



Microsoft ACT: Deployment Guide

Microsoft Corporation

Published: August 2010

Abstract

This paper provides planning guidance for a Microsoft® Application Compatibility Toolkit (ACT) 5.6 deployment within an organization. It provides guidelines and procedures for IT Professionals on how to plan for, deploy, and provision resources for the most effective use of the Toolkit.

This information applies for the following operating systems:

- Windows® 7
- Windows Vista®
- Windows Vista with Service Pack 1
- Windows Server 2008 R2
- Microsoft Windows Server 2003
- Microsoft Windows XP with Service Pack 2 (SP2)
- Microsoft Windows 2000

Microsoft

Copyright Information

This document is provided “as-is”. Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

© 2010 Microsoft Corporation. All rights reserved.

Active Directory, Internet Explorer, Microsoft, Windows, Windows NT, Windows XP, Windows Vista, Windows 7, and Windows Server are trademarks of the Microsoft group of companies.

All other trademarks are property of their respective owners.

Contents

Microsoft ACT: Deployment Guide	4
1. Introduction.....	4
1.1 Architecture and Supported Topologies	4
1.2 Types of Compatibility Evaluators	8
2. Identifying Computers for DCP Deployment	8
2.1 Determining Where and How to Deploy a DCP	8
2.1.1 Determining Where to Deploy a DCP	9
2.1.2 Determining the Best Method for Your DCP Deployment	12
2.1.3 Special Guidelines for the Update Compatibility Evaluator (UCE).....	13
2.1.3.1 Hard Drive Space Guidelines.....	13
2.1.3.2 Log File Sizing and Hard Drive Guidelines	13
2.1.3.3 Mitigating the UCE Data Load	14
2.1.3.4 Redeploying UCE	14
2.1.4 DCP Log Files	15
3. Case Study of an ACT 5.6 Deployment for Windows 7	16
3.1 General Information	16
3.2 DCP Log File Processing and Disk Space Utilization.....	17
4. ACT 5.6 Core Usage Scenarios.....	20
4.1 Deploying a New Operating System.....	20
4.2 Applying a Windows Update	22
5. ACT 5.6 Software, Hardware, and Configuration Requirements	24
5.1 Software Requirements	24
5.2 Hardware Requirements	25
5.3 Special Software and Hardware Considerations	26
5.3.1 Special Requirements for Using the UCE	26
5.3.1.1 UCE Supported Environments.....	26
5.3.2 Special Requirements for Using the Compatibility Administrator.....	26
5.4 Recommended ACT Database Configuration and Modifications	27
5.4.1 ACT Database Role Assignments.....	27
5.4.2 Additional ACT Database Recommendations	28
5.5 Required Privileges for the ACT Log Share	28
5.5.1 Share-Level Permissions	28
5.5.2 Folder-Level Permissions (NTFS Only)	29
5.5.3 Additional Troubleshooting Notes	29
5.6 Required Infrastructure for the Microsoft Compatibility Exchange	29

Microsoft ACT: Deployment Guide

1. Introduction

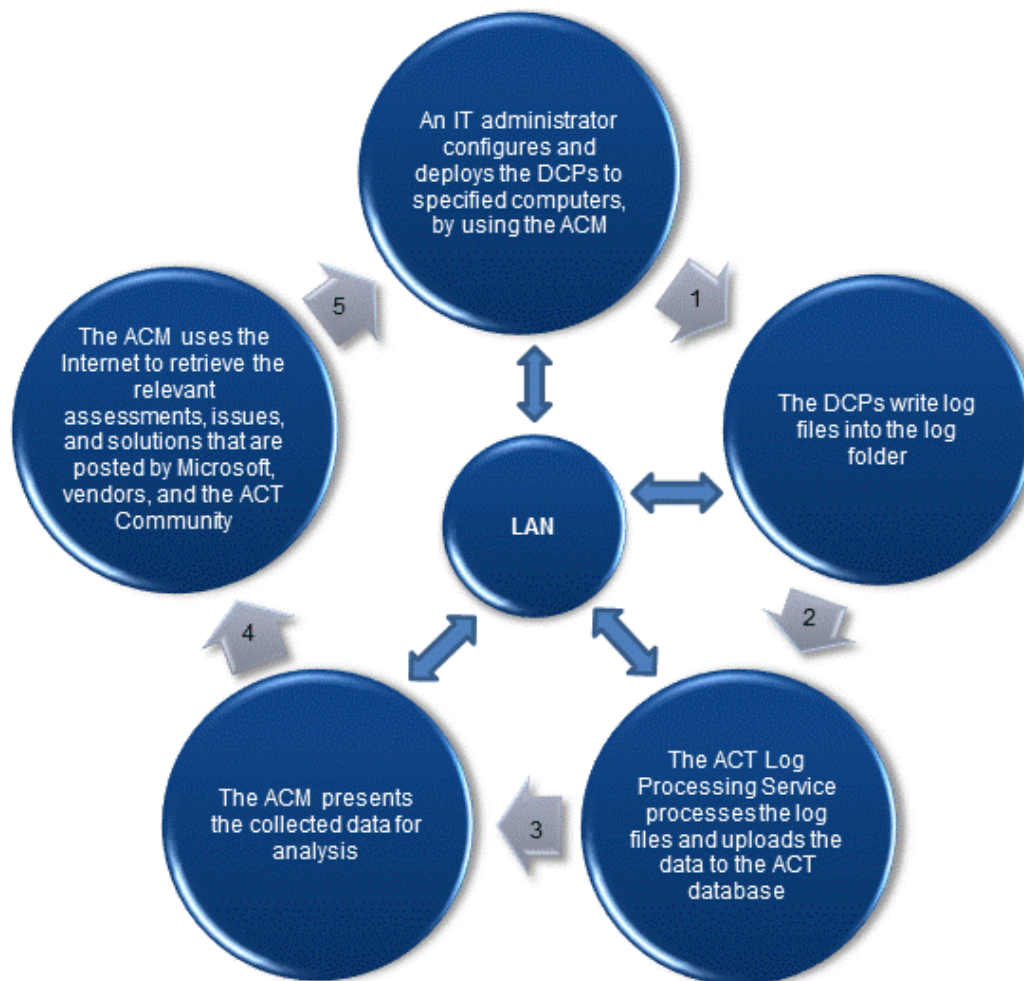
This document guides you through how to deploy the Microsoft® Application Compatibility Toolkit (ACT) 5.6 and how to strategize your data collection package (DCP) deployment to suit your organization's needs. To assist you with defining your deployment strategy, this document intends to answer the following questions:

- My organization has a large number of computers. Do I need to deploy the DCPs on all of the computers to capture the application and driver information?
- My organization is spread across many geographic locations. Do I need to deploy a separate instance of ACT in each location?
- My organization has a well-defined set of divisions (for example, Human Resources, Sales, IT, and so on) that have different kinds of applications installed. How do I plan a DCP deployment?
- My organization has more than one version of the Microsoft Windows operating system deployed. Do I need to create separate DCPs for each version? Can the DCPs run on all of the versions?
- Some applications are seasonal in nature. Will the DCP be able to collect the required information?
- My organization has a strict policy on software distribution practices. For example, we employ one or more of the following tools to deploy applications: Group Policy, IntelliMirror, Microsoft System Center Configuration Manager 2007, and so on. Can the information we have in these tools assist us with our compatibility testing?
- Some of our desktop users run as local Administrators and can freely install applications. How can I ensure that I capture this information?
- What is the best way to gather an inventory of hardware drivers in my organization?
- We have a large number of laptops in our organization. Are there any special considerations?

1.1 Architecture and Supported Topologies

The following diagram (Figure 1) illustrates the interaction between the various ACT components.

Figure 1: ACT 5.6 architecture



As shown in the diagram, the ACT 5.6 architecture encompasses the following major components:

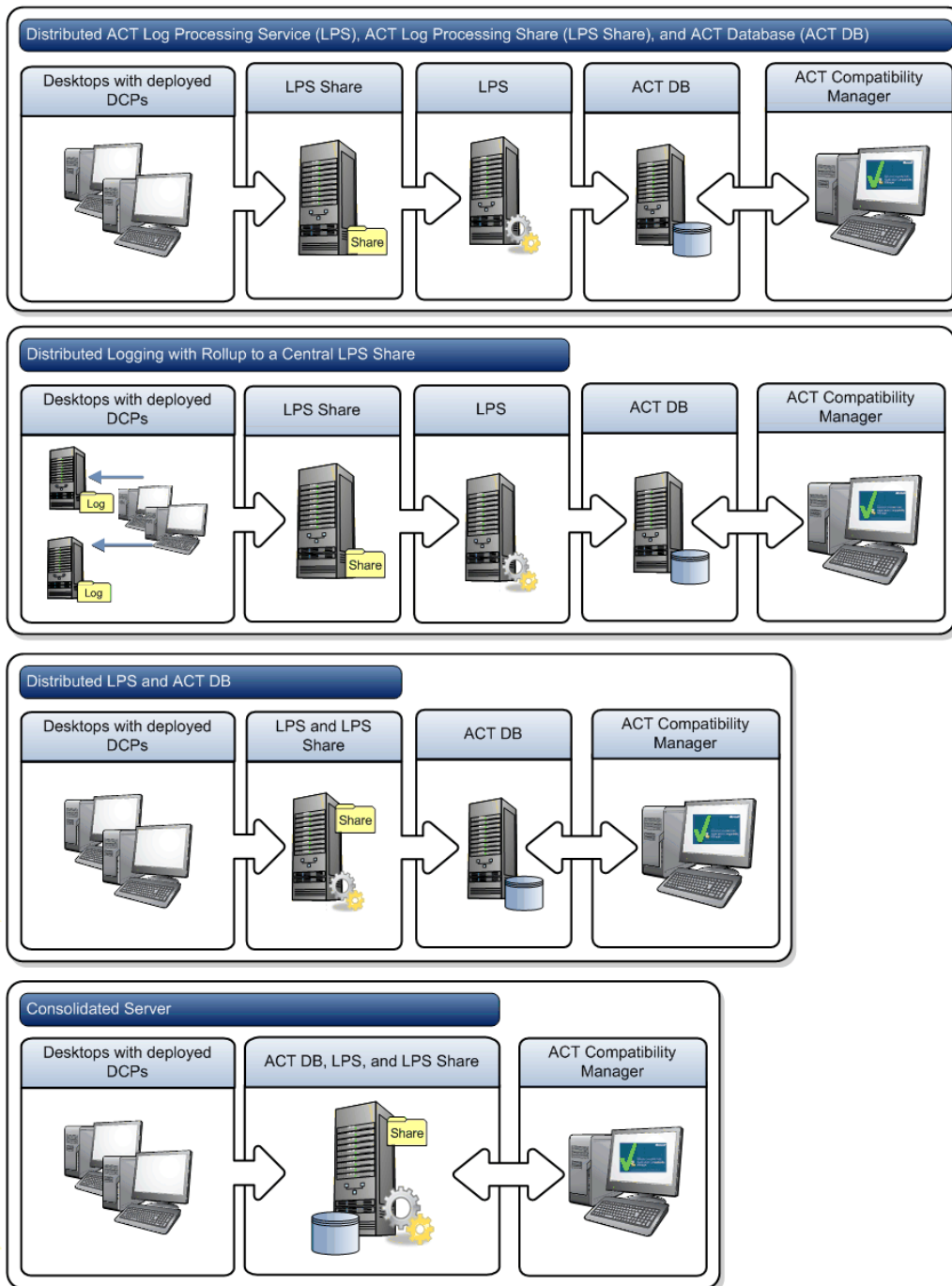
- **Application Compatibility Manager (ACM).** A tool that enables you to configure, to collect, and to analyze your data so you can fix any issues prior to deploying a new operating system or deploying a Windows update in your organization.
- **Data Collection Package (DCP).** A Microsoft Setup Installation (.msi) file created by the ACM for deploying to each of your client computers. Each DCP can include one or more compatibility evaluators, depending on what you are trying to evaluate
- **ACT Log Processing Service.** A service used to process the ACT log files uploaded from your client computers. It adds the information to your ACT database.
- **ACT Log Processing Share.** A file share, accessed by the ACT Log Processing Service, to store the log files that will be processed and added to the ACT database.

ACT Deployment Guide

- **ACT Database.** A Microsoft SQL Server™ database that stores the collected application, computer, device, and compatibility data. You can view the information stored in the ACT database as reports from the ACM.
- **Microsoft Compatibility Exchange.** A Web service that propagates application compatibility issues from the server to the client and enables the client computers to connect to Microsoft via the Internet to check for updated compatibility information.

The following diagram (Figure 2) illustrates the supported deployment topologies for an ACT 5.6 installation

Figure 2: ACT 5.6 supported topologies



The diagram shows the supported topologies for ACT 5.6 in their recommended usage order. For example, we highly recommend using the distributed ACT Log Processing Service, ACT Log Processing share, and ACT Database topology, and least recommend using a Consolidated Server.

