IBM Tivoli Configuration Manager

Readme File for Interim Fix 4.2.3-TCM-0002

Version 4.2.3

IBM Tivoli Configuration Manager

Readme File for Interim Fix 4.2.3-TCM-0002

Version 4.2.3

Note

Before using this information and the product it supports, read the information in "Notices" on page 43.

First Edition (December 2005)

This edition applies to interim fix 4.2.3-TCM-0002 for version 4, release 2, modification level 3 of IBM Tivoli Configuration Manager (program number 5724-C06).

Contents

Tables

Chapter 1. IBM Tivoli Configuration Manager Readme File for Interim Fix 4.2.3-TCM-0002

This readme file provides important information about 4.2.3-TCM-0002 interim fix for IBM® Tivoli® Configuration Manager Version 4.2.3. This interim fix fixes a variety of defects on Inventory, Scalable Collection Service, Software Distribution, Activity Planner, and Patch Management components.

Please review this section thoroughly before installing or using this interim fix.

About this release

This section includes the following topics:

Directory structure

IBM Tivoli Configuration Manager, Version 4.2.3 interim fix 4.2.3-TCM-0002 includes the following directories:

Table 1. IBM Tivoli Configuration Manager, Version 4.2.3 interim fix 4.2.3-TCM-0002

Directory or path	Contents
/docs	Readme files.
/xml	To install interim fixes using the ISMP installation program, the `423CM002.xml` file contained in this directory must be copied locally and referred to at the installation time.
/images	Images required for this interim fix.
/package	Software package block files used to patch GUI components and the `CM423_SPB_0002.xml` descriptor file.
/spb_installer	SPB Patch Installer that installs SPB interim fixes locally.

New features

The following new features have been introduced in this interim fix:

Table 2. Customer enhancement request references in this interim fix

Emergency patch management	Feature 56053
Patch Management deployment paradigm	
Enable Move Data to retrieve AS/400 spool file	Feature 56336

Emergency patch management - Feature 56053

The Configuration Manager Patch Management solution identifies the set of patches to be deployed to each endpoint on the basis of a preventive endpoint inventory scan. This scan might cause critical delay in the patch installation. When the Administrator responsible for approval determines that an update, released in an important Microsoft security bulletin, needs to be implemented immediately, he can use the emergency patch management feature to defer the preventive inventory scan and install the update as soon as possible. For more information on this feature, see "Managing emergency patches" on page 21.

Patch Management deployment paradigm

This feature extends Software Distribution capabilities to the Patch Management solution, enabling the Patch Management component to retrieve the software package to be installed from a depot or a file server, rather than the source host. Use this feature in environments with communication problems, when retrieving a software package from a source host might take time. For more information on this feature, see "Deployment Paradigms" on page 22.

Enable Move Data to retrieve AS/400 spool file - Feature 56336

With this feature the Data Moving Service in an OS/400 environment has been extended. You can now move OS/400 spool files from an OS/400 system to a Windows or UNIX target. Target systems can be endpoints or managed nodes. To differentiate the spooled files from the OS/400 native files, when running the **wspmvdata** command, specify the path name using the following format:

```
Job Number/Job User/Job Name/Spooled File Number
```

Ensure that `Job Number` is not preceded by a slash.

As an example see the following command:

```
wspmvdata -c -s @swd400 -t @intermesoli -P
sp:028421/qtivoli/qlcfd/1 -P tp:/targetdir qprint
```

Where:

swd400
: Is the OS/400 host name.

intermesoli
: Is the receiver host name, either a managed node or an endpoint.

sp:028421/qtivoli/qlcfd/1
: Identifies the spool file on the OS/400 system. If you omit the spooled file number (1 in this example), and more than one spool file exists for the same job, the last created spooled file is retrieved.

/targetdir
: Is the destination path on the target system.

qprint
: Is the spooled file name to be retrieved. Do not use wildcards for spooled file names.

When performing a retrieve operation of an OS/400 spooled file, a new file is created under the specified destination directory using the following naming convention:

```
JobNumber.JobUser.JobName.SpooledFileNumber.SpooledFileName
```

In the example described above this file is `/targetdir/028421.qtivoli.qlcfd.1.qprint`.

Notes:

1. Notice the usage of the codepage translation option (**ûc**) in the example described above. Using this argument results in the OS/400 spooled file being translated from EBCDIC to ASCII codepage, before it is written to the UNIX or Windows destination location.
2. If the target system is a managed node, a subdirectory with the name of the origin host is created inside the destination directory on the target system. The naming convention for the subdirectory is as follows:

   `endpointname_distributionID_timestamp`

For more details on the **wspmvdata** command, refer to the IBM Tivoli Configuration Manager: Reference Manual for Software Distribution.

Backward compatibility issues

This interim fix generates no compatibility issues.

Product compatibility

Compatibility is defined as whether different versions of a Tivoli product can communicate with different versions of Tivoli Management Framework.

IBM Tivoli Configuration Manager, Version 4.2.3 interim fix 4.2.3-TCM-0002 was tested using Tivoli Management Framework, Version 4.1.1 Fix Pack 3 or later. Tivoli Management Framework, Version 4.1.1 Fix Pack 3 contains the following interim fixes:

- 4.1.1-TMF-0046 interim fix for Tivoli management region servers, managed nodes, and gateways.
- 4.1.1-TMF-0039 interim fix for Mobile, JRIM, JCF, MDist 2 GUI, and Tivoli Desktop for Windows.
- 4.1.1-LCF-0020 interim fix for endpoints.

Limitations

Defect 56419

Using the Data Moving Service and retrieving large files, having a size between 300 MB and 1 GB, from an OS/400 system might fail. In this case the distribution status becomes INTERRUPTED. The problem is caused by the amount of time required to build the software package on the OS/400 system.

On the gateway, to which the OS/400 endpoint is connected, as a workaround for this problem you can set a higher value for the **execute_timeout** parameter as shown in the following example:

```
wmdist -s gateway_name execute_timeout=3600
```

Defect 56430

In an interconnected environment, the `from_depot` option does not work when the `plan_creation_mode` key is set to `per_tmr_region`. Leave the default value `per_enterprise`.

Defect 181204

AMD Opteron processor is not correctly discovered by Inventory on Windows 2003 workstations. This problem has been reported to Microsoft.

Defect 183012

On AIX platforms, if a network adapter is configured with two different IP addresses, the Inventory scan does not report the correct value for the subnet mask. The problem occurs because AIX does not provide a programmatic mechanism to retrieve these subnet masks. This limitation applies to all Inventory releases.

Defect 183229

When distributing an inventory scan using the **Update data** option, the **BOOT_TIME** and **ALIAS** values are not reported correctly from the Inventory scan.

Product fix history

IBM Tivoli Configuration Manager, Version 4.2.3, interim fix 4.2.3-TCM-0002 must be installed on top of IBM Tivoli Configuration Manager, Version 4.2.3 fix pack 1.

Fixes contained in this interim fix

Table 3 lists the fixes included in this interim fix:

Table 3. Fixes included in this interim fix

Interim fix	Component/Service
4.2.3-INV-0006	Inventory, Version 4.2.3
4.2.3-INVGW-0006	Inventory Gateway, Version 4.2.3
4.2.3-CLL-0002	Scalable Collection Services, Version 4.2.3
4.2.3-SWDSRV-F1P1	Software Distribution, Version 4.2.3
4.2.3-SWDGW-F1P1	Software Distribution Gateway, Version 4.2.3
4.2.3-SWDJPS-F1P1	Software Package Editor, Version 4.2.3
4.2.3-APM-F1P1	Activity Planner, Version 4.2.3
4.2.3-PMG-F1P1	Patch Management, Version 4.2.3

Inventory: The following APARs for Inventory were fixed:

Table 4. Inventory APARs included in this interim fix

Inventory and Inventory Gateway, Version 4.2.3, 4.2.3-INV-0006 and 4.2.3-INVGW-0006				
IY74730	IY76623	IY76692	IY76778	IY77367
IY77438	IY77522	IY77660	IY78414	IY78731
IY78778	IY78907	IY79519		

The following section describes each APAR or defect in detail:

APAR IY74730

Abstract:

Incorrect IP information when endpoint configured with two IP addresses

Error Description:

If an adapter is configured with two IP addresses, then Inventory scan reports in the IP Address Table two entries with the same value in the Address field.

APAR IY76623

Abstract:
TIVHSCAN.MIF file parsing error

Error Description:
The processor speed reported in the MIF file is reported with a negative value.

APAR IY76692

Abstract:
WTRANSFER with option -T ALL_GW fails in evaluating the target directory

Error Description:
When trying to copy a file to all gateways with the **wtransfer** command using the **-t all_gw** option, and using a variable for specifying the destination path, the file is copied into an incorrect path starting from the second gateway.

APAR IY76778

Abstract:
Obsolete information from WMI queries

Error Description:
In the tivhscan.mif file there are invalid entries in the IP Address Table with _A , and _B. It is a Microsoft known problem.

APAR IY77367

Abstract:
OS/400 **before scan** scripts are not executed

Error Description:
Any **before scan** script does not run on OS/400 endpoints.

APAR IY77438

Abstract:
Missing processor information for Linux endpoints

Error Description:
No physical CPU is detected when hyperthreading is enabled for Red Hat Enterprise Linux AS release 4 installed on VMware endpoints.

APAR IY77522

Abstract:
WSCANNER.EXE is unable to use the CITMDRV.SYS driver on T42 thinkpads

Error Description:
Using IBM Tivoli Configuration Manager 4.2.3 Fix Pack 1, the **wscanner** command fails on T42 thinkpads running Windows XP SP2. The command works fine with IBM Tivoli Configuration Manager 4.2.3 GA Version, or with IBM Tivoli Configuration Manager 4.2.3 Fix Pack 1 on other thinkpad models such as T41.

