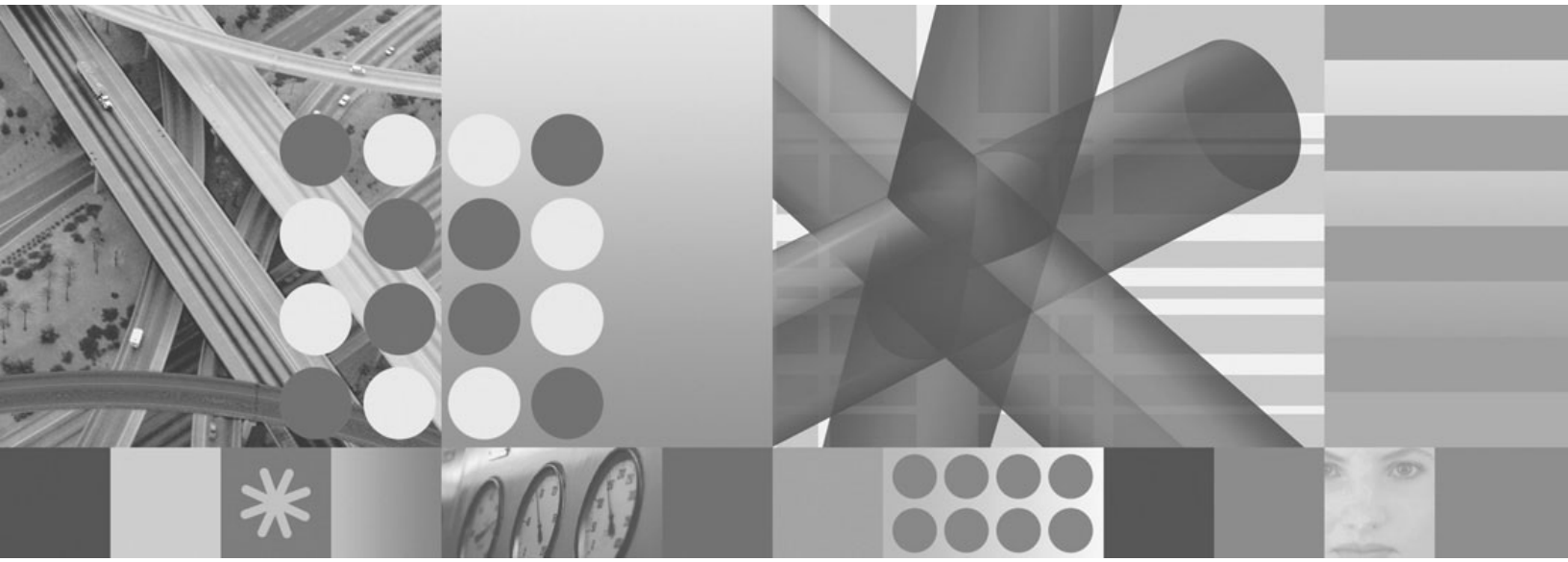
Tivoli® IBM Tivoli Monitoring

Version 6.1

Fix Pack 003 Readme and Documentation Addendum

Tivoli® IBM Tivoli Monitoring

Version 6.1



Fix Pack 003 Readme and Documentation Addendum

Note
Before using this information and the product it supports, read the information in Appendix C, "Notices," on page 125.

First edition (August 2006)

This edition applies to the version 6, release 1, modification 0 of IBM Tivoli Monitoring (product number 5724-C04) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Chapter 1. Fix Pack 003 overview

Fix Pack 003 is a cumulative fix pack for IBM® Tivoli® Monitoring, Version 6.1.0. This readme and documentation addendum file provides details about installing the fix pack and information about changes to IBM Tivoli Monitoring in this release.

IBM Tivoli Monitoring, Fix Pack 003, contains the component fix packs listed in Table 1. See Chapter 2, "Installation instructions," on page 21 for detailed installation procedures for all of these fix packs.

Table 1. Fix Pack 003 component fix packs

Fix pack name	Description
6.1.0-TIV-ITM_INST-FP0003	IBM Tivoli Monitoring Global-common Component (required for all monitoring components)
6.1.0-TIV-ITM_TEMS-FP0003	Tivoli Enterprise™ Management Server
6.1.0-TIV-ITM_TEP-FP0003	Tivoli Enterprise Portal desktop client
6.1.0-TIV-ITM_TEPS-FP0003	Tivoli Enterprise Portal Server
6.1.0-TIV-ITM_TEMA-FP0003	IBM Tivoli Monitoring Shared Libraries for the monitoring agent
6.1.0-TIV-ITM_UA-FP0003	Universal Agent
6.1.0-TIV-ITM_TDW-FP0003	Warehouse Summarization and Pruning agent and Warehouse Proxy agent
6.1.0-TIV-ITM_LINUX-FP0003	Linux OS Monitoring agent
6.1.0-TIV-ITM_UNIX-FP0003	UNIX® OS Monitoring agent
6.1.0-TIV-ITM_i5OS-FP0003	i5/OS™ OS Monitoring agent
6.1.0-TIV-ITM_UXLOG-FP0003	UNIX Log agent
6.1.0-TIV-ITM_TEC-FP0003	IBM Tivoli Monitoring Tivoli Enterprise Console event synchronization
6.1.0-TIV-ITM-LP-FP0003	IBM Tivoli Monitoring V6.1.0.3 Language Pack

Attention:

1. If you are running your monitoring server on a z/OS system, be sure to check for the z/OS Fix Pack 003 PTF, available from IBM Software Support.
2. There is no new fix pack for the Windows OS agent. Use Fix Pack 002, available from IBM Software Support, for this agent.

What's new in this fix pack

The following new functions have been added to IBM Tivoli Monitoring in this fix pack:

Note: The new functions listed below are available in all languages, although they are displayed in English only. Although the interfaces for these functions are English-only, the functions themselves work in all locales. The interfaces will be translated in the next release of IBM Tivoli Monitoring.

- Support for the Tivoli Enterprise Portal Server on AIX version 5.3. See Chapter 5, “Installing and configuring the portal server on AIX,” on page 65 for installation information.
- Support for the Warehouse Proxy on AIX version 5.3. See Chapter 6, “Installing and configuring the Warehouse Proxy on AIX and Linux,” on page 69 for more information.
- Support for accessing and displaying data from an Oracle database for your Tivoli Data Warehouse when you are running the Tivoli Enterprise Portal Server on a Linux computer. See Chapter 7, “Configuring a Linux portal server to support an Oracle data warehouse,” on page 77.
- Support for importing and exporting workspaces from the Tivoli Enterprise Portal through the command-line interface. You can now easily use a set of commands to export a workspace from one system to another, reducing the amount of time you need to spend customizing your monitoring environment. For information about the commands that enable this function, see Chapter 12, “New tacmd commands,” on page 101.
- Support for creating managed system lists (a defined set of managed systems) through the command-line interface. You can create your own managed system lists for any grouping of managed systems and apply them to the following tasks:
  - The distribution of a situation
  - The distribution for policies correlated by business application group
  - Managed system assignments for queries
  - Managed system assignments for Navigator items in custom Navigator views

  For information about the new commands that enable this function, see Chapter 12, “New tacmd commands,” on page 101.
- Dynamic workspace linking. A new link type has been added to the workspace link feature that enables the link author to identify the target workspace by the host identifier. The dynamic link type adds more opportunities for workspace linking, such as to provide links to workspaces of other types of monitoring agents. For detailed information on using this new function, see the ″New in this release″ help topic in the Tivoli Enterprise Portal online help.
- Ability to create a topology view in the Tivoli Enterprise Portal. For monitoring products that support the topology view, you can add the view to a workspace to graphically show objects and their logical relationships to one another. For detailed information on using this new function, see the ″New in this release″ help topic in the Tivoli Enterprise Portal online help.
- TMS Infrastructure view. The Tivoli Enterprise Monitoring Server has a topology view called TMS (Tivoli Monitoring Services) Infrastructure view, which visually expresses the relationships and linking of monitoring agents and other components to the hub monitoring server. For detailed information on using this new function, see the ″New in this release″ help topic in the Tivoli Enterprise Portal online help.
- Enhancements to event management through the Tivoli Enterprise Portal. You can now add more detailed note information, as well as attach files, to individual events. A new user permission has been added to enable users to attach files. Also, the way that events are acknowledged has also been improved. For detailed information on using these new functions, see the ″New in this release″ help topic in the Tivoli Enterprise Portal online help. For information on configuration changes to support these functions, see “Event management configuration” on page 60.

- Additional hyperlinks can be added to the Event Tools view (part of the event management enhancements). These links can be pointers to Web sites, as well as mechanisms for launching applications on the client computer. The links are defined in the eventtools.htm file, located in the *ITMinstall_dir*/cnb directory, where *ITMinstall_dir* is the directory where you installed IBM Tivoli Monitoring. To add new hyperlinks or to modify existing hyperlinks, open the eventtools.htm file in a text editor. Instructions for editing the hyperlinks are contained in this file as comments.
- A Discovery Library adapter (DLA) for use in a configuration management database (CMDB), such as IBM Tivoli Change and Configuration Management Database. The DLA scans the IBM Tivoli Monitoring environment and identifies the managed systems in the environment. You can then feed this information into IBM Tivoli Change and Configuration Management Database or another CMDB. For more information, see Chapter 8, "Using the Tivoli Monitoring Services Discovery Library adapter," on page 83.
- The IBM Tivoli Monitoring Tivoli Enterprise Console event synchronization installation wizard has been updated to provide the option to automatically stop and restart your event server. In previous releases, you had to do this manually. For information about installing the event synchronization fix pack that enables this change, see "Installing the IBM Tivoli Enterprise Console event synchronization fix pack" on page 42.

  If you are installing the event synchronization for the first time (instead of updating an existing installation), use the installation instructions provided in "Chapter 6: Installing the IBM Tivoli Enterprise Console event synchronization" in the *IBM Tivoli Monitoring Installation and Setup Guide*. This document is available in the IBM Tivoli Monitoring information center at http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/index.jsp?toc=/com.ibm.itm.doc/toc.xml.
- Ability to link from a situation event in the embedded Tivoli Enterprise Console event console to the Event Results workspace in the Tivoli Enterprise Portal. To use this new function, right-click a situation event from inside the Tivoli Enterprise Console event console and click **ITM Situations → Situation Results**.
- For the Tivoli Enterprise Portal, the HTTP proxy server parameters have been removed from the Configure Tivoli Enterprise Portal Browser window, and the instructions in the Administrator's Guide to Enable the HTTP Proxy Server for the browser client are no longer valid. See "Change to enablement of HTTP proxy server on browser client" on page 61 for more information.
- For the Tivoli Enterprise Portal, when you have security enabled, you can now control the number of log in attempts before a user is locked out of the portal. See "Controlling the number of log in attempts" on page 59 for more information.
- A new utility, secureMain, has been added to change the file permissions level for files on Linux and UNIX computers. After initial installation, many files have a 777 permission level. The secureMain script enables you to easily change these permissions. See Chapter 9, "Using the secureMain utility," on page 85 for more information.
- The Linux OS agent has added Linux File and Directory monitoring, file information attributes to refer to file information characteristics. The File Information workspace shows a list of files and directories on your file system. The default directory shown is the / directory. See "Linux File and Directory monitoring" on page 87 for additional information.
- The UNIX OS agent has added AIX Printer Queue Support monitoring, as well as the ability to monitor disk attributes (such as available free space) in

megabytes and gigabytes (instead of kilobytes). See "UNIX OS agent enhancements" on page 87 for more information.

