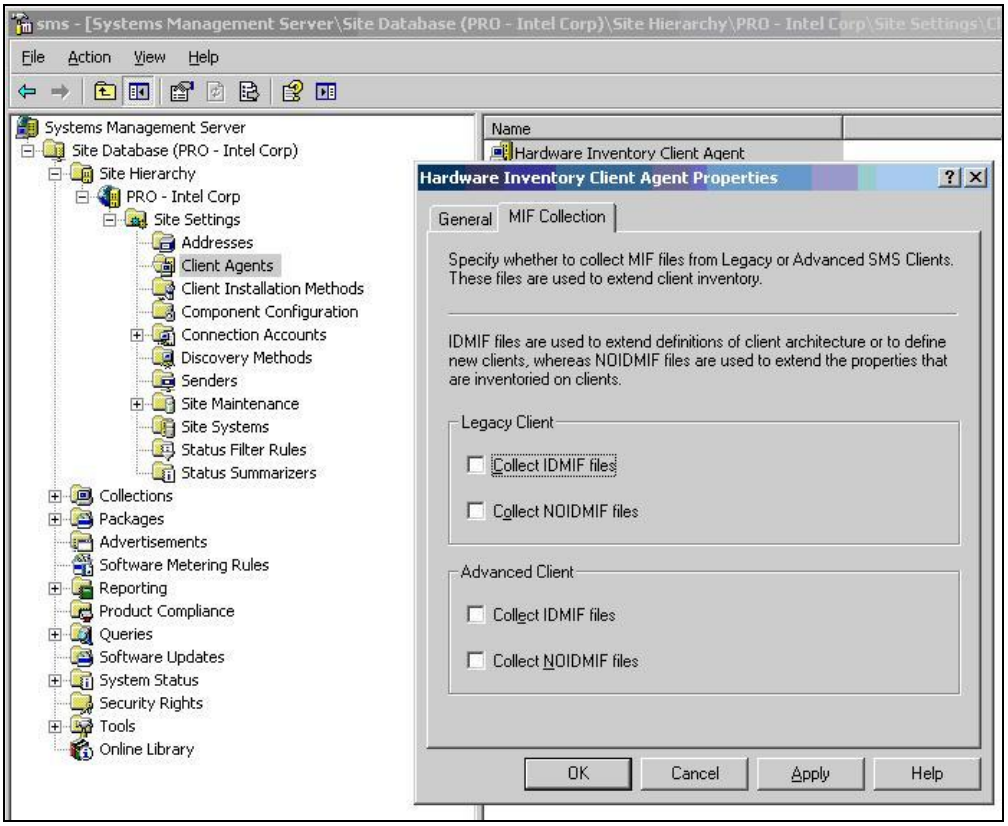


2. From the **Hardware Inventory Client Agent Properties** dialog box **General** tab, enable and schedule hardware inventory.

   Configure the **Maximum custom MIF file size (KB):** that will be processed by the site as needed. Click the **MIF Collection** tab.



3. From the **MIF Collection** tab, for Legacy and Advanced clients specify whether to collect **IDMIF** or **NOIDMIF** files from clients. Click **OK**.



Imaging and Re-imaging Use Case

ACTORS:

1. **Field Service Support person(s)** responsible for putting the PC on the end user's desk and connecting power and network and installing the Operating System (O/S) and any additional application.
2. **Service desk personnel** responsible for Management, Software administration for the environment.

SCENARIO:

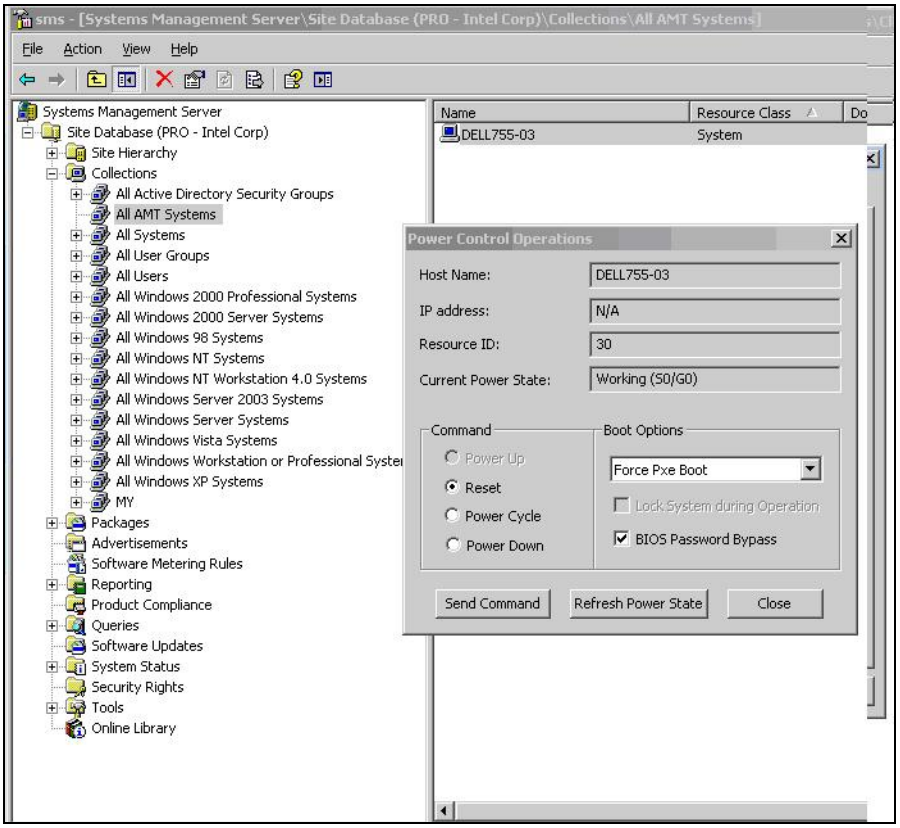
With companies today having employees located all over the globe and the need to support this global workforce with a few strategic locations of Field Service Support staff, the need to be able to perform imaging time- and cost-effectively is paramount. The Field Service Support resource brings the new PC with Intel vPro technology to the end user's office, takes it out of the box, places it on the desk, and connects the power and network cables to the device. Then the Field Service Support resource spends 1 to 4 hours per device installing and configuring the operating system and any additional applications from a CD or DVD.

SOLUTION:

This process will enable the Field Support staff to deliver the device to the end user's desk and connect it to the company network and power. Once powered on, the device will automatically configure the vPro capabilities by registering the device with the Management Software. Using the capabilities of Intel vPro technology and the Management Software, the Service Desk resource will initiate the device to PXE boot starting the automated deployment of the base operating system image and additional applications. This frees up the Field Support and Service Desk resources to address a higher number of service requests. In addition to a single machine being imaged, this process can support reimaging to a group of devices. An example is reimaging a bank of training room systems after each class to ensure students receive a clean build.

PREREQUISITES: Remote Installation Services (RIS) or Windows Deployment Services (WDS) should be installed and running on a supporting infrastructure server.

1. Select the system with Intel vPro technology that requires a diagnosis operation. Right-click and select **All Tasks->Intel® AMT Tasks->Power Control.** From **Command** select **Reset** or **Power Cycle.** From the **Boot Options**, select **Force PXE Boot**. Click **Send Command** button.



2. The managed PC should start booting by executing Pre-Boot execution environment. Its black screen should display a text similar to one on the right.

   On the screen there should be progress:

   Initializing Intel® Boot Agent GE v1.2.50
   PXE 2.1 Build 086 (WfM 2.0)
   CLIENT MAC ADDR: … GUID …
   CLIENT IP: …
   TFTP
   PXE …

Power Saving Use Case

ACTORS:

1. **Workplace Administration Team** is responsible for workplace patch testing, consolidation, distribution, and reporting.
2. **Facilities Management Team** is responsible for energy conservation programs and has budgetary responsibility for paying energy bills.

SCENARIO:

Each month the Workplace Administration Team downloads and tests the patch set from the operating systems vendor. They also consolidate the resulting tested patch set into a bundle for distribution via the centralized workplace management system. Upon release of the patch bundle onto the workplace systems, the Workplace Administration Team collects and reports compliance metrics to management. This team also responds to emergency patch releases from the operating systems vendors. In this instance, the team completes the same planning, testing, distribution, and reporting cycle, only using a much shorter completion timeline. In order to ensure patches are distributed to the most workplace personal computers as possible, the power policy for this company is simple – Leave all of the workplace systems perpetually powered on.

