IBM Tivoli Configuration Manager

IBM

Readme File for Fix Pack 1 - PTF U804307

Version 4.2.3

IBM Tivoli Configuration Manager

Readme File for Fix Pack 1 - PTF U804307

Version 4.2.3

> **Note**
>
> Before using this information and the product it supports, read the information in "Notices" on page 53.

Contents

Tables

IBM Tivoli Configuration Manager 4.2.3 ReadMe File for Fix Pack 4.2.3-TCM-FP01 (PTF U804307)

This readme file provides important information about Fix Pack 1 (PTF U804307) for IBM® Tivoli® Configuration Manager Version 4.2.3. This readme file is the most current information for the fix pack and takes precedence over all other documentation for IBM Tivoli Configuration Manager, Version 4.2.3. This fix pack fixes a variety of defects of Tivoli Configuration Manager.

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

About this release

This section includes the following topics:

- "CD-ROM structure"
- "New features" on page 2
- "Backward compatibility issues" on page 5
- "Product compatibility" on page 5
- "Product fix history" on page 5
- "Limitations" on page 20

CD-ROM structure

IBM Tivoli Configuration Manager, Version 4.2.3 Fix Pack 1 includes *one* CD-ROM:

Table 1. IBM Tivoli Configuration Manager, Version 4.2.3 Fix Pack 1 CD

Directory or path	Contents
/xml	The XML file to be used by the ISMP installation program.
/docs	Readme file.
/images/INVENTORY	Images required for Inventory fix pack.
/images/MCOLLECT	Images required for the Scalable Collection Services fix pack.
/images/SWD	Images required for Software Distribution, Activity Planner, Change Manager, Tivoli Resource Manager, Patch Management, Pristine Manager, and Web User Interface.
/LoginControl	Software package block (SPB) and executable files used to implement the concurrent login feature. For more information on this feature, see "New features" on page 2.
/package	Software package block (SPB) files used to patch GUI components and the XML descriptor file.
/spb_installer	SPB Patch Installer that installs SPB fix pack locally and the SPB Patch Installer Guide.
/JarVersion	Scripts to retrieve and display the version of the .jar files currently installed.
/PocketPC	Files to implement fix for APAR IY75778

New features

This section contains a cumulative list of new features introduced in the previous interim fix and in the current fix pack.

- "New features in this fix pack"
- "New features in the previous interim fix" on page 3

New features in this fix pack

The following features have been introduced in this fix pack:

Table 2. Customer enhancement request references

Description	Feature
Performing patch management using WSUS	Feature 55317
Maintaining the access attributes of already existing files and directories on a UNIX® target, a new attribute (preserve_unix) is available.	Feature 55359
New 32-bit MRMBIOS.EXE	Feature 180357
Running a program before the reboot of a commit	Feature 55409
Managing software packages	Feature 55487
Working with the Software Distribution Endpoint Notification dialog	Feature 55522

Performing patch management using WSUS - Feature 55317
> You can perform patch management using WSUS to implement the approval mechanism of patches and to download up-to-date patches from the Microsoft® Web site. For more details on this new automated patch management solution, see the updated version of the *IBM Tivoli Patch Management Guide*.

> ---
> **Important**
>
> To continue working with SUS, do not install the Patch Management fix pack component and do not run the new inventory SQL scripts available with this fix pack.
> ---

Maintaining the access attributes of already existing files and directories - Feature 55359
> You can maintain the access attributes of already existing files and directories on UNIX. To enable this feature, select the **Maintain existing value** check box in the Add File System Objects Properties - Advanced window, **UNIX Attr.** tab of Software Package Editor or set preserve_unix to y in the add_directory or add_file stanzas of the SPD file.

A 32 bit scanner, `mrmbios.exe`, substitutes the 16 bit scanner - Feature 180357
> With this feature the Windows® 64-bit platforms support has been extended. The old 16-bit mrmbios.exe file has been now replaced by a 32-bit file having the same name, and using new device drivers. The new mrmbios.exe file allows you to scan, in addition to the old platforms, new platforms such as AMD 64 and Itanium 64.

Running a program before the reboot of a commit - Feature 55409
> You can run a program before the reboot of a commit by setting the following variables in swdis.var:

__COMMIT_REBOOT_FORCED__
Specifies YES to force a reboot when a commit is run with `-cr` or `-co` parameters.

__BEFORE_REBOOT_PROG_PATH__
Specifies the path of the program to be run on the endpoints. If this variable is empty no program is run.

__BEFORE_REBOOT_PROG_ARGS__
Specifies arguments passed to the program. Separate arguments with a blank space.

__BEFORE_REBOOT_PROG_TIMEOUT__
Specifies the time, expressed in seconds, to wait for the completion of the program. Default is `60`.

To enable this feature, you must set at least `__COMMIT_REBOOT_FORCED__` to YES and define the program path in `__BEFORE_REBOOT_PROG_PATH__`.

Managing software packages - Feature 55487
You can set the `use_real_capabilities` key to `true` with the **wswdmgr** command to not distribute a software package on targets belonging to policy regions where the administrator, submitting the distribution, does not have the required roles. The default is `false`.

Working with the Software Distribution Endpoint Notification dialog - Feature 55522   The Software Distribution Endpoint Notification dialog that pops up on the screen of the endpoint when a software package is submitted for distribution is changed. In the title bar the Close button (X) no longer appears. The Cancel push button is replaced by the Reset push button that resets the changed values in this dialog with the default values for this operation. To close the dialog you must click OK.

New features in the previous interim fix
The following features have been introduced in the previous interim fix:

Table 3. Customer enhancement request references

Description	Feature
Enabling proxy support for the SUS Patch Management solution	
Avoiding concurrent logins during critical distributions	Feature 54613
Performing the logoff operation on Windows endpoints	Feature 55186
Displaying the .jar files version	Feature 55204
Displaying the patch level for the Activity Plan Editor and Activity Plan Monitor	Feature 55205
Completing workflows separately	Feature 55260

Enabling proxy support for the SUS Patch Management solution
You can use a proxy server to access the Microsoft Web site, or your local HTTP server where the mssecure.cab file has been downloaded.

You can customize the HTTP proxy server name (if enabled) and the related user ID and password (if required by the proxy settings). Proxy parameters are defined at installation time in the tpm_update.req file, as described in the readme of the interim fix. This feature guarantees a higher security when accessing the Internet or your local network.

Avoiding concurrent logins during critical distributions - Feature 54613

On Windows operating systems, you can use the concurrent login feature to prevent the end user from logging in to the workstation and performing a shutdown while a distribution is taking place. This feature guarantees that critical distributions are not interrupted. You can also define a maximum number of logins that can be performed during a distribution. In this case, the distribution is paused and restarts after the user logs off. For more information, see "Implementing the concurrent login feature" on page 30.

Performing the logoff operation on Windows endpoints - Feature 55186

You can perform the logoff operation on Windows endpoints. A new action has been added to the software package definition file. You can define the logoff operation in the following phases:

- during_install
- during_remove
- during_commit
- during_undo

For more information on this feature, see "Documentation notes" on page 41.

Displaying the .jar files version - Feature 55204

You can display the version of APM .jar files, if the version is indicated in the .jar file. You can start the command on Tivoli servers and managed nodes after having set the Tivoli environment, as described below:

On UNIX operating systems:
. ./wjarversion.sh *jarfile*

On Windows operating systems:
wjarversion.bat *jarfile*

where:

jarfile   Is the name of the .jar file for which you want to display the version. The following are the .jar files supported for this feature:

- apm.jar
- apm_utils.jar
- swd_plugin.jar
- tl_plugin.jar

The files required for implementing this feature are located in the /JarVersion folder in IBM Tivoli Configuration Manager, Fix Pack 4.2.3-TCM-FP01.

Displaying the patch level for the Activity Plan Editor and Activity Plan Monitor - Feature 55205

You can display the patch level installed for the Activity Plan Editor and Activity Plan Monitor by selecting the **About** menu item in the **Help** menu.

Completing workflows separately - Feature 55260

You can decide whether patch management workflows are completed in one or in two steps. This feature guarantees a higher flexibility in the workflow process. For more information on this feature, see "Documentation notes" on page 41.

Backward compatibility issues

To continue working with SUS, do not install the Patch Management fix pack component and do not run the new inventory SQL scripts available with this fix pack.

However, Tivoli suggests migrating to the WSUS automated patch management solution because of the SUS Microsoft limited support.

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 Fix Pack 1 was tested using Tivoli Management Framework, Version 4.1.1 plus fix pack 3 containing the following interim fixes:
- 4.1.1-LCF-0020 to be installed on the Tivoli gateways.
- 4.1.1-TMF-0039 to be installed on the managed nodes with JRIM and JCF components installed.
- 4.1.1-TMF-0046 to be installed on Tivoli servers, managed nodes, and gateways.

and 4.1.1-LCF-0024T to enable the AMD64 and IA64 support.

Product fix history

The following sections include all interim fixes shipped since the IBM Tivoli Configuration Manager, Version 4.2.3 release. It is divided into the following subsections:
- "Fixes contained in this fix pack"
- "Fixes contained in previous interim fixes" on page 18

Fixes contained in this fix pack

Table 4 lists the fixes included in this fix pack:

Table 4. Fixes included in this fix pack

Fix pack	Component/Service
4.2.3-INV-FP01	Inventory, Version 4.2.3
4.2.3-INVGW-FP01	Inventory Gateway, Version 4.2.3
4.2.3-CLL-FP01	Scalable Collection Service, Version 4.2.3
4.2.3-SWDSRV-FP01	Software Distribution, Version 4.2.3
4.2.3-SWDGW-FP01	Software Distribution Gateway, Version 4.2.3
4.2.3-SWDJPS-FP01	Software Distribution Software Package Editor, Version 4.2.3
4.2.3-APM-FP01	Activity Planner, Version 4.2.3
4.2.3-CCM-FP01	Change Manager, Version 4.2.3
4.2.3-WEB-FP01	Web Interface, Version 4.2.3
4.2.3-TRMSRV-FP01	Resource Manager, Version 4.2.3
4.2.3-TRMGW-FP01	Resource Manager Gateway, Version 4.2.3
4.2.3-PMSRV-FP01	Pristine Manager, Version 4.2.3
4.2.3-PMG-FP01	Patch Management, Version 4.2.3

APARs and internal defects fixed for Inventory: Table 5 lists the APARs and internal defects that were fixed for Inventory:

Table 5. APARs and internal defects for Inventory

Inventory, Version 4.2.3, 4.2.3–INV-FP01		
IY71821	IY73290	IY73560
IY73562	IY73952	IY74343
IY74421	IY74693	IY74769
IY75165	IY75168	IY75169
IY75350	IY75358	IY75611
IY75778	IY75835	IY76004
IY76150	IY76421	175653

APAR IY71821

Abstract:
Add the support for a new "exclude DFS™" configuration tag

Error Description:
On UNIX workstations, the scan of the DFS filesystem can take a long time if the DFS filesystem is very big.

APAR IY73290

Abstract:
`wscanner` hangs on USB component with Targus port replicator

Error Description:
When distributing a hardware scan to a Windows machine with a Targus port replicator device attached, the `wscanner` process hangs on the target machine. If you deselect the USB component in the scan hardware configuration, the scan ends correctly.

APAR IY73560

Abstract:
Failure generating `nativ_id`

Error Description:
The process of generating `nativ_id` for installed software using `rpm` `pkginfo` is not working, if two different rpm packages having the same name are installed on a machine.

