Microsoft ACT: Phase 1 - Collecting Data

Microsoft Corporation

Published: May 2010

Abstract

This paper provides step-by-step information about using the Microsoft® Application Compatibility Toolkit (ACT) 5.6 to create data collection packages (DCPs) and deploy them within your organization.

This information applies to the following operating systems:

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

Copyright Information

Contents

Microsoft ACT: Phase 1 - Collecting Data

Microsoft® Application Compatibility Toolkit (ACT) 5.6 enables software developers, independent software vendors (ISVs), and IT professionals who work in a corporate environment to determine, before rolling out within the organization, whether their applications are compatible with a new version of the Windows® operating system. ACT also enables such individuals to determine how an update to the new version will impact their applications.

You can use the ACT features to:

- Verify your application's, device's, and computer's compatibility with a new version of the Windows operating system, including determining your risk assessment.

- Verify a Windows update's compatibility, including determining your risk assessment.

- Become involved in the ACT Community, including sharing your risk assessment with other ACT users.

- Test your applications for User Account Control (UAC)-related issues by using the Standard User Analyzer (SUA) tool.

- Test your Web applications and Web sites for compatibility with new releases and security updates to Internet Explorer® by using the Internet Explorer Compatibility Test Tool.

> **Important**
> For more detailed information about all of the material in this white paper, see the ACT Help.

How ACT Works

ACT 5.6 provides a way for you to create an inventory for your organization, including your installed applications, computers, and devices. It also enables you to collect compatibility data, to determine the impact of that data in your organization, and, finally, to create mitigation packages to fix the compatibility issues, when possible. There are three phases for effectively using ACT in your organization. The three phases are:

- **Phase 1: Collecting Data**. Before you can analyze your potential compatibility issues, you must first collect your organization's inventory and the associated compatibility issues. This information is included in this white paper.

- **Phase 2: Analyzing Issues**. After collecting your inventory and associated compatibility data, you can organize and analyze your issues. This includes categorizing, prioritizing, setting your deployment status, and setting your application assessment to create customized reports. For more information, see the "Microsoft ACT: Phase 2 - Analyzing Issues" white paper, available for download from the **Related Resources** section of the Microsoft Application Compatibility Toolkit 5.6 Download Web page.

- **Phase 3: Mitigating Issues by Using Compatibility Fixes**. After analyzing your compatibility issue reports, you can do the following:

- Manually test your applications for functionality-related issues
- Use the Standard User Analyzer (SUA) tool to automatically test for user account control (UAC)-related issues
- Create mitigation packages for valid issues by using the Compatibility Administrator

For more information, see the Microsoft ACT: Phase 3 –Mitigating Issues by Using Compatibility Fixes white paper, available for download from the **Related Resources** section of the Microsoft Application Compatibility Toolkit 5.6 Download Web page.

Data Collection Workflow

The ACT collects data according to the following workflow.

1. You create a new data collection package (DCP), by using the Application Compatibility Manager. Each DCP can contain one or more compatibility evaluators, including the Inventory Collector.

2. You deploy the DCPs to your identified subset of client computers, by using the Microsoft System Center Configuration Manager 2007, Group Policy, or any other software distribution technology. The evaluators run for the length of time that you specified when creating the DCP, and then the data (.cab) file is uploaded to your ACT Log Processing share.

3. The ACT Log Processing Service, running on a server, accesses the data from the ACT Log Processing share, processes the data.

4. The ACT Log Processing Service uploads the information to your ACT database.

5. Finally, the Application Compatibility Manager reads the data from your ACT database to determine how many computers have uploaded data and the status of the collection process. The Application Compatibility Manager also uses the data from the ACT database to enable reporting and viewing of the collected data.

Collecting Your Compatibility Data

By using the Application Compatibility Manager, you can create DCPs—a package of compatibility evaluators that are used to gather your installed software, hardware, and device information, in addition to determining any associated compatibility issues based on application or Windows® update—for your selected client computers. ACT includes the following compatibility evaluators.

- **Inventory Collector**. Examines each of your organization's computers, identifying the installed applications and system information. The Inventory Collector is automatically included in any DCP that you create because the Application Compatibility Manager requires a complete inventory from your identified computers before it can determine any associated issues.

- **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® or Windows 7 operating system. UACCE monitors

your running applications to verify interactions with the operating system and to identify potentially incompatible activities.

- **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.