**Important**

If you choose to employ a topology based on distributed logging with a roll up to your central share, you must move the files to the ACT Log Processing share before actual processing can occur. You can move the files manually or use a technology like Distributed File System Replication (DFSR) or any other similar technology already employed in your organization.

1.2 Types of Compatibility Evaluators

In addition to collecting application and hardware inventory, ACT 5.6 includes compatibility evaluators. Compatibility evaluators are run-time detection tools specifically designed to log behaviors as they occur on the user's computer and locate potential compatibility issues. ACT 5.6 includes the following compatibility evaluators:

- **Inventory Collector.** Examines each of your organization's computers, identifying the installed applications and system information.
- **User Account Control Compatibility Evaluator (UACCE).** Identifies potential compatibility issues due to an application running under a Protected Administrator (PA) or Standard User (SU) account on the Windows Vista® operating system. When running, UACCE monitors your running applications to verify interactions with the operating system and identify potentially incompatible activities.
- **Update Compatibility Evaluator (UCE).** Identifies the potential impact of a new Windows Update. By using the update impact data, you can prioritize your testing and reduce the potential risk of compatibility issues when you deploy Windows Updates.
- **Windows Compatibility Evaluator (WCE).** Identifies potential compatibility issues due to deprecated components in the new operating system, Graphical Identification and Authentication (GINA) DLLs, and the isolation required by Session 0 applications.

A DCP can include one or more compatibility evaluators, depending on what you are evaluating. The Application Compatibility Manager automatically groups the evaluators based on tasks, which include deploying a new operating system or a service pack or applying a Windows Update.

2. Identifying Computers for DCP Deployment

For greater control over your collected data, IT administrators should target their DCPs for deployment to a small subset of computers based on specific categories. For example, a DCP targeted to users in the United States Human Resources department. This enables better categorization and analysis of an application throughout the organization. For more information about deploying a DCP, see the "Deploying a Data Collection Package" topic in the ACT Help.

2.1 Determining Where and How to Deploy a DCP

You must ensure that all device drivers are captured so the proper impact can be assessed during an operating system or patch upgrade, in addition to locating potential issue and solution

data provided by Microsoft Corporation, Independent Software Vendors (ISVs), and Independent Hardware Vendors (IHVs).

2.1.1 Determining Where to Deploy a DCP

If your organization already has a hardware asset inventory list, it is recommended that you sample each unique hardware configuration so you can synchronize with the Microsoft Compatibility Exchange and obtain the relevant driver compatibility issues. If you do not have a comprehensive inventory, we recommend that you distribute the DCPs based on the factors described in the following table.

Question	Description
Do you have a managed, unmanaged, or mixed environment?	<p>You categorize your organization as a managed environment, an unmanaged environment, or a mixed management environment.</p> <ul style="list-style-type: none"> • Managed environment. IT administrators strictly control and manage the application installation and usage based on need and the various divisions in the organization. In this situation, an IT administrator can deploy a DCP on a limited subset of computers for each department, based on known needs and requirements. • Unmanaged environment. Users typically have administrator privileges on their computers and can install applications at their own discretion. Because users in an unmanaged environment can install any software they choose, you would need to deploy your DCPs to more computers than you would if you were in a managed environment. • Mixed environment. Your organization uses both managed and unmanaged environments, depending on an individual group's needs and administrative privileges.
How do you use specific applications in your organization?	It is very important that you provide coverage for all applications required by users in your organization but even more important that you provide coverage for your line-of-business (LOB) applications. For the most complete

Question	Description
	<p>coverage of application usage, you must:</p> <ul style="list-style-type: none"> • Consult with your local administrators, support engineers, and department leads to ensure that all applications are in use during the data-collection process. • Ensure that "seasonal" applications are covered. For example, fiscal year accounting applications might be used only once a year. • Attempt to perform the data collection when there are few employee vacations scheduled or at the beginning of the week to avoid weekends. Otherwise, you might have limited or incomplete results due to the decreased application usage.
Do you use role-based applications?	<p>Your organization may use role-based applications, which are applications that relate to job function and the role that a user performs within your organization. A common example is accountants (a financial role) and their finance-related applications. Reviewing application usage in conjunction with job function and roles enables better application coverage in your organization.</p>
How do you distribute your applications in your organization?	<p>You can distribute applications in many ways within an organization, for example, by using Group Policy, IntelliMirror, Microsoft System Center Configuration Manager 2007, or a custom distribution method. Reviewing your software distribution system policies in conjunction with your application inventory enables better application coverage and narrows the deployment of your DCPs.</p>
What is the geographic breakdown of your organization?	<p>You must consider the geographic distribution of your organization when planning for your DCP deployment (for example, if you have branches in North America, Asia, and Europe). You must then consider the application-usage patterns across each geographic region. You must account for divisional applications, localized versions of applications, and</p>

Question	Description
	<p>applications specific to the geographic location and export restrictions. We recommended that you consult with technical and business leaders from each region to understand these differences.</p>
<p>What types of computers do you have in your organization and how are they used?</p>	<p>Computer types and usage patterns can play an important role in your DCP deployment. The following sections describe some of the most common computer types and usage patterns.</p> <ul style="list-style-type: none"> Mobile and Laptop Computers. Mobile users frequently work offline, occasionally synchronizing with the corporate network through either a LAN or VPN connection. Because there is a high possibility of a user going offline for long periods of time, you must consider the odds of the user being online for the DCP to be downloaded and installed, and then online again for the logged data to be uploaded. Multi-user Computers. Multi-user computers are typically in university computer labs, libraries, and organizations that enable job sharing. These computers are highly secure and include a core set of applications that are always available, as well as many applications that can be installed and removed as necessary. Because these computers typically have a basic set of applications assigned to users or computers, you can narrow the application coverage and usage to identify only a subset of client computers to receive the DCP. AppStations/TaskStations. AppStations running vertical applications are typically for marketing, claims and loan processing, and customer service. TaskStations are typically dedicated to running a single application, such as on a manufacturing floor as an entry terminal or in a call center. Because both of these types of computers do not commonly allow users to add or to remove applications, and might be

Question	Description
	<p>designated for specific users and job roles, the application coverage and usage can be narrowed to identify a subset of client computers to receive the DCP.</p> <ul style="list-style-type: none"> • Kiosks. Kiosks are generally in public areas. These computers run unattended and are highly secure, generally running a single program by using a single-use account and automatic logon. Because these computers typically run a single application, the application coverage and usage can be narrowed to identify a subset of computers to receive the DCP.