APAR IY73562

Abstract:
Failure during hardware scan printer section

Error Description:
The `wscanner` command failure occurs when the printer component is selected in the hardware scan. The problem might occur if the user is not logged onto the machine. Running the `wscanner` command manually is successful.

Additional Info:
When getting the failure, the `tivhscan.mif` file is incomplete and the `libInvHW.log` file contains the following last lines:

```
Begin Group Printer getTable()
Netware client not found.
WMI Instance Enumeration unsuccessful.
Reverting to legacy detection.
```

APAR IY73952

Abstract:

Wscanner high CPU usage

Error Description:

Wscanner uses 100% of CPU when determining processor speed on Windows.

APAR IY74343

Abstract:

A Dr. Watson error occurs on hardware scan with USB device

Error Description:

The legacy scan of USB might produce a Dr. Watson error. You can use the new environment variable, USEWMIFORUSB, to force the use of WMI for running the USB scan. You must run a reboot before performing a scan.

APAR IY74421

Abstract:

Incorrect directory used by the **winviso** command on Windows endpoints

Error Description:

On Windows endpoints, the **winviso** command creates, under the path %LCFROOT%/inv/ISOLATED, a directory whose name is INV followed by a four-digit number representing the Inventory scan ID:

%LCFROOTi%/inv/ISOLATED/INVxxxx

The correct directory name should be the InventoryConfig profile name:

%LCFROOT%/inv/ISOLATED/*inv_profile_name*

The problem does not occur on UNIX endpoints.

APAR IY74693

Abstract:

Unable to detect UltraSPARC IV workstations.

Error Description:

Inventory shows Processor type SPARC Family

APAR IY74769

Abstract:

PCI scan does not return data on Solaris system

Error Description:

PCI scans do not return data on Solaris Sun Fire 6800 systems on IBM Tivoli Configuration Manager Inventory

APAR IY75165

Abstract:

Different processor speed in MIF file and database

Error Description:

Inventory does not manage the processor speed value.

APAR IY75168

Abstract:

MIF parse error in the `mrmbios.mif` file

Error Description:

When parsing the `mrmbios.mif` file, the hardware scan might fail with the following error:

`Mrmbios.mif: line 1: Syntax error: CompName unexpected`

APAR IY75169

Abstract:

The Inventory header scan works with errors

Error Description:

The inventory header scan works without problems, even if running a query on one of the endpoint subscribers of the scan, for some packages the version reported is the version of the previous row.

APAR IY75350

Abstract:

Ultrasparc III and processor not properly recognized

Error Description:

Inventory shows Processor type SPARC Family.

APAR IY75358

Abstract:

BIOS_DATE in PC_BIOS_VIEW and SMBIOS_DATA_VIEW do not match

Error Description:

Logs show that the `BIOS_DATE` attribute has a different value in the `mrmbios.mif` file and in the `tivscan.mif` file.

APAR IY75611

Abstract:

wgetinvglobal output cannot be parsed

Error Description:

wgetinvglobal output cannot be parsed

APAR IY75778

Abstract:

Distributing inventory scan to Wince device causes IBM agent to crash

Error Description:

When you distribute an inventory scan to Wince device, the IBM agent crashes.

Additional information:

You can enable the PocketPC device agent, as follows:

1. On the source host, in a temporary directory such as `C:\temp`, copy the `ceagent.arm.CAB` and `Tivoli_PocketPC_ARM_Agent_Patch.v4.2.3.FP01.spd` files from the directory `PocketPC`.
2. Edit the package `Tivoli_PocketPC_ARM_Agent_Patch.v4.2.3.FP01.spd` by setting the value of the `agent_name_dir`, `location`, and `name` variables. The `agent_name_dir` is the Agent path on the device, while the `location` and `name` are used to set the path of the `ceagent.arm.CAB` file on the source host, such as `C:\temp\agent`.
3. Import the package.
4. On the Tivoli Web Gateway, stop the Device Manager Server
5. Update the Device Manager database.

   Note: All pending operations should be completed and connections to the database closed while you are performing the following steps:
   a. Invoke a DB2CMD shell on the database server.
   b. Change directories to the Device Manager server install directory: `dms_home/bin /data`.
   c. Connect to the Device Manager database. (For example: db2 connect to dms user dmsadmin using password).
   d. Invoke the patch script. For example: `db2 -tvf IY75778_db2.sql`
6. On the Tivoli Web Gateway, start the Device Manager Server
7. Distribute the package to the device. The package installs the files on a permanent path of the device.

   Note: During the Agent installation, you receive a message on the device asking if you want to install the IBM agent again. Click **OK** to confirm the installation.

APAR IY75835

Abstract:
   wscanner.exe - Entry Point Not Found

Error Description:
   When you use an inventory profile to scan a Windows NT® endpoint, the scan fails.

APAR IY76004

Abstract
   Inventory hardware scan crashes backup tapes

Error Description:
   When you run a hardware scan on a Solaris or a Linux™ endpoint with Ultrium tape running, the tape robot ejects the tape.

APAR IY76150

Abstract:
   Duplicated `NATIV_ID` values for different products on AIX®

Error Description:
> When performing a software native scan on AIX machines, some installed packages detected in the `tivrscan.mif/bk1` file are not inserted into the database, in the `NATIV_SWARE` table.

APAR IY76421

Abstract
> Update internal tables for Intel® and AMD processors

Error Description:
> The tables used by the Inventory scanner to discover Intel and AMD processors must be updated.

Defect 175653
> The WebUI client does not send a report for an inventory scan.

APARs and internal defects fixed for Scalable Collection Service: Scalable Collection Service component does not currently contain any fixed APARs.

APARs and internal defects fixed for Software Distribution: Table 6 lists the APARs and internal defects that were fixed for Software Distribution:

Table 6. APARs and internal defects for Software Distribution

Software Distribution, Version 4.2.3, 4.2.3-SWDSRV-FP01		
IY73006	IY73540	IY74170
IY74230	IY74344	IY74847
IY75068	IY75474	IY75754
IY76041	IY76315	
54100	55566	55783
55828	55829	55830
55839	55877	
Software Distribution Gateway, Version 4.2.3, 4.2.3-SWDGW-FP01		
IY74170	IY74578	IY74585
IY74764	IY74801	IY75236
IY75754	IY76041	
54100	55566	55783
Software Package Editor, Version 4.2.3, 4.2.3-SWDJPS-FP01		
IY76041		
Software Package Editor for Endpoints, Version 4.2.3, 4.2.3-SWDEP-FP01		
IY74392		

APAR IY73006

Abstract:
> `EXEC_TIME` incorrectly updated for undoable software packages

Error Description:
> When you install a package using the undoable option, all the packages with the same name and old version are wrongly updated in the database.

APAR IY73540

Abstract:
>
> MSB files left in Software Distribution message directory in case of load operations with deleted nested software packages

Error Description:
>
> Start a load operation and immediately delete the main or a nested package. The MSB files remain in the message directory when the reports return to the Tivoli server, and are never removed.

APAR IY74170

Abstract:
>
> SD_INST EXEC_TIME is blank after issuing the command `wcommtsp -cr`

Error Description:
>
> If you install a software package and then commit it by using the following commands:
>
> ```
> winstsp -ty -uy
> wcommtsp -cr
> ```
>
> when the commit is completed, the field EXEC_TIME taken from SD_INST is empty.

APAR IY74344

Abstract:
>
> Running a program before the reboot of a commit

Error Description:
>
> You cannot run a program before the reboot of a commit.

APAR IY74392

Abstract:
>
> Problem retrieving a file with variables in the filename

Error Description:
>
> When you perform a retrieve data from an endpoint to a managed node and the name of the file to be retrieved contains a variable, the file is retrieved without creating the default *endpointname_distributionID_timestamp* sub-directory under the specified destination directory on the source host.

APAR IY74578

Abstract:
>
> Undoable installation does not complete if endpoint is turned off

Error Description:
>
> You install a software package using the undoable option and you turn off the endpoint during the file transfer interrupting the distribution. When the endpoint is turned on again, the distribution restarts, but does not complete.

APAR IY74585

Abstract:
>
> EXECUTE_USER_PROGRAM using SUCCESS_REBOOT_NOW_REEXECUTE does not work correctly when using commit with user reboot

Error Description:
>
> If you run `wcommtsp -c y` against a software package containing a script

ending with a return code equal to `success_reboot_now_reexecute`, after the user reboot, the commit action starts and the script runs and exits with a `success_reboot_now_reexecute` code. The endpoint reboots but does not re-execute the script.

APAR IY74764

Abstract:
Problem sending multiple software packages using commit in a user reboot

Error Description:
If you distribute multiple software packages using commit in a user reboot, by running the command `winstsp -ty -cy`, and then perform a manual reboot, the packages are not always committed in the correct order.

APAR IY74801

Abstract:
Problem with packages with a `USER_PROGRAM DURING_COMMIT`

Error Description:
When resinit must process more than one package, it performs all the possible operations on all packages before a reboot (if required). To change this behavior, a key in swdis.ini has been added: `resinit_one_reboot`. If you set `resinit_one_reboot=n` to swdis.ini (on target), resinit will process the packages one-by-one and if one of them requires a reboot, it is performed immediately. The default value is `resinit_one_reboot=y`.

APAR IY74230

Abstract:
Sending notices to notice groups does not work properly

Error Description:
After distributing a software package with the **Notice to software distribution group** check box checked, in the notices the administrator name is corrupt.

APAR IY74847

Abstract:
Datamoving - Send operation from GUI displays the selected pre-script at origin file in the wrong field

Error Description:
In the Data Moving Service Send Operation panel of the DSL GUI, if you set **Data Origin Type** to **EndPoint** and select a file for **Pre-script at Origin** using the **...** button, the selected file is written in the **File Path at Origin** and **File Name** fields.

APAR IY75068

Abstract:
wspmvdata causes access violation error using empty target list

Error Description:
If you run the **wspmvdata** command using an empty target list file on a Windows Tivoli server, an Access Violation error occurs.

APAR IY75236

Abstract:
> The success_in_a_reboot exit code does not work correctly.

Error Description:
> The success_in_a_reboot exit code returned from a user program does not cause the next action in the package to be performed.

APAR IY75474

Abstract:
> Priority is not honored when performing data moving wspmvdata between endpoints

Error Description:
> If you submit a send data moving operation with a low priority, when the distribution reaches the target endpoint, the priority is changed.

APAR IY75754

Abstract:
> The order of remove operation for actions in container is not reverted

Error Description:
> The actions within a container are not reverted at the remove time as is the case with the actions listed as software package actions.

APAR IY76041

Abstract:
> Corruption of registry keys with exported packages.

Error Description:
> Registry keys ending with the \ character are corrupted during the software package export.

APAR IY76315

Abstract:
> Software distribution goes in interrupted status

Error Description:
> If you install a software package with the option `from_depot=y` and you set `wswdmgr from_depot=yes`, when the distribution reaches the endpoint an INTERRUPTED event is generated and an incorrect package size is sent back.

Defect 54100
> Using the Tivoli Resource Monitor synchronous operation, the maximum number of devices that can be managed is 3000. If the system discovers more than that number of devices, an error is returned.

Defect 55566
> If you use the **wsecgensp** command when the RDBMS server is not working, an empty package is created and a general Tivoili Management Framework error is displayed.

