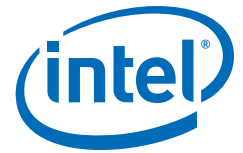


White Paper and ROI Study

Intel® Core™2 Processor with vPro™ Technology

Office of Technology, State of Indiana

Government



State of Indiana achieves ROI of 405% by improving patching for wired and wireless PCs through Microsoft SCCM* enabled by Intel® vPro™ Technology



The State of Indiana's IT division, the Indiana Office of Technology (IOT),¹ has been deploying both laptops and desktop PCs with the Intel® Core™2 processor with vPro™ technology² in an environment managed by Microsoft SCCM*. IOT found that Intel® vPro™ technology enabled remote patching of desktop PCs, even for PCs that were powered off at the start of the patch cycle. Because SCCM supports Intel vPro technology, IOT can now remotely power up PCs (via the built-in Intel vPro technology power-up/down capability), patch the systems, then power the systems back down. Recently, IOT also began deploying laptops with Intel vPro technology. IOT then investigated the return on investment (ROI) from using Intel vPro technology to enable improved patching on both wired and wireless PCs. Results of the investigation showed a break-even point in year 2, with a projected positive ROI of 405% over 5 years, and projected savings of over \$117,000.³

Author: Manoj Punamia
Advanced Technical Sales, Intel Corporation

Author: Mohan Veeramachaneni
Advanced Technical Sales, Intel Corporation

Author: Kam Lee
Advanced Technical Sales, Intel Corporation

Table of Contents

Remote patching for wireless laptops, via Microsoft SCCM,* enabled by Intel® vPro™ technology	3
Activating Intel vPro technology in the wireless environment	3
Configure the environment to support wired and wireless PCs	4
Configuring the 802.1x network for Intel AMT.....	4
Supporting Microsoft SCCM patch advertisement.....	4
Turning off the wake-on-LAN (WOL) in Intel AMT.....	4
Configuring pre-logon wireless profile for laptops	4
ROI study in production environment: Projected 405% positive ROI in 5 years	5
TCO/ROI investigation.....	6
Positive results	6
More Information	7

Executive Summary

Over the past two years, the State of Indiana's IT division, the Indiana Office of Technology (IOT),¹ has been deploying desktop PCs with Intel® Core™2 processor with vPro™ technology² to improve remote patching. Recently, IOT expanded remote patch management into their wireless environment by deploying laptops with Intel® vPro™ technology. IOT then investigated the benefits of using a management application, Microsoft SCCM,* enabled by Intel vPro technology, to remotely patch even wireless laptops that are powered off at the start of the patching cycle. Results of the investigation show that remote patching of wireless laptops can significantly reduce the number of patch failures and cut the IT time typically spent on desk-side resolution of patch issues. In turn, these factors accelerate the time to patch saturation. Based on the results of their study, IOT projects a break-even point in year 2, with a projected positive ROI of 405%, and projected cumulative savings of over \$117,000 within 5 years.³ IOT expects that implementing other features of Intel vPro technology for wired and wireless PCs could deliver additional benefits as well, including faster problem resolution and less user downtime.

Remote patching for wireless laptops, via Microsoft SCCM,* enabled by Intel® vPro™ technology

State of Indiana successfully implements remote patching in a wireless environment, speeds up patching, and increases the patch saturation target to 97% saturation within hours instead of days.

One of the highest priorities for information technology (IT) administrators is security. With an increase in off-hours work and an increasingly mobile workforce, securing mobile assets is more important than ever. However, delivering remote services to both wired and wireless PCs is challenging. Users often forget to leave PCs powered up, and leave laptops connected to AC power and the network to allow remote updates and patching. For organizations that serve large geographic areas, it is even more critical to be able to remotely secure systems reliably and quickly without requiring costly on-site services.