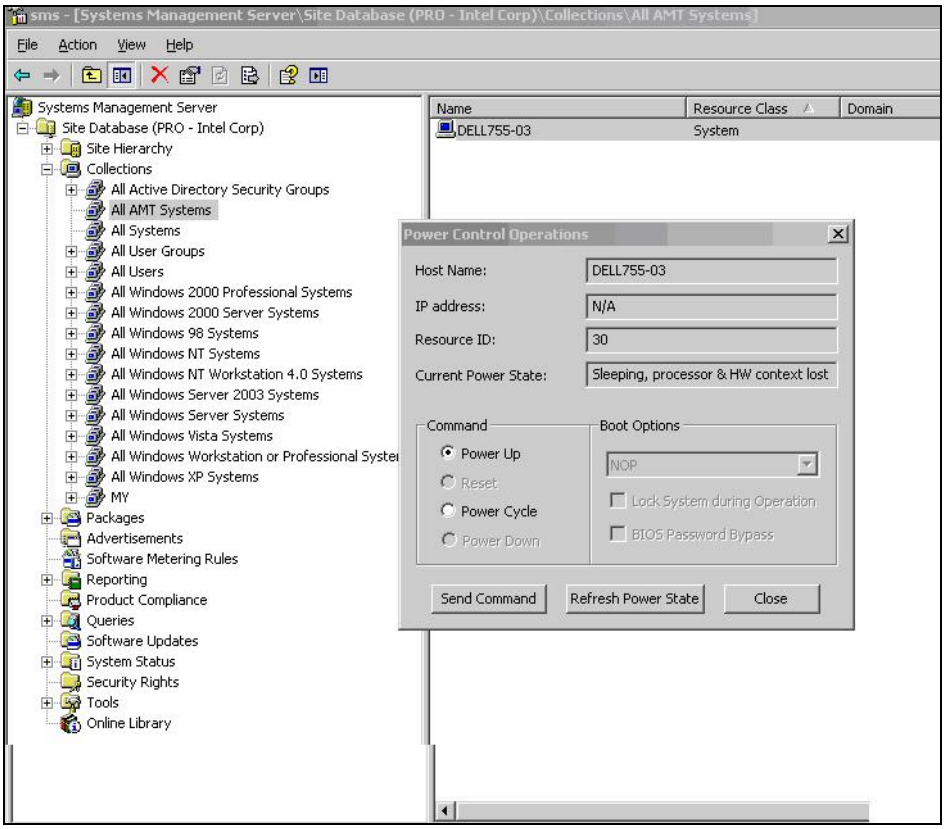
The Facilities Management Team needs to ensure that corporate objectives for energy conservation and savings are met. In order to do this, the team has instituted policies to turn off unused lighting, heating, ventilation, and air conditioning systems where not being used. In order to achieve its next milestone, the Facilities Management Team has recommended that all workplace personal computers be turned off when the user is not in the office. These two group's mandates are diametrically opposed. The Workplace Team cannot patch workplace systems during off hours because the machines must be powered on. Patching during working hours results in productivity losses due to workplace system reboots. Working hour patches also allows users to delay the patching sequence causing lower patch compliance percentages. The facilities team desire to not run the systems at off hours is purely an economic decision and their monetary savings requirement is fundamental to corporate strategy.

SOLUTION:

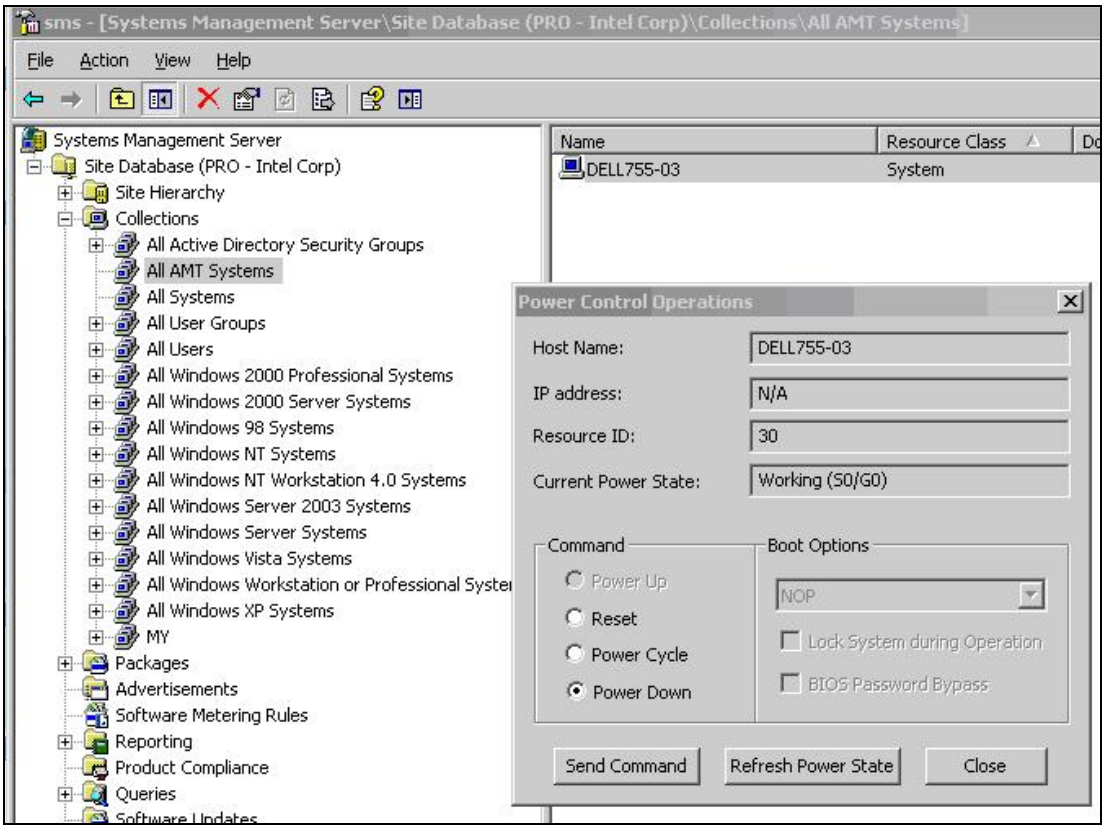
In order to meet both sets of requirements, Intel vPro technologies and associated workplace software technologies can be used to power on or off workplace machines at designated times to meet a company's energy savings requirements. Furthermore, Intel vPro technology can be employed to power on workplace platforms allowing patching at any time the Workplace Management Team chooses, and upon patch completion will shut the workplace platform down upon patch completion.

HOW TO: POWER ON/OFF

1. From the System Management Server console, navigate to **System Management Server**->**Site Database (<site name>)**->**Collections-><collection name>**. Select one or more AMT systems on the right pane. Right-click and navigate to **All Tasks-> Intel AMT Tasks -> Power Control Operations.**



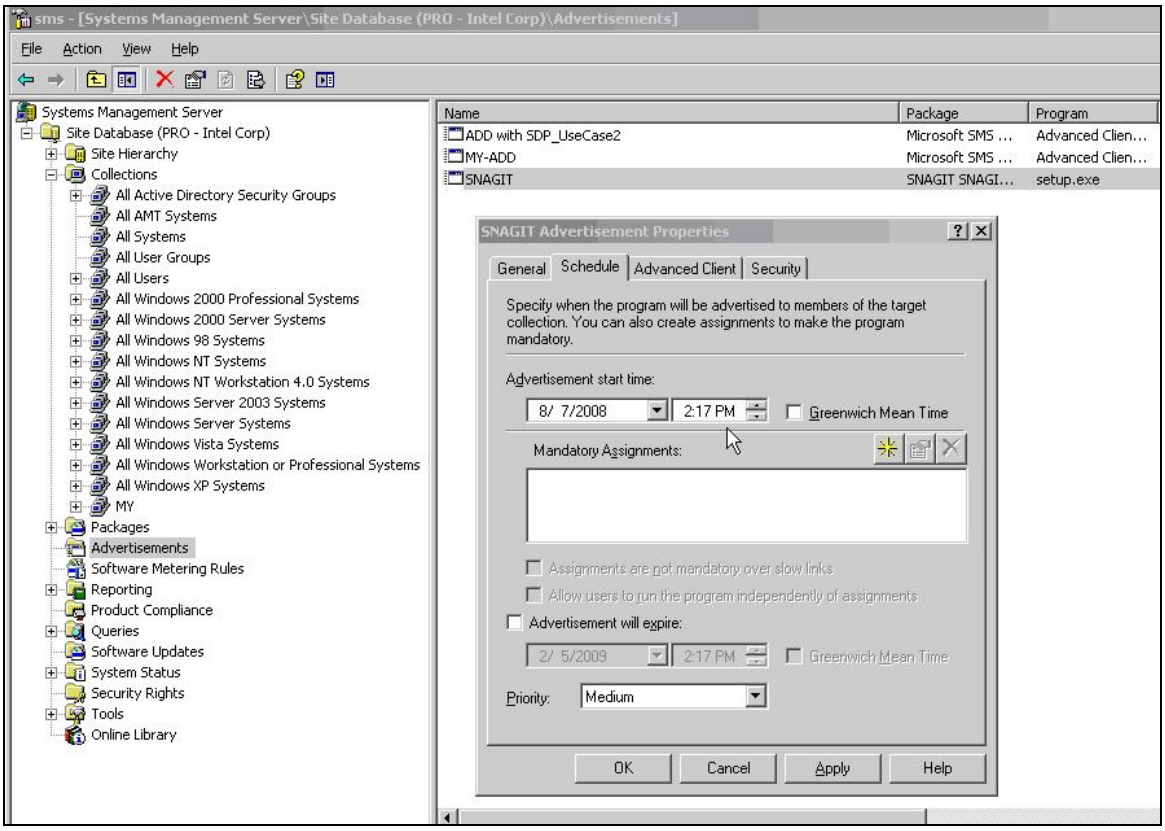
2. In the Power Control dialog box, select **Power Up** or **Power Down** radio button. Press **Send Command**