Defect 55783
> The following commands are not valid for wldsp:
> ```
> multicast =y and from_fileserver=y from_fileserver
> multicast =y and from_cd=y from_cd
> ```

Defect 55828
> After submission of an Activity Plan Monitor generated from patch

management, a user notification panel is displayed on the target endpoints. The date format for 'Defer Time' and Show Details --> 'Mandatory Date' is different. The first one reports dd/mm/yy, the second one mm/dd/yy.

Defect 55829

An asynchronous discover does not retrieve all devices.

Defect 55830

The following error occurs when trying to import an existing package using the impspo -f *filename*.spd:

DISSE0064E The software package object `@*filename*.1.0' does not exist.

Defect 55839

When installing a software package using the Install Software Package GUI, and you install the package using the **Install** (instead of **Install & close**), then click again on **Install**, the GUI can stop with a generic oserv failure.

Defect 55877

If you install a package in IC state, then install a package in undoable mode that has the same name but with a greater version, the first package becomes hidden, but when you undo the package it will remain hidden.

APARs and internal defects fixed for Activity Planner: Table 7 lists the APARs and internal defects that were fixed for Activity Planner:

Table 7. APARs and internal defects for Activity Planner

Activity Planner, Version 4.2.3, 4.2.3–APM-FP01		
IY73578	IY73642	IY74285
IY74288	IY74438	IY74754
IY74842	IY75060	IY75114
IY75608	IY75767	IY75834
IY76002	55871	

APAR IY73578

Abstract:

wmonpln command cores trying to manage an exception

Error Description:

The wmonpln command might generate a core dump on AIX platforms, if it is invoked while the APM processes are up and running but the oserv process is going down.

APAR IY73642

Abstract:

In the Activity Planner monitor GUI the activities are listed in the incorrect order after selecting a filter

Error Description:

If you apply a filter on a plan and then you restore the All Plans view in the Activity Planner monitor GUI, the resulting activities are listed in an incorrect order.

APAR IY74285

Abstract:

Default filter cannot be set using `wapmfltr`

Error Description:

If you define a default filter by using `wapmfltr DEFAULT_FILTER=y` an error message is displayed saying that the equal key is not valid for `DEFAULT_FILTER`.

APAR IY74288

Abstract:

Add a new option to `wapmfltr`

Error Description:

If you have the `APM_View` role you cannot save filters or set default filters. You must specify the owner of the filter using the `-u` option in the `wapmfltr` command. For further information see "User's Guide for Deployment Services" on page 45.

APAR IY74438

Abstract:

Operation conditioned by depot does not work

Error Description:

In an activity plan, a software distribution operation activity, such as a transactional installation, that is conditioned by Completion Depot or Success Depot of a previous load activity, does not start on the endpoints when the related gateway completes, but it starts when all the gateways have completed.

APAR IY74754

Abstract:

APM activities are not cancelled after their completion

Error Description:

In the APM monitor GUI, the APM activities are not cancelled after their completion, if the endpoint is in the interrupted status. When the `complete_not_after` event expires, all waiting activities are cancelled.

APAR IY74842

Abstract:

Activity plan monitor GUI loops when refreshing data for huge plans (more than 400® activities)

Error Description:

From the Activity plan monitor you refresh data for some plans consisting of hundreds of activities. If you click **Reload Data for the selected item** on the plan, the Activity plan monitor GUI loops. No problem occurs if you click **Reload data from APM database**.

APAR IY75060

Abstract:

APM does not meet the max_rpc_threads setting.

Error Description:

APM does not manage the maximum number of Tivoli methods defined in the max_rpc_threads setting.

APAR IY75114

Abstract:
> Endpoint status is not updated

Error Description:
> When the plan is completed, the endpoint status for a distribution (wmdist -e <activity_id>) is not updated with the final status.

APAR IY75608

Abstract:
> Conditioning CD(load) and ST(install) do not work

Error Description:
> If you condition an install activity by depot and you save the plan as a template or you submit it, the following message is displayed:
> ```
> AMN0164E Conditioning by depot cannot be used for activity "Install"
> because at least one conditioning activity has no targets of type ManagedNode
> ```

APAR IY75767

Abstract:
> APM does not correctly manage Failure on Target conditioning

Error Description:
> APM does not correctly manage the Failure on Target conditioning.

APAR IY75834

Abstract:
> Indexing does not prevent deadlock condition

Error Description:
> An exception occurs in the Activity Planner Command Line Interface Trace, due to a deadlock shown in the RIM object traces.

APAR IY76002

Abstract:
> wcntpln -f does not set the plan status to cancelled.

Error Description:
> Even if you force a cancel of a plan activity, the final status of the plan is successful.

Defect 55871
> The **-u** option of the **wapmfltr** command is not documented in the catalog for the command. The option does work.

APARs and internal defects fixed for Change Manager: Change Manager component does not currently contain any fixed APARs.

APARs and internal defects fixed for the Web Interface: Table 8 lists the APARs and internal defects that were fixed for Web Interface:

Table 8. APARs and internal defects for Web Interface

Web Interface, Version 4.2.3, 4.2.3-WEB-FP01		
55829		

Defect 55829

An asynchronous discover does not retrieve all devices.

APARs and internal defects fixed for the Resource Manager: Table 9 lists the APARs and internal defects that were fixed for Resource Manager:

Table 9. APARs and internal defects for Resource Manager

Resource Manager, Version 4.2.3, 4.2.3-TRMSRV-FP01		
54100	55781	

Defect 54100

Using the Tivoli Resource Monitor synchronous operation, the maximum number of devices that can be managed is 3000. If the system discovers more than that number of devices, an error is returned.

Defect 55781

If you start the **wresgw discover** command, all the Tivoli Web Gateway endpoints are discovered, instead of the user being able to specify a specific endpoint name.

APARs and internal defects fixed for Pristine Manager: Pristine Manager component does not currently contain any fixed APARs.

APARs and internal defects fixed for Patch Management: Table 10 lists the APARs and internal defects that were fixed for Patch Management:

Table 10. APARs and internal defects for Patch Management

Patch Management, Version 4.2.3, 4.2.3–PMG-FP01		
55566	55773	55776
55783	55812	55851
55934	55938	

Defect 55566

If you use the **wsecgensp** command when the RDBMS server is not working, an empty package is created and a general Tivoili Management Framework error is displayed.

Defect 55773

RECORD TIME is different when **wsecrprt -kC** is used with either the **-ge** or **-gp** parameters.

Defect 55776

During the execution of TCM_MS_Discover_Patches, the disk space to where the patches are copied from Tivoli Patch Manager becomes full. The workflow goes on and completes successfully, but only the patches managed when disk space was available are correctly imported from Tivoli Patch Manager.

AT®

Defect 55783

The following commands are not valid for wldsp:

```
multicast =y and from_fileserver=y from_fileserver
multicast =y and from_cd=y from_cd
```

Defect 55812

When network failures occur, the workflow can fail when the timeout expires and no clear error message is displayed.

Defect 55851

A problem with absolute and relative paths can occur when defining new templates for the **wsacgenplan** and **wsecgensp** commands using the **wseccfg** command. For example, you might need to specify the absolute path for the **wsecgensp** command (for example, wseccfg -s standard_template_file=C:tmpnicola.spd) but if you do the same for **wsacgenplan** you will get an error.

Defect 55934

When running the Group_Status_Updater or TCM_Update_Patches workflow and the Tivoli Administrator does not have the APM_Edit role, an incorrect warning message is displayed:

```
WARN: Cannot delete the activity plans. You do not have the necessary role
assigned to exec the command: >wdelplan<
Removing obsolete SPs and Queries for TCM Generating SPs and Plans for
missing patches
```

The **wdelplan** command displayed in the message is incorrect, it should be **wdelpln**.

Defect 55938

The following error can occur if the patch being downloaded is too large:

```
Error downloading patch.
Message: COPDEX044E An error occurred in the embedded logical operation:
"COPDEX044E An error occurred in the embedded logical operation:
"COPCOM116E The operation timed out.
```

Fixes contained in previous interim fixes

The following APARS and defects were shipped in the previous interim fix.

Table 11. APARs and internal defects for Inventory included in this fix pack from

Inventory, Version 4.2.3, 4.2.3–INV-0001		
IY69466	IY70916	IY70604
IY71015	IY72989	IY73177
IY73657	179423	179893
180462		
Inventory Gateway, Version 4.2.3, 4.2.3–INVGW-0001		
IY63636	IY70006	IY70234
IY70308	IY70912	IY70951
IY71000	IY71001	IY71336
IY72224	IY72269	IY72860
IY72944		

Table 12. APARs and internal defects for Scalable Collection Service included in this fix pack from

Scalable Collection Service, Version 4.2.3, 4.2.3–CLL-0001		
IY66400	IY69816	IY70039
IY70283		

Table 13. APARs and internal defects for Software Distribution included in this fix pack from

Software Distribution, Version 4.2.3, 4.2.3–SWDSRV-0001		
IY70587	IY70596	IY73905
IY71192	IY71401	IY71403
IY71443	IY71461	IY71795
IY72216	IY72454	54846
55063	55194	55275
Software Distribution Gateway, Version 4.2.3, 4.2.3-SWDGW-0001		
IY68380		
IY69280	IY70198	IY70495
IY71010	IY71192	IY71983
IY71991	IY72454	IY72698
IY72786	55063	55194
55275		
Software Package Editor, Version 4.2.3, 4.2.3-SWDJPS-0001		
IY67885	IY72632	
Software Package Editor for Endpoints, Version 4.2.3, 4.2.3-SWDEP-0001		
IY68380	IY69280	IY70198
IY70495	IY71010	IY71991
IY72698	IY72490	IY72786

Table 14. APARs and internal defects for Activity Planner included in this fix pack from

Activity Planner, Version 4.2.3, 4.2.3–APM-0001		
IY69394	IY70587	IY71064
IY71340	IY71810	IY71812
IY71963	IY72845	IY72998
IY73503		IY74468
IY74948	54559	

Table 15. APARs and internal defects for Change Manager included in this fix pack from

Change Manager, Version 4.2.3, 4.2.3–CCM-0001		
IY64369		

Table 16. APARs and internal defects for Web interface included in this fix pack from

Web Interface, Version 4.2.3, 4.2.3–WEB-0001		
IY70838	IY71394	

Table 17. APARs and internal defects for Pristine Manager included in this fix pack from

Pristine Manager, Version 4.2.3, 4.2.3-PRI-0001		
IY71465		

Table 18. APARs and internal defects for Patch Management included in this fix pack from

Patch Management, Version 4.2.3, 4.2.3-PMG-0001		
53932	53934	54956
55130	55273	55329

Limitations

Defect 182062: In IBM Tivoli Configuration Manager, Version 4.2.3 Fix Pack 1, the legacy scan for USB devices on Itanium machines has been disabled because of a Microsoft problem.

Defect 181204: When you distribute a hardware scan profile to a Windows 2003 with an AMD Opteron processor, the processor being detected is incorrect. It results in "Pentium® M" instead of "AMD Opteron Family" because of a Microsoft problem.

Defect 55849: After the Tivoli Resource Manager upgrade from 4.2.2 to 4.2.3, to display the Nokia9300 type in the Software Package Editor GUI, run the $BINDIR/TRM/RegisterPervasive.sh script and the **reexec** command on the Tivoli server.

