

IBM Tivoli Configuration Manager



Readme File for Fix Pack 2 - PTF U806551

Version 4.2.3

Note

Before using this information and the product it supports, read the information in "Notices" on page 77.

First Edition, June 2006

This edition applies to fix pack 2 (PTF U806551) for version 4, release 2, modification level 3 of IBM Tivoli Configuration Manager (program number 5724-C06)

© Copyright International Business Machines Corporation 2003, 2006. All rights reserved.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Tables	v
-------------------------	----------

IBM Tivoli Configuration Manager 4.2.3 ReadMe File for Fix Pack 4.2.3-TCM-FP02 (PTF U806551)	1
---	----------

About this release	1
CD-ROM structure	1
Enhancements	2
New in this fix pack	2
New features in the previous fix packs and interim fixes	5
Prerequisites	10
Product fix history	10
Fixes contained in this fix pack	10
APARs and internal defects fixed for Inventory	11
APARs and internal defects fixed for Scalable Collection Service	17
APARs and internal defects fixed for Software Distribution	17
APARs and internal defects fixed for Activity Planner	27
APARs and internal defects fixed for Change Manager	30
APARs and internal defects fixed for the Web Interface	30
APARs and internal defects fixed for the Resource Manager	30
APARs and internal defects fixed for Pristine Manager	30
APARs and internal defects fixed for Patch Management	30
Fixes contained in previous fix packs and interim fixes	31
Limitations	35
Installation	36
Hardware and software requirements	36
Supported platforms	36
System requirements	37
Upgrading large environments	37
Traditional fix pack installation methods	37
Installing fix packs using ISMP	38
Installing fix packs using the Tivoli desktop	39
Installing fix packs using the CLI	39
wpatch command	39
winstall command	40
Installing fix packs using SIS	41
Software package block (SPB) fix pack installation for GUI components	42
SPB Patch Installer	45
Software Distribution server command	45
Software Distribution disconnected command	46
Software package block fix packs	46
Updating the inventory schema	47
Updating the inventory queries	48
Updating the Inventory signatures and packages	48
Creating the Active Directory schema	48
Upgrading the Patch Management component	49
Upgrading plug-ins	49
Implementing the concurrent login feature	49
Installing the concurrent login feature	49
Configuring the concurrent login feature	50
wdepcem	55
Avoiding concurrent logins during critical distributions	59
Implementing the activity plan group management feature	61
Preparing to use the tool	61
Creating a group of activity plans	62
Submitting and tracking an activity plan group	63

Documentation notes	63
Documentation problems and corrections contained in this fix pack	63
Planning and Installation Guide	63
User's Guide for Inventory	64
User's Guide for Deployment Services	64
Reference Manual for Software Distribution	64
User's Guide for Software Distribution	65
User's Guide for Operating System Imaging Solution	65
Database Schema Reference	66
Patch Management Guide (for the SUS configuration)	66
Messages and Codes	66
Software Package Editor online help	66
Man page missing updates	66
Documentation problems and corrections contained in previous fix packs	67
Planning and Installation Guide	67
User's Guide for Inventory	68
User's Guide for Deployment Services	69
Reference Manual for Software Distribution	70
User's Guide for Software Distribution	72
Database Schema Reference	72
Patch Management Guide (for the SUS configuration)	72
Messages and Codes	74
Software Package Editor online help	74
Notices	77
Trademarks	78

Tables

1. IBM Tivoli Configuration Manager, Version 4.2.3 Fix Pack 2 CD 1	1	20. Software Distribution APARs included from 4.2.3-SWDSRV-F1P2 4.2.3-SWDGW-F1P2 4.2.3-SWDJPS-F1P2 and 4.2.3-SWDEP-F1P2 . . .	34
2. IBM Tivoli Configuration Manager, Version 4.2.3 Fix Pack 2 CD 2	2	21. APARs and internal defects for Activity Planner included from 4.2.3-APM-0001 . . .	34
3. Customer enhancement request references	2	22. APARs and internal defects for Activity Planner included from 4.2.3-APM-FP01 . . .	34
4. Customer enhancement request references	5	23. Activity Planner APARs included from 4.2.3-APM-F1P1	34
5. Fixes included in this fix pack	10	24. Activity Planner APARs included from 4.2.3-APM-F1P2	34
6. APARs and internal defects for Inventory	11	25. APARs and internal defects for Change Manager included from 4.2.3-CCM-0001 . . .	35
7. APARs and internal defects for the Scalable Collection Service component	17	26. APARs and internal defects for Web interface included from 4.2.3-WEB-0001	35
8. APARs and internal defects for Software Distribution	17	27. APARs and internal defects for Web Interface included from 4.2.3-WEB-FP01	35
9. APARs and internal defects for Activity Planner	27	28. APARs and internal defects for Resource Manager included from 4.2.3-TRMSRV-FP01 . . .	35
10. APARs and internal defects for Patch Management included from 4.2.3-PMG-FP02 . . .	30	29. APARs and internal defects for Pristine Manager included from 4.2.3-PRI-0001 . . .	35
11. APARs and internal defects for Inventory included from 4.2.3-INV-0001 and 4.2.3-INVGW-0001	31	30. APARs and internal defects for Patch Management included from 4.2.3-PMG-0001 . . .	35
12. APARs and internal defects for Inventory included from 4.2.3-INV-FP01	32	31. APARs and internal defects for Patch Management included from 4.2.3-PMG-FP01 . . .	35
13. Inventory APARs included from 4.2.3-INV-0006 and 4.2.3-INVGW-0006	32	32. APARs and internal defects for Directory Query included from 4.2.3-QDY-0001	35
14. Inventory APARs included from 4.2.3-INV-0007 and 4.2.3-INVGW-0007	32	33. Space requirements for the License Management Extension	37
15. APARs and internal defects for Scalable Collection Service included from 4.2.3-CLL-0001	32	34. IND files included in this fix pack	40
16. Scalable Collection Service APARs included from 4.2.3-CLL-0002	32	35. IND files included in this fix pack	40
17. APARs and internal defects for Software Distribution included from 4.2.3-SWDSRV-0001, 4.2.3-SWDGW-0001, 4.2.3-SWDJPS-0001, and 4.2.3-SWDEP-0001 . . .	32	36. Default variables defined in SPB fix packs	42
18. APARs and internal defects for Software Distribution included from 4.2.3-SWDSRV-FP01, 4.2.3-SWDGW-FP01, 4.2.3-SWDJPS-FP01, and 4.2.3-SWDEP-FP01 . . .	33	37. Names of SPB files and software profiles	46
19. Software Distribution APARs included from 4.2.3-SWDSRV-F1P1, 4.2.3-SWDGW-F1P1 4.2.3-SWDJPS-F1P1, and 4.2.3-SWDEP-F1P1 . . .	33	38. WSUS patch management files	69
		39. SPD file attribute of the logoff stanza	71
		40. Directory assignments in swdis.ini file	72

IBM Tivoli Configuration Manager 4.2.3 ReadMe File for Fix Pack 4.2.3-TCM-FP02 (PTF U806551)

This readme file provides important information about Fix Pack 2 (PTF U806551) 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”
- “Enhancements” on page 2
- “Prerequisites” on page 10
- “Product fix history” on page 10
- “Limitations” on page 35

CD-ROM structure

IBM Tivoli Configuration Manager, Version 4.2.3 Fix Pack 2 includes *two* CD-ROMs as detailed in the following tables:

Table 1. IBM Tivoli Configuration Manager, Version 4.2.3 Fix Pack 2 CD 1

Directory or path	Contents
/xml	The XML file to be used by the ISMP installation program.
/docs	Readme file.
/CIT_SPB	Software package block (SPB) files used to upgrade the CIT component to version 2.2.1.
/images/AD_INTEGRATION	Images required for Microsoft® Active Directory integration.
/images/EXTENSION	Images required for the license management extension
/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, Directory Query, and Web User Interface fix pack.
/images/SWD/L10N/	Images required to install the national language support fix pack for Software Distribution.
/images/INVENTORY/L10N/	Images required to install the national language support fix pack for inventory.
/images/REMBO	Images required to install Image Management Services.

Table 2. IBM Tivoli Configuration Manager, Version 4.2.3 Fix Pack 2 CD 2

Directory or path	Contents
/LoginControl	Software package block (SPB) and executable files used to implement the concurrent login feature. For more information on this feature, see "Enhancements."
/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
/apm_reporting_tool	Files to implement the Activity plan group creation, submission, and tracking. For more information, see "Implementing the activity plan group management feature" on page 61.
/tpm_install	Files to implement an improved installation for Automation Server. To use the improved installation, in the installation image that you have copied from the Pre-requisite Software Installer for Automation Server CD. 2, replace the files in the /tpm_install directory with these files. For more information, see <i>IBM Tivoli Configuration Manager Patch Management Guide</i> .

Enhancements

This section contains a cumulative list of enhancements introduced in the previous fix packs and interim fixes and in the current fix pack.

- "New in this fix pack"
- "New features in the previous fix packs and interim fixes" on page 5

New in this fix pack

The following enhancements have been introduced in this fix pack:

Table 3. Customer enhancement request references

	Enhancement	Reference
New features	Tivoli Configuration Manager license management extension	
	Patch management extension	
	Active Directory integration	
New agent support	Solaris x86 support	
APM	Search facility for saved activity plans	MR124044922
	Activity plan group creation, submission, and tracking	
	Immediate start for unique targets in conditioned activities	
	Image management services integration (Rembo)	

Table 3. Customer enhancement request references (continued)

	Enhancement	Reference
Inventory	Signature management improvement	MR0102021824
	Improved locale information management	MR0818036425 MR0708046050
	Correlation of software recognition data	M50408055916
	Windows® service information available on Inventory database	MR022103576
	Dynamic logical partitioning (LPAR) information on processor allocated on partitions	MR0216064754
	64-bit support for Inventory operations.	
	Wild card matching	
CCM	Stop on failure check box	

Tivoli Configuration Manager license management extension

You can use the Configuration Manager license management extension to provide license management facilities. For details see *IBM Tivoli Configuration Manager: License Management Extension*.

Patch Management extension

The solution manages Microsoft patches, service packs, and update rollups for the following operating systems and applications:

- Windows 2000 Professional SP™ 3 or later
- Windows 2000 Server SP 3 or later
- Windows 2000 Advanced Server SP 3 or later
- Windows XP Professional
- Windows XP Home Edition
- Windows 2003 Server Standard Edition
- Windows 2003 Server Enterprise Edition
- Windows 2003 Server Web Edition
- Internet Explorer 5.01 or later
- Media Player 6.4 or later
- Exchange 2000 Server
- Exchange Server 2003
- Microsoft Office 2000
- Microsoft Office XP
- Microsoft Office 2003

For details, see *IBM Tivoli Configuration Manager Patch Management Guide*.

Active Directory integration

IBM Tivoli Configuration Manager provides the capability of merging Active Directory and endpoint information into a relational database. See *Tivoli Monitoring: Active Directory Agent* for more information.

Solaris x86 support

Tivoli Configuration Manager is supported on Tivoli Management Framework 4.1.1 endpoints running Solaris 8, 9, 10 for x86 architecture, in particular Solaris 10 for AMD Opteron processor.

