

IBM Tivoli Configuration Manager



Readme File for Fix Pack 6 - PTF U816095

Version 4.2.3

Note

Before using this information and the product it supports, read the information in "Notices" on page 97.

This edition applies to fix pack 6 (PTF U816095) for version 4, release 2, modification level 3 of IBM Tivoli Configuration Manager (program number 5724-C06)

© **Copyright International Business Machines Corporation 2003, 2008. 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-TIV-TCM-FP0006 (PTF U816095)	1
About this release	1
CD-ROM structure	1
Manuals updated in previous fix packs	4
Enhancements	4
New features in this fix pack	5
New features in the previous fix packs and interim fixes	8
Product compatibility	20
Limitations	21
Internationalization limitations	23
Product fix history	23
Fixes contained in this fix pack	23
APARs and internal defects fixed for Inventory	24
APARs and internal defects fixed for Scalable Collection Service.	27
APARs and internal defects fixed for Software Distribution	27
APARs and internal defects fixed for Activity Planner	27
APARs and internal defects fixed for Change Manager	28
APARs and internal defects fixed for the Web Interface.	28
APARs and internal defects fixed for Tivoli Web Gateway	28
APARs and internal defects fixed for the Resource Manager	28
APARs and internal defects fixed for Pristine Manager	28
APARs and internal defects fixed for Patch Management	28
APARs and internal defects fixed for Query Directory for Microsoft Active Directory - Command Line Interface	28
APARs and internal defects fixed for Query Directory for Microsoft Active Directory.	28
APARs and internal defects fixed for CM Extension for Tivoli License Manager	28
APARs and internal defects fixed for CM Endpoint Extension	29
Fixes contained in previous fix packs and interim fixes	29
Installation	37
Hardware and software requirements.	37
Supported platforms	38
System requirements	38
Upgrading large environments	38
Traditional fix pack installation methods.	39
Installing fix packs using ISMP.	39
Installing fix packs using the Tivoli desktop	40
Installing fix packs using the CLI	40
wpatch command	40
Installing fix packs using SIS	42
New components installation methods	42
Installing new components using the Tivoli desktop.	43
Installing new components using the CLI	43
winstall command	43
Installing new components using SIS	44
Software package block (SPB) fix pack installation for GUI components	45
SPB Patch Installer	49
Software Distribution server command	49
Software Distribution disconnected command	50
Software package block fix packs	50
Updating the inventory schema	51
Upgrading from a Configuration Manager 4.2.2 environment.	52
Updating the inventory queries.	53

Updating the Inventory signatures and packages	53
Creating the Active Directory schema.	53
Upgrading plug-ins.	54
Installing the Web Gateway component	54
Implementing the concurrent login feature	55
Installing the concurrent login feature	55
Configuring the concurrent login feature	55
wdepcem	60
Avoiding concurrent logins during critical distributions	64
Implementing the activity plan group management feature	66
Preparing to use the tool	66
Creating a group of activity plans	67
Submitting and tracking an activity plan group	68
Documentation notes	68
Documentation problems and corrections contained in this fix pack	68
User's Guide for Deployment Services	68
Patch Management Guide	69
User's Guide for Inventory	70
Database Schema Reference	70
Messages and Codes	72
Documentation problems and corrections contained in previous fix packs	73
Planning and Installation Guide	73
User's Guide for Deployment Services	73
Reference Manual for Software Distribution	74
User's Guide for Inventory	74
Database Schema Reference	85
Patch Management Guide	88
User's Guide for Operating System Deployment Solution	89
Tivoli Integration Pack for NetView User's Guide.	92
Messages and Codes	92
Release Notes	92
Software Package Editor online help	93
Man page missing updates	94
Notices	97
Trademarks	98

Tables

1. IBM Tivoli Configuration Manager, Version 4.2.3 Fix Pack 6 CD 1	1	32. Software Distribution APARs included from 4.2.3-TCM-FP02	33
2. IBM Tivoli Configuration Manager, Version 4.2.3 Fix Pack 6 CD 2	2	33. Software Distribution APARs and internal defects included from 4.2.3.2-TIV-TCM-IF0001	33
3. IBM Tivoli Configuration Manager, Version 4.2.3 Fix Pack 6 CD 3	3	34. Software Distribution APARs and internal defects included from 4.2.3.2-TIV-TCM-IF0002	33
4. Customer enhancement request references	5	35. Software Distribution APARs included from 4.2.3-TIV-TCM-FP0003	34
5. Customer enhancement request references	9	36. Software Distribution APARs included from 4.2.3-TIV-TCM-FP0004	34
6. Fixes included in this fix pack	23	37. Software Distribution APARs included from 4.2.3-TIV-TCM-FP0005	34
7. APARs for Inventory	24	38. Activity Planner APARs and internal defects included from 4.2.3-TCM-0001	34
8. APARs for Software Distribution	27	39. Activity Planner APARs and internal defects included from 4.2.3-TCM-FP01	35
9. APARs for Activity Planner	27	40. Activity Planner APARs included from 4.2.3-TCM-0002	35
10. APARs for Tivoli Web Gateway	28	41. Activity Planner APARs included from 4.2.3-TCM-0003	35
11. Inventory APARs and internal defects included from 4.2.3-TCM-0001	29	42. Activity Planner APARs included from 4.2.3-TCM-FP02	35
12. Inventory APARs and internal defects included from 4.2.3-TCM-FP01	29	43. Activity Planner APARs included from 4.2.3.2-TIV-TCM-IF0001	35
13. Inventory APARs included from 4.2.3-TCM-0002	29	44. Activity Planner APARs included from 4.2.3-TIV-TCM-FP0003	35
14. Inventory APARs included from 4.2.3-TCM-0003	29	45. Activity Planner APARs included from 4.2.3-TIV-TCM-FP0004	35
15. Inventory APARs included from 4.2.3-TCM-FP02	29	46. Activity Planner APARs and internal defects included from 4.2.3-TIV-TCM-FP0005	36
16. Inventory APARs and internal defects included from 4.2.3.2-TIV-TCM-IF0001	30	47. Change Manager APAR included from 4.2.3-TCM-0001	36
17. Inventory internal defects included from 4.2.3.2-TIV-TCM-IF0002	30	48. Web interface APARs included from 4.2.3-TCM-0001	36
18. Inventory APARs included from 4.2.3.TIV-TCM-FP0003	30	49. Web interface internal defect included from 4.2.3-TCM-FP01	36
19. Inventory APARs included from 4.2.3.TIV-TCM-FP0004	30	50. Web interface APAR included from 4.2.3-TCM-FP02	36
20. Inventory APARs and internal defects included from 4.2.3.TIV-TCM-FP0005	30	51. Web Interface APAR included from 4.2.3-TIV-TCM-FP0003	36
21. Scalable Collection Service APARS included from 4.2.3-TCM-0001	31	52. Web Interface APAR included from 4.2.3-TIV-TCM-FP0005	36
22. Scalable Collection Service APARS included from 4.2.3-TCM-0002	31	53. Resource Manager internal defects included from 4.2.3-TCM-FP01	36
23. Scalable Collection Service APARS included from 4.2.3-TCM-FP02	31	54. Pristine Manager APAR included from 4.2.3-TCM-0001	36
24. Scalable Collection Service APARS included from 4.2.3.2-TIV-TCM-IF0001	31	55. Patch Management internal defects included from 4.2.3-TCM-0001	36
25. Scalable Collection Service APAR included from 4.2.3-TIV-TCM-FP0003	31	56. Patch Management internal defects included from 4.2.3-TCM-FP01	37
26. Scalable Collection Service APARS included from 4.2.3-TIV-TCM-FP0004	31	57. Patch Management APARs included from 4.2.3.2-TIV-TCM-IF0001	37
27. Scalable Collection Service APARS included from 4.2.3-TIV-TCM-FP0005	31	58. Patch Management APARs included from 4.2.3-TCM-FP02	37
28. Software Distribution APARs and internal defects included from 4.2.3-TCM-0001	31	59. Directory Query APAR included from 4.2.3-TCM-0001	37
29. Software Distribution APARs and internal defects included from 4.2.3-TCM-FP01	32		
30. Software Distribution APARs included from 4.2.3-TCM-0002	32		
31. Software Distribution APARs included from 4.2.3-TCM-0003	33		

60.	Query Directory for Microsoft Active Directory internal defects included from 4.2.3.2-TIV-TCM-IF0001	37	67.	SQL scripts for updating the Historical Inventory schema	51
61.	Space requirements for the License Management Extension	38	68.	WSUS patch management files	75
62.	IND files included in this fix pack	41	69.	Versions of VMware supported by CIT	77
63.	IND files included in this fix pack	43	70.	Enabler executable files	77
64.	Default variables defined in SPB fix packs	45	71.	Enabler return codes	78
65.	Names of SPB files and software profiles	50	72.	Commands and configuration files on Windows platforms	80
66.	SQL scripts for updating the Inventory schema	51	73.	Commands and configuration files on UNIX platforms	80
			74.	Return codes	81

IBM Tivoli Configuration Manager 4.2.3 ReadMe File for Fix Pack 4.2.3-TIV-TCM-FP0006 (PTF U816095)

This readme file provides important information about Fix Pack 6 (PTF U816095) 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.

The Common Inventory Technology (CIT) level distributed in this fix pack is 2.5.1003 (build level 20080218v2.5).

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

About this release

This section includes the following topics:

- “CD-ROM structure”
- “Manuals updated in previous fix packs” on page 4
- “Enhancements” on page 4
- “Product compatibility” on page 20
- “Limitations” on page 21
- “Product fix history” on page 23

CD-ROM structure

IBM Tivoli Configuration Manager, Version 4.2.3 Fix Pack 6 includes **three** CD-ROMs as detailed in the following tables:

Table 1. IBM Tivoli Configuration Manager, Version 4.2.3 Fix Pack 6 CD 1

Directory or path	Contents
/xml	The XML file to be used by the ISMP installation program.
/docs	Readme file.
/cit_enabler	Enabler for Inventory scan on VMware environments.
/CIT_SPB	Software package block (SPB) files used to upgrade the CIT component to version 2.5.1003.
/dii	Files required for the Discovery Library Integration Framework Plug-in for Tivoli Configuration Manager.
/dla	Files required for the Tivoli Configuration Manager 7.1 Discovery Library Adapter.
/images/INVENTORY	Images required for Inventory fix pack.
/images/MCOLLECT	Images required for the Scalable Collection Services fix pack.

Table 1. IBM Tivoli Configuration Manager, Version 4.2.3 Fix Pack 6 CD 1 (continued)

Directory or path	Contents
/images/SWD	Images required for Software Distribution, Activity Planner, Change Manager, Tivoli Resource Manager, Patch Management, Pristine Manager, Directory Query, Web User Interface, Query Directory for Microsoft Active Directory, Query Directory for Microsoft Active Directory-Command Line Interface, CM Endpoint Extension, CM Extension for Tivoli License Manager fix pack, and Tivoli Provisioning Manager for Operating System Deployment Integration.
/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.
/NewComponents/AD_INTEGRATION	Images required for Microsoft® Active Directory integration.
/NewComponents/EXTENSION	Images required for the license management extension
/NewComponents/TPMOSD	Images required to install Image Management Services.
/rad	The RAD file required to install Tivoli Provisioning Manager for Operating System Deployment.

Table 2. IBM Tivoli Configuration Manager, Version 4.2.3 Fix Pack 6 CD 2

Directory or path	Contents
/tools/LoginControl	Software package block (SPB) and executable files used to implement the concurrent login feature. For more information on this feature, see “Enhancements” on page 4.
/tools/JarVersion	Scripts to retrieve and display the version of the jar files currently installed.
/tools/apm_reporting	Files to implement the Activity plan group creation, submission, and tracking. For more information, see “Implementing the activity plan group management feature” on page 66.
/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.
/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 Prerequisite 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> .

Note: The /PocketPC folder, existing in previous fix packs, has been removed because the fix related to APAR IY75778 has been implemented in the Tivoli

Web Gateway installation images, located under the /twg_installer directory.

Table 3. IBM Tivoli Configuration Manager, Version 4.2.3 Fix Pack 6 CD 3

Directory or path	Contents
/twg_installer	Installshield program used to install the Tivoli Web Gateway component.

Manuals updated in previous fix packs

The following manuals have been updated with the new features of Tivoli Configuration Manager 4.2.3 Fix Pack 3:

- *IBM Tivoli Configuration Manager: Planning and Installation Guide*. It describes how to install Tivoli Web Gateway fix pack 3.
- *IBM Tivoli Configuration Manager: User's Guide for Software Distribution*. It describes how to use the Nokia s60 device actions.
- *IBM Tivoli Configuration Manager: Reference Manual for Software Distribution*. It describes the new supported actions for Nokia s60 devices.
- *IBM Tivoli Configuration Manager: User's Guide for Deployment Services*. It describes how to enable security for Nokia s60 devices.
- *IBM Tivoli Configuration Manager: Patch Management Guide*. It describes how to define filters for grouping endpoints and deploy the security patches to those groups of endpoints. It also describes how to use the new Microsoft .cab file.
- *IBM Tivoli Configuration Manager: User's Guide for Operating System Deployment Solution*. It describes how to implement an operating system imaging solution based on an IBM Tivoli Configuration Manager and Tivoli Provisioning Manager for Operating System Deployment environment.
- *IBM Tivoli Configuration Manager: License Management Extension*. It describes how to provide license management facilities in your Configuration Manager environment.
- *IBM Tivoli Configuration Manager: License Management with License Compliance Manager version 2.3*. It describes installation and upgrade procedures for implementing license management facilities from IBM Tivoli License Compliance Manager Version 2.3 into the Configuration Manager environment.
- *IBM Tivoli Configuration Manager: User's Guide for Inventory*. It describes how to install and uninstall the Common Inventory Technology component.
- *IBM Tivoli Configuration Manager: Database Schema Reference*. It describes new queries, tables, and views related to new enhancements such as the Nokia s60 support.
- *IBM Tivoli Configuration Manager: Release Notes*. It describes the supported operating systems and databases.

You can find the updated manuals on the Tivoli software information center Web site. Access the Tivoli software information center by first going to the Tivoli software library at the following Web address:

<http://publib.boulder.ibm.com/tividd/td/link/tdprodlist.html>.

Click **Tivoli product manuals**. In the Tivoli Technical Product Documents Alphabetical Listing window, click **IBM Tivoli Configuration Manager**, to access your product library at the Tivoli software information center.

Enhancements

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

- “New features in this fix pack” on page 5
- “New features in the previous fix packs and interim fixes” on page 8

New features in this fix pack

The following enhancements have been introduced in this fix pack:

Table 4. Customer enhancement request references

	Enhancement	Reference
APM	Targets resolved by APM Executer and no longer by APM Handler	59552
Patch Management	WSUS 3.0 support	59432
	Windows 2008 endpoint support (1)	
New Endpoint support	Windows 2008 support	
	AIX 6.1 support	
DLA support	TCM Discovery Library Adapter v7.1	
New component (connector)	Discovery Library Integration Framework Plug-in for Tivoli Configuration Manager	
Software distribution	Add scripts as arguments in sp_val_operation for data moving operations	59700
	Ignore option extended to targets not scanned	59702

Note: (1) No operating system patches are supported, only patches related to software applications.

Targets resolved by APM Executer and no longer by APM Handler - Feature 59552

To fully use this enhancement, activity plans must be submitted with target resolution at plan submission and not at activity execution.

To enable this feature, add the following entry to the `apm.ini` file:

```
resolve_targets_in_executer=yes
```

in the [ENGINE_TUNING] section of the file.

Enabling this feature, the Activity Planner Handler can now handle other activity plan actions, while the targets are being resolved by the Activity Planner Executer.

WSUS 3.0 support - Feature 59432

Prerequisites for using WSUS version 3.0 are the following:

1. Install the "Microsoft SQL Server Native Client" from the Microsoft Web site.
2. Install the "Microsoft SQL Server 2005 Command Line Query Utility" from the Microsoft Web site.
3. Set the two `wseccfg` command parameters as follows:
 - `wsus_db_host=\\.\pipe\MSSQL$MICROSOFT##SSEE\sql\query`
 - `wsus_version=3`

With this feature the `WSUS_info_retriever.sh` script has been modified to accept the `-v3` new parameter.

Windows 2008 endpoint support for Patch Management

Endpoints having Windows 2008 installed are now supported among the targets managed by the Patch Management solution. On these targets, no

operating system patches are supported, only patches related to software applications. The support for operating system patches is deferred until an operating system patch is provided for testing purposes.