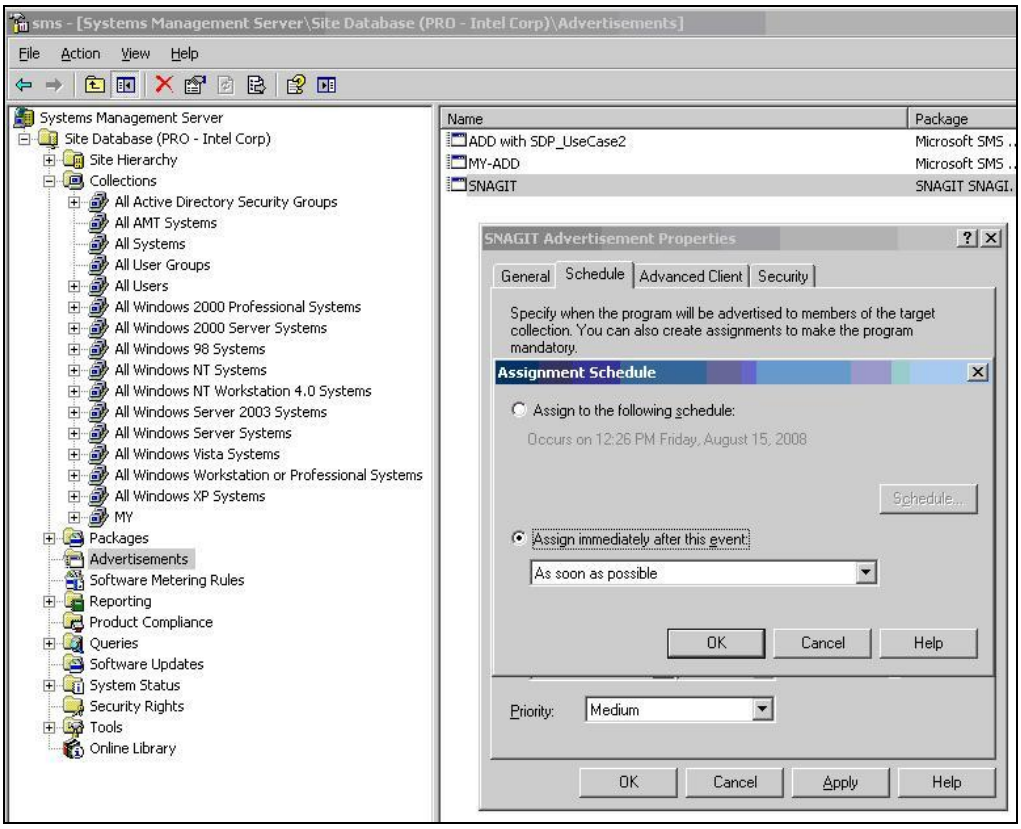
HOW TO: WAKE UP ON ADVERTISEMENT

Wake on Advertisement use cases can only be performed on PCs with Intel vPro technology with an SMS Advanced Client agent installed and active. PCs with Intel vPro technology should belong to a local SMS site.

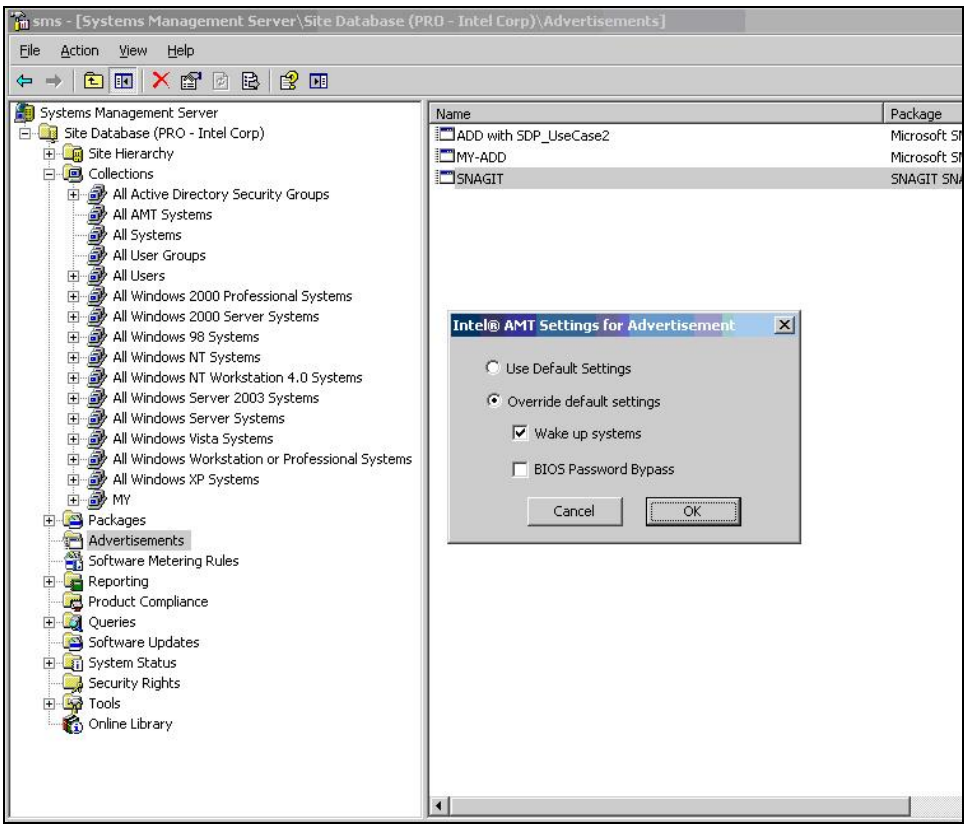
1. From the System Management Server console, create a **Package** using SMS instructions. Create a **Program** that will execute the package. Create an **Advertisement** to launch the program. Select the Advertisement **Properties**. A new window **Advertisement Properties** should appear. Fill the **Advertisement start time** fields and create a **Mandatory Advertisement** by pressing (*) icon on the right. Press OK.



2. Setting controls in a new **Assignment Schedule** dialog box as presented on the picture will appear. Select the Assignment option or click **Schedule**, and then click **OK.**



3. From the selected **Advertisement** right click and select **All Tasks->Intel ® AMT Tasks -> Wake Up** Option. Intel® AMT Settings for Advertisement box pops up. Make selections as shown and press **OK**.



Remote Diagnostic and Repair Use Case

ACTORS:

1. **Support Staff** – responsible for customer call resolution, often located in a central location.
2. **End User** – uses the PC for day to day activities within the enterprise.

SCENARIO:

Most end user data resides on server resources, or server based applications via network file shares or hosted applications. During an end user PC failure, a call is placed to the support staff for resolution. In most cases the initial support staff personnel are not local to the end user's PC which presents challenges to problem resolution resulting in either shipping the PC back to second level support, or dispatch of a regional service technician. This situation can significantly impact an end user's productivity level, and drive support costs up as every physical touch to an end user PC can increase support costs.