- **Update Compatibility Evaluator (UCE)**. Identifies the potential impact of a new Windows Update. By using the collected update impact data, you can prioritize your testing and reduce the potential risks of compatibility issues when you deploy the Windows Updates.

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.

💠 **Important**

The compatibility evaluators are not supported on earlier versions of the listed operating systems or on Windows NT®.

Creating a DCP

From the Application Compatibility Manager, you can create new DCPs, which can then be deployed to your client computers to collect inventory and potential issue data.

▶**To access the Collect screen**

- In the Application Compatibility Manager navigation pane, click **Collect**.

  The **Collect** screen appears with all of your existing DCPs sorted by name or by status.

▶**To create a new data-collection package**

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 a custom name for your data-collection package.

3. In the **Evaluate compatibility when** area, click one of the following options:

   - **Deploying a new Operating System or Service Pack**. Enables you to detect potential issues with your installed software and devices, due to the deployment of a new operating system or a service pack. This option runs the Inventory Collector, the Windows Compatibility Evaluator (WCE), and the User Account Control Compatibility Evaluator (UACCE) evaluators.

   - **Applying Windows Updates**. Enables you to detect potential software and device issues that might occur due to the deployment of a Windows update. This option runs the Inventory Collector and the Update Compatibility Evaluator (UCE) evaluators.

4. Click **Advanced**.

The **Advanced Settings** dialog box appears.

5. Review the compatibility-evaluator information. You can clear any compatibility-evaluator check boxes that you do not want to run in your organization, if required.

    Important

    If you intend to deploy your DCP to any computer that is running the Windows 2000 operating system, you must select the **Prompt users to restart if required by the installation (Microsoft Windows 2000 only)** check box.

    Note

    If you are creating a DCP for the **Applying Windows Updates** option, you will be able to configure additional settings, such as whether to disable registry logging, the maximum amount of disk space to use, whether to include filtered applications, and so on.

6. In the **When to monitor application usage** area, define when your data-collection package will run and for how long, including:

    *   **Starting**: To set the date and the time that your data-collection package will begin collecting data, click one of the following options:

        *   **As soon as possible after install**
        *   **At specified date and time**

            Important

            ACT uses Coordinated Universal Time (UTC) instead of local time. Therefore, if you set your data-collection package to start at 6:05 P.M. Eastern Standard Time and run for five minutes, the data-collection package will actually start at 3:05 P.M. Pacific Standard Time, 5:05 P.M. Central Standard Time, 6:05 P.M. Eastern Standard Time, and so on. Selecting a specific date and time means that your compatibility evaluators will not begin collecting data until your configured date and time. However, you must deploy your data-collection package prior to your specified time, so it can install your compatibility evaluators.

    *   **Duration**: In the box, type a numerical value that defines how long the data-collection package will run, and then select **Days**, **Hours**, or **Minutes** in the list.

        Important

        Your data-collection package duration runs in chronological time. Therefore, if you shut down your computer and the specified duration elapses while the computer is off, when you turn the computer back on, the data is uploaded and the data-collection package exits.

    *   **Upload data every**: Select **2 hours**, **4 hours**, **8 hours**, or **12 hours**, depending on how long you set ACT to wait between each upload of your application-compatibility data.

> 🔹 **Important**
>
> If you are running a data-collection package based on the Applying Windows Updates option, we recommend that you select the 2-hour upload option.

7. In the **Output Location** field, browse to the directory location to store your log files.

8. In the **Label name** field, add any unique text you want to use to identify your collected data. For example, if the data will be collected from your sales department, you can add the term, "Sales" and it will be automatically added to every returned data item.

9. On the toolbar, click **Save and Create Package**, click **Browse** to select the directory location to store your compiled package, and then click **Save**.

   The data-collection package is created and stored in your selected location, and then the **New <DCP_Name>** dialog box closes.

10. Deploy and run your data-collection package.

Deploying Your DCP

The following sections provide guidance about the deployment process, including helping you to determine which computers should be used, which method of deployment you should use, and how to deploy the DCP using that deployment method.

Determining Where to Deploy a DCP

You deploy your DCPs to only a subset of the computers in your organization. To help you determine which computers to use, consider the following:

- Ensure that you return a complete application inventory, including all of your business-critical and day-to-day required line-of-business (LOB) and third-party applications. We highly recommend that this list include any application that is used by at least one person to perform his or her daily tasks. To ensure that this list is complete, we also recommend that you use a cross-section of computers from your organization.