Windows 2008 and AIX 6.1 support

The endpoint support has now been extended to endpoints having the following Windows platforms installed:

- Windows Server 2008 Standard (ix86 only)
- Windows Server 2008 Enterprise (ix86 only)

and to endpoints having the AIX platform version 6.1 installed.

This extended support is for endpoints only. Web Interface and GUI functions are not supported on these platforms, because Java version 1.3.1 is not supported.

Install the Windows 2008 and AIX 6.1 endpoint using the endpoint setup released with the following patch:

4.1.1-LCF-0051.

TCM 7.1 Discovery Library Adapter (DLA) support

This Discovery Library Adapter (DLA) collects data from Tivoli Configuration Manager 4.2.3 and creates Discovery Library books containing information about the resource instances and their relationships known to the system. The Discovery Library books can be imported into CCMDB or into a data store for which a Discovery Library Reader exists.

This DLA package is located on the Tivoli Configuration Manager Version 4.2.3 Fix Pack 6 CD 1 under the `/dla` directory.

For more details about the DLA package, refer to the *Readme* contained in the zip file named **TCM_DLA.zip** stored on the Tivoli Configuration Manager Version 4.2.3 Fix Pack 6 CD 1 under the `/dla` directory.

Discovery Library Integration Framework Plug-in for Tivoli Configuration Manager

The Discovery Library Integration Framework provides a set of reusable software components which work together to perform discoveries of Configuration Items (CIs) that are to be maintained by CCMDB. The plug-in for Tivoli Configuration Manager is responsible for discovering the CIs specific to the Tivoli Configuration Manager product.

This plug-in is located on the Tivoli Configuration Manager Version 4.2.3 Fix Pack 6 CD 1 under the `/dii` directory.

For more details about the plug-in, refer to the *User's Guide* contained in the zip file named **TDI_CCMDB_TCM_plugin1.2.zip**. The file name for the User's Guide is **TDI_CCMDB_TCM_plugin_UserGuide.pdf**.

Add scripts as arguments in `sp_val_operation` for data moving operations - Feature 59700

Add the pre- and post-scripts to the arguments that the data moving operation passes to the **sp_val_operation** validation policy script. For more details about the **sp_val_operation** validation policy, refer to the *IBM Tivoli Configuration Manager: Reference Manual for Software Distribution*. With this feature the arguments that the data moving operation passes to the **sp_val_operation** validation policy script are the following:

For the **Delete** operation:

```

$1 --> DataMovingRequests.1
$2 --> delete
$3 --> <target_path>
$4 --> <file>
$5 --> SCRIPT_LIST
<stdin> --> <target endpoint list>

```

For the **Send** operation:

```

$1 --> DataMovingRequests.1
$2 --> send
$3 --> <source_path>
$4 --> <target_path>
$5 --> <file>
$6 --> <source_host>
$7 --> SCRIPT_LIST
<stdin> --> <target endpoint list>

```

For the **Retrieve** operation:

```

$1 --> DataMovingRequests.1
$2 --> retrieve
$3 --> <source_path>
$4 --> <target_path>
$5 --> <file>
$6 --> <source_host>
$7 --> SCRIPT_LIST
<stdin> --> <target endpoint list>

```

For the **Endpoint to Endpoint** operation:

```

$1 --> DataMovingRequests.1
$2 --> retrieveE2E
$3 --> <source_path>
$4 --> <target_path>
$5 --> <file>
$6 --> <source_endpoint>
$7 --> SCRIPT_LIST
<stdin> --> <target endpoint list>

```

where: **SCRIPT_LIST** is a single argument which contains the following four lines:

```

spre:<spre_script>
spost:<spost_script>
tpre:<tpre_script>
tpost:<tpost_script>

```

separated by the `\r` character.

On UNIX platforms, a direct "echo" of the entire **SCRIPT_LIST** causes the following behavior: every line is written above the previous one, because `\r` represents the carriage return. For this reason you can only see the last line of the script.

You must create a validation script to extract the four lines contained in the **SCRIPT_LIST** argument. For example, for a **Retrieve** operation on Solaris platforms, a simple way to do this is as follows:

```

echo $7 | awk -F'^M' '{print $1"\n"$2"\n"$3"\n"$4}' | while read a
do
  <use $a variable that contains a single line>
done

```

where:

^M Does not represent the characters `^` and `M`. It represents the sequence of the `ctrl-v` and `ctrl-m` key combinations.

Another example of how to create the validation script is the following:

```
echo $7 | awk '{n=split($0, v, "\n"); print v[1]"\"v[2]"\"v[3]"\"v[4]}'
| while read a
do
  <use $a variable that contains a single line>
done
```

Ignore option extended to targets not scanned - Feature 59702

The **ignore** option for the remove operation has been extended to targets which have not been scanned and do not have an entry in the COMPUTER table. If a remove operation is performed on mixed targets (some have an entry in the COMPUTER table while others do not) by the Activity Planner using the **ignore** option (-I), the targets that do not have an entry in the COMPUTER table are skipped, and the remove operation proceeds with the targets that have been scanned. In the software package log file, the following error message is displayed for the targets that do not have an entry in the COMPUTER table:

```
DISSE0072E List of targets on which the requested operation cannot be
submitted:
endpoint_name DISSE0407E Failed cm_status check.
```

You must take remediation actions on these targets by either running a scan on them, or by sending a dummy software package before performing a remove operation on them. If the remove operation is performed by the Activity Planner, a target on which the validation fails shows the "success" state. If you want a validation failure to be considered as a failure, also by the Activity Planner, you must set the **FailOnValidationFailure** option using the Activity Planner, in addition to the **ignore** option. In case of mixed targets, scanned and not scanned, the DISSE0329E error message keeps displaying if you do not use the **ignore** option. The text of the error message has been changed as follows:

```
DISSE0329E Mixed targets (with an entry in COMPUTER table and without
an entry) are not allowed in the remove operation if the force option
is not set. Use the ignore option to skip the not scanned targets or
submit two different requests or perform a scan for all targets.
```

Also, the text of the DISSE0330E error message has been changed as follows

```
DISSE0330E Remove operation for targets having a different package state
in the Inventory database is not allowed if the force option is not set.
You can use the ignore option to skip the not installed targets if you
disable the remove_not_installed by running
wswdcfg -s disable_remove_not_installed=y.
```

to indicate the possibility of using the **ignore** option to skip the non-installed targets, if you disable the **remove_not_installed** option by running the following command:

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

Using this setting, you do not receive the DISSE0330E error message in case of mixed targets, installed and not installed.

New features in the previous fix packs and interim fixes

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

Table 5. Customer enhancement request references

	Enhancement	Reference
New component	Tivoli Configuration Manager license management extension	
	Active Directory integration	
	Tivoli Provisioning Manager for Operating System Deployment integration	58233
	Tivoli Provisioning Manager for Operating System Deployment internationalized	
New platform	Solaris x86 support	
New Endpoint support	Windows Vista support	
APM	Search facility for saved activity plans	MR124044922
	Activity plan group creation, submission, and tracking	
	Immediate start for unique targets in conditioned activities	56060
	Cancel as preferred final status for a plan	56137
	Displaying the .jar files version	55204
	Displaying the patch level for the Activity Plan Editor and Activity Plan Monitor	55205
	Configure the Ignore option results	58122
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	
	Enabling TCM-TPM coexistence	
	Send a Tivoli notice managing lcf script package attributes	
	New 32-bit MRMBIOS.EXE	180357
	Virtual resource scan	MR0508067421
	Multi core support	MR0826056352
	Collect real and virtual network adapters	205563
	VMware host serial number	205720
	Collect LPAR information in a VMware environment	205561
CCM	Stop on failure check box	

Table 5. Customer enhancement request references (continued)

	Enhancement	Reference
Patch Management	Emergency patch management	56053
	Patch Management deployment paradigm	56053
	Completing workflows separately	55260
	Performing patch management using WSUS	55317
	Patch Management extension	
	Patch automation for target filtering	MR0404064528
	New Microsoft catalog and WUA support	
	New options supported by wsubpln command: submit_plans	MR0503066815
	New options supported by wsubpln command: skip_plans_creation	MR0414062811
Software distribution	Enable Move Data to retrieve AS/400® spool file	56336
	Avoiding concurrent logins during critical distributions	54613
	Performing the logoff operation on Windows endpoints	55186
	Customize the source host	
	Enabling TCM-TPM coexistence	
	Send a Tivoli notice managing lcf script package attributes	
	Maintaining the access attributes of already existing files and directories on a UNIX® target, a new attribute (preserve_unix) is available	55359
	Running a program before the reboot of a commit	55409
	Managing software packages	55487
	Working with the Software Distribution Endpoint Notification dialog	55522
	Add "defer" as possible default_action	IY92880
Tivoli Web Gateway	Nokia s60 devices support	
	Nokia 9300i devices support	

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 55.

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 68.

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 68.

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*.

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, mrmmbios.exe, substitutes the 16 bit scanner - Feature 180357

With this feature the Windows 64-bit platforms support has been extended. The old 16-bit `mrmmbios.exe` file has been now replaced by a 32-bit file having the same name, and using new device drivers. The new `mrmmbios.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.

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 66 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.

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.

Enabling Tivoli Configuration Manager - Tivoli Provisioning Manager coexistence

A new resource, ReportManager, has been included in Software Distribution product. It is needed to enable the Tivoli Configuration Manager - Tivoli Provisioning Manager coexistence. ReportManager is used to provide the reports to Tivoli Provisioning Manager when distributions are initiated by Tivoli Provisioning Manager itself. To enable the integration, the \$BINDIR/TME/ReportManager/rep_DB_Vendor.sql script must be executed to update the inventory database. Supported database vendors are DB2 and Oracle.

Send a Tivoli notice managing lcf script package attributes

For Software Distribution a Tivoli notice is sent each time a value related to the following package attributes is enabled during the import operation, or changed when re-importing or using the wsetspgs command. The change can be performed using both SPEDITOR or command line interfaces. The notice is not sent if the value remains the same.

This is the list of the existing attributes for which the notice is activated with the current feature:

- lcf_before_prog_path
- lcf_before_prog_args
- lcf_before_prog_timeout
- lcf_after_prog_path
- lcf_after_prog_args
- lcf_after_prog_timeout

For Inventory a tivoli notice is sent to the inventory notice group, when the (after and/or before) script content for unix (and/or pc) of an InventoryConfig profile changes. For Inventory four different messages have been added: one for every script content that changes. The message is related to one of the following four scripts:

- the before script for pc
- the after script for pc
- the before script for unix
- the after scripts for unix

Customize the source host for Data Moving endpoint to endpoint

With this feature the source host for Data Moving endpoint to endpoint send and delete operations is not necessarily the Tivoli server anymore. With this feature the source host can be customized. A default value can be set using the following command:

```
wswdcfg -s datamoving_source_host=ManagedNode name
```

Nokia s60 support

With this feature, the Nokia device support has been extended. IBM Tivoli Configuration Manager now supports Nokia s60 devices. The entire set of functions already supplied for the Nokia 9500 and Nokia 9300 devices is supported. Moreover some new functions are supported only for Nokia s60 devices. This means:

- The ability of defining the device using TRM
- The ability of creating and managing software packages capable of performing device provisioning, device management, application distribution, and notification actions
- The ability of managing all the supported configuration options when performing device management operations
- The ability of performing the following actions:
 - TARM config
 - wipe
 - reboot
 - process listing
 - process stop
 - generic
- The ability of performing hardware, software, and configuration scanning of the Nokia s60 device.

Virtual resource scan - Feature MR0508067421

With this feature, it is possible to report the virtual SCSI devices assigned to a logical partition, only for AIX platforms. When running an Inventory hardware scan to discover storage devices on a logical partition of an AIX workstation, the virtual SCSI devices are now reported in the

STORAGE_DEV_QUERY, which displays the new storage device type called "Virtual Disc". The operating systems for which this information can be discovered are the following:

- IBM AIX 5.2 (32-bit and 64-bit)
- IBM AIX 5.3 (32-bit and 64-bit)

Multi core support - Feature MR0826056352

With this feature, it is possible to report the correct number of physical processors, logical processors assigned to each core, and the cores on the physical processor in the inventory tables, views, and queries. A multi-core processor is one that combines two or more independent processors into a single package. The operating systems for which this information can be discovered by the Common Inventory Technology are the following:

- AIX
 - IBM AIX 5.2 (32-bit and 64-bit)
 - IBM AIX 5.3 (32-bit and 64-bit)
- HP-UX
 - HP-UX 11i PA-RISC
 - HP-UX 11i for Itanium
- Linux
 - Red Hat Enterprise Linux 3.0 (U1) AS/ES/WS for i386
 - Red Hat Enterprise Linux 4.0 AS/ES/WS for i386
 - Red Hat Enterprise Linux 4.0 x86_64 AS/ES/WS
 - Red Hat Enterprise Linux 3.0 (U2) (AS) PPC for iSeries and pSeries 64-bit (AS)
 - Red Hat Enterprise Linux v4.0 PPC for iSeries and pSeries 34-bit (AS)
 - Red Hat Enterprise Linux 3.0 (U1) s390/s390x for S/390 and zSeries (AS)
 - Red Hat Enterprise Linux 4.0 s390/s390x for S/390 and zSeries (AS)
 - SuSE Linux Enterprise Server 8 (SP2a) for i386
 - SuSE Linux Enterprise Server 9 for i386
 - SuSE Linux Enterprise Server 9 for x86_64
 - SuSE Linux Enterprise Server 8 (SP3) PPC for iSeries and pSeries 64-bit
 - SuSE Linux Enterprise Server 9 PPC for iSeries and pSeries 64-bit
 - SuSE Linux Enterprise Server 8 s390/s390x for S/390 and zSeries
 - SuSE Linux Enterprise Server 9 s390/s390x for S/390 and zSeries
 - SuSE Linux Enterprise Server 10 for i386
 - SuSE Linux Enterprise Server 10 for x86_64
 - SuSE Linux Enterprise Server 10 s390/s390x for S/390 and zSeries
 - SuSE Linux Enterprise Server 10 PPC for iSeries and pSeries 64-bit
- Sun Solaris
 - Sun Solaris 8 SPARC (32-bit and 64-bit)
 - Sun Solaris 9 SPARC (32-bit and 64-bit)
 - Sun Solaris 10 SPARC (32-bit and 64-bit)
 - Sun Solaris 10 x86
- Windows
 - Windows 2000 Professional/Server/Advanced Server (SP3)

- Windows XP Professional (32-bit)
- Windows 2003 Server (Standard and Enterprise Editions)
- Windows 2003 x64 (Standard and Enterprise Editions)
- Windows Vista (Desktop)

Patch automation for target filtering - Feature MR0404064528

With this feature, you can define filters for grouping endpoints and deploy the security patches to these groups of endpoints. It is now possible to define filters based on the information already available in the Inventory database, and also to create groups of endpoints using the new `wsecgrp` command. For more details on this command, see the IBM Tivoli Configuration Manager: Patch Management Guide.

New Microsoft catalog and WUA support

You can perform patch management also using the new Microsoft .cab file and its associated WUA. For details see the IBM Tivoli Configuration Manager: Patch Management Guide.

New options supported by the `wsubpln` command - Features MR0503066815 and MR0414062811

The `wsubpln` command now supports the following new options:

submit_plans

If this option is enabled, an automatic plan submission occurs immediately after the plan creation.

skip_plans_creation

If this option is enabled, the plan is created at the end of the workflow.

For more details on this command, see the IBM Tivoli Configuration Manager: Patch Management Guide.

Tivoli Provisioning Manager for Operating System Deployment integration - Feature 58233

This fix pack provides the integration with the product Tivoli Provisioning Manager for Operating System Deployment Version 5.1 through the new component Tivoli Provisioning Manager for Operating System Deployment integration Version 4.2.3. Only English version is currently available, the localized versions will be available in the next fix pack. This integration replaces the old "Image Management Services Integration, Version 4.2.3" released with fix pack 2, that needs to be uninstalled before installing the Tivoli Provisioning Manager for Operating System Deployment integration. For more details, refer to the IBM Tivoli Configuration Manager: User's Guide for Operating System Deployment Solution.

Windows Vista support

The endpoint support has now been extended to endpoints having the Windows Vista platform installed. As prerequisite, you must install the following Framework patch on the Windows Vista endpoints of your environment:

4.1.1-LCF-0042

The Web Interface component is not supported on Windows Vista endpoints.