Defect 55356: The configuration of the SUS server as proxy host in the tpm_update.req file is not supported with IBM Tivoli Configuration Manager, Version 4.2.3 and Interim Fix 0001. You must specify any other proxy host different from the SUS server.

Defect 182246: On Windows Server 2003 Enterprise Edition the scanner does not detect mapped drives.

Installation

This section describes how to install fix pack 1 to upgrade the various components of IBM Tivoli Configuration Manager, Version 4.2.3. The method of installation depends on the component you are upgrading. Once you have installed the fix pack, you cannot uninstall it automatically. Ensure that you perform a complete backup of your system before installing this fix pack.

This section includes the following topics:
- "Hardware and software requirements"
- "Traditional fix pack installation methods" on page 21
- "Software package block (SPB) fix pack installation for GUI components" on page 24
- "Updating the Inventory schema" on page 29

Hardware and software requirements

This section includes the following topics:
- "Supported platforms" on page 21

- "System requirements"

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*.

Upgrading large environments

To upgrade large environments you should start installing the fix pack on the Tivoli gateways. If you cannot install the fix pack on the Tivoli server and all the gateways at the same time, to ensure that all gateways work, perform the following steps:

1. Install the Inventory, Version 4.2.3, backward compatibility patch on the Tivoli Inventory server. See Table 19 on page 23 for information about the related IND file.
2. Install the fix pack on the Tivoli gateways.

Traditional fix pack installation methods

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

- "Installing fix packs using ISMP"

  The InstallShield MultiPlatform (ISMP) program, which installs the appropriate IBM Tivoli Configuration Manager fix pack components for the entire Tivoli management region (Tivoli region).
- "Installing fix packs using the Tivoli desktop" on page 22

  A graphical user interface that you use to select the fix pack components to install and the target workstations on which to install them.
- "Installing fix packs using the CLI" on page 23

  Tivoli Management Framework command that you use to specify the fix pack components to install and the target workstations on which to install them from the command line interface.
- "Installing fix packs using SIS" on page 24

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

Installing fix packs using ISMP

The InstallShield MultiPlatform (ISMP) program provides a wizard-guided process for installing fix packs. 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.

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

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

1. Locate the setup executable and run the following command in the root directory of IBM Tivoli Configuration Manager Installation CD:
   - 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 fix pack directory. Click **Next**.

4. The actions necessary to upgrade your environment are being generated. When the process completes, a panel displays the fix pack components to 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 fix packs using the Tivoli desktop

When installing fix packs using the Tivoli desktop, the images are located in the images subdirectory on the IBM Tivoli Configuration Manager, Version 4.2.3 Fix Pack 1 CD. 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 fix packs using the CLI