Search facilities for saved activity plans

A dynamic search has been added to group saved plans.

Activity plan group creation, submission, and tracking

This feature introduces a tool that manages groups of activity plans as a single entity. A script is used to create the group of activity plans and assign a name to the group. A further script is then scheduled as a repeating job to first submit the group of plans and then produce HTML format reports of its progress by querying the APM and MDIST2 databases. See “Implementing the activity plan group management feature” on page 61 for instructions about using this tool.

Immediate start for unique targets in conditioned activities

With this feature you can add a new submission parameter to the Activity Planner. When submitting a plan, it is now possible to enable the Activity Planner server to evaluate all the conditioned activities of a plan, as soon as the plan is submitted. In this way if a conditioned activity has a target, which is not contained in a conditioning activity, the operation for that target starts immediately. One limitation is that a plan with at least one activity, having the option `target computation at activity execution set`, cannot be submitted if this feature is enabled.

To enable this feature from the Activity Planner command line, run the **wsubpln** command in the following way:

```
wsubpln -r plan_name -Dpre_eval_conditions=true
```

To enable this feature from the Activity Planner GUI, the **Pre-evaluate conditions at plan submission** check box has been added to the **Plan Submission Parameters** panel.

To enable this feature from the Change Manager command line, specify the **-e** option when running the **wsyncrmod** command, or select the **Pre evaluate conditions at plan submission** check box which has been added to the **Select activity plan name** panel.

Image management services integration

Integration of Rembo Autodeploy, build level 4.0.034.16, into Configuration Manager provides services for deploying operation system images in Windows environments. See *IBM Tivoli Configuration Manager: Image Management Services*

Signature management improvement

To allow a more accurate software scan, Inventory has been modified to use complex signatures and a new catalog including not only files, but registry keys, mixed and extended signatures. See *IBM Tivoli Configuration Manager: User's Guide for Inventory*

Improved locale information management

With this feature the Inventory scan distinguishes language specific operating system information for Windows operating systems. The mixed language environment is supported. See *IBM Tivoli Configuration Manager: User's Guide for Inventory*.

Correlation of software recognition data

Enhancement of the Inventory signature scan to retrieve the path for file signatures and store them in the database. This enhancement enables the scan to identify and differentiate between multiple instances of a signature on the same endpoint. See *IBM Tivoli Configuration Manager: User's Guide for Inventory*.

Windows service information

Information on the services present on a Windows workstation is added to the set of information that Inventory can collect. See *IBM Tivoli Configuration Manager: User's Guide for Inventory*.

Dynamic logical partitioning (LPAR) information on processor allocated on partitions

In environments that have logical partitions, Inventory can collect LPAR information. The operating systems on which LPAR information can be discovered are the following:

- AIX®, version 5.3 on P5
- Red Hat Enterprise Linux® Advanced Server, version 4.0 on PowerPC® iSeries™
- SuSE Linux Enterprise Server, version 9 on PowerPC iSeries
- HP-UX, version 11.11 on HP9000
- Sun Solaris Operating Environment, version 10 on Sun SPARC

Stop on failure check box

With this feature you can soften the check performed by Change Manager on each ex-requisite dependency, related to a Software Distribution element, to avoid a failure in the synchronization process, if the condition is not met on one of the target machines. Using this feature you can control the Change Manager behavior when evaluating the dependency. The **Stop on failure** check box has been added to Change Manager to activate the feature.

To enable this feature, perform one of the following actions:

- Right-click the **Dependencies** pane of the **Software Distribution element** panel. Select the **Software Distribution Ex-requisite** dependency type from the **Add** menu. By default, the **Stop on failure** check box is selected and active, to maintain compatibility with the previous fix pack level.
- Select **Software Distribution element** from the **Add** menu. The **Software Distribution element** panel is displayed. Click the **Distribution Options** button to display the **Distribution Options** panel. By default, the **Stop on failure** check box is greyed out. It becomes active after adding a Software Distribution ex-requisite dependency to the Software Distribution element specified.
- From the **Edit** menu, select **Create Reference Model**. The **Properties** panel is displayed. By default, the **Stop on failure** check box is greyed out. It becomes active after adding a Software Distribution element, which contains a Software Distribution ex-requisite dependency.

New features in the previous fix packs and interim fixes

The following enhancements were introduced in the previous fix pack and interim fixes:

Table 4. Customer enhancement request references

Description	Feature
Cancel as preferred final status for a plan	56137
Emergency patch management	56053
Patch Management deployment paradigm	
Enable Move Data to retrieve AS/400® spool file	56336
Enabling proxy support for the SUS Patch Management solution	

Table 4. Customer enhancement request references (continued)

Description	Feature
Avoiding concurrent logins during critical distributions	54613
Performing the logoff operation on Windows endpoints	55186
Displaying the .jar files version	55204
Displaying the patch level for the Activity Plan Editor and Activity Plan Monitor	55205
Completing workflows separately	55260
Performing patch management using WSUS	55317
Maintaining the access attributes of already existing files and directories on a UNIX® target, a new attribute (preserve_unix) is available.	55359
New 32-bit MRMBIOS.EXE	180357
Running a program before the reboot of a commit	55409
Managing software packages	55487
Working with the Software Distribution Endpoint Notification dialog	55522
Emergency patch management	56053
Patch Management deployment paradigm	
Enable Move Data to retrieve AS/400 spool file	56336

Cancel as preferred final status for a plan - Feature 56137

Before submitting a plan, you can define its final status to Cancel if any of the plan activities have been cancelled and the others are successful, either by selecting **Set Cancel as preferred final status** in the General page of the **Plan Submission Parameters** notebook or by specifying `-Dis_cancel_preferred=y` in the **wsubpln** command.

Emergency patch management - Feature 56053

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

Patch Management deployment paradigm - Feature 56053

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

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

With this feature the Data Moving Service in an OS/400® environment has been extended. You can now move OS/400 spool files from an OS/400 system to a Windows or UNIX target. Target systems can be endpoints or

managed nodes. To differentiate the spooled files from the OS/400 native files, when running the **wspmvdata** command, specify the path name using the following format:

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

Ensure that Job Number is not preceded by a slash.

As an example see the following command:

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

Where:

swd400

Is the OS/400 host name.

intermesoli

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

sp:028421/qtivoli/qlcfd/1

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

/targetdir

Is the destination path on the target system.

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

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

JobNumber.JobUser.JobName.SpooledFileNumber.SpooledFileName

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

Notes:

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

endpointname_distributionID_timestamp

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

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 49.

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 63.

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 63.

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.

Prerequisites

IBM Tivoli Configuration Manager, Version 4.2.3 Fix Pack 2 requires the following Tivoli Management Framework versions and fixes:

- Tivoli Management Framework, Version 4.1.1 plus fix pack 4 containing the following interim fixes:
 - 4.1.1-LCF-0028 to be installed on the Tivoli gateways.
 - 4.1.1-TMF-0055 to be installed on the managed nodes with JRIM and JCF components installed.
 - 4.1.1-TMF-0058 to be installed on Tivoli servers, managed nodes, and gateways.
- 4.1.1-LCF-0024 to enable the AMD64 and IA64 support.
- 4.1.1-LCF-0032 to enable Solaris 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 fix packs and interim fixes” on page 31

Fixes contained in this fix pack

Table 5 lists the fixes included in this fix pack:

Table 5. Fixes included in this fix pack

Fix pack	Component/Service
4.2.3-INV-FP02	Inventory, Version 4.2.3
4.2.3-INVGW-FP02	Inventory Gateway, Version 4.2.3
4.2.3-CLL-FP02	Scalable Collection Service, Version 4.2.3
4.2.3-SWDSRV-FP02	Software Distribution, Version 4.2.3
4.2.3-SWDGW-FP02	Software Distribution Gateway, Version 4.2.3
4.2.3-SWDJPS-FP02	Software Distribution Software Package Editor, Version 4.2.3
4.2.3-APM-FP02	Activity Planner, Version 4.2.3
4.2.3-CCM-FP02	Change Manager, Version 4.2.3
4.2.3-WEB-FP02	Web Interface, Version 4.2.3
4.2.3-TRMSRV-FP02	Resource Manager, Version 4.2.3
4.2.3-TRMGW-FP02	Resource Manager Gateway, Version 4.2.3
4.2.3-PMSRV-FP02	Pristine Manager, Version 4.2.3
4.2.3-PMG-FP02	Patch Management, Version 4.2.3
4.2.3-DQY-FP02	Directory Query, Version 4.2.3

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

Table 6. APARs and internal defects for Inventory

Inventory, Version 4.2.3, 4.2.3-INV-FP02 and 4.2.3-INVGUI-FP02				
IY77378	IY78108	IY78940	IY79236	IY79372
IY80066	IY80608	IY80625	IY80837	IY80912
IY81297	IY81359	IY81437	IY81772	IY81879
IY82061	IY82415	IY82479	IY82635	IY82964
IY83074	IY82977	IY83087	IY83181	IY83338
IY84170	IY84708	IY84735	IY84736	IY84739
IY84876	IY85317	IY85496		

APAR IY77378

Abstract:

INV000 folders left in data handler runtime directory after APM notification

Error Description:

Using Activity Planner to distribute Inventory profiles, after the scan the INV000 folders in the data handler runtime directory are not deleted. Submitting a scan outside of Activity Planner works correctly.

APAR IY78108

Abstract:

Inventory GUI not opened due to a NOT_FOUND error in odstat

Error Description:

The Inventory GUI on UNIX cannot be opened due to a NOT_FOUND error in the odstat. The problem might occur when the Framework WD_DESKTOP_HOST variable contains the fully qualified hostname of the local workstation, and there is no managed node with this fully qualified hostname in the odlist output. The workaround consists of adding a short hostname in the odadmin odlist for the affected managed node.

APAR IY78940

Abstract:

Inventory GUI does not open with a non-administrative user

Error Description:

After installing the Tivoli Desktop and the Inventory GUI component on an Windows machine, if you log on as a non-administrative user, the Inventory GUI does not open and the *InvGuiDebug.log* is not written. This error does not occur if you log on as an Administrator.

APAR IY79236

Abstract:

Data is not complete for the package_ers field in the native_sware table

Error Description:

In the nativ_sware query output, the package_ers field is incomplete. The data is being truncated to less than 32 characters, even though the field is defined as string with a length of 128.

APAR IY79372

Abstract:

Inv_cb_meths process core dumps on HP-UX when it detects a corrupted CTOC

Error Description:

On HP-UX platforms, a core dump occurred when the inv_cb_meths process detected a corrupted CTOC.

APAR IY80066

Abstract:

wscanner.exe crashes if the serial number contains special characters.

Error Description:

When the hardware scan is performed on some HP laptops, it crashes because it interprets serial numbers that contain special characters as corrupt. When the fix is applied, the scan does not crash even if the serial number is corrupt.

APAR IY80608

Abstract:

The script for creating inventory tables failed on MVS™.