Configure the Ignore option results in APM - Feature 58122

A new check box has been added to customize the behavior of the Activity

Planner Monitor for those targets failing the CM_STATUS validity check for a software distribution (SWD) activity when the "Ignore" option is set. This new check box will be enabled only when the "Ignore" check box is set. When the check box is set, all targets on which the validation fails will be marked as 'failed'. If this check box is not checked (default) the old behavior will be in effect: targets for which the validation failed will be marked as successful.

Add "defer" as possible default_action - Feature IY92880

When a software distribution is performed specifying some options in the User Notification Settings panel, not only "accept" and "reject" can be selected as default action, but also "defer". The default action is the action that is run after the specified timeout if no changes are performed on the User Notification Settings panel.

Nokia 9300i devices support

With this feature, the Nokia device support has been extended. IBM Tivoli Configuration Manager now supports Nokia 9300i devices. For these new devices, the same set of functionalities of the Nokia 9300 devices is supported.

Tivoli Provisioning Manager for Operating System Deployment internationalized

With this feature, the Tivoli Provisioning Manager for Operating System Deployment product has been internationalized. To enable this feature, install SWD_L10N under the /images path and the Tivoli_APM_GUI_L10N_Fix.v4.2.3.FP04.spb software package block under the /packages path.

Collect real and virtual network adapters - Feature 205563

The network adapter table needs to differentiate between real and virtual adapters. A new table ALL_NET_ADAPTER (H_ALL_NET_ADAPTER) having ADAPTER_ID and COMPUTER_SYS_ID as fields was created. New views (ALL_NET_CARD_VIEW, H_ALL_NET_CARD_VIEW) and new queries (ALL_NET_CARD_QUERY, H_ALL_NET_CARD_QUERY) were also created.

VMware host serial number - Feature 205720

Scanning a Windows VMware guest workstation, Inventory reports the serial number of the VMware host in the SERIAL NUMBER column of the LPAR view.

Collect LPAR information in a VMware environment - Feature 205561

Inventory now uses the Common Inventory Technology (CIT) capability to collect LPAR information in a VMware environment. CIT provides an enabler to export correct data to the guest systems so that CIT instances installed on each operating system partition can discover and return correct data. The enabler is provided to bypass current limitations of some virtualization software and should not be seen as a standard part of the Inventory offering.

Product compatibility

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

IBM Tivoli Configuration Manager, Version 4.2.3 fix pack 4.2.3.-TIV-TCM-FP0006 was tested using:

- Tivoli Management Framework, Version 4.1.1 plus the following interim fixes:
 - 4.1.1-LCF-0049 to be installed on the Tivoli gateways.
 - 4.1.1-TMF-0091 to be installed on the managed nodes with JRIM and JCF components installed.
 - 4.1.1-TMF-0090 to be installed on Tivoli servers, managed nodes, and gateways.
- Tivoli Management Framework interim fix 4.1.1-TMF-0075LA to be installed on Tivoli servers and managed nodes with JAVA components installed.
- Tivoli Provisioning Manager for Software, version 5.1
- Tivoli Provisioning Manager for Operating System Deployment , version 5.1 plus fix pack 1
- The license management extension for IBM Tivoli Configuration Manager version 4.2.3 fix pack 5 can be implemented using one of the following supported releases:
 - IBM Tivoli License Compliance Manager, Version 2.2 plus fix pack 3.
 - IBM Tivoli License Compliance Manager, Version 2.3 plus fix pack 2.

Limitations

Defect 59806: A patch installation might fail with exit code 1641. The workstation is automatically rebooted, and the patch installation is completed when the workstation restarts. If the patch installation was performed using an activity plan, also the activity plan fails. Use the **wsecrprt** command to verify the patch installation.

Defect 59828: An activity plan for installing Microsoft service packs might fail. In the Software Distribution log file, one or more patches, contained in the service pack, fail with exit code 1642. This exit code does not mean that the service pack installation has failed, it means that the specific patch is not needed as the specific software module you are trying to upgrade is not present.

Defect 59811: The "2007 Microsoft Office Suite Service Pack 1" installation fails. If you perform a query in Patch Management using the **wsecrprt** command, the patch is missing. Despite this error, in most cases the patch has been installed correctly. Verify the patch installation from the **Add or Remove Programs** list of the Windows operating system. A ticket has been opened to Microsoft for this software limitation.

APAR IZ16608: If you have problems because the 64-character size of the **KEYBOARD_TYPE** column of the **COMPUTER** table is too small, the fix introduced by **APAR IY68842** with Tivoli Configuration Manager Version 4.2.3 Fix Pack 4, which enlarges the **KEYBOARD_TYPE** column to 128 characters, does not apply if the following conditions are met:

- You have installed Tivoli Configuration Manager Version 4.2.3 without migrating from previous versions.
- You have run the SQL fresh install scripts before installing Tivoli Configuration Manager Version 4.2.3 Fix Pack 4.

In this case you can solve this issue by running from the database vendor interface the following SQL statement against the Inventory database:

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

APAR IY88658: The SSL connection is not supported for the Enterprise Directory Query component.

Defect 58552: When running an activity plan to install a patch on a Windows 2000 Advanced Server, the patch installation might fail with exit code 1. The problem is generated by the way parameters are parsed by the operating system.

As a workaround to successfully install the patch, you must modify the `inhibit_parsing` key. Inhibit parsing prevents the standard parsing of the values passed to the patch installation script. To modify the value of the `inhibit_parsing` key, perform the following steps:

1. In the Patch Management policy region locate the patch you are trying to install and unbuild it by converting the software package
2. Launch the Software Package Editor and edit the Execute Program object named `$(temp_dir)\Hotfix\$(EXE)`
3. Select **Advanced**
4. Clear the **Inhibit Parsing** check box
5. Save and close the modified software package
6. Rebuild the software package by converting it
7. Distribute the software package only to the endpoints on which the distribution failed previously.

Refer to the *IBM Tivoli Configuration Manager: Reference Manual for Software Distribution* and *IBM Tivoli Configuration Manager: User's Guide for Software Distribution* for more information about the inhibit parsing option.

Defect 201407: If the Common Inventory Technology (CIT) package is installed on the endpoint in transactional mode, and the following commit operation is not performed or fails, a subsequent transactional installation of the same package fails with RC=10.

To avoid this problem, before installing CIT, you must perform the commit operation or manually uninstall CIT. This problem might occur especially when you install CIT through an inventory scan.

Defect 200891: After the installation of this fix pack, the first distribution of an Inventory Profile might end showing an error message. This happens when the profile is configured to run a hardware scan with Data Options set as "Update with differences" and on the endpoint there is already the `tivhscan.bk1` file. The encountered error is the following:

```
Q MethInit ** Exception caught in run_impl: MIF parse error:  
Type mismatch for group.
```

The problem does not occur when distributing an Inventory Profile configured to run a hardware scan with Data Options set as "Replace with current results".

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 3, 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 58779: In the Distribution Status Monitor and Activity Planner Monitor GUIs running with JRE 1.3.1 on Windows Vista, the time is always displayed in GMT time zone. This is a bug of JRE 1.3.1 on Windows Vista operating system: the `TimeZone.getDefault()` method returns GMT no matter the operating system locale. As a result, all Java GUIs on Windows Vista have this problem.

Defect 58827: Message sent to the Activity Plan Monitor and stored in the activity plan database are truncated if their length is greater than the length defined in the schema. All the messages, except for Tivoli Provisioning Manager for Operating System Deployment messages, are truncated at the end. The Tivoli Provisioning Manager for Operating System Deployment messages are truncated at the beginning since they start with the copyright information that is not useful for the error explanation.

Internationalization limitations

Defect 58877: Messages displayed in **Error Messages** when you monitor an IBM Tivoli Provisioning Manager for Operating System Deployment plan, by selecting a target and then **Show/Hide Details** from the pull-down menu of the Activity Plan Monitor GUI, are sometimes in English.

Defect 58757: The Tivoli Provisioning Manager for Operating System Deployment messages that are displayed in the Activity Plan Monitor after you submit a plan are garbled. **Workaround:** You can either change the language of Tivoli Provisioning Manager for Operating System Deployment to English or open the `rbagent.log` log and search the corresponding error message.

Defect 58916: When a DB2 error occurs on Tivoli Provisioning Manager for Operating System Deployment in non-English environment, the DB2 error message shown in Activity Plan Monitor might be garbled. This is due to a known problem of IBM Tivoli Provisioning Manager for Operating System Deployment fix pack 1. To identify the error look for the DB2 message ID and SQL code in the DB2 message reference.

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 29

Fixes contained in this fix pack

Table 6 lists the fixes included in this fix pack:

Table 6. Fixes included in this fix pack

Fix pack	Component/Service
4.2.3-TIV-INV-FP0006	Inventory, Version 4.2.3
4.2.3-TIV-INVGW-FP0006	Inventory Gateway, Version 4.2.3
4.2.3-TIV-CLL-FP0006	Scalable Collection Service, Version 4.2.3

Table 6. Fixes included in this fix pack (continued)

Fix pack	Component/Service
4.2.3-TIV-SWDSRV-FP0006	Software Distribution, Version 4.2.3
4.2.3-TIV-SWDGW-FP0006	Software Distribution Gateway, Version 4.2.3
4.2.3-TIV-SWDJPS-FP0006	Software Distribution Software Package Editor, Version 4.2.3
4.2.3-TIV-APM-FP0006	Activity Planner, Version 4.2.3
4.2.3-TIV-CCM-FP0006	Change Manager, Version 4.2.3
4.2.3-TIV-WEB-FP0006	Web Interface, Version 4.2.3
4.2.3-TIV-TRMSRV-FP0006	Resource Manager, Version 4.2.3
4.2.3-TIV-TRMGW-FP0006	Resource Manager Gateway, Version 4.2.3
4.2.3-TIV-PMSRV-FP0006	Pristine Manager, Version 4.2.3
4.2.3-TIV-PMG-FP0006	Patch Management, Version 4.2.3
4.2.3-TIV-DQY-FP0006	Directory Query, Version 4.2.3
4.2.3-TIV-ADICLI-FP0006	Query Directory for Microsoft Active Directory - Command Line Interface, Version 4.2.3
4.2.3-TIV-ADIENG-FP0006	Query Directory for Microsoft Active Directory, Version 4.2.3
4.2.3-TIV-TLMEXT-FP0006	CM Extension for Tivoli License Manager, Version 4.2.3
4.2.3-TIV-CMEXT-FP0006	CM Endpoint Extension, Version 4.2.3
4.2.3-TIV-TPOSD-FP0006	Tivoli Provisioning Manager for Operating System Deployment Integration, Version 4.2.3

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

Table 7. APARs for Inventory

Inventory, Version 4.2.3, 4.2.3-TIV-INV-FP0006 and 4.2.3-TIV-INVGW-FP0006				
IZ11136	IZ12162	IZ12656	IZ12695	IZ13300
IZ14763	IZ15108	IZ15654		

APAR IZ11136

Abstract:

Native software scan does not handle DBCS fields

Error Description:

When performing the native software scan on workstations which return strings containing double-byte characters, the collected data is not inserted into the Inventory database due to the following failure:

```
00005368 Tue Nov 20 17:44:29 2007 Connection ID: 0, Operation:
val_insert_rows::SQLExecute, DB Call: insert into NATIV_SWARE
(NATIV_ID, PACKAGE_NAME, PACKAGE_VERS, PUBLISHER, PACKAGE_ID)
values (?,
?, ?, ?, ?)
SQL Command: insert into NATIV_SWARE (NATIV_ID, PACKAGE_NAME,
PACKAGE_VERS, PUBLISHER, PACKAGE_ID) values (?, ?, ?, ?, ?)
```

MS SQL Error: Msgno 8152 Level 8152 State
815222001 Microsoft ODBC SQL
Server Driver SQL Server String or binary data would be
truncated.

Additional information:

The problem is caused by the size of the **package_name** field of the temporary table **#NATIV_SWARE**. The field is too small to handle double-byte character (DBCS) values. The temporary table **#NATIV_SWARE** was still created using the **PACKAGE_NAME (64)** column instead of using **PACKAGE_NAME(128)** .

APAR IZ12162

Abstract:

inv_config_ep_meths process uses 100% CPU if running **wcancelscan** while downloading signatures

Error Description:

The **inv_config_ep_meths** process shows 100% CPU usage on the target workstation and it hangs. This issue occurs when the **wcancelscan** command is run while the **inv_config_ep_meths** process is reading the MDist segment containing the signatures.

APAR IZ12656

Abstract:

Endpoint label changes in COMPUTER table

Error Description:

In an interconnected Tivoli server environment, if the **swd autoscan_active=y** option is set on a hub, when the first activity issued from that hub against an endpoint, present on a spoke, is a software distribution, such as the installation of a software package, a record is inserted in the COMPUTER table, with the **tme_object_label** column value having the following format:

endpoint_name#region-region

When an Inventory scan is performed against the same endpoint, the COMPUTER table is updated, and the **tme_object_label** column value is modified into:

endpoint_name

Additional information:

After the fix, the endpoint label has the same format:

endpoint_name

for both activities, software distributions and Inventory scans.

APAR IZ12695

Abstract:

Error when updating local signature catalog during endpoint Inventory scan

Error Description:

Inventory is unable to update the local signature catalog after applying Configuration Manager version 4.2.3 Fix Pack 2. In the **INVxxxxx.LOG** file the following error message is displayed:

ERROR: Call function pointer register_packages failed. errno=2

Additional information:

With Fix Pack 2, the signature ID was changed from string type to integer. After this change an error always occurred when attempting to update the local Software Distribution catalog (**epsp.cat**) for signatures associated to software packages discovered during an Inventory software signature scan.

APAR IZ13300**Abstract:**

Configuration changes for AUTOFS file systems

Error Description:

If you are interested in the code changes implemented for the Common Inventory Technology (CIT) APAR IZ04274, before running an Inventory scan on your endpoints, set the environment variable named ASSUMEAUTOFSREMOTE to YES, or create a file named ASSUMEAUTOFSREMOTE under the *inv/SCAN* directory.

APAR IZ14763**Abstract:**

"FS FREE SIZE" value is bigger than "FS TOTAL SIZE" value

Error Description:

In the Inventory repository the "FS Free Size" value is bigger than the "FS Total Size" value, while in the MIF file the reported values are correct.

Additional information:

To solve this problem, a new table named INST_PARTITION_MB, a new view named PARTITION_MB_VIEW, and a new query named PARTITION_MB_QUERY have been created. In all these new objects, the size values are in megabytes. To define the new queries, run the *inventory_query.sh* and *h_inventory_query.sh* scripts.

APAR IZ15108**Abstract:**

After running **wscansw** and **wscanfs** commands, *cache_data* is filled up with files

Error Description:

After running an Inventory software scan and a scan for signature matching, the following endpoint directories:

```
/opt/tivoli/cit/cache_data/$adminuser/*
```

or

```
C:\Program Files\Tivoli\cit\cache_data\_administrator
```

are filled up with files. These directories on the endpoint are not cleaned up after the scan.

Additional information:

This problem occurred because the **wscanfs -reset** command issued to reset the Common Inventory Technology (CIT) cache is run before starting the Inventory scan, but it is not run after all scans are completed.

APAR IZ15654**Abstract:**

Unable to exclude a DFS file system from an Inventory scan

Error Description:

Large DFS file systems on Solaris and UNIX workstations. When running an Inventory scan on these workstations, the scan hangs. The exclude mechanism is not working. Therefore, even when trying to exclude the DFS file systems, the scan still hangs.

Additional information:

The fix introduced by this APAR applies only if, before running an Inventory scan on your endpoints, you set the environment variable named EXCLUDE_DFS to YES, or create a file named EXCLUDE_DFS under the *inv/SCAN* directory.

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

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

Table 8. APARs for Software Distribution

Software Distribution, Version 4.2.3, 4.2.3-TIV-SWDSRV-FP0006				
None				
Software Distribution Gateway, Version 4.2.3, 4.2.3-TIV-SWDGW-FP0006				
IZ13885				
Software Package Editor, Version 4.2.3, 4.2.3-TIV-SWDJPS-FP0006				
None				
Software Package Editor for Endpoints, Version 4.2.3, 4.2.3-TIV-SWDEP-FP0006				
IZ13885				

APAR IZ13885**Abstract:**

Software distribution installation not working on iSeries in Configuration Manager 423 Fix Pack 4

Error Description:

Configuration Manager is unable to perform any software distribution installation on iSeries endpoints. The installation is submitted using the **winstsp** command, the **spd_eng** is spawned on the endpoint, but the job fails.

