Save on IT costs by upgrading to new systems powered by Intel® Core™ vPro™ processors

Manage systems remotely to reduce help desk expenses

Many enterprises resist upgrading their users' notebooks. If the old ones still turn on, why spend money on new systems? Based on our investigation of three laptops, we have the answer: A newer laptop can decrease the burden on your IT staff, which can translate to savings for your company.

Here at PT, we examined a new laptop with a 6th generation Intel® Core™ vPro™ processor and two 7-year-old laptops: one with a 1st generation Intel Core vPro processor and one with a 1st generation Intel Core processor. We added all three laptops to a corporate management environment to learn how easy they were to manage. Compared to the older system without the Intel vPro platform technologies, the new laptop can dramatically reduce the time, effort, and cost for IT staff to perform everyday management tasks and resolve problems.

Whether your company was an early adopter of the Intel vPro platform or not, upgrading to new laptops with sixth-generation Intel Core vPro processors can translate to savings. In this report, we show you how.

Save on IT management costs

Solve problems remotely

Run updates remotely

Keep employee systems updated without hands-on work

Shut down systems faster

Quickly, remotely turn systems on and off

A key to savings: The Intel vPro platform

Available since 2006, the Intel vPro platform is a set of hardware and software technologies used for building business computers featuring Intel Core vPro processors. (For more information from Intel, visit intel.com/vpro.) Though we tested only laptops for this study, you can also purchase desktops powered by Intel Core vPro processors.

Via Intel® Active Management Technology (Intel® AMT), a key feature of the Intel vPro platform, 6th generation Intel Core vPro processors boast several features that can improve manageability and user experience, including:

- Keyboard Video Mouse Remote Control: Allows IT to run diagnostics, turn systems on and off, and perform other management tasks from anywhere with an Internet connection
- PC Alarm Clock: Enables IT to remotely schedule updates and patches for any time, even when the system is off
- Power Control: Allows IT to change the power state of a system remotely
- Inventory Collection: Allows IT to use a single console to track management statistics about any system they manage using Intel AMT
- Access Monitor: Shows IT who has logged into a system and from where

Optimize your IT budget with remote management

To avoid the expense of hiring IT professionals for every office, many businesses with multiple locations rely on a centralized IT staff. Without a remote management solution in place, however, this centralized model can introduce new challenges. When users at remote locations encounter tech problems, IT may have to physically travel to fix the issue. This can create enormous cost, delay, and downtime for the employee experiencing the problem. A 2011 Gartner study found that with a traditional dispatch approach, determining and resolving a single problem can cost $289 and take more than an hour.[1]

With the Intel vPro platform, your company has the potential to reduce the number of help desk calls that require travel. This can help cut costs, leaving more room in the budget for innovative new tools and investments.

Get "hands-on" with KVM

A key benefit of the Intel vPro platform is remote management via Intel Active Management Technology (Intel AMT). Remote management is enabled by an Intel AMT feature called Keyboard Video Mouse (KVM) Remote Control. KVM lets IT do more than take control of the user's screen: They can get fully "hands-on," going behind the operating system to access the system's pre-boot environment. This lets them run hardware diagnostics or change settings that are not accessible from within the operating system.

Because the KVM connection occurs at the hardware rather than the software level, it enables IT to connect to a laptop even when the operating system is unresponsive or someone has disabled the network adapter. This means that even if a system gets hit with a virus that disables or alters the operating system or other software, IT staff will still be able to access the laptop and figure out how to solve the problem.

Push updates and patches remotely with PC Alarm Clock

Another Intel AMT feature, PC Alarm Clock, allows IT to schedule updates and patches to run any time, even when a system is off. With this feature, IT can schedule a system in a remote location to turn on at a designated time, receive and install updates from a central server, and then shut down again.

