

## Remediating Applications When Migrating from Microsoft Windows XP\* to Microsoft Windows 7\*

Intel continues to see tremendous value in migrating to Microsoft Windows 7\* on Intel®-based platforms.

—Diane Bryant  
Chief Information Officer  
Intel Corporation

### Executive Overview

To help ensure application compatibility during Intel's enterprise-wide migration from Microsoft Windows XP\* to Microsoft Windows 7\*, Intel IT implemented a carefully controlled workflow that brought application owners, users, and their applications together in one common test environment. So far, out of more than 1,000 applications tested, we have encountered fewer than 10 that could not be remediated within our migration timeframe using standard methods. We anticipate that migration to the new OS will provide Intel with significant business value in the form of reduced deployment, operating, and support costs, and improved user productivity.

Following a beta migration of 300 application owners and users to Microsoft Windows 7 in 2009, we initiated an early-adopter migration involving 3,000 additional participants in the first quarter of 2010. During both migration phases, participants tested their applications using our workflow and test environment, along with tools provided by Microsoft Application Compatibility Toolkit\* (Microsoft ACT), to quickly identify and remediate most application installation and runtime issues.

For those issues that could not be easily remediated, we implemented two safety-net solutions. These solutions allow Microsoft Windows XP applications to run alongside Microsoft Windows 7 applications until application owners and suppliers can recode them:

- Applications run in Microsoft Windows Terminal Services Mode in a multi-

user Microsoft Windows Server 2003\* environment that is compatible with Microsoft Windows XP applications.

- Applications run in virtual Microsoft Windows XP Mode, which is enhanced by Intel® Virtualization Technology (Intel® VT) available with Intel® vPro™ technology.

As we continue to migrate additional segments of Intel's workforce to the new OS, we anticipate using Microsoft Enterprise Desktop Virtualization\* (MED-V) as our single safety-net solution as it becomes available for the 64-bit version of Microsoft Windows 7. We expect that MED-V will provide a more controlled, secure, and scalable solution as greater numbers of users migrate to the new OS.

John Dunlop  
Enterprise Architect, Intel IT

Roy Ubry  
Staff Engineer, Intel IT

## Contents

Executive Overview.....	1
Background.....	2
Solution.....	3
Inventory.....	3
Normalization.....	5
Prioritization.....	5
Testing.....	5
Self-Service Remediation.....	6
Standard Remediation.....	6
Safety-Net Solutions.....	6
Results.....	7
Next Steps.....	7
Conclusion.....	7
For More Information.....	8
Acronyms.....	8

## IT@INTEL

IT@Intel is a resource that enables IT professionals, managers, and executives to engage with peers in the Intel IT organization—and with thousands of other industry IT leaders—so you can gain insights into the tools, methods, strategies, and best practices that are proving most successful in addressing today's tough IT challenges. Visit us today at [www.intel.com/IT](http://www.intel.com/IT) or contact your local Intel representative if you'd like to learn more.

## BACKGROUND

**Intel is migrating from Microsoft Windows XP\* to Microsoft Windows 7\* because the new OS better meets our long-term performance, security, manageability, and productivity needs. We anticipate that migration to the new OS will provide Intel with significant business value in the form of reduced deployment, operating, and support costs, and improved user productivity. This is largely due to reduced support costs associated with improved OS stability and built-in troubleshooting tools designed to reduce calls to the Service Desk.**

After a successful beta migration of 300 participants to Microsoft Windows 7 in 2009, we initiated enterprise-wide migration in the first quarter of 2010 with a population of early adopters. To help ensure OS and application readiness for Intel's more than 80,000 users, these early adopters included 3,000 users, application owners, and developers selected from all Intel business groups. As we move into the second quarter of 2010, we are expanding deployment of the new OS beyond our early adopters to the rest of our employees.

By the end of 2009, testing showed that approximately 25 percent of our Microsoft Windows XP applications might require some form of remediation before they would install or execute properly on Microsoft Windows 7. Further investigation using a third-party application compatibility tool confirmed this number.

We learned that the majority of applications require remediation for five reasons:

- Microsoft Windows XP and Microsoft Windows 7 have different security models, and this can cause both installation and runtime failures.

- We require that all applications function with Microsoft User Account Control (Microsoft UAC), a feature that helps prevent malware from writing to protected areas of the file system or to the registry. Any applications that do not properly comprehend this feature require remediation.