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

Table 9. APARs for Activity Planner

Activity Planner, Version 4.2.3, 4.2.3-TIV-APM-FP0006				
IZ09864				

APAR IZ09864**Abstract:**

APM editor: list of software packages not displayed in alphabetical order

Error Description:

The Activity Plan Editor should display the list of the software packages in alphabetical order, to make the software package search much easier.

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

APARs and internal defects fixed for Tivoli Web Gateway: Table 10 lists the APARs that were fixed for Tivoli Web Gateway:

Table 10. APARs for Tivoli Web Gateway

Web Gateway, Version 4.2.3, 4.2.3-TIV-WEBGW-FP0006				
IZ13733				

APAR IZ13733**Abstract:**

JAVA.LANG.UNSATISFIEDLINKERROR during the startup of the results collector servlet

Error Description:

When installing Tivoli Configuration Manager on the Tivoli Web Gateway component, the Windows 2003 operating system is not recognized as a valid platform.

APARs and internal defects fixed for the Resource Manager: Resource Manager component does not currently contain any fixed APARs. Install this component because fixes have been released for some quality improvements.

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: Patch Management component does not currently contain any fixed APARs. Install this component because fixes have been released for some quality improvements.

APARs and internal defects fixed for Query Directory for Microsoft Active Directory - Command Line Interface: Query Directory for Microsoft Active Directory - Command Line Interface component does not currently contain any fixed APARs. Install this component because fixes have been released for some quality improvements.

APARs and internal defects fixed for Query Directory for Microsoft Active Directory: Query Directory for Microsoft Active Directory component does not currently contain any fixed APARs. Install this component because fixes have been released for some quality improvements.

APARs and internal defects fixed for CM Extension for Tivoli License Manager: CM Extension for Tivoli License Manager component does not currently contain any fixed APARs. Install this component because fixes have been released for some quality improvements.

APARs and internal defects fixed for CM Endpoint Extension: CM Endpoint Extension component does not currently contain any fixed APARs. Install this component because fixes have been released for some quality improvements.

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. Inventory APARs and internal defects included from 4.2.3–TCM-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. Inventory APARs and internal defects included from 4.2.3–TCM-FP01

Inventory, Version 4.2.3, 4.2.3-INV-FP01 and 4.2.3-INVGW-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–TCM-0002

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–TCM-0003

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. Inventory APARs included from 4.2.3–TCM-FP02

Inventory, Version 4.2.3, 4.2.3-INV-FP02 and 4.2.3-INVGW-FP02				
IY77378	IY78108	IY78940	IY79236	IY79372
IY80066	IY80608	IY80625	IY80837	IY80912

Table 15. Inventory APARs included from 4.2.3–TCM-FP02 (continued)

Inventory, Version 4.2.3, 4.2.3–INV-FP02 and 4.2.3–INVGW-FP02				
IY81297	IY81359	IY81437	IY81772	IY81879
IY82061	IY82415	IY82479	IY82635	IY82964
IY83074	IY82977	IY83087	IY83181	IY83338
IY84170	IY84708	IY84735	IY84736	IY84739
IY84876	IY85317	IY85496		

Table 16. Inventory APARs and internal defects included from 4.2.3.2-TIV-TCM-IF0001

Inventory and Inventory Gateway, Version 4.2.3.2, 4.2.3.2-TIV-INV-IF0001 and 4.2.3.2-TIV-INVGW-IF0001				
IY83381	IY85621	IY85965	IY86092	IY86229
IY86785	IY87021	IY87284	IY87805	IY88548
IY88885	IY88956	IY89009	IY89011	193723

Table 17. Inventory internal defects included from 4.2.3.2-TIV-TCM-IF0002

Inventory and Inventory Gateway, Version 4.2.3.2, 4.2.3.2-TIV-INV-IF0002 and 4.2.3.2-TIV-INVGW-IF0002				
195918	199809			

Table 18. Inventory APARs included from 4.2.3.TIV-TCM-FP0003

Inventory, Version 4.2.3, 4.2.3–TIV-INV-FP0003 and 4.2.3–TIV-INVGW-FP0003				
IY84371	IY86231	IY86274	IY88194	IY89503
IY89573	IY89732	IY89795	IY89973	IY90238
IY90360	IY90869	IY90993	IY91031	IY91186
IY91237	IY91440	IY91547	IY91674	IY92105
IY92128	IY92385	IY92618		

Table 19. Inventory APARs included from 4.2.3.TIV-TCM-FP0004

Inventory, Version 4.2.3, 4.2.3–TIV-INV-FP0004 and 4.2.3–TIV-INVGW-FP0004				
IY92776	IY92969	IY93009	IY93564	IY93587
IY93613	IY93634	IY93682	IY94648	IY94698
IY95362	IY95548	IY95710		

Table 20. Inventory APARs and internal defects included from 4.2.3.TIV-TCM-FP0005

Inventory, Version 4.2.3, 4.2.3–TIV-INV-FP0005 and 4.2.3–TIV-INVGW-FP0005				
206186	IY94770	IY97538	IY97653	IY98365
IY99251	IY99327	IY99839	IZ00054	IZ00381
IZ01609	IZ01679	IZ02233	IZ02945	IZ03006
IZ03008				

Table 21. Scalable Collection Service APARS included from 4.2.3–TCM-0001

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

Table 22. Scalable Collection Service APARS included from 4.2.3–TCM-0002

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

Table 23. Scalable Collection Service APARS included from 4.2.3-TCM-FP02

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

Table 24. Scalable Collection Service APARS included from 4.2.3.2-TIV-TCM-IF0001

Scalable Collection Service, Version 4.2.3.2, 4.2.3.2-TIV-CLL-IF0001			
IY86174	IY87041	IY87448	

Table 25. Scalable Collection Service APAR included from 4.2.3–TIV-TCM-FP0003

Scalable Collection Service, Version 4.2.3, 4.2.3-TIV-CLL-FP0003			
IY87132			

Table 26. Scalable Collection Service APARS included from 4.2.3–TIV-TCM-FP0004

Scalable Collection Service, Version 4.2.3, 4.2.3-TIV-CLL-FP0004			
IY93632	IY93681	IY94652	IY94776

Table 27. Scalable Collection Service APARS included from 4.2.3–TIV-TCM-FP0005

Scalable Collection Service, Version 4.2.3, 4.2.3-TIV-CLL-FP0005				
IY97209	IY97613	IY97898	IY99130	IZ02945

Table 28. Software Distribution APARS and internal defects included from 4.2.3–TCM-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
IY71991	IY72454	IY72698
IY72786	55063	55194

Table 28. Software Distribution APARs and internal defects included from 4.2.3–TCM-0001 (continued)

Software Distribution, Version 4.2.3, 4.2.3-SWDSRV-0001		
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 29. Software Distribution APARs and internal defects included from 4.2.3–TCM-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 30. Software Distribution APARs included from 4.2.3-TCM-0002

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

Table 31. Software Distribution APARs included from 4.2.3-TCM-0003

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 32. Software Distribution APARs included from 4.2.3-TCM-FP02

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
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			

Table 33. Software Distribution APARs and internal defects included from 4.2.3.2-TIV-TCM-IF0001

Software Distribution, Version 4.2.3.2, 4.2.3.2-TIV-SWDSRV-IF0001				
IY85877	IY86951	IY88574	IY89014	
Software Distribution Gateway, Version 4.2.3.2, 4.2.3.2-TIV-SWDGW-IF0001				
IY86926	IY88089			
Software Package Editor for Endpoints, Version 4.2.3.2, 4.2.3.2-TIV-SWDEP-IF0001				
IY86926	58114			

Table 34. Software Distribution APARs and internal defects included from 4.2.3.2-TIV-TCM-IF0002

Software Distribution, Version 4.2.3.2, 4.2.3.2-TIV-SWDSRV-IF0002				

Table 34. Software Distribution APARs and internal defects included from 4.2.3.2-TIV-TCM-IF0002 (continued)

58170	58176	58182	58186	58198
IY91469				

Table 35. Software Distribution APARs included from 4.2.3-TIV-TCM-FP0003

Software Distribution, Version 4.2.3, 4.2.3-TIV-SWDSRV-FP0003				
IY86341	IY87352	IY89298	IY89665	IY90438
IY90443	IY90445	IY90955	IY91076	IY91436
IY91469	IY92137	IY92678		
Software Distribution Gateway, Version 4.2.3, 4.2.3-TIV-SWDGW-FP0003				
IY89709	IY89761	IY90729		
Software Package Editor, Version 4.2.3, 4.2.3-TIV-SWDJPS-FP0003				
None				
Software Package Editor for Endpoints, Version 4.2.3, 4.2.3-TIV-SWDEP-FP0003				
IY86341	IY89709	IY89761	IY90147	IY90729

Table 36. Software Distribution APARs included from 4.2.3-TIV-TCM-FP0004

Software Distribution, Version 4.2.3, 4.2.3-TIV-SWDSRV-FP0004				
IY92117	IY93503	IY95003		
Software Distribution Gateway, Version 4.2.3, 4.2.3-TIV-SWDGW-FP0004				
IY92683	IY94555	IY94960	IY95411	
Software Package Editor, Version 4.2.3, 4.2.3-TIV-SWDJPS-FP0004				
None				
Software Package Editor for Endpoints, Version 4.2.3, 4.2.3-TIV-SWDEP-FP0004				
IY95411				

Table 37. Software Distribution APARs included from 4.2.3-TIV-TCM-FP0005

Software Distribution, Version 4.2.3, 4.2.3-TIV-SWDSRV-FP0005				
None				
Software Distribution Gateway, Version 4.2.3, 4.2.3-TIV-SWDGW-FP0005				
IZ00655	IZ01027	IZ01595	IZ01673	IZ04234
Software Package Editor, Version 4.2.3, 4.2.3-TIV-SWDJPS-FP0005				
IZ03869				
Software Package Editor for Endpoints, Version 4.2.3, 4.2.3-TIV-SWDEP-FP0005				
IZ01027	IZ01595	IZ01673		

Table 38. Activity Planner APARs and internal defects included from 4.2.3-TCM-0001

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

Table 38. Activity Planner APARs and internal defects included from 4.2.3–TCM-0001 (continued)

Activity Planner, Version 4.2.3, 4.2.3-APM-0001		
IY74948	54559	

Table 39. Activity Planner APARs and internal defects included from 4.2.3–TCM-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 40. Activity Planner APARs included from 4.2.3-TCM-0002

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

Table 41. Activity Planner APARs included from 4.2.3-TCM-0003

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

Table 42. Activity Planner APARs included from 4.2.3-TCM-FP02

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			

Table 43. Activity Planner APARs included from 4.2.3.2-TIV-TCM-IF0001

Activity Planner, Version 4.2.3.2, 4.2.3.2-TIV-APM-IF0001				
IY88122	IY89499			

Table 44. Activity Planner APARs included from 4.2.3–TIV-TCM-FP0003

Activity Planner, Version 4.2.3, 4.2.3-TIV-APM-FP0003				
IY86738	IY87635	IY88552	IY89231	IY89281
IY89282	IY89667	IY90259	IY90706	IY91115

Table 45. Activity Planner APARs included from 4.2.3–TIV-TCM-FP0004

Activity Planner, Version 4.2.3, 4.2.3-TIV-APM-FP0004				
IY94022	IY94074	IY95473	IY95703	

Table 46. Activity Planner APARs and internal defects included from 4.2.3–TIV-TCM-FP0005

Activity Planner, Version 4.2.3, 4.2.3–TIV-APM-FP0005				
59151	IZ00375	IZ00420	IZ01919	IZ01947
IZ02679	IZ03032	IZ03951		

Table 47. Change Manager APAR included from 4.2.3–TCM-0001

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

Table 48. Web interface APARs included from 4.2.3–TCM-0001

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

Table 49. Web interface internal defect included from 4.2.3–TCM-FP01

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

Table 50. Web interface APAR included from 4.2.3–TCM-FP02

Web Interface, Version 4.2.3, 4.2.3–WEB-FP02		
IY83967		

Table 51. Web Interface APAR included from 4.2.3–TIV-TCM-FP0003

Web Interface, Version 4.2.3, 4.2.3–TIV-WEB-FP0003				
IY89223				

Table 52. Web Interface APAR included from 4.2.3–TIV-TCM-FP0005

Web Interface, Version 4.2.3, 4.2.3–TIV-WEB-FP0005				
IZ02348				

Table 53. Resource Manager internal defects included from 4.2.3–TCM-FP01

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

Table 54. Pristine Manager APAR included from 4.2.3–TCM-0001

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

Table 55. Patch Management internal defects included from 4.2.3–TCM-0001

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

Table 56. Patch Management internal defects included from 4.2.3-TCM-FP01

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

Table 57. Patch Management APARs included from 4.2.3.2-TIV-TCM-IF0001

Patch Management, Version 4.2.3.2, 4.2.3.2-TIV-PMG-IF0001				
IY84828	IY84889	IY86639	IY86651	IY88895

Table 58. Patch Management APARs included from 4.2.3-TCM-FP02

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

Table 59. Directory Query APAR included from 4.2.3-TCM-0001

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

Table 60. Query Directory for Microsoft Active Directory internal defects included from 4.2.3.2-TIV-TCM-IF0001

Query Directory for Microsoft Active Directory, Version 4.2.3.2, 4.2.3.2-TIV-ADIENG-IF0001 and 4.2.3.2-TIV-ADICLI-IF0001				
57898	57944	57946	57948	57995

Installation

This section describes how to install fix pack 6 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 39
- “Software package block (SPB) fix pack installation for GUI components” on page 45
- “Updating the inventory schema” on page 51

Hardware and software requirements

This section includes the following topics:

- “Supported platforms” on page 38

- “System requirements”

Supported platforms

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

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

System requirements

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:

Windows Vista

Patch 4.1.1-LCF-0042 for the Windows Vista endpoint support

Inventory running on HP-UX 11.00

- Quality Pack For HP-UX 11.00, March 2004 (QPK1100 B.11.00.64.4)
- HSS_26945 HP aC++ -AA runtime libraries (aCC A.03.37)

License Management Extension space requirements

Table 61. 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 keep working, perform the following steps:

1. Install the fix pack on the Tivoli gateways.

2. Install the fix pack on the Inventory server.
3. Upgrade the Inventory database on the Inventory server.

Note: Until you perform step 2 and 3 of the procedure, you can only run Inventory scans on endpoints attached to the gateways, on which you have still not installed Fix Pack 6.

Traditional fix pack installation methods

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

- “Installing fix packs using ISMP”

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

- “Installing fix packs using the Tivoli desktop” on page 40

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 40

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 42

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 6 CD 1. 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

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

Use 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 62 on page 41. 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 6 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 62. IND files included in this fix pack

IND file	Component name	Tag
CLLFP6.IND	Scalable Collection Service, Version 4.2.3	4.2.3-TIV-CLL-FP0006
INVFP6.IND	Inventory, Version 4.2.3	4.2.3-TIV-INV-FP0006
LCFFP6.IND	Inventory Gateway, Version 4.2.3	4.2.3-TIV-INVGW-FP0006
SWDFP6.IND	Software Distribution, Version 4.2.3	4.2.3-TIV-SWDSRV-FP0006
SDGWFP6.IND	Software Distribution Gateway, Version 4.2.3	4.2.3-TIV-SWDGW-FP0006
SDJFP6.IND	Software Distribution Software Package Editor, Version 4.2.3	4.2.3-TIV-SWDJPS-FP0006
APMFP6.IND	Activity Planner, Version 4.2.3	4.2.3-TIV-APM-FP0006
CCMFP6.IND	Change Manager, Version 4.2.3	4.2.3-TIV-CCM-FP0006
WEBUIFP6.IND	Web Interface, Version 4.2.3	4.2.3-TIV-WEB-FP0006
TRMFP6.IND	Resource Manager, Version 4.2.3	4.2.3-TIV-TRMSRV-FP0006
TRMGWFP6.IND	Resource Manager Gateway, Version 4.2.3	4.2.3-TIV-TRMGW-FP0006

Table 62. IND files included in this fix pack (continued)

IND file	Component name	Tag
PMFP6.IND	Pristine Manager, Version 4.2.3	4.2.3-TIV-PMSRV-FP0006
PMGFP6.IND	Patch Management, Version 4.2.3	4.2.3-TIV-PMG-FP0006
ICOMPFP6.IND	Inventory, Version 4.2.3, backward compatibility patch	4.2.3-TIV-INV-COMP-FP0006
DQYFP6.IND	Directory Query, Version 4.2.3	4.2.3-TIV-DQY-FP0006
ADCLIFP6.IND	Query Directory for Microsoft Active Directory - Command Line Interface, Version 4.2.3	4.2.3-TIV-ADICLI-FP0006
ADENGFP6.IND	Query Directory for Microsoft Active Directory, Version 4.2.3	4.2.3-TIV-ADIENG-FP0006
TLMXTFP6.IND	CM Extension for Tivoli License Manager, Version 4.2.3	4.2.3-TIV-TLMEXT-FP0006
CMEXTFP6.IND	CM Endpoint Extension, Version 4.2.3	4.2.3-TIV-CMEXT-FP0006
TPOSDFP6.IND	Tivoli Provisioning Manager for Operating System Deployment Integration, Version 4.2.3	4.2.3-TIV-TPOSD-FP0006

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 62 on page 41.