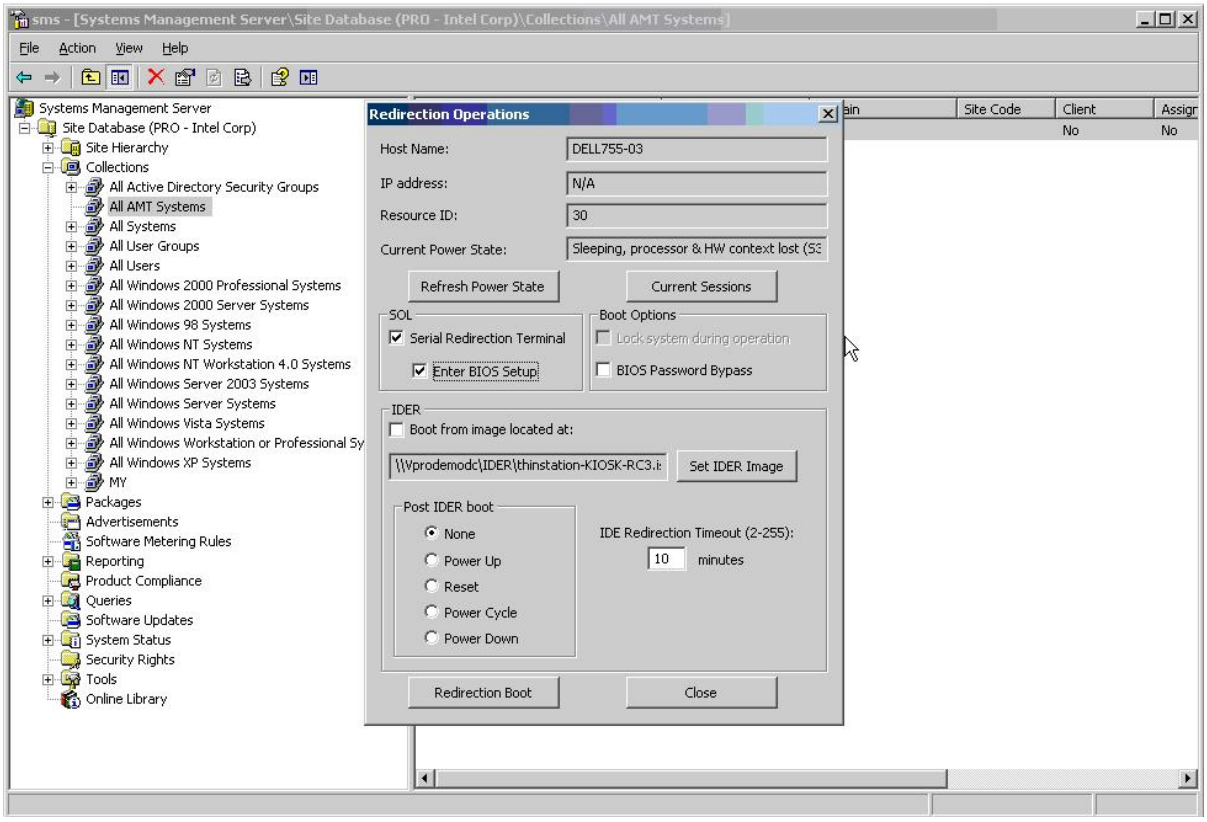
SOLUTION:

Increase end user productivity and reduce physical touch via Intel vPro technologies. By using IDE-R or IDE Redirection, the end user PC can now boot to remotely stored files, providing both remote diagnostic/repair and alternate user desktop capabilities. In the remote diagnostic/repair scenario the support staff would now have the ability to boot the troubled PC into a special diagnostic OS allowing the remote technician to perform detailed troubleshooting, or OS repair activities during the initial support call. Additionally, if it is determined that a hardware problem with the PCs physical hard drive to be the culprit, support staff now have the option to boot the troubled PC into a temporary environment with basic end user services such as Terminal Server Client, Citrix Client, and web browser support while hardware is being dispatched.

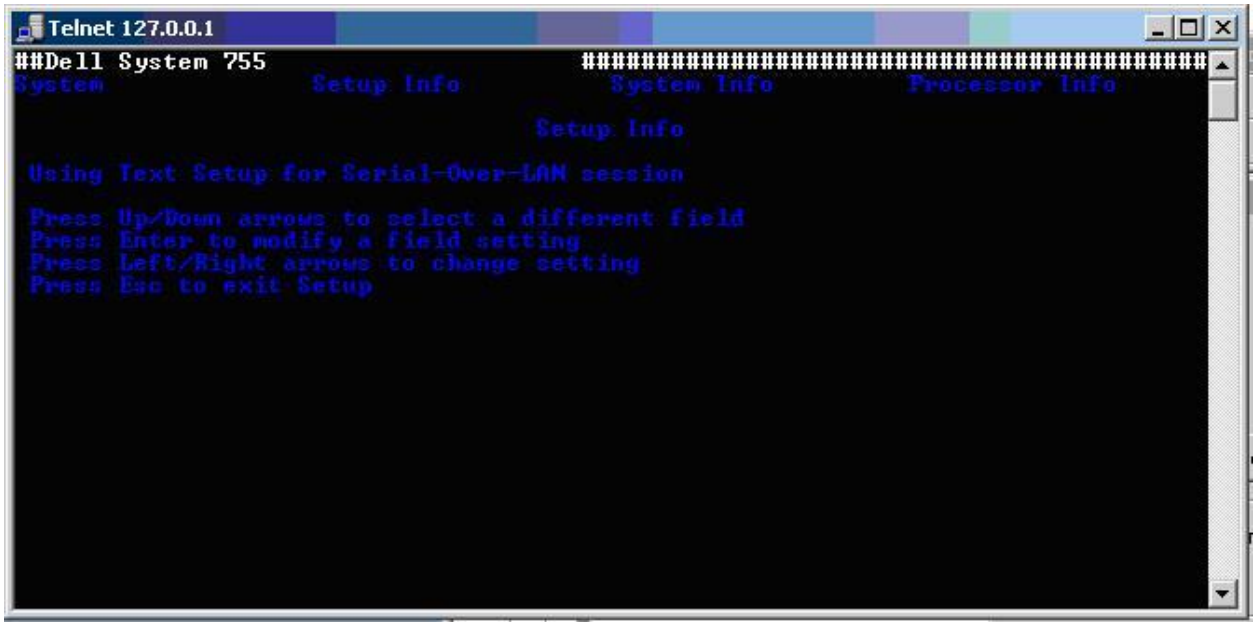
Reducing Desk-side visits	Current Process	With Intel vPro technology	Percent Improvement
Average desk-side visits for software fix	1.64	0.14	91.4%
Average desk-side visits for hardware fix	2.29	1	56.3%

HOW TO: REMOTE DIAGNOSIS (SOL)

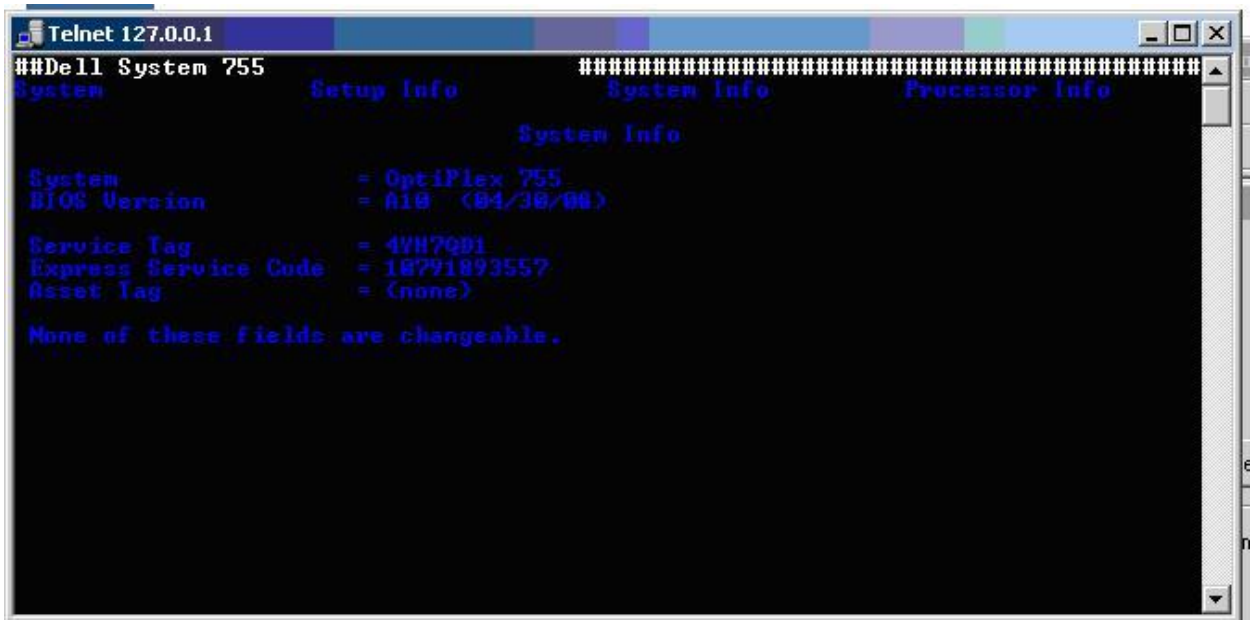
1. Select the PC with Intel vPro technology that requires a diagnosis operation. Right-click on the selected system in the right pane and select **All Tasks->Intel® AMT Tasks->Redirection Operations. Redirection Operations** window pops up.