APAR IY77660

Abstract:
Before/After script cannot be executed.

Error Description:

If an inventory profile, enabled to run a **before/after** script, is distributed to a Windows endpoint configured to start every program from C: drive, the following error message is displayed:

```
INVCF0001E MDist returned the following error for scan ID 1585
on client DSG__DMPHCCM01_EP:
Command `beforesc.cmd' failed (argv[0] = `beforesc.cmd' status =
0 errno = 256).
```

APAR IY78414

Abstract:

TIVHSCAN.MIF parse error in Storage table

Error Description:

Hardware scan might fail on some Windows endpoints showing the following MIF parse error:

```
tivhscan. mif: line 816: syntax error Context: "-"
Found -1 in entry for Storage Table for Oxford, IDE device entry
Failing Entry is: 3,"54799cf527324776551a413e04bfc9de",30,
"Oxford Semiconductor OXFORD IDE Device LUN 0 IEEE 1394 SBP2 Device",
"Oxford","",-1,1,1,2097151}
```

The error is due to a negative value in the Storage table corresponding to the cylinders attribute.

APAR IY78731

Abstract:

inv_rcv_meths memory leak

Error Description:

When the traces are not enabled, the memory allocated by the inv_rcv_meths process during the data processing is not freed.

APAR IY78778

Abstract:

Table INST_SMBIOS_DATA contains multiple entries for one system

Error Description:

The Inventory table INST_SMBIOS_DATA contains multiple entries for one system.

APAR IY78907

Abstract:

Incorrect logical disk partition detection on Windows XP and Windows 2000

Error Description:

On Windows XP and Windows 2000 platforms, the **wscanner** command always uses the legacy algorithm to discover the logical disks.

APAR IY79519

Abstract:

WSCANNER hangs on AIX workstations

Error Description:

On some AIX workstations the **wscanner** command hangs while computing the IPAddressGroup table.

Scalable Collection Service: The following APARs for Scalable Collection Service were fixed:

Table 5. Scalable Collection Service APARs included in this interim fix

Scalable Collection Service, Version 4.2.3 4.2.3-CLL-0002				
IY77219	IY79215	IY79225		

The following section describes each APAR in detail.

APAR IY77219

Abstract:
`IOM_SEND` error for `MC_GET_DATA` with `SINGLE_PORT_BDT` enabled

Error Description:
If setting the `single_port_bdt` option and leaving the port number to the default value, which is 9401, the following communication error occurs in the `mcollect.log` file:

```
iom_send failed with code 67: communication failure.
```

APAR IY79215

Abstract:
Fifo order of ctocs in data handler input queue changes after restart

Error Description:
When running the data handler with 13 threads and having an output queue of about 80 threads, if you run the `wcstat -q o@InvDataHandler:inv_data_handler` command , you get the list of entries in the output queue. If you stop and restart the data handler, and rerun the `wcstat -q o @InvDataHandler:inv_data_handler` command, the entries that were at the end of the output queue are now at the start of the queue.

APAR IY79225

Abstract:
TCP connection remains in `CLOSE_WAIT` state

Error Description:
This problems seems to occur every time the communication with the endpoint fails.

Software Distribution: The following APARs for Software Distribution were fixed:

Table 6. Software Distribution APARs included in this interim fix

Software Distribution, Version 4.2.3, 4.2.3-SWDSRV-F1P1				
IY76698	IY77526	IY77936	IY78598	IY78973
Software Distribution Gateway, Version 4.2.3, 4.2.3-SWDGW-F1P1				
IY75263	IY76010	IY76694	IY77516	IY77601
IY77602	IY78195	IY78976		
Software Package Editor, Version 4.2.3, 4.2.3-SWDJPS-F1P1				
IY76008	IY77833			
Software Package Editor for Endpoints, Version 4.2.3, 4.2.3-SWDEP-F1P1				
IY76008	IY76488	IY77508	IY77833	IY78976

The following section describes each APAR or defect in detail.

APAR IY75263

Abstract:
Registry entry left in HKLM subkey after a `resinit.bat` execution

Error Description:
To perform a manual reboot on the endpoint, Software Distribution adds the keyword `HKLM/SOFTWARE/Tivoli/Swdis/SwdisRestart` value to the `resinit.bat` path. This keyword is readable and left after the reboot execution.

Additional Info:
After the fix, the key is encrypted.

APAR IY76008

Abstract:
Unable to save a second SPB using Speditor for AS/400

Error Description:
Using the Speditor for AS/400 to build a software package, you are able to save the first software package built. When saving the next software package built, the Speditor indicates that it is saved. However, when you open it, it shows the same content as the first saved software package.

Additional info:
The following error might be displayed when saving any software package built next:

```
DISSP6019E Failed to build
```

APAR IY76010

Abstract:
On AS/400 endpoints, *ALLOBJ special authority is required to build a package

Error Description:
To build a software package, *ALLOBJ special authority is required for a user profile.

Additional Info:
Ensure that the user home directory exists.

APAR IY76488

Abstract:
`TEMP.SP` and `TEMP.SPB` files not deleted after package built on AS/400

Error Description:
When you build a software package with Software Package Editor for AS/400, the file `temp.spb` is created under the directory `/tmp` on the AS/400. After the build the file `temp.spb` should be removed.

APAR IY76694

Abstract:
`SUCCESS_REBOOT_NOW_REEXECUTE` exit code does not allow to force the reboot

Error Description:

When you specify an exit code that relates to a `success_reboot_now_reexecute` value, you reboot the PC using only a soft reboot. An option is needed to specify a hard reboot.

APAR IY76698

Abstract:

On Solaris Tivoli server, `SWDMGR` does not honor `MAX_RPC_THREADS`

Error Description:

On the Solaris Tivoli server, when the environment is extremely busy, the following error might occur in the `oserv` log file:

```
Unknown failure sending method request
```

APAR IY77508

Abstract:

`SPE_GUI` variable defined in the Software Package Editor for Endpoints

Error Description:

When installing the Software Package Editor on the endpoint, the `SPE_GUI` variable has been introduced. This variable, by default set to yes, enables you to update the Software Package Editor GUI.

APAR IY77516

Abstract:

Software package installed with `-ty -cn` or `-ty -cy` remains in `IP-BC` status

Error Description:

When installing a software package using either the option `-ty -cn` or `-ty -cy`, the software package never reaches the status `IC---` and remains in `IP-BC`.

APAR IY77526

Abstract:

`REG_TL_PLUGIN.SH` is not downloaded when upgrading Configuration Manager from 4.2 to 4.2.x

Error Description:

The script `REG_TL_PLUGIN.SH` is not downloaded to the Tivoli server during an upgrade of IBM Tivoli Configuration Manager from 4.2 to 4.2.x.

APAR IY77601

Abstract:

Defer option not working for user notification

Error Description:

When distributing a software package to a Windows endpoint with the endpoint notification enabled, the mandatory date, the defer option allowed, and the Daylight Saving Time set on, the comparison between defer time and mandatory date is performed without considering the Daylight Saving Time.

APAR IY77602

Abstract:

No `AM/PM` indicator in the **Time to defer** field of the User Notification panel

Error Description:
The **Time to defer** field on the User Notification panel does not display the AM/PM option.

APAR IY77833

Abstract:
Check disk space allows only non-numeric entries

Error Description:
When entering the drive field of the check disk space properties panel, only an alphabetic character is accepted. A numeric value, if entered, is cancelled.

APAR IY77936

Abstract:
Temporary files are not deleted when MESSAGE_DIR_USABLE_QUOTA is reached

Error Description:
When the message_dir_usable_quota value is reached, new temporary files are created but the old ones are not deleted.

APAR IY78195

Abstract:
Software Distribution failure

Error Description:
When a software distribution contains nested packages, in case of checkpoint restart the distribution of some packages might fail on different endpoints.

APAR IY78598

Abstract:
Notification manager performance issue

Error Description:
The invocation of the Gateway remote method from the Notification manager shows a performance problem for load and unload operations.

APAR IY78973

Abstract:
A new parameter added to the **wswdcfg** command

Error Description:
The new parameter **return_code** has been added to the **wswdcfg** command to ensure that the return code is displayed in the command output.

Additional Info:
Set the new parameter **return_code** to **y** to activate this feature.

APAR IY78976

Abstract:
Disconnected CLI does not update the target log in case of locked files

Error Description:
When using the disconnected CLI to install software packages, the failure due to the locked file condition does not update the target log on the endpoint.

Additional Info:
The same problem occurs also when using the connected CLI.

Activity Planner: The following APARs for Activity Planner were fixed:

Table 7. Activity Planner APARs included in this interim fix

Activity Planner, Version 4.2.3, 4.2.3-APM-F1P1				
IY74892	IY77319	IY77688	IY77811	IY78143
IY78261	IY78280	IY78980	IY79210	

The following section describes each APAR in detail.

APAR IY74892

Abstract:
If the variable `TARGET_LIST` contains a curly braket, the APM engine loops

Error Description:
If the activity plan specifies the target by the `TARGET_LIST` variable and the first parenthesis is a curly braket, the APM_engine loops causing 100% of CPU usage.

APAR IY77319

Abstract:
Discrepancy between `WMDIST` and `WMONPLN` when deleting endpoints

Error Description:
When you delete endpoints during the running of a submitted plan with set deadline, the `wmonpln` and `wmdist` outputs contain different information. While the first reports a completion status for the activity, the second reports a waiting status for the deleted endpoints.