This keeps the system up to date without interrupting the workday, which has several benefits for users and IT administrators alike:

- **Improves application performance:** Often, updates and patches can help applications work faster and more smoothly, which can help users be more productive.
- **Reduces power usage:** Users can turn off their systems at the end of the workday, and IT can turn them on remotely for an update if necessary. Without Intel AMT, IT may have been able to do some remote management tasks after hours, but only if users left their systems on.
- **Eases IT management burden:** PC Alarm Clock allows administrators to spend fewer midnight hours manually pushing updates, which improves their work-life balance and decreases costly overtime hours.
- **Helps secure your infrastructure:** Security best practices advise running updates and patches as quickly as possible, because sometimes they can fix security vulnerabilities in earlier versions of the OS or other software.

PC Alarm Clock was available on both systems based on the Intel vPro platform. However, the system without Intel AMT lacked this feature, meaning IT would have to manually install updates and patches. During busy periods, systems could languish for days or weeks without new software. Not only would that leave users without the latest and greatest application and OS versions, it could potentially make the systems more exposed to attack.

A key to savings: Avoid the cost of replacing failing components

The older a system, the closer its components are to failure. A 2013 Techaisle whitepaper claimed that small businesses spend 1.3 times as much money repairing systems that are over four years old as they do on systems that are less than four years old.[2] The paper reported that the number of repairs needed by systems over four years old increases every year, resulting in more lost revenue and lost hours of productivity.

In that paper, the systems greater than four years old would have been released in 2009 or earlier. The two older systems we tested were also released in 2009. If the businesses surveyed for that study were already spending dramatically more on maintaining their 2009 systems, can you imagine how much those companies would have to spend now if they were still using those systems today?

Upgrading to new laptops or desktops could be a great boon for these companies. Because newer systems typically require less frequent, less complex maintenance, they also require less time from IT and result in fewer hours of downtime for users, which can ultimately save money for the business.

Perform a graceful shutdown remotely

As part of our testing, we remotely turned on and logged into both of the systems with Intel AMT. We also performed a graceful shutdown on all three systems, doing so remotely on the laptops with Intel AMT. (A graceful shutdown is the equivalent of clicking "shut down" on a system rather than forcing a shutdown.) The new laptop shut down up to 18 seconds faster than the older ones. In addition, we had to be physically present next to the laptop without Intel AMT in order to shut it down. In the real world, that would mean that a system accidentally left on and unplugged all night would simply stay on until its battery ran out.

Though we did not test desktops, you can also purchase desktops with Intel AMT, which could offer similar benefits. Being able to remotely shut down desktops could translate to energy savings for your company, because IT could turn off any systems that users left on at night rather than letting them waste power during non-working hours

For both systems with Intel AMT, we performed a graceful shutdown by connecting to the system via a remote desktop protocol. But companies may choose to disable that feature for security reasons. Even if the remote desktop protocol is disabled, shutting down the new system with 6th generation processors is still significantly easier than shutting down the older system.

To shut down the older system, IT would have to log into the management console, connect to KVM, log into the target system, and click the shutdown button. In contrast, shutting down the newer system simply involves logging into the management console and sending the graceful shutdown command. The more time and effort your IT staff can save on these everyday tasks, the more time they can devote to resolving problems and developing new IT solutions.

A key to savings: Windows® 10

As Microsoft® Windows 7 phases out, many companies that have relied on it for years are considering alternatives. Windows 10 was "designed together" with 6th generation Intel Core processors, with features of each product built to enhance the other.[3] New features in Windows 10, such as Windows Hello and built-in touch functionality, can enhance your employees' workflows, and faster boot times can let users get to work faster, giving them more time for productivity.[4]

Keep close track of devices with Inventory Collection

Both of the laptops with Intel AMT supported Inventory Collection, which allows IT to track the device through a single management console. With this feature, IT can see things such as the OS version and the most recent updates, which can help them plan update schedules and other routine maintenance more effectively. This feature was not available on the older laptop without Intel vPro platform technologies. If a company's fleet of laptops did not have Intel AMT enabled, IT would have to examine each device individually to determine those characteristics.

Comply with security best practices

According to a 2016 study from IBM® Security and the Ponemon Institute, the average total cost of a security breach to an enterprise is $4 million, a 29 percent increase since 2013.[5] Cybersecurity Ventures predicts that the worldwide annual costs of cyber crime will rise to $6 trillion by 2021.[6] More than ever, your company can't afford to drop its guard.