Applications can interact with Microsoft UAC in one of two ways. They can avoid writing to protected areas entirely. Alternately, they can prompt the user when an attempt is made to write to protected areas, indicating that the application is attempting a task that requires administrative intervention. The user must then decide whether to permit the action if they are aware of it, or deny the action in cases where they suspect malicious activity. In cases where the application does not properly interact with Microsoft UAC, however, the application or installation fails with no message explaining why.

- Our decision to move to 64-bit computing allows us to take advantage of new systems with higher memory capabilities, while positioning Intel to take advantage of 64-bit applications as they become available. Moving to this computing model also provides additional security benefits, including Data Execution Prevention (DEP), which helps prevent malicious code exploits by disallowing applications from executing code from a non-executable memory region. Because 16-bit components within 32-bit legacy applications will not install or execute on a 64-bit OS, and because some legacy applications were packaged using 16-bit installers, they will need to be remediated. Furthermore, some 32-bit applications may not execute properly on Microsoft Windows 7 due to different hard-coded paths used at runtime for 32-bit program files and 64-bit program files.

- Microsoft Internet Explorer 8\* compatibility is a must-have requirement for Microsoft Windows 7. Therefore, Intel's Web applications that are currently coded for Microsoft Internet Explorer 6\* may not execute properly on Microsoft Windows 7.
- Rather than performing minimum OS version checking, some applications perform specific OS version checking, which can cause installation or runtime failures on Microsoft Windows 7.

We needed efficient and accurate tools to help us implement our migration plans to the new OS. We also needed safety-net solutions to deal with incompatible applications that could not be remediated quickly within our migration timeframe and to allow such applications to continue to run in a Microsoft Windows XP environment alongside Microsoft Windows 7 applications until such time that Intel application owners or suppliers could fix compatibility issues found during testing.

## SOLUTION

**During our early-adopter migration to the new OS, we provided 3,000 Intel application owners, developers, and users with a carefully controlled workflow, shown in Figure 1. This workflow brought participants and their applications together in a common testing environment. We also provided tools to help them quickly and accurately inventory, normalize, prioritize, and test applications, as well as to remediate any compatibility issues found during testing. For those business-critical applications that participants could not quickly remediate, we also implemented safety-net solutions that allowed these applications to continue running in a Microsoft Windows XP environment.**

As with our beta release in 2009, Intel selected the 3,000 early adopter participants from all major business areas including manufacturing, marketing, product development, human resources, and IT. All laptops and desktops

involved in the migration had to meet the minimum deployment specifications listed in Table 1 in order to meet our virtualization, performance, and manageability requirements.

## Inventory

We provided participants with tools for creating and managing an application inventory. These tools helped determine which applications could be migrated easily to the new OS, which applications could be placed in end-of-life status, and which applications required remediation.

### INVENTORY AGENT

Inventory Agent, a component of Microsoft Application Compatibility Toolkit\* (Microsoft ACT), inventoried all hardware and software, and recorded all pertinent information in a Microsoft ACT database. This information helped us to identify many known compatibility issues before we began our own tests and later helped us prioritize applications to be tested. Figure 2, on page 5, shows an example of an application report from Inventory Agent.

Table 1. Minimum Deployment Specifications

#### Minimum Deployment Specifications

- Support for Intel® Virtualization Technology (Intel® VT) available with Intel® vPro™ technology
- 2 GB of RAM
- Intel® Mobile 965 Express series chipset or later
- Intel® X25-M Mainstream SATA Solid-State Drive, replacing existing hard disk drive

**Controlled Workflow**

**Inventory**

- Microsoft Application Compatibility Toolkit\* (Microsoft ACT)
- Intel Application Profiler

**Normalization**

- Consolidate application versions
- Eliminate like applications

**Prioritization**

- Assess business importance of applications
- Count total affected PCs that will use applications

**Testing**

- Microsoft ACT
- Deploy lab systems
- Deploy virtual PC

**Standard Remediation**

- Microsoft ACT
- Microsoft Standard User Analyzer
- Determine if application can be end-of-lived
- Recode if necessary
- Create shims if necessary
- Deploy in virtualized environment if necessary

**Self-Service Remediation**

**Step 1**  
Run application in Microsoft Windows 7\* Application Compatibility Mode

**Step 2**  
Run application in Microsoft Windows 7 Application Compatibility Mode as an administrator

**Step 3**  
Search tested applications list to determine if application requires special instructions

**Step 4**  
Report application to Intel IT for remediation

*If applications failed to install or run correctly, application owners could apply a four-step, self-service process to help them remediate their own applications before reporting issues to Intel IT.*