APAR IY77688

Abstract:
Problem selecting the targets at a Pristine Manager

Error Description:
When selecting the targets at a Pristine Manager installation activity, the Pristine target is listed twice.

APAR IY77811

Abstract:
Problem cancelling a plan with Pristine activities

Error Description:
When submitting a plan containing a Pristine Manager installation activity to two Pristine targets, and deleting the plan once the status is STARTED, the plan and activity status is SUCCESS.

APAR IY78143

Abstract:

Launching APM Editor GUI and APM Monitor GUI the file permissions for BINDIR/TME/APM/PLUGINS are incorrect

Error Description:

A non-root user is unable to launch the Activity Planner Editor GUI and the Activity Planner Monitor GUI. If a root user tries to log in, the BINDIR/TME/APM/plugins directory is created, but the permissions for that directory are incorrect.

APAR IY78261

Abstract:

Problem submitting APM plans to endpoints with the same label

Error Description:

A problem occurs when submitting Activity Planner plans to endpoints with the same label but belonging to different regions, if the retrieve_gateways_info option is set to No in the apm.ini file.

APAR IY78280

Abstract:

APMLOG1 is overwritten instead of being appended

Error Description:

The apmlog1 file is overwritten instead of being appended when Activity Planner is restarted and apmlog1 is the last current log file. If the last current log file is apmlog0, the problem does not occur.

APAR IY78980

Abstract:

MDist 2 GUI not starting from Activity Planner GUI on Windows XP platforms

Error Description:

The MDist 2 GUI does not start from the Activity Planner Monitor GUI using the Tivoli Desktop on Windows XP platforms.

APAR IY79210

Abstract:

Password containing special characters does not launch MDist 2 GUI from APM Monitor GUI

Error Description:

If the user password contains a special character, the MDist 2 GUI does not start from the Activity Planner Monitor GUI using the Tivoli Desktop on Windows platforms.

Patch Management: The Patch Management interim fix enables the emergency patch management and deployment paradigm features. For details see "Patch Management features" on page 21.

Installation

This section describes how to install the interim fix 4.2.3-TCM-0002 on top of IBM Tivoli Configuration Manager, Version 4.2.3 fix pack 1. The method of installation depends on the component you are upgrading. After you have installed the interim fix, you cannot uninstall it automatically. For this reason, before installing it, ensure you perform a complete backup of your system. After installing the interim fix installation, the `WSUSSCANCAB^1.0` software package is created and imported in the Tivoli desktop under the `Windows_Patch_Tools` policy region.

This section includes the following topics:

Hardware and software requirements

This section includes the following topics:

Supported platforms

Supported platforms at the time of the release are detailed in the *IBM Tivoli Configuration Manager: Release Notes*. For the most recent information, consult the supported platforms matrix on the IBM software support Web site: http://www.ibm.com/software/support.

1. From the Web site, select **Tivoli** from the **Other support sites** list.
2. When the page displays, select **IBM Tivoli Configuration Manager** from the **Choose a product** pull-down list.
3. Click the **Get The Latest Supported Platforms Matrix** link.
4. Enter your IBM registration ID and password.

System requirements

Hardware and software prerequisites are detailed in the *IBM Tivoli Configuration Manager: Release Notes*. There are currently no changes to the information included in the *Release Notes*.

Extracting the interim fix contents

Perform the following steps to extract the interim fix contents:

1. Extract the contents into a scratch directory. Assume that the symbol $PATCH points to this directory. Four tar files are provided:
   - `4.2.3-TCM-0002_docs.tar`
   - `4.2.3-TCM-0002_images.tar`
   - `4.2.3-TCM-0002_package.tar`
   - `4.2.3-TCM-0002_spb_installer.tar`
2. cd $PATCH

3. tar -xvf `4.2.3-TCM-0002_docs.tar`. Under the $PATCH directory, you find the following directory or path contents:

   /docs

   Readme files.

4. tar -xvf `4.2.3-TCM-0002_images.tar`. Under the $PATCH directory, you find the following directories or path contents:

   /xml

   To install interim fixes using the ISMP installation program, the `423CM002.xml` file contained in this directory must be copied locally and referred to at the installation time.

   /images

   Images required for this interim fix.

5. tar -xvf `4.2.3-TCM-0002_package.tar`. Under the $PATCH directory, you find the following directory or path contents:

   /package

   Software package block files used to patch GUI components and the `CM423_SPB_0002.xml` descriptor file.

6. tar -xvf `4.2.3-TCM-0002_spb_installer.tar`. Under the $PATCH directory, you find the following directory or path contents:

   /spb_installer

   SPB Patch Installer that installs SPB interim fixes locally.

Traditional interim fix installation methods

You can install the interim fix for IBM Tivoli Configuration Manager using any of the following different installation methods:

- "Installing interim fixes using ISMP"

  The InstallShield MultiPlatform (ISMP) program, which installs the appropriate IBM Tivoli Configuration Manager interim fix for the entire Tivoli management region (Tivoli region).

- "Installing interim fixes using the Tivoli desktop" on page 15

  A graphical user interface that you use to select the interim fix to install and the target workstations on which to install them.

- "Installing interim fixes using the CLI" on page 16

  Tivoli Management Framework command that you use to specify the interim fix to install and the target workstations on which to install them from the command line interface.

- "Installing interim fixes using SIS" on page 16

  The SIS console or SIS commands you use to specify the interim fix to install and on which target workstations to install them.

Installing interim fixes using ISMP

The InstallShield MultiPlatform (ISMP) program provides a wizard-guided process for installing interim fixes. It performs a check of the environment and installs the prerequisites, if any, to perform the upgrade process.

This installation can be used on all platforms supported as a Tivoli server, excluding Linux®® for S/390®.

Note: Before starting the upgrade process, back up the object database on the Tivoli server and each affected managed node.

For details about performing backup operations, see *Tivoli Management Framework Maintenance and Troubleshooting Guide*.

To upgrade your IBM Tivoli Configuration Manager environment with a interim fix, complete the following steps:

1. Locate the setup executable and run the following command in the root directory:
   - On Windows® platforms, `setup.exe –cmpatch`
   - On all other platforms, `setup_$(INTERP).bin –cmpatch`, where `$(INTERP)` represents the operating system on which you are launching the upgrade process.
2. Accept the Software License Agreement. Click **Next**.
3. Select the /xml directory. Click **Next**.
4. The actions necessary to upgrade your environment are being generated. When the process completes, a panel displays the interim fix components you must install. Click **Next**.
5. Select one of the following Depot options:

   Query when needed
   The InstallShield wizard prompts you for the location of product images. This option requires you to respond to a series of prompts during the installation process. This is the default setting.

   Verify local depot
   The InstallShield wizard prompts for the directory to which you have copied the installation images. The InstallShield wizard then searches all subdirectories of this directory to verify that all images are present. If an image is not found, you are prompted to provide its location. The installation process can then run unattended.

   Remote
   Select this option if images are deployed on a managed node before you start the installation.

   Click **Next**.
6. In the Step List, select the steps you want to run. Change the status of steps you do not want to run immediately to Held.
7. Click **Run All** to run all steps whose status is Ready or click **Run Next** to run steps individually.

For more information about installing using ISMP, see *IBM Tivoli Configuration Manager: Planning and Installation Guide*.

Installing interim fixes using the Tivoli desktop

When installing interim fixes using the Tivoli desktop, the images are located in the /images directory. The Tivoli desktop can upgrade the same product on multiple workstations sequentially.

The basic procedure for using the Tivoli desktop to upgrade a product is as follows:

1. From the Tivoli desktop, select **Install->Install Patch** from the Desktop menu.
2. Select the media and component to be upgraded.
3. Select the workstations where the component is to be upgraded.
4. Click **Install**.

For detailed information about using the Tivoli desktop to install or upgrade products, see *Tivoli Enterprise™: Installation Guide*.

Installing interim fixes using the CLI

When upgrading products using the **wpatch** command, specify the name of the index file using the file shown in Table 8. When using the **wpatch** command to upgrade a product, you specify the following information on the command line:

- The location of the image on the installation media.
- The name of the index file associated with the product to be installed or upgraded.
- The workstations where the image is to be installed.

Example:

```
wpatch -c /images -i index_file managed node
```

where:

-c /images
: Specifies the path to the /images directory.

-i *index_file*
: Specifies the product installation index file to which the interim fix is installed.

managed node
: Specifies the managed node on which the interim fix is installed.

If you do not specify a workstation when running the **wpatch** command, the image is installed on all managed nodes in the Tivoli region where there is a prior version of this image.

For detailed information about using the **wpatch** command, see *Tivoli Management Framework: Reference Manual*.

The following table contains a list of IND files included in this interim fix.

Table 8. IND files for components

IND file	Component name	Tag
423INV06	Inventory, Version 4.2.3	4.2.3-INV-0006
423LCF06	Inventory Gateway, Version 4.2.3	4.2.3-INVGW-0006
423CLL02	Scalable Collection Service, Version 4.2.3	4.2.3-CLL-0002
SWDF1P1	Software Distribution, Version 4.2.3	4.2.3-SWDSRV-F1P1
SDGWF1P1	Software Distribution Gateway, Version 4.2.3	4.2.3-SWDGW-F1P1
SDJPF1P1	Software Package Editor, Version 4.2.3	4.2.3-SWDJPS-F1P1
APMF1P1	Activity Planner, Version 4.2.3	4.2.3-APM-F1P1
PMGF1P1	Patch Management, Version 4.2.3	4.2.3-PMG-F1P1

Installing interim fixes using SIS

When installing interim fixes using Tivoli Software Installation Service, select the interim fixes to be installed using the component name shown in Table 8.