Investing in Intel vPro platforms and activating Intel AMT can be one step toward improving your security and avoiding an expensive breach. For example, Intel AMT requires all traffic between the laptop and the IT management console to be encrypted via Transport Layer Services (TLS). Additionally, Intel vPro platforms with Intel AMT enabled offer the Access Monitor feature, which allows IT to see who has logged into a system and where the login occurred. If a widespread security issue (or other problem) originated at a specific system, this feature could help IT to find the person responsible by learning who logged into that system. Alternatively, if a laptop or desktop were recovered after loss or theft, IT could determine whether someone had logged in and had the opportunity to steal information.

Quick problem resolution gets users back to work faster

Your employees rely on their laptops and desktops. When technical problems arise, their productivity declines or halts altogether until the issue is fixed. Gartner found that when companies use a traditional dispatch approach to IT problem-solving, end-users can lose over three hours of productivity per help desk call.[7] According to the Gartner study, a traditional approach might result in 3.25 hours of lost productivity, whereas utilizing a CompuCom and Intel vPro platform solution could reduce the average incident productivity loss to only 5.3 minutes.[7] As every company knows, hours of lost productivity can lead to lost revenue.

Conclusion

Inevitably, your IT staff will need to spend some amount of time performing routine device maintenance and management and helping users solve problems. But the less time they spend on those tasks, the more time and energy they have to initiate new IT projects that can help your company boost its efficiency and revenue. With remote management via Intel AMT, IT can resolve more issues without leaving their desks, reducing the time and expense associated with travel.

In our research, we also found significant benefits to choosing a system with 6th generation Intel Core vPro processors over an older system. Both of the systems based on the Intel vPro platform offered features that can help improve security and boost productivity at your organization, but the newer system was significantly faster at a graceful shutdown and offered unique compatibilities with Windows 10. If you've been putting off your PC upgrade, today may be the day to start planning. Consider a new system powered by Intel Core vPro processors to gain the remote management capabilities that can help you save money across your organization.

---

1 Gartner, Benchmarking Hardware Support Operations North America, 2011. (as cited in: https://www.compucom.com/sites/default/files/CompuCom-ClientLink-EU-Orchestrator-Powered-by-Intel.pdf)

2 http://i.crn.com/custom/WhitePaper_AgeingPCEffect.pdf

3 http://www.theverge.com/2015/9/1/9238379/intel-skylake-launch-ifa-2015-kirk-skaugen-interview

4 http://www.principledtechnologies.com/Microsoft/Windows_10_upgrade_boot_0815.pdf

5 http://www-03.ibm.com/security/infographics/data-breach/

6 http://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

7 Gartner, Benchmarking Hardware Support Operations North America, 2011. (as cited in: https://www.compucom.com/sites/default/files/CompuCom-ClientLink-EU-Orchestrator-Powered-by-Intel.pdf)

On February 29, 2017, we finalized the hardware and software configurations we tested. Updates for current and recently released hardware and software appear often, so unavoidably these configurations may not represent the latest versions available when this report appears. For older systems, we chose configurations representative of typical purchases of those systems. We concluded hands-on testing on March 3, 2017.

Appendix A: System configuration information

System	Dell™ Latitude E6410 with 1st generation Intel Core vPro processor	Dell Latitude E6410 with 1st generation Intel Core processor	Dell Latitude E7470 with 6th generation Intel Core vPro processor
Processor			
Vendor	Intel	Intel	Intel
Name	Core	Core	Core
Model number	i5-560M	i5-560M	i5-6300U
Core frequency	2.66 GHz	2.66 GHz	2.40GHz
Number of cores	2	2	2
Cache	3 MB L3	3 MB L3	3 MB L3
Memory			
Amount	4 GB	4 GB	16 GB
Type	DDR3	DDR3	DDR4
Speed (MHz)	1,333	1,333	2,133
Integrated graphics			
Vendor	Intel	Intel	Intel
Model number	HD Graphics	HD Graphics	HD Graphics 520
Storage			
Amount (GB)	250	250	180
Type	Spindle	Spindle	SSD
Connectivity/expansion			
Wired internet	Intel 82577LM Gigabit	Intel 82577LM Gigabit	Intel I219-LM
Wireless internet	Intel Centrino® Advanced-N 6200 AGN	Dell DW1501 Wireless-N	Intel 8260 Dual Band Wireless-AC
Bluetooth	N/A	N/A	4.0
USB	4 x 2.0	4 x 2.0	3 x 3.0
Video	1 x VGA	1 x VGA	1 x HDMI® 1 x Mini DisplayPort
Battery			
Type	Lithium-polymer	Lithium-polymer	Lithium-polymer
Size	6 cell	6 cell	3 cell