Error Description:

When the configuration repository is installed on a DB2® MVS RDBMS, the winvrnode command generates the SQL error:

SQL0540N The definition of table "DB2TVUSR.SYNCDM_CON_PX" is incomplete because it lacks a primary index or a required unique index.

APAR IY80625

Abstract:

Custom scan hanging

Error Description:

When the endpoint timeout expires, a new inv_config_ep_meth is spawned. So if a custom script hangs, many inv_config_ep_meth methods will run in parallel on one endpoint and this can have an impact on performance.

APAR IY80837

Abstract:

Software scans very slow to write to database.

Error Description:

Running any software scan takes too long. The rim.log file contains a trace entry about the problem.

APAR IY80912

Abstract:

The h_inv_db2_schema_423_fp01.sql does not update the SCHEMA_VERS table.

Error Description:

The INV SQL script, provided with Tivoli Configuration Manager, version

4.2.3, FP01 to update schema with historical data, does not update the SCHEMA_VERS table. This problem occurs for all supported databases.

APAR IY81297

Abstract:

The UNMATCHED_FILES AND FILE_DESC tables are not populated by the software scan.

Error Description:

After upgrading to Tivoli Configuration Manager, version 4.2.2 base, the software scan does not populated the UNMATCHED_FILES and FILE_DESC tables when MS SQL is being used.

APAR IY81359

Abstract:

Memory problem caused by inv_rcv_meths

Error Description:

If multiple .DAT files are uploaded incorrectly from an isolated machine to the *inv/ISOLATED/depot* directory, a trailing *0x0A* is added at the end of each file, and the command **wloadiso -f a.dat b.dat c.dat** causes a crash due to a memory fault. This problem does not occur if the files are uploaded one by one through a list.

APAR IY81437

Abstract:

Create signatures for Tivoli Configuration Manager.

Error Description:

The signature files *INV422.SIG / INV423.SIG* and *INV422GW.SIG / INV423GW.SIG* are not installed with versions 4.2.2 and 4.2.3, making it impossible to define signatures for these versions of Configuration Manager.

APAR IY81772

Abstract:

Insert fails for the H_PM_PRODUCT_INFO table when the historical feature is enabled.

Error Description:

When the **h_inv_db_patch_mgmt.sql** and **h_db_schema.sql** scripts (where *db* represents the database type, for example *db2*) have been run to enable historical tracking for inventory patch management, checking the scan for patches information in the inventory scan options causes rim errors writing to the database

APAR IY81879

Abstract:

H_SYS_INSTANCE.TME_OBJECT_LABEL not updated if endpoint renamed

Error Description:

If an endpoint is renamed using the command **wep oldlabel set_label newlabel**, re-scanning the endpoint does not change the *tme_object_label* in H_SYS_INSTANCE.

APAR IY82061

Abstract:

mrmmbios.exe ends with error when BIOS contains special characters

Error Description:

On a Windows machine, where a BIOS field contains characters between 0x00 and 0x20, the *mrmmbios.exe* ends with an error.

APAR IY82415

Abstract:

Expired inventory activity remains started.

Error Description:

If the user who submits an activity plan that includes expired inventory activities does not have a senior role the submission fails and the *mcollect.log* file shows that an error occurred when sending a report to the APM because of insufficient authorization.

APAR IY82479

Abstract:

Creation of tables fails with the message "Name too long"

Error Description:

The *inv_db2_mvs_custom_421_FP03.sql* includes two table names that are longer than 18 characters: *TMP_INST_SMBIOS_DATA* and *TMP1_INST_SMBIOS_DATA*. The maximum length for table names on MVS is 18 characters. The table names have been changed to *TMP_I_SMBIOS_DATA* and *TMP1_I_SMBIOS_DATA*.

APAR IY82635

Abstract:

INV_STAT_METHS process on AIX - Memory Leak - core dumps.

Error Description:

The *inv_stat_meths* process has a memory leak. It continues to consume a large amount of memory until it crashes with signal 11. This happens particularly when many scans are pending.

APAR IY82924

Abstract:

If notification type is FAIL, Data Handler does not send reports to APM

Error Description:

If the *InventoryConfig* profile has defined FAIL as notification type and the profile is distributed through the Activity Planner Monitor, the Data Handler does not send the report to the Activity Planner Monitor, if the distribution succeeds, because Data Handler sends to the Activity Planner Monitor only failed reports.

APAR IY82977

Abstract:

MATCHED_SWARE is not updated with a signature package after installation of a software package.

Error Description:

After installation of a software package including signatures, the MATCHED_SWARE table is not updated.

APAR IY83074**Abstract:**

The **Replace** option does not work in the custom scan if there are no entries to be inserted.

Error Description:

If the Replace option is used for the custom scan, all existing entries in the custom table for the scanned endpoint should be removed and replaced with the new entries. If there are no new entries to insert, the existing entries should be removed, but this does not happen.

APAR IY83087**Abstract:**

Memory leak in the **wwaitscan** command

Error Description:

If one target of the distribution is switched off, the **wwaitscan -i scan_id** command does not exit until the target is switched on, or the distribution deadline expires, or the scan is cancelled using the **wcancelscan** command.

APAR IY83181**Abstract:**

Scanner is not able to manager prtdiag output.

Error Description:

The scanner is not able to parse some output from prtdiag. For example:

IO Type	Port ID	Bus Side	Slot	Bus Freq MHz	Max Bus Freq MHz	Dev, Func	State	Name	Model
PCI	8	B	2	33	33	2,0	ok	SUNW,q1c-pci1077,2300.1077.106.1+	
PCI	8	B	3	33	33	3,0	ok	SUNW,q1c-pci1077,2300.1077.106.1+	
PCI	8	A	0	66	66	1,0	ok	pci-pci8086,b154.0/pci (pci)	PCI-BRIDGE

APAR IY83338**Abstract:**

Inventory configuration parameter 'Endpoint timeout' for 4.1 endpoints.

Error Description:

A parameter for setting endpoint timeouts is required for version 4.1 endpoints.

APAR IY84170**Abstract:**

Inventory after scan script executes before ITCM 423 patch

Error Description:

When "Scan For Patch Information" is checked in the Inventory *InventoryConfig* Profile The Inventory Server, updates the contents of the after scan script section adding, after the custom script (if any), the Patch Management scanner commands.

APAR IY84708

Abstract:

Inventory data handler core dump when output queue has a blank CTOC.

Error Description:

The Inventory data handler does not correctly handle an empty CTOC in the output queue.

APAR IY84735

Abstract:

* in COMPUTER_SYS_ID when GUID is shorter than 28 characters

Error Description:

Inventory pads the GUID string with *, if the GUID size is shorter than 28 characters on Windows endpoints. The COMPUTER_SYS_ID value has the remaining characters filled by *.

APAR IY84736

Abstract:

CITMDRV cannot be shared between two processes.

Error Description:

The CITMDRV driver cannot be shared between concurrent scans on the same machine.

APAR IY84739

Abstract:

Selecting executables only from Inventory GUI in PC software is not retained and does not update profile.

Error Description:

On the Inventory GUI; the PC-software configuration is not correctly saved when the "Executable only" check box is selected. When the configuration is subsequently reloaded, the check box is no longer selected and issuing the `wgetinvpcsw` command shows the "Scan for Executables only" parameter set to **No**.

APAR IY84876

Abstract:

Patch automation - MIF file contains null fields

Error Description:

The Patch Management inventory scan contains some fields with no content. Null constraints on Oracle database prevent rows being inserted that include these fields.

APAR IY85317

Abstract:

Serial number not retrieved properly on Sun boxes.

Error Description:

The hardware scan does not correctly retrieve the serial number for Sun endpoints.

APAR IY85496

Abstract:

Inventory: inv_ora_schema.sql has the temporary tables off by default.

Error Description:

During the configuration of an Oracle RDBMS, the inv_ora_schema.sql script, which installs the inv_db_repository schema, disables the temporary tables by default.

APARs and internal defects fixed for Scalable Collection Service: Table 7 lists the APARs and internal defects that were fixed for the Scalable Collection Service component.

Table 7. APARs and internal defects for the Scalable Collection Service component

Scalable Collection Service, Version 4.2.3, 4.2.3-CLL-FP02				
IY79101	IY84553			

APAR IY79101**Abstract:**

wcancellscan command roles changed

Error Description:

Changes have been made to the level of authorization required to run the **wcancellscan** command. Users no longer require the super or senior roles. The admin and Dist_control roles are sufficient.

APAR IY84553**Abstract:**

Scans hanging at one gateway collector.

Error Description:

Scans remain in pending state. One gateway is continually crashing. The following error message can be found in the *mcollect.log* file:

```
c:\Tivoli\bin\w32-ix86\TAS\Collector\Collector_prog1.exe
(method:2155-mc_start, PID:420) exited unexpectedly, status=6
```

APARs and internal defects fixed for Software Distribution: Table 8 lists the APARs and internal defects that were fixed for Software Distribution:

Table 8. APARs and internal defects for Software Distribution

Software Distribution, Version 4.2.3, 4.2.3-SWDSRV-FP02				
IY77018	IY77069	IY77071	IY77687	IY78897
IY79008	IY80104	IY80472	IY80616	IY80647
IY81040	IY81283	IY81596	IY81621	IY81968
IY82317	IY82563	IY82581	IY83183	IY83456
IY83758	IY85493			
Software Distribution Gateway, Version 4.2.3, 4.2.3-SWDGW-FP02				
IY75145	IY76100	IY76968	IY77261	IY77363
IY77687	IY77689	IY78072	IY79151	IY80647
IY80648	IY81144	IY81540	IY81596	IY81773
IY82317	IY82467	IY82563	IY82975	IY83339
IY83340	IY83456	IY83527	IY84105	IY85098

Table 8. APARs and internal defects for Software Distribution (continued)

Software Distribution, Version 4.2.3, 4.2.3-SWDSRV-FP02				
Software Package Editor, Version 4.2.3, 4.2.3-SWDJPS-FP02				
IY77361	IY81040			
Software Package Editor for Endpoints, Version 4.2.3, 4.2.3-SWDEP-FP02				
IY76100	IY76968	IY77261	IY77361	IY77689
IY78072	IY79151	IY80647	IY80648	IY81040
IY81144	IY82317	IY82467	IY82563	IY83456
IY83462	IY83508			

APAR IY75145

Abstract:

Importing Windows CE SPB from endpoint generates error

Error Description:

When trying to import a Windows CE software package block from the endpoint in a freshly installed Configuration Manager 4.2.2 environment, the following error occurs:

ISSE0045E E Software package operation failed libtwg.dll not found

APAR IY76100

Abstract:

Execution fails on AS/400 endpoint when execute_user_program is processed

Error Description:

User tries to install a software package block containing an user program. Execution fails because spd_eng tries to spawn the user program with userid=qsecofr. In the software package editor GUI, the default user program UID and GUID are both set to -1 (they refer to the user qtivroot).

APAR IY76968

Abstract:

Wrong behavior when installing software package with native MSI package that installs only one of several features.

Error Description:

Using the Software Package Editor, create or edit a MSI package that installs several features. Set the Do not install option for one feature. The problem is that, during the installation, the package forces the installation of all features.