Tivoli Software Installation Service does not distinguish between products and interim fixes. Whether the installation image is used for an installation or upgrade, Tivoli Software Installation Service refers to all installation images as products.

Tivoli Software Installation Service can install multiple products on multiple workstations in parallel. This software can install several products on several computer systems in less time than using the installation methods provided by Tivoli Management Framework.

The basic procedure for using Tivoli Software Installation Service to install products is as follows:

1. Import the product images into the Tivoli Software Installation Service depot.
2. Select the components to be installed.
3. Select the workstations where each component is to be installed.
4. Click **Install**.

For detailed information about using Tivoli Software Installation Service, see *Tivoli Enterprise: Installation Guide*.

Software package block (SPB) interim fix installation for GUI components

To upgrade the GUI components of IBM Tivoli Configuration Manager using the SPB interim fixes on endpoints or standalone workstations, use one of the following installation methods:

- "SPB Patch Installer" on page 18
- "Software Distribution server command" on page 19
- "Software Distribution disconnected command" on page 19

IBM Tivoli Configuration Manager, Version 4.2.3 Fix Pack 1 is a prerequisite of the SPB interim fixes.

To successfully install interim fixes using any of these installation methods, ensure that the values of the default variables specified in the software package block correspond to the existing installation on the workstation to be upgraded. If they do not correspond, ensure they are stored in the swdis.var file. If these values were deleted from the swdis.var file, you must overwrite them at interim fix installation time using the appropriate panel of the SPB Patch Installer, or using the "-D" command line option (**wdinstsp** -D variable=value GUI_component.spb).

The default variables for each component defined in the SPB interim fixes are listed in Table 9.

Table 9. Default variables defined in SPB interim fixes

Variable	Value	Description
Tivoli_APM_GUI_Fix.v4.2.3.FP01.P1		
DSWIN_DIR	$(program_files)\Tivoli\Desktop	The directory where the Tivoli Desktop is installed.
TME_JAVATOOLS	$(program_files)\Tivoli\JavaTools	The directory where the JRE 1.3 is installed.
Tivoli_SWDEP_PC_Fix.v4.2.3.FP01.P1		
target_dir	$(product_dir)\speditor	The directory where the Software Package Editor is installed.

Table 9. Default variables defined in SPB interim fixes (continued)

Variable	Value	Description
TME_JAVATOOLS	$(program_files)\Tivoli\JavaTools	The directory where the JRE 1.3 is installed.
SPE_GUI	YES	Enables you to update the Speditor GUI.
Tivoli_SWDEP_UNIX_Fix.v4.2.3.FP01.P1		
target_dir	$(product_dir)/speditor	The directory where the Software Package Editor is installed.
TME_JAVATOOLS	/opt/Tivoli/JavaTools	The directory where the JRE 1.3 is installed.
SPE_GUI	YES	Enables you to update the Speditor GUI.
Tivoli_SWDEP_NTAS400_Fix.v4.2.3.FP01.P1		
target_dir	$(product_dir)\speditoras400	The directory where the Software Package Editor for AS/400® is installed.
TME_JAVATOOLS	$(program_files)\Tivoli\JavaTools	The directory where the JRE 1.3 is installed.
Tivoli_SWDEP_400PS_Fix.v4.2.3.FP01.P1 **Note:** This package has to be installed on the AS/400 system to which user wants to connect through Software Package Editor for AS/400.		
package_type	ALL	
target_dir	$(product_dir)\speditor	

SPB Patch Installer

This installation method uses ISMP technology that you can use to install interim fixes on an endpoint or standalone workstation to upgrade IBM Tivoli Configuration Manager, Version 4.2.3 GUI components. The SPB Patch Installer is supported on Microsoft® Windows, IBM AIX®, Solaris Operating Environment, Linux for Intel®, and HP-UX.

The following is a summary of the upgrade process using the SPB Patch Installer.

To install the SPB interim fixes using the SPB Patch Installer, perform the following steps:

1. Locate and run the setup program located in the /spb_installer directory.
   - On Windows, run the setup.exe file.
   - On all other platforms, run the setup_platform.bin.
2. Read the Welcome panel and click **Next**.
3. Specify the `CM423_SPB_0002.xml` file for the interim fix located in the /package directory. Click **Next**.
4. Select **Apply** and click **Next**.
5. Specify the components you want to install and click **Next**.
6. Clear the selection of the components for which you do not want to install in undoable mode. Click **Next**.
7. You might be prompted to specify the value of some variables defined in the SPB. Ensure that they are consistent with the existing installation on the workstation to be upgraded.
8. A Summary panel is displayed. Click **Next**.
9. The upgrade process starts.

Software Distribution server command

To use this type of installation, your Tivoli environment must contain an installation of the Software Distribution Server component, the Software Distribution Gateway component, and a Tivoli endpoint. The following steps must be performed to apply the SPB interim fix on the targets:

1. Create a new Profile in a Profile Manager, using the naming convention described in Table 10.
2. Import the SPB interim fix provided into the new Profile.
3. Select the endpoints to which you want to distribute the interim fix.
4. Submit the installation using either the command line or the Tivoli desktop.

If you need to overwrite the values of the default variables, use the ″-D″ option (winstsp -D variable=value GUI_component.spb) from the command line, or the Default Variables panel from the Tivoli desktop.

Software Distribution disconnected command

To use this type of installation, you must have the Software Distribution Software Package Editor component installed on the endpoint. If you need to overwrite the values of the default variables, use the ″-D″ option (wdinstsp -D variable=value GUI_component.spb) from the command line.

Software package block interim fixes

Table 10 contains the names of the interim fix 4.2.3-TCM-0002 software package blocks and the names of the software profiles that must be used when using SPBs to install components. IBM Tivoli Configuration Manager, Version 4.2.3 fix pack 1 SPBs are a prerequisite of the interim fix SPBs.

Table 10. Names of SPB files and software profiles

SPB Files	Package name with Version
Tivoli_APM_GUI_Fix.v4.2.3.FP01.P1.spb	Tivoli_APM_GUI_Fix.v4.2.3.FP01.P1
Tivoli_SWDEP_$(interp)_Fix.v4.2.3.FP01.P1.spb	Tivoli_SWDEP_$(interp)_Fix.v4.2.3.FP01.P1
Tivoli_SWDEP_NTAS400_Fix.v4.2.3.FP01.P1.spb	Tivoli_SWDEP_NTAS400_Fix.v4.2.3.FP01.P1
Tivoli_SWDEP_400PS_Fix.v4.2.3.FP01.P1.spb	Tivoli_SWDEP_400PS_Fix.v4.2.3.FP01.P1

Updating the Inventory schema

When you install this interim fix, you might need to update the Inventory schema.

This interim fix installation places files named inv_*db_vendor*_423_423INV06.sql on the managed nodes where the patch is installed, in the following directory:

```
$BINDIR/../generic/inv/SCRIPTS/RDBMS
```

where:

db_vendor
: Is the shortname for the database

Copy the appropriate schema scripts to any system where SQL access is available (such as the database server or the database client workstation if the client allows for SQL connectivity) to run the schema scripts.

Note: Error or information messages might be displayed when running the database scripts. Each database has unique behavior, so some messages can be expected.

Upgrading plug-ins

To upgrade plug-ins, you need to run the upgrade scripts.

Activity Planner

If you have installed 4.2.3-APM-F1P1, 4.2.3-SWDSRV-F1P1, and 4.2.3-INV-0006, run the following scripts located in the `$BINDIR/TME/APM/SCRIPTS` directory. You need the APM_Admin Tivoli region authorization role to run them in the following way:

- sh reg_swd_plugin.sh -r
- sh reg_inv_plugin_patch.sh
- sh reg_tl_plugin.sh -r

The first script enables the Activity Planner for Software Distribution, the second script enables the Activity Planner for Inventory, while the third script enables the Task Library.

Upgrading the Patch Management Automation Server driver

If you installed the Patch Management solution, Version 4.2.3 Fix Pack 1, you need to uninstall the previous Patch Management Automation Server driver and install the new driver provided with this interim fix. To install the new driver, perform the following steps:

1. Stop the Tivoli Configuration Manager Automation Server:
   a. Log on as user `tioadmin`.
   b. Open a Cygwin bash window and switch to the `$TIO_HOME/` tools directory.
   c. Run the **./tio_stop.cmd** command
   d. At the User name prompt, type wasadmin and press **Enter**.
   e. At the Password prompt, if you have not changed the password for WebSphere Application Server, type the default password wasadmin and press **Enter**.
   f. Check the `$TIO_HOME/logs/tio_stop.log` log file for errors.
2. Uninstall the previous Patch Management Automation Server driver:
   a. In the $TIO_HOME/tools directory, run the **./tc-driver-manager.cmd UninstallDriver tcm-ms-patches** command.
   b. Remove the `$TIO_HOME/drivers/lib/tcm-ms-patches.jar` file.
3. Install the new version of the Patch Management component:
   a. Switch to the `$BINDIR/TME/PATCH_MGMT/TPM_TCM_DRIVER` directory.
   b. Copy the tcm-ms-patches.tcdriver file, which represents the new version of the Patch Management Automation Server driver, to the `$TIO_HOME/drivers` directory.
   c. Switch to the `$TIO_HOME/tools` directory.
   d. Run the `./tc-driver-manager.cmd installDriver tcm-ms-patches` command.

   Note: You do not need to reinitialize the Patch Management environment.
4. Start the Tivoli Configuration Manager Automation Server:
   a. Switch to the `$TIO_HOME/tools` directory.
   b. Start the application by running the `./tio_start.cmd` command.
   c. At the User name prompt, type `wasadmin` and press **Enter**.
   d. At the Password prompt, if you have not changed the password for WebSphere Application Server, type the default password `wasadmin` and

press **Enter**. A window will display a message that Tivoli Configuration Manager Automation Server is ready to run.