System	Dell™ Latitude E6410 with 1st generation Intel Core vPro processor	Dell Latitude E6410 with 1st generation Intel Core processor	Dell Latitude E7470 with 6th generation Intel Core vPro processor
Rated capacity (Wh)	60	60	42
Display			
Size (in.)	14.1	14.1	14.0
Type	WXGA+ Anti-Glare LED	WXGA Anti-Glare LED	FHD Anti-Glare LCD
Resolution	1440 x 900	1280 x 800	1920 x 1080
Touchscreen	No	No	No
Operating system			
Vendor	Microsoft	Microsoft	Microsoft
Name	Windows 7 Professional x64 SP1	Windows 7 Professional x64 SP1	Windows 10 Pro
Build number or version	6.1.7601	6.1.7601	10.0.14393
BIOS			
BIOS name and version	Dell A16	Dell A16	Dell 1.12.3
Dimensions			
Height (in.)	1.20	1.20	0.76
Width (in.)	13.20	13.20	13.19
Depth (in.)	9.40	9.40	9.13
Weight (lbs.)	4.26	4.26	3.13

Appendix B: How we tested

Our environment included a preexisting Active Directory® virtual machine (VM) and a second VM with Microsoft System Center Configuration Manager (SCCM) server as a management VM. We also included a third VM as a root certificate authority. All 3 VMs used Windows Server® 2012 R2 Datacenter Edition and were joined to our local domain.

Configuring the management server to provision vPro processor-powered systems

Creating Active Directory accounts for Intel AMT provisioning

1. Log into the Domain Controller using the domain\administrator account.
2. Open Active Directory Administrative Center.
3. Under test(local), click New→Group.
4. On the Create Group window, for Group name, use Kerberos Admins; for Group type, use security.
5. Add Kerberos Admins as a member of the Domain Admins group.
6. Add the computer account of the SCCM server to the Kerberos Admins security group.
7. Create an Organizational Unit for AMT managed systems. We used `AMT`
8. Create a security group called `AMT`
9. Add the Kerberos Admins group to the AMT security group.

Creating certificate templates for out-of-band (OOB) management

1. Log into Certificate Authority as domain\administrator.
2. Click Start→Administrative Tools→Certification Authority.
3. Right-click test-CA-CA, and click Properties.
4. On the General tab, click View Certificate.
5. On the Details tab, scroll to and select Thumbprint. Copy the 40-character code displayed in the details. You will add this information to the AMT BIOS later.
6. To close the Certificate Authority properties, click OK.
7. Expand the Certification Authority, and select Certificate Templates.
8. Right-click Certificate Templates, and select Manage.
9. Locate Web Server in the list of available certificate templates. Right-click the template, and select Duplicate Template.
10. Select Windows 2003 Enterprise, and click OK.
11. Change the template name for the AMT Provisioning certificate. We used `AMT Provisioning`.
12. On the Subject Name tab, select Build from this Active Directory Information. Select Common Name, and choose the option UPN.
13. On the Security tab, add the security group created for the SCCM site server. We used the Kerberos Admin group. Add the Enroll permission for the security group. Ensure Domain Admins and Enterprise Admins have Enroll permissions.
14. On the Extensions tab, select Application Policies, and click Edit.
15. Click Add. Click New. Type `AMT Provisioning` for the name, and `2.16.840.1.113741.1.2.3` as the Object Identifier. Click OK.
16. Ensure AMT Provisioning and Server Authentication are listed, and click OK.
17. To close the template properties, click OK.
18. Right-click the AMT Web Server Certificate template, and select Duplicate Template.
19. Select Windows 2003 Enterprise, and click OK.
20. Change the template name for the AMT Web Server Certificate. We used `AMT Web Server Certificate Template`
21. On the General tab, choose the option Publish Certificate in Active Directory.
22. On the Subject Name tab, select Supply in the request.
23. On the Security tab, ensure Domain Admins and Enterprise Admins have Enroll permissions.
24. To close the template properties, click OK.
25. In Certification Authority, navigate to Certificate Templates.
26. For both the AMT Provisioning Template, and the AMT Web Server Certificate Template, repeat the following steps:
    a. Right-click the central panel, and select New→Certificate Template to Issue.
    b. Select the AMT Provisioning Template.
    c. Click OK.
27. Log into the management server as domain\administrator.
28. Click Start→Run. Type `mmc`, and press Enter.
29. In the mmc console, click File→Add/Remove Snap-in…
30. Select Certificates, and click Add. Select Computer account. Click Next.
31. Select Local computer, and click Finish.
32. Click OK.
33. Expand Certificates (Local Computer)→Personal→Certificates.