The State of Indiana governs an area of over 36,000 square miles, with a population of about 6.2 million residents.¹ The state manages state offices and agencies, natural resources, parks, museums, memorials, and universities. The state's IT division, the Indiana Office of Technology (IOT), provides PC management and support services for the state's assets. Currently, the state operates approximately 28,000 PCs in 80 executive branches. About half the PCs are deployed in campuses with local IT support. The other 14,000 PCs are distributed across over 600 remote locations. IOT manages about 90% of the PCs, of which approximately 18,000 are desktop systems and 7,200 are laptops.

Because the PCs are used to provide critical services for residents, IOT priorities include:

- Protecting assets by improving security
- Increasing reliability and saturation of patch deployment
- Reducing site visits
- Minimizing user disruptions from patching

However, the state's large number of remote sites makes it expensive and time-consuming to travel to the 600 remote sites to manage assets, whether desktop PCs or laptops.

Over the past two years, IOT has been deploying desktop PCs with the Intel® Core™2 processor with vPro™ technology to enable better remote patching and improve service efficiencies. IOT has been using the remote power up/down capability of Intel® vPro™ technology to allow remote patching even for PCs that are powered off at the start of the patch cycle.

Recently, IOT deployed and activated laptops with Intel vPro technology to support remote patching in the State of Indiana's wireless network environment. Like desktop PCs with Intel vPro technology, the laptops have built-in capabilities that allow remote patching, even if a wireless laptop is powered off at the start of the patch cycle. IOT can now patch laptops automatically and reliably – in a wireless environment – as long as users leave their laptops in the office connected to A/C power once a week.

With both desktop and laptop PCs enabled for remote patching regardless of power state, IOT was able to eliminate virtually all deskside visits typically required for patching and increase the patch success rate from 80% to 97%.³ IOT has already realized a positive ROI, and is projecting a total positive ROI of 405% across 5 years.³

Activating Intel vPro technology in the wireless environment

IOT worked with Intel to deploy the Intel vPro technology capabilities in their wireless environment, and to activate the capabilities with their existing management application, Microsoft SCCM.*

IOT faced key challenges in deploying and activating Intel vPro technology in their wireless environment. First, IOT had to adapt their infrastructure to allow remote management of wired and wireless PCs. In order to do that, IOT had to match authentication protocols for firmware (deep, in-system communication) with an authentication system configured only for OS-level communication. This discussion explains their solution to matching authentication protocols.

IOT enabled Intel® Active Management Technology⁴ (Intel® AMT) for the wireless infrastructure by resolving challenges in these areas:

- Configuring the 802.1x network for Intel AMT
- Supporting Microsoft SCCM patch advertisement
- Turning off wake-on-LAN in Intel AMT
- Configuring pre-logon wireless profile for laptops

IOT continued to use the WPA2/AES-CCMP wireless encryption for access points, which is supported by Intel AMT, and so required no change to the infrastructure.

Configure the environment to support wired and wireless PCs

Remote manageability of PCs with Intel vPro technology requires that the systems be provisioned with Intel® AMT, and the IT infrastructure configured to support Intel AMT. Laptop and desktop PCs require different infrastructure configurations. One of the differences is that wireless laptops rely heavily on wireless LAN (WLAN/802.11) to maintain dynamic links with access points, and rely on 802.1x for WLAN link security.

Configuring the 802.1x network for Intel AMT

The key challenge in configuring the 802.1x network was in matching authentication protocols. IOT uses the 802.1x standard for layer-2 authentication for wireless users who request access to the network. 802.1x security is based on credentials using either the machine name and/or user credentials (username and password). Intel AMT version 3.0 and up supports 802.1x with various EAP methods. Intel AMT communication occurs “below” the OS, in system firmware, and requires robust security schemes. All but one of the Intel AMT protocols require a client certificate to secure Intel AMT communication to and from the PC.

Before deploying Intel AMT, IOT used EAP-FAST Radius protocol for 802.1x. EAP-FAST is flexible protocol that allows authentication by either client certificate or username/password. The IOT configuration of the Radius server used username/password authentication, without requiring certificates. In this configuration, the mobile user connects to the access point. The EAP-FAST protocol verifies authentication, and passes the Windows-cached username and password to the Cisco Radius server to complete authentication.