- The i5/OS OS monitoring agent has added support for using the SSL communication protocol for communication between the agent and the monitoring server. For information on configuring this support, see "Support for SSL communication with the i5/OS monitoring agent" on page 88.

The following functions were added to IBM Tivoli Monitoring in a previous fix pack:

- Support for the Warehouse Proxy on Linux® operating systems. See Chapter 6, "Installing and configuring the Warehouse Proxy on AIX and Linux," on page 69 for more information.
- Support for multiple Warehouse Proxy agents in a single monitoring environment. See Chapter 11, "Installing and configuring multiple Warehouse Proxy agents," on page 97 for more information.
- Enhanced ease of adding new views within the Tivoli Enterprise Portal. See the online help in the Tivoli Enterprise Portal for information.
- Enhanced firewall functionality through the use of a gateway feature. For information about this function, see the ″Firewall Gateway Feature″ document in the IBM Tivoli Monitoring information center (located at http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/index.jsp?toc=/com.ibm.itm.doc/toc.xml).
- Increased default security for the Tivoli Enterprise Portal on Windows.

  When you are installing the full media that contains the fixes in IBM Tivoli Monitoring V6.1 Fix Pack 003 and related agent fix packs, there is a new requirement to type a Tivoli Enterprise Portal Server sysadmin password. You are prompted for this new password during installation. For silent installations, you can set the SYSADMINPWSD=value in the response file. A Windows® ID, sysadmin, is created.

  The password is *only* required for fresh installations on Windows (not on Linux). Any upgraded installations continue to function in the same way as the installation from which you are upgrading. Because the password is verified by the Windows operating system, you must create a password that conforms to any Windows password rules. The sysadmin ID must also conform to account policies on the computer where the software is installed.

In addition a number of customer APARs are addressed in this fix pack.

Supported operating systems

Fix Pack 003 adds support for additional operating systems. The following tables show which operating systems are supported for the different IBM Tivoli Monitoring components in this fix pack: monitoring server, portal server, portal client, monitoring agent, Warehouse Proxy, and Warehouse Proxy Summarization and Pruning agent. Support that has been added in this fix pack is marked with **bold** highlighting.

For additional information about the operating systems supported, see http://www-306.ibm.com/software/sysmgmt/products/support/Tivoli_Supported_Platforms.html.

Table 2 shows the support for monitoring components on Windows computers.

Table 2. Supported Windows operating systems

Operating system	Monitoring server	Portal server	Portal client[1]	OS monitoring agent[2]	Warehouse Proxy	Warehouse Summarization and Pruning agent
Windows 2000 Professional[3]			X	X		X
Windows 2000 Server	X	X	X	X	X	X
Windows 2000 Advanced Server	X	X	X	X	X	X
Windows XP[3]			X	X	X	X
Windows 2003 Server SE (32 bit) with Service Pack 1[5]	X	X	X	X	X	X
Windows 2003 Server EE (32 bit) with Service Pack 1[5]	X	X	X	X	X	X
Windows 2003 SE (64 bit)				X		
Windows 2003 EE (64 bit)				X		
Windows 2003 Server on Itanium2				X		
Windows 2003 on VMWare ESX Server V2.5.2	**New**	**New**		**New**	**New**	**New**

Notes:

1. The Tivoli Enterprise Portal desktop client is supported on marked platforms. However, the browser client can only be accessed from Windows computers running Internet Explorer 6.
2. The **Monitoring agent** column indicates the platforms on which an operating system monitoring agent is supported. It does not indicate that any agent runs on any operating system. For example, to monitor a Linux computer, you must use a Linux monitoring agent, not a Windows monitoring agent.

   For information about the operating systems supported for non-OS agents, see the documentation for the specific agents you are using in your environment.
3. For the Windows 2000 Professional and Windows XP operating systems, the Microsoft End User License Agreement (EULA) does not license these operating systems to function as a server. Tivoli products that function as a server on these operating systems are supported for demonstration purposes only.
4. For Windows 2003 Server: If you do not plan to deploy Service Pack 1 in your environment at this time, you must download and install Microsoft® Installer 3.1 (KB893803), which is available from the Microsoft Download Web site (www.microsoft.com/downloads).

Table 3 shows the support for monitoring components on UNIX (non-Linux), i5/OS, and z/OS computers.

Table 3. Supported UNIX, i5/OS, and z/OS operating systems

Operating system	Monitoring server	Portal server	Portal client	OS monitoring agent[1, 2]	Warehouse Proxy	Warehouse Summarization and Pruning agent
AIX® V5.1 (32/64 bit)				X		X
AIX V5.2 (32/64 bit)	X			X		X
AIX V5.3 (32/64 bit)	X	**NEW**		X	**NEW**	X
Solaris Operating Environment V8 (32/64 bit)	X			X		X
Solaris V9 (SPARC)	X			X		X
Solaris V10 (SPARC)	X			X		X
Solaris V10 (x86-64) on AMD Opteron	X			X		
Solaris Zones[3]	**New**			**New**[4]	`	
HP-UX 11.11 and 11.23 (32/64 bit) on PA-RISC[5]				X		
HP-UX 11.23 on Itanium2				X		
OS/400® 5.2				X		
i5/OS 5.3				X		
i5/OS 5.4				X		
z/OS® 1.4[6, 7]	X			X		
z/OS 1.5	X			X		
z/OS 1.6	X			X		
z/OS 1.7	X			X		

Notes:

1. The **Monitoring agent** column indicates the platforms on which an operating system monitoring agent is supported. It does not indicate that any agent runs on any operating system. For example, to monitor a Linux computer, you must use a Linux monitoring agent, not a Windows monitoring agent.

   For information about the operating systems supported for non-OS agents, see the documentation for the specific agents you are using in your environment.
2. If you are installing the OMEGAMON XE for Messaging agent on a 64-bit operating system, you must install the 32-bit version of the agent framework. See the OMEGAMON XE for Messaging bullet in Chapter 3, "Known problems and limitations," on page 53 for details on installing this framework.
3. The monitoring server can run in both local and global zones on Solaris; however, the OS monitoring agent can run only in global zones.
4. You cannot use the remote deployment function for the OS agent on this operating system. This applies to both fresh installations and upgrades. Instead, you must install locally.
5. For HP-UX, patch PHSS_30970 is required.
6. For information about installing the monitoring server on z/OS, see the Program Directory that comes with that product.
7. The OS monitoring agent for z/OS computers is part of the IBM Tivoli OMEGAMON for z/OS product.

Table 4 shows the monitoring components supported on Linux operating systems.

Table 4. Supported Linux operating systems

Operating system	Monitoring server	Portal server	Portal client[1]	OS monitoring agent[2]	Warehouse Proxy	Warehouse Summarization and Pruning agent
RedHat Enterprise Linux 2.1 Intel®				X		X
RedHat Enterprise Linux 3 on Intel				X	X	X
RedHat Enterprise Linux 3 on zSeries® 31 bit				X	X	X
RedHat Enterprise Linux 3 on zSeries 64 bit				X	X	X
RedHat Enterprise and Desktop Linux 4 Intel	X	X	X	X	X	X
RedHat Enterprise Linux 4 on AMD64/EM64T				**NEW**		
RedHat Enterprise Linux 4 on Itanium 64-bit				**NEW**		
RedHat Enterprise Linux 4 on iSeries™ and pSeries®[3]				X		
RedHat Enterprise Linux 4 on z/Series 31-bit	X	X		X	X	X
RedHat Enterprise 4 on zSeries 64 bit				X	X	X
RedHat Enterprise Linux 4 for Intel on VMWare ESX Server V2.5.2	**New**	**New**		**New**	**New**	**New**
SUSE Linux Enterprise Server 8 Intel				X	X	X
SUSE Linux Enterprise Server 8 for z/Series 31-bit				X	X	X
SUSE Linux Enterprise Server 8 for z/Series 64-bit				X	X	X
SUSE Linux Enterprise Server 9 Intel	X	X	X	X	X	X
SUSE Linux Enterprise Server 9 on AMD64/EM64T[4]				**NEW**		
SUSE Linux Enterprise Server 9 on Itanium 64-bit[5]				**NEW**		
SUSE Linux Enterprise Server 9 for iSeries and pSeries				X		
SUSE Linux Enterprise Server 9 for z/Series 31-bit	X	X		X	X	X
SUSE Linux Enterprise Server 9 for z/Series 64-bit				X	X	X

Table 4. Supported Linux operating systems (continued)

Operating system	Monitoring server	Portal server	Portal client[1]	OS monitoring agent[2]	Warehouse Proxy	Warehouse Summarization and Pruning agent

Notes:

1. The Tivoli Enterprise Portal desktop client is supported on marked platforms. However, the browser client can be accessed only from Windows computers running Internet Explorer 6.
2. The **Monitoring agent** column indicates the platforms on which an agent is supported. This column does not indicate that any agent runs on any operating system. For example, to monitor a Linux computer, you must use a Linux monitoring agent, not a Windows monitoring agent.
3. For RedHat Enterprise Linux 4 on System p, you must install the following libraries:
   libgcc-3.4.5-2.ppc64.rpm
   libstdc++-3.4.5-2.ppc64.rpm
   compat-libstdc++-33-3.2.3-47.3.ppc64.rpm
   compat-libstdc++-33-3.2.3-47.1.ppc.rpm

   These libraries are available on the RedHat Enterprise Linux operating system installation media.
4. For SUSE Linux Enterprise Server 9 on AMD64/EM64T, you must install the compat-libstdc++-lsb-4.0.2_20050901-0.4.x86_64.rpm library. This library is available in the SUSE Linux Enterprise Server 9 for AMD64 and Intel EM64T Service Pack 3.
5. You cannot use the remote deployment function for the OS agent on this operating system. This applies to both fresh installations and upgrades. Instead, you must install locally.

   If you try to use the remote deployment function, you'll receive the following error:

   ```
   KUICCN064E An appropriate installation image for the target platform, LINUX,
   could not be found on the local server.
   ```

Supported databases for Tivoli Enterprise Portal Server and Tivoli Data Warehouse

The following tables show the supported databases for the portal server and the Tivoli Data Warehouse.

Table 5 shows the supported databases for the portal server. Note that the database and the portal server must be installed on the same computer.

Table 5. Supported databases for the portal server

Portal server operating system	Portal server database ("TEPS"*)	
	IBM DB2	**MS SQL**
AIX	IBM DB2 UDB V8 with Fix Pack 10 or higher (32 and 64-bit)	
Linux	IBM DB2 UDB V8 with Fix Pack 10 or higher (32 and 64-bit)	
Windows	IBM DB2 UDB V8 with Fix Pack 10 or higher (32 and 64-bit)	MS SQL 2000 SP3
* "TEPS" is the default database name for the database used by the portal server.		