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*.

New components installation methods

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

- “Installing new components using the Tivoli desktop” on page 43

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

- “Installing new components using the CLI”
Tivoli Management Framework command that you use to specify the new components to install and the target workstations on which to install them from the command line interface.
- “Installing new components using SIS” on page 44
The SIS console or SIS commands you use to specify the new components to install and on which target workstations to install them.

Installing new components using the Tivoli desktop

When installing new components using the Tivoli desktop, the images are located in the NewComponents subdirectory on the IBM Tivoli Configuration Manager, Version 4.2.3 Fix Pack 6 CD 1. 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:
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 new components using the CLI

Use the **winstall** command to install new components.

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 63. IND files included in this fix pack

IND file	Component name	Tag
ADICLI.IND ¹	Query Directory for Microsoft Active Directory - Command Line Interface, Version 4.2.3	ADICli
ADIENG.IND ¹	Query Directory for Microsoft Active Directory, Version 4.2.3	ADIEng
TLMEXT.IND ^{1, 2}	CM Extension for Tivoli License Manager, Version 4.2.3	tlm_ext
CMEXT.IND ^{1,2}	CM Endpoint Extension, Version 4.2.3	cm_ext
TPOSD.IND	Image management services integration, Version 4.2.3	TPMforOSDeployment

¹ For these components, you need to install also the related patch. These patches can be found under the /images/SWD directory.

Table 63. IND files included in this fix pack (continued)

IND file	Component name	Tag
² For information on how to implement License Compliance Manager in your Configuration Manager environment see <i>IBM Tivoli Configuration Manager License Management Extension</i> .		

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

Example:

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

where:

-c CD-ROM/NewComponents

Specifies the path to the images on the IBM Tivoli Configuration Manager, Version 4.2.3 Fix Pack 6 CD 1.

-i index_file

Specifies the product installation index file

managed_node

Specifies the managed node on which you want to install the new component

installation_options

Specifies the installation options.

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

Installing new components using SIS

When installing new components using Tivoli Software Installation Service, select the component to be installed using the component name shown in Table 63 on page 43.

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 49
- “Software Distribution server command” on page 49
- “Software Distribution disconnected command” on page 50

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 64.

Table 64. Default variables defined in SPB fix packs

Variable	Value	Description
Tivoli_INV_GUI_Fix.v4.2.3.FP06		
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.FP06		
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.FP06		
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.FP06		
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.FP06		
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.

Table 64. Default variables defined in SPB fix packs (continued)

Variable	Value	Description
Tivoli_CCM_GUI_L10N_Fix.v4.2.3.FP06		
DSWIN_DIR	\$(program_files)\Tivoli\Desktop	The directory where the Tivoli Desktop is installed.
TME_JAVATOOLS	\$(program_files)\Tivoli\JavaTools	The directory where the JRE 1.3 is installed.
Tivoli_SWDEP_AIX_Fix.v4.2.3.FP06		
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.FP06		
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.FP06		
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.FP06		
target_dir	\$(product_dir)/speditor	The directory where the Software Package Editor is installed.
Tivoli_SWDEP_LINUXPPC_Fix.v4.2.3.FP06		
target_dir	\$(product_dir)/speditor	The directory where the Software Package Editor is installed.
TME_JAVATOOLS	/opt/Tivoli/JavaTools	The directory where JRE 1.3 is installed.
Tivoli_SWDEP_NT_Fix.v4.2.3.FP06		
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.FP06		
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.FP06		

Table 64. Default variables defined in SPB fix packs (continued)

Variable	Value	Description
target_dir	\$(product_dir)\speditor	The directory where the Software Package Editor is installed.
Tivoli_JRE_SOLARIS_IX86_Fix.v4.2.3.FP06		
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_SOLARIS_IX86.423		
Tivoli_SWDEP_SOLARIS_IX86_Fix.v4.2.3.FP06		
target_dir	\$(product_dir)\speditor	The directory where the Software Package Editor is installed.
Tivoli_SWDEP_L10N_Fix.v4.2.3.FP06		
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_JRE_AIX		
TME_JAVATOOLS	/opt/Tivoli/JavaTools	The directory where JRE 1.3 is installed.
Tivoli_JRE_version	1.3.0	The version of the JRE
Tivoli_JRE_HP		
TME_JAVATOOLS	/opt/Tivoli/JavaTools	The directory where JRE 1.3 is installed.
Tivoli_JRE_version	1.3.0	The version of the JRE
Tivoli_JRE_LINUX_IX86		
TME_JAVATOOLS	/opt/Tivoli/JavaTools	The directory where JRE 1.3 is installed.
Tivoli_JRE_version	1.3.0	The version of the JRE
Tivoli_JRE_LINUX_S390		
TME_JAVATOOLS	/opt/Tivoli/JavaTools	The directory where JRE 1.3 is installed.
Tivoli_JRE_version	1.3.0	The version of the JRE
Tivoli_JRE_NT		
TME_JAVATOOLS	\$(program_files)\Tivoli\JavaTools	The directory where JRE 1.3 is installed.
Tivoli_JRE_version	1.3.0	The version of the JRE
Tivoli_JRE_SOLARIS		
TME_JAVATOOLS	/opt/Tivoli/JavaTools	The directory where JRE 1.3 is installed.
Tivoli_JRE_version	1.3.0	The version of the JRE
Tivoli_Web_Gateway_DB_Fix.v4.2.3.FP06		

Table 64. Default variables defined in SPB fix packs (continued)

Variable	Value	Description
Tivoli_Web_Gateway_L10N		
WAS_CELL	CellName	Specifies the WebSphere® Application Server cell name.
AppServer	C:\Program Files\WebSphere\AppServer	Specifies where the WebSphere® Application Server home is located.
WAS_PROFILE	default	Specifies the WebSphere® Application Server profile.
DMS.Destination	C:\Program Files\TivTwg	Specifies where the Tivoli Web Gateway is installed.
Tivoli_Web_Gateway_SRV_Fix.v4.2.3.FP06		
WAS_CELL	CellName	Specifies the WebSphere® Application Server cell name.
LCF_LIBDIR.UNIX	\$(LCFROOT)/lib/\$(INTERP)	
CLUSTER_ENV	false	Specifies whether the cluster Tivoli Web Gateway Server is to be upgraded.
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)	
WAS_PROFILE	default	Specifies the WebSphere® Application Server profile.
LCFROOT	/opt/Tivoli/lcf	Specifies the LCFROOT directory for the endpoint.
LCF_DATDIR	/opt/Tivoli/lcf/dat/1	Specifies the LCFDAT 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.
Tivoli_WebUI_Fix.v4.2.3.FP06		
Tivoli_WebUI_L10N		
WAS_CELL	CellName	Specifies the WebSphere® Application Server cell name.
AppServer	/opt/WebSphere/AppServer	Specifies where the WebSphere® Application Server home is located.
WAS_PROFILE	default	Specifies the WebSphere® Application Server profile.
WebSrvDoc	/opt/IBMHttpServer/htdocs/en_US	Specifies the directory for the Web Server documentation.

Note: When you install the fix pack, if you are using the APM or CCM GUI components, you should also install the remote desktops at the same fix pack level.

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 6 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 6 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_FP06.xml` file for the fix pack located in the `/package` subdirectory on the IBM Tivoli Configuration Manager, Version 4.2.3 Fix Pack 6 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 65 on page 50.
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 65 contains the names of the fix pack 6 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 65. Names of SPB files and software profiles

SPB Files	Package name with Version
Tivoli_INV_GUI_Fix.v4.2.3.FP06.spb	Tivoli_INV_GUI_Fix.v4.2.3.FP06
Tivoli_INV_GUI_L10N_Fix.v4.2.3.FP05.spb	Tivoli_INV_GUI_L10N_Fix.v4.2.3.FP05
Tivoli_APM_GUI_Fix.v4.2.3.FP06.spb	Tivoli_APM_GUI_Fix.v4.2.3.FP06
Tivoli_APM_GUI_L10N_Fix.v4.2.3.FP05.spb	Tivoli_APM_GUI_L10N_Fix.v4.2.3.FP05
Tivoli_CCM_GUI_Fix.v4.2.3.FP06.spb	Tivoli_CCM_GUI_Fix.v4.2.3.FP06
Tivoli_CCM_GUI_L10N_Fix.v4.2.3.FP05.spb	Tivoli_CCM_GUI_L10N_Fix.v4.2.3.FP05
Tivoli_SWDEP_AIX_Fix.v4.2.3.FP06.spb	Tivoli_SWDEP_AIX_Fix.v4.2.3.FP06
Tivoli_SWDEP_HP_Fix.v4.2.3.FP06.spb	Tivoli_SWDEP_HP_Fix.v4.2.3.FP06
Tivoli_SWDEP_LINUXPPC_Fix.v4.2.3.FP06.spb	Tivoli_SWDEP_LINUXPPC_Fix.v4.2.3.FP06
Tivoli_SWDEP_LINUX_IX86_Fix.v4.2.3.FP06.spb	Tivoli_SWDEP_LINUX_IX86_Fix.v4.2.3.FP06
Tivoli_SWDEP_LINUX_S390_Fix.v4.2.3.FP06.spb	Tivoli_SWDEP_LINUX_S390_Fix.v4.2.3.FP06
Tivoli_SWDEP_NTAS400_Fix.v4.2.3.FP06.spb	Tivoli_SWDEP_NTAS400_Fix.v4.2.3.FP06
Tivoli_SWDEP_NT_Fix.v4.2.3.FP06.spb	Tivoli_SWDEP_NT_Fix.v4.2.3.FP06
Tivoli_SWDEP_SOLARIS_Fix.v4.2.3.FP06.spb	Tivoli_SWDEP_SOLARIS_Fix.v4.2.3.FP06
Tivoli_JRE_SOLARIS_IX86.spb	Tivoli_JRE_SOLARIS_IX86
Tivoli_SWDEP_SOLARIS_IX86.spb	Tivoli_SWDEP_SOLARIS_IX86
Tivoli_SWDEP_SOLARIS_IX86_Fix.v4.2.3.FP06.spb ⁽¹⁾	Tivoli_SWDEP_SOLARIS_IX86_Fix.v4.2.3.FP06
Tivoli_SWDEP_L10N_Fix.v4.2.3.FP05.spb	Tivoli_SWDEP_L10N_Fix.v4.2.3.FP05
Tivoli_JRE_AIX.spb ⁽²⁾	Tivoli_JRE_AIX
Tivoli_JRE_HP.spb ⁽²⁾	Tivoli_JRE_HP
Tivoli_JRE_LINUX_IX86.spb ⁽²⁾	Tivoli_JRE_LINUX_IX86
Tivoli_JRE_LINUX_S390.spb ⁽²⁾	Tivoli_JRE_LINUX_S390
Tivoli_JRE_NT.spb ⁽²⁾	Tivoli_JRE_NT
Tivoli_JRE_SOLARIS.spb ⁽²⁾	Tivoli_JRE_SOLARIS
Tivoli_Web_Gateway_DB_Fix.v4.2.3.FP06.spb ⁽²⁾	Tivoli_Web_Gateway_DB_Fix.v4.2.3.FP06
Tivoli_Web_Gateway_L10N.spb ⁽²⁾	Tivoli_Web_Gateway_L10N
Tivoli_Web_Gateway_SRV_Fix.v4.2.3.FP06.spb ⁽²⁾	Tivoli_Web_Gateway_SRV_Fix.v4.2.3.FP06
Tivoli_WebUI_Fix.v4.2.3.FP06.spb ⁽²⁾	Tivoli_WebUI_Fix.v4.2.3.FP06
Tivoli_WebUI_L10N.spb ⁽²⁾	Tivoli_WebUI_L10N

Notes:

1. ⁽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.spb. 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. ⁽²⁾ Install these software package blocks you find under the /package path to enable the Daylight Saving Time (DST) feature. It is not mandatory to perform this installation. If you do not install these software package blocks, the time stamp of log and trace files is not at Daylight Saving Time used by the following countries:
 - United States
 - Canada
 - Brazil
 - Bermuda
 - Western Australia

Updating the inventory schema

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

A fix pack does not necessarily contain fixes on SQL scripts and, if present, these fixes do not necessarily apply to all database vendors.

Table 66 lists the SQL scripts, released with the different fix packs, to run for updating the **Inventory schema**:

Table 66. SQL scripts for updating the Inventory schema

	Oracle	DB2	MSSQL	Sybase	Informix	DB2 MVS	DB2 MVS custom
inv_db_423_FP01.sql	X	X	X	X	X	X	X
inv_db_423_FP02.sql	X	X	X	X	X	X	X
inv_db_423_FP03.sql	X	X	X	X	X	X	X
inv_db_423_FP04.sql	X	X	X	X	X	X	X
inv_db_423_FP05.sql	X	X	X	X	X	X	X
inv_db_423_FP06.sql	X	X	X	X	X	X	X

Table 67 lists the SQL scripts, released with the different fix packs, to run for updating the **Historical Inventory schema**:

Table 67. SQL scripts for updating the Historical Inventory schema

	Oracle	DB2	MSSQL	Sybase	Informix	DB2 MVS	DB2 MVS custom
h_inv_db_423_FP01.sql	X	X	X	X	X	X	X

Table 67. SQL scripts for updating the Historical Inventory schema (continued)

	Oracle	DB2	MSSQL	Sybase	Informix	DB2 MVS	DB2 MVS custom
h_inv_db_423_FP02.sql	X	X	X	X	X	X	X
h_inv_db_423_FP03.sql	X	X	X	X	X	X	X
h_inv_db_423_FP04.sql	X	X	X	X	X	X	X
h_inv_db_423_FP05.sql	X	X	X	X	X	X	X
h_inv_db_423_FP06.sql	X	X	X	X	X	X	X

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 SQL connectivity) to run the schema scripts. If you have already installed and configured the previous fix packs, you do not need to run the *inv_db_vendor_423_FP0x.sql* and *h_inv_db_vendor_423_FP0x.sql* (where *x* = 1, 2, 3, 4, or 5) scripts again.

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

For instance, if you use DB2 and install this fix pack, to update the Inventory schema, refer to the **DB2** column of Table 66 on page 51 and run the scripts identified in the table rows by **X** in the order specified:

- *inv_db2_423_FP01.sql*
- *inv_db2_423_FP02.sql*
- *inv_db2_423_FP03.sql*
- *inv_db2_423_FP04.sql*
- *inv_db2_423_FP05.sql*
- *inv_db2_423_FP06.sql*

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

Upgrading from a Configuration Manager 4.2.2 environment

Run the following steps if you want to migrate from a Tivoli Configuration Manager Version 4.2.2 to a Tivoli Configuration Manager Version 4.2.3 environment:

1. Download the latest Tivoli Configuration Manager 4.2.2 fix pack.
2. Run all the *%inv%423_FP0%.sql* scripts available for your *dbvendor*, 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 related scripts again.

For instance, if you are at Tivoli Configuration Manager Version 4.2.2 fix pack 2 level, and you download Tivoli Configuration Manager Version 4.2.2 fix pack 6, you need to run the following scripts:

- *dbvendor%422_FP03.sql*
- *dbvendor%422_FP04.sql*
- *dbvendor%422_FP05.sql*
- *dbvendor%422_FP06.sql*

3. Download the latest Tivoli Configuration Manager 4.2.3 fix pack .

Note: You must download the latest fix pack because it contains the refreshed %inv%upgrade_422_423.sql and %inv%423_FP0%.sql scripts.

4. Run the %inv%upgrade_422_423.sql script which was installed when downloading the Tivoli Configuration Manager 4.2.3 fix pack depending on your *dbvendor*.
5. Edit the appropriate *dbvendor%inv%423_FP0%.sql* script and search for the 422_423 string. If the string is found, follow carefully the instructions.
6. Run all %inv%423_FP0y.sql scripts, where y is the Tivoli Configuration Manager 4.2.3 fix pack level you have downloaded.