IOT wanted to keep this existing practice of using only username/password authentication – without requiring a certificate. Because of this, IOT retained the EAP-FAST protocol for authentication of in-band communication with the OS.

To establish robust security for the Intel AMT “out-of-band” remote communication channel, IOT reconfigured their server to use the EAP-PEAP protocol for Intel AMT communication (which occurs “below” the OS, in system firmware). EAP-PEAP is an Intel AMT-supported protocol, and is the only AMT-supported protocol that does not require a client certificate for authentication.

To make the solution work, IOT reconfigured their 802.1x infrastructure to support multiple protocols and switch seamlessly between Intel AMT out-of-band authentication and the subsequent authentication via user log-on from the OS.

Supporting Microsoft SCCM patch advertisement

OEM laptop vendors do not typically support laptop manageability when the systems are in low-power (Sx)/DC states, because of the extra drain on battery life, as well as some safety issues. However, when managing PCs with Intel vPro technology, SCCM patch advertisement must be able to wake the laptop – without a user being logged in. To enable this, IOT had to reconfigure their Radius Server to allow machine authentication using their EAP-FAST protocol on the server. Machine authentication allows the SCCM advertisement to use a system account to apply the patch without the user being logged on.

Turning off the wake-on-LAN (WOL) in Intel AMT

IOT also enabled Intel AMT power policies for S0/S3-S5 (AC) power states to effectively turn off the wake-on-LAN (WOL) feature in the Intel AMT firmware. They did this to ensure that Intel AMT would stay alive and ready for SCCM patch advertisements. This helped avoid a possible failure of the advertisement scripts to wake the client.

Configuring pre-logon wireless profile for laptops

Typically, a PC running Windows* XP makes a wireless connection only after the user logs in. To use the Intel AMT remote management capabilities in wireless laptops, the PCs must be connected to the wireless network before the user logs in. To resolve this challenge, IOT configured Windows XP with a persistent wireless profile.

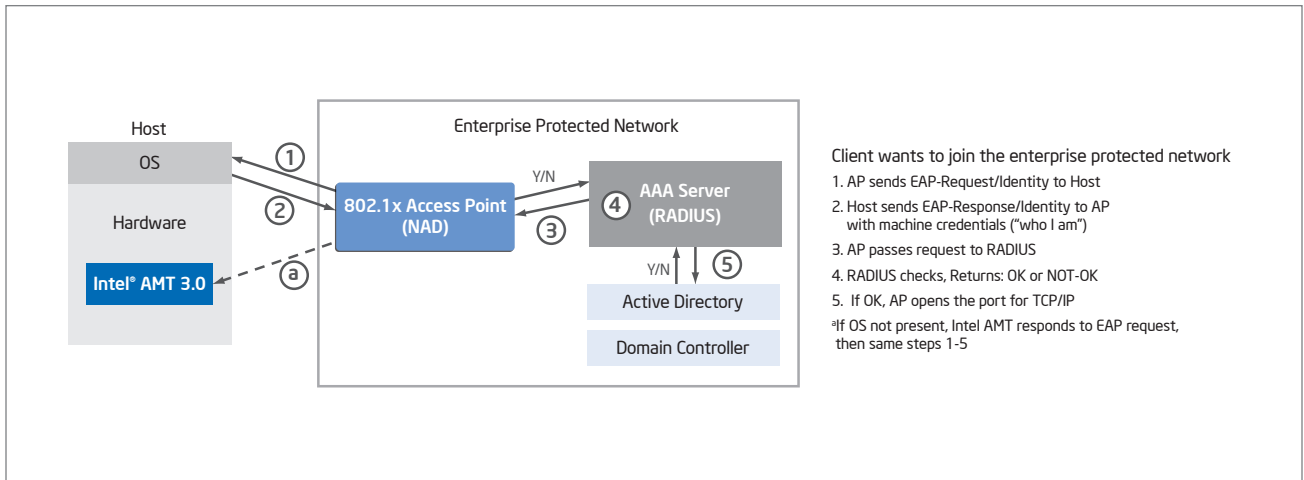


Figure 1. Out-of-band versus OS-level communication. Integration of PCs with Intel® vPro™ technology included managing the transition of secure, remote communication with Intel vPro technology, to OS-level communication with the management application (Microsoft SCCM*).