**Safety-Net Solutions**

**Current Safety-Net Solutions**

**Microsoft Windows Terminal Service**

- Users share broad-based applications
- Application looks like a virtual machine (VM) but is not

**Microsoft Windows XP Mode**

- True VM
- Runs Microsoft Windows XP\* applications from Microsoft Windows 7 host

**Future Safety-Net Solution**

**Microsoft Enterprise Desktop Virtualization\***

- Delivers applications in VM that runs Microsoft Windows XP
- More controlled, secure, and scalable than Microsoft Windows XP Mode
- Intel expects to adopt when available in 64-bit environments

Figure 1. Intel IT created a carefully controlled workflow for application migration.

As a registered Microsoft ACT Community member, Intel receives access to all information pertaining to compatibility issues shared by other member companies around the world. Through Microsoft Compatibility Exchange, an information sharing service, we are able to upload our Microsoft ACT database and learn about compatibility issues encountered by other members who have tested the same applications. This allows us to explore issues and remediation solutions logged by other members before we even begin testing.

**INTEL APPLICATION PROFILER**

We used Intel Application Profiler, a tool we had previously developed, for application management. This profiler, which is both a tool and a database, is Intel's authoritative system of record (SOR) for scheduling remediation work. It helped us track data obtained during the inventory and testing phases. During inventory, we stored information in the database such as application ownership, system requirements, and which applications and application versions were stored on workstations involved in the migration.

Once we tested applications using Microsoft ACT, we updated the database to reflect Microsoft Windows 7 compatibility status.

**Normalization**

Once we created an accurate inventory, we knew which applications resided on laptops and desktops and who owned applications. We also knew how many versions of the same application resided on each machine, including outdated and unsupported versions. The inventory helped us identify redundant applications, and we then worked with application owners to decide which applications would be retained and which would be placed in end-of-life status. This normalization process reduced the number of applications that required testing, migration, and remediation. Identifying application versions that have proven compatibility with Microsoft Windows 7 helped us reduce the time and cost associated with remediation. The normalization phase also helped us develop plans for upgrading laptops and desktops with the latest versions of applications.

**Prioritization**

We worked with application owners to prioritize the remaining applications according to selection criteria such as business importance. Prioritization helped determine the order in which owners should test and remediate their applications for compatibility with Microsoft Windows 7. This process helped further identify which applications would be retained and which would be placed in end-of-life status.

**Testing**

Application owners used Microsoft ACT to test application compatibility and determine where applications encountered installation problems and where they attempted to perform operations that did not conform to Microsoft Windows 7 security standards. We also used Microsoft ACT to check Web applications for Microsoft Internet Explorer 8 capability. Application owners then added testing data to the Intel Application Profiler and later used this data to prioritize and schedule any remediation issues identified.

Windows 7 RC - Application Report								
Application Name	Version	Company	My Assessment	Vendor Assessment	Community Assessment	Active Issues	Computers	
Application 1	9.0.1.8	Company 1			4  0  0	0	4	
Application 1	9.0.3	Company 1				0	0	
Application 1	9.2.0.23	Company 1				0	3	
Application 1	9.0.3.15	Company 1				1	57	
Application 1	8.2.1.6	Company 1			4  0  0	2	1	
Application 2	10.4.0	Company 1			5  0  0	0	6	
Application 3	8.2					0	2	
Application 4	2.4	Company 2				0	1	
Application 5	10.7.0	Company 3				0	1	

Figure 2. Microsoft Inventory Agent lists information, such as redundant applications, that aids with prioritization and test planning. Two assessment columns indicate whether vendors or members of the Microsoft Application Compatibility Toolkit\* (Microsoft ACT) Community found the application to work (green), work with issues (yellow), or not work (red) with Microsoft Windows 7\*.

## Self-Service Remediation

If an application did not install or run correctly, we provided application owners with a four-step, self-service process to help them remediate their own applications before reporting issues to Intel IT. If one step in this process did not prove helpful, owners moved on to the next.