For instance, if you have downloaded Tivoli Configuration Manager Version 4.2.3 fix pack 6, you need to run the following scripts:

- *dbvendor%423_FP01.sql*
- *dbvendor%423_FP02.sql*
- *dbvendor%423_FP03.sql*
- *dbvendor%423_FP04.sql*.
- *dbvendor%423_FP05.sql*.
- *dbvendor%423_FP06.sql*.

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 have not already run the command *winvmigrate* to migrate Configuration Manager signatures from the old SWSIGS.INI format to the new IBM software catalog format, or if you imported the IBM software catalog before installing Configuration Manager 4.2.3 Fix Pack 6, then you must migrate the signatures belonging to the IBM software catalog. To do this, after having installed Configuration Manager 4.2.3 Fix Pack 6, perform the following steps:

1. Run the *inv_db_vendor_423_FP06.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 implement license management facilities in your Configuration Manager environment, refer to the IBM Tivoli Configuration Manager: License Management with License Compliance Manager version 2.3.

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 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 plug-ins

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

Activity Planner

If you have installed 4.2.3-TIV-APM-FP0006, 4.2.3-TIV-SWDSRV-FP0006, and 4.2.3-TIV-INV-FP0006 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, after running the scripts.

Change Manager

If you have installed 4.2.3-TIV-CCM-FP0006, 4.2.3-TIV-SWDSRV-FP0006, and 4.2.3-TIV-INV-FP0006 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`

Installing the Web Gateway component

The Tivoli Web Gateway component is responsible for providing support for Nokia S60 devices. Because this component requires newer versions of DB2 UDB and WebSphere Application Server, it is provided as a fresh installation and not as a patch to be installed on previous levels. A procedure for migrating data from the old to the new Tivoli Web Gateway environment is provided.

The InstallShield program for this component is available on the on the IBM Tivoli Configuration Manager, Version 4.2.3 Fix Pack 6 CD 3 under the `/twg_installer` directory.

For more details on the Web Gateway prerequisites, installation and data migration refer to the IBM Tivoli Configuration Manager: Planning and Installation Guide.

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-TIV-SWDSRV-FP0006** Software Distribution fix pack to update the Software Distribution command line and GUI.
2. Install the **4.2.3-TIV-SWDGW-FP0006** Software Distribution gateway fix pack to update Windows endpoints at the next distribution.
3. Install the **4.2.3-TIV-APM-FP0006** 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 54.
5. Distribute the **Tivoli_login_control_4.2.3.spb** software package to the endpoints.
6. Type the following command to enable the feature on the specified endpoint:
`wep endpoint_name set allow_distribution_control on`

where:

endpoint_name

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

Repeat the command for each endpoint where the feature is to be enabled.

7. Download the `wdepcem.exe` file from the `/LoginControl` folder to the endpoints.

Configuring the concurrent login feature

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

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

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

- HKEY_LOCAL_MACHINE\SOFTWARE\Tivoli\SWDnotification\wmansd

To view and edit the registry keys, use the **wdepccm** command. For more information on this command, see “wdepccm” on page 60.

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\nContact 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 67
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 68.

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 *wcftplog.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 wrtplng.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

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 IZ10192

In Chapter 4 "Troubleshooting", in the "Specific Problems and Workarounds" section, at the end of the section add the following information:

JCF paths for the APMCLASSPATH environment variable are wrong

If you migrate from older releases to Tivoli Configuration Manager 4.2.3 release, the odadmin environment variable APMCLASSPATH wrongly points to the following paths:

- 4.1 JRIM.jar
- 4.1 JCF.jar
- 4.1 ibmjsse.jar
- 4.1 jsafe.zip

even if you have migrated to the correct Tivoli Management Framework level.

Manually correct the paths by modifying them as follows:

- 4.1.1 JRIM.jar
- 4.1.1 JCF.jar
- 4.1.1 ibmjsse.jar
- 4.1.1 jsafe.zip

Note: On AIX platforms, do not use the VI editor to modify these paths.

Patch Management Guide

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

Defect 59751

In Chapter 6 "Automated patch management command line" in section "wsecgensp" add the following information to the "Options" subsection:

- H 9 Specifies whether software packages are generated using the installer for Windows 2008 and Windows Vista. If this option is not specified or if you enter a value different from 9, the packages are created using the default installer.

and add to the current usage of the command the following information:

[-H 9]

APAR IZ13447

In Chapter 3 "Configuration and administrative tasks" in section "Configuring automated patch management settings" add the following information at the end of the section:

winvmgr command

Specify if you want to use the Microsoft WSUS Server for your patch management operations by running the following Inventory command:

```
winvmgr -c PM_WSUS_enabled=y
```

Defect 59810

In Chapter 1 "Introduction" in section "Operating systems and applications managed with this solution" add to the current list the following bullets:

- Windows Server 2008 Standard (ix86 only)
- Windows Server 2008 Enterprise (ix86 only)

and add after the bulleted list the following note:

Note: No operating system patches are supported for Windows Server 2008, only patches related to software applications.

User's Guide for Inventory

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

APAR IZ13447

In Appendix B "Commands" in section "**winvmgr**" add the following command parameter when describing the **-c** option:

PM_WSUS_enabled=y | n

Specifies if you want to use the Microsoft WSUS Server for the Automated Patch Management solution provided by Tivoli Configuration Manager.

Defect 59750

In Appendix E "Installing and uninstalling Common Inventory Technology (CIT)" in section "Installing Common Inventory Technology (CIT)" replace the current step 5 of the procedure with the following information:

On the Inventory server, run the following command:

```
winstsp -f -ty @CIT.2.5.1003 @Endpoint:ep1  
wcommtsp -f @CIT.2.5.1003 @Endpoint:ep1
```

where:

ep1 Is the name of the endpoint.

Note: This installation method is not supported on OS/400 systems.

Database Schema Reference

This section contains new and updated information for IBM Tivoli Configuration Manager Database Schema Reference:

APAR IZ11361

In Chapter 3 "Configuration repository views", in the "PROCESSOR_VIEW" section, add the following row to the current table:

Column Name

IS_ENABLED

Description

The enablement of the processor. Possible values are:

Y The processor is enabled.

N The processor is not enabled.

H (Windows platforms only) The hyperthreading feature is enabled.

and check all operating systems listed in the table.

APAR IZ14763

In Chapter 5 "Configuration repository tables", before the "INST_PARTITION" section, add the following table:

INST_PARTITION_MB

Describes a disk partition on a drive on the system. One record exists for each partition for each system scanned.

Populated by an inventory hardware scan.

The columns in this table are as follows:

COMPUTER_SYS_ID (primary key)

FS_ACCESS_POINT (primary key)

DEV_NAME

PARTITION_TYPE

MEDIA_TYPE

PHYSICAL_SIZE_MB ⁽¹⁾

FS_TYPE

FS_MOUNT_POINT

FS_TOTAL_SIZE_MB ⁽¹⁾

FS_FREE_SIZE_MB ⁽¹⁾

RECORD_TIME

Note: ⁽¹⁾ The size values of these columns are specified in megabytes.

APAR IZ14763

In Chapter 3 "Configuration repository views", before the "PARTITION_VIEW" section, add the following view:

PARTITION_MB_VIEW

Displays information about disk partitions on target systems.

Based on the COMPUTER and INST_PARTITION_MB tables.

The columns in this view are as follows:

Column Name	Description	AIX	HP-UX	Linux (S/390)	Linux (PC)	NetWare	OS/2	OS/400	Solaris	Windows 98	Windows NT/2000
TME_OBJECT_LABEL	The object label for the system.	✓	✓	✓	✓		✓	✓	✓	✓	✓
TME_OBJECT_ID	The object ID for the system.	✓	✓	✓	✓		✓	✓	✓	✓	✓
COMPUTER_SYS_ID	The computer system ID.	✓	✓	✓	✓		✓	✓	✓	✓	✓
FS_ACCESS_POINT	The location where the partition is mounted.	✓	✓	✓	✓		✓	✓	✓	✓	✓
DEV_NAME	The device name.	✓	✓	✓	✓		✓	✓	✓	✓	✓
PARTITION_TYPE	The type of partition on the drive.	✓	✓	✓	✓		✓	✓	✓	✓	✓
MEDIA_TYPE	The media type that contains the partition.	✓	✓	✓	✓		✓	✓	✓	✓	✓
PHYSICAL_SIZE_MB	The size of the drive that contains the partition in MB.	✓	✓	✓	✓		✓	✓	✓	✓	✓
FS_TYPE	The file system type.	✓	✓	✓	✓		✓	✓	✓	✓	✓

Column Name	Description	AIX	HP-UX	Linux (S/390)	Linux (PC)	NetWare	OS/2	OS/400	Solaris	Windows 98	Windows NT/2000
FS_MOUNT_POINT	The point where the partition attaches to the operating system.	✓	✓	✓	✓		✓	✓	✓	✓	✓
FS_TOTAL_SIZE_MB	The size of the partition in MB.	✓	✓	✓	✓		✓	✓	✓	✓	✓
FS_FREE_SIZE_MB	The amount of free space on the partition in MB.	✓	✓	✓	✓		✓	✓	✓	✓	✓
RECORD_TIME	The time that the data was updated at the database.	✓	✓	✓	✓		✓	✓	✓	✓	✓

APAR IZ14763

In Chapter 4 "Queries", before the "PARTITION_QUERY" section, add the following query:

PARTITION_MB_QUERY

Returns information about disk partitions on target systems.

Runs against the view PARTITION_MB_VIEW.

The columns in this query are as follows:

TME_OBJECT_LABEL

TME_OBJECT_ID

COMPUTER_SYS_ID

FS_ACCESS_POINT

DEV_NAME

PARTITION_TYPE

MEDIA_TYPE

PHYSICAL_SIZE_MB

FS_TYPE

FS_MOUNT_POINT

FS_TOTAL_SIZE_MB

FS_FREE_SIZE_MB

RECORD_TIME

Messages and Codes

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

Defect 59754/59755

The message text for the DISSE0330E error message has been modified as follows:

DISSE0330E Remove operation for targets having a different package state in the Inventory database is not allowed if the force option is not set. You can use the ignore option to skip the not installed targets if you disable the remove_not_installed by running
wswdcfg -s disable_remove_not_installed=y.

The current explanation for the **CMW0007E** error message has been modified as follows:

One of the steps you performed during the silent installation has failed.

The current operator response for the **CMW0007E** error message has been modified as follows:

See the upper sections of this log file to determine the nature of the error.
Correct the error and try the operation again.

Documentation problems and corrections contained in previous fix packs

Planning and Installation Guide

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

Defect 56291

In Chapter 5 "IBM Tivoli Configuration Manager Installation and Upgrade", in the "Custom Server Installation" section, at the end of step 10 add the following information:

Ensure that the password you specify does not contain a special character at the end.

Defect 58844

In Chapter "Component Installation Prerequisites", in the "IBM Tivoli Configuration Manager packaging" change the **IBM Tivoli Configuration Manager Desktop, Version 4.2.3** description as follows:

This contains the installation image and the InstallShield wizard for a fresh installation or an upgrade of IBM Tivoli Configuration Manager on any workstation that is not a managed node or a Tivoli server.

User's Guide for Deployment Services

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

Defect 56271

In Chapter 2 "Performing Activity Planner Operations", in the "Launching the Activity Planner GUIs" section, add to the third bullet of the procedure the following information:

To use the Activity Plan Editor and the Activity Plan Monitor GUIs from the Tivoli desktop, the user password can contain all the special characters from ASCII 32 to ASCII 127. The only special character that cannot be used is "double quotes".

Defect 58571

In Chapter 4 "Troubleshooting" add after the last section the following information:

If you are using a Sybase database in your Tivoli environment and the manual configuration of the environment is performed before installing the

Activity Planner component, then the same configuration should be repeated after the Activity Planner installation because the settings of the LD_LIBRARY_PATH environment variable are overwritten by the Activity Planner installation.

Defect 58569

In Chapter 24 "Troubleshooting" add after the last section the following information:

If you are using a Sybase database in your Tivoli environment and the manual configuration of the environment is performed before installing the Directory Query component, then the same configuration should be repeated after the Directory Query installation because the settings of the LD_LIBRARY_PATH environment variable are overwritten by the Directory Query installation.

Reference Manual for Software Distribution

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

APAR IY97515

In Chapter 1 "Editing the Software Package Definition File" in section "execute_user_program" in subsection called "Format of the execute_user_program Stanza" add before the paragraph:

The corequisite_file stanza comprises two different sets of attributes, the add_file set and add_directory set.

the following information:

When you create a package that contains:

- user_program during_install with corequisite files (for example a file named coreq_install)
- user_program during_commit with corequisite files (for example a file name coreq_commit)

and install it in transactional, the two corequisite files (coreq_install and coreq_commit) are downloaded on the target. During the package installation, the coreq_install file is used and then deleted. During the package commit, the coreq_commit file is used but it is not deleted, because it might be used in the remove operation if performed in transactional mode.

APAR IY98382

In Chapter 1 "Editing the Software Package Definition File" modify the table contained in section "Attributes in the File System Stanzas" as follows:

in the table row for "name" under the column "required" replace "yes" with "no".

User's Guide for Inventory

This section contains new and updated information for IBM Tivoli Configuration Manager 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, mbsacli.exe, and ApprovedItems.txt files with the following files everywhere:

Table 68. WSUS patch management files

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

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.

APAR IY92834

In Appendix B "Commands", in the "wtransfer" section, add to the command description the following information:

The wtransfer command uses TAR software to compress the files to be transferred from one managed node to another. Some HP-UX platforms do not allow long file names, the size limit depends on the specific HP-UX version. So if the TAR software on the source workstation allows long file names, and the TAR software on an HP-UX target workstation does not, the files are not transferred. This problem can be solved only if a patch for the specific HP-UX version is available.

APAR IY96075

In Appendix E "Installing and uninstalling Common Inventory Technology (CIT)", in the "Installing Common Inventory Technology (CIT)" section, add the following information at the end of the current section:

Another way to change the CIT installation directory is to overwrite the default CIT_DestinationDirectory variable by editing the CIT_Preinstall.spb software package. The modified CIT_Preinstall.spb should then be distributed against all the gateway bundle directories replacing the old software package.

After installing any Tivoli Configuration Manager fix pack or interim fix and before performing any Tivoli Configuration Manager activity on the endpoints of your environment, perform the following steps:

1. Make a backup copy of the old CIT_Preinstall.spb software package before replacing it with the new one.
2. Import the software package using the **CIT_import.pl** command. This command creates a profile manager called Inventory_CIT_PM and adds to the profile manager the following software packages:

```
CIT.2.5.1003
CIT_Preinstall.CIT
```

Note: The CIT version 2.5.1003 might vary depending on which fix pack or interim fix you have installed.

3. Open the Inventory_CIT_PM profile manager and right-click CIT_Preinstall.CIT.
4. Select **Convert → Unbuild**.
5. Specify a path where to unbuild the software package, then select **Convert & Close**.
6. Open CIT_Preinstall.CIT using the software package editor and select **edit → variable list editor**. The default value for CIT_DestinationDirectory is:

```
$(Destination_$(os_family))$(FileSeparator)
tivoli$(FileSeparator)cit
```

Modify this value for example into

```
$(Destination_$(os_family))$(FileSeparator)
..$(FileSeparator)mydir
```

The new CIT installation directory is C:\Program Files\..\my_cit_dir on Windows workstations, or /opt/./my_cit_dir path on UNIX.

7. Save the modified variable value.
8. Right-click again CIT_Preinstall.CIT.
9. Select **Convert**.
10. Specify the old name and path of the software package, select the **overwrite** check box, then select **Convert & Close**. The default path used by the new CIT_preinstall.spb software package has been updated.
11. Replace the CIT_preinstall.spb software package on all the gateway bundle directories of your environment. All the following software packages must be replaced with the new .spb file:

```
lcf_bundle.41100\lib\aix4-r1\inv\CIT\SPB\CIT_Preinstall.spb
lcf_bundle.41100\lib\hpux10\inv\CIT\SPB\CIT_Preinstall.spb
lcf_bundle.41100\lib\linux-ix86\inv\CIT\SPB\CIT_Preinstall.spb
lcf_bundle.41100\lib\linux-ppc\inv\CIT\SPB\CIT_Preinstall.spb
lcf_bundle.41100\lib\linux-s390\inv\CIT\SPB\CIT_Preinstall.spb
lcf_bundle.41100\lib\solaris2\inv\CIT\SPB\CIT_Preinstall.spb
lcf_bundle.41100\lib\solaris2-ix86\inv\CIT\SPB\CIT_Preinstall.spb
lcf_bundle.41100\lib\w32-ix86\inv\CIT\SPB\CIT_Preinstall.spb
```

Note: It is recommended to test the new variable on some endpoints, before deploying it to the entire environment.