Table 6 on page 9 shows the supported databases for the Tivoli Data Warehouse.

Table 6. Supported databases for the Tivoli Data Warehouse

Tivoli Data Warehouse database ("WAREHOUS"[1])		
IBM DB2	**MS SQL**	**Oracle[2]**
IBM DB2 UDB V8, Fix Pack 10 and higher on the following operating systems: • AIX V5.3 • Solaris 10 • Windows 2003 Server • SUSE Linux Enterprise Server 9 for Intel • RedHat Enterprise Linux 4 for Intel	MS SQL 2000 MS SQL 2005	Oracle V9.2, 10g Release 1, and 10g Release 2 on the following operating systems: • AIX V5.3 • Solaris 10 • Windows 2003 Server • SUSE Linux Enterprise Server 9 for Intel • RedHat Enterprise Linux 4 for Intel

Notes:

1. "WAREHOUS" is the default database name for the database used by Tivoli Data Warehouse.
2. See the Oracle company support Web site (www.oracle.com) for information about installing and configuring Oracle on Solaris V10.

APARs addressed by this fix pack

The following APARs are addressed by this fix pack.

Documentation APARs

The following APAR is addressed in Fix Pack 003:

APAR Number	Symptom
IY89022	The Fix Pack 003 readme required update: • Two additional known limitations (the first two bulleted items in the list) were added. • The descriptions of the environment variable and configuration file to modify on Linux and UNIX monitoring servers in order to enable log in validation were not clear. • The incorrect JDBC driver for Oracle was used. Instead of "ojdbc14_g.jar," it should be the "ojdbc14.jar" JDBC driver.

INST component APARs

The following APARs are addressed in Fix Pack 003:

APAR Number	Symptom
IY80007	DB2 monitoring agent will not start when not installed as the DB2 instance owner.
IY80118	The Solaris OS agent fails due to missing GSKIT64 libraries.
IY80519	Situations are not firing when re-imported with tacmd and reassociated.
IY81101	GSKIT installed only on C drive one Windows systems. (New Installs only)
IY81412	Reconfiguring TEMS Windows service causes the service "Log On" account to revert to the Local System account, no matter what it was set to previously.
IY81610	When application support is added for an agent which requires a CLASSPATH update for the TEP desktop client, and there are more than one instance of the TEP desktop client, only one of those instances gets updated with the changed Java CLASSPATH.
IY81616	While using a proxy server, attempting to access a URL, the error "Server refushes to serve document" occurs.

APAR Number	Symptom
IY83425	The install.sh script sets permissions for all installed products to 777.
IY83538	The ″tacmd viewsit″ command output is empty for situations for the Universal Agent.
IY83577	Caching error: unable to store or update files in the cache.
IY83660	If Reconfigure of Portal Browser Client is selected from Manage Tivoli Services, the loaded JAR file box show all JAR files as unchecked, even though the products are installed. Also, the Edit box is disabled.
IY83824	For Windows TEMS to UNIX/Linux createnode deploys, checking the disk space of the target install directory when the directory's parent doesn't exist can give incorrect results. Forward slashes are changed to backslashes when the parent is checked, which causes the free space method to return the temp space available.
IY84168	The ″tacmd″ command fails if the user's password includes ″@″
IY84275	The ″tacmd login″ command fails when the -p option is specified.
IY84338	DB2 agent causes core dumps when running multiple instances because a single history file is being utilized.
IY84339	When the DB2 agent was started, and then crashed, the core file would be put in the DB2 user home dir. The large core files, especially if there is more than a few, can get large and disrupt operations.
IY84518	ITM 6.1 does not install the JRE 1.4.2 on a system with Java 1.5 (new installation only)
IY84540	Unix agent creates temporary file .KUXTMP.XXXXXX in the tmp directory.
IY84844	When installing 6.1.0-TIV-ITM_INST-FP0001 or 6.1.0-TIV-ITM_INST-FP0002, the install_kui.sh script returns: Err_report fail product ″ui″ not installed for this architecture install_kui.sh failure: product ″ui″ not installed for this architecture.
IY85163	Backup copies of .ver files causes itmpatch command to fail on Windows with a Dr Watson error.
IY85477	HTTP proxy server configuration not saved when MTEMS restarts.
IY85824	Eliminate proxy server options for browser client configuration.
IY86257	After applying ITM 6.1 FP1 patch install for a remote TEMS on AIX 5.2 64-bit, the remote TEMS terminates with a core dump.
IY87503	The user login process fails when installing as a non-root user and configuring the TEMS for user security.

The following APARs were addressed in previous fix packs and carried forward in Fix Pack 003:

APAR number	Symptom
IY80187	User Security Validation does not work because the Manage Tivoli Monitoring Services GUI is not changing the owner of the required file [kdsvlunx] to root.
IY80546	Prior to Fix Pack 2, the user must run the ″SetPerm -s″ command to enable User Validation Security but the documented process failed to include this step.
IY82516	Running tacmd updateAgent core dumps on Solaris TEMS.
IY82519	The addSystem and configureSystem CLIs don't allow encrypted password parameters.
IY82524	addSystem and configureSystem give false success messages when bad agent configuration data is entered.
IY83359	The ″tacmd addsystem″ command is failing with RC8 when deploying UA to a Windows Managed System.

APAR number	Symptom
IY84088	On Unix and Linux systems, ″itmpatch.exe″ creates the patchlogs directory with root only access.
IY84099	When a customer attempts to use the ″tacmd updateAgent″ command for a Universal Agent with multiple subnodes, the ″tacmd updateAgent″ command might terminate unexpectedly on all platforms.
IY84119	After installing Fix Pack 1 all situations are no longer associated.
IY84340	Installation of 6.1.0-TIV-ITM_INST-FP0001 may fail when the citnt.ver still exists on the system and install_kui.sh terminates with a memory fault (SIGSEGV).
IY84370	On Windows systems, ″itmpatch.exe″ program generates an Access Violation error message when attempting to run KinCInfo.exe -r.
IY84516	After installation of 6.1.0-TIV-ITM_INST-FP0001, the ″tacmd createNode″ command no longer works.

Tivoli Enterprise Monitoring Agent APARs

The following APARs are addressed in Fix Pack 003:

APAR number	Symptom
IY82134	We create a situation to monitor the ″file Info″ for Unix OS agent called test_file defined as: *IF *VALUE File_Information.File_U *NE 'ccc.txt' --> this is true for all files on the unix box. The is correctly evaluated at agent and data seems to be sent to TEMS but the situation never becomes TRUE. This does not work for any file path specified.
IY84059	On some UNIX/Linux platforms, execute permissions are lost when a UA script is copied from the agent depot directory to the UA scripts directory.
IY86480	During an agent registration with it's TEMS, if the TEMS is not available the agent is suspended using BSS1_Sleep. This can cause the agent to hang if the agent is shutdown while waiting for the BSS1_Sleep time to expire.
IY87818	KDCB0_HOSTNAME variable is not created in IBM Tivoli Monitoring V6.1 on z/OS by ICAT.
IY87841	With PTF: UA25220 the kwe messages sometimes get truncated.
IY87858	Remote TEMS loses connection to hub TEMS and fails to reconnect.
IY87902	Direct TEMA to bind to specific ip or interface.
IY87903	CMS registration gets wiped out if SPUFI is run.

The following APARs were fixed in previous fix packs and carried forward in Fix Pack 003:

APAR number	Symptom
IY81237	Warehouse Database tables have garbage in some columns, Data in historical files is corrupted and TEP historical reports show big negative numbers in the columns where they are not expected. The problem usually occurs on AIX5.2 and Solaris 5.9 64-bit machines that have in excess of 8 CPUs.
IY81988	The default Japanese UNIX/Linux code pages map the \ (0x5C) character to a Japanese character (0x7F), which causes problems in agent deploys from Windows TEMS to Japanese UNIX/Linux agent machines where the deploy agent code does not recognize the character as a \ and does not build the agent bundle depot correctly as a result.
IY82424	Take Action or Policy Commands directed at a z/OS(R) or OS/400(R) agent do not return their status data.

APAR number	Symptom
IY82431	Agents exhibit memory leak when processing historical reports.
IY82785	TEMS abends while processing history data record.

Tivoli Enterprise Monitoring Server APARs

The following APARs are addressed in Fix Pack 003:

APAR number	Symptom
IY80674	If an in-progress System Command is cancelled, the generation number of the request is zeroed to ensure the response is ignored. The request is then put back in the available pool for reuse. When a subsequent command is issued and this same request is reused, because the generation number is zero, the response to the command is discarded by the AsyncNotify process. Consequently, the requestor waits indefinitely for a response.
IY80809	TEMS shutdown hangs in KFAXCSRV.C when KFAXCMON.C receives an error executing KLE_XCFOPEN().
IY82460	Update to ″managed system list″ to add new target for situation distribution does not work.
IY82892	TEMS crashes when situation uses the SCAN function. Changes were made to both the portal and the monitoring server to correct the STR syntax to quote only the second argument, as follows. *STR 1,'my string' This is now interpreted correctly and accounts for the embedded space in the second argument, generating the correct value for the rule. If there are product-provided *STR functions that still contain the deprecated syntax and have a trailing space, the portal generates a syntax error 1203. The following is an example of such a function: `*STR '1 mystring '` Note the trailing space. To correct this problem, the TSITDESC.PDT *STR portion of the predicate should be modified using a Fix Pack 003 level portal to remove the first quote in the situation editor presentation of the string value. Save your changes - this will rebuild the PDT correctly. Product-provided situations should use quotes around only the second argument.
IY83327	On multiple interface hosts where users may need to manually specify this value to regain connectivity. The connectivity issue is caused by the selection of an unreachable server interface on the client side.
IY83945	Running spoofy and it was wiping out the cms registration. The kdstsns command is laid down in the cms directory it uses the kbhenv environment which sets the KDH_SERVICEPOINT, which in turn wipes out the cms registration.
IY85130	Startup processing when there are many custom manage lists incurred an enormous performance penalty due to inefficiencies in the nodelist expansion for user access lists. The TEMS would appear to be hung, but it was really just behaving poorly. The key to the issue was large number of custom manage lists.
IY86835	TEMS loops at startup.
IY87814	SYSPLEX product unable to collect data.

APAR number	Symptom
IY87850	TEMS shutdown hangs in kfaxcsrv.c when kfaxcmon.c receives and error executing kle_xcfopen().
IY87851	TEC events not forwarded w/ single quotes in managed system name.
IY87856	When a remote TEMS loses connectivity to the hub TEMS it is not always able to reconnect successfully.
IY87694	A SOAP request with a filter tag using HGBLSTMSTMP will crash the TEMS against ISITSTSH table.
IY87897	Direct TEMA to bind to specific ip or interface.