ROI study in production environment: Projected 405% positive ROI in 5 years

Recently, IOT investigated the benefits of improved patch management in their full environment of both wired and wireless PCs. On average, IOT deploys about 52 patches per year – each patch is rolled out to approximately 20% of PCs per week. With more than 600 sites to manage, patching has traditionally been a significant challenge. In the past, IOT patched PCs during business hours while PCs were typically powered up, but this approach interrupted workers.

Before deploying desktop and laptop PCs with Intel vPro technology, the patch success rate was 80%, with 75% of failures due to PCs being powered down.⁵ The patch failure rate was the same for both laptops and desktop PCs.⁵ To achieve a 95% patch saturation, IOT used e-mail contact with workers in order to bring the patch success rate up to 93%.⁵ To reach the 95% target, the last 2% was achieved via deskside visits to resolve patching issues.⁵

With the deployment of laptop and desktop PCs with Intel vPro technology, IOT has been able to use SCCM to remotely patch even PCs that are powered off at the start of the patching

Key findings from ROI analysis

- **Positive ROI within 5 years of 405%** by deploying laptops and desktop PCs with Intel® vPro™ technology to support patch deployment in a wired and wireless environment.³
- **Break-even point achieved within 2 years.**³
- **Projected cumulative benefits of over \$117,000** over 5 years.³

cycle. This significantly reduces the number of patch failures and cuts the IT time typically spent on deskside resolution of patch issues. It also helps accelerate the time to patch saturation.

Since implementing Intel vPro technology for laptops, IOT has realized almost \$23,000 of savings just by reducing deskside visits for patch deployment.³ IOT is projecting cumulative savings over 5 years of approximately \$117,000 solely by reducing IT costs for patching.³ IOT has achieved a break-even point in less than 2 years and is projecting a positive ROI of 405% across 5 years.³

Table 1. Benefits of patch deployment using Intel® vPro™ technology with Microsoft SCCM³

Use case	Without Intel® vPro™ technology	Desktop and laptop PCs with Intel® vPro™ technology					Estimated savings with 100% PCs with Intel® vPro™ technology
	Year 0 ^a 25,200 PCs (100%)	Year 1 ^a	Year 2 ^a	Year 3 ^b	Year 4 ^b	Year 5 ^b	
		2,250 (9% of total PCs) Intel vPro PCs	6,750 (27% of total PCs) Intel vPro PCs	13,088 (52% of total PCs) Intel vPro PCs	21,163 (84% of total PCs) Intel vPro PCs	25,200 (100% of total PCs) Intel vPro PCs	
Annual site visits required	5,616 site visits	4,901 site visits	3,496 site visits	1,369 site visits	128 site visits	<100 site visits	Site visits: reduced by 98%
IT worker-hours required to resolve patch issues, remotely or deskside	1,319 hours	1,140 hours	789 hours	293 hours	32 hours	25 hours	Cumulative savings in IT support costs: over \$137,000 savings
Deskside visits required to resolve on-site patch issues	5,242 visits	4,526 visits	3,121 visits	1,137 visits	128 visits	100 visits	
Annual IT support cost for on-site issues	\$45,210 cost	\$36,490 cost	\$25,250 cost	\$9,370 cost	\$1,020 cost	\$800 cost	
Annual IT savings from improved patching with Intel vPro technology	NA	\$6,583 savings	\$17,000 savings	\$32,800 savings	\$41,200 savings	\$41,400 savings	
ROI							
Net costs	N/A	\$13,900 cost	\$5,200 cost	\$1,100 cost	\$900 cost	\$800 cost	Break-even point: year 2
Net savings	N/A	\$-6,400 savings	\$11,800 savings	\$31,600 savings	\$40,000 savings	\$40,000 savings	Positive ROI: 405% in year 5 ^{c,5}
Cumulative benefits NPV	N/A	\$-6,400 savings	\$5,400 savings	\$37,000 savings	\$77,000 savings	\$117,000 savings	Cumulative NPV savings across 5 years: \$117,000 ^{c,5}

^a Data is the result of measurements.