When upgrading products using the **wpatch** command, specify the name of the index file using the file shown in Table 19. 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 CD-ROM/images -i index file managed node
```

where:

-c *CD-ROM*/**images**
> Specifies the path to the images on the IBM Tivoli Configuration Manager, Version 4.2.3 Fix Pack 1 CD.

-i *index file*
> Specifies the product installation index file to which the fix pack is installed.

managed node
> Specifies the managed node on which the fix pack 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 fix pack.

Table 19. IND files included in this fix pack

IND file	Component name	Tag
CLLFP1.IND	Scalable Collection Service, Version 4.2.3	4.2.3-CLL-FP01
INVFP1.IND	Inventory, Version 4.2.3	4.2.3-INV-FP01
LCFFP1.IND	Inventory Gateway, Version 4.2.3	4.2.3-INVGW-FP01
SWDFP1.IND	Software Distribution, Version 4.2.3	4.2.3-SWDSRV-FP01
SDGWFP1.IND	Software Distribution Gateway, Version 4.2.3	4.2.3-SWDGW-FP01
SDJPFP1.IND	Software Distribution Software Package Editor, Version 4.2.3	4.2.3-SWDJPS-FP01

Table 19. IND files included in this fix pack (continued)

IND file	Component name	Tag
APMFP1.IND	Activity Planner, Version 4.2.3	4.2.3-APM-FP01
CCMFP1.IND	Change Manager, Version 4.2.3	4.2.3-CCM-FP01
WEBUIFP1.IND	Web Interface, Version 4.2.3	4.2.3-WEB-FP01
TRMFP1.IND	Resource Manager, Version 4.2.3	4.2.3-TRMGW-FP01
TRMGWFP1.IND	Resource Manager Gateway, Version 4.2.3	4.2.3-TRMGW-FP01
PMFP1.IND	Pristine Manager, Version 4.2.3	4.2.3-PRI-FP01
PMGFP1.IND	Patch Management, Version 4.2.3	4.2.3-PMG-FP01
ICOMPFP1.IND	Inventory, Version 4.2.3, backward compatibility patch	4.2.3-INV-COMP-FP01

Installing fix packs using SIS

When installing fix packs using Tivoli Software Installation Service, select the fix pack component to be installed using the component name shown in Table 19 on page 23.

Tivoli Software Installation Service does not distinguish between products and fix packs. 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) fix pack installation for GUI components

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

* "SPB Patch Installer" on page 27
* "Software Distribution server command" on page 28
* "Software Distribution disconnected command" on page 28

IBM Tivoli Configuration Manager, Version 4.2.3 GA package is a prerequisite of the SPB fix packs.

To successfully install fix packs using any of these installation methods, you must 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 fix pack 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 fix packs are listed in Table 20.

Table 20. Default variables defined in SPB fix packs

Variable	Value	Description
Tivoli_APM_GUI_Fix.v4.2.3.FP01		
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_CCM_GUI_Fix.v4.2.3.FP01		
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_AIX_Fix.v4.2.3.FP01		
target_dir	$(product_dir)/speditor	The directory where the Software Package Editor is installed.
TME_JAVATOOLS	/opt/Tivoli/JavaTools	The directory where JRE 1.3 is installed.
Tivoli_SWDEP_HP_Fix.v4.2.3.FP01		
target_dir	$(product_dir)/speditor	The directory where the Software Package Editor is installed.
TME_JAVATOOLS	/opt/Tivoli/JavaTools	The directory where JRE 1.3 is installed.
Tivoli_SWDEP_LINUX_IX86_Fix.v4.2.3.FP01		
target_dir	$(product_dir)/speditor	The directory where the Software Package Editor is installed.
TME_JAVATOOLS	/opt/Tivoli/JavaTools	The directory where JRE 1.3 is installed.
Tivoli_SWDEP_LINUX_S390_Fix.v4.2.3.FP01		
target_dir	$(product_dir)/speditor	The directory where the Software Package Editor is installed.
Tivoli_SWDEP_LINUXPPC_Fix.v4.2.3.FP01		

Table 20. Default variables defined in SPB fix packs (continued)

Variable	Value	Description
target_dir	$(product_dir)/speditor	The directory where the Software Package Editor is installed.
TME_JAVATOOLS	/opt/Tivoli/JavaTools	The directory where JRE 1.3 is installed.
Tivoli_SWDEP_NT_Fix.v4.2.3.FP01		
target_dir	$(product_dir)\speditor	The directory where the Software Package Editor is installed.
TME_JAVATOOLS	$(program_files)\Tivoli\JavaTools	The directory where JRE 1.3 is installed.
Tivoli_SWDEP_NTAS400_Fix.v4.2.3.FP01		
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_SOLARIS_Fix.v4.2.3.FP01		
target_dir	$(product_dir)\speditor	The directory where the Software Package Editor is installed.
Tivoli_SWDEP_WIN95_Fix.v4.2.3.FP01		
target_dir	$(product_dir)\speditor	The directory where the Software Package Editor is installed.
TME_JAVATOOLS	$(program_files)\Tivoli\JavaTools	The directory where the JRE 1.3 is installed.
Tivoli_Web_Gateway_DB_Fix.v4.2.3.FP01		
No variables		
Tivoli_Web_Gateway_SRV_Fix.v4.2.3.FP01		
CLUSTER_ENV	false	Specifies whether the cluster Tivoli Web Gateway Server is to be upgraded.
LCF_LIBDIR.UNIX	$(LCFROOT)/lib/$(INTERP)	
INTERP	aix4-r1	Specifies the INTERP of the Tivoli Web Gateway Server.
LCF_LIBDIR	$(LCF_LIBDIR.$(os_family))	The LCF_LIBDIR of the endpoint
AppServer	/opt/WebSphere/AppServer	Specifies where the WebSphere® Application Server home is located.
LCF_LIBDIR.PC	$(LCF_BINDIR)	
LCF_DATDIR	/opt/Tivoli/lcf/dat/1	Specifies the LCFDAT directory for the endpoint.
LCFROOT	/opt/Tivoli/lcf	Specifies the LCFROOT directory for the endpoint.

Table 20. Default variables defined in SPB fix packs (continued)

Variable	Value	Description
DMS.Destination	/usr/TivTWG	Specifies where the Tivoli Web Gateway is installed.
LCF_BINDIR	$(LCFROOT)/bin/$(INTERP)/mrt	Specifies the LCFBINDIR directory for the endpoint.
Hostname	hostname.domain	Specifies the Tivoli Web Gateway hostname.
Tivoli_WebUI_Fix.v4.2.3.FP01		
AppServer	/opt/WebSphere/AppServer	Specifies the WebSphere Application Server home directory.
WebSrvDoc	/usr/IBMHttpServer/htdocs/en_US	Specifies the directory for the Web Server documentation.
LCF_LIBDIR	/opt/Tivoli/lcf/lib/aix4-r1	Specifies the LCFLIB directory for the endpoint.

SPB Patch Installer

This installation method uses ISMP technology that you can use to install fix packs 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. Refer to the *SPB Patch Installer Guide* located in the spb_installer directory on the IBM Tivoli Configuration Manager, Version 4.2.3 Fix Pack 1 CD for complete instructions on using this tool.

To install the SPB fix packs using the SPB Patch Installer, perform the following steps:

1. Insert the IBM Tivoli Configuration Manager, Version 4.2.3 Fix Pack 1 CD.
2. 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_$(interp).bin.
3. Read the Welcome panel and click **Next**.
4. Specify the CM423_SPB_FP01.xml file for the fix pack located in the /package subdirectory on the IBM Tivoli Configuration Manager, Version 4.2.3 Fix Pack 1 CD. Click **Next**.
5. Select **Apply** and click **Next**.
6. Specify the components you want to install and click **Next**.
7. Clear the selection of the components for which you do not want to install in undoable mode. Click **Next**.
8. 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.
9. A Summary panel is displayed. Click **Next**.
10. 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 at least a Tivoli endpoint. The following steps must be performed to apply the SPB fix pack on the targets:

1. Create a new Profile in a Profile Manager, using the naming convention described in Table 21.
2. Import the SPB file provided into the new Profile.
3. Select the endpoints to which you want to distribute the fix pack.
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 fix packs

Table 21 contains the names of the fix pack 1 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 GA SPBs are a prerequisite of the fix pack SPBs.

Table 21. Names of SPB files and software profiles

SPB Files	Package name with Version
Tivoli_APM_GUI_Fix.v4.2.3.FP01.spb	Tivoli_APM_GUI_Fix.v4.2.3.FP01
Tivoli_CCM_GUI_Fix.v4.2.3.FP01.spb	Tivoli_CCM_GUI_Fix.v4.2.3.FP01
Tivoli_SWDEP_AIX_Fix.v4.2.3.FP01.spb	Tivoli_SWDEP_AIX_Fix.v4.2.3.FP01
Tivoli_SWDEP_HP_Fix.v4.2.3.FP01.spb	Tivoli_SWDEP_HP_Fix.v4.2.3.FP01
Tivoli_SWDEP_LINUXPPC_Fix.v4.2.3.FP01.spb	Tivoli_SWDEP_LINUXPPC_Fix.v4.2.3.FP01
Tivoli_SWDEP_LINUX_IX86_Fix.v4.2.3.FP01.spb	Tivoli_SWDEP_LINUX_IX86_Fix.v4.2.3.FP01
Tivoli_SWDEP_LINUX_S390_Fix.v4.2.3.FP01.spb	Tivoli_SWDEP_LINUX_S390_Fix.v4.2.3.FP01
Tivoli_SWDEP_NTAS400_Fix.v4.2.3.FP01.spb	Tivoli_SWDEP_NTAS400_Fix.v4.2.3.FP01
Tivoli_SWDEP_NT_Fix.v4.2.3.FP01.spb	Tivoli_SWDEP_NT_Fix.v4.2.3.FP01
Tivoli_SWDEP_SOLARIS_Fix.v4.2.3.FP01.spb	Tivoli_SWDEP_SOLARIS_Fix.v4.2.3.FP01
Tivoli_SWDEP_WIN95_Fix.v4.2.3.FP01.spb	Tivoli_SWDEP_WIN95_Fix.v4.2.3.FP01
Tivoli_WebUI_Fix.v4.2.3.FP01.spb	Tivoli_WebUI_Fix.v4.2.3.FP01
Tivoli_Web_Gateway_DB_Fix.v4.2.3.FP01.spb	Tivoli_Web_Gateway_DB_Fix.v4.2.3.FP01
Tivoli_Web_Gateway_SRV_Fix.v4.2.3.FP01.spb (*)	Tivoli_Web_Gateway_SRV_Fix.v4.2.3.FP01

(*): With the Tivoli_Web_Gateway_SRV_Fix.v4.2.3.FP01.spb package you can solve the SSL connection problem with Nokia devices. If you do not install this package, the device, after the certificate authentication, connects to TWG using HTTP protocol instead of passing through WebSeal with HTTPS protocol.

Updating the Inventory signatures

The latest software signatures are packaged in fix pack 4.2.3-INV-FP01. After you install the fix pack, the signatures are located in the $BINDIR/../generic/inv/SIGNATURE directory in the SWSIGS.INI file. For more information on how to install these signatures, see the **winvsig** command in the *IBM Tivoli Configuration Manager: User's Guide for Inventory*.

Updating the Inventory schema

The inventory server fix pack component stores in the directory $BINDIR/../generic/inv/SCRIPTS/RDBMS the following scripts:

- inv_*dbvendor*_schema_423_FP01.sql
- h_inv_*dbvendor*_schema_423_FP01.sql
- h_inv_*dbvendor*_patch_mgmt_423_FP01.sql

where:

db_vendor
        Is the shortname for the database

The first script updates the inventory tables, while the second one the historical inventory tables, and the third one the historical patch management tables.

Do not run these scripts if you are working with the patch management SUS configuration and you have applied all the fix pack components except for the patch management one.

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.

Upgrading the Patch Management component

If you installed the Automated Patch Management solution, Version 4.2.3, and you want to use the WSUS configuration, install the patch management fix pack component as described in the updated version of *Patch Management Guide*.

Upgrading plug-ins

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

Activity Planner

If you have installed 4.2.3-APM-FP01, 4.2.3-SWDSRV-FP01, and 4.2.3-INV-FP01 run the following scripts located in the $BINDIR/TME/APM/SCRIPTS directory. You need the APM_Admin Tivoli region authorization role to run them.

- sh reg_swd_plugin.sh -r
- sh reg_inv_plugin.sh -r
- 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 Activity Planner for the Task Library. Run the **wstopapm** and **wstartapm** commands.

Change Manager

If you have installed 4.2.3-CCM-FP01, 4.2.3-SWDSRV-FP01, and 4.2.3-INV-FP01 run the following scripts located in the $BINDIR/TME/CCM/SCRIPTS directory. You need the CCM_Admin Tivoli region authorization role to run them.

- sh reg_swd_plugin.sh -r
- sh reg_invscan_plugin.sh -r

Implementing the concurrent login feature

This section explains how to install, configure, and use the concurrent login feature to prevent the end user from logging in to the workstation during critical distributions.

If you have already installed and configured the login feature with the 4.2.3-TCM-0001 interim fix, you do not need to perform the steps described below.

Installing the concurrent login feature

Before you can install this feature, you must have installed Software Distribution and Activity Planner, as described in *IBM Tivoli Configuration Manager: Planning and Installation Guide*.

To install the concurrent login feature, perform the following steps:

1. Install the **4.2.3-SWDSRV-FP01** Software Distribution patch to update the Software Distribution command line and GUI.
2. Install the **4.2.3-SWDGW-FP01** Software Distribution gateway patch to update Windows endpoints at the next distribution.
3. Install the **4.2.3-APM-FP01** Activity Planner patch to update the Activity Planner GUI.
4. Upgrade the Activity Planner plug-ins, as described in "Upgrading plug-ins" on page 29.
5. Distribute the **Tivoli_login_control_4.2.3.spb** software package to the endpoints.
6. Type the following command to enable the feature on the specified endpoint:

   wep *endpoint_name* set allow_distribution_control on

   where:

   endpoint_name
   > Is the name of the endpoint where the feature is to be enabled.

   Repeat the command for each endpoint where the feature is to be enabled.
7. Download the wdepcem.exe file from the /LoginControl folder to the endpoints.

Configuring the concurrent login feature

After installing the concurrent login feature as described in "Installing the concurrent login feature," you can configure the registry keys created on the endpoints with the **Tivoli_login_control_4.2.3.spb** software package.

The registry keys are created in the following locations within the Registry Editor:

- HKEY_LOCAL_MACHINE\SOFTWARE\Tivoli\SWDnotification
- HKEY_LOCAL_MACHINE\SOFTWARE\Tivoli\SWDnotification\upcall
- HKEY_LOCAL_MACHINE\SOFTWARE\Tivoli\SWDnotification\wmansd

To view and edit the registry keys, use the **wdepcem** command. For more information on this command, see "wdepcem" on page 35.

The following is a list of all the registry keys created on the endpoints:

**Keys located in
HKEY_LOCAL_MACHINE\SOFTWARE\Tivoli\SWDnotification**

IsEnabled
> Specifies whether the concurrent login feature is enabled. Supported values are **1**, which means that the feature is enabled, and **0**, which means that the feature is disabled. The default value is **1**.

TraceLevel
> Specifies the tracing level. Supported values are as follows:

> **0**   Traces are disabled. This is the default value.

> **1**   Standard tracing is enabled.

> **2**   Verbose tracing is enabled.

TracePath
> Specifies the full path and name of the trace files. The default value is: $(system_drive)\SWDnotification.log.

DenyPopupEnabled
> Specifies whether a message must be displayed on the endpoint to notify the user that login is temporarily disabled. Supported values are **1**, which means that the dialog is displayed, and **0** which means that the dialog is not displayed. The default value is **1**.

PopUpTimeout
> Specifies how many seconds the message must be displayed on the endpoint if you set the **DenyPopupEnabled** key to **1**. The default value is **10**.

LoginDeniedTitle
> Defines the title of the dialog box displayed on the endpoint if you set the **DenyPopupEnabled** key to **1**. The default value is SWDNotification.

LoginDeniedMsg
> Defines the text contained in the dialog box displayed on the endpoint if you set the **DenyPopupEnabled** key to **1**. When customizing the message, you can use the \r\n symbols for inserting a carriage return. The default value is: "Distribution in progress\r\nLogon temporarily disabled."

DenyLogonOnPauseError
> Specifies whether the user can be allowed to log in to the workstation if an error occurs during an attempt to pause the distribution. Supported values are **1**, which means the user is not allowed to log in, and **0**, which means the user is allowed to log in. The default value is **1**.

LoginDeniedMsgOnPauseError
> Defines the text contained in the dialog box displayed on the endpoint if the distribution cannot be paused and you set the **DenyLogonOnPauseError** key to **1**. When customizing the message, you can use the \r\n symbols for inserting a carriage return and the $(DIST_ID) variable which is replaced at run time with the distribution ID. The default value is: " The pause failed for distribution $(DIST_ID)\r\n Contact system administrator."

SwitchPopupDesktop

Specifies whether the message displayed on the endpoint if you set the **DenyPopupEnabled** key to **1**, must be shown on a new Windows desktop. Supported values are **0**, which means the default Windows desktop is used, and **1**, which means a new Windows desktop is used. The default value is **1**.

LogoffType

Specifies which type of logoff must be performed. Supported values are as follows

0   Performs a standard logoff. This is the default value.

1   Performs a forced logoff ending all active processes.

2   Performs a logoff ending active and hung processes.

DefaultShutdownAllowdBeforeReset

Defines the number of shutdown operations after which the user is allowed to log in again. This key prevents the user from being irrecoverably logged out of the workstation. The default value is **20**.

CompletionPopupEnabled

Specifies whether a message is displayed on the endpoint to notify the user that the last distribution has completed and login is allowed. Supported values are **0**, which means the message is not displayed, and **1**, which means the message is displayed.

CompletionProgramPath

Specifies the path to the application that manages the message to be displayed if you set the **CompletionPopupEnabled** to **1**. Use this key if you modified the path where wcompmsg.exe is installed or if you want to use a different application for managing the message.

CompletionPopupTitle

Defines the title of the dialog box displayed on the endpoint if you set the **CompletionPopupEnabled** key to **1**. The default value is SWDNotification.

CompletionPopupMsg

Defines the text contained in the dialog box displayed on the endpoint if you set the **CompletionPopupEnabled** key to **1**. When customizing the message, you can use the \n symbol for inserting a carriage return. The default value is: ″Distribution complete\nLogon is now permitted.″

ShutdownPopupEnabled

Specifies whether a message is displayed when you attempt to perform a shutdown during a distribution for which the shutdown has been disabled. You must choose between performing a logoff immediately, performing a restart immediately, or performing a logoff immediately and subsequently a shutdown when the last distribution completes. See also LogoffShutdownString. Supported values are **0**, which means the message is not displayed, and **1**, which means the message is displayed. The default value is **1**.

ShutdownPopupMsg

Defines the text contained in the dialog box displayed on the endpoint if you set the **ShutdownPopupEnabled** key to **1**. When customizing the message, you can use the \n symbol for inserting a carriage return. The default value is: ″The machine will shutdown when the distribution completes.″

Keys located in HKEY_LOCAL_MACHINE\SOFTWARE\Tivoli\SWDnotification\upcall

LCF_BINDIR
Is the fully qualified path to the LCF_BINDIR.

LCF_CACHEDIR
Is the fully qualified path to the LCF_CACHEDIR.

LCF_DATDIR
Is the fully qualified path to the LCF_DATDIR.

UpcallProgram