1. Run the application in Microsoft Windows 7 Application Compatibility Mode. The Compatibility Mode feature enables users to run programs written for earlier versions of Microsoft Windows\*.
2. Run the application as an administrator in Microsoft Windows 7 Application Compatibility Mode. Some programs require administrator rights to run correctly.
3. Search a list of applications that have already completed testing to determine if the application requires special instructions to install or run correctly.
4. Report the application to Intel IT. Owners could contact the Service Desk for urgent issues, or they could fill out a request form to place their program in Intel IT's application remediation queue. We requested that owners continue checking the list of known applications needing special instructions.

## Standard Remediation

Application owners used Microsoft ACT in the testing environment to fix most installation and runtime execution failures. For applications that failed to install cleanly, Microsoft ACT helped to determine root causes by walking application owners through a series of steps designed to identify most problems. For applications that failed to execute properly once they

installed cleanly, we pointed owners to the Microsoft Troubleshoot Compatibility Option. This component runs the application through a series of simple troubleshooting and mitigation steps, making necessary adjustments—such as virtualizing registry components and the file system—to help solve most runtime execution problems. It also performs operations that emulate a Microsoft Windows XP SP3\* environment to allow the application to execute properly.

Microsoft Standard User Analyzer (Microsoft SUA) reports all variances between what the application attempts to do and the default security policies defined in Microsoft Windows 7. In cases where application owners are able to repair application failures using tools provided within Microsoft ACT, they can then use Microsoft SUA to create a package that incorporates the recommended changes into an installer, which can then be included in the application distribution package. The installer creates the necessary “shims” to cause the application to execute correctly on target systems.

Shims modify the way an application runs so that it responds as if it were executing on the OS for which it was coded. For example, if an application is hard coded to look for Microsoft Windows XP but is actually running on Microsoft Windows 7, shims virtualize the file system to make the application think that it is running in a Microsoft Windows XP environment. However, shims cannot bypass the security model of Microsoft Windows 7. Therefore, applications still fail in cases where they try to perform operations forbidden by the security model.

Intel application owners also used Microsoft SUA to create shims to deal with applications that attempted to write to areas of the file

system that Microsoft Windows 7 protects. To work around this problem, they used Microsoft SUA to create shims that redirect such applications to a virtual location, allowing them to run unobstructed without compromising the improved security features of Microsoft Windows 7.

## Safety-Net Solutions

For cases where Microsoft Troubleshoot Compatibility Option and Microsoft SUA tool using shims both fail to remediate installation or runtime failures, and the application cannot be recoded or placed in end-of-life status, Intel IT deployed two interim safety-net solutions: Microsoft Windows Terminal Services (Microsoft WTS) and Microsoft Windows XP Mode. These solutions allow applications to seamlessly run in a Microsoft Windows XP-compatible environment alongside applications that run smoothly in the Microsoft Windows 7 environment. As a stop-gap measure, these solutions provide time for application owners and suppliers to recode incompatible applications so that they install and execute correctly in Microsoft Windows 7.

## MICROSOFT WINDOWS TERMINAL SERVICES

We used Microsoft WTS for broad-based applications made available to many users. Applications run in a multi-user Microsoft Windows Server 2003\* environment that is compatible with Microsoft Windows XP applications. Users have their own desktops or laptops and their own settings, but they share applications installed with Microsoft WTS. When users execute an application, it appears to them like a miniature desktop on their machine, inside its own window. The application looks like a virtual machine (VM) to the user but is not.

We found that Microsoft WTS worked especially well in cases where application suppliers were not yet ready to support their applications in a virtualized environment or through the use of shims. Executing those applications using Microsoft WTS allows them to run until versions are available that are compatible with Microsoft Windows 7.

### **MICROSOFT WINDOWS XP MODE**

Microsoft Windows XP Mode, enabled by Intel® Virtualization Technology (Intel® VT) available with Intel® vPro™ technology, makes it easy for Intel's application owners to install and run Microsoft Windows XP applications directly from a Microsoft Windows 7 host. This mode provides a true VM on a laptop or desktop that runs Microsoft Windows XP SP3. The VM presents applications in such a way that users can view them from the host Microsoft Windows 7 OS, providing seamless integration between the host machine and the VM. We implemented this mode by supplying a downloadable version that provides a standard, secured client that delivers the Microsoft Windows XP Mode experience.