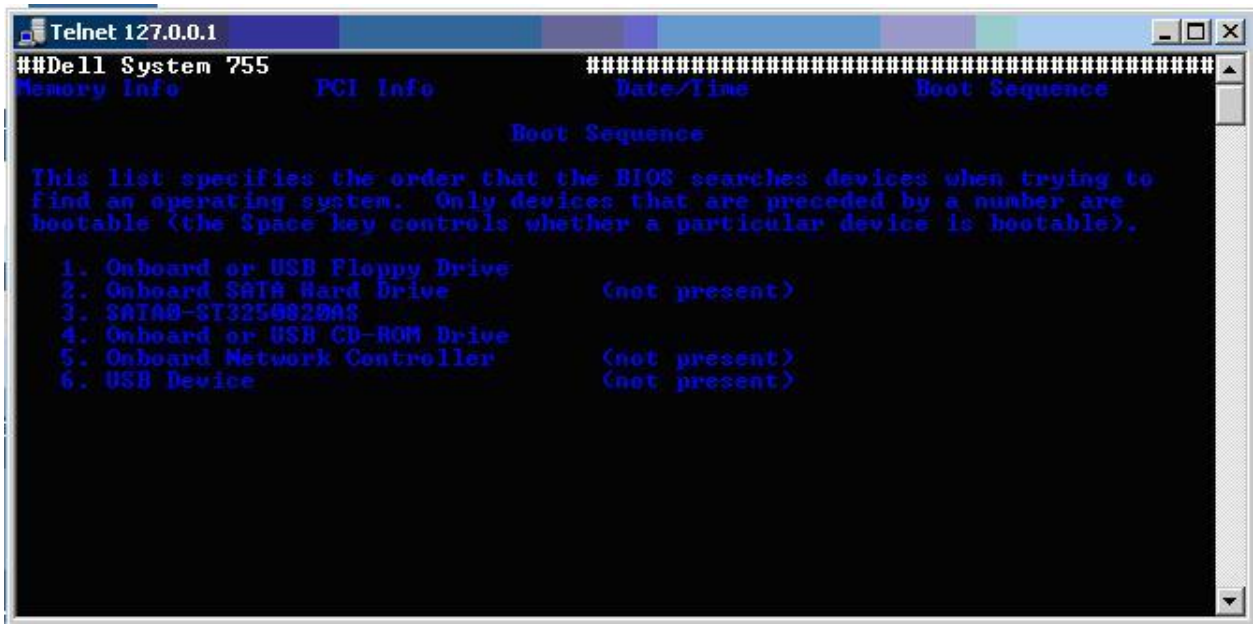
2. In the **Redirection Operations** window check **SOL** and **Enter BIOS Setup** box and uncheck all others. Press the button **Redirection Boot**. A Telnet session starts, and Serial Connection Text menu will pop up on the screen.



3. Using buttons as instructed on the previous Telnet screen menu, navigate to the item of interest.

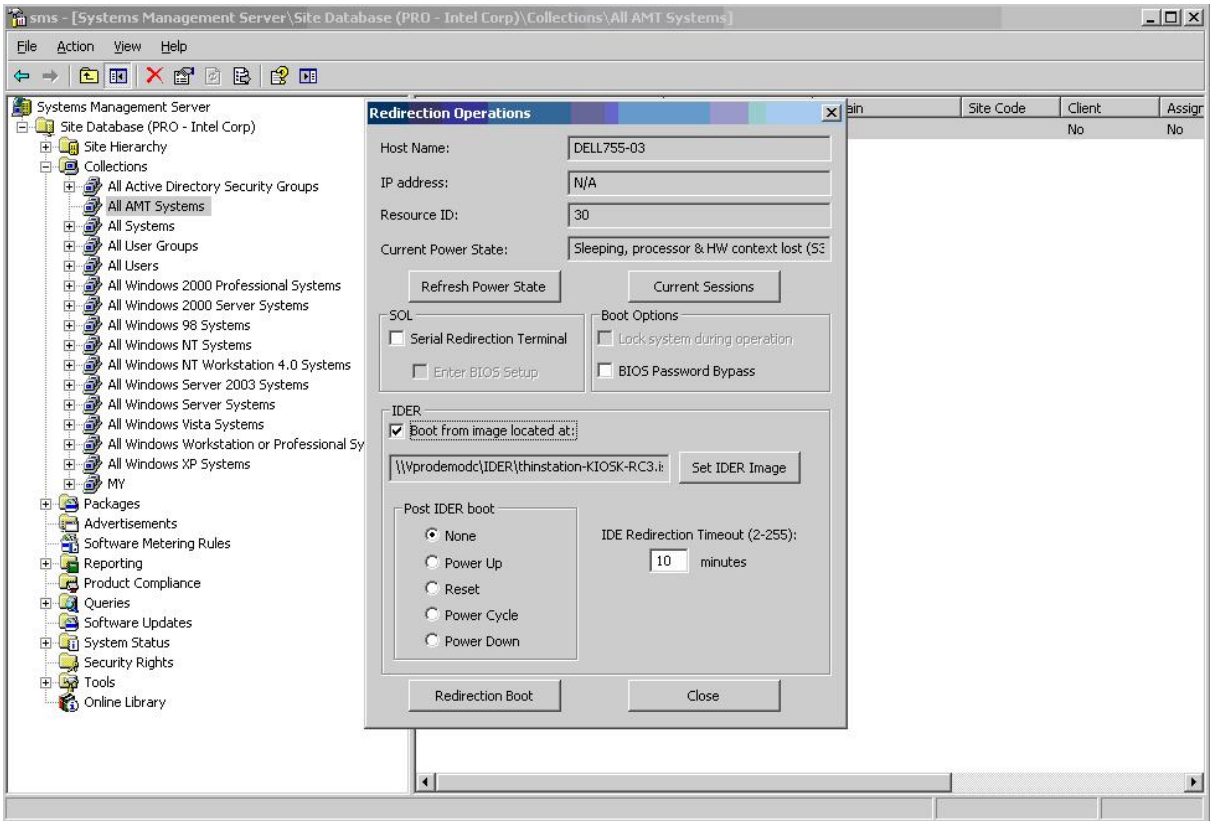


4. Modify or view the BIOS configuration as needed. When completed, Save/Ignore changes as needed. The system then reboots into normal operation.

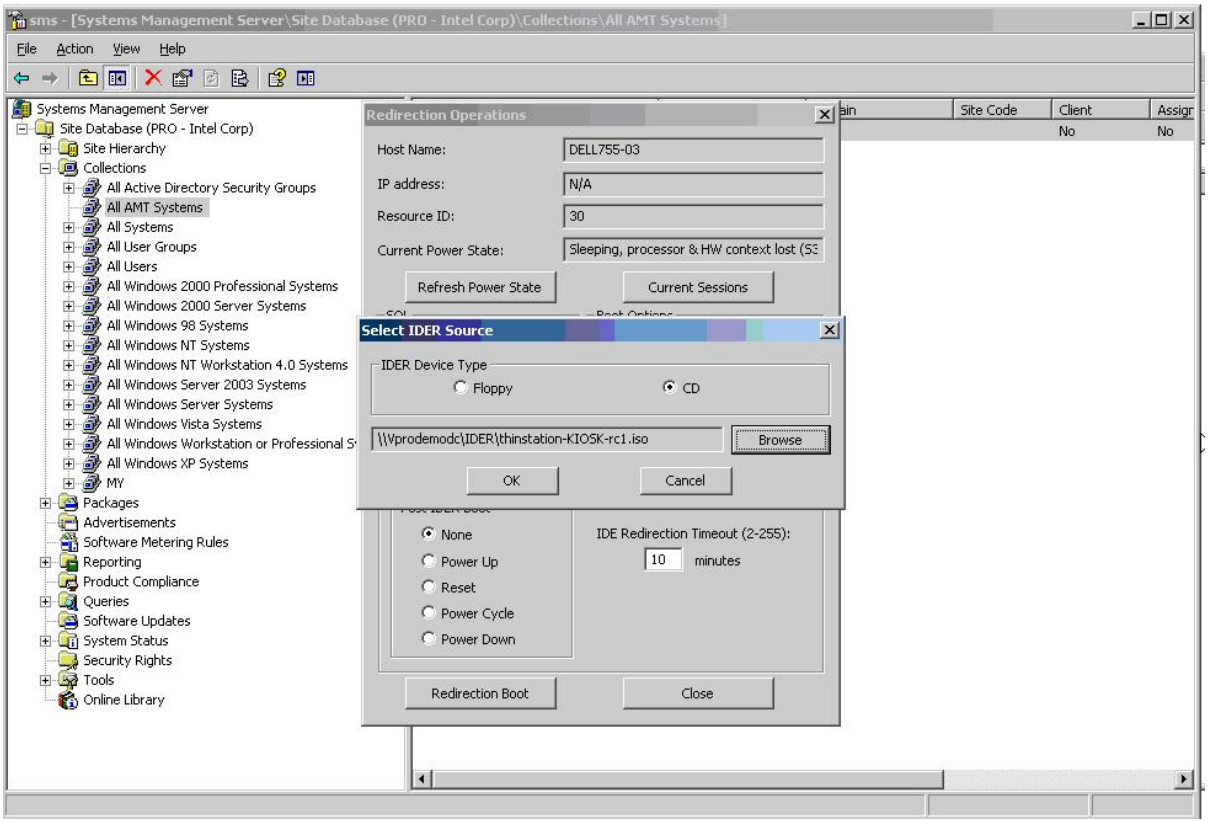


HOW TO: REMOTE BOOT (IDE-R)