The following APARs were fixed in previous fix packs and carried forward in Fix Pack 003:

APAR number	Symptom
IY79123	A remote V350 or V360 TEMS connected to an ITM 6.1 TEMS HUB abends during startup. Various abends can result because the cause is a storage overlay in the remote TEMS. The storage overlay is a SOC 4 U0000.
IY79554	TEMS abends while processing history data record
IY79774	TEMS crashed when distributing a Situation with 21 scan functions.
IY79799	Trying to create UNIX OS situations using the ″File_Information″ attribute group, but every situation created shows a status of ″Problem″. These exact same situations worked in version 350, but do not work in ITM V6.1. There is no error message to say what the problem is and there is nothing in the logs to go on.
IY79985	Agent offline situation events not forwarded to TEC server (all platforms).
IY80322	Single quote in attribute data causes TEC server event parsing error
IY80433	The problem occurs when the user requests historical data collection of the TEMS TEIBLOGT table from a REMOTE TEMS.
IY81467	When the afilter tag is used against a z/OS(R) TEMS, the value remains in ASCII. The SELECT built by SOAP is not valid on z/OS with an ASCII value for non-UTF8 column.
IY81988	Installation of any additional agent (non Operating System) on Linux RedHat from TEPD fails if the locale is set to JA_jp.EUCJP.
IY82221	Need OTEA event mapping changes to match changes in BAROC files.
IY82471	Due to a problem in the msg slot formatting code, attributes name in the msg slot may be truncated. Also enum attribute values are not properly replaced with external values.
IY82475	When the TEC server is down, TEC event will be stored in the EIF cache file. When the cache file is full, the TEC EIF tec_put_event call will take upward of 2 minutes before it returns. This causes send requests to be backed up in the request queue causing memory growth.
IY82476	Situation events containing an attribute with the name ″state″ is not properly prefixed with the application prefix when being translated to a TEC event causing parse error on the TEC server.
IY82786	ITM610 TEP TakeAction command request directed to an ITM610 based Z/OS agent does not return a result status to the TEP UI.
IY82789	Agents can exhibit a gradual growth in memory utilization when reports for historical data are issued from the TEP.
IY82851	The Warehouse Proxy crashes when he attempting to insert a converted table name in the WAREHOUSEID column.

APAR number	Symptom
IY83311	Workspace views using filters eventually goes blank with no data after a continual automatic refresh.
IY83965	The TEMS goes in to a loop with high CPU and memory growth.

Tivoli Enterprise Portal APARs

The following APARs are addressed in Fix Pack 003:

APAR number	Symptom
IY79662	Export to .csv file function failing to output historical data.
IY80530	TEP user can see certain navigator items that are not in their ″allowed applications″ list.
IY81417	TEP crashes when using the tep situation editor to edit omegamon xe for cics on z/os product provided situations.
IY81694	Attribute substitution in universal message action doesn't work in correlated situations.
IY81870	Adding a TEC console view to a workspace, but cancelling the TEC info dialog; the TEC info prompt is still presented. Workaround: To resolve any pre-existing problems of the being prompted for TEC information when a TEC console icon was drug into a workspace and then cancelled, delete the workspace that prompts for TEC Information and create a new workspace identical to that workspace. Save the Navigation view.
IY81881	Cannot use pound sign in value of situation predicate.
IY82484	The Manage Tivoli Enterprise Monitoring Services utility needs to have the -dcnp.navigator.branch.pagesize=100 parameter added to it.
IY82582	Event workspace is too large with display set to 1024x780
IY82638	Situation take action editor places extra quotes around system command.
IY82773	Portal displays situation both with and without underscores.
IY83733	TEP desktop fails to start with the -d parameters for http proxy and port.
IY84608	Kfwitm220e error when attempting to view historical situation.
IY84691	**Remove managed system** option is missing from the physical navigator tree.
IY84812	Pasting text from excel introduced control characters into situation definitions that caused errors on export.
IY85060	TEP is showing negative values when looking at historical summarized performance. The negative values are shown for the attributes: Processor performance (avg over months):processor interrupts/sec, Memory performance (avg over months):page faults/sec
IY85540	Reconfiguring the historical collection of a universal agent application fails as the lower buttons are greyed out.
IY85582	Truncation is occurring in take action command when a : (colon) is used.
IY86084	Custom physical navigator doesn't order managed systems alphanumerically.

The following APARs were addressed in previous fix packs and carried forward in Fix Pack 003:

APAR number	Symptom
IY74835	2035-NOT_AUTHORIZED error when trying to open a dead letter queue.

APAR number	Symptom
IY76788	SYSPLEX managed systems not displayed in physical navigator tree.
IY79546	Situations stopped when started running for no more than a few minutes.
IY79860	KFWITM023W error during situation edit specifying an action.
IY82892	TEMS crashes when a situation is distributed if the SCAN function argument is not enclosed in quotes.

Tivoli Enterprise Portal Server APARs

The following APARs are addressed in Fix Pack 003:

APAR number	Symptom
IY82270	Acknowledgement ″notes″ not updated properly when highlighting and acknowledging multiple situation events.
IY84784	The migrate-export utility shuts down the portal server.
IY86056	DOS2UNIX failure to convert files in importagentteps.sh causes the application support not to complete correctly.
IY86849	Running migration-export.bat as described in ITM 6.1 Administrators Guide cannot work as it contains a wrong database name.
IY87991	Situations are shown as stopped in the portal after switching from a remote TEMS to another.
IY87072	The migrate-import.bat has to run under control of db2admin user ID.

The following APARs were addressed in previous fix packs and are carried forward in Fix Pack 003:

APAR number	Symptom
IY74835	2035-NOT_AUTHORIZED error when trying to open a dead letter queue.
IY76788	SYSPLEX managed systems not displayed in physical navigator tree.
IY79224	Situation severities are not correctly transferred to TEC.
IY79546	Situations stopped when started running for no more than a few minutes.
IY79860	KFWITM023W error during situation edit specifying an action.
IY81400	CTIRA_HOSTNAME value used to set up clustered agents to provide a unique windows system name in the TEP navigator is ignored.
IY84078	After completing the installation of the 6.1.0-TIV-ITM_TEPS-FP0001 patch, the TEP client renders a different set of workspaces at the Enterprise node level for DE licensed customers.

Tivoli Data Warehouse APARs

The following APARs are addressed in Fix Pack 003:

APAR number	Symptom
IY80894	Summarization and Pruning agent does not work correctly on when Warehouse database is on Oracle. The historical data are correctly loaded. However, summarization does not work and summarization tables are not created and filled for any resources for which the summarization was enabled. Also Pruning does not work.

APAR number	Symptom
IY82223	I found out that there is something in the remote control product (in this case DAMEWARE) that is affecting the operation of the Summarization and Pruning Agent (SPA). When one logs off the Windows account, then disconnects the remote control product, the SPA will be shut down.
IY82881	Summarization and Pruning agent does not properly handle the IBM Tivoli Monitoring 5.x tables.
IY87206	Summarization and Pruning agent fails with a SQL error: SQLCODE: -805 SQLSTATE: 51002

The following APARs were addressed in previous fix packs and are carried forward in Fix Pack 003:

APAR number	Symptom
IY79253	Warehouse migration tool issue: UNIXDISK table is not migrated. The warehouse proxy agent older than V350 was changing the Disk table name to UNIXDISK and User to UNIXUSER for the UNIX agent. It was also changing the column name User to User_Name for the table OS400_Job for the OS400 agent. This behavior disappeared at V350. For all the customers that created those tables with a Warehouse Proxy version previous to V350, the migration tool is now successfully migrating the UNIXDISK table to the Disk table, the UNIXUSER table to the User table, and the User_Name column to the User column.
IY80343	The Summarization and Pruning agent is failing to summarize the table SYSTEM Error, which results in the log showing the following error trying to alter the table: ALTER TABLE ″ITMUSER″.″SYSTEM″ ADD ″LOAD_AVERAGE_1_MIN″ NUMERIC (31,2) For an unknown reason the data type of the column LOAD_AVERAGE_1_MIN had been created with a datatype Decimal in the MSSQL warehouse database. This datatype was not recognized by the S&P agent. which is expecting a numeric datatype in that case. The S&P has been modified to recognize this datatype as well.
IY80350	The Warehouse Proxy crashes when it must insert a conversion for a table name in the WAREHOUSEID table.
IY80971	When using the warehouse migration tool, the tables are created in the Warehouse database without the index on the ORIGINNODE, TMZDIFF, WRITETIME.
IY83743	The SQL UPDATE statements used during summarization take a long time to complete when using MS SQL Server 2000 in the back end.
IY84092	Daylight Savings Time change causes the Summary and Pruning Agent to process all data.
IY84255	The aggregation agent fails during processing due to an unexpected column.
IY84290	MS SQL Server 2000 FP3 JDBC driver fails when there are a large number of tables with many columns configured for aggregation. The SQL Server will generate several exceptions including ″Out of Memory″ exception.

Tivoli Enterprise Console APARs and defects

The following APARs are addressed in Fix Pack 003:

APAR number	Symptom
IY81615	A pair of missing brackets in the omegamon.rls rule set file is causing 3 extra spaces to appear in the rules.trace file each time a rule is run. The brackets are missing from the check_sitforwarder_status timer rule, which by default runs every 10 minutes to check the status of the situation update forwarder, causing the file to grow to a large size.

APAR number	Symptom
IY84931	The installer checks every rule base for sentry.baroc and updates all rule bases that do not have sentry.baroc.

The following product defects are addressed in Fix Pack 003:

- The omsync_maxentries configuration parameter of the omegamon.rls rule set file is not being honored.
- AIX only: TEC_FP1:Errors appear on terminal during console install
- No backup of rule base
- Manual restart of TEC Server
- Loading Default rule base at end of uninstall

The following APAR was addressed in a previous fix pack and carried forward in Fix Pack 003:

- IY82191: In the rule set file omegamon.rls the administrator field is not being set when a situation received from IBM Tivoli Monitoring V6.l causes a Tivoli Enterprise Console event to be acknowledged or closed.

i5/OS OS monitoring agent APARs and defects

The following APARs are addressed in Fix Pack 003:

APAR number	Symptom
IY82162	ITM agent loops when TCP/IP subsystem is shutdown. When the customer wants to perform a backup of the system, they bring down the TCP/IP subsystem. When they do that, the ITM 6.1 agent starts looping and consumes lots and lots of CPU (90%). Additional Information: Immediate workaround is to stop the agent before stopping TCP/IP and start the agent after the TCP/IP servers are started.
IY82485	When a situation checks for specific message ID in QSYSOPR, MSG. Situations that use the OS400_Message query receive the same message events repeatedly.
IY82901	Job resource details not displayed if subsystem name is blank. Some jobs would not display job resource details data when selected from the job resource table. The job resource details view displayed but no fields contained values. This occurred if the job's priority was zero, indicating a system job not assigned to a subsystem. Response time of the "Job Resource Information" view in "Jobs and Queues" workspace is improved. Job list will display quicker than before. To take advantage of this fix on OS/400 V5R2 you must install OS/400 option 12, OS/400 - Host Servers. If option 12 is not installed then the existing code will be used for the OS400_Job attribute group. If option 12 is installed, or if you are using i5/OS V5R3 or V5R4 then the new code delivered with this fix will be used. Additional Information: A query was changed in fix pack 2 to allow system jobs to display information. That change partially fixed this APAR. This fix pack completes the fix for the job resource details display being too slow.
IY83540	The ITM 6.1 agent for I5/OS pure event situation OS_400_SPOOL always fires. Situations that use the OS400_Message query receive the same message pure event repeatedly.