APAR IY77018

Abstract:

Software packages are removed from profile managers.

Error Description:

If you remove a software package from a collection on the Tivoli desktop, it is deleted from its profile manager and moved to the lost-n-found collection. The same action for other objects removes the object from the collection but does not delete it from the profile manager. After applying the fix, the software packages have the same behavior as other objects.

APAR IY77069

Abstract:

wfptosp does not handle Linux interpreter type

Error Description:

Using the **wfptosp** utility to convert a file package to software package, the package automatically generated does not contain a valid mapping for Linux endpoints.

APAR IY77071

Abstract:

Warning message importing a software package created by the **wfptosp** command

Error Description:

Use the **wfptosp** utility to convert a file package having an entry such as `unix_xxx_input_from_src=y` to software package. When importing the software package, the following warning message is displayed:

Unread attribute `descend_dirs` in context `corequisite_files`.

APAR IY77261

Abstract:

Checkpoint and restart do not work for delta packages if a network failure occurs

Error Description:

If a network failure occurs when performing a delta package installation, the distribution fails and the following error is logged on the Tivoli server:

DISSE0045E Software package operation failed. Error message:
DISSE0423E Failed to run HPCP delta algorithm. Error number: -1.

APAR IY77361

Abstract:

The Software Package Editor does not work correctly using Install HP packages

Error Description:

The Software Package Editor does not work correctly using the **Install HP packages** feature, when the file does not exist on the machine where you are creating the package. In this case, no information about the package file is saved and the package cannot be installed.

APAR IY77363

Abstract:

Software package issue

Error Description:

When you build a package with the following settings for the `execute_user_program` on commit:

`transactional = y`
- `bootable = y`
- `retries = 1` (or greater)

When the user program is run for the first time, it initiates a hard reboot and does not exit before the machine is rebooted.

APAR IY77687

Abstract:

The attribute retry of an execute user program does not work properly.

Error Description:

If the retry attribute is set for the execute_user_program in the COMMIT stanza, the user program should run each time the commit operation is performed, but it only works correctly the first time.

APAR IY77689

Abstract:

If an endpoint is manually rebooted the retry attribute is not run when the endpoint is up and running again

Error Description:

When installing transactionally, and then committing with a user reboot, a software package containing a script in the COMMIT stanza with the following options set:

- bootable=y
- retry=1

The retry of the script does not occur when the endpoint is up and running again.

APAR IY77871

Abstract:

Plan remains WAITING if restarted after COMPLETE_NOT_AFTER

Error Description:

When submitting a plan with a complete_not_after date set, if the plan fails and gets restarted after the complete_not_after date, it goes into WAITING status and no plan activity is run.

APAR IY78072

Abstract:

Commit program does not run in case of checkpoint restart

Error Description:

If a software package is installed transactionally, auto-commit with a user reboot, the commit program does not run after the user reboot if there is a checkpoint restart.

APAR IY78730

Abstract:

Conditioned activities might not start if execution windows are specified on Sunday

Error Description:

When you submit a plan on Sunday with many conditioned activities, some activities might not start even if the conditions are met.

APAR IY78897

Abstract:

wexpso causes hang when using again software package in lost-n-found

Error Description:

When a software package is in lost-n-found and you run the following command against the software package: **wexpspo software_package_name** the prompt hangs. Control -c is the only way to get back your prompt.

APAR IY79008**Abstract:**

wfptosp does not manage & when used for package names causing script failure

Error Description:

On UNIX platforms, the migration of a file package, whose name contains special characters such as &, using the **wfptosp** command, fails with the following error:

```
FRWTT0003E An instance named instance_name of resource FilePackage_name was not found.
```

APAR IY79151**Abstract:**

The *post.cat* and *post.cat.sem* files are locked by other Software Distribution processes

Error Description:

Software distributions might fail on some servers. The Software Distribution traces show that the *post.cat* and *post.cat.sem* files cannot be unlocked.

APAR IY80104**Abstract:**

SWD GUI Advanced options, distribution settings panel option.

Error Description:

There is an inconsistency between the default setting for the deadline setting in the GUI advanced options, distribution settings panel and the default for mdist2. Using the GUI to schedule a software package option, when you select the Distribution settings from the Advanced options menu and set one of the keys, for example Wake on LAN[®], the deadline default setting is one day. The default for mdist2 is three days.

APAR IY80472**Abstract:**

Added a new key to the **wswdcfg -s** command

Error Description:

There was no method of disabling the removal of software packages that had not been installed. A parameter has been added to the configuration of the Tivoli Management Region server, providing the capability to disable this feature. The parameter is **disable_remove_not_installed** and permitted values are **y** and **n**.

To disable the removal of software packages that have not yet been installed:

```
wswdcfg -s disable_remove_not_installed=y
```

When the feature is disabled on the Tivoli Management Region server, an attempt to remove a software package that has not yet been installed will fail.

APAR IY80616

Abstract:

The `force_mandatory=n` parameter does not work with `wspmldata`.

Error Description:

If a mandatory date that is in the past is specified, the `wspmldata` ignores the setting of the `force_mandatory` parameter and forces the mandatory distribution without confirmation from the user. This behavior should only occur when the parameter is set to `y`. When the parameter is set to `n`, the user should be able to choose not to start the distribution.

APAR IY80647

Abstract:

Keywords not used in `all_line` stanza are mistakenly written in `SP` text

Error Description:

The `add_line` and `add_token` stanza contain `remove_if_modified`, `replace_if_existing`, and `replace_if_newer`, all of which are not used.

APAR IY80648

Abstract:

Need to make `REG_SZ` compatible with `REG_EXPAND_SZ`

Error Description:

For certain registry keys like `PATH`, some Windows installation uses `REG_SZ` and other installations use `REG_EXPAND_SZ`. If the software package adds a key with the `REG_SZ` type and then finds a key with the `REG_EXPAND_SZ` type, it considers the two types different, so it replaces the old key instead of simply adding the new value at the end of the existing one. For example, on the target machine, you create a registry value of type `REG_SZ` with the name `mypath` and value `one;two`. You then create a package that should append `three` to that registry value, defined in the package as `REG_EXPAND_SZ`. The expected value of `mypath` should be `one;two;three`, but it will actually be just `three`.

APAR IY81040

Abstract:

`install_hp_packages` works on HP-UX 11.00, but fails on HP-UX 11.11

Error Description:

User has a software package that works properly on HP-UX 11.00, but fails on HP-UX 11.11. In the package log, there is this warning:

The file `"/home/gussorlk/sw999997"` defines an option `"loglevel=2"` which is not a valid option for `swinstall`.

APAR IY81144

Abstract:

Symbolic link not created when variable is passed

Error Description:

User is trying to pass path variable, then create a link, however this does not work on UNIX endpoints. User is using a variable to set a symbolic link.

APAR IY81283

Abstract:

The before_program action no longer executes after upgrade.

Error Description:

Following upgrade of Configuration Manager from version 4.2.1 to version 4.2.3, the before_program actions of software packages that are contained in software package profiles created using 4.2.1 no longer run.

APAR IY81540

Abstract:

Access violation in *spd_eng.exe*

Error Description:

The distribution ends unexpectedly, apparently after the lcf_after_program has completed successfully. It was not possible to reproduce the problem. Additional tracing has been added.

APAR IY81596

Abstract:

Running a data moving command with a postscript creates error file in */tmp*

Error Description:

Description: If you run a datamoving command, and specify a post script on the managed node, the standard error of the script is kept in the */tmp* directory.

APAR IY81621

Abstract:

Tivoli Enterprise Console® adapters throwing exceptions.

Error Description:

Exceptions generated by the Tivoli Enterprise Console adapters are not correctly handled. Following application of the fix, Tivoli Enterprise Console exception causes a warning message to be logged.

APAR IY81773

Abstract:

DMS-OS/400: Incorrect formatting moving native AS/400 files.

Error Description:

When a file is moved from an OS/400 arabic endpoint (codepage 420) to a Windows arabic endpoint (codepage 1256), the data has to be reversed because the 1256 codepage reads from left to right.

To ensure that this fix will work, also install the most recent fix pack for Tivoli Management Framework.

APAR IY81968

Abstract:

SWDMGR abends in t_swdmgr_matched_software after a sigmap_query fails

Error Description:

A core dump occurs during an inventory scan in the sigmap_query is not successful.

APAR IY82317**Abstract:**

FP01 - install_msi_product stanza contains a package_file attribute that contains variables

Error Description:

Following installation of FP01, variables are not correctly handled in the check made to validate the MSI file name.

APAR IY82467**Abstract:**

Customize the number of retries of the call.

Error Description:

When initiate_system_shutdown fails with a not ready error, the operation is retried a maximum of five times and this maximum cannot be changed.

To make the retrying of this operation customizable the following parameters are added to the swdis.var file:

__SWD_REBOOT_FAIL_RETRY_TIMES__

The number of times the operation should be retried.

__SWD_REBOOT_FAIL_RETRY_SLEEP_TIME__

The length of time in seconds between successive retries.

APAR IY82563**Abstract:**

User notification dialog contains garbled characters.

Error Description:

In Japanese environments, the user notification panel on the endpoint contains garbled characters.

APAR IY82581**Abstract:**

S=11 in spo_core when performing a publish operation with validation enabled in a Manage Resource policy.

Error Description:

An error is generated when publishing or unpublishing a software package in a policy region where validation is enabled.

APAR IY82975**Abstract:**

SPD_ENG crashes on the endpoint during a from_fileserver installation

Error Description:

This problem occurs because the file server is not available. The condition

is not checked when the gateway contacts the endpoint following a checkpoint restart caused by a network error.

APAR IY83183

Abstract:

wmdist -I shows the wrong size if send (**wspmvdata**) uses "*"

Error Description:

The size of the package being sent, reported by **wmdist -I**, is incorrect when the wildcard * has been used to include multiple files in a **wspmvdata** send operation. The number of files to be sent is wrongly multiplied by the number of endpoints to which the package is to be sent.

APAR IY83339

Abstract:

Extra characters added when transferring files

Error Description:

When the data moving function is used to move files from Windows to AS/400 , additional characters are added to the files.

APAR IY83340

Abstract:

No page break found while transferring spool files from AS/400 to Windows using the data moving utility.

Error Description:

When the data moving function is used to move spool files from AS/400 to Windows targets, the page-break control is not successfully transferred.

APAR IY83456

Abstract:

Byte-level difference software distribution - DISSE0423E Failed to run.

Error Description:

Distribution of a software package using byte-level differencing fails with message DISSE0423E. This problem occurs if software packages involved in the delta distribution are large. Following installation of the fix, byte-level differencing can be used with large software packages.

APAR IY83462

Abstract:

wdsetsps: New option to manage IP-BC state on local catalog

Error Description:

It is not currently possible to force the reinstallation of a software package for which a not final status is registered in the endpoint catalog. A new option, **-e (Success | Failure)**, is added to the disconnected command **wdsetsps** to allow you to force the package status to a final status, as follows:

- To force the package status to Success:
wdsetsps -e Success
- To force the package status to Failure:
wdsetsps -e Failure

After running the command, you should immediately perform a new forced installation as other operations could cause unexpected behavior.