- Capture the runtime properties and the dependencies of installed applications, including accessed DLLs and accessed or modified registry settings. These dependencies can help locate potential compatibility issues.

- Ensure that all device drivers are captured so that the proper impact can be assessed during an operating system or a patch upgrade, in addition to being able to locate potential issue and solution data provided by original equipment manufacturers (OEMs) and independent software vendors (ISVs).

Factors to Consider for Data-Collection Package Deployment

For greater control over your collected data, IT administrators should focus their DCPs for deployment to a small subset of computers based on specific categories. For example, a data-collection package targeted to users in the United States Human Resources department. This enables better categorization and analysis of an application throughout the organization.

📝 Note

If your organization already has a hardware-asset inventory list, we recommend 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 as widely as possible to obtain this list.

In addition, you must consider the following questions during your data-collection package deployment:

- Do you have a managed, unmanaged, or mixed environment?
- How do you use specific applications in your organization?
- Do you use role-based applications?
- How do you distribute your applications in your organization?
- What is the geographic breakdown of your organization?
- What types of computers do you have in your organization? How are they used?

Managed and Unmanaged Environments

An organization can be categorized into a managed environment, an unmanaged environment, or a mixed management environment.

- **Managed environment.** IT administrators strictly control and manage the application installation and the usage based on need and the various divisions in the organization. In this situation, an IT administrator can deploy a data-collection package 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 will 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.

Application Usage

It is very important that you provide coverage for all applications required by users in your organization. However, it is even more important that you provide coverage for your LOB applications. For the most complete coverage of application usage, you must:

- Consult with your local administrators, support engineers, and department leads to ensure that all applications are being used during the data-collection process.
- Ensure that "seasonal" applications are covered. For example, fiscal year–accounting applications may 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 may get limited or incomplete results due to the decreased application usage.

Role-based Application Usage

Your organization may use role-based applications. These are applications that relate to job function and the role a user performs within your organization. A common example is accountants (a finance role) and their finance-related applications. Reviewing application usage in conjunction with job function and roles enables better application coverage in your organization.

Software Distribution Practices

You can distribute applications in many ways within an organization, for example, by using Group Policy, IntelliMirror, Microsoft System Center Configuration Manager, or a customized distribution method. Reviewing your software distribution–system policies with your application inventory enables better application coverage and narrows your data-collection package deployment targets.

Geographic Distribution of the Organization

Your organization's geographic distribution must be considered when planning for your data-collection package 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 will need to account for divisional applications, localized versions of applications, and applications specific to the geographic location and export restrictions. We highly recommend that you consult with technical and business leaders from each region to understand these differences.

Computer Types and Usage

Computer types and usage patterns can play an important role in your data-collection package deployment. The following sections describe some of the most common computer types and usage patterns.

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 data-collection package 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 destination computers to receive the data-collection package.

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 enable users to add or remove applications and may be focused

for specific users and job roles, the application coverage and usage can be narrowed to identify what should receive the data-collection package.

Kiosks

Kiosks are generally in public areas. These computers run unattended and are highly secure, generally running a single program 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 what should receive the data-collection package.

Determining How to Deploy a DCP

There are several ways to distribute a data-collection package (DCP) to your desired destination computers. Four recommended methods are:

- **Group Policy Software Installation**. Use the Group Policy Software Installation feature of Active Directory® 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 data-collection package. Installing with a logon script requires administrator credentials on the local computer.

- **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.

  Note

  For more information about using Configuration Manager, refer to the product documentation.

- **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. Please note that self-installation of a data-collection package requires administrator credentials on the local computer.

The method that you choose will depend on your specific organization and preferences.

Important

ACT uses Coordinated Universal Time (UTC) instead of the local time. Therefore, if you set your data-collection package to start at 6:05 P.M. Eastern Standard Time and run for five minutes, the data-collection package will actually start at 3:05 P.M. Pacific Standard Time, 5:05 P.M. Central Standard Time, 6:05 P.M. Eastern Standard Time, and so on.

Deploying a DCP

The following sections provide instructions for deploying your DCP into your environment, based on the deployment method you selected.

Deploying a DCP by Using Group Policy

If your organization has an existing Active Directory infrastructure, you can deploy the DCPs to your identified subset of client computers by using Group Policy Software Installation.