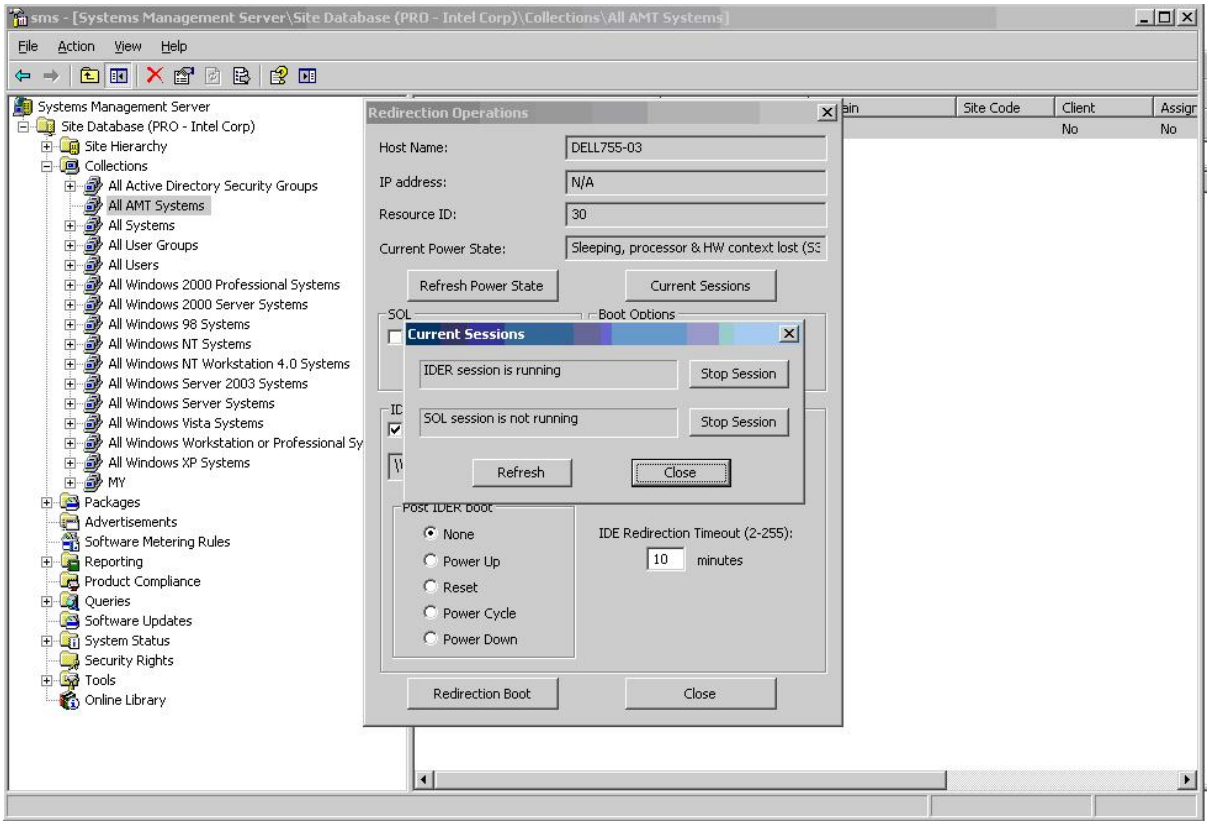
1. In the SMS Console select the PC with Intel vPro technology that requires a diagnosis operation. Right-click on the selected system in the right pane and select **All Tasks->Intel® AMT Tasks->Redirection Operations. Redirection Operations** windows pops up.



2. Check **Boot from image location at:** box. Press the button **Set IDER Image** and select the *.iso image file to use as an IDE-R source. Press **OK** and return to **Redirection Options** window.



3. Press the button **Redirection Boot.** AMT device starts booting from the selected image. To verify the status, press **Current Sessions** button. The IDE-R session can be stopped by pressing **Stop Session** and **Close** buttons.



Security: Timely isolation off the network

ACTORS:

1. **Workplace Administration and Operation Teams** are responsible for applying configuration updates to workplace endpoints.
2. **Network Security, Administration and Operation Teams** are responsible for defining policies which should be implemented by Workplace Administration Team
3. **Endpoint Threat Management team** is responsible for diagnostic and remediation of the end points exhibiting a suspicious worm-like behavior.

SCENARIO:

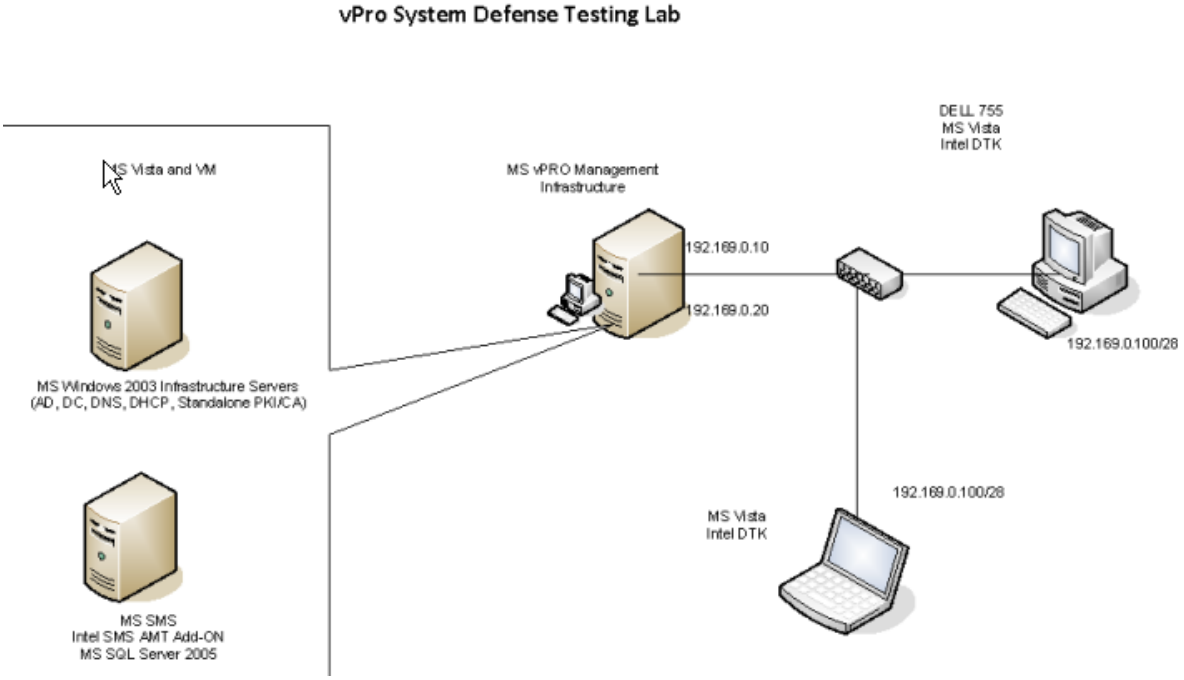
In certain situations a user's PC should be isolated from a corporate network in a timely manner. It may be a situation with a terminated employee or with a temporary unattended PC which is creating undesirable traffic on the network. Assuming control and isolating these PCs in a timely manner via corporate network may be a challenge.

SOLUTION:

System Defense provides a solution for isolating an endpoint from a corporate network by controlling it out-of-band (OOB), as long as this endpoint is powered on and connected to the network. Network Security or Workplace Administration and Operation teams should be capable to identify a targeted PC on the network, either by the machine name or by the source of malicious traffic. The Workplace Administration and Operation should be able to find that PC on the management console GUI and apply to it a System Defense policy which would deny at least any outbound network traffic. The isolation policy for this type of situations may be prepared and tested in advance. If the situation was related to a suspicious malicious behavior of that individual endpoint, that endpoint can be physically attended by the Endpoint Threat Management team for further investigation.

HOW TO IMPLEMENT SYSTEM DEFENSE POLICY

Network Lab Layout



Prerequisites

Network Lab Layout Infrastructure and SMS with AMT add-on servers	Microsoft Vista, VM with following virtual machines: Infrastructure (with DC, AD, DHCP, DNS SMS (with SMS server with the Intel Client Manageability Add-on, Microsoft SQL Server)
Managed vPro machine configured and managed within current infrastructure with Intel Client Manageability Add-on for Microsoft SMS.	Microsoft Vista, Intel Manageability Developer's Toolkit (DTK)
Test supporting client machine	Microsoft Vista, Intel Manageability DTK