Important: Do not close the window informing you that the application is running. If you close this window, the Tivoli Configuration Manager Automation Server does not start.

e. Check the `$TIO_HOME/logs/tpm_start.log` log file for any errors.

Patch Management features

This section describes the following Patch Management features:

- "Managing emergency patches"
- "Deployment Paradigms" on page 22

Managing emergency patches

If you are the Administrator responsible for approval and you determine that an update, released in an important Microsoft security bulletin, needs to be implemented immediately, you can use the emergency patch feature to defer the preventive inventory scan and install the update as soon as possible.

You can specify the list of patches you want to manage as emergency patches using the `emergency_patches` configuration key in the **wseccfg** command as follows:

`wseccfg -s emergency_patches=`*`patchInfo1`*`, `*`patchInfo2`*`,..., `*`patchInfoN`*

The *patchInfoN* values must be separated by a comma.

Before defining the *patchInfoN* values, you must identify the patch on WSUS and approve it. At this point you can collect the *updateID* and the platform on which to install the patch and then define the *patchInfoN* value as follows:

`updateID``.`*`os_base_name`*`[.`*`os_architecture`*`[.`*`os_type`*`[.`*`os_subtype`*`]]]`

where:

updateID
: Is the unique identifier for the patch (it is not the Qnumber) and is defined in WSUS.

os_base_name
: Identifies the name of the operating system (`winxp`, `win2k`, `win2k3`).

os_architecture
: Identifies the `x86` architecture.

os_type
: Identifies the type of the operating system: `srv`, `wks`.

os_subtype
: Identifies the subtype of the operating system: `dtc`, `ent`, `pro`, `bld`, `hom`, `ts`, `std`.

The *updateID* and *os_base_name* parameters are mandatory. They are used to determine the targets to which the patch has to be deployed. If other non-required parameters (such as `os_architecture`, `os_type`, `os_subtype`) are not specified, very complex APM plan might be created which addresses a high number of endpoints causing network overload problems.

For example, if you want to distribute a patch for Windows 2000 Professional and the *patchInfoN* key that you specify is *updateID*.win2k, the patch is sent to all Windows 2000 endpoints.

Instead, if the *patchInfoN* key that you specify is *updateID*.win2k.x86.wks, the patch is sent only to Windows 2000 Professional endpoints.

TCM_Emergency_Patches Workflow

You can manage emergency patches using the new TCM_Emergency_Patches.wkf workflow. Its execution depends on the emergency_patches variable settings. If the variable is not set, an error is reported.

Before running the TCM_Emergency_Patches.wkf workflow, ensure you run the Windows_Initial_Patch_Scan on the endpoints.

Software packages, queries, and APM plans for the emergency patches are created with the following naming convention and are considered separately from the standard patches:

Emergency software packages	**hot_patch.***qnumber*.*guid*.*os_base_name*.[*os_architecture*].[*os_type*].[*os_subtype*].[b]^1.0**
Emergency queries	hot_query.*qnumber*.*guid*.*os_base_name*.[*os_architecture*].[*os_type*].[*os_subtype*].[b]
Emergency plan	hot_patch.*plan_name*

The workflow performs the following steps:

1. Downloads emergency patches and ApprovedChanges.txt from WSUS.
2. Downloads the Microsoft Security Policy Catalog from the Microsoft Web site.
3. Uploads the catalogs to the Tivoli servers and Tivoli gateways.
4. Invokes the **wsecgensp** command to create all software packages and queries related to the specified emergency patches.

   Note: To delete software packages, queries, and the APM plan related to previous emergency patches, set the emergency_delete_packages_plan configuration key to yes.
5. If the email_notification_address key was configured using the **wseccfg** command, sends an e-mail when the workflow has completed to the Administrator.
6. Invokes the **wsecgenplan** command to generate APM plans with activities that install emergency patches. These activities are conditioned by the installation of the WSUSSCANCAB^1.0 software package, used to:
   - Refresh the wsusscan.cab catalog on the endpoints. The wsusscan.cab catalog is taken from the $DBDIR/inventory directory of the Tivoli server specified in the TMR_server_list key of the **wseccfg** command.
   - Deploy the check_patch.cmd file on the endpoints. This batch file runs the lcf_before_program script and execute_user_program script to determine if a patch has to be installed on an endpoint.

Deployment Paradigms

The capability of retrieving software packages to be installed from a depot or a file server can be extended from Software Distribution to Patch Management by using the deployment_paradigm key in the **wseccfg** command as follows:

```
wseccfg -s deployment_paradigm=[standard | from_depot | from_fileserver]
```

where:

standard
Specifies that the software package to be installed resides on the source host. This is the default value.

from_depot
Specifies that the software package to be installed resides on the repeater depot, rather than on the source host. With the `from_depot` key you can also specify the following keys in the **wseccfg** command:

-s sp_patches_depots=*depot1, depot2,...*
Use this key to specify in *depot1, depot2,...* the name of the gateways or stand-alone repeaters where to load the packages. These names must be separated by a comma.

-s sp_patches_depots_file=*depotfile*
Use this key to specify in the *depotfile* file the list of gateways or stand-alone repeaters where to load the packages.

-s depots_unload=[yes(default) | no]
Use this key to specify if the unload operation must be performed or not.

from_fileserver
Specifies that the images referenced in the software package are to be retrieved from a file server. After the software package, query, and plan creation through the workflow and before the plan submission, perform the following configuration steps:

1. Create an installable image of the software package block using the following command:

   ```
   wldsp -l depot_image_dir=provider_spb_dir  @SoftwarePackage:spobj_name
   [@subscribers ...]
   ```

   Where:

   provider_spb_dir
   Is the directory on the source host where the .spb files are copied after the software package for a given patch has been created. This value is specified in the **wseccfg** command.

   @subscribers
   Specifies the source hosts defined using the **wseccfg** command.

   Refer to the *Reference Manual for Software Distribution* for the syntax and usage of the **wldsp** command.

   These commands create two files with the extensions `.itc/.toc` and `.dat`. These two files contain the data to be used during the distribution operation.
2. Load or copy the `.itc/.toc` and `.dat` files to the file server in a directory shared by all endpoints.
3. Create and configure the `remote.dir` file on the endpoints to access the file server.
4. Copy the `remote.dir` file under `$LCF_DATDIR` on each endpoint. This file contains a list of available file servers, one per line. You can use Software Distribution to distribute the `remote.dir` file to the endpoints in a software package. When the endpoint lcfd receives the distribution, it looks for the content of the distribution in the specified shared

directory of the first file server listed in the `remote.dir` file. If it does not find the file, it looks for it on the next file server listed in the `remote.dir` file.

5. Mount the shared directory of the file server on each endpoint using, for example, the **wlcftap** command.

Automated patch management command line

To address the emergency patch and the patch deployment paradigm features the **wseccfg**, **wsecgensp**, and **wsecgenplan** commands have been modified. Changes are marked using revision bars.

wseccfg

Modifies or retrieves patch management settings for the managed node.

Syntax: **wseccfg -s [***key* **[=***value***]]**

wseccfg -d *key*

wseccfg [-x *separator***] {-a** *key value* **| -c** *key value***}**

Description: You can use the **wseccfg** command to configure, retrieve, and change the patch management settings for the managed node. Some of the keys listed below are not displayed by default, but are available for configuration.

Options:

-s *key*=*value*

Sets a custom key and its value, or allows you to define existing variables and their values. Specifying the **wseccfg -s** command without the *key* argument, displays all keys with the corresponding settings currently used. Specifying the **wseccfg -s** *key* command without a value, displays the value set for the specified key. Specifying the *key* argument with a value, sets the key to the specified value.

product_dir

Identifies the directory where Patch Management data, such as logs and traces, is stored. The default directory is *$(BINDIR)*`/../patch_mgmt`.

trace_size

Specifies the size of the trace file. The default value is 1 000 000 bytes. When the maximum size is exceeded, a new trace file is created.

trace_level

Specifies the trace level. Supported values are as follows:

0 none

1 fatal

2 error

3 warning

4 information

5 verbose

The default value is **0**.

source_host_list

Identifies a list of source hosts, separated by commas, used by Automation Server to send patch files. Specify only one source per region. At installation time, this option is completed with the name of the Tivoli server. This option is used only by the Automation Server.