34. In the right panel, click More Actions→All Tasks→Request a new certificate…
35. Click Next.
36. Accept the defaults, and click Next.
37. Select the new AMT Provisioning certificate. Click Enroll.
38. Click File→Add/Remove Snap-in…
39. Select Certificates, and click Add. Select Computer account. Click Next.
40. Select My user account, and click Finish.
41. Click OK.
42. Expand Certificates→Personal→Certificates.
43. In the right panel, click More Actions→All Tasks→Request a new certificate…
44. Click Next.
45. Accept the defaults, and click Next.
46. Select the new AMT Provisioning certificate. Click Enroll.
47. Click File→Add/Remove Snap-in…
48. Select Certificates, and click Add. Select My user account. Click Next.
49. Select Local computer, and click Finish.
50. Click OK.
51. Expand Certificates – Current User→Personal→Certificates.
52. From Certificates (Local)→Personal→Certificates, click and drag the certificate created using the AMT Provisioning template into Certificates – Current User→Personal→Certificates.
53. Click Close.

Installing Intel Setup and Configuration Software (SCS) 11.1

1. Download IntelSCS_11.1.zip from https://downloadcenter.intel.com/download/26505.
2. Extract the contents to C:\IntelSCS_11.1.
3. Browse to C:\IntelSCS_11.1\IntelSCS\RCS.
4. Run IntelSCSInstaller.exe.
5. At the Welcome screen, click Next.
6. Select I accept the terms of the license agreement, and click Next.
7. Check the Boxes for Remote Configuration Service (RCS), Database Mode, and Console.
8. Enter the credentials of the Domain account that will run the service. We used `test.local\administrator`. Click Next.
9. Select db.test.local as the location for the SCS database. This information may populate automatically. Select Windows Authentication, and click Next.
10. On the Create Intel SCS Database pop-up, click Create Database.
11. On the confirmation screen, click Close.
12. On the confirmation screen, leave the default Installation Folder, and click Install.
13. Once the installation is complete, click Next.
14. Click Finish.

Installing the provisioning certificate

1. Open MMC, and add the certificates snap-in, targeted at the local computer.
2. Navigate to Personal, Certificates.
3. Right-click the AMT Provisioning Certificate, and choose Open.
4. On the Details tab, click Copy to file.
5. On the Welcome screen, click Next.
6. On the Export Private Key screen, choose Yes, export the private key, and then choose Next.
7. On the Export File Format screen, check the boxes for Include all certificates in the certification path if possible and Export all extended properties. Click Next.
8. On the Password screen, enter a password to protect the private key.
9. On the File to Export screen, enter `C:\Install_Files\scs-prov-cert.pfx`, and click Next.
10. On the Completed screen, click Close.
11. From an elevated command prompt, run the following command:
```
RCSutils.exe /Certificate Add c:\Install_Files\scs-prov-cert.pfx  /RCSuser NetworkService net stop rcsserver && net start rcsserver
```
12. To verify, run the following command, and make sure the expected certificate is listed:
```
RCSUtils.exe /certificate view /RCSuser NetworkService /log file C:\rcsout.txt
```