2.1.2 Determining the Best Method for Your DCP Deployment

There are several ways to distribute a DCP to your identified client computers, including:

- **Group Policy Software Installation.** Use the Group Policy Software Installation feature of Active Directory in Windows Server® 2008 R2 for deployment.

Important

All client computers to which you will deploy the DCP must be part of the Active Directory forest.

- **Logon script.** You can use Windows Script Host (WSH) to create a logon script for deploying the DCP. Installing with a logon script requires administrator credentials on the local computer.
- **Microsoft System Center Configuration Manager 2007 and customized deployment methods.** You can use Configuration Manager or a customized deployment method to deploy the data-collection package in your organization.
- **Manual distribution.** You can use a file server on your network as a software distribution point for the ACT DCPs. At rollout time, you can send an e-mail to users, explaining the pending upgrade and providing a link to the distribution point. Note that self-installation of a DCP requires administrator credentials on the local computer.

We recommend basing your method for deploying the DCP on your existing infrastructure. The preference of deployment methods is as follows:

1. If you have an existing Configuration Manager infrastructure, you can use this to deploy the DCP.
2. If you have an Active Directory infrastructure, use Group Policy Software Installation.
3. If you have an identity and authentication infrastructure other than Active Directory, use logon scripts.
4. If none of these other options work, use a manual deployment to deploy from a network share or from a CD.

2.1.3 Special Guidelines for the Update Compatibility Evaluator (UCE)

The Update Compatibility Evaluator (UCE) generates considerable amounts of data when deployed to a large number of client computers. This can lead to issues with the log file share, the ACT database, and the performance of your client computers. Because the UCE log files are six to seven times the size of the log files from other ACT compatibility evaluators, it is strongly recommended that you initially deploy the UCE to 50 computers or less for less than three days to understand the amount of data generated before deploying the compatibility evaluator throughout your organization.

The following best practices apply to large deployments:

- Host the ACT Log Processing Service on a server primarily dedicated to running the ACT and limit other running applications.
- Ensure your log file share is always accessible for uploads by the computers to which the UCE is deployed.
- Verify that you have at least 60 megabytes (MB) of free space, per computer for each day you run the compatibility evaluator, in the log file share.
- Ensure you do not deploy the UCE to computers with less than 1 gigabyte (GB) of free space or less than 256 MB of RAM.

2.1.3.1 Hard Drive Space Guidelines

The following table provides hard drive space estimates for different upload intervals.

Upload Interval (in Hours)	Free Space per Computer per Day (in MB)
2	240
4	120
8 (default)	60
12	40

2.1.3.2 Log File Sizing and Hard Drive Guidelines

The following table provides guidance for the required amount of free hard drive space, based on a three-day deployment and an eight-hour upload interval.

Total Number of Computers	Total Size of Log Files (in GB)
1	.18
10	1.8
50	9
100	18
500	90

Total Number of Computers	Total Size of Log Files (in GB)
1000	180

2.1.3.3 Mitigating the UCE Data Load

The UCE generates a considerable amount of data; however, you can mitigate the data load by following these guidelines:

- Start with a small deployment of the UCE over a short duration of time to get an understanding of the size of the log files and the necessary hard drive space.
- Verify that your file share can handle more than 60 MB of log files per computer per day that the compatibility evaluator runs. If this is not possible, you can:
 - Create multiple file shares on different computers, sending the UCE data to the various file shares through different ACT Log Processing Services.
 - or-
 - Create multiple file shares on different computers, periodically reconfiguring your ACT Log Processing Service to point to the additional file shares.
- Remove the processed log files from the **Processed** folder before redeploying the compatibility evaluator.
- Use "rolling deployments," avoiding simultaneously starting the UCE on the computers to which it was deployed.

2.1.3.4 Redeploying UCE

You can redeploy the UCE to your client computers as often as you deem necessary. The following are two possible redeployment strategies are:

- **Before the release of security updates.** This strategy requires you to deploy the compatibility evaluator prior to the release of security updates. Deployment should start several days before the release so there is time to evaluate the security updates and any flagged issues prior to deciding whether to install these updates.
- **Whenever your application profile changes.** This strategy requires you to deploy the compatibility evaluator whenever a new application becomes part of your enterprise's profile or when updates or changes occur to existing applications.

Important

If you redeploy the compatibility evaluator to a computer already running the evaluator, the original version uninstalls and the new version installs and starts. Because deployments are cumulative, the ACT database saves your existing application dependencies from previous deployments indefinitely. Redeployment is a good time to delete your log files from the **Processed** folder to free up disk space for future files.

2.1.4 DCP Log Files

When you are creating a DCP in the Application Compatibility Manager, you can select an output location for your log files. The configuration options are:

- **Select a default ACT Log Processing share location.** If you use this option, the DCP automatically writes the log files to the file share. If the file share is unavailable when the specified upload time interval is reached, the DCP will make two more attempts. If the problem persists, the DCP will store the log file in one of the locations listed in the following table, based on the operating system. All files are then retried during the next upload interval.

Operating System	Location
Windows 7 Windows Vista® Windows Server 2008 R2	%SYSTEMDRIVE% \Users\All Users\Microsoft\Application Compatibility Toolkit\LogProcessor\Failed
Windows Server® 2003 Windows XP Windows XP with Service Pack 2	%SYSTEMDRIVE% \Documents and Settings\All Users\Application Data\Microsoft\Application Compatibility Toolkit\LogProcessor\Failed

- **Select the Local (%ACTAppData%\DataCollector\Output) location.** If you use this option, the DCP creates the log files on the local system (as shown in the following table) and the computer Administrator must manually copy the files to the file share location. This is a good option for mobile users that are not always connected to the network.

Important

There is a situation whereby a mobile user may not generate compatibility data due to the irregularity of corporate network connection and the length of time the DCP should run. If the DCP cannot upload data to the network share after three attempts, the log files are stored in the failed location as shown in the following table. If the next time the user connects to the network share, the duration of the DCP has expired; the DCP will not attempt to upload the information again and instead uninstalls itself, removing any of the data previously stored in the failed location.

Operating System	Location
Windows 7 Windows Vista Windows Server 2008 R2	%SYSTEMDRIVE% \Users\All Users\Microsoft\Application Compatibility Toolkit\DataCollector\Output
Windows Server 2003 Windows XP Windows XP with Service Pack 2 (SP2)	%SYSTEMDRIVE% \Documents and Settings\All Users\Application Data\Microsoft\Application Compatibility Toolkit\DataCollector\Output

- **Type an alternate network share location.** If you use this option, you must verify that the DCP service can write to the location. This is a good option for companies that are geographically diverse (for example, if you have branches in North America and Europe). An IT Administrator can create DCPs and file shares individually for North America and Europe, which further enables administrators at a central location to roll up all of the collection log files to a central location. These log files are then mapped to the file share for final processing and entry into the ACT database.