The following APARs were addressed in previous fix packs and are carried forward in Fix Pack 003:

APAR number	Symptom
IY80507	Incorrect ODI change occurs for OS400_MESSAGE. Error message ″KFWITM051 The Display Item feature cannot be used with this situation because you can only use Attributes from groups that return multiple rows. OS400_message does not return multiple rows.″ was received when attempting to use the 'Advanced->Display Item' function with an OS400_Message query in a situation.
IY80641	Performance problem with real-time monitoring. There were performance issues while doing real-time monitoring with ITM 6.1 agent. The time to display several of the predefined workspaces was too long. For certain workspaces, like Disk and I/O, the agent waited a certain time interval between collecting the performance related data and this time period was not acceptable.
IY82092	Disk usage percentage of ITM 6.1 I5/OS agent can show as negative. The Percent Used field in the Disk Unit table of the Disk and I/O workspace could show incorrect values including negative percentages. The computation would fail if the disk capacity or disk space used number of bytes was greater than about 21,475,000 kilobytes.
IY82901	Job resource details not displayed if subsystem name is blank. Some jobs would not display job resource details data when selected from the job resource table. The job resource details view displayed but no fields contained values. This occurred if the job's priority was zero, indicating a system job not assigned to a subsystem.

The following product defects are addressed in Fix Pack 003:

- In the APPN Topology workspace the fly-over text doesn't match the table column header. There is no fly-over text for ″Time″, the fly-over text for ″Time″ appears in the next column header for ″Node Congestion″, and this continues through the rest of the window, each fly-over being the one for the header before.
- On the CFGOMA, Configure i5/OS Monitoring Agent, command a *NONE parameter can't be set for the port numbers.
- Added two attributes to the OS400_Job attribute group. The two new attributes are: Time Active - The amount of time (in seconds) that the job has been active, or zero if the job is not currently active. Time in System - The amount of time (in seconds) that the job has been in the system.

The following product defect was addressed in a previous fix pack and carried forward in Fix Pack 003:

- Various exceptions occur using workspaces and situations including: MCH3601 exceptions with performance collections; agent fails on system with more than 10,000 jobs; agent fails when ending APPN related situation. Storage pool reports were inaccurate and slow

Linux OS monitoring agent APARs

The following APAR is addressed in Fix Pack 003:

APAR number	Symptom
IY82465	The Linux OS Agent does not report CPU values correctly on long running systems.

Universal Agent APARs

The following APARs are addressed in Fix Pack 003:

APAR number	Symptom
IY79012	On UNIX platforms, directly running KUMPCON causes KUMPV599E error

APAR number	Symptom
IY82812	UA metafile parser should not allow leading digit in APPL name
IY84293	Script DP not treating multiple arguments separately on UNIX platforms
IY84694	um_cleanup script does not remove UA work files from Linux-based TEPS
IY85346	TTL defaults to 0 for API and Socket Event tables, results in loss of data
IY85413	ManagedSystemName SOURCE parameter not supported in ODBC metafiles
IY85565	UA restart fails on UNIX/Linux platforms with an error message indicating that DCH port 1919 is already in use. This problem occurs if the Script Data Provider launched a script during the previous UA startup, and that script hasn't exited.
IY85529	If a script outputs greater than 4096 bytes in one script execution, the output data line at the 4K boundary is incorrectly broken into two separate rows.
IY86181	UA restart fails if script launched from Script DP is still running
IY86404	Redirected Socket DP table goes offline before its expiration time
IY86814	Socket DP record prefixing fails if using ManagedSystemName and UA instance

The following APARs were addressed in previous fix packs and are carried forward in Fix Pack 003:

APAR number	Symptom
IY78337	Unreliable data delivery when Socket DP metafile uses invisible table
IY81503	File DP COPY mode fails if first file record is blank
IY81922	Dynamic filename switches not occurring
IY82435	UA crashes if derived attribute function has null input
IY82436	Script stops outputting data on UNIX if interrupt signal received
IY82438	Active stderr pipe on UNIX blocks stdout data in same script execution
IY82767	ENVFILE values not being set for script process on UNIX platforms
IY83756	Fix Socket DP handling of fully qualified hostnames
IY83757	Hung Script DP processes on AIX not always being terminated
IY85529	Large Script DP output > 4K not handled correctly
IY85697	File DP data sometimes displays in TEP under wrong managed system name

UNIX Log Agent APARs

The following APARs are addressed in Fix Pack 003:

APAR number	Symptom
IY83266	The agent's BAROC file used a reserved keyword ("class") as a slot name.
IY83975	The resource field of AIX errlogs is not mapped into the data collected by the UNIX Log Agent.

The following APARs were addressed in previous fix packs and carried forward in Fix Pack 003:

APAR number	Symptom
IY80825	The UNIX Log Agent does not display error log entries on 64-bit AIX systems.

APAR number	Symptom
IY81251	The UNIX Log Agent does not display log entries from utmp-style logs on 64-bit HP-UX systems.
IY81759	The Source and Description attributes for syslog entries are the same.

UNIX OS monitoring agent APARs

The following APARs are addressed in Fix Pack 003:

APAR number	Symptom
IY83133	Incorrect percentages in TEDW for Unix agent.
IY83614 IY86219	No data for virtual memory stats on Solaris 8 when LANG=JA.
IY83868	Unable to export data from ″System Detail″ workspace view.
IY84123	Summarization and Pruning Agent improperly pruning UNIX OS, UNIX CPU, UNIX PROCESS and UNIX NFS tables
IY84933	UNIX OS agent does not support disk volumes over 2,147,483,647 and UNIX OS agent displaying negative numbers and values greater than 2,147,483,647 display negative numbers in portal fixed in UNIX OS and UNIX CPU tables
IY85020	UNIX OS agents fail to report 1 MIN and 15 MIN load averages for 64-bit AIX
IY85880	Seed file KUX_KCJ.SQL has all the -102 properties set to the default framework type. Thus, all UNIX workspace links failed when an OM350 agent is connected to an ITM 6.1 TEPS.

The following APARs were addressed in previous fix packs and carried forward in Fix Pack 003:

APAR number	Symptom
IY80163	On AIX 5.1 and 5.2 machines both On-line and Off-line Cpu’s are displayed. Display only On-Line Cpu’s similar to AIX 5.3.
IY80584	UNIX agent ″LOGIN_TIME″ column is null when no users logged-on, which in turn causes Summarization and Pruning Agent to fail.
IY80820	ITM 6.1 UNIX OS agent on HP-UX 11.11 cannot handle more than 20 PPAs. Systems with more than 20 PPAs (network interfaces) crash because the agent overwrites the bounds of the PPA array.
IY81880	ITM 6.1 UNIX OS agent on Solaris 8 64 bit crashes.
IY83133	Improper percentages in data warehouse for UNIX system VIRTUAL% on 32-bit.

Chapter 2. Installation instructions

The following table outlines the steps required to install the fix pack in your environment.

Table 7. Overall installation steps for Fix Pack 003

Goal	Where to find information
Ensure your monitoring environment is prepared for fix pack installation.	"Before you install the fix pack"
Gather the information you need to perform the installations.	"Fix pack installation planning worksheets" on page 25
Update your monitoring server.	"Monitoring server checklist" on page 29
Update your portal server.	"Portal server checklist" on page 33
Update your portal desktop clients.	"Portal desktop client checklist" on page 35
Update your remote monitoring servers.	"Monitoring server checklist" on page 29
Update your local monitoring agents.	"Monitoring agent checklist - local installation" on page 37
Remotely update other monitoring agents.	"Monitoring agent checklist - remote installation" on page 38
Update your local i5/OS OS agents, if applicable.	"Installing the fix pack for the i5/OS monitoring agent" on page 40
Update your event synchronization on your IBM Tivoli Enterprise Console event server, if appropriate.	"Installing the IBM Tivoli Enterprise Console event synchronization fix pack" on page 42

Before you install the fix pack

Do the following before you install this fix pack:

- *Note that you must upgrade all base monitoring components (monitoring server, portal server, and portal desktop client) to the same fix pack level.* For example, you cannot have a Fix Pack 001 portal server and a Fix Pack 003 monitoring server. Monitoring agents do not need to be at the latest fix pack level - you can continue to use older monitoring agents in your upgraded environment, although you might consider upgrading as soon as possible to take advantage of new functions and fixes available with the newer agents.
- Any prerequisite fix packs or other software must be installed for all component fix packs you are going to install.
- Note regarding re-adding application support for agents: During the installation of this fix pack, or during future agent upgrades, you might be presented with a list of agents for which to add application support to the monitoring server. Use caution when you select those agents for which to add support, as any customizations you've made to situations can be lost during this process. During the installation of this fix pack, add application support for *only* the OS agents and the UNIX Log agent. This prevents the loss of customizations to other agents. During future agent upgrades and new agent installations for this monitoring server, add application support for only those agents that you are upgrading or adding.

- Before installing any fix packs on UNIX or Linux computers, set the environment variable CANDLEHOME to the IBM Tivoli Monitoring installation directory by running the following command:

  ```
  export CANDLEHOME=ITMinstall_dir
  ```

  where *ITMinstall_dir* is the location where IBM Tivoli Monitoring is installed.
- Before installing any fix packs, stop the collection of all historical data. You can restart historical data collection after you have finished installing fix packs. For information on historical data collection, see the *IBM Tivoli Monitoring Administrator's Guide*.
- If you are installing fix packs on Linux or UNIX computers, and you installed the IBM Tivoli Monitoring components (both the base monitoring components like the monitoring server and any monitoring agents) as a non-root user, you must perform the following steps to ensure that the user who installs the fix packs has the appropriate permissions:

  Note: *ITMinstall_dir* is the installation location for IBM Tivoli Monitoring and *user_id* is the ID that was used to install the IBM Tivoli Monitoring components.