APAR IY83508

Abstract:

Hidden files on Solaris are not read by the 4.2.3 SPE browser

Error Description:

Using the Software Package Editor on Solaris and Windows platforms, hidden files that start with a dot are not visible when the browse function is used to add a file. If the file name is manually entered, the file is found and successfully added.

APAR IY83527

Abstract:

When *post.cat* is corrupted the lock is not removed and this causes a loop.

Error Description:

During versioning, the *post.cat* file is locked and if it is found to be corrupted, the operation being performed fails but the lock is not removed. During the report phase, the *post.cat* file is accessed again and because it is still locked, a loop starts. After the fix is applied, the behavior changes so that the corrupted file is deleted and recreated.

APAR IY83758

Abstract:

winstsp of a non-lenient software package generates unnecessary trace points when Resource Manager is not installed.

Error Description:

When the **winstsp** command is used to install a non-lenient software package, the command performs look-up actions related to Resource Manager even if that component is not installed.

APAR IY84105

Abstract:

spd_eng traps and its files remain locked

Error Description:

When the spd_eng process traps, a popup message is displayed on the workstation, and all the files used by spd_eng remain locked. After the conn_retry interval, the gateway recontacts the endpoint and another spd_eng process starts. This new spd_eng causes a loop on the locked files.

APAR IY84167

Abstract:

Moving data from AS/400 does not convert LamAlef characters.

Error Description:

LamAlef characters are not converted during data moving operations from AS/400 systems.

APAR IY85098

Abstract:

% character in software package causes Linux endpoints to trap in case of failure

Error Description:

Create a software package with a name that contains a % character, add a user_program with some arguments that contain % as well, distribute the software package to Linux endpoints. The following error message is reported in the lcfld.log file:

Format has illegal types, need standard catalog entry

APAR IY85493

Abstract:

Software package log on server starts with STANDARD OUTPUT/ERROR END

Error Description:

The start marker of the software package trace log on the server is set to STANDARD OUTPUT/ERROR END instead of STANDARD OUTPUT/ERROR BEGIN

APARs and internal defects fixed for Activity Planner: Table 9 lists the APARs and internal defects that were fixed for Activity Planner:

Table 9. APARs and internal defects for Activity Planner

Activity Planner, Version 4.2.3, 4.2.3-APM-FP02				
IY77871	IY78730	IY79210	IY80188	IY80397
IY80844	IY81197	IY81769	IY83067	IY83772
IY83968	IY84411	IY84511	IY84627	IY84738
IY85127	IY85313			

APAR IY77871

Abstract:

Plan remains waiting if restarted after complete_not_after date

Error Description:

If a plan that has a complete_not_after date defined fails and is later restarted on a date that is later than the specified complete_not_after date, the plan is moved to 'Waiting' status and is never activated.

APAR IY78730

Abstract:

Conditioned activities might not start if execution windows cover Sunday time

Error Description:

If a plan that is submitted to run on a Sunday includes conditioned activities, some of the activities might not be performed even though the conditions are met.

APAR IY79210

Abstract:

Passwords that contain special characters fail to launch the MDIST2 GUI from the APM monitor GUI.

Error Description:

When the MDIST2 GUI is launched from the APM monitor GUI, special characters included in the password are not correctly handled. Some special characters are accepted and others are not. After the fix pack is installed all special characters other than double quotes are accepted.

APAR IY80188**Abstract:**

APM GUI hangs when **Switch gateway grouping on/off** is selected and a reload occurs.

Error Description:

On the Activity Plan Monitor GUI, if you select **Switch gateway grouping on/off** or select Target Grouping -> By Manager from the View menu, the following problems occur:

- You cannot select **Details** on the endpoint.
- If you perform a reload or wait for an automatic update, the GUI hangs with CPU usage 100%.

APAR IY80397**Abstract:**

Target list for queries truncates on display.

Error Description:

On the Activity Plan Monitor GUI, the target list for queries does not display all existing queries.

APAR IY80844**Abstract:**

Targets are not sorted in order after plan submission

Error Description:

If you have a text file containing a list of targets in alphabetic order, then create a plan with two activities using that text file, after you submit the plan, the target lists in each activity are not sorted in alphabetic order.

APAR IY81197**Abstract:**

wmonpln output does not sort order by plan ID

Error Description:

The **wmonpln -lw** output does not sort plan ID in order. This is not the correct behavior - The plan ID column should be sorted in order.

APAR IY81769**Abstract:**

Resume/Start plan on a paused plan resolves the target list ahead of time.

Error Description:

When a paused plan is resumed or started, the target list is immediately resolved even if target resolution at activity execution has been specified and the start_not_before date and time has not been reached.

APAR IY83067

Abstract:

Delete activity does not resolve the variable used as destpath

Error Description:

If an activity included in a plan contains variables, for example for the destination path of the activity, the activity is only successful the first time the plan is executed. Any subsequent attempts fail because of incorrect setting of the variable.

APAR IY83772**Abstract:**

Recursive plan remains "Waiting" when RIM planner is deleted

Error Description:

If the planner RIM object is deleted and then restored, and a commit operation is performed in the time interval during which RIM is not available, an exception is raised causing the recursive plan to stay in Waiting status.

APAR IY83968**Abstract:**

Data moving operation from endpoint to endpoint does not work when started from APM

Error Description:

When submitting a data moving operation from endpoint to endpoint using the Activity Planner Monitor, the distribution does not complete and the output of the **wmdist -q** command shows the target endpoint in WAITING status.

APAR IY84411**Abstract:**

Activity Planner Monitor is able to pause a task activity in a plan

Error Description:

From the Activity Planner Monitor you are able to pause a task activity in a plan. This is not a correct behavior, since this type of operation is not supported by the application plug-in.

APAR IY84511**Abstract:**

Searching the plan to submit through the Activity Planner Monitor is not immediate

Error Description:

There is currently no search facility when selecting from the Activity Planner Monitor a plan to submit. When pressing a specific key, the Activity Planner Monitor should immediately show all the plans starting with that particular character-key.

APAR IY84627**Abstract:**

APPL_SPEC_ACT_ID duplicated under specific conditions

Error Description:

Under specific circumstances, the APPL_SPEC_ACT_ID value for one

activity might be duplicated for the activity in another plan. The values for APPL_SPEC_ACT_ID should be unique.

APAR IY84738

Abstract:

Pausing an activity plan does not set its status to "Paused"

Error Description:

After pausing a plan, the plan status remains "Started" and does not change into "Paused". This happens when at least one activity in the plan is canceled_by_condition.

APAR IY85127

Abstract:

wstopapm command does not display any error message

Error Description:

No error message is displayed when the command wstopapm -f fails because the user does not have administrator or root privileges.

APAR IY85313

Abstract:

APM processing is slow when many plans with execution windows are submitted.

Error Description:

When many plans with execution windows are submitted, CPU usage by the APM engine becomes very high and processing becomes very slow. Submitted plans can be listed with a status of WAITING for up to 30 minutes.

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: Web Interface component does not currently contain any fixed APARs.

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

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 the Patch Management component.

Table 10. APARs and internal defects for Patch Management included from 4.2.3-PMG-FP02

Patch Management, Version 4.2.3, 4.2.3-PMG-FP02				
IY84197	IY84241	IY84243	IY85839	

APAR IY84197

Abstract:

CMYSE0203E Keyword prepare_patches_requiring_connectivity or prepare_patches_requiring_user_input not found in configuration object

Error Description:

This error is generated during workflow execution when the keywords `prepare_patches_requiring_connectivity` and `prepare_patches_requiring_user_input` have not been configured. Though the keywords, which were introduced in 4.2.3-TCM-FP01 FixPack for Tivoli Patch Management, are optional, errors occur if they are not explicitly coded or specified using `wseccfg` command.

APAR IY84241**Abstract:**

Workflow is very slow when the `wsecrprt -sM` command runs.

Error Description:

The `wsecrprt -sM` query reports the same entry multiple times.

APAR IY84243**Abstract:**

Patch automation - logging typo

Error Description:

In the patch management log, the command name `wsecrprt` is reported as `wsecrptr`.

APAR IY85839**Abstract:**

Preparation phase of activity plan fails with CMYSE022

Error Description:

An activity plan for patch management fails with error message CMYSE022 during its preparation phase.

Fixes contained in previous fix packs and interim fixes

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

Table 11. APARs and internal defects for Inventory included from 4.2.3-INV-0001 and 4.2.3-INVGW-0001

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 Inventory included from 4.2.3–INV-FP01

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

Table 13. Inventory APARs included from 4.2.3–INV-0006 and 4.2.3–INVGW-0006

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

Table 14. Inventory APARs included from 4.2.3–INV-0007 and 4.2.3–INVGW-0007

Inventory and Inventory Gateway, Version 4.2.3, 4.2.3–INV-0007 and 4.2.3–INVGW-0007				
IY79372	IY79890	IY80644	IY80837	IY80912

Table 15. APARs and internal defects for Scalable Collection Service included from 4.2.3–CLL-0001

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

Table 16. Scalable Collection Service APARs included from 4.2.3–CLL-0002

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

Table 17. APARs and internal defects for Software Distribution included from 4.2.3–SWDSRV-0001, 4.2.3–SWDGW-0001, 4.2.3–SWDJPS-0001, and 4.2.3–SWDEP-0001

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

Table 17. APARs and internal defects for Software Distribution included from 4.2.3-SWDSRV-0001, 4.2.3-SWDGW-0001, 4.2.3-SWDJPS-0001, and 4.2.3-SWDEP-0001 (continued)

Software Distribution, Version 4.2.3, 4.2.3-SWDSRV-0001		
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 18. APARs and internal defects for Software Distribution included from 4.2.3-SWDSRV-FP01, 4.2.3-SWDGW-FP01, 4.2.3-SWDJPS-FP01, and 4.2.3-SWDEP-FP01

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		

Table 19. Software Distribution APARs included from 4.2.3-SWDSRV-F1P1, 4.2.3-SWDGW-F1P1, 4.2.3-SWDJPS-F1P1, and 4.2.3-SWDEP-F1P1

Software Distribution, Version 4.2.3, 4.2.3-SWDSRV-F1P1				
IY76698	IY77526	IY77936	IY78598	IY78973
Software Distribution Gateway, Version 4.2.3, 4.2.3-SWDGW-F1P1				
IY75263	IY76010	IY76694	IY77516	IY77601
IY77602	IY78195	IY78976		

Table 19. Software Distribution APARs included from 4.2.3-SWDSRV-F1P1, 4.2.3-SWDGW-F1P1 4.2.3-SWDJPS-F1P1, and 4.2.3-SWDEP-F1P1 (continued)

Software Package Editor, Version 4.2.3, 4.2.3-SWDJPS-F1P1				
IY76008	IY77833			
Software Package Editor for Endpoints, Version 4.2.3, 4.2.3-SWDEP-F1P1				
IY76008	IY76488	IY77508	IY77833	IY78976

Table 20. Software Distribution APARs included from 4.2.3-SWDSRV-F1P2 4.2.3-SWDGW-F1P2 4.2.3-SWDJPS-F1P2 and 4.2.3-SWDEP-F1P2