▶**To deploy a DCP by using Group Policy Software Installation**

1. Ensure that your identified client computers are members of the Active Directory forest.
2. Create a Group Policy object (GPO) for publishing the data-collection package.
3. Assign the GPO to the organizational units (OUs) containing your identified subset of client computers.
4. Create and publish a new software installation package by using Group Policy Software Installation.

   📝 **Note**

   For more information about the Group Policy Software Installation process, see Best practices for Group Policy Software Installation.

Deploying a DCP by Using a Logon Script and Active Directory

You can deploy your DCPs to your client computers by creating a logon script and then assigning the script to your organizational unit through the Microsoft Active Directory service and Group Policy. For more information about logon scripts, see Assign a Logon Script to a User in the Active Directory and How to Automate Logon Processes Using Scripts

Creating a Logon Script

The following is a simple logon script example.

```
Set ws = WScript.CreateObject("WScript.Shell")

ws.Run("\\servername\collector\DCP_name.exe")
```

After creating the script, you must save it to a network location that is accessible to everyone who is required to run the script. When users log on to their computers, the script automatically runs, collecting the data and storing it in the location defined by the script.

Deploying the DCP by Using the Logon Script and Active Directory

You can assign your logon script to run for a specific Group Policy, by using the **Active Directory Users and Computers** console. From the console, you can modify the properties for an Active Directory container, and then assign your Group Policy to your specific Active Directory organizational unit.

🔵 **Important**

To change Group Policy, you must be a Domain Administrator and have security access to the organization unit.

▶**To assign a logon script to an organization unit by using Active Directory**

1. Save your script in the SYSVOL\Scripts folder.

2. To open the Active Directory console, click **Start**, then point to **All Programs**, then **Administrative Tools**, and then click **Active Directory Users and Computers**.

3. Right-click the organizational unit that you intend to assign the logon script to, click **Properties**, and then click the **Group Policy** tab.

4. Click **New** to add a new Group Policy object, or select an existing Group Policy object, and then click **Edit**.

    The **Group Policy Management Console** appears.

5. In the left pane, expand the **User Configuration** object, expand the **Windows Setting** object, and then click **Scripts (Logon/Logoff)**.

6. In the right pane, double-click the **Logon** script.

    The **Logon Properties** dialog box appears.

7. Click **Add**.

    The **Add a Script** dialog box appears.

8. Click **Browse**, browse to the \\<*domain*>\Sysvol\Scripts folder, select your script, and then click **Open**.

    The script appears in the **Add a Script** dialog box.

9. Click **OK** to close the **Logon Properties** dialog box.

10. Close the **Group Policy Management** console and the **Active Directory Users and Computers** console.

11. On a client computer that is both a member of the domain and a part of the organization unit, log on as an organization unit user.

12. Open a **Command Prompt** window, and then type `GPUPDATE /force` to force the update of the Group Policy.

13. At the command prompt, type `RSOP.msc` to verify your Group Policy assignment.

    The **Resultant Set of Policy** console appears.

14. In the left pane, expand the **Computer Configuration** object, expand the **Windows Setting** object, and then click **Security Settings**.

15. Expand **Account Policies**, click **Password Policy**, and verify the assigned Group Policy.

16. Close the **Resultant Set of Policy** console and the **Command Prompt** window.

    ◆ **Important**

    To keep the installation from running repeatedly, your script needs to create a marker.

Deploying a DCP by Using System Center Configuration Manager

If your organization has existing Configuration Manager infrastructure, you can deploy the DCPs to your identified subset of client computers by using the Configuration Manager software distribution feature.

▶**To deploy a DCP by using System Center Configuration Manager**

1. Verify that the specified client computers are included in your Configuration Manager inventory.
2. Create a Configuration Manager computer collection that includes the specified computers.
3. Create a shared folder with the source image of the DCP.
4. Create a Configuration Manager package that is based on the source image in the shared folder. For more information about creating a package, see How to Create a Package.
5. Specify the Configuration Manager software distribution points.
6. Create a Configuration Manager program, including the required commands and command-line options to deploy the DCP. For more information about creating a program, see How to Create a Program.
7. Create a Configuration Manager advertisement, instructing Configuration Manager clients to run the program specified in the previous step. For more information about creating an advertisement, see How to Create an Advertisement.

Manually Deploying a DCP

You can deploy your data-collection package to your client computers, either by saving the package to a CD or by placing the executable file on a network share and instructing your users how to download and to run the file.