Is the fully qualified path to the application which communicates with the gateway.

UpcallTimeout
Specifies the timeout in seconds for communicating with the gateway. The default value is **120** seconds.

Keys located in HKEY_LOCAL_MACHINE\SOFTWARE\Tivoli\SWDnotification\wmansd

Title Defines the title of the dialog box displayed on the endpoint if you set the **ShutdownPopupEnabled** key to **1** and the user attempts to perform a shutdown during a distribution for which the shutdown has been disabled. The default value is SWDNotification.

Message
Defines the message contained in the dialog box displayed on the endpoint if you set the **ShutdownPopupEnabled** key to **1** and the user attempts to perform a shutdown during a distribution for which the shutdown has been disabled. When customizing the message, you can use the \n symbol for inserting a carriage return. The default value is: "Please choose one of the following."

Timeout
Specifies a timeout in seconds for choosing between a logoff, a restart, and a logoff and shutdown. If you set the timeout to **0**, the message is not displayed and the default action is performed. Otherwise, the default action is performed after the timeout expires. For more information on the default action, see DefaultAction. The default value is **0**.

LogoffString
Defines the first option displayed in the message to request whether a logoff should be performed. If you select this option, a logoff is performed immediately. The default value is "Logoff".

LogoffShutdownString
Defines the second option displayed in the message to request whether a logoff and a shutdown should be performed. If you select this option, a logoff is performed immediately and a shutdown is performed when the last distribution completes. The default value is "Logoff and shutdown when complete".

RestartString
Defines the third option displayed in the shutdown message to request whether a restart should be performed. If you select this option, a restart is performed immediately. The default value is "Restart".

DefaultAction

Specifies the default action to be performed when the timeout expires or is set to **0**. Supported values are as follows:

1   Performs a logoff immediately.

2   Performs a logoff immediately and a shutdown when the last distribution completes. This is the default value.

3   Performs a restart immediately.

LeftLogonPopupEnabled

Specifies whether a message must be displayed on the endpoint listing the number of logins allowed on the workstation. You can define this key when limited logins are allowed during the distribution. If an error occurs and the distribution cannot be paused, the message is not displayed. Supported values are **0**, which means the message is not displayed, and **1**, which means the message is displayed. The default value is **1**.

LeftLogonPopupMsg

Defines the message contained in the dialog box displayed on the endpoint if you set the **LeftLogonPopupEnabled** key to **1**. When customizing the message, you can use the \n symbol for inserting a carriage return and the $(LEFT_LOGON) variable which is replaced at run time with the number of allowed logins. The default value is: ″The current distribution has been paused\nYou can logon $(LEFT_LOGON) times.″

wdepcem

Displays and configures the registry keys created when the concurrent login feature is installed on the endpoint. It can also unlock a workstation that has been locked by mistake.

Syntax: **wdepcem** [**-r** | **-g** *property* | **-s** *property*]

Options:

-r   Unlocks a workstation that has been locked by mistake.

-g *property*
      Displays the setting defined for the specified registry key.

-s *property*
      Defines a setting for the specified registry key, as follows:

      -e [true | false]
            Specifies whether the concurrent login feature is enabled. Supported values are **true**, which means that the feature is enabled, and **false**, which means that the feature is disabled. The default value is **true**.

      -p [true | false]
            Specifies whether a message must be displayed on the endpoint to notify the user that login is temporarily disabled. Supported values are **true**, which means that the dialog is displayed, and **false** which means that the dialog is not displayed. The default value is **true**.

      -t *timeout*
            Specifies how many seconds the message must be displayed on the endpoint if you set the **-p** option to **true**. The default value is **10**.

      -l *popup_title*
            Defines the title of the dialog box displayed on the endpoint if you set the **-p** option to **true**. The default value is SWDNotification.

      -L *popup_msg*
            Defines the text contained in the dialog box displayed on the endpoint if you set the **-p** option to **true**. The default value is: "Distribution in progress\r\nLogon temporarily disabled."

      -m [true | false]
            Specifies whether the user can be allowed to log in to the workstation if an error occurs during an attempt to pause the distribution. Supported values are **true**, which means the user is not allowed to log in, and **false**, which means the user is allowed to log in. The default value is **true**.

      -M *popup_msg*
            Defines the text contained in the dialog box displayed on the endpoint if the distribution cannot be paused and you set the **-m** option to **true**. When customizing the message, you can use the \r\n symbols for inserting a carriage return and the $(DIST_ID) variable which is replaced at run time with the distribution ID. The default value is: "The pause failed for distribution $(DIST_ID)\r\n Contact the system administrator."

      -x *level* Specifies the tracing level. Supported values are as follows:

            0   Traces are disabled. This is the default value.

1	Standard tracing is enabled.
2	Verbose tracing is enabled.

-y *pathname*
> Specifies the full path and name of the trace files. The default value is: $(system_drive)\SWDnotification.log.

-s [true | false]
> Specifies whether the message displayed on the endpoint if you set the **-p** option to **true**, must be shown on a new Windows desktop. Supported values are **true**, which means a new Windows desktop is used, and **false**, which means the default desktop is used. The default value is **true**.

-d *max_shutdowns*
> Defines the number of shutdown operations after which the user is allowed to log in again. This key prevents the user from being irrecoverably logged out of the workstation. The default value is **20**.

-o [0 | 1 | 2]
> Specifies which type of logoff must be performed. Supported values are as follows:

0	Performs a standard logoff. This is the default value.
1	Performs a forced logoff ending all active processes.
2	Performs a logoff ending also hung processes.

-c [true | false]
> Specifies whether a message is displayed on the endpoint to notify the user that the last distribution has completed and log in is allowed. Supported values are **true**, which means the message is displayed, and **false**, which means the message is not displayed. The default value is **true**.

-b *pathname*
> Specifies the path to the application that manages the message to be displayed if you set the **-c** option to **true**. Use this key if you modified the path where wcompmsg.exe is installed or if you want to use a different application for managing the message.

-u *popup_title*
> Defines the title of the dialog box displayed on the endpoint if you set the **-c** option to **true**. The default value is SWDNotification.

-v *popup_msg*
> Defines the text contained in the dialog box displayed on the endpoint if you set the **-c** option to **true**. When customizing the message, you can use the \r\n symbols for inserting a carriage return. The default value is: "Distribution complete\nLogon is now permitted."

-w [true | false]
> Specifies whether a message is displayed when you attempt to perform a shutdown during a distribution for which the shutdown has been disabled. You must choose between performing a logoff immediately, performing a restart immediately, or performing a logoff immediately and subsequently a shutdown when the last distribution completes. See also the - H option. Supported values

are **true**, which means the message is displayed, and **false**, which means the message is not displayed. The default value is **true**.

-z *shut_popup_msg*

Defines the text contained in the dialog box displayed on the endpoint if you set the **-w** option to **true**. When customizing the message, you can use the \n symbol for inserting a carriage return. The default value is: "The machine will shut down when the last distribution completes."

-B *pathname*

Specifies the fully qualified path to the LCF_BINDIR.

-C *pathname*

Specifies the fully qualified path to the LCF_CACHEDIR.

-D *pathname*

Specifies the fully qualified path to the LCF_DATDIR.

-U *pathname*

Specifies the fully qualified path to the application which communicates with the gateway.

-W *timeout*

Specifies the timeout in seconds for communicating with the gateway. The default value is **120** seconds.

-E *popup_title*

Defines the title of the dialog box displayed on the endpoint if you set the **-w** option to **true** and the user attempts to perform a shutdown during a distribution for which shutdown has been disabled. The default value is SWDNotification.

-F *popup_msg*

Defines the message contained in the dialog box displayed on the endpoint if you set the **-w** option to **true** and the user attempts to perform a shutdown during a distribution for which the shutdown has been disabled. When customizing the message, you can use the \n symbol for inserting a carriage return. The default value is: "Please choose one of the following"

-G *timeout*

Specifies a timeout in seconds for choosing between a logoff, a restart, and a logoff and shutdown. If you set the timeout to **0**, the message is not displayed and the default action is performed. After the timeout expires, the default action is performed. For more information on the default action, see the -J option. The default value is **0**.

-T *logoff_str*

Defines the first option displayed in the message to request whether a logoff should be performed. If you select this option, a logoff is performed immediately. The default value is "Logoff".

-H *logoff_and_shut*

Defines the second option displayed in the message to request whether a logoff and a shutdown should be performed. If you select this option, a logoff is performed immediately and a shutdown is performed when the last distribution completes. The default value is "Logoff & shutdown when complete".

-K *restart_str*

> Defines the third option displayed in the shutdown message to request whether a restart should be performed. If you select this option, a restart is performed immediately. The default value is "Restart".

-J [1 | 2 | 3]

> Specifies the default action to be performed when the timeout expires or is set to 0. Supported values are as follows:

> **1** Performs a logoff immediately.

> **2** Performs a logoff immediately and a shutdown when the last distribution completes. This is the default value.

> **3** Performs a restart immediately.

-P [true | false]

> Specifies whether a message must be displayed on the endpoint listing the number of logins allowed on the workstation. You can define this key when limited logins are allowed during the distribution. Supported values are **true**, which means the message is displayed, and **false**, which means the message is not displayed. The default value is **true**.

-Q *message*

> Defines the message contained in the dialog box displayed on the endpoint if you set the **-P** option to **1**. When customizing the message, you can use the \n symbol for inserting a carriage return and the $(LEFT_LOGON) variable which is replaced at run time with the number of allowed logins. The default value is: "The current distribution has been paused\nYou can logon $(LEFT_LOGON) times."

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

0 Indicates that **wdepcem** completed successfully.

other than zero
> Indicates that **wdepcem** failed due to an error.

Examples:

1. To display the value set for the **-p** option, type the following command:

   wdepcem –g p

2. To set the default action to be performed when the timeout expires so that an immediate logoff is performed, type the following command:

   wdepcem –s J 1

Avoiding concurrent logins during critical distributions

Using the GUI or the command line, you can define a set of software packages for which user login and shutdown operations can be disabled while the distribution is taking place. This feature guarantees that critical distributions are not interrupted. You can also define a maximum number of logins that can be performed during a distribution. If the user logs in, the distribution is paused and restarts after the user logs off.

Using a series of configurable messages, you can notify the user of the distribution taking place on the workstation, list the number of logins allowed, if any, and prompt the user who is trying to perform a shutdown during a distribution for which the shutdown is disabled to choose between logoff options.

In the Software Distribution command line, the **-X {none|first|middle|last|both}**, **-Y** *max_login_allowed*, and **-W** options have been added to the following commands, as described below:

- waccpst
- wcommtsp
- winstsp
- wspmvdata
- wremovsp
- wundosp

-X {none|first|middle|last|both}

> Use this option to define a set of software packages for which user login and shutdown operations can be disabled while the distribution is taking place. If you define a package as **first**, this package is the first in a series for which you can define these options. Define the other packages in the series as **middle** and the last package as **last**. A software package defined as **last** must exist for each software package defined as **first**. If the series consists of just one package, define this package as **both**, which means the software package is both first and last in the series. The default value is **none** which means user login and shutdown operations cannot be disabled.

> **-Y** *max_login_allowed*

>> Use this option to specify whether users can log on to the workstation while a distribution is taking place. This setting can be defined only for software packages defined as **first** or **both**. It applies to software packages defined as **first**, **middle**, **last**, or **both**. Supported values are **0** (no login is allowed), **-1** (an unlimited number of logins is allowed), and any positive integer. If a login is performed while the distribution is taking place, the distribution is paused until the user performs a logoff.

> **-W** Specifies that the user cannot perform a shutdown while a distribution is taking place. If the user attempts to perform a shutdown and the timeout is set to a value other than zero using the **Timeout** key, a dialog box is displayed on the endpoint listing the allowed operations and requesting the user to select one. The user can choose between performing a restart, a logoff, or a logoff and shutdown. The restart and logoff operations are performed immediately, while the shutdown is performed after the last distribution has completed. If the user does not respond to the

dialog within the allotted time, the default action is performed. The default action is logoff and shutdown.

In the Activity Planner and Software Distribution GUI, the Concurrent Login section was added to the panels for the following operations, as described below:

- Accept
- Commit
- Delete
- Install
- Retrieve
- Send
- Remove
- Undo

Type   Define a set of software packages for which user login and shutdown operations can be disabled while the distribution is taking place. If you define a package as **first**, this package is the first in a series for which you can define these options. Define the other packages in the series as **middle** and the last package as **last**. A software package defined as **last** must exist for each software package defined as **first**. If the series consists of just one package, define this package as **both**, which means the software package is both first and last in the series. The default value is **none** which means user login and shutdown operations cannot be disabled.

Max Login Allowed

Specify whether users can log on to the workstation while a distribution is taking place. You can specify this setting only for software packages defined as **first** or **both**. Packages defined as **middle** or **last** inherit the settings defined for the package defined as **first**. Supported values are **0** (no login is allowed), **-1** (an unlimited number of logins is allowed), and any positive integer. If a login is performed while the distribution is taking place, the distribution is paused until the user performs a logoff.

Disable Shutdown

Select this check box to specify that the user cannot perform a shutdown while a distribution is taking place. If the user attempts to perform a shutdown and the timeout is set to a value other than zero using the **Timeout** key, a dialog box is displayed on the endpoint listing the allowed operations and requesting the user to select one. The user can choose between performing a restart, a logoff, or a logoff and a shutdown. The restart and log off operations are performed immediately, while the shutdown is performed after the last distribution has completed. If the user does not respond to the dialog within the allotted time, the default action is performed. The default action is log off and shutdown. You can specify this setting only for software packages defined as **first** or **both**. Packages defined as **middle** or **last** inherit the settings defined for the package defined as **first**.

Dataless packages cannot be paused, therefore you should add them in a series of packages and define them as **middle**.

For more information on the Software Distribution GUI and command line, refer to *IBM Tivoli Configuration Manager: User's Guide for Software Distribution* and *IBM Tivoli Configuration Manager: Reference Manual for Software Distribution*.

Documentation notes

This section contains new information and documentation corrections contained in this fix pack.

Documentation problems and corrections contained in this fix pack

Planning and Installation Guide

This section contains new and updated information for IBM Tivoli Configuration Planning and Installation Guide:

Defect 55431, 55432

In Chapter 3 "Component installation prerequisites", section "Using the Web Gateway component with Tivoli Access Manager", subsection "Installing and Configuring the Java™ Runtime Environment", replace the existing example for Windows operating systems with the following example:

```
cd C:\Program Files\Tivoli\Policy Director\sbin pdjrtecfg -action  \
config -host hostname -java_home drive:%WAS_HOME%\java\jre
-host /<access_manager_server_name>
```

and replace the command to be run on the Web Gateway server to create the SSL configuration file and keystores with the following example:

```
java com.tivoli.mts.SvrSslCfg userName Password pdmgrdHostname \
pdacldHostname pdmgrdPort pdacldPort configuration_file \
keystore_file create
```

where:

userName
> The name of the Access Manager application to create and associate with the SSL communication. The application name must be unique. Other instances of the application, which are running on this or other systems, must each be given a unique name. A distinguished name can be used when an LDAP-based user registry is used with Access Manager.

Password
> The password associated with the master security user.

pdmgrdHostname
> The name of the system where the Access Manager policy server process, ivmgrd, is running.

pdacldHostname
> The name of the system where the Access Manager authorization server process, ivacld, is running. This can be the same system as the policy server.

pdmgrdPort
> The port used for SSL communication with the policy server. The default is 7135.

pdacldPort
> The port used for SSL communication with the authorization server. The default is 7136.

configuration_file

> The URL of the configuration file. The URL must use the **file:///** format. The default is *java_home/PdPerm.properties*. The *PDPerm.properties* and *PdPerm.ks* files must be in the same directory.

keystore_file

> The URL of the keystore file. The URL must use the **file:///** format. The default is *java_home/PdPerm.ks*. The *PDPerm.properties* and *PdPerm.ks* files must be in the same directory.

APAR IY71740

> In Chapter 1. Overview of Configuration Management, add the following information to the Software Distribution component description: You must install the Software Distribution component on the Tivoli server before you can install either the Software Distribution or Software Distribution Gateway component on any managed node in the local Tivoli region.

> In Chapter 1. Overview of Configuration Management, at the end of section IBM Tivoli Configuration Manager Components and Services, delete the following paragraph: You must install these components on the Tivoli server before you can install them on a managed node or before you can install the associated gateway component on a gateway. For example, you must install the Software Distribution component on the Tivoli server before you can install either the Software Distribution or Software Distribution Gateway component on any managed node in the local Tivoli region.

APAR IY75134

> In Chapter 3. Component Installation Prerequisites, add the following note under Table 5 and Table 6:

> **Note:** The index file for the Scalable Collection Service component does not appear in the table because it cannot be upgraded but must be fresh-installed.

APAR IY76046

> In Chapter 5. IBM Tivoli Configuration Manager Installation and Upgrade, section "Custom Server Installation", step 10, add the following information to the `- Directory` description:

> For more details on these files, refer to the *IBM Tivoli Configuration Manager 4.2.3 Patch Management Guide*.

User's Guide for Inventory

This section contains new and updated information for IBM Tivoli Configuration User's Guide for Inventory:

APAR IY76046

> In Chapter 3. Working with Inventory profiles, section "Software patch scan options for PC", add at the end of the section the following paragraph:

> For more details on these files, refer to the *IBM Tivoli Configuration Manager 4.2.3 Patch Management Guide*.

Defect 182301

> In Chapter 4. Distributing Inventory profiles, section "Performing an endpoint initiated scan"', add the following information at the end of the third paragraph:

As software scan options for PC and UNIX, ensure you select **Run the scan** to perform a scan on the endpoint, and **Send the results to the configuration repository** to create the DAT file on the endpoint. If the upload of the results is needed, you can run the **wepscan -s** command.

Defect 179423

In Appendix B "Commands", replace the usage of the **wloadiso** command with the following usage:

wloadiso [-d { 1 | 2 | 3 }] -f *filename* **| -l** *listfilename* and replace the description of the **-f** *DAT file* option with the following two options:

-f *filename*

The name of the .DAT file to be sent to the configuration repository. You can specify more than one .DAT file.

-l *listfilename*

The name of a file containing a list of .DAT files.

APAR IY70039

In Appendix B "Commands", section **wcollect**, replace the description of the -n option with the following text:

-n   Enables a threshold for the number of entries that can be added to the Wan entry Point Collector input and output queue. When the threshold is exceeded, entries are rejected. Entries are added again when the threshold is no longer reached.

Defect 55686, 55847

In section "Scanning disconnected system" replace Step 4, Step 9, and Step 11 with the following:

Step 4:

On the endpoint, locate the zip file (for example `w32-ix86.zip`) in the `$LCFROOT/inv/ISOLATED/common/` directory, and manually copy the file from this directory to the directory on the disconnected system that you created in step 3.

Step 9:

On the disconnected system unzip the zip file, from the directory that you created in Step 3, and run:
```
wepscan -i -n DAT_file_name
```

where:

DAT_file_name

Is the name of the DAT file.

Note: On Solaris, before running the **wepscan** command, set the library path to the local directory. From the local directory run:
```
export LD_LIBRARY_PATH=.:$LD_LIBRARY_PATH
```

Step 11:

Run the **wloadiso** command from the $LCFROOT/inv/ISOLATED/depot directory on the endpoint to send the scan data to the configuration repository. Before running the **wloadiso -f** `file.dat` command, set up the lcf environment to access the shared libraries needed by the command. See **wepscan** for the procedure on how to set the environment.

Defect 55565

If you installed the WSUS Patch Automation solution, in Appendix B "Commands", replace the current usage of the **wsetinvpcsw** command with the following usage:

```
wsetinvpcsw [-b {SCAN | UPDATE | BOTH | NO}]
[-c {QUICK | FULL | MD5 | NONE}] [-f {Y | N}]
[-h {SCAN | UPDATE | BOTH | NO}] [-r {SCAN | UPDATE | BOTH | NO}]
[-s {SCAN | UPDATE | BOTH | NO}] [-x {Y | N}] [-m {Y | N}]
[-d {Y | N} [-n file_ name]] profile_name
```

and add the following entries at the end of the Options list:

-d   Specifies whether the swsigs.txt file must be downloaded to the endpoint. The default value is N, which means that the file is downloaded to the endpoint with every profile distribution. To prevent the file from being downloaded, set the option to Y. You can use the -n option to select a different file to be downloaded.

-n *file_name*

Specifies the name of the file to be downloaded to the endpoint. You can choose one of the following two files:

swsigs.txt

Contains Inventory signatures.

wsusscan.cab

Contains the security policy catalog.

This option can be used only with the -d option.

In Appendix B "Commands", replace the current usage of the **wgetinvpcsw** command with the following usage:

```
wgetinvpcsw [-b] [-c] [-f] [-h] [-r] [-s] [-x] [-m] [-d] profile_name
```

and add the following entry at the end of the Options list:

-d   Specifies whether the swsigs.txt file must be downloaded to the endpoint.

In Appendix B "Commands", replace the current usage of the **wsetinvunixsw** command with the following usage:

```
wsetinvunixsw [-b {SCAN | UPDATE | BOTH | NO}]
[-c {QUICK | FULL | MD5 | NONE}] [-f {Y | N}]
[-p {SCAN | UPDATE | BOTH | NO}]
[-s {SCAN | UPDATE | BOTH | NO}] [-x {Y | N}] [-d {Y | N}] profile_name
```

and add the following entry at the end of the Options list:

-d   Specifies whether the swsigs.txt file must be downloaded to the endpoint. The default value is N, which means that the file is downloaded to the endpoint with every profile distribution. To prevent the file from being downloaded, set the option to Y.

In Appendix B "Commands", replace the current usage of the **wgetinvunixsw** command with the following usage:

```
wgetinvunixsw [-b] [-c] [-f] [-p] [-s] [-x] [-d] profile_name
```

and add the following entry at the end of the Options list:

-d   Specifies whether the swsigs.txt file must be downloaded to the endpoint.

APAR IY76815

In Appendix B ″Commands″, section ″wcancelscan″, replace the description of the Authorization sub-section with the following text: Super and senior.

WSUS Automated Patch Management Solution

If you installed the WSUS Patch Automation solution, replace the mssecure.cab, mbsacli.exe, and ApprovedItems.txt files with the following files everywhere:

Table 22. WSUS patch management files

SUS Files	WSUS Files
mssecure.cab	wsusscan.cab
mbsacli.exe	WindowsUpdateAgent20-x86.exe
ApprovedItems.txt	ApprovedChanges.txt

User's Guide for Deployment Services

Defect 55898

Add at the end of Chapter 4. Troubleshooting, the following section:

APM login failure on Linux

If Activity Planner fails and the following message is displayed

```
AMN0121E Activity Planner initialization failed. Check whether
the Activity Planner user has been created correctly and/or
the user and password maintained by Activity Planner are syncronized
with the corresponding values of the operating system.
```

and the oservlog contains reports similar to the following:

```
2005/09/19 10:50:58 -01: PAM: pam_acct_mgmt failed=User account has expired (13)
2005/09/19 10:50:58 -01: @verify_password: Invalid username or password
2005/09/19 10:50:58 -01: @rconnect:  Login failed for tivapm from host 100007f
```

Go to */etc/pam.d* and edit the oserv file

```
#%PAM-1.0
# Created by etc-tivoli.cfg for DS/Win and JCF login on systems with Pluggable
# Authentication Modules (PAM). Install will not overwrite this file if it
# exists. See the PAM doc for your platform for details on modifying this file.
auth    required        /lib/security/pam_unix.so
```

Add the following line:

```
account required        /lib/security/pam_unix.so
```

APAR IY74288

In Chapter 3. Using the Command Line, section ″Managing Activity Plans″, sub-section ″wapmfltr″, add the **-u** *user@hostname.domain* parameter to the syntax of the **wapmfltr** command.

At the end of the ″Option″ section add the following option description:

-u *user@hostname.domain*

Enables you to specify the owner of the filter you create when you have the APM_View role.

APAR IY66346

In Chapter 1. Using Activity Planner, section Before You Start, modify the sentence:

- RIM_view or RIM_update role, depending on database operation.

as follows:

- RIM_view and RIM_update roles.

In Understanding the Activity Planner Environment sub-section, modify Table 1. Activity Planner roles and operations by adding the RIM_view and RIM_Update roles in all the cells of the **Required roles** column.

Defect 55797, 55826

In Chapter 19 "Using the command line", section "wresgw", replace the existing usage for the **wresgw** discover syntax with the following usage:

```
wresgw discover [-v] [-C resource_gateway_type] endpoint...
```

Change the endpoint description in the Options list as follows:

endpoint

Specifies the endpoint on which the resource gateway is installed.

For the wresgw ls command, lists all known resource gateway types on the endpoint that you specify.

For the wresgw update command, indicates the endpoint for which the object ID or endpoint label is being updated. This option is mandatory.

Add the following options at the end of the Options list:

-f   Discovers all devices on the specified endpoint. If you do not specify this option, the discovery operation returns only devices added since the last discovery operation.

-a   Discovers devices asynchronously. The results of the operation are saved to the discover.log file located in the /work directory. This operation is provided with a distribution ID and you can view its status with the **wmdist** command. For more information on this command, refer to *Tivoli Management Framework Reference Manual*.

APAR IY75060

In Chapter 4 "Troubleshooting", section "Activity Planner Core Trace", add the following information:

The `APM_RPC_MAX_THREADS` environment variable has been added to the APM_core process. This variable sets the maximum number of concurrent remote procedure call threads handled by the dispatcher. The default value is 250.

Reference Manual for Software Distribution

This section contains new and updated information for IBM Tivoli Configuration Reference Manual for Software Distribution:

Feature 55186

In chapter "Editing the software package definition file", section "System actions", add the following text after the "check_disk_space" section:

logoff stanza

To perform a logoff operation on Windows endpoints, use the logoff stanza, the format of which is as follows:

```
logoff
   force = y/n    (default = n)
   force_if_locked = y/n    (default = n)
```

```
              during_install = y/n   (default = n)
              during_commit = y/n   (default = n)
              during_undo = y/n   (default = n)
              during_remove = y/n   (default = n)
          end
```

Table 23. SPD file attribute of the logoff stanza

| Attribute | Comments | | | |
	Values	Required	Default	Stanza
force	The logoff operation is forced also if any applications are currently active on the workstation.			
	String expression	No	**n**	logoff
force_if_locked	The logoff operation is forced if the workstation is locked.			
	String expression	No	**n**	logoff
during_install	The logoff operation is performed during the during_install phase.			
	String expression	No	**n**	logoff
during_commit	The logoff operation is performed during the during_commit phase.			
	String expression	No	**n**	logoff
during_undo	The logoff operation is performed during the during_undo phase.			
	String expression	No	**n**	logoff
during_remove	The logoff operation is performed during the during_remove phase.			
	String expression	No	**n**	logoff

SPD File Example: logoff

The following section shows an example of a software package definition file containing a logoff stanza:

```
'TIVOLI Software Package v4.2.3 - SPDF'

package
  ##
  ## Package attributes
  ##
   logoff
   force = y
   force_if_locked = n
   during_install = n
   during_commit = y
   during_undo = n
   during_remove = n
  end
end
```

APAR IY66515

In Chapter 1. Editing the Software Package Definition File, section Software Package Name and Version , add the following sentence after the first list:

The length of the string that defines the name and version of a software package can vary depending on how you distribute it:

- If you use Activity Planner, the maximum length of the string must be 128 characters. It includes name, delimiter, version (64 characters), and #region name.
- If you do not use Activity Planner, the maximum length of the string must be 230 characters. It includes name, delimiter, and version (64 characters).

User's Guide for Software Distribution

This section contains new and updated information for IBM Tivoli Configuration User's Guide for Software Distribution:

APAR IY73165

> In chapter 11 "Configuring a Network Topology", section "Scenario 3: Distributing from a Source Host through Repeater Depots" remove the following sentence:

> However, do not use depots for extremely large distributions.

APAR IY73289

> In chapter 15 "Troubleshooting", section "Hints and tips", add the following entry at the end of the list:

> **Error while generating a software package using Autopack**

> During the creation of the first Autopack snapshot, some system resources might be included in the snapshot. This might cause a failure when Autopack generates the software package. If the creation of the software package fails with one or both of the following error messages:
>
> DISSP6018E Failed to build *file_name*
>
> DISSE0282E Error compressing the file *file_name* in the Software Package Block.
>
> generate the software package again excluding the files listed in the error messages, as explained in "Creating the first snapshot" in Chapter 8.

APAR IY74801:

> In Chapter 15 "Troubleshooting", section "Base Configuration Information on the Endpoint", add to table 17 "Directory assignments in swdis.ini file" the following key and its description:

Table 24. Directory assignments in swdis.ini file

Key	Description
resinit_one_reboot	Defines the endpoint behavior in processing software packages. If you change the default value resinit_one_reboot=y and set it to resinit_one_reboot=n, the packages are processed one by one, and if a package requires a reboot, the endpoint is rebooted immediately.

Defect 55498

> Add the following section at the end of the Chapter 15. Troubleshooting:

> **Using the Save option of the Software Package Editor**Software Package Editor is unable to save a software package on an AIX endpoint that has Software Package Editor Version 4.2.3 and fix pack 1 installed. No error message is displayed. The workaround is to select a file between those displayed in the panel. Then the **Save** option works properly. This problem is a known issue of JRE 1.3.1.

Database Schema Reference

If you install the Patch Management fix pack component, see the updated version of the *Patch Management Guide* to see the new patch management tables and views.

Patch Management Guide (for the SUS configuration)

This section contains new and updated information for IBM Tivoli Configuration Patch Management Guide:

Feature 55260

In chapter 6 "Automated patch management command line", in the description of the **wseccfg** command, add the following parameter to the list under the **-s** option:

workflow_activities

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

sync Performs all operations in the workflows without creating software packages and plans.

preparation

Creates software packages and plans without performing any other operation.

all Performs all operations contained in the workflows. This is the default value.

Defect 53932

In chapter 6 "Automated patch management command line", in the description of the **wseccfg** command, add the following parameter to the list under the **-s** option:

catalog_proxy_enabled

Enables or disables proxy support. You can use an HTTP proxy to access the Microsoft Web site, or your local HTTP server where the mssecure.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 component" on page 29.

Defect 55470

In chapter 7 "Troubleshooting", section "Other common problems", add the following entry at the end of the section:

The activity plan fails on targets deleted from the Tivoli database

Deleting endpoints from the Tivoli database does not delete those endpoints from the configuration repository. This might cause the activity plan to fail on the deleted endpoints because targets for the workflow are defined based on the information in the configuration repository.

To prevent this problem, after deleting the endpoints using the **wdelep** command, run the **winvrmnode** command to remove hardware and software scan information from the configuration repository. For more information on these commands refer to *Tivoli Management Framework: Reference Manual* and *IBM Tivoli Configuration Manager: User's Guide for Inventory*.

Defect 55340

In chapter 7 "Troubleshooting", section "Other common problems", add the following entry at the end of the section:

SUS server synchronization problem

Cause: If you work with the SUS server, during the SUS server synchronization on the Microsoft web site, the following error message `INVCC0264E No files to transfer` is displayed.

Solution: To avoid the problem you can perform one of the following tasks:

- Run a reinit to reset the information stored in the Automation Server database. Using this workaround, all the customizations set during the installation are lost.
- Open the `console.log` file and check for which patch the **wtransfer** command has failed. Manually remove the patch from the database.

Defect 55799

In chapter 7 "Troubleshooting", section "Other common problems", add the following entry at the end of the section:

Cause: ITCM 4.2.3 plus interim fix 0001. If you set `delete_plans=yes` in the patch management configuration and run the workflow when there are no entries in the APM database, the following error message is logged in the execution log of the workflow: ERROR: Command >wlstpln< failed.

Solution: The process completed successfully. Ignore the error message.

Defect 55832

In "Chapter 5. Patch Management Command Line", section "wsecgensp", change the **RUR** *lang* option into **RURU** and add **HEEN** (hebrew enabled) to the list of *lang* option values.

Messages and Codes

This section contains new and updated information for IBM Tivoli Configuration Manager Messages and Codes:

Defect 55666

CMYSE0265E	You cannot create the software package because the SWD-Inventory integration is currently disabled.

Explanation: The command you are using requires integration with Inventory.

System action: The operation failed.

Operator response: If inventory integration is required, use the **wswdmgr** software distribution command and the **wsetinvswd** Inventory command to enable integration. See: *IBM Tivoli Configuration Manager: Reference Manual for Software Distribution*, SC23-4712 and *IBM Tivoli Configuration Manager: User's Guide for Inventory*, SC23-4713 for more information.

Defect 55824

DISSE0624E	An error occurred contacting the managed node `*managed node*`. Make sure the managed node is defined as a gateway or stand-alone repeater and is working properly.

Explanation: See message.

System action: The install operation failed.

Operator response: Ensure you defined the source host as a Tivoli gateway or a repeater. Check that the Tivoli gateway or the repeater is running. See the **wrpt** or **wgateway** commands in the *Tivoli Management Framework: Reference Manual*, GC32-0806.

Software Package Editor online help

This section contains new information for the Software Package Editor online help:

Feature 55186

The following is the help panel for the Logoff Properties dialog box:

Use this dialog box to specify whether you want a logoff operation to be performed on Windows endpoints and to define the settings for the logoff operation. You can select one or more of the following options:

Logoff during install

The logoff operation is performed during the during_install phase.

Logoff during undo

The logoff operation is performed during the during_undo phase.

Logoff during remove
> The logoff operation is performed during the during_remove phase.

Logoff during commit
> The logoff operation is performed during the during_commit phase.

Force The logoff operation is forced also if any applications are currently active on the workstation.

Force if locked
> The logoff operation is forced if the workstation is locked.

For more information on defining conditions, see the Conditions help panel.

Defect 55461
> The **Maintain existing value** check box has been added to the Add Directory Properties and Add File Properties dialogs. The following is the help panel for this check box:
>
> Select this check box to maintain the file or directory access attributes and the ownership if the file or directory already exists on the target. If the file or directory does not exist, the check box selection has no effect, and the default value (**Use system value** check box), or the ones that you selected, are assumed.

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.

IBM

Program Number: 5724-C06