Software Distribution, Version 4.2.3, 4.2.3-SWDSRV-F1P2				
IY79792	IY80807	IY80811		
Software Distribution Gateway, Version 4.2.3, 4.2.3-SWDGW-F1P2				
IY81773				
Software Package Editor, Version 4.2.3, 4.2.3-SWDJPS-F1P2				
None				
Software Package Editor for Endpoints, Version 4.2.3, 4.2.3-SWDEP-F1P1				
IY80762				

Table 21. APARs and internal defects for Activity Planner included from 4.2.3-APM-0001

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 22. APARs and internal defects for Activity Planner included from 4.2.3-APM-FP01

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	

Table 23. Activity Planner APARs included from 4.2.3-APM-F1P1

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

Table 24. Activity Planner APARs included from 4.2.3-APM-F1P2

Activity Planner, Version 4.2.3, 4.2.3-APM-F1P2				
IY78519	IY80151			

Table 25. APARs and internal defects for Change Manager included from 4.2.3-CCM-0001

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

Table 26. APARs and internal defects for Web interface included from 4.2.3-WEB-0001

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

Table 27. APARs and internal defects for Web Interface included from 4.2.3-WEB-FP01

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

Table 28. APARs and internal defects for Resource Manager included from 4.2.3-TRMSRV-FP01

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

Table 29. APARs and internal defects for Pristine Manager included from 4.2.3-PRI-0001

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

Table 30. APARs and internal defects for Patch Management included from 4.2.3-PMG-0001

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

Table 31. APARs and internal defects for Patch Management included from 4.2.3-PMG-FP01

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

Table 32. APARs and internal defects for Directory Query included from 4.2.3-QDY-0001

Directory Query, Version 4.2.3, 4.2.3-QDY-0001		
IY82979		

Limitations

Defect 184765: In an environment where Hub and Spoke Rim hosts refer to the same RDBMS and where Spoke regions are upgraded before the Hub region, in the period between upgrade of the Spokes and upgrade of the Hub signature matching signature scans can only be requested from the Hub region.

Defect 182062: In IBM Tivoli Configuration Manager, Version 4.2.3 Fix Pack 2, 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 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 fix pack 2. You must specify any other proxy host different from the SUS server.

For Directory Query, enabling automatic replications causes manual and scheduled replications to be disabled.

Installation

This section describes how to install fix pack 2 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.

Note: After upgrading the Tivoli Resource Manager to 4.2.3, run the `$BINDIR/TRM/RegisterPervasive.sh` script and the `reexec` command on the Tivoli server to display the Nokia9300 type in the Software Package Editor GUI.

This section includes the following topics:

- "Hardware and software requirements"
- "Traditional fix pack installation methods" on page 37
- "Software package block (SPB) fix pack installation for GUI components" on page 42
- "Updating the inventory schema" on page 47

Hardware and software requirements

This section includes the following topics:

- "Supported platforms"
- "System requirements" on page 37

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

This section details additional requirements introduced with this fix pack. Other hardware and software prerequisites are detailed in the *IBM Tivoli Configuration Manager: Release Notes*.

The following requirements are added:

Inventory running on HP-UX 11.00

Quality Pack For HP-UX 11.00, March 2004 (QPK1100 B.11.00.64.4)

License Management Extension space requirements

Table 33. Space requirements for the License Management Extension

Component	Space
Configuration Manager Extension for License Manager	2 MB on Managed Node
Configuration Manager Endpoint Extension	12 MB on Gateway
	3 MB on OS/400 endpoints
	1 MB on other endpoints
Tivoli License Manager agent bundle, version 2.2.0	195 MB on Gateway
	17 MB on Windows endpoints
	32 MB on AIX endpoints
	52 MB on Solaris SPARC endpoints
	26 MB on Solaris X86 endpoints
	34 MB on HP-UX endpoints
	22 MB on Linux x86 endpoints
23 MB on Linux PPC endpoints	

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 34 on page 40 for information about the related IND file.
2. Install the fix pack on the Tivoli gateways.
3. Install the fix pack on the Inventory server.

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” on page 38
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 39
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 39
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 41
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®. It cannot be used to install the License Management Extension or the Active Directory feature.

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 2 CD1. 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:

Upgrading an existing component
Install->Install Patch

Adding a new component
Install->Install Product

2. Select the media and component to be upgraded or added.
3. Select the workstations where the component is to be upgraded or added.
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

This fix pack contains new components and updates to existing components. Use the **winstall** command to install new components and the **wpatch** command to install updates to existing components.

wpatch command: When upgrading existing components using the **wpatch** command, specify the name of the index file using the file shown in Table 34 on page 40. 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 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 2 CD 1.

-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 for existing components included in this fix pack.

Table 34. IND files included in this fix pack

IND file	Component name	Tag
CLLFP2.IND	Scalable Collection Service, Version 4.2.3	4.2.3-CLL-FP02
INVFP2.IND	Inventory, Version 4.2.3	4.2.3-INV-FP02
LCFFP2.IND	Inventory Gateway, Version 4.2.3	4.2.3-INVGW-FP02
SWDFP2.IND	Software Distribution, Version 4.2.3	4.2.3-SWDSRV-FP02
SDGWFP2.IND	Software Distribution Gateway, Version 4.2.3	4.2.3-SWDGW-FP02
SDJFP2.IND	Software Distribution Software Package Editor, Version 4.2.3	4.2.3-SWDJPS-FP02
APMFP2.IND	Activity Planner, Version 4.2.3	4.2.3-APM-FP02
CCMFP2.IND	Change Manager, Version 4.2.3	4.2.3-CCM-FP02
WEBUIFP2.IND	Web Interface, Version 4.2.3	4.2.3-WEB-FP02
TRMFP2.IND	Resource Manager, Version 4.2.3	4.2.3-TRMGW-FP02
TRMGWFP2.IND	Resource Manager Gateway, Version 4.2.3	4.2.3-TRMGW-FP02
PMFP2.IND	Pristine Manager, Version 4.2.3	4.2.3-PRI-FP02
PMGFP2.IND	Patch Management, Version 4.2.3	4.2.3-PMG-FP02
ICOMPFP2.IND	Inventory, Version 4.2.3, backward compatibility patch	4.2.3-INV-COMP-FP02
DQYFP2.IND	Directory Query, Version 4.2.3	4.2.3-DQY-FP02
REMBO.IND	Image management services integration (Rembo) , Version 4.2.3	rembo

winstall command: When using the **winstall** command to install 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.

The following table contains a list of index files for new components included in this fix pack.

Table 35. IND files included in this fix pack

IND file	Component name	Tag
ADICLI.IND	Query Directory for Microsoft Active Directory - Command Line Interface, Version 4.2.3	ADICli
ADIENG.IND	Query Directory for Microsoft Active Directory, Version 4.2.3	ADIEng

Table 35. IND files included in this fix pack (continued)

IND file	Component name	Tag
TLMEXT.IND (*)	CM Extension for Tivoli License Manager, Version 4.2.3	tlm_ext
CMEXT.IND (*)	CM Endpoint Extension, Version 4.2.3	cm_ext

(*): For information on how to implement License Compliance Manager in your Configuration Manager environment see *IBM Tivoli Configuration Manager License Management Extension*.

- The workstations where the image is to be installed.
- The installation options

Example:

```
winstall -c CD-ROM/images -i index_file managed_node installation_options
```

where:

-c CD-ROM/images

Specifies the path to the images on the IBM Tivoli Configuration Manager, Version 4.2.3 Fix Pack 2 CD 1.

-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.

installation_options

Specifies the installation options.

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

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 34 on page 40.

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 45
- “Software Distribution server command” on page 45
- “Software Distribution disconnected command” on page 46

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 36.

Table 36. Default variables defined in SPB fix packs

Variable	Value	Description
Tivoli_INV_GUI_Fix.v4.2.3.FP02		
Version	4.2.3	The version of Inventory to which the SPB applies
DSWIN_DIR	\$(program_files)\Tivoli\Desktop	The directory where the Tivoli Desktop is installed.
Tivoli_INV_GUI_L10N_Fix.v4.2.3.FP02		
Version	4.2.3	The version of Inventory to which the SPB applies
DSWIN_DIR	\$(program_files)\Tivoli\Desktop	The directory where the Tivoli Desktop is installed.
Tivoli_APM_GUI_Fix.v4.2.3.FP02		
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_APM_GUI_L10N_Fix.v4.2.3.FP02		
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.FP02		
DSWIN_DIR	\$(program_files)\Tivoli\Desktop	The directory where the Tivoli Desktop is installed.

Table 36. Default variables defined in SPB fix packs (continued)

Variable	Value	Description
TME_JAVATOOLS	\$(program_files)\Tivoli\JavaTools	The directory where the JRE 1.3 is installed.
Tivoli_CCM_GUI_L10N_Fix.v4.2.3.FP02		
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_JRE_SOLARIS_IX86_Fix.v4.2.3.FP02		
Tivoli_JRE_version	1.3.0	The version of the JRE
TME_JAVATOOLS	/opt/Tivoli/JavaTools	The directory where JRE 1.3 is installed.
Tivoli_SWDEP_L10N_Fix.v4.2.3.FP02		
target_dir	\$(product_dir)/speditor	The directory where the Software Package Editor is installed.
interp	\$(INTERP)	
TME_JAVATOOLS	/opt/Tivoli/JavaTools	The directory where JRE 1.3 is installed.
Tivoli_SWDEP_AIX_Fix.v4.2.3.FP02		
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.FP02		
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.FP02		
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.FP02		
target_dir	\$(product_dir)/speditor	The directory where the Software Package Editor is installed.
Tivoli_SWDEP_LINUXPPC_Fix.v4.2.3.FP02		
target_dir	\$(product_dir)/speditor	The directory where the Software Package Editor is installed.

Table 36. Default variables defined in SPB fix packs (continued)

Variable	Value	Description
TME_JAVATOOLS	/opt/Tivoli/JavaTools	The directory where JRE 1.3 is installed.
Tivoli_SWDEP_NT_Fix.v4.2.3.FP02		
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.FP02		
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.FP02		
target_dir	\$(product_dir)\speditor	The directory where the Software Package Editor is installed.
Tivoli_SWDEP_SOLARIS_IX86_Fix.v4.2.3.FP02.spb		
target_dir	\$(product_dir)\speditor	The directory where the Software Package Editor is installed.
Tivoli_Web_Gateway_DB_Fix.v4.2.3.FP02		
No variables		
Tivoli_Web_Gateway_SRV_Fix.v4.2.3.FP02		
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.
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.

Table 36. Default variables defined in SPB fix packs (continued)

Variable	Value	Description
Tivoli_WebUI_Fix.v4.2.3.FP02		
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 2 CD 2 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 2 CD 2.
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_FP02.xml` file for the fix pack located in the `/package` subdirectory on the IBM Tivoli Configuration Manager, Version 4.2.3 Fix Pack 2 CD 2. 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 37 on page 46.