Setting up AMT provisioning with Intel SCS Remote Configuration Service

Creating the configuration profile

1. On the management server, launch the Intel Setup and Configuration Console.
2. Click Profiles.
3. To construct a profile for deployment, click New.
4. For Profile Name, enter a description of the target clients. We used `inteltest`. Click OK.
5. On the Getting Started Screen, choose Configuration / Reconfiguration.
6. On the Optional Settings screen, choose the options Active Directory Integration, Access Control List (ACL), and Transport Layer Security (TLS), and click Next.
7. On the AD Integration screen, browse for the OU created for the AMT managed devices. We used OU=AMT, DC=test, DC=local. Check the box for Always use host name, and click Next.
8. On the Access Control List screen, click Add.
9. Select Active Directory User/Group. Click Browse.
10. Add Kerberos Admin, Domain Admins, or other administrative users groups. Click OK.
11. For Access Type, select Remote.
12. Choose the option for PT Administration. Click OK.
13. Click Next.
14. On the TLS screen, from the drop-down menu, select the Enterprise Certificate Authority, ca.test.local.
15. Select the Server Certificate Template to be used to generate certificates for the AMT devices. We selected AMTWebServerCertificate. Click Next.
16. On the System Settings screen, choose the options Web UI, Serial Over LAN, IDE Redirection, and KVM Redirection.
17. Select Use the following password for all systems. Enter the password for use after provisioning is complete. We used `P@ssw0rd`
18. Click KVM Settings…
19. Enter the RFB Password for KVM sessions. We used `P@ssw0rd`
20. Enter the MEBX password. We used `P@ssw0rd`
21. Uncheck User Consent required before beginning KVM session, and click OK.
22. Choose the options Enable Intel AMT to respond to ping requests and Enable Fast Call for Help (within the enterprise network).
23. To Edit IP and FQDN settings, click Set.
24. In the Network Settings window, select Use the following as the FQDN, and choose Primary DNS FQDN from the drop-down menu.
25. Choose the option that indicates the device and the OS will have the same FQDN (Shared FQDN).
26. Select Get the IP from the DHCP server.
27. Select Update the DNS directly or via DHCP option 81. Click OK.
28. Click Next.
29. Click Finish.

Adding the configurator to a shared folder

1. Create a shared folder called `amtshare`
2. Copy the file at C:\IntelSCS_11.1\IntelSCS\Configurator to the shared C:\amtshare folder.

Configuring the clients

Repeat these steps for each system.

Reserving an IP address in DHCP

1. On the Domain Controller, run dhcpmgmt.msc.
2. Expand FQDN→IPv4→Scope, and click Reservations.
3. Click More Actions, and click New Reservation.
4. For Reservation Name, enter the host name of the target client.
5. Enter an IP address to reserve.
6. Enter the MAC address of the target client's Ethernet port.
7. Click Add.

Configuring policy on the target client

1. Log onto the target client using domain\administrator.
2. Download and apply applicable driver packages from the manufacturer's website.
3. Open Windows Firewall with Advanced Security.
4. Click Firewall Properties.
5. On the Domain Profile, Private Profile, and Public Profile tabs, set the Firewall state to Off. Click OK.
6. Set the host name and IP of each virtual machine as described above.
7. Run lusrmgr.msc.
8. Select Groups.
9. Right-click Administrators, and click Properties.
10. Click Add.
11. Select Object Types, check the box for Computers, and click OK.
12. Disable the wireless adapter.

Installing AMT tools on the management server

Installing the Manageability Commander Tool Mesh Edition

1. On the management server, download the tool from the following link: http://www.meshcommander.com/ManageabilityDeveloperToolKit.msi.
2. Run the installer, and complete using all defaults.

Adding systems to the Manageability Commander Tool Mesh Edition

1. Open the Manageability Commander Tool Mesh Edition.
2. Click File, then Add, then Add Intel AMT Computer…
3. Enter the FQDN, Username and Password for the target computer.