### **Results**

By the end of our beta Microsoft Windows 7 migration in late 2009, Intel IT learned that approximately 25 percent of the applications we planned to migrate would require remediation. Fortunately, we have seen very few issues that have forced application owners to employ safety-net solutions. For those applications that have not migrated smoothly, owners have been able to quickly remediate most problems using tools made available through Microsoft ACT. In the few cases where Microsoft ACT components could not remediate problems, users are able to continue running those applications using our safety-net solutions

until such time that application owners or suppliers can fix those problems. So far, fewer than 10 out of more than 1,000 applications tested required use of our safety-net options because we could not make them run natively on Windows 7 in a timeframe suitable for our migration to the new OS.

### **Next Steps**

As we continue our enterprise-wide migration to Microsoft Windows 7, we expect to adopt Microsoft Enterprise Desktop Virtualization\* (MED-V) as our single safety-net solution once it becomes available for 64-bit environments. MED-V seamlessly and transparently delivers applications in a VM that runs Microsoft Windows XP, similar to Microsoft Windows XP Mode, but in a more controlled, secure, and scalable environment. We anticipate that MED-V will help us to better deploy, provision, control, and support the virtual environment than our present safety-net solutions.

---

## **CONCLUSION**

**Any time a large enterprise migrates to a new OS, some remediation issues are to be expected. However, Microsoft ACT tools in combination with our safety-net solutions have helped ensure our application readiness for Microsoft Windows 7. So far, fewer than 10 out of more than 1,000 applications tested required use of our safety-net solutions because we could not make them run natively on Windows 7 in a timeframe suitable for our migration to the new OS.**

Since we began our enterprise-wide migration in the first quarter of 2010 with

3,000 early adopters, careful planning has helped ensure successful migration of approximately 2,500 legacy applications to the new OS. Such planning requires a carefully controlled workflow. Application owners, users, and their applications must be brought together under one common testing environment to inventory, normalize, prioritize, and test those applications, as well as to remediate any installation and execution failures found during testing.

Microsoft ACT tools have helped us to significantly ease our transition to Microsoft Windows 7. For the few incompatible applications that cannot be remediated in a timely manner using these Microsoft tools, we have implemented effective safety-net solutions that allow such applications to continue to run in the Microsoft Windows XP environment alongside those applications that migrate smoothly to Microsoft Windows 7. This allows time for Intel application owners and suppliers to recode these applications to work with the new OS. These safety-net solutions also allow our migration to proceed on schedule so that we can take advantage of the performance, security, manageability, and productivity features of Microsoft Windows 7.

As we move into the second quarter of 2010, we anticipate that Microsoft ACT tools and our safety-net solutions will continue to help ensure the success of our expanded Microsoft Windows 7 deployment to the remainder of Intel's 80,000 employees. With potential to realize significant business value in reduced deployment, operating, and support costs, plus gains in performance, security, manageability, and productivity, we are encouraged that our Microsoft Windows 7 deployment is on schedule and our expectations for success have not changed.

## FOR MORE INFORMATION

- "The Value of PC Refresh with Microsoft Windows 7\*." Intel Corporation, September 2009.  
[www.intel.com/IT](http://www.intel.com/IT)
- "Moving to New Intel®-based PCs and Microsoft Windows 7\*." Video featuring Intel CIO Diane Bryant.  
[http://video.intel.com/?fr\\_story=461411f967b3df8db801ef81f8ff5c2420b6d9c4&rf=bm](http://video.intel.com/?fr_story=461411f967b3df8db801ef81f8ff5c2420b6d9c4&rf=bm)

## ACRONYMS

DEP	Data Execution Prevention
Intel® VT	Intel® Virtualization Technology
MED-V	Microsoft Enterprise Desktop Virtualization*
Microsoft ACT	Microsoft Application Compatibility Toolkit*
Microsoft SUA	Microsoft Standard User Analyzer
Microsoft UAC	Microsoft User Account Control
Microsoft WTS	Microsoft Windows Terminal Services
SOR	system of record
VM	virtual machine

For more straight talk on current topics from Intel's IT leaders, visit [www.intel.com/it](http://www.intel.com/it).


This paper is for informational purposes only. THIS DOCUMENT IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE. Intel disclaims all liability, including liability for infringement of any proprietary rights, relating to use of information in this specification. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted herein.

Intel, the Intel logo, and Intel vPro are trademarks of Intel Corporation in the U.S. and other countries.

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

Copyright © 2010 Intel Corporation. All rights reserved.

Printed in USA  
0510/JLG/KC/PDF

 Please Recycle  
322972-001US