  1. Log into the computer as *user_id*.
  2. Run the following command to change ownership of any root owned files to *user_id*:

     ```
     su - root -c "ITMinstall_dir/bin/UnSetRoot user_id"
     ```
  3. Install the fix pack component fix packs on the computer, following the steps outlined in the checklists.
  4. Run the following command to reset the file permissions and file ownership as required:

     ```
     su - root -c "ITMinstall_dir/bin/SetPerm -a"
     ```
- Before you install the Tivoli Enterprise Portal Server component fix pack on a Windows computer, ensure that the Windows Script Host (WSH) is at least version 5.6. You can check the version by running the **cscript** command without any parameters.
- The fix pack for the Warehouse Proxy requires that you first install the 6.1.0-TIV-ITM_TEMA-FP0003 component fix pack. See "Installing fix packs using the itmpatch command" on page 117 for more information.
- To use the GUI version of the application support installer on a Linux or UNIX monitoring server, portal server, or portal client, you must install an X Window System. If you do not have an X Window System, you can run a silent installation of the application support files. See "Using a response file to install the application support files" on page 119 for detailed information.
- *You cannot use the full image or CD refresh of IBM Tivoli Monitoring to apply a fix pack.* Install the full image or CD refresh of IBM Tivoli Monitoring V6.1 only on computers where IBM Tivoli Monitoring V6.1 is not currently installed or for products for which new operating system support has been added as part of a fix pack (such as the Tivoli Enterprise Portal Server on AIX). Use the individual component fix packs to apply a fix pack to existing IBM Tivoli Monitoring V6.1 installations. These fix packs are available from the IBM Software Support Web site.
- For the Warehouse Summarization and Pruning agent, if you are using Microsoft SQL server, install the MS SQL 2005 JDBC driver. The Warehouse Summarization and Pruning agent might fail to run at the scheduled time on Windows computers because of a limitation of the number of tables it can retrieve. The MS

SQL 2005 JDBC driver addresses this limitation. You can download the JDBC driver from the Microsoft Web site, http://msdn.microsoft.com/data/jdbc/default.aspx.

- If you are running IBM Tivoli Monitoring in a globalized environment, for best results, after you apply a fix pack and reconfigure any components, re-install the base IBM Tivoli Monitoring language packs and any agent language packs.

  Note: This requirement also applies if you reconfigure any of the base components, such as the portal server.

- If you are installing Fix Pack 003 in an IBM Tivoli Monitoring environment that is running with a Japanese language pack and you do not want to reinstall the Japanese language pack (as described above) or you have reconfigured the portal server (for example, after adding agent application support files), you must perform the following steps prior to installing the fix pack or after reconfiguring:
  - For a portal server on Windows or Linux, do the following. If you do not, the browser client and all associated messages are displayed in English, instead of Japanese.
    1. Stop the portal server.
    2. Make a copy of the applet.html file (in the *<itm_install>*/*<platform>*/cw directory on Linux or the *<itm_install>*/CNB directory on Windows.
    3. Install the portal server fix pack.
    4. Edit both the pre-upgrade and post-upgrade versions of the applet.html file.
    5. In the pre-upgrade version, locate the lines regarding the *xxx*_ja.jar files. For example:

       ```
       -----
       document.writeln( '<!-- JARLIST: kjrall.jar, cnp.jar, ae.jar -->' );
       document.writeln( '<PARAM NAME = CACHE_ARCHIVE VALUE="cnp_vbjorball.jar,
       kjrall.jar,   util.jar, cnp.jar, chart.jar, ae.jar, cnp_jviewsall.jar,
       terminal.jar, browser.jar, icu4jm32.jar, deploy.jar, lp_ja.jar, kit_ja.jar,">' );
       document.writeln( '<PARAM NAME = CACHE_VERSION VALUE="6.5.0.7, 7.610.6173.a,
       2.2.8.9,  7.610.6173.a, 2.2.2.6, 7.610.6173.a, 5.2.5.B, 3.0.4.4, 6.0.1.5, 1.0.0.0,
       7.4.A.C, 0.0.1.2, 0.0.1.2,">' );
       -----
       ```

    6. Add these .jar file names to the post-upgrade version of the applet.html file.
    7. Add any version numbers associated with the .jar files.
    8. Save and close the applet.html files.
    9. Restart the portal server.
  - For a portal desktop client running on Linux, do the following:
    1. Search for any *_ja.jar files in the *ITM_installDir*/*platform*/cj/lib directory. Make a list of these files.
    2. Edit the *ITM_installDir*/*platform*/cj/original/cnp.sh_template file.
    3. Locate the CLASSPATH entry in this file and add any *_ja.jar files identified in Step1.

       For example:

       ```
       CLASSPATH=|CANDLEHOME|/JRE/|BINARCH|:.......:${KCJ_LIB}/lp_ja.jar:${KCJ_LIB}/kit_ja.jar
       ```

    4. Reconfigure the portal desktop client by running the following command:

       ```
       ./itmcmd config -A cj
       ```

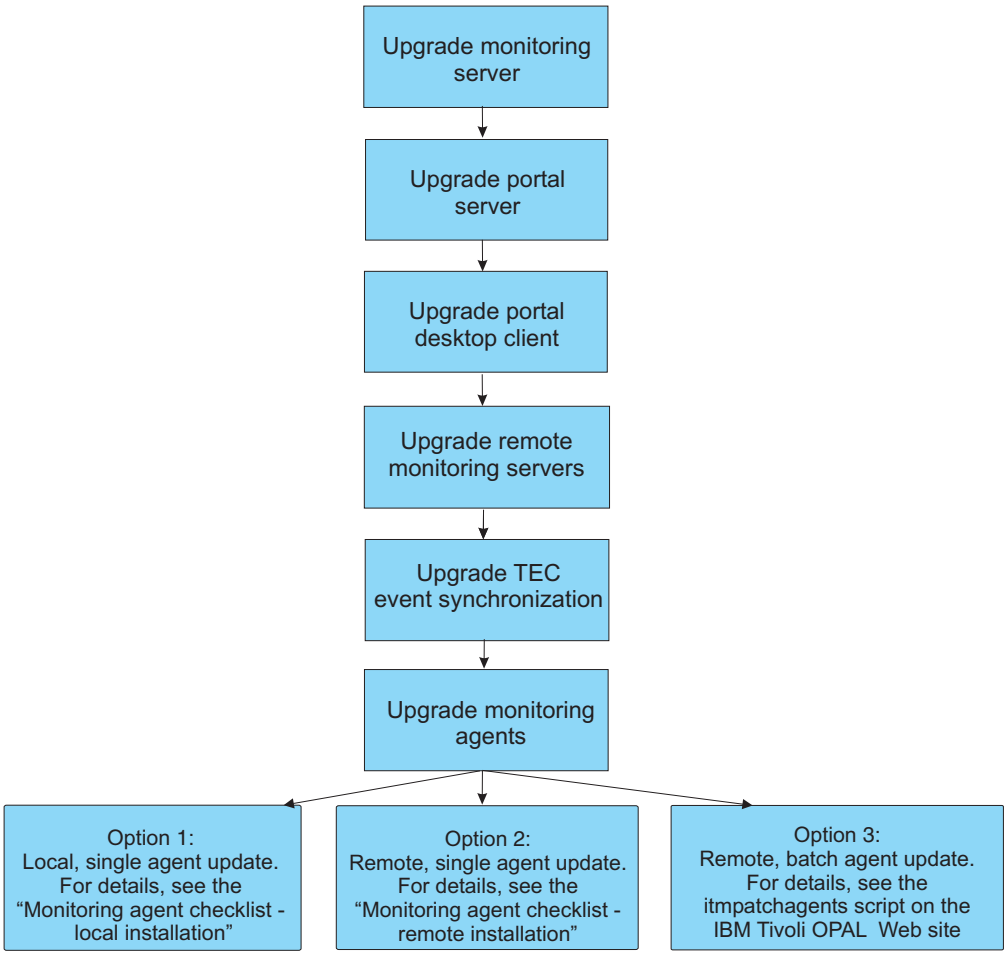
Installation checklists

The following checklists provide the installation steps for the IBM Tivoli Monitoring components.

Notes:

1. If your Warehouse Proxy agent or Summarization and Pruning agent are on machines other than the monitoring server or portal server, use the instructions in the "Monitoring agent checklist - local installation" on page 37 to install the updates.
2. These checklists provide the order and procedures for installing the required fix pack components. However, if you want more detail about using any of the commands or tools outlined in the checklists, see Appendix A, "Detailed installation procedures for installing the component fix packs," on page 117.

Install your environment in the following order:



You can use the "Fix pack installation planning worksheets" to gather the information required for the installation.

Note: If you have a large number of monitoring agents to which to deploy updates, consider using the itmpatchagents script, available as a sample from the IBM Tivoli Open Process Automation Library (http://www-18.lotus.com/wps/portal/topal). This script enables the automatic deployment of updates across your monitoring environment.

Fix pack installation planning worksheets

Use the following worksheet to gather information about your monitoring environment.

Also, consider printing a list of all the computers in your environment - you can check off each computer as you update it, ensuring that you do not miss any.

Table 8. Fix pack planning worksheet

IBM Tivoli Monitoring installation directory (CANDLEHOME environment variable): **Note:** This directory is referred to as *ITMinstall_dir* in this document				
Patch installation directory (where you extract the fix pack files): **Note:** This directory is referred to as *patch_dir* in this document				
What is needed	**Other components also installed on this computer (circle those that apply)**	**How to gather this information**	**When this information is used**	
Hub monitoring server host name	Portal server Portal desktop client Warehouse Proxy Summarization and Pruning agent	Manage Tivoli Enterprise Monitoring Server	"Monitoring server checklist" on page 29	
Remote monitoring server host name	Portal server Portal desktop client Warehouse Proxy Summarization and Pruning agent	Manage Tivoli Enterprise Monitoring Server	"Monitoring server checklist" on page 29	
Remote monitoring server host name	Portal server Portal desktop client Warehouse Proxy Summarization and Pruning agent	Manage Tivoli Enterprise Monitoring Server	"Monitoring server checklist" on page 29	
Remote monitoring server host name	Portal server Portal desktop client Warehouse Proxy Summarization and Pruning agent	Manage Tivoli Enterprise Monitoring Server	"Monitoring server checklist" on page 29	
Remote monitoring server host name	Portal server Portal desktop client Warehouse Proxy Summarization and Pruning agent	Manage Tivoli Enterprise Monitoring Server	"Monitoring server checklist" on page 29	
Remote monitoring server host name	Portal server Portal desktop client Warehouse Proxy Summarization and Pruning agent	Manage Tivoli Enterprise Monitoring Server	"Monitoring server checklist" on page 29	
Portal server host name	Monitoring server Portal desktop client Warehouse Proxy Summarization and Pruning agent	Manage Tivoli Enterprise Monitoring Server	"Portal server checklist" on page 33	

Table 8. Fix pack planning worksheet (continued)

IBM Tivoli Monitoring installation directory (CANDLEHOME environment variable): **Note:** This directory is referred to as *ITMinstall_dir* in this document				
Patch installation directory (where you extract the fix pack files): **Note:** This directory is referred to as *patch_dir* in this document				
What is needed	**Other components also installed on this computer (circle those that apply)**	**How to gather this information**	**When this information is used**	
Portal desktop client locations	Monitoring server Portal server Warehouse Proxy Summarization and Pruning agent	Manage Tivoli Enterprise Monitoring Server	"Portal desktop client checklist" on page 35	
Warehouse Proxy agent location	Monitoring server Portal server Portal desktop client Summarization and Pruning agent	Manage Tivoli Enterprise Monitoring Server	"Monitoring server checklist" on page 29 "Portal server checklist" on page 33	
Warehouse Summarization and Pruning agent location	Monitoring server Portal server Portal desktop client Warehouse Proxy	Manage Tivoli Enterprise Monitoring Server	"Monitoring server checklist" on page 29 "Portal server checklist" on page 33	
Agent types to update (product codes)		**tacmd listSystems**	"Monitoring server checklist" on page 29 "Monitoring agent checklist - local installation" on page 37	

Use the following table to identify the number of each type of agent to be updated.