3. Case Study of an ACT 5.6 Deployment for Windows 7

The following case study is intended to assist with the ACT deployment planning process in an organization.

3.1 General Information

An IT Administrator, in an unmanaged Enterprise environment, wants to deploy a DCP to evaluate the organization for potential compatibility issues, before upgrading to the newest version of the Windows operating system.

- **Number of client computers to receive the DCP:** Approximately 10,000 computers
- **DCP deployment strategy:** Microsoft System Center Configuration Manager 2007
- **Targeted operating system for the DCP:** Windows 7 and Windows Server 2008 R2
- **Duration of the DCP:** 3 days
- **Upload interval:** Every 8 hours
- **Output location:** Network share on a corporate network
- **Corporate environment:** Unmanaged
- **Topology:** Distributed ACT Log Processing Service and ACT database
- **Hardware used:**

Hardware	Description
Role	ACT Log Processing Service and ACT Log Processing share host
Processor	Intel Xeon 2 x 3.2 Gigahertz (GHz)
Memory	2 GB
Hard Disk	Disk Array 1\Volume 1 x3, SCSI, 10,000 RPM, 146GB, RAID 5
Network Adapter	1 x1,000 MB/s

Hardware	Description
Role	SQL Server 2005 (SP1)
Processor	Intel Xeon 2 x 3.2 Gigahertz (GHz)
Memory	2 GB
Hard Disk	Disk Array 1\Volume 1 x3, SCSI, 10,000 RPM, 146GB, RAID 5 Disk Array 2\Volume 2 x1, SCSI, 10,000 RPM, 146 GB, RAID 0 (log file)
Network Adapter	1 x1,000 MB/s

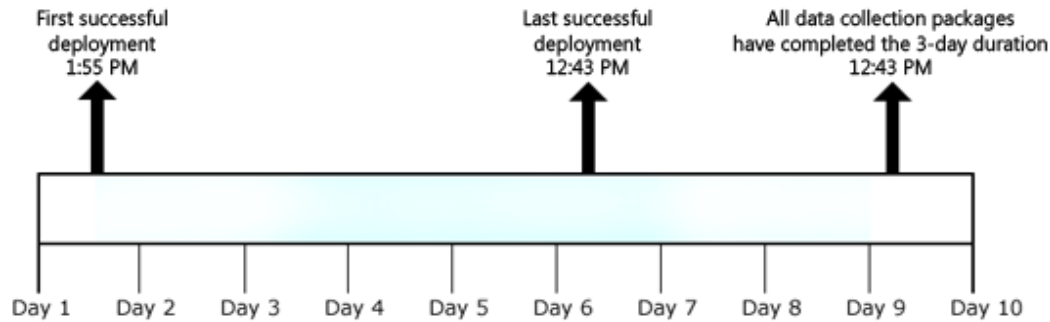
- Database settings used:

Database Portion	Initial Size	Growth	Final Size
Data	5 GB	500 MB	4.67 GB
Log Files	1 GB	100 MB	70 MB

3.2 DCP Log File Processing and Disk Space Utilization

The duration of the DCP is three days, which means that the DCP will run for three days after the successful deployment of the package to a client computer. The timeline (Figure 3) starts as soon as the first DCP is deployed and ends three days after the final DCP was deployed. Throughout this timeline, the file share is receiving data; however, the peak time occurs when the majority of the DCPs are installed and running.

Figure 3: Timeline of the DCP



The following tables provide data about processing times and disk space consumption for both the log files and database, while the graphs (Figure 4 and Figure 5) provide a graphic representation of the processing times for the data logs, and the database size based on computer.

Important

The DCP sends the compressed log files (.cab files) to the root folder of the file share. The ACT Log Processing Service decompresses the log files and stores them in the **Uncompressed** folder of the file share. After successfully processing the data from the uncompressed log file, the file is moved to the **Processed** folder, also located in the file share. In the event of a log file failure, the file is stored in the **Failed** folder of the file share, and an event is entered into the application event log, including the failure details. For the purposes of estimating disk space, we recommend using the average log size (uncompressed) value.

Data Log Files	Value
Total number of processed data log files	Approx. 67,494
Total processing time in hours	103
Average processing time	Approx. 18 seconds per log file
Average log file size (compressed)	78 kilobytes (KB)
Average log file size (uncompressed)	536 KB
Size of database for approx. 67,494 log files	Approx. 4.67 GB
Size of log files for approx. 67,494 log files	Approx. 70 megabytes (MB)

Status Log Files	Value
Total number of processed data log files	Approx. 97,748
Total processing time in hours	4.5

Status Log Files	Value
Average log file size (compressed)	.7 KB
Average log file size (uncompressed)	4 KB

Figure 4: Graphical representation of the processing time by the number of computers