^b Data in Q4 is the result of projections.

^c ROI is calculated conservatively, based on only one use case of patch management of all PCs. ROI calculations include a five-year projection to identify continued trends from taking advantage of the hardware-based capabilities, analysis assumes a conservative 15% "hurdle" or discount rate.

TCO/ROI investigation

The IOT investigation was conducted in a distributed environment with 25,200 laptop and desktop PCs, of which 9,050 were PCs with Intel vPro technology. Data was analyzed for only the one use case of remote patching. Data was then projected for 4 years, with the assumption that the number of PCs would not change, and that IOT would continue deploying PCs with Intel vPro technology as part of their planned 4-year refresh cycle. In the refresh cycle, 9% of PCs were refreshed in year 1, and 18% of PCs were refreshed in year 2. IOT expects to refresh an additional 25% of PCs in year 3, 32% in year 4, and 18% in year 5. ROI was calculated conservatively, based only on the one use case of patch management.

Positive results

IOT is extremely pleased that Intel vPro technology enables SCCM to automate the patch deployment process for both wired and wireless PCs, regardless of power state. The patch success rate has risen from 80% to 98%, and the time to patch saturation has been reduced from 1 week to 48 hours.³

Because of the effectiveness of Intel vPro technology in allowing successful remote patching, IOT has now raised their patch saturation target from 95% to 97%.³ In the past year alone, IOT has used Intel vPro technology to reduce IT service costs for patching by about 38% and has already realized a positive ROI.³ By the end of the additional 3 years, IOT projects a total positive ROI of 405%.³

IOT is continuing to deploy additional PCs with Intel vPro technology to complete their refresh cycle. IOT is also looking to implement additional capabilities of Intel vPro technology. IOT expects that the use of additional remote management and security capabilities will deliver further savings through console redirection and remote problem diagnostics and repair.

More Information

For more information about laptop and desktop PCs with the Intel Core 2 processor with vPro technology, visit www.intel.com/vpro

For more information about configuring for a wireless environment

For information about mobile manageability in low-power and OS-absent states, see Intel Technical Journal vol. 12, issue 04, Dec 23, 2008 at www.intel.com/technology/itj

For information about Intel vPro technology in a wireless configuration using Genscript, visit communities.intel.com/docs/DOC-3867

For information about Intel vPro technology in a Cisco ACS Configuration, visit communities.intel.com/docs/DOC-4203

For information about setting up multiple protocols for OS and AMT, visit communities.intel.com/docs/DOC-4206

For information about creating administrator profiles for Windows XP, visit communities.intel.com/docs/DOC-4143

¹ All content about State of Indiana and the Indiana Office of Technology was provided by the State of Indiana's Indiana Office of Technology.

² PCs with Intel® Core™2 processor with vPro™ technology include powerful Intel® Active Management Technology (Intel® AMT). 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. For more information, see www.intel.com/technology/platform-technology/intel-amt/.

³ Source: The State of Indiana - Indiana Office of Technology Pilot of PCs with Intel® Core™2 processor with vPro™ technology, conducted in 2008 and 2009, at the IOT's distributed sites in Indiana.

⁴ 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. For more information, see <http://www.intel.com/technology/platform-technology/intel-amt/>.

⁵ Source: The State of Indiana / Indiana Office of Technology knowledge base.

Copyright © 2009 Intel Corporation. All rights reserved. Intel, the Intel logo, Core, vPro, and Core inside are trademarks of Intel Corporation in the U.S. and other countries.

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