Feature 205561

In Appendix B "Commands" in section "wsetinvpchw" add to the list of the -a components the following new component:

Lpar Lists the number of processors allocated on each logical partition.

Feature 205561

In Appendix B "Commands" in section "wgetinvpchw" add at the end of the command output the following row:

```
Lpar:YES
```

Feature 205561

In Appendix E "Installing and uninstalling Common Inventory Technology (CIT)" after the "Managing the Inventory bundle dependency set" section, add the following new sections:

Scanning virtual environments

Inventory uses the CIT capability to collect LPAR information in a VMware environment.

VMware versions supported by CIT are shown in the table below:

Table 69. Versions of VMware supported by CIT

VMWare versions tested on CIT
ESX Server 3.0
ESX Server 3.01
ESX Server 3.02
ESX Server 2.5.3

Standard Inventory functions are not impacted whether the scans are performed on guest or host operating systems. However, due to a limitation of the data export function in the virtualization software, hardware and software discovery operations performed on guest operating systems might report incorrect data.

CIT provides an enabler to export correct data to the guest systems so that CIT instances installed on each operating system partition can discover and return correct data.

The CIT enabler stores the correct hardware information on the guest operating systems. In this way when a hardware Inventory scan starts on a guest operating system, the correct hardware configuration data is retrieved and stored in the Inventory RDBMS. You can query the data by running the LOGICAL_PARTITION_QUERY and the LOGICAL_PARTITIONED_SYSTEMS_QUERY

Starting the enabler

The CIT enabler is installed on the physical workstation which hosts the guest operating systems. The CIT enabler does not require an installation process. To use the CIT enabler, copy the files listed below from the /cit_enabler folder on the IBM Tivoli Configuration Manager, Version 4.2.3 Fix Pack 5 CD 1 to the workstation which hosts the guest operating systems:

Table 70. Enabler executable files

Virtual software	Supported OS	Files
VMware	Microsoft Windows	<ul style="list-style-type: none"> • cpuid.exe • retrieve.pl • wenvmw.exe
	Linux	<ul style="list-style-type: none"> • cpuid • dispatcher • retrieve.pl • wenvmw.sh

You must install VMware VmPerl Scripting API before starting the enabler for the first time.

To start the enabler, launch the executable file from a shell or command prompt. You can optionally specify the `-v` option to generate a log file named `env_out.txt`, which is created in the same directory where the executable file is located.

Notes:

1. The guest workstations must be active when the enabler is started.
2. Any guest workstations not active when the enabler is running, are not detected.
3. If you run the enabler after the configuration changes are applied to the guest workstation, the updated data is returned by the hardware scan.
4. The information retrieved by the enabler is deleted after a reboot.

Enabler return codes

The following is a list of the return codes returned by the enabler. Return codes help you identify the result of the command.

A return code of 0 indicates that the command completed successfully:

OK: CIT ENabler return code = 0

while a nonzero return code indicates that an error occurred. The following example shows the case in which the user does not have enough privileges, when running the CIT enabler executable:

OK: CIT ENabler return code = 11
 ERROR: dispatcher return code = 11"

A complete list of all nonzero return codes is provided in the table below:

Table 71. Enabler return codes

Return value	Code	Description
RETRIEVE_NODECAPACITY_ERROR	1	Cannot collect host system processor number.
RETRIEVE_NODEID_ERROR	2	Cannot collect host system serial number.
RETRIEVE_VMCAPACITY_ERROR	3	Cannot collect number of processors assigned to virtual machines.
RETRIEVE_VMID_ERROR	4	Cannot collect virtual machines IDs.
SET_GUESTINFO_ERROR	5	Cannot transfer information from host system to guest systems.
GET_VMLIST_ERROR	6	Cannot retrieve list of registered virtual machines.
CONNECT_VM_ERROR	7	Cannot establish connection with virtual machines.
NO_PRIVILEGES	11	User does not have enough privileges when running the CIT enabler executable.
GENERIC_ERROR	-1	A generic error has occurred. For more information, enter the command again with the <code>-v</code> option. The resulting information is logged into the <code>env_out.txt</code> file.

Table 71. Enabler return codes (continued)

Return value	Code	Description
VMWARENOTFOUND_ERROR	100	VMware Server not found on host system.
VMWARENOTSUPPORTED_ERROR	105	VMware Server version not supported.
VMPerl_NOT_FOUND	120	VmPerl Scripting API not found or incorrectly configured.

Defect 205492

In Appendix E "Installing and uninstalling Common Inventory Technology (CIT)" in section "Installing Common Inventory Technology (CIT)" replace the current step 5 of the procedure with the following information:

On the Inventory server, run the following command:

```
winstsp -f -ty @CIT.2.5.1003 @Endpoint:ep1
wcommstsp -f @CIT.2.5.1003 @Endpoint:ep1
```

where:

ep1 Is the name of the endpoint.

Defect 205493

In Appendix E "Installing and uninstalling Common Inventory Technology (CIT)" in section "Installing Common Inventory Technology (CIT)" replace the current step 2 of the procedure with the following information:

On the Inventory server, run the following command:

```
$BINDIR/./generic/inv/SCRIPTS/CIT_import.pl -d CD_ROM/CIT_SPB
```

where

CD_ROM/CIT_SPB

Specifies the path where the CIT_Preinstall.spb and CIT.spb software packages are located on the IBM Tivoli Configuration Manager, Version 4.2.3 Fix Pack 3 CD 1.

You can also copy the software packages to a local folder and run the command locally.

Defect 203233

In Appendix F "Troubleshooting" add the following new section called **Common Inventory Technology scanners**:

If you experience issues related to Inventory hardware and software scans, for example the scan fails or does not collect all the expected information, it is necessary to use a troubleshooting procedure specific for the Common Inventory Technology component.

Collect the configuration files that Tivoli Configuration Manager writes and passes to the Common Inventory Technology scanners as input parameters, and the command line syntax that Tivoli Configuration Manager uses when invoking the Common Inventory Technology scanners. Depending on the different customizations of the InventoryConfig profile and the platform on which the scan runs, the above-mentioned commands and configuration files are:

Table 72. Commands and configuration files on Windows platforms

Windows		
Type of scan	Command	Configuration file
Hardware scan	C:\Program Files\tivoli\cit \bin\wscanhw -c C:\win_ep_name\ \inv\SCAN\config.xml -o C:\win_ep_name\inv\SCAN\ tivhscan.mif-m	config.xml
Scan for installed products using signature matching	C:\Program Files\tivoli\cit \bin\wscansw -i C:\win_ep_name\ \inv\SCAN\wscansw.xml -o C:\win_ep_name\inv\SCAN\ swscan.xml -c C:\win_ep_name\ \inv\SCAN\config.xml -e C:\win_ep_name\inv\SCAN\ warning.out	wscansw.xml, config.xml
Scan files for basic information	C:\Program Files\tivoli\cit \bin\wscanfs -c C:\win_ep_name\ \inv\SCAN\config.xml -o C:\win_ep_name\ \inv\SCAN\tivfscan.mif -m	config.xml
Scan files for header information	C:\Program Files\tivoli\cit\ bin\wscanfs -c C:\win_ep_name\ \inv\SCAN\config3.xml -o C:\win_ep_name\inv\SCAN\ tivwscan.mif -m	config3.xml
Scan registry for product information	C:\Program Files\tivoli\cit\ bin\wscanvpd -c C:\win_ep_name\ \inv\SCAN\config.xml -o C:\win_ep_name\inv\SCAN\ tivrscan.mif -m	config.xml

Table 73. Commands and configuration files on UNIX platforms

UNIX		
Type of scan	Command	Configuration file
Hardware scan	/opt/tivoli/cit/bin/wscanhw -c /tivoli/unix_ep_name/ /inv/SCAN/config.xml -o /tivoli/unix_ep_name //inv/SCAN/ tivhscan.mif -m	config.xml
Scan for installed products using signature matching	/opt/tivoli/cit/bin/wscansw -i /tivoli/unix_ep_name/ /inv/SCAN/wscansw.xml -o /tivoli/unix_ep_name/ /inv/SCAN/swscan.xml -c /tivoli/unix_ep_name//inv/ SCAN/config.xml -e /tivoli/ unix_ep_name//inv/SCAN/ warning.out	wscansw.xml, config.xml
Scan files for basic information	/opt/tivoli/cit/bin/wscanfs -c /tivoli/unix_ep_name// inv/SCAN/config.xml -o /tivoli/unix_ep_name/ /inv/SCAN/tivfscan.mif -m	config.xml

Table 73. Commands and configuration files on UNIX platforms (continued)

UNIX		
Type of scan	Command	Configuration file
Scan registry for product information	/opt/tivoli/cit/bin/wscanvpd -c /tivoli/unix_ep_name//inv/ SCAN/config.xml -o /tivoli/ unix_ep_name//inv/SCAN/ tivrsan.mif -m	config.xml

The Common Inventory Technology scanners might return error codes. Return codes help you identify the result of the command: a return code of 0 indicates that the command completed successfully, while a nonzero return code indicates that an error occurred. A list of all nonzero return codes is given in Table 74:

Table 74. Return codes

Return value	Code	Description
WSRC_WRONG_PARMS	1	One or more CLI options are incorrect.
WSRC_INPUT_FILE_PARSE_ERROR	2	An error occurred while parsing the configuration file.
WSRC_SIGNATURE_FILE_PARSE_ERROR	3	An error occurred while parsing the signature file.
WSRC_OUTPUT_FILE_ERROR	4	An error occurred while writing the output file.
WSRC_INPUT_FILE_ERROR	5	An error occurred while reading the input file.
WSRC_MISSING_SIGNATURE_FILE	6	No signature file was specified and no default signature file is available.
WSRC_VALUE_OUT_OF_BOUND	7	One of the values you specified exceeds the assigned limits.
WSRC_INTERNAL_ERROR	8	An internal error has occurred.
WSRC_TIMEOUT_ELAPSED	9	The specified timeout has expired.
WSRC_UPGRADE_IN_PROGRESS	10	CIT is being upgraded and commands are momentarily not responding.
WSRC_FILE_READ_ONLY	11	The output file is read only.
WSRC_INIFILE_NOT_FOUND	12	The cit.ini file was not found.
WSRC_CITFILE_NOT_FOUND	13	The CIT configuration file was not found.
WSRC_CCLOGFILE_NOT_FOUND	14	The CitTrace.properties file was not found.
WSRC_KEY_NOT_FOUND	15	The value you specified is incorrect.
WSRC_VALUE_NOT_VALID	16	The specified value is not valid.
WSRC_KEY_CANNOT_CHANGE	17	The specified key cannot be modified.
WSRC_FILE_CANNOT_OPEN	18	Cannot open the specified file.
WSRC_FILE_CANNOT_RENAME	19	Cannot rename the specified file.
WSRC_FILE_CANNOT_DELETE	20	Cannot delete the specified file.

Table 74. Return codes (continued)

Return value	Code	Description
WSRC_CITFILE_NOT_VALID	21	The cit.ini file is corrupt.
WSRC_CIT_TRACEFILE_NOT_VALID	22	The trace file is corrupt.
WSRC_INVALID_AGE	24	The age you specified is incorrect.
WSRC_INVALID_TIMEOUT	25	The timeout you specified is incorrect.
WSRC_INVALID_ATTRIBUTE	26	The attribute you specified is incorrect.
WSRC_INVALID_OUTPUT_FORMAT	27	The output format you specified is not supported.
WSRC_CANNOT_LOAD_PROVIDER	28	The required .dll or shared library file is not available.
WSRC_QUERY_TIMED_OUT	29	The query has reached the timeout.
WSRC_QUERY_FAILED	30	The query has failed.
WSRC_PROCESS_INTERRUPTED	31	The process was interrupted.
WSRC_NO_CONFIG_NAME	32	No configuration file was specified.
WSRC_NO_CONFIG_OPTION	33	No configuration option was specified.
WSRC_NO_OUTPUT_NAME	34	No output file was specified.
WSRC_NO_PARMS	35	No parameters were specified.
WSRC_EMPTY_CONFIG_ELEMENT	36	The configuration file contains an empty element.
WSRC_FAILURE	37	An internal error has occurred.
WSRC_NO_SORT_FIELD_NAME	38	You specified the sort option in the command without specifying a sort criterion.
WSRC_INVALID_SORT_FIELD_NAME	39	The sort criterion you specified is incorrect.
WSRC_WARNING_FILE_ERROR	40	An error has occurred while attempting to create the warning file during a software scan.
WSRC_UNABLE_TO_INITIALIZE	41	The process initialization failed.
WSRC_MISSING_XSS_SCHEMA_FILE	42	Cannot find the signature catalog schema.
WSRC_UNABLE_INSTALL_DRIVER	45	Cannot install the CITMDRV_IA64.SYS, CITMDRV_AMD64.SYS, CITMDRV.SYS drivers.
WSRC_UNABLE_LOAD_CITMEMDLL	46	Cannot load the CITMEM.DLL library.
WSRC_UNABLE_LOAD_SYMBOL_IN_CITMEM	47	Cannot load the symbols in the CITMEM.DLL library.
WSRC_UNABLE_READ_CITMEMDLL	48	Cannot read the CITMEM.DLL library.
WSRC_FILE_ACCESS_DENIED	49	The user does not have sufficient rights to access the file.

Table 74. Return codes (continued)

Return value	Code	Description
WSRC_NOT_AUTHORIZED	50	The user does not have sufficient rights to perform the operation.
WSRC_FILE_NOT_FOUND	51	The specified file or directory does not exist.

Defect 204521

In Appendix F "Troubleshooting" add the following new section called **Common Inventory Technology installations:**

The default installation of Common Inventory Technology is performed on the endpoints using the Tivoli Configuration Manager Software Distribution disconnected command line.

Use the following troubleshooting procedure when installing Common Inventory Technology on Tivoli Configuration Manager workstations:

1. Enable the Software Distribution disconnected CLI traces by opening on the endpoint the Software Distribution swdis.ini file, which can be found under the %WINDIR% directory on Windows and the /etc/Tivoli directory on UNIX, and set the trace_level value to 5 in the MOBILE section of the file. A sample MOBILE section of the swdis.ini file follows:

```
[#MOBILE]
product_dir=C:\swdis
working_dir=C:\swdis\work
backup_dir=C:\swdis\backup
profile_dir=C:\swdis\work\profiles
trace_level=0
trace_size=1000000
send_timeout=300
autopack_dir=C:\swdis\autopack
staging_dir=swdis\service
user_file_variables=C:\swdis\swdis.var
import_libraries=spd,libecimp
```

2. Distribute an Inventory profile by running the wdistinv command using the inv_ep_debug option, so that when the Inventory scan runs on the endpoint, a log file called INVxxxxx.LOG (where xxxxx is the scan_id) is created under the inv/SCAN directory.
3. Collect under the inv/SCAN directory the file INVxxxxx.LOG, and under the product directory specified in the MOBILE section mentioned in step 2 the trace files *.trc, and under the working directory the epsp.cat file. Collect the cit.ini file, which can be found under the %WINDIR% directory on Windows or the /etc/Tivoli directory on UNIX.

APAR IY96992

In Appendix E "Troubleshooting" section "Common Inventory Technology traces" modify the following information:

The current path under "On Windows systems" should be replaced with:

```
C:/Program Files/ibm/tivoli/common/CIT/logs/traceCIT.log
```

The current path under "On UNIX systems" should be replaced with:

```
/usr/ibm/tivoli/common/CIT/logs/traceCIT.log
```

APAR IY99115

In Appendix B "Commands" section "winvmigrate" subsection "examples" replace:

```
winvmigrate -c C:\temp\ITLM22ForIBM_SoftwareCatalog_2006-06-30.xml
```

with:

```
winvmigrate -c C:\temp\IBM_SoftwareCatalog.xml
```

APAR IY99115

In Chapter 5 "Collecting custom information with Inventory" section "Using signatures" replace the current instructions at the end of the section with the following instructions:

- Navigate to <http://www.ibm.com>
- Select "Support and downloads"
- Select "Software"
- Select "Download"
- In the search bar enter "Software Signature Catalog"
- Search for the most recent
 - Software Catalog YYYY-MM-DD for ITLM, version 2.2/2.3 - All Software **or**
 - Software Catalog YYYY-MM-DD for ITCM 4.2.3 Fixpack 2 and Higher **or**
 - Software Catalog 2007-05-31 for Inventory

Note: This last catalog is in the old INI format.