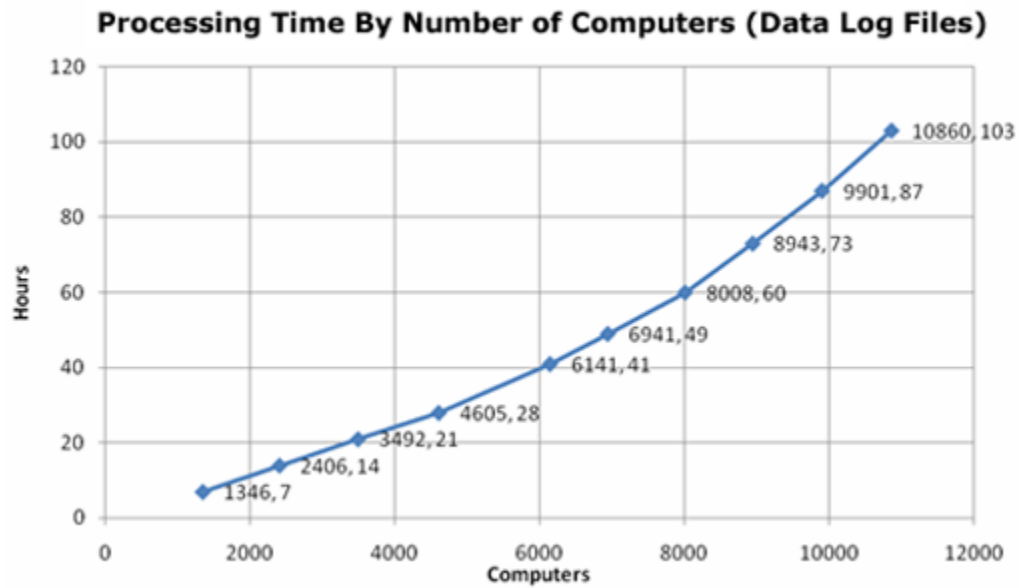
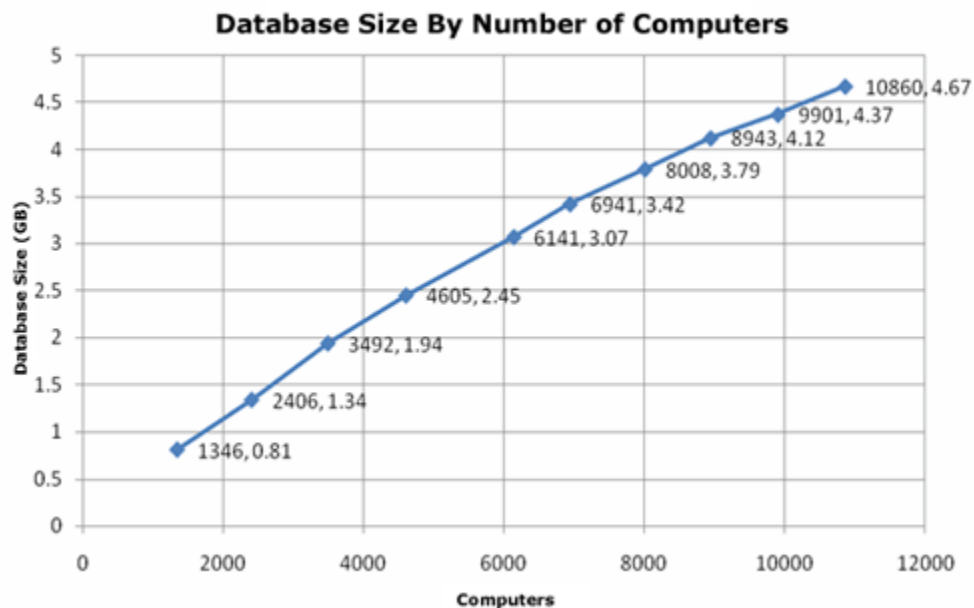


Figure 5: Graphical representation of the database size by the number of computers



4. ACT 5.6 Core Usage Scenarios

There are two core usage scenarios for ACT 5.6 in an Enterprise environment:

- Assessing compatibility issues around deploying a new operating system.
- Assessing compatibility issues around deploying a Windows Update.

The following are general recommendations for all of the usage scenarios, when employed in your organization:

- Ensure that your specified client computers represent all of your departments and geographic distribution.
- Collect your application, hardware, and device inventory from about 50,000 computers, but collect the compatibility data from only 5,000 computers if you have a large number of available client computers in your organization.
- If you are using a clean image in your test environment, you must ensure that you have installed all of your applications prior to running the DCP.

Note

This method is not recommended because your end users will not be using the applications while the DCP runs, and so will not ensure complete application usage.

4.1 Deploying a New Operating System

This walkthrough describes a scenario of an organization that is planning to deploy a new operating system into its environment, but first requires a more detailed assessment of the potential compatibility issues. For this scenario, you must deploy the associated data-collection

package (DCP) to at least one of your client computers that is running one of the following operating systems:

- Windows 7
- Windows Vista with Service Pack 1 or Service Pack 2
- Windows XP with Service Pack 2 or Service Pack 3
- Windows Server 2008 R2
- Windows Server 2003 with Service Pack 1 or Service Pack 2
- Microsoft Windows 2000 with Service Pack 4 and Update Rollup 1

To assess a new operating system deployment

1. On the taskbar, click **Start**, point to **All Programs**, point to **Microsoft Application Compatibility Toolkit 5.6**, and then click **Application Compatibility Manager**.
2. On the **Collect** screen, click **File** from the toolbar, and then click **New**.
The **New <DCP_Name>** dialog box appears.
3. In the **Package Name** box, type **Inventory_Collection**.
4. In the **Evaluate compatibility when** area, click **Deploying a new Operating System or Service Pack**.
5. Click **Advanced**.
The **Advanced Settings** dialog box appears.
6. Clear the **User Account Control Compatibility Evaluator** and **Windows Compatibility Evaluators** check boxes, and then click **OK**.
The **Advanced Setting** dialog box closes.
7. In the **When to monitor application usage** area, do not change the default options, but change the **Duration** to **10 Minutes**.
8. In the **Output Location** box, do not change the default value, previously specified in the ACT Configuration Wizard.
9. On the **File** menu, click **Save and Create Data Collection Package**.
10. Save the compiled DCP to your desktop.
The Application Compatibility Manager saves the DCP as a Microsoft® Windows® installer (.msi) file.
11. Determine which method you will use to deploy your DCP. These methods include Microsoft System Center Configuration Manager 2007, Group Policy Installation Software, logon scripts, or any custom deployment method already used within your organization.
12. Using the method determined in the previous step, deploy the DCP to your specified client computer's desktops.
13. Double-click the packaged DCP from each identified client computer's desktop.
The DCP runs on the client computer.

To view and synchronize your data

1. Click **Analyze** from the left-hand navigation pane.
The **Analyze** screen appears.
2. On the **Analyze** screen of your client computers, click **Send and Receive**.
The **Send and Receive Data** dialog box appears.
3. Click **Review the data before sending**.
The dialog box changes to show the applications that will send and will receive information from Microsoft during the synchronization process.



Note

You can disable specific applications from the synchronization process, so that you do not share the related issue data with Microsoft or the ACT Community. For more information, see the "Selecting Your Send and Receive Status" topic in the ACT Help.

4. Click **Send**.
Data synchronization occurs between your computer and the Microsoft Compatibility Exchange.
5. Return to the **Analyze** screen and review the updated issue data for your applications.

► **To collect your compatibility data**

1. On the **Collect** screen, click **File** from the toolbar, and then click **New**.
The **New <DCP_Name>** dialog box appears.
2. In the **Package Name** box, type **OS_Deployment**.
3. In the **Evaluate compatibility when** area, click **Deploying a new Operating System or Service Pack**.
4. In the **Output Location** box, do not change the default values.
5. On the **File** menu, click **Save and Create Data Collection Package**.
6. Save the compiled DCP to your desktop.
7. As you did previously, deploy your DCP and synchronize your data.