TMR_server_list

Identifies a list of Tivoli servers, separated by commas, that Automation Server will use to send the **wsusscan.cab** and

ApprovedChanges.txt files. At installation time, this option is completed with the name of the Tivoli server. This option is used only by Automation Server.

delete_packages
Specifies whether software packages objects containing patches with revoked approval must be removed from Tivoli Framework. Supported values are **yes** and **no**. The default value is **no**.

delete_plans
Specifies whether existing activity plans are to be deleted before a new plan is created. Supported values are **yes** and **no**. The default value is **no**.

plan_creation_mode
Specifies whether only one plan or whether a plan for each Tivoli region in the Enterprise should be created. Specify **per_enterprise** to create one plan, or specify **per_tmr_region** to create a plan for each Tivoli region in the Enterprise. The default value is **per_enterprise**. This option applies to the creation of plans in the workflow.

plan_grouping_mode
Specifies how the activity plan must be created. Specify **by_patch_id** to create one plan per patch ID, or specify **none** to create one plan for all the available patch IDs. The default value is **none**. This option applies to the creation of plans in the workflow.

tme_object_scope_for_plan
Specifies whether resources such as software packages or Inventory scans used in activity plans must be located on the hub or spoke region. Specify **hub** to indicate that activities in the plan must refer to resources located on the hub region, specify **spoke** to indicate that activities in the plan must refer to resources located on the spoke regions for which the plan was created. If you specify **spoke**, a source host located in the spoke region must be specified with the **source_host_list** key. The default value is **hub**. This option applies to interconnected regions.

email_notification_address
Specifies the e-mail address used to send notifications about the workflow completion. This option is used only by Automation Server.

remove_patch_files_if_built
Specifies whether the patch executable files must be removed from the *$BINDIR*/../patch_repos directory after creating the software package. Specify **yes** to remove the patch files, or specify **no** not to remove the patch files. The default value is **yes**. For more information on the **wsecgensp** command, see "wsecgensp" on page 33.

reboot_template_file
Specifies a relative path to the .spd template used to create the software package for patches requiring a reboot. The relative path must already exist. It is appended to the *$(BINDIR)*/TME/PATCH_MGMT/TEMPLATES default path as follows: *$(BINDIR)*/TME/PATCH_MGMT/TEMPLATES/*reboot_template_file*. If you do not specify this key, the following default template is used:

$(BINDIR)/TME/PATCH_MGMT/TEMPLATES/reboot_template.spd

standard_template_file
Specifies a relative path to the .spd template used to create the software package for standard patches. The relative path must already exist. It is appended to the *$(BINDIR)*/TME/PATCH_MGMT/TEMPLATES default path as follows: *$(BINDIR)*/TME/PATCH_MGMT/TEMPLATES/*standard_template_file*. If you do not specify this key, the following default template is used:

$(BINDIR)/TME/PATCH_MGMT/TEMPLATES/standard_template.spd

exclusive_template_file
Specifies a relative patch to the .spd template used to create the software package for exclusive patches. The relative path must already exist. It is appended to the *$(BINDIR)*/TME/PATCH_MGMT/TEMPLATES default path as follows: *$(BINDIR)*/TME/PATCH_MGMT/TEMPLATES/*exclusive_template_file*. If you do not specify this key, the following default template is used:

$(BINDIR)/TME/PATCH_MGMT/TEMPLATES/exclusive_template.spd

emergency_reboot_template_file
Specifies a relative path to the .spd template used to create the software package for emergency patches requiring a reboot. The relative path must already exist. It is appended to the *$(BINDIR)*/TME/PATCH_MGMT/TEMPLATES default path as follows:

$(BINDIR)/TME/PATCH_MGMT/TEMPLATES/
emergency_reboot_template_file

If you do not specify this key, the following default template is used:

$(BINDIR)/TME/PATCH_MGMT/TEMPLATES/emergency_reboot_template.spd

emergency_template_file
Specifies a relative path to the .spd template used to create the software package for emergency standard patches. The relative path must already exist. It is appended to the *$(BINDIR)*/TME/PATCH_MGMT/TEMPLATES default path as follows: *$(BINDIR)*/TME/PATCH_MGMT/TEMPLATES/*emergency_template_file*. If you do not specify this key, the following default template is used:

$(BINDIR)/TME/PATCH_MGMT/TEMPLATES/emergency_template.spd

emergency_exclusive_template_file
Specifies a relative patch to the .spd template used to create the software package for exclusive emergency patches. The relative path must already exist. It is appended to the *$(BINDIR)*/TME/PATCH_MGMT/TEMPLATES default path as follows:

$(BINDIR)/TME/PATCH_MGMT/TEMPLATES/
emergency_exclusive_template_file

If you do not specify this key, the following default template is used:

$(BINDIR)/TME/PATCH_MGMT/TEMPLATES/emergency_exclusive_template.spd

provider_spb_dir
Specifies the directory on the source host where the .spb files are copied after the software package for the given patch has been created. If no value is specified, the .spb files are created in the *$(BINDIR)*/../patch_mgmt directory.

provider_patch_dir
Specifies the directory on the source host containing the patch executables used to build the software package. If this option is not specified, the *$BINDIR*/../patch_mgmt directory is assumed.

provider_patch_host
Specifies the source host used to build the software package. If this option is not specified, the local workstation is assumed.

custom_plan_template
Specifies a relative path to the template file used to customize the activity plan. The relative path must already exist. It is appended to the *$(BINDIR)*/TME/PATCH_MGMT/TEMPLATES default path as follows:
$(BINDIR)/TME/PATCH_MGMT/TEMPLATES/*custom_plan_template*. If you do not specify this key, the following default template is used:
$(BINDIR)/TME/PATCH_MGMT/TEMPLATES/APM_PLAN_Template.xml

std_activity_template
Specifies a relative path to the template file used to customize an activity that installs a standard patch. The relative path must already exist. It is appended to the *$(BINDIR)*/TME/PATCH_MGMT/TEMPLATES/ default path as follows:
$(BINDIR)/TME/PATCH_MGMT/TEMPLATES/*std_activity_template*. If you do not specify this key, the following default template is used:
$(BINDIR)/TME/PATCH_MGMT/TEMPLATES/APM_STD_Activity_Template.xml

reboot_activity_template
Specifies a relative path to a template file used to customize an activity that performs a reboot. The relative path must already exist. It is appended to the *$(BINDIR)*/TME/PATCH_MGMT/TEMPLATES/ default path as follows:
$(BINDIR)/TME/PATCH_MGMT/TEMPLATES/*reboot_activity_template*. If you do not specify this key, the following default template is used:
$(BINDIR)/TME/PATCH_MGMT/TEMPLATES/APM_REBOOT_Activity_Template.xml

excl_activity_template
Specifies a relative path to a template file used to customize an activity that installs an exclusive patch. The relative path must already exist. It is appended to the default path as follows:*$(BINDIR)*/TME/PATCH_MGMT/TEMPLATES/*excl_activity_template*. If you do not specify this key, the following default template is used:
$(BINDIR)/TME/PATCH_MGMT/TEMPLATES/APM_EXCL_Activity_Template.xml

last_activity_template
Specifies a relative path to a template file used to customize the last activity of the plan. The relative path must already exist. It is appended to the default path as follows:
$(BINDIR)/TME/PATCH_MGMT/TEMPLATES/*last_activity_template*. If you do not specify this key, the following default template is used:
$(BINDIR)/TME/PATCH_MGMT/TEMPLATES/APM_LAST_Activity_Template.xml

If you modify the name of the last activity in this template, you must use the same name in the APM_PLAN_TEMPLATE.xml or in the template you specify with the **std_activity_template** key.

max_apm_bootable_threshold
Specifies how many activities requiring a reboot are to be grouped

together. For each group of activities requiring a reboot, a specific reboot activity is generated and conditioned to all the above activities. The default value is **10**.

wsus_inst_path
Specifies the WSUS Update Source directory. This key is mandatory. For details, see *Deploying Microsoft Windows Server Update Services*.

wsus_db_name
Specifies the name of the database used by WSUS to store data. The key is not mandatory and its default value is the `SUSDB`.

wsus_db_host
Specifies the hostname of the SQL Server used by WSUS to store data. You can retrieve this name from the SQL Server Service Manager (sqlmangr.exe) on the WSUS server. This key is mandatory.

cab_gateways_list
Specifies the list of gateways to which the wsusscan.cab and ApprovedChanges.txt files have to be uploaded if changed since the last download from the Microsoft site. The keyword all_gw can be used to indicate all the gateways in the network. If you do not specify this key, the wsusscan.cab and ApprovedChanges.txt files are not copied.

cab_gateways_file
Specifies the name of the file that contains the list of the gateways to which the file has to be uploaded (see cab_gateways_list option).

prepare_patches_requiring_connectivity
Some Microsoft patches require connectivity to Internet to be installed. Specifies if these patches are to be prepared. You can set the key to `yes` or `no`. The parameter is optional and its default value is `no`.

prepare_patches_requiring_user_input
Some Microsoft patches require user input (for example acceptance of EULA license) when installed. These patches are prepared only if the value of the prepare_patches_requiring_user_input is set to `yes`. You can set the key to `yes` or `no`. This key is optional and the default value is `no`.

catalog_proxy_enabled
Enables or disables proxy support to download the wsusscan.cab file. You can use an HTTP proxy to access the Microsoft Web site, or your local HTTP server where the wsusscan.cab file has been downloaded. Proxy parameters are defined at installation time in the tpm_update.req file, as described in "Upgrading the Patch Management Automation Server driver" on page 20. This key is optional and the default value is `no`.

workflow_activities
Specifies whether workflows are completed in one step or are separated into two steps. Supported values are as follows:

sync Performs the following operations:

1. Synchronizes WSUS approved patches with the Automation Server database.

2. Downloads wsuscan.cab from the Microsoft Web site.
3. Creates ApprovedChanges.txt.
4. Copies wsuscan.cab and ApprovedChanges.txt on the workstations defined in the TMR_server_list, cab_gateways_list, and cab_gateways_file.

preparation
Creates software packages, queries, and APM plans.

all Performs all sync and preparation operations. This is the default value.

This key is optional and the default value is `all`.

emergency_patches

Specify this key to identify the list of patches to be installed immediately. Supported values have the following format: *patchInfo1*, *patchInfo2*,..., *patchInfoN* separated by a comma.

Before defining the *patchInfoN* values, you must identify the patch on WSUS and approve it. At this point you can collect the *updateID* and the platform on which to install the patch and then define the *patchInfoN* value as follows:

updateID.*os_base_name*[.*os_architecture*[.*os_type*[.*os_subtype*]]]

where:

updateID
Is the unique identifier for the patch (it is not the Qnumber) and is defined in WSUS.

os_base_name
Identifies the name of the operating system (`winxp`, `win2k`, `win2k3`).

os_architecture
Identifies the `x86` architecture.

os_type
Identifies the type of the operating system: `srv`, `wks`.

os_subtype
Identifies the subtype of the operating system: `dtc`, `ent`, `pro`, `bld`, `hom`, `ts`, `std`.