Table 9. Agent updates table

Agent type	**Number to update**
UX (UNIX OS)	
LZ (Linux OS)	
UL (UNIX Log)	
A4 (i5/OS)	
UM (Universal Agent)	

Monitoring server checklist

The following checklist provides the fix pack installation steps for the hub and remote monitoring servers.

Note: The process for updating the hub and remote monitoring servers is the same, although you must update the hub monitoring server first, as shown in the fix pack installation flow chart.

Table 10. Checklist for installing the fix pack on the monitoring server

✔	Installation step
	1. Gather information about the monitoring components in your environment. See "Fix pack installation planning worksheets" on page 25.
	2. Download and extract the fix pack files to a temporary location on your computer. **Patch directory:**
	3. Before installing any fix packs, stop the monitoring server (and portal server, if present) through the Manage Tivoli Enterprise Monitoring Services utility (CandleManage on Linux and UNIX). Also stop the Manage Tivoli Enterprise Monitoring Services utility. You can also run the following command to stop Linux or UNIX monitoring servers: `itmcmd server stop server_name` where *server_name* is the name of the monitoring server.

	4. Install the 6.1.0-TIV-ITM_INST-FP0003 fix pack.
	On Windows computers, run the following command from the command line:
	`cd patch_dir`
	`install_kui.bat`
	On UNIX or Linux computers, run the following command from the command line:
	`cd patch_dir`
	`./install_kui.sh`
	where *patch_dir* is the directory where you extracted the fix pack files.

	5. Run the **itmpatch** command to install the 6.1.0-TIV-ITM_TEMA-FP0003 fix pack.
	For Windows computers:
	`ITMinstall_dir\bin\itmpatch.exe -h ITMinstall_dir -i patch_dir\6.1.0-TIV-ITM_TEMA-FP0003`
	where *ITMinstall_dir* is the IBM Tivoli Monitoring installation directory.
	For Linux and UNIX computers:
	`ITMinstall_dir/bin/itmpatch -h ITMinstall_dir -i patch_dir/6.1.0-TIV-ITM_TEMA-FP0003`

	6. Run the **itmpatch** command to install the 6.1.0-TIV-ITM_TEMS-FP0003 fix pack.
	For Windows computers:
	`ITMinstall_dir\bin\itmpatch.exe -h ITMinstall_dir -i patch_dir\6.1.0-TIV-ITM_TEMS-FP0003`
	where *ITMinstall_dir* is the IBM Tivoli Monitoring installation directory.
	For Linux and UNIX computers:
	`ITMinstall_dirbin/itmpatch -h ITMinstall_dir -i patch_dir/6.1.0-TIV-ITM_TEMS-FP0003`

Table 10. Checklist for installing the fix pack on the monitoring server (continued)

✓	Installation step
	7. Start the monitoring server through the Manage Tivoli Enterprise Monitoring Services utility. On Linux and UNIX computers, you can run the following command to start the monitoring server: `itmcmd server start` *`server_name`* where *server_name* is the name of the monitoring server.
	8. Optionally install the following IBM Tivoli Monitoring component fix packs for components on the same computer as your monitoring server: • Warehouse Proxy agent - 6.1.0-TIV-ITM_TDW-FP0003 • Warehouse Summarization and Pruning agent - 6.1.0-TIV-ITM_TDW-FP0003 Use the **itmpatch** command. See "Monitoring agent checklist - local installation" on page 37 for more information. Restart these agents after you update them.

Table 10. Checklist for installing the fix pack on the monitoring server (continued)

✓	Installation step

	9. Run the application support installer to add the application support files for the IBM Tivoli Monitoring OS agents (Linux, UNIX, and i5/OS, as well as the UNIX Log agent) to the monitoring server. Application support files are located in a subdirectory of the agent fix pack package.
	Download and extract the agent fix pack file (the 6.1.0-TIV-ITM_*platform*-FP003.tar file, where *platform* identifies the specific operating system, such as "UNIX") for each OS agent in your environment and follow these steps to run the application support installer.
	Note: This GUI requires an X Window System on UNIX and Linux computers. If you do not have an X Window System, you can run a silent installation of the application support files. See "Using a response file to install the application support files" on page 119 for information.
	a. Extract the compressed files that contain the application support files for each fix pack. Look for a file named "*pc*__tems_teps_tepd_fp0003.tar," where *pc* is "k" plus the 2-letter product code for the agent. For example, the file for the UNIX OS agent is kux_tems_teps_tepd_fp0003.tar.
	Note: Extract the application support files for each OS agent to a unique directory; otherwise, files from the different agents will over-write each other.
	b. From the directory where you extracted the application support files, launch the application support installer by running the following command:
	`java -jar directory\CD-ROM\setup.jar`
	where *directory* is the directory where you extracted the support files.
	Note: If you do not have the Java™ JRE in your path statement, change to the CD-ROM subdirectory and invoke the JRE executable file directly by specifying the path to it on the command line.
	For example, to run the application support installer for the UNIX OS agent, run the following commands:
	`cd c:\FP2_IMAGES\6.1.0-TIV-ITM_UNIX-FP0003\CD-ROM`
	`c:\program files\ibm\java142\jre\bin\java -jar setup.jar`
	See "Installing application support" on page 117 for more information.
	c. Follow the prompts in the application support installation wizard.
	d. Repeat this for each OS agent in your environment.
	See "Installing application support" on page 117 for more information about installing this support, including information about identifying the Java installation directory and the detailed steps for the application support installation wizard.
	Note: Before you install the application support on any remote monitoring servers, ensure that the hub monitoring server is running.
	Attention: The agent component fix pack might include modifications to product-provided situations. These changes are not merged automatically. While the changes are included, the updates fail and error messages are displayed when you install the application support. The changes made to each agent's situations are listed in the agent component readme. You can edit your situations, using the change descriptions provided in the agent component readmes, to merge the changes. For more information on editing a situation, see the "Customizing a situation" section of Chapter 10, "Situations for event-based monitoring" in the *IBM Tivoli Monitoring User's Guide*.

Table 10. Checklist for installing the fix pack on the monitoring server (continued)

✓	Installation step
	10. If you are planning on remote deploying the agent fix packs (or the common component fix pack), run the **tacmd addBundles** command to add the fix packs to the agent depot (an installation directory from which you deploy agents and maintenance packages) on the monitoring server. `ITMinstall_dir/bin/tacmd addBundles -i patch_name -n` where *patch_name* is the name of the fix pack to add to the agent depot, such as `6.1.0-TIV-ITM_UNIX-FP0003`. Repeat this step for each agent fix pack. Ensure that you include all of the prerequisite fix packs. For example, the OS agent fix packs require the TEMA fix pack, so it needs to be in the depot before you can deploy the OS agent fix packs. You can remote deploy the following fix packs: • 6.1.0-TIV-ITM_INST-FP0003 -- IBM Tivoli Monitoring Global-common Component (UI) • 6.1.0-TIV-ITM_TEMA-FP0003 -- ITM Shared Libraries (AX [UNIX] or GL [Windows]) • 6.1.0-TIV-ITM_UA-FP0003 -- Universal Agent (UM) • 6.1.0-TIV-ITM_LINUX-FP003 – Linux OS monitoring agent (LZ) • 6.1.0-TIV-ITM_UNIX-FP0003 -- UNIX OS monitoring agent (UX) • 6.1.0-TIV-ITM_UXLOG-FP0003 – UNIX Log agent (UL) See "Adding fix packs to the agent depot" on page 120 for more information.
	11. Install the remaining component fix packs: portal server, portal desktop client, and monitoring agents (local and remote).

Portal server checklist

The following checklist provides the fix pack installation steps for the portal server.

Table 11. Checklist for installing the fix pack on the portal server

✓	Installation step
	1. Gather information about the monitoring components in your environment. See "Fix pack installation planning worksheets" on page 25.
	2. Download and extract the fix pack files to a temporary location on your computer. **Patch directory:**
	3. Before installing any fix packs, stop the portal server (and monitoring server, if present) through the Manage Tivoli Enterprise Monitoring Services utility (CandleManage on Linux). Also stop the Manage Tivoli Enterprise Monitoring Services utility. On Linux computers, you can run the following command to stop the portal server: `./itmcmd agent stop cq`

	4. Install the 6.1.0-TIV-ITM_INST-FP0003 fix pack.
	On Windows computers, run the following command from the command line:
	`cd patch_dir`
	`install_kui.bat`
	On Linux computers, run the following command from the command line:
	`cd patch_dir`
	`./install_kui.sh`
	where *patch_dir* is the directory where you extracted the fix pack files.

	5. Use the **itmpatch** command to install the 6.1.0-TIV-ITM_TEPS-FP0003 fix pack.
	For Windows computers:
	`itmpatch.exe -h ITMinstall_dir -i patch_dir\6.1.0-TIV-ITM_TEPS-FP0003`
	where *ITMinstall_dir* is the IBM Tivoli Monitoring installation directory.
	For Linux computers:
	`ITMinstall_dir/bin/itmpatch -h ITMinstall_dir -i patch_dir/6.1.0-TIV-ITM_TEPS-FP0003`

	6. On Windows computers, reconfigure the portal browser client from the Manage Tivoli Enterprise Monitoring Services utility: a. In Manage Tivoli Enterprise Monitoring Services, right-click the Tivoli Enterprise Portal - Browser client and click **Reconfigure**. b. In the Configure Tivoli Enterprise Browser window, click **OK** without making any changes.
	7. Start the portal server through the Manage Tivoli Enterprise Monitoring Services utility. On Linux computers, you can run the following command to start the portal server: `./itmcmd agent start cq`

Table 11. Checklist for installing the fix pack on the portal server (continued)

✓	Installation step
	8. Optionally install the following IBM Tivoli Monitoring component fix packs for components on the same computer as your monitoring server: • IBM Tivoli Monitoring Share Libraries for the monitoring agent - 6.1.0-TIV-ITM_TEMA-FP0003 (a prerequisite for the Warehouse Proxy agent fix pack) • Warehouse Proxy agent - 6.1.0-TIV-ITM_TDW-FP0003 • Warehouse Summarization and Pruning agent - 6.1.0-TIV-ITM_TDW-FP0003 Use the **itmpatch** command. See "Monitoring agent checklist - local installation" on page 37 for more information. Restart these agents after you update them.