4.2 Applying a Windows Update

This walkthrough describes a scenario of an organization that is planning to deploy a Windows update into its environment, but first requires a more detailed assessment of the potential compatibility issues. For this scenario, you must deploy the associated DCP to at least one of your client computers that is running one of the following operating systems:

- Microsoft Windows 7
- Windows Vista with Service Pack 1 (SP1) or Service Pack 2 (SP2)
- Windows XP with Service Pack 2 (SP2) or Service Pack 3 (SP3)
- Windows Server 2008 R2
- Windows Server 2003 with Service Pack 1 (SP1) or Service Pack 2 (SP2)

- Microsoft Windows 2000 with Service Pack 4 (SP4) and Update Rollup 1

To assess a Windows update deployment

1. On the taskbar, click **Start**, point to **All Programs**, point to **Microsoft Application Compatibility Toolkit 5.6**, and then click **Application Compatibility Manager**.
2. On the **Collect** screen, click **File** from the toolbar, and then click **New**.
The **New <DCP_Name>** dialog box appears.
3. In the **Package Name** box, type **Inventory_for_Updates**.
4. In the **Evaluate compatibility when** area, click **Applying Windows Updates**.
5. Click **Advanced**.
The **Advanced Settings** dialog box appears.
6. Clear the **Update Compatibility Evaluator** check box, and then click **OK**.
The **Advanced Setting** dialog box closes.
7. In the **When to monitor application usage** area, do not change the default options, but change the **Duration** to **10 Minutes**.
8. In the **Output Location** box, do not change the default value, previously specified in the ACT Configuration Wizard.
9. On the **File** menu, click **Save and Create Data Collection Package**.
10. Save the compiled DCP to your desktop.
The Application Compatibility Manager saves the DCP as a Windows installer (.msi) file.
11. Determine which method you will use to deploy your DCP. These methods include Microsoft System Center Configuration Manager 2007, Group Policy Installation Software, logon scripts, or any custom deployment method already used within your organization.
12. Using the method determined in the previous step, deploy the DCP to your specified client computer's desktops.
13. Double-click the packaged DCP from each identified client computer's desktop.
The DCP runs on the client computer.

To view and synchronize your data

1. Click **Analyze** from the left-hand navigation pane.
The **Analyze** screen appears.
2. On the **Analyze** screen of your client computers, click **Send and Receive**.
The **Send and Receive Data** dialog box appears.
3. Click **Review the data before sending**.
The dialog box changes to show the applications that will send and will receive information from Microsoft during the synchronization process.



Note

You can disable specific applications from the synchronization process, so that

you do not share the related issue data with Microsoft or the ACT Community.
For more information, see the "Selecting Your Send and Receive Status" topic in the ACT Help.

4. Click **Send**.
Data synchronization occurs between your computer and the Microsoft Compatibility Exchange.
5. Return to the **Analyze** screen and review the updated issue data for your applications.

► **To collect your compatibility data**

1. On the **Collect** screen, click **File** from the toolbar, and then click **New**.
The **New <DCP_Name>** dialog box appears.
2. In the **Package Name** box, type **Update_Deployment**.
3. In the **Evaluate compatibility when** area, click **Applying Windows Updates**.
4. In the **Output Location** box, retain your default value, previously specified in the ACT Configuration Wizard.
5. On the **File** menu, click **Save and Create Data Collection Package**.
6. Save the compiled DCP to your Desktop.
The Application Compatibility Manager saves the DCP as a Windows installer (.msi) file.
7. As done previously, deploy your DCP and synchronize your data.



5. ACT 5.6 Software, Hardware, and Configuration Requirements

Before configuring and running ACT 5.6, you must verify that you are running supported software, that you meet the minimum hardware requirements, and that you have configured the required permissions and infrastructure.

5.1 Software Requirements

The following sections list the software and hardware requirements for using ACT 5.6.

Type of Software	Supported Versions
Operating Systems	<ul style="list-style-type: none"> • Windows 7 • Windows Vista • Windows Vista with Service Pack 1 or Service Pack 2 • Windows XP with Service Pack 2 or Service Pack 3 • Windows Server 2008 R2

Type of Software	Supported Versions
	<ul style="list-style-type: none"> Windows Server 2003 with Service Pack 2 <p> Important The Application Compatibility Manager, the Internet Explorer Compatibility Test Tool (IECTT), and the Compatibility Administrator are not supported on Windows 2000. However, you can run DCPs on computers running Windows 2000 Update Rollup 1 for SP4.</p>
Database Components	<p>After ACT has been installed, it requires one of the following database components:</p> <ul style="list-style-type: none"> Microsoft SQL Server 2008 SQL Server 2005 SQL Server 2008 Express SQL Server 2005 Express Edition <p> Note ACT 5.6 does not support SQL Server 2000 or the Microsoft Database Engine (MSDE).</p>
.NET Framework	ACT requires the .NET Framework 3.5 or newer.

5.2 Hardware Requirements

The following table contains the minimum and recommended hardware requirements.

ACT components	Minimum requirements	Recommended requirements
Application Compatibility Manager client and ACT Log Processing Service servers	550-megahertz (MHz) processor with 256 megabytes (MB) of RAM	2.8-gigahertz (GHz) processor with 2 gigabytes (GB) of RAM
ACT client databases	1-GHz processor with 512 MB of RAM	2.8-GHz processor with 2 GB of RAM

5.3 Special Software and Hardware Considerations

There are special system requirements that you must provide before you can successfully use the Update Compatibility Evaluator (UCE) or the Compatibility Administrator.

5.3.1 Special Requirements for Using the UCE

The UCE data collection packages require that you use only specific operating systems, meet specific hardware requirements, and provide sufficient disk space.

5.3.1.1 UCE Supported Environments

The following operating systems are supported by the UCE.

- Windows 7
- Windows Vista with Service Pack 1 or Service Pack 2
- Windows XP with Service Pack 2 or Service Pack 3
- Windows Server 2008 R2
- Windows Server 2003 with Service Pack 1 or Service Pack 2
- Windows 2000 with Service Pack 4 and Update Rollup 1

**Note**

The UCE is not supported on earlier versions of the previously listed operating systems, including Windows NT.

5.3.1.2 Hardware Requirements

The following minimum hardware requirements are necessary to run the UCE:

- **Disk drive.** 1 GB of free space
- **RAM.** 256 MB

5.3.1.3 Disk Space Usage

By default, the UCE limits its disk space usage to 50 percent of available disk space. This setting attempts to provide enough padding so that the compatibility evaluator does not use all of the free disk space. During an average deployment, the UCE typically logs at least 100 MB per hour of Event Tracing Log (ETL) files. Therefore, if you use a four-hour upload interval, the compatibility evaluator will require at least 400 MB of free space. You can modify the percentage of disk space used in the **Advanced Settings** dialog box.