The *updateID* and *os_base_name* parameters are mandatory. They are used to determine the targets to which the patch has to be deployed. If you specify a non-required parameter, you must specify all the previous parameters in the *patchInfoN* key.This key is optional.

deployment_paradigm
Specifies the way to retrieve software packages. Supported values are as follows:

standard
Specifies that the software package to be installed resides on the source host. This is the default value.

from_depot
Specifies that the software package to be installed resides

on the repeater depot, rather than on the source host. With the `from_depot` key you can also specify the following keys in the **wseccfg** command:

-s sp_patches_depots=*depot1, depot2,...*
Use this key to specify in *depot1, depot2,...* the name of the gateways or stand-alone repeaters where to load the packages. These names must be separated by a comma.

-s sp_patches_depots_file=*depotfile*
Use this key to specify in the *depotfile* file the list of gateways or stand-alone repeaters where to load the packages.

-s depots_unload=[yes(default) | no]
Use this key to specify if the unload operation must be performed or not.

from_fileserver
Specifies that the images referenced in the software package are to be retrieved from a file server. File servers must be configured if this value is used. For more details, see "Deployment Paradigms" on page 22.

This key is optional.

-d *key* Deletes the specified key.

-a *key value*
Appends the specified value to the given key. If the **-x** option is not specified, the comma is used as separator.

-c *key value*
Removes the specified value from the given key. If the **-x** option is not specified, the comma is used as separator. The specified value is removed only if you specify the correct separator. Before running this command, run **wseccfg -s** to find out the exact separator used for the key.

-x *separator*
Specifies the separator symbol used to process the arguments in the string when the option **-a** or **-c** is specified. If this option is not specified, the default separator is a comma (,).

Note: If you are using a semicolon as separator on UNIX® systems, include the semicolon between single inverted quotes.

Authorization:

user For viewing configuration information

senior For modifying configuration information

Return Values: The **wseccfg** command returns one of the following:

0 Indicates that **wseccfg** completed successfully.

other than 0
Indicates that **wseccfg** failed due to an error.

Examples:

1. To set the trace level, enter the following command:

```
wseccfg -s trace_level=5
```

2. To set the trace size, enter the following command:

   ```
   wseccfg -s trace_size=1000000
   ```

3. To set the directory on the source host where the software package blocks are stored, enter the following command:

   ```
   wseccfg -s provider_spb_dir=/Tivoli/bin/patch_mgmt/spb
   ```

4. To set the directory on the source host containing the patch executables used to build the software package blocks, enter the following command:

   ```
   wseccfg -s provider_patch_dir=/Tivoli/Patches
   ```

5. To set the source host where the software package blocks are built, enter the following command:

   ```
   wseccfg -s provider_patch_host=lab133109
   ```

6. To specify the source host list used by Automation Server to send patch files, enter the following command:

   ```
   wseccfg -s provider_patch_host=lab133109,lab13486,lab13879
   ```

7. To specify the Tivoli server list for Automation Server to use to send the `wsusscan.cab` and `ApprovedChanges.txt` files, enter the following command:

   ```
   wseccfg -s TMR_server_list=linux111,lab13875,lab13542
   ```

8. To add a key and its value to the Patch Management configuration, enter the following command:

   ```
   wseccfg -x , -a test 80
   ```

9. To verify that the specified key was correctly added, enter the following command:

   ```
   wseccfg -s
   ```

10. To remove the specified value, enter the following command:

    ```
    wseccfg -x , -c test 80
    ```

    This command removes the value, while the `test` key is still present. To remove the `test` key, enter the following command:

    ```
    wseccfg -d test
    ```

11. To remove values from the `colors` key, enter the following commands:

    a. To discover the separators used in the `colors` key, enter the following command:

       ```
       wseccfg –s
       ```

       The following is an abstract of the output returned by the command:

       ```
       colors=green,red;blue;black,white,purple
       ```

    b. To remove the `white` value from the `colors` key, enter the following command:

       ```
       wseccfg -x , -c colors white
       ```

    c. To remove the `red;blue;black` values from the `colors` key, enter the following command:

       ```
       wseccfg -x , -c colors red;blue;black
       ```

See Also: “wsecgensp” on page 33, “wsecgenplan” on page 35.

wsecgensp

The **wsecgensp** command generates the software packages required for installing the specified patch or patches on target workstations and creates the queries for determining the target workstations on which the patches need to be installed.

Syntax: **wsecgensp -p** *patch_id* **-g** *GUID* **[-t** *patchInfo1*, ...,*patchInfoN*] **[-q { 0 | 1 }] [{ -b | -x }] -f** *patch_file* **-a** *args* **[-h** *source_host* **-d** *patch_dir*] **[-v] [-o]**

Description: The **wsecgensp** command generates the software package and the associated query for the specified patch ID. Packages are prepared using templates stored in the *$BINDIR*/TME/PATCH_MGMT/TEMPLATES directory. To modify the default template, use the **reboot_template_file**, **standard_template_file**, **exclusive_template_file**, **emergency_template_file**, **emergency_reboot_template_file**, and **emergency_exclusive_template_file** options with the **wseccfg** command.

Options:

-p *patch_id*
Specifies the Q number of the patch.

-g *GUID*
Specifies the globally unique identifier.

-t *patchInfo1*, ..., *patchInfoN*

Specifies the information for the patch to be installed immediately. Each *patchInfoN* value must be separated by a comma.

The *patchInfoN* syntax is the following:

updateID.*os_base_name*[.*os_architecture*[.*os_type*[.*os_subtype*]]]

where:

updateID
Is the unique identifier for the patch (it is not the Qnumber) and is defined in WSUS.

os_base_name
Identifies the name of the operating system (winxp, win2k, win2k3).

os_architecture
Identifies the x86 architecture.

os_type
Identifies the type of the operating system: srv, wks.

os_subtype
Identifies the subtype of the operating system: dtc, ent, pro, bld, hom, ts, std.

The *updateID* and *os_base_name* parameters are mandatory. They are used to determine the targets to which the patch has to be deployed. If other non-required parameters (such as os_architecture, os_type, os_subtype) are not specified, very complex APM plan might be created which addresses a high number of endpoints causing network overload problems..

-q 0 | 1
Specifies whether the query should be created. Specify **1** to create the query, specify **0** to skip the creation of the query. The default value is **1**.

-b Indicates that the patch requires a reboot. Uses the reboot_template_file template.

-x Indicates that the patch is exclusive. Uses the exclusive_template_file template.

-f *patch_file*
Specifies the full path to the file that installs the patch.

-a *args* Specifies the arguments for the patch installation. The arguments vary depending on the patch to be installed. For more information on supported arguments for a patch, search the patch ID on the Microsoft WSUS server.

-h *source_host*
Specifies the source host node where the patch files are stored. If this option is not specified, the value defined in the **provider_patch_host** option in the **wseccfg** command is assumed. For more information on this command, see "wseccfg" on page 25.

-d *directory*
Specifies the directory on the source host where the patch executable files are stored. If this option is not specified, the value defined in the **provider_patch_dir** option in the **wseccfg** command is assumed. For more information on this command, see "wseccfg" on page 25.

-v Displays in preview the software package name without generating the software package. The software package name contains information about the type of patch to be installed and must not be modified.

-o Overwrites any existing packages with the same name, if present.

Authorization: senior.

Return Values: The **wsecgensp** command returns one of the following:

0 Indicates that **wsecgensp** completed successfully.

other than 0
Indicates that **wsecgensp** failed due to an error.

Examples: To create a software package for the patch 873339 to be applied on English Windows 2000 workstations with the specified installation arguments, enter the following command:

```
wsecgensp -p 873339 -g 47159B36-A90E-4253-B1F7-1629DA5D0328 -b
-f 500E4656B4F0CA34315656319890 90BBEEB74BCC.exe -a "-q /Z -ER"
```

The patch.873339.47159B36-A90E-4253-B1F7-1629DA5D0328.b software package is created.

See Also: "wseccfg" on page 25.

wsecgenplan

The **wsecgenplan** command creates the activity plan to be submitted for installing one or more patches.

Syntax: wsecgenplan {-p *software_package_list* **| -P** *packages_file***} {-e emergency_software_package_list | -E emergency_software_packages_file} [-f** *subscriber_file***] [-t] [-n** *name***] [-d deployment_paradigm [-D depot_file [-u]]]**

Description: The activity plans are generated based on templates stored in the *$BINDIR*/TME/PATCH_MGMT/TEMPLATES directory. To specify a different template, use the **custom_plan_template**, **std_activity_template**, **reboot_activity_template**, **excl_activity_template**, **last_activity_template**, **emergency_template_file**, **emergency_reboot_template_file**, and **emergency_exclusive_template_file**options with the **wseccfg** command. For more information on this command, see "wseccfg" on page 25.

Options:

-p *software_package_list*
Specifies a list of patch IDs, separated by commas, that the activity plan to be created must install.

-P *packages_file*
Specifies a file containing the list of patches that the activity plan to be created must install. Specify one package per line. Blank or empty lines are skipped. Lines starting with # are considered as comments and are ignored.

-e *emergency_software_package_list*
Specifies a list of emergency patches, separated by commas, that the activity plan to be created must install.

-E *emergency_software_package_file*
Specifies a file containing the list of emergency patches that the activity plan to be created must install. Specify one package per line. Blank or empty lines are skipped. Lines starting with # are considered as comments and are ignored.