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 37 contains the names of the fix pack 2 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 37. Names of SPB files and software profiles

SPB Files	Package name with Version
Tivoli_APM_GUI_Fix.v4.2.3.FP02.spb	Tivoli_APM_GUI_Fix.v4.2.3.FP02
Tivoli_APM_GUI_L10N_Fix.v4.2.3.FP02.spb	Tivoli_APM_GUI_L10N_Fix.v4.2.3.FP02
Tivoli_CCM_GUI_Fix.v4.2.3.FP02.spb	Tivoli_CCM_GUI_Fix.v4.2.3.FP02
Tivoli_CCM_GUI_L10N_Fix.v4.2.3.FP02.spb	Tivoli_CCM_GUI_L10N_Fix.v4.2.3.FP02
Tivoli_SWDEP_L10N_Fix.v4.2.3.FP02.spb	Tivoli_SWDEP_L10N_Fix.v4.2.3.FP02
Tivoli_SWDEP_AIX_Fix.v4.2.3.FP02.spb	Tivoli_SWDEP_AIX_Fix.v4.2.3.FP02
Tivoli_SWDEP_HP_Fix.v4.2.3.FP02.spb	Tivoli_SWDEP_HP_Fix.v4.2.3.FP02
Tivoli_SWDEP_LINUXPPC_Fix.v4.2.3.FP02.spb	Tivoli_SWDEP_LINUXPPC_Fix.v4.2.3.FP02
Tivoli_SWDEP_LINUX_IX86_Fix.v4.2.3.FP02.spb	Tivoli_SWDEP_LINUX_IX86_Fix.v4.2.3.FP02
Tivoli_SWDEP_LINUX_S390_Fix.v4.2.3.FP02.spb	Tivoli_SWDEP_LINUX_S390_Fix.v4.2.3.FP02
Tivoli_SWDEP_NTAS400_Fix.v4.2.3.FP02.spb	Tivoli_SWDEP_NTAS400_Fix.v4.2.3.FP02
Tivoli_SWDEP_NT_Fix.v4.2.3.FP02.spb	Tivoli_SWDEP_NT_Fix.v4.2.3.FP02
Tivoli_SWDEP_SOLARIS_Fix.v4.2.3.FP02.spb	Tivoli_SWDEP_SOLARIS_Fix.v4.2.3.FP02
Tivoli_JRE_SOLARIS_IX86.spb	Tivoli_JRE_SOLARIS_IX86
Tivoli_SWDEP_SOLARIS_IX86_Fix.v4.2.3.FP02.spb ⁽¹⁾	Tivoli_SWDEP_SOLARIS_IX86_Fix.v4.2.3.FP02
Tivoli_INV_GUI_Fix.v4.2.3.FP02.spb	Tivoli_INV_GUI_Fix.v4.2.3.FP02
Tivoli_INV_GUI_L10N_Fix.v4.2.3.FP02.spb	Tivoli_INV_GUI_L10N_Fix.v4.2.3.FP02
Tivoli_WebUI_Fix.v4.2.3.FP02.spb	Tivoli_WebUI_Fix.v4.2.3.FP02
Tivoli_Web_Gateway_DB_Fix.v4.2.3.FP02.spb	Tivoli_Web_Gateway_DB_Fix.v4.2.3.FP02
Tivoli_Web_Gateway_SRV_Fix.v4.2.3.FP02.spb ⁽²⁾	Tivoli_Web_Gateway_SRV_Fix.v4.2.3.FP02

Notes:

1. If you are installing the Software Package Editor component for Solaris on x86, using the Software Distribution command line, you need to install the following prerequisite packages first:
 - a. Tivoli_JRE_SOLARIS_IX86.spb. This package is a prerequisite for installing the Software Package Editor GUI on Solaris 8 and Solaris 9.

- b. Tivoli_SWDEP_SOLARIS_IX86_Fix.v4.2.3.FP02. This is an empty package used to update the local catalog in accordance with the adopted SPB naming convention on Solaris 8, 9 and 10.

If you are installing the SPB components via SPB_patch_installer, the prerequisite packages are automatically installed.

2. With the Tivoli_Web_Gateway_SRV_Fix.v4.2.3.FP02.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 schema

When you install a new fix pack, you need to update the Inventory schema.

This fix pack installation places files named `inv_dbvendor_schema_423_FP02.sql` and `h_inv_dbvendor_schema_423_FP02.sql` on the managed nodes where the patch is installed, in the following directory:

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

where `dbvendor` is the shortname for the database.

If you have already installed and configured the previous fix packs, you do not need to run the `inv_dbvendor_schema_P01.sql` and `h_inv_dbvendor_schema_423_FP01` scripts again.

For instance, if you use DB2 and install this fix pack over a 4.2.3 GA Version you need to run the following scripts:

- `inv_db2_schema_423_FP01.sql`
- `inv_db2_schema_423_FP02.sql`

If you have already run one of these scripts because you have already installed the related fix pack, you do not need to run it again.

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.

During the running of the scripts, temporary copies are made of information held in `MATCHED_SWARE`, `SIG_PACKAGE`, and `SIGS_MAP` tables. If the tables, particularly `MATCHED_SWARE`, the inventory temporary table space might not be sufficient. During testing on a database with 20000 endpoints and 400000 entries in the `MATCHED_SWARE` table, the inventory temporary tablespace variable `inv_temp_ts` was increased from the default value of 10 MB to 100 MB. In addition, the size of the transaction log for `INV_DB` was increased to 50 MB. Take this into consideration when preparing to run the scripts.

Notes:

1. With DB2 7.2: if an error occurs when running the `inv_db2_schema_423_FP02.sql` script, increase the application heap size with the following command:

```
db2 update db cfg for <inv_db_name> using applheapsz 256
```

Then rerun the first instruction in the `inv_db2_schema_423_FP02.sql` file:

```
alter table COMPUTER alter column OS_NAME set data type varchar(128);
```

2. If you are running a customizable script in an MVS environment (`inv_db2_mvs_<cm version>_<fix pack level>.sql`), some variables can be

customized. For information about the variables, refer to the header information in the `inv_db2_mvs_admin.sql` script.

3. Error or information messages might be displayed when running the database scripts. Each database has unique behavior, so some messages can be expected .
4. When you run the `inv_db2_mvs_custom_423_FP02.sql` script the alter table NATIV_SWARE alter column PACKAGE_NAME set data type varchar(128) instruction might not alter the NATIV_SWARE table. To avoid this problem you must perform the following steps:
 - a. Backup the table and the related views
 - b. Delete the table and all related views
 - c. Recreate table and related views

Updating the inventory queries

This fix pack installation provides scripts to update inventory queries with the new database information introduced by the fix pack. The scripts `inventory_query.sh` and `h_inventory_query.sh` are located on the managed nodes where the patch is installed, in the following directory:

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

Updating the Inventory signatures and packages

If you plan to install IBM Tivoli License Manager Extension, or if you imported the IBM software catalog before installing Configuration Manager 4.2.3 Fix Pack 2, you must migrate the signatures belonging to the IBM software catalog. To do this, after having installed Configuration Manager 4.2.3 Fix Pack 2, perform the following steps:

1. Run the `inv_db_vendor_423_FP02.sql` script.
2. Download the latest IBM software catalog file from the following Web site:
<http://www-306.ibm.com/software/sysmgmt/products/support/IBMTivoliLicenseManager.html>
3. Run the following command:

```
winvmigrate -c IBM_software_catalog_file
```

If you plan to install IBM Tivoli License Manager Extension, proceed with the IBM Tivoli License Compliance Manager, Version 2.2, Fix Pack 2.2.0-TIV-TLCM-FP0001.

Creating the Active Directory schema

The `admin` and the `schema` scripts used by Query Directory for Microsoft Active Directory are located on IBM Tivoli Configuration Manager Installation, Version 4.2.3 in the `$BINDIR/TME/ADI/SCRIPTS` directory. The names of the these scripts are

- `adi_dbvendor_admin.sql`
- `adi_dbvendor_schema.sql`

where:

dbvendor

Is the shortname for the database

The first script creates the container for all the logical objects (users, views, and so forth) and creates the tablespace that stores all the physical data in the tables, while the second one creates the tables and views in the allocated tablespace.

Copy the appropriate admin and 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 these scripts. For additional details see *Guide for Active Directory integration*.

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-FP02, 4.2.3-SWDSRV-FP02, and 4.2.3-INV-FP02 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-FP02, 4.2.3-SWDSRV-FP02, and 4.2.3-INV-FP02 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 or later, 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*.

The **4.1.1-TMF-004** Tivoli Framework fix or later must also be installed on the Tivoli server and gateways.

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

1. Install the **4.2.3-SWDSRV-FP02** Software Distribution fix pack to update the Software Distribution command line and GUI.
2. Install the **4.2.3-SWDGW-FP02** Software Distribution gateway fix pack to update Windows endpoints at the next distribution.
3. Install the **4.2.3-APM-FP02** Activity Planner fix pack to update the Activity Planner GUI.
4. Upgrade the Activity Planner plug-ins, as described in “Upgrading plug-ins” on page 49.
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 `wdepccm.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” on page 49, 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\wmands

To view and edit the registry keys, use the **wdepccm** command. For more information on this command, see “wdepccm” on page 55.

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."

wdepccem

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: `wdepccem [-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 **wdepccm** command returns one of the following:

0 Indicates that **wdepccm** completed successfully.

other than zero

Indicates that **wdepccm** failed due to an error.

Examples:

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

Implementing the activity plan group management feature

This feature introduces a means of creating, submitting, and tracking groups of related activity plans. The scripts and other related files that make up this tool are provided together with the fix pack and must be copied manually on to the target system or systems.

Implementation of the tool comprises the following tasks:

- Preparation activities that you must do once only before using the scripts. See “Preparing to use the tool.”
- Creation of a group of plans, including the definition of input files and the running of the creation script. See “Creating a group of activity plans” on page 62

To use the creation script, you must install perl 5.

- Submission and tracking of a group of plans by the definition of a recurring job. See “Submitting and tracking an activity plan group” on page 63.

Preparing to use the tool

Before using the tool for the first time, complete the following steps:

1. Run the appropriate SQL script to create the USER_TAB_COLUMNS view in the APM and MDIST2 databases. This task is not required for Oracle databases.

The following scripts are provided:

```
create_db2_mvsv_user_tab_columns.sql
create_db2_user_tab_columns.sql
create_infx_user_tab_columns.sql
create_ms_sql_user_tab_columns.sql
create_syb_user_tab_columns.sql
```

2. In the EtcTivoli directory, create the configuration file *wcfsplng.ini* to contain the following parameters:

TmpDir : Temporary directory

WorkDir: The main working directory of the tool

WebBase: Directory in which the output HTML reports are stored

ExclusionList: The full path name of a file containing a list of targets to be excluded from plan submissions.

LogFile: The full path where the log file for the tool is stored.

LogLevel; Possible values are 0 (fatal errors), 1 (errors), 2 (warnings), 3 (information). 0 is the default.

MailList: List of mail addresses for notifications.

MailLevel: Possible values are 1 (high importance), 2 (normal). 1 is the default.

MailHost: For Windows only, the host name of the mail server.

HTTPBase: Link to the location on the HTTP server to which the reports will be transferred.