Policy design

In Notepad or another text editor, prepare a policy file **SDP_UseCase1.sdp:**

##############

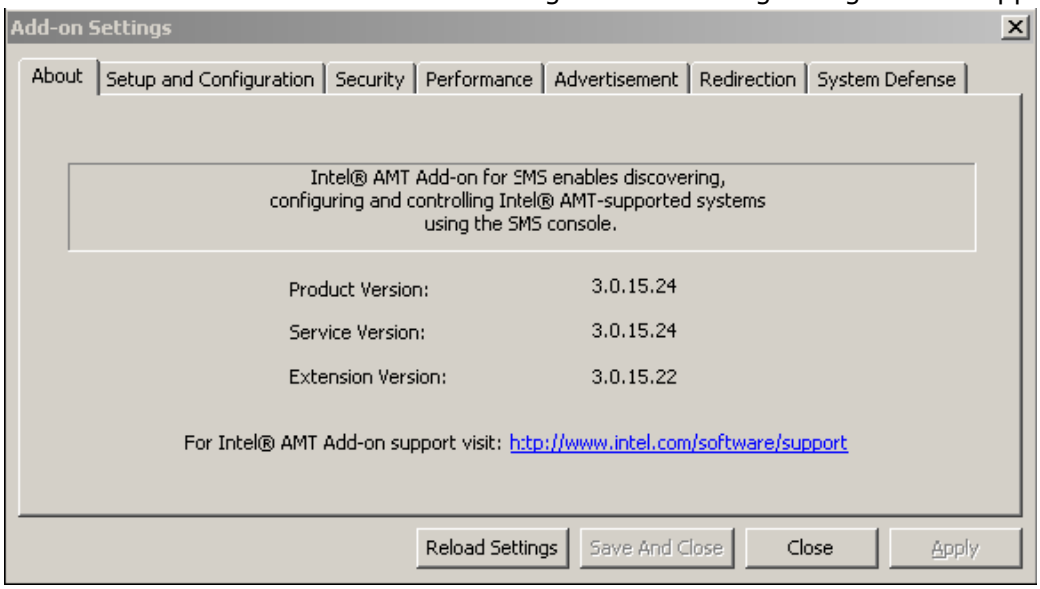
Version 3.0
#Manually Isolate a PC of enterprise network
Policy_Start
Policy_Type SDP

Policy_Name SDP_UseCase1
AntiSpoofing TRUE
#Allow ARP Protocol
permit Ethernet 2054
#Allow access to SMS Management Point (SMS Server) and Domain Controller
permit IP 192.168.0.20
permit IP 192.168.0.10
#Deny access to/from the rest of the systems
DefaultRxFilter Deny_all
DefaultTxFilter Deny_all
Policy_end

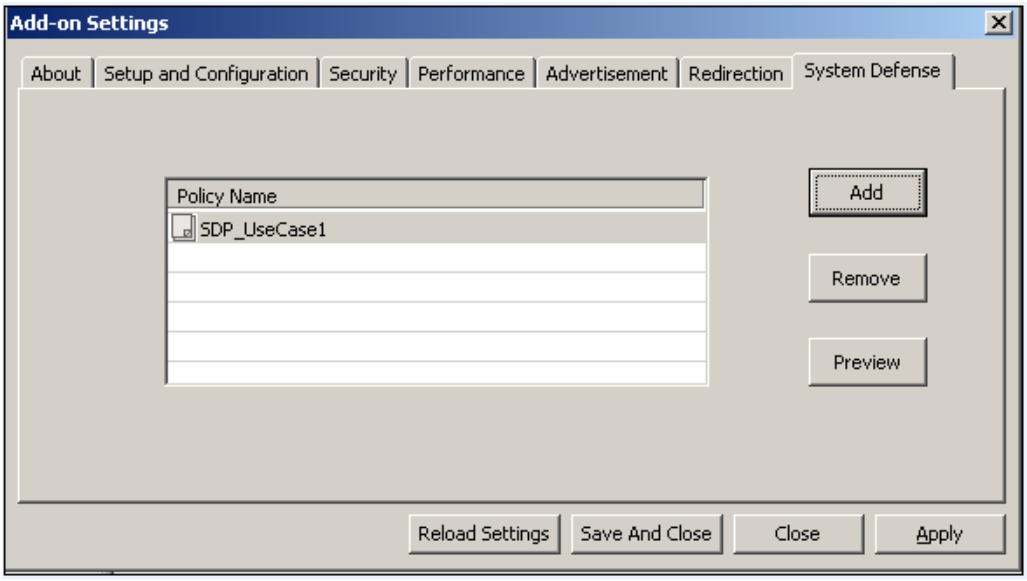
Policy Installation

1. Place the policy file in any directory on the server with the Intel Client Manageability Add-on for Microsoft SMS (it will be c:/systemdefense in this example).

2. Start the SMS Administrator Console and navigate to:
   System Management Server->Site Database (vPro - Intel Corp)->Collections->All Tasks->Intel AMT Tasks->Add on Settings. The following dialog box will appear:

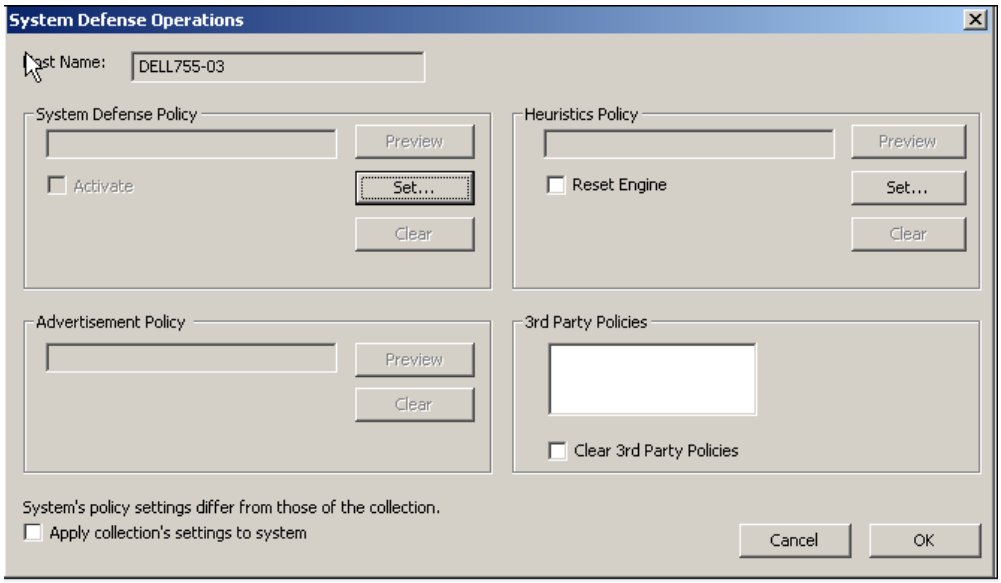


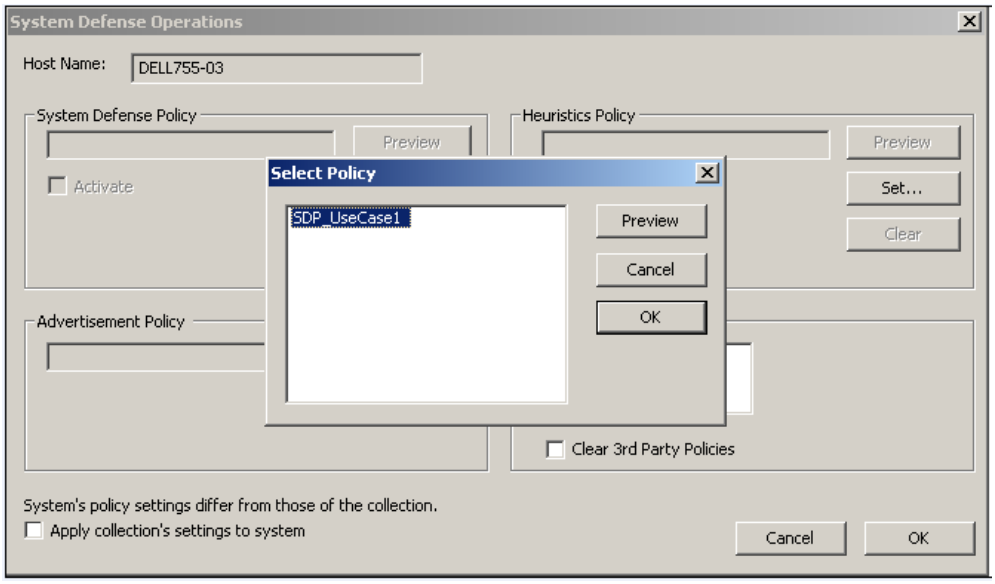
3. Select "System Defense" tab and click "Add." Navigate to the system defense policies directory (c:/systemdefense) and select the policy file Sdp_usecase1.sdp. Click "Apply."



4. In the SMS Administrator Console, navigate to the specific machine under test: Site Database (vPro - Intel Corp)->Collections->All AMT Systems->Dell755-03->All Tasks->Intel AMT Tasks->System Defense Operations.

5. In the dialog box, click "Set…" in the "System Defense Policy" section and select the policy SDP_UseCase1 which was loaded into SMS on the previous step.



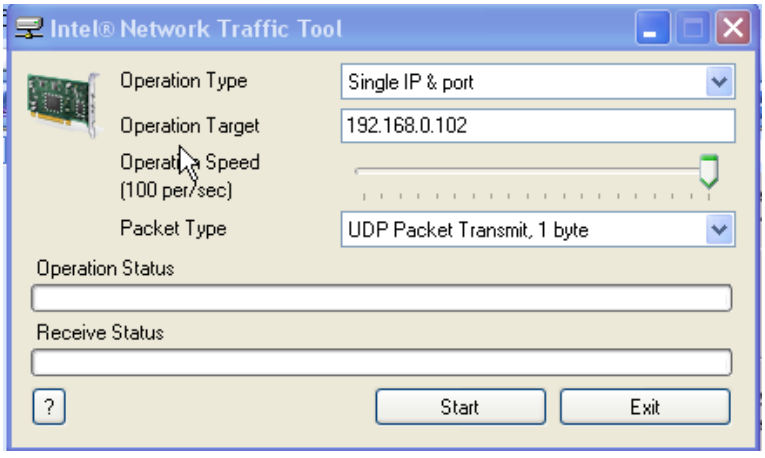


6. After "OK" the policy will be installed on the managed AFT device. It should essentially isolate this device from the network, leaving just access to/from SMS server.