⬥ **Important**

Regardless of the deployment method that you use, you must indicate an output path where the log file should appear on the user's computer. If you do not define an output path, the log file will appear on your current ACT Log Processing Service share. Additionally, if you specify **local** when you create your data-collection package, your default local folder will appear within the All Users\Application Data folder.

Deploying a DCP from a Network Share

The following procedure explains how to deploy your data-collection package executable file from a network share.

▶**To deploy a DCP from a network share**

1. Store your data-collection package (.msi) file in a shared folder on your network.
2. Create an e-mail message for distribution to all of the client computers that require the

data-collection package.

3. Create a hyperlink to the shared folder that you created in step 1.

📝 **Note**

> An example of the hyperlink is *File://\\server\share\collect.exe*. In this case, the output log will be stored on the user's desktop by default.

4. Instruct your users to run the executable file and to return the generated log file, either by sending it in an e-mail message or by placing it on a network share created for this purpose.

Deploying a DCP from a CD

If you have remote users who rarely connect to your network, you can choose to distribute your data-collection package, by using a CD.

▶**To deploy a DCP by using a CD**

1. Burn your data-collection package (.msi) file to a CD.

📝 **Note**

> You can also create an Autorun.inf file to cause the DCP file to run automatically when the user inserts the CD into the CD drive.

2. Send the CD to your users, instructing them to run the file and to return the generated log file, either by sending it in an e-mail message or by placing it on a network share created for this purpose.

Viewing the Status of Your DCPs

The **Collect** screen enables you to view your existing DCPs by name or by status.

Viewing Your DCPs by Name

You can sort and view your existing DCPs by name.

▶**To sort by name**

1. In the Application Compatibility Manager navigation pane, click **Collect**.

2. Click **By Name** from the **Current View** area of the **Collect** screen.

   The **Collect** screen shows the existing DCPs sorted by name, including the following information:

   - **Data Collection Package Name**. Your unique name for the DCP.

   - **Last Updated**. The date that the DCP was last changed.

   - **Log File Location**. The location selected for storing the log file for this DCP.

   📝 **Note**

Double-clicking on the DCP name opens the
<data_collection_package_name>- **Application Compatibility Manager**
dialog box so that you can modify the DCP.

Viewing Your DCPs by Status

You can sort and view your existing DCPs by status.

▶ **To sort by status**

1. In the Application Compatibility Manager navigation pane, click **Collect**.
2. Click **By Status** from the **Current View** area of the **Collect** screen.

   The **Collect** screen shows the existing DCPs, including the following information:

   - **Data Collection Package Name**. Your unique name for the DCP.
   - **Number of Computers**. The number of computers on which the DCP has run.
   - **Complete**. The number of computers on which the DCP has successfully completed.
   - **In Progress**. The number of computers on which the DCP is currently running.
   - **With Errors**. The number of computers on which the DCP generated errors.

   📝 **Note**

   Double-clicking the name of a DCP opens the
   <data_collection_package_name> dialog box so that you can view any issues
   and the general status information for the DCP.

Exporting and Importing DCPs

ACT 5.6 enables you to export and import existing DCPs. When exporting a DCP, ACT makes a copy of the file, enabling you to change the name and use the existing settings, without requiring you to start with a blank DCP. When importing a DCP, you must verify that the imported file name does not match another package already present in the ACT database. If the name already exists, you will receive an error. To fix this issue, rename the DCP that you are importing.

🔹 **Important**

Your DCPs must be sorted by name to export or import your packages.

▶ **To export a data-collection package**

1. On the Application Compatibility Manager toolbar, click **Export data collection package(s)**.

   The **Export <DCP_Name>** dialog box appears.

2. Browse to the folder that you want to store your DCP in, and then click **Save**.

   The Application Compatibility Manager exports your DCP settings, uses them to create a copy of your DCP executable (.exe) file, and then saves the information in the folder that

you specified.

📝 **Note**

>   After you create the DCP, you can deploy it within your organization.

▶ **To import a data-collection package**

1. On the Application Compatibility Manager toolbar, click **Import data collection package**.

    The **Open** dialog box appears.

2. Browse to the folder that contains your existing DCP, and then click **Open**.

    The Application Compatibility Manager saves the settings used to define your DCP, and the information becomes available on the **Collect** screen.

📝 **Note**

>   An error will occur if you attempt to import a DCP with the same name as that of a package already present in the ACT database. To fix this issue, rename the DCP that you are importing.