Installing the Intel Manageability Commander

1. Download the tool from the following link: https://downloadcenter.intel.com/download/26375/Intel-Manageability-Commander.
2. Run the installer, and complete using all defaults.

Adding systems to the Intel Manageability Commander

1. Open the Intel Mangeability Commander.
2. Click File, then Add Intel AMT Computer…
3. In the Add Computer Window, give the computer a friendly name.
4. Enter the FQDN of the target system.
5. For Auth/Security, select Digest/TLS. Enter the username and password for the target device.

Installing certificates on target systems

1. On each target system, during boot, press Ctrl + P to enter the Intel Management Engine BIOS Extension.
2. Enter the Intel ME Password. The default is admin.
3. Navigate to Intel ME General Settings, Remote Setup and Configuration, TLS PKI, and select Manage Hashes.
4. Hit the insert key to Add a certificate hash.
5. Enter a name for the hash.
6. Enter the 40 character thumbprint recorded before.
7. Exit the MEBx menu.

Running our tests

Provisioning Intel AMT

1. Start the timer.
2. Log into the target system.
3. Navigate to the amtshare folder on the configuration server, and copy the Configurator folder onto the desktop.
4. Open the target folder.
5. Click File, navigate to Open command prompt, then click Open command prompt as Administrator.
6. Run the following command in the elevated command prompt:
```
ACUConfig.exe /Verbose /Output console ConfigViaRCSOnly cm.test.local inteltest
```
7. Stop the timer.

Performing a graceful shutdown

Note: All computers start powered on and at the login screen.

Latitude E6410 (without AMT)

1. Start the timer.
2. At the target computer, enter the login name and password.
3. Once on the desktop, open the start menu and select Shutdown.
4. Once the desktop is visible, click start and select shutdown.
5. Stop the timer when the system displays "Shutting Down..."

Latitude E6410 (with AMT)

1. Start the timer
2. From the management server, open the Intel Manageability Commander.
3. Select the target system, and click Connect.
4. Select Remote Desktop.
5. Click Connect.
6. Click Ctrl+Alt+Delete.
7. Enter the login name and Password.
8. Once on the desktop, open the start menu, and select Shutdown.
9. Stop the timer when the system displays "Shutting Down..."

Latitude E7470 (with AMT)

1. Start the timer.
2. From the management server, open the Intel Manageability Commander.
3. Select the target system, and click Connect.
4. On the System Status tab, click power Actions…
5. In the Power Actions window, select Soft-off.
6. Click OK.
7. Stop the timer.

Logging into the systems

System without AMT

1. Start the timer.
2. At the target computer, enter the login name and password.
3. Stop the timer when the desktop is visible.

vPro processor-powered systems

1. Start the timer
2. From the management server, open the Intel Manageability Commander.
3. Select the target system, and click Connect.
4. Select Remote Desktop.
5. Click Connect.
6. Click Ctrl+Alt+Delete.
7. Enter the login name and password.
8. Start the timer once the desktop is visible.

Updating during off hours using PC Alarm Clock on vPro processor-powered systems

In order to complete this test, we used our existing SCCM server to host and deploy updates. Using the PC Alarm Clock function, we then booted the system before applying the patch.

1. On the configuration server, open the Manageability Commander Tool Mesh Edition.
2. On the connection tab, select the target system, and click Connect.
3. On the Management Engine tab, click the button next to Alarm Clock.
4. In the Alarm Window, check the box for Enable Automatic Wakeup, and enter a time.
5. Select Enable Recurring Alarm, and set the time to 1 day.

Viewing system information via Access Monitor on vPro processor-powered systems

1. On the configuration server, open the Manageability Commander Tool Mesh Edition.
2. On the connection tab, select the target system, and click Connect.
3. Select the Hardware Information tab to view a system's Hardware Information.

Viewing system information via System Inventory on vPro processor-powered systems

1. On the configuration server, open the Manageability Commander Tool Mesh Edition.
2. On the connection tab, select the target system, and click Connect.
3. Select the Audit Log tab to view the Access Monitor Log.

This project was commissioned by Intel Corp.

Facts matter.®