-f *subscriber_file*
Specifies the fully-qualified path to the file containing the target list for each activity in the plan. In the file, specify one subscriber per line. If this option is not specified, the query associated to the patch package is used to evaluate the targets for each activity in the plan.

-t Specifies whether a single plan must be created for each Tivoli region. The targets of each plan are filtered by the region number. Therefore, each plan addresses only endpoints belonging to the same region. If this option is not specified, only one plan is generated to address all the endpoints in the enterprise.

-n *name*
Specifies the name to be assigned to the plan to be created. If this option is not specified, a default name is automatically generated. The default naming convention is as follows: patch.*mm-dd-yy_hh_mm_ss_patchID#regionID*, where

mm-dd-yy
The date the plan was created.

hh_mm_ss
The time the plan was created.

patchID
The ID of the patch contained in the plan. This item might not be present depending on the plan configuration.

regionID
The ID of the region for which the plan is created. This item might not be present depending on the plan configuration.

-d deployment_paradigm
Specifies the way to retrieve software packages. If you do not specify this key, the software package is retrieved from the source host. Supported values are as follows:

standard
Specifies that the software package to be installed resides on the source host. This is the default value.

from_depot
Specifies that the software package to be installed resides on the repeater depot, rather than on the source host.

from_fileserver
Specifies that the images referenced in the software package are to be retrieved from a file server.

This key is optional.

-D *depot_file*
Specifies the file containing the list of gateways or stand-alone repeaters where to load the packages. This option is valid only with the `-d from_depot` parameter.

-u Specify if the unload operation must be performed or not. This option is valid only with the `-D` *depot_file* parameter. The following APM templates manage the activities of `WSUSSCANCAB^1.0` installation and of the load and unload of depots: `APM_CAB_Activity_Template.xml` and `APM_DEPOT_Activity_Template.xml`.

Authorization: user, APM_Edit.

Return Values: The **wsecgenplan** command returns one of the following:

0 Indicates that **wsecgenplan** completed successfully.

other than 0
Indicates that **wsecgenplan** failed due to an error.

Examples:

1. To generate an activity plan for packages

```
patch.842526.DF8B7CBC-80DB-427D-BACD-42F7F8DD2C0A.b^1.0,
patch.888113.3754C547-772F-4C0F-9A17-1A7754CB4A6C.b^1.0,
patch.891781.3128B719-219E-4273-A706-F417D8872C39.b^1.0
```

   using the tgt_list.txt file to specify subscribers, enter the following command:

```
wsecgenplan -p patch.842526.DF8B7CBC-80DB-427D-BACD-42F7F8DD2C0A.b^1.0,
patch.888113.3754C547-772F-4C0F-9A17-1A7754CB4A6C.b^1.0,
patch.891781.3128B719-219E-4273-A706-F417D8872C39.b^1.0
-f /Tivoli/act_plans/tgt_list.txt
```

2. Creates a plan by including all the software packages specified in the package.txt file.

```
wsecgenplan -P packages.txt
```

3. Creates a plan for each Tivoli region with source hosts specified with the **source_host_list** key in the **wseccfg** command that includes the specified package.

   ```
   wsecgenplan -p patch.891781.3128B719-219E-4273-A706-F417D8872C39.b^1.0 -t
   ```

See Also: "wseccfg" on page 25.

Chapter 2. Support information

This section describes the following options for obtaining support for IBM products:

- "Searching knowledge bases"
- "Obtaining fixes"
- "Contacting IBM Software Support" on page 40

Searching knowledge bases

If you have a problem with your IBM software, you want it resolved quickly. Begin by searching the available knowledge bases to determine whether the resolution to your problem is already documented.

Search the information center on your local system or network

IBM provides extensive documentation that can be installed on your local computer or on an intranet server. You can use the search function of this information center to query conceptual information, instructions for completing tasks, reference information, and support documents.

Search the Internet

If you cannot find an answer to your question in the information center, search the Internet for the latest, most complete information that might help you resolve your problem. To search multiple Internet resources for your product, expand the product folder in the navigation frame to the left and select **Web search**. From this topic, you can search a variety of resources including:

- IBM technotes
- IBM downloads
- IBM Redbooks™
- IBM developerWorks®
- Forums and newsgroups
- Google

Obtaining fixes

A product fix might be available to resolve your problem. You can determine what fixes are available for your IBM software product by checking the product support Web site:

1. Go to the IBM Software Support Web site (http://www.ibm.com/software/support).
2. Under **Products A - Z**, select your product name. This opens a product-specific support site.
3. Under **Self help**, follow the link to **All Updates**, where you will find a list of fixes, fix packs, and other service updates for your product. For tips on refining your search, click **Search tips**.
4. Click the name of a fix to read the description and optionally download the fix.

To receive weekly e-mail notifications about fixes and other news about IBM products, follow these steps:

1. From the support page for any IBM product, click **My support** in the upper-right corner of the page.
2. If you have already registered, skip to the next step. If you have not registered, click register in the upper-right corner of the support page to establish your user ID and password.
3. Sign in to **My support**.
4. On the My support page, click **Edit profiles** in the left navigation pane, and scroll to **Select Mail Preferences**. Select a product family and check the appropriate boxes for the type of information you want.
5. Click **Submit**.
6. For e-mail notification for other products, repeat Steps 4 and 5.

For more information about types of fixes, see the *Software Support Handbook* (http://techsupport.services.ibm.com/guides/handbook.html).

Contacting IBM Software Support

IBM Software Support provides assistance with product defects.

Before contacting IBM Software Support, your company must have an active IBM software maintenance contract, and you must be authorized to submit problems to IBM. The type of software maintenance contract that you need depends on the type of product you have:

- For IBM distributed software products (including, but not limited to, Tivoli, Lotus®, and Rational® products, as well as DB2® and WebSphere® products that run on Windows or UNIX operating systems), enroll in Passport Advantage® in one of the following ways:
  - **Online**: Go to the Passport Advantage Web page (http://www.lotus.com/services/passport.nsf/WebDocs/Passport_Advantage_Home) and click **How to Enroll**.
  - **By phone**: For the phone number to call in your country, go to the IBM Software Support Web site (http://techsupport.services.ibm.com/guides/contacts.html) and click the name of your geographic region.
- For IBM eServer™ software products (including, but not limited to, DB2 and WebSphere products that run in zSeries®, pSeries®, and iSeries™ environments), you can purchase a software maintenance agreement by working directly with an IBM sales representative or an IBM Business Partner. For more information about support for eServer software products, go to the IBM Technical Support Advantage Web page (http://www.ibm.com/servers/eserver/techsupport.html).

If you are not sure what type of software maintenance contract you need, call 1-800-IBMSERV (1-800-426-7378) in the United States or, from other countries, go to the contacts page of the IBM Software Support Handbook on the Web (http://techsupport.services.ibm.com/guides/contacts.html) and click the name of your geographic region for phone numbers of people who provide support for your location.

Follow the steps in this topic to contact IBM Software Support:

1. Determine the business impact of your problem.
2. Describe your problem and gather background information.

3. Submit your problem to IBM Software Support.

Determine the business impact of your problem

When you report a problem to IBM, you are asked to supply a severity level. Therefore, you need to understand and assess the business impact of the problem you are reporting. Use the following criteria:

Severity 1	**Critical** business impact: You are unable to use the program, resulting in a critical impact on operations. This condition requires an immediate solution.
Severity 2	**Significant** business impact: The program is usable but is severely limited.
Severity 3	**Some** business impact: The program is usable with less significant features (not critical to operations) unavailable.
Severity 4	**Minimal** business impact: The problem causes little impact on operations, or a reasonable circumvention to the problem has been implemented.

Describe your problem and gather background information

When explaining a problem to IBM, be as specific as possible. Include all relevant background information so that IBM Software Support specialists can help you solve the problem efficiently. To save time, know the answers to these questions:

- What software versions were you running when the problem occurred?
- Do you have logs, traces, and messages that are related to the problem symptoms? IBM Software Support is likely to ask for this information.
- Can the problem be re-created? If so, what steps led to the failure?
- Have any changes been made to the system? (For example, hardware, operating system, networking software, and so on.)
- Are you currently using a workaround for this problem? If so, please be prepared to explain it when you report the problem.

Submit your problem to IBM Software Support

You can submit your problem in one of two ways:

- **Online**: Go to the "Submit and track problems" page on the IBM Software Support site (http://www.ibm.com/software/support/probsub.html). Enter your information into the appropriate problem submission tool.
- **By phone**: For the phone number to call in your country, go to the contacts page of the IBM Software Support Handbook on the Web (techsupport.services.ibm.com/guides/contacts.html) and click the name of your geographic region.

If the problem you submit is for a software defect or for missing or inaccurate documentation, IBM Software Support creates an Authorized Program Analysis Report (APAR). The APAR describes the problem in detail. Whenever possible, IBM Software Support provides a workaround for you to implement until the APAR is resolved and a fix is delivered. IBM publishes resolved APARs on the IBM product support Web pages daily, so that other users who experience the same problem can benefit from the same resolutions.

For more information about problem resolution, see Searching knowledge bases and Obtaining fixes.

Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information in softcopy form, the photographs and color illustrations might not display.

Trademarks

IBM, the IBM logo, AIX, DB2, IBMLink, Informix, OS/2, OS/400, Tivoli, the Tivoli logo, and, the Tivoli Enterprise Console are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

Lotus and Lotus Notes are trademarks of International Business Machines Corporation and Lotus Development Corporation in the United States, other countries, or both.

Intel, the Intel Inside logos, MMX, and Pentium are trademarks of Intel Corporation in the United States, other countries, or both.

Microsoft and Windows NT are registered trademarks of Microsoft Corporation in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product, and service names may be trademarks or service marks of others.

Program Number: 5724-C06