5.3.2 Special Requirements for Using the Compatibility Administrator

The computer on which you intend to use the Compatibility Administrator must have one of the following operating systems:

- Windows 7
- Windows Vista with Service Pack 1 or Service Pack 2
- Windows XP with Service Pack 2 or Service Pack 3
- Windows Server 2008 R2
- Windows Server 2003 with Service Pack 2

- Windows 2000 with Service Pack 3 or newer



Note

The Compatibility Administrator does not support Limited User Account (LUA) mode in Windows 2000.

5.4 Recommended ACT Database Configuration and Modifications

You can create the ACT database by using one of the following options:

- While you are configuring ACT, you can use the ACT Configuration Wizard to create a new database.
- or-
- You can run the CreateDB.sql file. Refer to the following table for the location, based on your operating system:

Operating System	Location of the CreateDB.sql File
Windows 7 Windows Vista Windows Server 2008 R2	%SYSTEMDRIVE%\ProgramData\Microsoft\Application Compatibility Toolkit\CreateDB.sql
Windows XP with Service Pack 2 or Service Pack 3 Windows Server 2003 with Service Pack 1 Microsoft Windows 2000 Server with Update Rollup 1 for Service Pack 4	%SYSTEMDRIVE%\Documents and Settings\All Users\Application Data\Microsoft\Application Compatibility Toolkit\CreateDB.sql

5.4.1 ACT Database Role Assignments

You must assign the following database roles to the specified accounts.

- You must assign the **db_datareader**, **db_datawriter**, and **db_owner** database roles to the user and local service accounts that will be used to run the ACT Log Processing Service.
- You must assign the **db_datareader** and **db_datawriter** database roles to the user account that will log on to the computer running the Application Compatibility Manager.



Important

You must grant the following explicit permissions to each specific user on the ACT database. Without these permissions, the Application Compatibility Toolkit will fail to function for that user.

- SELECT

- INSERT
- UPDATE
- DELETE
- EXECUTE

5.4.2 Additional ACT Database Recommendations

We also recommend that you make the following changes to the database, as a part of your deployment planning:

- Create a larger database, including a larger log file size setting, and then set the growth increments appropriately. If you create a database with the default setting for data storage, then the data portion of the database will have an initial size of 1 megabyte (MB), and a growth increment of 1 MB. If you create a database with the default setting for the log file storage, then the log file portion of the database will have an initial size of 1 MB, and a growth increment of 10 percent. We recommend that you try to maintain a data-to-log file ratio of 5:1 or 4:1. For example, if your data portion is 5 gigabytes (GB), then your log file portion should be 1 GB.
- Change the recovery model of your database. The default recovery model is **Full**, but we recommend that you change this model setting to **Simple**.
- Separate the hard drives on which you store your data portion and log file portion. The default, unless altered by your SQL Administrator, is for both the data and log files to be stored on the same hard drive. Separating the data from the log files will reduce disk I/O contention.

5.5 Required Privileges for the ACT Log Share

You must have two sets of permissions configured for the ACT Log Processing Service share:

- Permission for the DCPs that run on your local computers to upload the log files to the ACT Log Processing Service share.
- Permission for the ACT Log Processing Service to process the data provided from the share to the ACT client database.



Note

The ACT Configuration Wizard automatically sets these permissions.

If you are having trouble writing to the ACT Log Processing Service share or processing the log files from the ACT Log Processing Service share, you must verify that you have the correct permissions at both the share level and the folder level.

5.5.1 Share-Level Permissions

You must verify that the **Everyone** group has **Change** and **Read** permissions for the ACT Log Processing Service share folder.

► To verify the share-level permissions

1. Right-click the ACT Log Processing Service share folder, and then click **Properties**.
2. Click the **Sharing** tab, share the folder, and then click **Permissions**.
3. Add the **Everyone** group, if it is not already there, and then click the **Change** and **Read** permission check boxes in the **Allow** column.

5.5.2 Folder-Level Permissions (NTFS Only)

You must verify the following permissions:

- The **Everyone** group has **Write** access.
- The ACT Log Processing Service account has **List Folder Contents**, **Read**, and **Write** permissions, based on the following criteria:
 - **Local System Account**. You must apply these permissions to the `<domain_name>\<machine_name>$` account.
 - **User Account**. You must apply these permissions to the specific user.

To verify or to change the folder-level permissions

1. Right-click the ACT Log Processing Service share folder, and then click **Properties**.
2. Click the **Security** tab, add the ACT Log Processing Service share account, and then click the **List Folder Contents**, **Read**, and **Write** permission check boxes in the **Allow** column.
3. Add the **Everyone** group, if it is not already there, and then click the **Write** permission check box in the **Allow** column.

5.5.3 Additional Troubleshooting Notes

If you are still having issues uploading your log files to the file share, you can try these additional troubleshooting methods:

- If you are using computers from different domains to run your DCPs and the ACT Log Processing share, you must provide explicit **Write** permissions for the **Anonymous** group to the ACT Log Processing share. You must also provide these permissions if you are uploading data from a non-domain-joined computer. For more information, see [Everyone Group Does Not Include Anonymous Security Identifier](#).
- If you are running your DCPs on computers using Windows 2000 and uploading your collected data to an ACT Log Processing share located in a different domain, in addition to the tip above, you must also explicitly enable null session access for the ACT Log Processing share. For more information, see [How to enable null session shares on a Windows 2000-based computer](#)

5.6 Required Infrastructure for the Microsoft Compatibility Exchange

You must configure your organization's infrastructure to support the Microsoft Compatibility Exchange, while also protecting your intranet security and stability. The recommended method of

configuration requires you to allow the appropriate users, on designated computers, to access the Microsoft Compatibility Exchange through your security and network infrastructure. Configure your firewalls and URL scanners to allow access to the Microsoft Compatibility Exchange, as follows:

- Allow outbound access for the standard Secure Sockets Layer (SSL) TCP port 443, on any computer running the Application Compatibility Manager.
- Restrict outbound access to the Microsoft Compatibility Exchange, allowing access only from designated computers and designated users within your organizations.
- Enable access to the Microsoft Compatibility Exchange URL, **<https://appinfo.microsoft.com/AppProfile50/ActWebService.asmx>**, (only necessary if passing through a firewall).