Test

1. On the PC with Intel vPro technology (source) start the Intel Network Traffic Tool and set the Operation Target to the address of another client on the same test network. Click "Start." A green progress bar "Operation Status" should display

2. Start the same tool on the other machine (target), but do not press the "Start" button. Neither progress bar should be displayed, because currently the outgoing traffic from the source AMT machine is blocked by the applied policy (see Policy Design).



3. Open "System Defense Operations" by navigating within SMS Administration Console, as described above. Click "Clear" in the "System Defense Policy" section and then click OK. Shortly after that the green progress bar in the "Intel Traffic Tool" on the receiving PC will start moving, because the network isolation of the sender was removed when the policy was cleared.

Security: Patch Management isolation off the network

ACTORS:

1. **Workplace Administration and Operation Teams** are responsible for applying configuration updates to workplace endpoints.
2. **Network Security, Administration and Operation Teams** are responsible for defining policies which should be implemented by Workplace Administration Team
3. **Endpoint Threat Management team** is responsible for diagnostic and remediation of the end points exhibiting a suspicious worm-like behavior

SCENARIO:

When a serious vulnerability is disclosed and a corporation is making its efforts to obtain and apply a critical security patch, Workplace Administration along with Endpoint Threat Management teams may need to decide how to minimize the risk until the patch is really applied. Because of the nature of SMS and SCCM infrastructure, time interval between a critical patch package advertisement and its real installation may be significant. Some limited network isolation may be a compromise for this situation, but it should address the vulnerability as precise as possible and also should apply to each individual machine only until the critical patch is installed. Any network restriction applied to a machine should be lifted as soon as it is remedied. Intel® vPro System Defense for Advertisement, which works out-of-band, may help.

SOLUTION:

System Defense Policy (SDP) can be developed to partially isolate the machines waiting for a critical patch. System Defense for Advertisement integrates System Defense with System Management Advertisement. It applies the developed SDP to the machines which are receiving advertisements for security patch installation. So, the SDP isolates the systems according to the filters included in the SDP, until the patches are delivered, downloaded and installed.

HOW TO IMPLEMENT SYSTEM DEFENSE ON ADVERTISEMENT

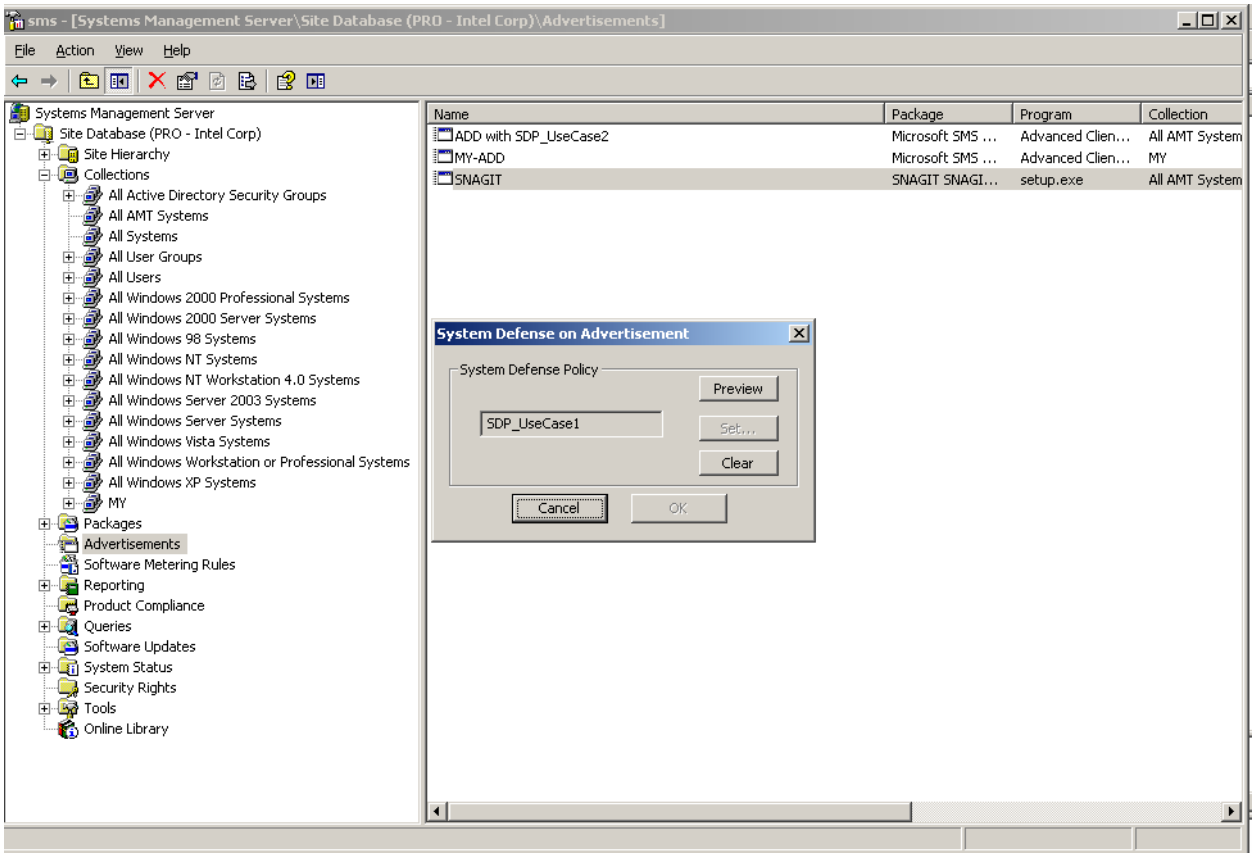
Network Lab Layout
Same as Use Case 1

Prerequisites
Same as Use Case 1

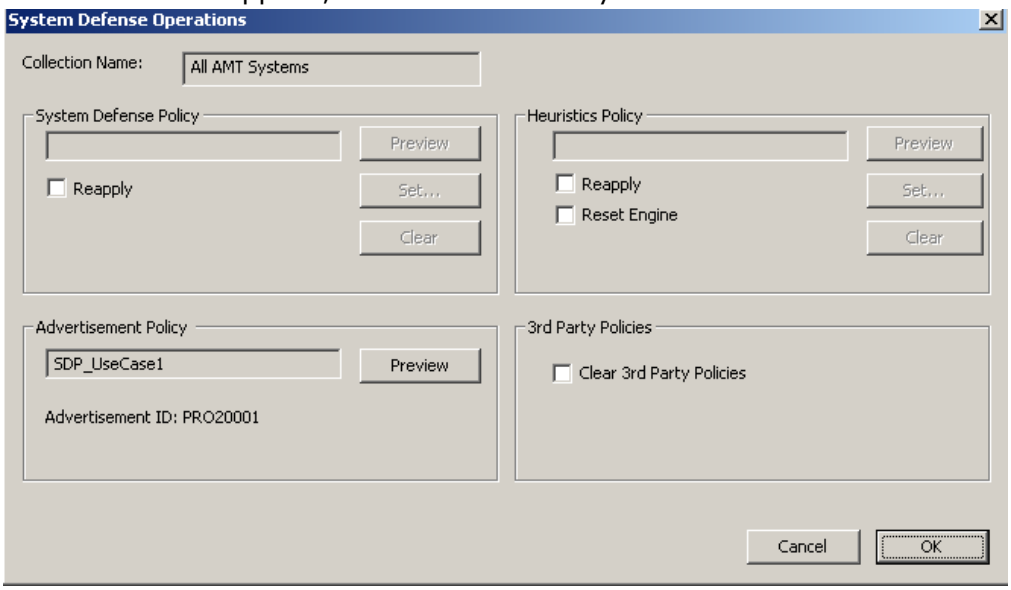
Policy design
Same as Use Case 1

Policy Installation

1. In the Advertisement windows of SMS Administrator Console, select the advertisement and navigate to All Tasks->Intel AMT Tasks ->System Defense Operations. In the dialog box (see below) press the "Set" button and select the policy SD_UseCase1, which was loaded into SMS at the beginning of the Use Case 1.



2. Press OK and the policy is applied to the advertisement. It will appear in the "Advertisement policy" field in of the "System Defense Operations" window for the collection it was applied, which is "All AMT Systems":



Test

Please see Test steps 1-2 for the Use Case 1.

Once the advertised package is installed – repeat steps 1-2. The result should duplicate the results of the step 3 for the Use Case 1