APAR IY99115

In Chapter 5 "Collecting custom information with Inventory" section "Using signatures" add at the end of the section the following new information:

From the following FTP Web site

```
ftp://ftp.software.ibm.com/software/tivoli_support/misc/Cand0/TivoliCatalog/
```

you can download the following catalog files:

- ITLM22_SoftwareCatalog_YYYY-MM-DD.xml
- YYMMDDSWSIGS.INI
- ITLM22ForIBM_SoftwareCatalog_YYYY-MM-DD.xml
- IBMUseOnlySoftwareCatalog_YYYY-MM-DD.xml
- IBMSoftwareCatalog_YYYY-MM-DD.xml

Note: The files that can be used by Tivoli Configuration Manager are:

- ITLM22_SoftwareCatalog_YYYY-MM-DD.xml
- YYMMDDSWSIGS.INI

The other files are for Tivoli License Manager only.

Since June 2007 the new naming convention of these files is the following:

- itlcm22-ibmProducts-fullSwCat-YYYYMMDD.xml
- itlcm22-allProducts-fullSwCat-YYYYMMDD.xml
- itlcm21-ibmProducts-fullSwCat-YYYYMMDD.xml
- itlcm21-allProducts-fullSwCat-YYYYMMDD.xml
- inventory-allProducts-fullSwCat-YYYYMMDD.ini

Note: The files that can be used by Tivoli Configuration Manager are:

- itlcm22-allProducts-fullSwCat-YYYYMMDD.xml
- inventory-allProducts-fullSwCat-YYYYMMDD.ini

The other files are for Tivoli License Manager only.

Database Schema Reference

This section contains new and updated information for IBM Tivoli Configuration Manager Database Schema Reference:

Defect 202144

In Chapter 3 "Configuration repository views", in the "Inventory views" section, at the end of the MATCH_SWARE_VIEW description add the following note:

The extended signatures are not displayed by the MATCH_SWARE_VIEW, while they are displayed by the INST_SWARE_VIEW.

APAR IY95425

In Chapter 5 "Configuration repository tables", in the "Inventory tables" section, at the end of the FILE_DESC table description add the following note:

The following columns:

FILE_COMMENTS
FILE_INTERNAL_NAME
FILE_PRODUCT_NAME
FILE_COMPANY_NAME
FILE_LEG_COPYRIGHT
FILE_PROD_VERSION
FILE_DESCRIPTION
FILE_LEG_TRADEMARK
FILE_PRIVATE_BUILD
FILE_VERSION
FILE_ORIG_FILENAME
FILE_SPECIAL_BUILD

are populated only by data coming from scans run against pervasive devices.

Feature 205561

In Chapter 3 "Configuration repository views" in section "LPAR_VIEW" check all the Windows NT/2000 columns of the table and add the following note after the table:

Note: For these operating systems, on a VMware environment, you must run the CIT enabler on the host server after starting the guest workstation and before running the scan.

Feature 205561

In Chapter 3 "Configuration repository views" in section "LOGICAL_PARTITIONS_VIEW" check all the Windows NT/2000 columns of the table and add the following note after the table:

Note: For these operating systems, on a VMware environment, you must run the CIT enabler on the host server after starting the guest workstation and before running the scan.

Feature 205561

In Chapter 3 "Configuration repository views" in section

"LPAR_SYSTEMS_VIEW" check all the Windows NT/2000 columns of the table and add the following note after the table:

Note: For these operating systems, on a VMware environment, you must run the CIT enabler on the host server after starting the guest workstation and before running the scan.

Feature 205563

In Chapter 5 "Configuration repository tables" section "Inventory tables" add the following new subsection:

ALL_NET_ADAPTER

Describes the physical and virtual network adapter installed on a system. One record exists for each network adapter for each system scanned.

Populated by an inventory hardware scan.

The columns in this table are as follows:

COMPUTER_SYS_ID (primary key)

ADAPTER_ID (primary key)

PERM_MAC_ADDR

CURRENT_ADDR

ADAPTER_TYPE

ADAPTER_MODEL

MANUFACTURER

INST_DATE

RECORD_TIME

Feature 205563

In Chapter 4 "Queries" section "Inventory queries" add the following new subsection:

ALL_NET_CARD_QUERY

Returns information about network cards on target systems.

Runs against the view ALL_NET_CARD_VIEW.

The columns in this query are as follows:

TME_OBJECT_LABEL

TME_OBJECT_ID

COMPUTER_SYS_ID

ADAPTER_ID

PERM_MAC_ADDR

CURRENT_ADDR

ADAPTER_TYPE

ADAPTER_MODEL

MANUFACTURER

INST_DATE

RECORD_TIME

Feature 205563

In Chapter 4 "Queries" section "Historical inventory queries" add **H_ALL_NET_CARD_QUERY** to the existing list.

Feature 205563

In Chapter 3 "Configuration repository views" in section "Inventory views" add the following new subsection:

ALL_NET_CARD_VIEW

Displays information about physical and virtual network cards on target systems.

Based on the COMPUTER and ALL_NET_ADAPTER tables.

The columns in this view are as follows:

Column Name	Description	AIX	HP-UX	Linux (S/390)	Linux (PC)	NetWare	OS/2	OS/400	Solaris	Windows 98	Windows NT/2000
TME_OBJECT_LABEL	The object label for the system.	✓	✓	✓	✓		✓		✓	✓	✓
TME_OBJECT_ID	The object ID for the system.	✓	✓	✓	✓		✓		✓	✓	✓
COMPUTER_SYS_ID	The computer system ID.	✓	✓	✓	✓		✓		✓	✓	✓
ADAPTER_ID	The unique ID of the adapter.	✓	✓	✓	✓		✓		✓	✓	✓
PERM_MAC_ADDR	The permanent media access control (MAC) address for the system.	✓	✓		✓				✓	✓	✓
CURRENT_ADDR	The current network address for the system.	✓	✓		✓				✓	✓	✓
ADAPTER_TYPE	The network adapter installed on the system.	✓	✓	✓	✓					✓	✓
ADAPTER_MODEL	The model of the network adapter installed on the system.	✓		✓	✓		✓		✓	✓	✓
MANUFACTURER	The manufacturer of the network adapter installed on the system.						✓		✓	✓	✓
INST_DATE	The date that the network card was installed on the system.								✓		^w
RECORD_TIME	The time that the data was updated at the database.	✓	✓	✓	✓		✓		✓	✓	✓

^w Reported only on systems with WMI.

Feature 205563

In Chapter 3 "Configuration repository views" in section "Historical inventory views" add **H_ALL_NET_CARD_VIEW** to the existing list.

APAR IY97995, IY97996

In Chapter 3 "Configuration repository views" in section "Inventory views" before the subsection called "ASP_VIEW" add the following new note:

Note: Some views, created by the .sql scripts, such as CAT_SIG_V and CHECK_SIG are not described in this manual because they are used for product internal tasks only, and do not apply to an external user.

APAR IY97094

In Chapter 5 "Configuration repository tables" at the end of the "SIGNATURE" section add the following note:

Note: The possible values for the IBM_SOURCE key are:

CUSTOM

A signature you created.

IBM

A signature loaded from the IBM signature catalog.

SWD

A signature created by the Tivoli Configuration Manager Software Distribution.

APAR IY97190

In Chapter 3 "Configuration repository views" section "COMPUTER_VIEW" insert a row in the existing table having as column name OS_KERNEL_MODE, as description "The operating system kernel mode (32-bit or 64-bit)" and check all operating systems except for OS/2, NetWare, OS/400 and Linux (pc).

APAR IY97190

In Chapter 4 "Queries" section "COMPUTER_QUERY" add OS_KERNEL_MODE to the existing list.

APAR IY97190

In Chapter 5 "Configuration repository tables" section "COMPUTER" add OS_KERNEL_MODE to the existing list.

Patch Management Guide

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

In Chapter 2 "Installing the automated patch management solution", in the "Upgrading the Patch Management Automation Server driver" section, replace step 6 with the following text:

- Create the tcm-dcm_xx.xml file by running the bash `$TIO_HOME/xml/xml_update.sh` command from a Windows command prompt. The tcm-dcm_xx.xml file is created, where the xx value depends on the level of fix pack you are installing.

Note: To determine which XML file to use run the following command from a command prompt:

```
ls -la "$TIO_HOME"/xml
```

In Chapter 7 "Troubleshooting", at the end of the "Other common problems" section, add the "Wrong code set" sub-section:

Cause: If you are defining a name for a group, a patch, or any other object, containing a character code set that is not defined in the Tivoli environment, the character is not displayed correctly in the name.

Solution: Set the TIS_CODESET variable to the appropriate code set as follows:

1. Copy the Tivoli environment settings to a temporary file:

```
odadmin environ get >env.out
```

2. Add the following line to the temporary file:

```
TIS_CODESET = TIS_CODESET
```

where *TIS_CODESET* is the new value of the code set.

3. Import the new *TIS_CODESET* setting value in the Tivoli environment:

```
odadmin environ set < env.out
```

4. Stop and start the Tivoli server:

```
reexec oserv all
```

APAR IY98107

In Chapter 1 "Introduction" in section "Planning your environment" modify the table called "Patch tools" as follows:

At the end of the *wsusscn2.cab* description add the following note:

Note: The *wsusscn2.cab* file is renamed as *wsuscan.cab* during the download process. After updating the catalog with the new *wsusscn2.cab* file, verify if the date of the *wsuscan.cab* file matches the size and date of the new *wsusscn2.cab* file.

Defect 59014

In Chapter 3 "Configuration and administrative tasks" in section "Configuring automated patch management settings" add the following information:

At the end of the **Add tioadmin login** description add the following note:

Note: Ensure that the *tioadmin* user is allowed to write to the following product directories:

- *product_dir*
- *provider_patch_dir*
- *provider_spb_dir*

This is valid only if these directories are local.

Defect 59003

In Chapter 1 "Introduction" in section "Operating systems and applications managed with this solution" replace the current bullet:

- Windows Vista (valid for fix pack 3)

with the following information:

- Windows Vista (valid for fix pack 3 or later fix packs using WSUS server 2.1)

APAR IZ01645

In Chapter 7 "Troubleshooting" in section "Common problems and troubleshooting scenarios" add at the end of the subsection called "Other common problems" the following information:

Windows Update Agent (WUA) does not work properly

For the Microsoft Windows Update Agent (WUA) to work properly, ensure that the following Windows services are enabled and set to Automatic:

- Automatic Updates
- Background Intelligent Transfer Service (BITS)

In addition, for the WUA to receive necessary updates from other Microsoft products, ensure that Windows Installer 3.1 is installed.

User's Guide for Operating System Deployment Solution

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

In Chapter 1 "Overview", in the "Components of an operating system imaging solution" section, replace the note under the **IBM Tivoli Provisioning Manager for Operating System Deployment server at Spoke level** description with the following:

Note: The IBM Tivoli Provisioning Manager for Operating System Deployment server at Spoke level must be a managed node and endpoint. The `config.csv` file contains a line for the IBM Tivoli Provisioning Manager for Operating System Deployment server at Spoke level. The "Description" field of this line must contain a name equal to the label of the endpoint installed on the IBM Tivoli Provisioning Manager for Operating System Deployment server at Spoke level.

In Chapter 2 "Planning and installing your environment", at the end of the "Configuring the `Rembo.ini` file" section, add the following information:

After you customized the `rembo.ini` file, you must stop and start the Activity Planner engine by running the following commands from the Tivoli server bash shell:

```
wstopapm
wstartapm
```

In Chapter 2 "Planning and installing your environment", in the "Installation requirements for Tivoli Provisioning Manager for Operating System Deployment" section, after the "Server system requirements information", add the following information:

Operating System Requirements:

The Tivoli Provisioning Manager for Operating System Deployment servers must be installed on Windows platforms only.

In Chapter 2 "Planning and installing your environment", in the "How to set up Tivoli Provisioning Manager for Operating System Deployment" section, change the text as follows:

- Add the following step before step 6:
Configure the **Rembo Server** service to run logged on as a user that is a member of the Windows Administrators group, and that has one of the following Tivoli authorization roles:
 - super
 - senior
- Replace step 5 with the following step description:
Customize the `config.csv` file according to the guidelines described in:
http://www-1.ibm.com/support/docview.wss?rs=3176&context=SS3HLM&q1=config.csv&uid=swg21247013&loc=en_US&cs=utf-8&lang=en
and store a copy in the directory you created in the previous step for all the Tivoli Provisioning Manager for Operating System Deployment servers in your production environment.
- After step 6 add the following step:
Stop and start the **Rembo Server** service to load the customized `config.csv` file.

In Chapter 2 "Planning and installing your environment", in the "Requirements for the installation" section, replace the link in step 1 with the following:

<http://www.microsoft.com/downloads/details.aspx?familyid=0CAA294C-29D9-4449-81D5-4B69B97DF7AE&displaylang=en>

In Chapter 4, "Generating differential Tivoli Provisioning Manager for Operating System Deployment files", in the "Step 1: Generating the Differential RAD activity plan:" sub-section, modify step 3 as follows:

Enter a RAD file name that does not include special characters. This is because the **Update Slaves** activity passes the file name to a Tivoli bash script and the Tivoli bash does not support special characters.

In Chapter 4 "Implementing the operating system imaging solution", in the "Backing up user settings" section, replace the first two bullets under step 3 with the following:

- In the **Repository information** fields, define the location and access credentials for the repository where the user settings are to be backed up. It is recommended that you define a network drive as repository location. An example of repository location is the following:
`\\128.143.71.21\shared_directory_name\repository_directory.`

Note: If a plan that includes the backup activity 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.

- In the **Local user information** fields, define the target workstation user credentials for accessing the network.

In Chapter 4 "Implementing the operating system imaging solution", in the "Refreshing a workstation" section, replace the first two bullets under step 3 with the following:

- In the **Repository information** fields, define the location and access credentials for the repository where the endpoint information is to be backed up. It is recommended that you define a network drive as repository location. An example of repository location is the following:
`\\128.143.71.21\shared_directory_name\repository_directory.`
- In the **Local user information** fields, define the target workstation user credentials for accessing the network.

In Chapter 4 "Implementing the operating system imaging solution", in the "Refreshing a workstation" section, replace the first two bullets under step 3 with the following:

- In the **Repository information** fields, define the location and access credentials for the repository where the user settings are backed up. It is recommended that you define a network drive as repository location. An example of repository location is the following: `\\128.143.71.21\shared_directory_name\repository_directory.`

Note: If a plan that includes the restore activity 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.

- In the **Local user information** fields, define the target workstation user credentials for accessing the network.

Tivoli Integration Pack for NetView User's Guide

This section contains new and updated information for IBM Tivoli Integration Pack for NetView User's Guide:

APAR IY92481

In Chapter 3, in the "Configuring Tivoli Discovery" section, add the following sentence at the end of the existing note:

The NetView database and the Tivoli Report are updated only with those resources having the transport protocol set to AF_INET.

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*.

Release Notes

This section contains new and updated information for IBM Tivoli Configuration Manager Release Notes:

APAR IY81403

In the section "Supported Databases" the following paragraph should be added at the end of the section:

The "temporary tables" feature does not apply to Sybase and Informix, because these two RDBMS databases do not clean up the contents of a temporary table after the commit operation, but only after releasing the session to the database. You can therefore receive the following error message, which might cause a performance decrease:

Sybase Server Error: Msgno 3621 Level 10 State 0
Command has been aborted.

APAR IY90442

In Chapter 2 "Installation and Upgrade Notes", in the "Supported

operating systems" section, the table "Supported operating systems by administrative interfaces and endpoint" should be modified as follows:

- Two new columns under the header "Endpoint" should be added.
- The columns should contain "Software Distribution" and "Inventory scan" respectively.
- Under both columns all the platforms listed below in the table should be marked with an "X".

APAR IZ01088

In Chapter 3 "Software limitations, problems, and workarounds", in section "Automated Patch Management" add the following limitation:

The Windows Server Update Services (WSUS) server version 3.0 is not supported. Use the WSUS server version 2.1.

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.

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

- wswdcfg
- waccptsp
- wcommtsp
- winstsp
- wremovsp
- wspmldata
- wswdmgr
- wundosp
- wversp

The changes to these commands are documented in the *IBM Tivoli Configuration Manager: Reference Manual for Software Distribution*.

Activity Planner

- wsubpln

The changes to this command are documented in the *IBM Tivoli Configuration Manager: User' Guide for Deployment Services*.

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 *IBM Tivoli 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

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.