Note: The HTML reports must be transferred from the **WebBase** directory to the **HTTPBase** after each iteration of the reporting script. You can avoid this task by directly mapping the directory to the managed node where the script is run or by configuring the managed node as an HTTP server.

ActivityDelimiter: A character that is used in the definition of an activity plan to separate the name of the activity to be performed from the name of the software package. The default is %.

SWDPackageCheck: Indicates whether the plan group creation script should check the existence of software packages specified in the script

parameters. The values **F**, **f**, **N**, **n**, and **0** indicate that no check should be made. Any other value indicates that the check should be made.

ActiveLimit: The maximum number of activities that can be current at any one time. The script that submits and tracks activity plan groups considers this limit when submitting the activities included in the plans.

UnavailAsActive: This can be set to false (the default), which can be indicated as **F**, **f**, **N**, **n**, or **0**, or true, which can be indicated as **T**, **t**, **Y**, **y**, or **1**.

This parameter is used by the submission and tracking script when it determines whether submitting an activity will cause the **ActiveLimit** to be exceeded. If the parameter is set to false, any activities that have been submitted and not yet completed on targets that are either unavailable or interrupted are not included in the number of current activities. For example, **ActiveLimit** is set to 100 and 90 submitted activities have not yet completed of which 10 are on targets that are not available. In such a scenario, if this parameter is set to false, a maximum of 20 activities can be submitted by the script, while if this parameter is set to true only 10 can be submitted.

3. In the directory specified as **WorkDir**, create the subdirectories *cfg* and *Targets*.
4. If required, create a file containing the list of targets to be excluded from plan submissions and save it with the path name specified in the **ExclusionList** parameter.

Creating a group of activity plans

To create a group of activity plans, complete the following steps:

1. In the *<WorkDir>\cfg* directory, for each plan you want to include in the group, create a plan configuration file with the following CSV format:

```
Xml_Name:Target_File:From_Depot[:ActivityName<delimiter>SWD_Package...]
```

Where:

Xml_Name is a name that will form part of the unique name of the plan within the group.

Target_file is the name of a text file containing the list of targets for the plan.

From_Depot indicates whether the software package distributed by the plan is to be distributed from a depot. Possible values are **T** (true) and **F** (false).

ActivityName identifies an activity that is to be performed on the specified software package. The ActivityName must identify an activity that is defined in the XML template you are using for this group of plans. The XML template to be used is defined in the *xml_base* parameter at the next step.

SWD_Package is the name of the software package to be distributed by the plan. .

The parameters **ActivityName** and **SWD_Package** form a pair separated by a delimiter (by default %). Repeat this pair of parameters for each activity and software package that are to be included in the plan.

2. For each plan configuration file you created, create a file containing the list of targets for the plan and save it in the *<WorkDir>\Targets* directory with the name *<Target_file>.txt*
3. In the *<WorkDir>\cfg* directory, create the file *Master_CFG.lst* .

This file is in CSV format. Each line represents a base APM plan and has the following format:

```
xml_base:id:Cfg_Plan:Exclusion_Flag
```

Where:

xml_base is the name of the XML file to be used as a template for the APM plan.

Id is an identifier that will form part of the unique name of the plan within the group.

Cfg_Plan is the name of an plan configuration file that you created for the plan.

Exclusion_Flag indicates whether the ExclusionList file is to be used when determining targets for this plan. Possible values are **y** and **n**.

4. Ensure that each XML file, identified by the **xml_base** parameter for each line in the *Master_CFG.lst* file, is present in the `<WorkDir>` directory.
5. Run the activity plan group creation script:

```
perl wcrtplng.pl base_name
```

Where *base_name* is a name that will identify the group as a whole and form part of the name of each plan that is included in the group.

The script creates an XML file for each line in the *Master_CFG.lst* file. The name of each file is constructed as follows: *base_name_id_xml_name*. The script imports the XML files to generate APM plans and creates the file *base_name_dist_pln.lst* containing information about all the plans that have been created. All files are created in a subdirectory of `<WorkDir>` called *base_name*.

Submitting and tracking an activity plan group

The **wmngplng.sh** script is used to submit the activity plan group and to track its progress. You should set it up as a regularly repeating job with the following syntax:

```
wmngplng.sh base_name
```

The *base_name* parameter identifies the group that is to be processed and enables the script to retrieve the *base_name_dist_pln.lst* which contains details of the plans to be managed.

The script first attempts to submit each activity for each target included in the plan group. Depending on the number of activities currently active and the values of the **ActiveLimit** and **UnavailAsActive** parameters, some activities might not be submitted the first time the script runs. For subsequent runs, the script checks for any activities that have not been submitted and attempts to submit them. It also tracks the progress of activities that have already been submitted in previous runs, producing detail and summary reports for each plan and creating or updating the file *index.html* which contains the links to the detail and summary reports. All files are stored in the directory `<WebDir>\base_name`

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 Manager Planning and Installation Guide:

User's Guide for Inventory

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

APAR IY81403

The "temporary tables" feature does not apply on Sybase and Informix®, because these 2 RDBMS vendor do not clean up the contents of a temporary table after the commit; only after releasing the session to the database. So, you will see some messages like:

```
Sybase Server Error: Msgno 3621 Level 10 State 0 Command has
been aborted due to "unique constraint violation" errors
caused by attempts to insertrows already present in the database.
```

This error can cause a decrease in performance.

User's Guide for Deployment Services

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

APAR IY84666

The section **Interrupting the Recursion of an Activity Plan** includes incorrect cross references for the **wcntpln** command. The cross references refer to the *Reference Manual for Software Distribution*, but the documentation of the **wcntpln** command is included in the *User's Guide for Deployment Services*.

IY84216

The documented level of authorization for running the **wstopapm** command is insufficient if the force option (-f) is specified. To stop the activity plan engine, interrupting operations that are running, you must have root authority in addition to the required Tivoli roles.

Reference Manual for Software Distribution

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

APAR IY85208

The description of the `execute_user_program` stanza does not include an explanation of the behavior if the timeout is set to 0.

If `execute_user_program.timeout` is equal to 0 and the user program is the last action in the software package, the timeout value set for the gateway repeater is used.

APAR IY86140

In the `wswdmgr` command description, the explanation for the option "Deadline" must be changed as follows:

Deadline: Specifies the number of hours, starting from the time the distribution is submitted, after which a distribution expires. Valid values are all integers greater than zero. For example if you schedule a distribution to start at 16:00 and the operation is executed at 15:00, the deadline is computed starting from 15:00 and not at 16:00 .

Defects 57682 and 57685

New parameters are added to the data moving command, **wspmvdta** and to the Software Distribution configuration command, **wswdcfg**, to support the customization of the source host for send E2E and delete data moving operations. Formerly , the source host for these operation was always the Tivoli server.

The new parameter in the **wspmvdata** command is **-h** and the value specified must identify a Tivoli Managed Node.

If no source host is specified in the **wspmvdata** command, the default host is used. The default host is now configurable. To set it, use the **wswdcfg** command, as follows:

```
wswdcfg -s datamoving_source_host=<managed_node_name>
```

The Tivoli server is used as the source host if no value is specified either in the **wspmvdata** or the **wswdcfg** commands

The man pages for these commands have not been updated to reflect these changes.

Defect 57811

A new parameter is added to the Software Distribution configuration command, **wswdcfg**, to support the option to enable and disable the capability to remove software packages that have not yet been installed.

The new parameter is **disable_remove_not_installed** and possible values are **y** and **n**. In the default configuration, this parameter is set to **n**, permitting the removal of software packages that have not been installed. To disable the capability to remove software package that have not been installed, issue the command:

```
wswdcfg -s disable_remove_not_installed = y
```

The man pages for this command has not been updated to reflect this change.

User's Guide for Software Distribution

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

APAR IY85208

In Chapter 15 "Troubleshooting", in the section "Setting Timeout Values for a Distribution" in the subsection called "User Program Timeout" the following information should be added after the third paragraph:

If the timeout is set to 0 and the user program is the last action in the software package, the timeout value set for the gateway repeater is used.

User's Guide for Operating System Imaging Solution

This section contains additional information for the IBM Tivoli Configuration Manager User's Guide for Operating System Imaging Solution that is not included in the manual:

Encryption of passwords in XML import files

The Operating System Imaging activities for backing up and restoring user settings include passwords. If plans that include one of these activities is defined and imported using an XML file, the password must be specified using the XML tags:

- RepClearPassword
- LocClearPassword

When these tags are used, the specified passwords are recognized as unencrypted values and are encrypted during the import process.

Software package deletion after timeout of an Update Slaves operation

If an Update Slaves operation fails during the phase when packages for

distribution are being created on the Hub server, the incomplete set of software packages must be deleted before trying the operation again.

These packages are created under the profile manager specified in the `profile_manager` parameter of the configuration file `rembo.ini`. The package names have the following format: `<timestamp>-<number>.1` or `<timestamp>-parent.1`. Locate the packages and delete them before retrying the operation.

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:

Messages and Codes

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

Software Package Editor online help

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

Man page missing updates

This section provides information about commands that have been added or changed but for which new man pages are not available.

Software distribution

- `wspmvdata`
- `wswdcfg`

The changes to these commands are documented in this readme. See “Reference Manual for Software Distribution” on page 64.

Inventory

`wcollect` `wepscan` `winvdeps` `winvmgr` `winvmigrate` `winvpackage` `winvsig`
`wloadiso` `wsetinvpchw` `wsetinvswd` `wsetinvunixhw`

- `wcollect`
- `wepscan`
- `winvdeps`
- `winvmgr`
- `winvmigrate`
- `winvpackage`
- `winvsig`
- `wloadiso`
- `wsetinvpchw`
- `wsetinvswd`
- `wsetinvunixhw`

The changes to these commands are documented in the *Configuration Manager: User's Guide for Inventory*.

License Manager Extension

The License Manager Extension changes the `winvsig` command and introduces the following new commands:

- wtlmdh
- wtlmhandler
- wtlminfoget

The new and changed commands are documented in *Configuration Manager: License Manager Extension*

Microsoft Active Directory Integration

Microsoft Active Directory Integration introduces the following new commands:

- wadquerydc
- wadquerycfg
- wadqueryrep

Documentation problems and corrections contained in previous fix packs

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 \
pdaclHostname pdmgrdPort pdaclPort 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, *ivaclcd*, 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.

Defect 57681

The guide omits guidance for the installation of the Common Inventory Technology (CIT) for Inventory.

When installing the CIT by distributing the software package **CIT.<version number>.spb**, you do not need to commit the software package. The script *CIT_import.pl*, which is used to import the software package, enables the properties **transactional** and **autocommit**.

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*.

WSUS Automated Patch Management Solution

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

Table 38. WSUS patch management files

SUS Files	WSUS Files
mssecure.cab	wsusscan.cab
mbsacl.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 synchronized
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 39. 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 40. 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 <code>resinit_one_reboot=y</code> and set it to <code>resinit_one_reboot=n</code> , 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 49.

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 **winvrnode** 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.

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.

Operator response: If inventory integration is required, use the **wswdmgr** software distribution command and the **wsetinvsd** 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.

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.