	9. Run the application support installer to add the application support files for the IBM Tivoli Monitoring OS agents (Linux, UNIX, and i5/OS, as well as the UNIX Log agent) to the portal server. Application support files are located in a subdirectory of the agent fix pack package.
	Download and extract the agent fix pack file (the 6.1.0-TIV-ITM_*platform*-FP003.tar file, where *platform* identifies the specific operating system, such as "UNIX") for each OS agent in your environment and follow these steps to run the application support installer.
	Note: This GUI requires an X Window System on UNIX and Linux computers. If you do not have an X Window System, you can run a silent installation of the application support files. See "Using a response file to install the application support files" on page 119 for information.
	a. Extract the compressed files that contain the application support files for each fix pack. Look for a file named "*pc*__tems_teps_tepd_fp0003.tar," where *pc* is "k" plus the 2-letter product code for the agent. For example, the file for the UNIX OS agent is kux_tems_teps_tepd_fp0003.tar.
	Note: Extract the application support files for each OS agent to a unique directory; otherwise, files from the different agents will over-write each other.
	b. From the directory where you extracted the application support files, launch the application support installer by running the following command:
	`java -jar directory\CD-ROM\setup.jar`
	where *directory* is the directory where you extracted the support files.
	Note: If you do not have the Java JRE in your path statement, change to the CD-ROM subdirectory and invoke the JRE executable file directly by specifying the path to it on the command line.
	For example, to run the application support installer for the UNIX OS agent, run the following commands:
	`cd c:\FP2_IMAGES\6.1.0-TIV-ITM_UNIX-FP0003\CD-ROM`
	`c:\program files\ibm\java142\jre\bin\java -jar setup.jar`
	See "Installing application support" on page 117 for more information.
	c. Follow the prompts in the application support installation wizard.
	d. Repeat this for each OS agent in your environment.
	See "Installing application support" on page 117 for more information about installing this support, including information about identifying the Java installation directory and the detailed steps for the application support installation wizard.

	10. If you are running IBM Tivoli Monitoring in a globalized environment, re-install the base IBM Tivoli Monitoring language pack and then install the Fix Pack 003 Language Pack Fix Pack (6.1.0-ITM-LP-FP0003.zip or 6.1.0-ITM-LP-FP0003.tar). For information about installing the language packs, see the "Installing the language packs" section of Chapter 5, "Installing IBM Tivoli Monitoring" in the *IBM Tivoli Monitoring Installation and Setup Guide*.
	11. Install the remaining component fix packs: portal desktop client and monitoring agents (local and remote).

Portal desktop client checklist

The following checklist provides the fix pack installation steps for the portal desktop client. Repeat this checklist for each desktop client in your environment.

Table 12. Checklist for installing the fix pack on the portal desktop client

✓	Installation step
	1. Gather information about the monitoring components in your environment. See "Fix pack installation planning worksheets" on page 25.
	2. Download and extract the fix pack files to a temporary location on your computer. **Patch directory:**
	3. Before installing any fix packs, stop the Manage Tivoli Enterprise Monitoring Services utility (CandleManage on Linux) if it is running.

	4. Install the 6.1.0-TIV-ITM_INST-FP0003 fix pack.
	On Windows computers, run the following command from the command line:
	`cd patch_dir`
	`install_kui.bat`
	On Linux computers, run the following command from the command line:
	`cd patch_dir`
	`./install_kui.sh`
	
	where *patch_dir* is the directory where you extracted the fix pack files.

	5. Use the **itmpatch** command to install the 6.1.0-TIV-ITM_TEP-FP0003 fix pack.
	For Windows computers:
	`itmpatch.exe -h ITMinstall_dir -i patch_dir\6.1.0-TIV-ITM_TEP-FP0003`
	
	where *ITMinstall_dir* is the IBM Tivoli Monitoring installation directory.
	For Linux computers:
	`ITMinstall_dir/bin/itmpatch -h ITMinstall_dir -i patch_dir/6.1.0-TIV-ITM_TEP-FP0003`

Table 12. Checklist for installing the fix pack on the portal desktop client (continued)

✓	Installation step

	6. Run the application support installer to add the application support files for the IBM Tivoli Monitoring OS agents (Linux, UNIX, and i5/OS, as well as the UNIX Log agent) to the portal desktop client. Application support files are located in a subdirectory of the agent fix pack package.
	Download and extract the agent fix pack file (the 6.1.0-TIV-ITM_*platform*-FP003.tar file, where *platform* identifies the specific operating system, such as "UNIX") for each OS agent in your environment and follow these steps to run the application support installer.
	Note: This GUI requires an X Window System on UNIX and Linux computers. If you do not have an X Window System, you can run a silent installation of the application support files. See "Using a response file to install the application support files" on page 119 for information.
	a. Extract the compressed files that contain the application support files for each fix pack. Look for a file named "*pc*__tems_teps_tepd_fp0003.tar," where *pc* is "k" plus the 2-letter product code for the agent. For example, the file for the UNIX OS agent is kux_tems_teps_tepd_fp0003.tar.
	Note: Extract the application support files for each OS agent to a unique directory; otherwise, files from the different agents will over-write each other.
	b. From the directory where you extracted the application support files, launch the application support installer by running the following command:
	`java -jar directory\CD-ROM\setup.jar`
	where *directory* is the directory where you extracted the support files.
	Note: If you do not have the Java JRE in your path statement, change to the CD-ROM subdirectory and invoke the JRE executable file directly by specifying the path to it on the command line.
	For example, to run the application support installer for the UNIX OS agent, run the following commands:
	`cd c:\FP2_IMAGES\6.1.0-TIV-ITM_UNIX-FP0003\CD-ROM`
	`c:\program files\ibm\java142\jre\bin\java -jar setup.jar`
	See "Installing application support" on page 117 for more information.
	c. Follow the prompts in the application support installation wizard.
	d. Repeat this for each OS agent in your environment.
	See "Installing application support" on page 117 for more information about installing this support, including information about identifying the Java installation directory and the detailed steps for the application support installation wizard.

	7. Reconfigure the desktop client. In Manage Tivoli Enterprise Monitoring Services (or Manage Candle Services on Linux), right-click the desktop client and click **Reconfigure**. Click **OK** on the configuration window without making any changes.
	8. If you are running IBM Tivoli Monitoring in a globalized environment, re-install the base IBM Tivoli Monitoring language pack and then install the Fix Pack 003 Language Pack Fix Pack (6.1.0-ITM-LP-FP0003.zip or 6.1.0-ITM-LP-FP0003.tar). For information about installing the language packs, see the "Installing the language packs" section of Chapter 5, "Installing IBM Tivoli Monitoring" in the *IBM Tivoli Monitoring Installation and Setup Guide*.
	9. Install the monitoring agents (local and remote).

Monitoring agent checklist - local installation

The following checklist provides the high-level local installation steps for monitoring agents. Each agent fix pack is accompanied by a readme file that contains additional information. Be sure to check this readme file for any additional or unique installation steps.

Note: This checklist is for a local installation of the monitoring agent fix pack. You can also use the remote deployment function to deploy the fix packs across your monitoring environment. To use remote deploy, use the steps in the "Monitoring agent checklist - remote installation" on page 38.

Table 13. Checklist for locally installing the fix pack on an agent

✓	Installation step
	1. Gather information about the monitoring components in your environment. See "Fix pack installation planning worksheets" on page 25.
	2. Download and extract the fix pack files to a temporary location on your computer. **Patch directory:**
	3. Before installing any fix packs, stop all running IBM Tivoli Monitoring services through the Manage Tivoli Enterprise Monitoring Services utility (CandleManage on Linux and UNIX). Also stop this utility.

	4. Install the 6.1.0-TIV-ITM_INST-FP0003 fix pack.
	On Windows, run the following command from the command line:
	`cd patch_dir`
	`install_kui.bat`
	On UNIX or Linux, run the following command from the command line:
	`cd patch_dir`
	`./install_kui.sh`
	where *patch_dir* is the directory where you extracted the fix pack files.

	5. Run the **itmpatch** command to install the agent fix packs. `itmpatch -h ITMinstall_dir -i patch_file` See "Installing fix packs using the itmpatch command" on page 117 for more information.
	6. For OS agents, if you are running IBM Tivoli Monitoring in a globalized environment, re-install the base IBM Tivoli Monitoring language pack and then install the Fix Pack 003 Language Pack Fix Pack (6.1.0-ITM-LP-FP0003.zip or 6.1.0-ITM-LP-FP0003.tar). For information about installing the language packs, see the "Installing the language packs" section of Chapter 5, "Installing IBM Tivoli Monitoring" in the *IBM Tivoli Monitoring Installation and Setup Guide*.

Monitoring agent checklist - remote installation

The following checklist provides the remote installation steps for monitoring agents. Each agent fix pack is accompanied by a readme file that contains additional information. Be sure to check this readme file for any additional or unique installation steps.

Attention:

1. You must have already added these updates to your agent depot, as specified in step 10 in the "Monitoring server checklist" on page 29.
2. You cannot use the remote deploy function to update an agent locally. If you need to update an agent on the local computer, use the procedure outlined in "Monitoring agent checklist - local installation" on page 37.
3. Consider increasing the **tacmd** timeout period to ensure that you can successfully deploy the fix pack. The default value is 30 seconds. Increase this period to at least 60 seconds (1 minute). Use the following steps to increase the timeout period:

   On Linux and UNIX computers, edit the <*install_dir*>/bin/tacmd file and change the following environment variable:

   ```
   TACMD_TIMEOUT=30
   ```

   On Windows computers, edit the <*install_dir*>/bin/KUIENV file and change the following environment variable:

   ```
   TACMD_TIMEOUT=30
   ```
4. If you are remote deploying Windows OS Fix Pack 002, you must first manually deploy the prerequisite fix packs, 6.1.0-TIV-ITM_INST-FP0003 and 6.1.0-TIV-ITM_TEMA-FP0003. Because these prerequisite fix packs are at a different level than the Windows OS Fix Pack, they are not automatically deployed as part of the process that deploys the Windows OS fix pack. Use the steps in the table below to deploy these prerequisite fix packs.

Table 14. Checklist for remotely deploying the fix pack to an agent

✓	**Installation step**
	1. Ensure that the Manage Tivoli Enterprise Monitoring Services utility (the kinconfg.exe process) is stopped on all monitoring agents to which you are going to deploy fix packs.

Table 14. Checklist for remotely deploying the fix pack to an agent (continued)

✓	Installation step

	2. On the monitoring server, run the **tacmd updateAgent** command to remotely deploy the agent fix packs (which you previously added to the agent depot).
	`tacmd updateAgent -t pc -n node_name`
	
	where:
	pc Identifies the product to update, by product code. You have the following choices:
	• AX (UNIX) or GL (Windows) - Tivoli Enterprise Monitoring Agent
	• UI - Common install component (INST fix pack)
	• LZ - Linux OS agent
	• UL - UNIX Log agent
	• UM - Universal agent
	• UX - UNIX OS agent
	node_name
	Identifies the node, the directory on monitoring system where the OS agent is installed, to which you want to add the agent. The name of a node includes the computer where the OS agent is installed and the product code for the OS agent. For example, stone.ibm.com:LZ is the name of the node on computer stone.ibm.com, which has a Linux OS agent installed.
	The following example updates the Windows OS agent to the latest level available in the agent depot:
	`tacmd updateAgent -n Primary:WIN1:NT -t NT`
	The following example updates a Universal Agent running on UNIX to a specific fix pack level:
	`tacmd updateAgent -n unix1:KUX -t um -v 061003010`
	See "Deploying fix packs to remote agents" on page 120 for more information.

	3. For OS agents, if you are running IBM Tivoli Monitoring in a globalized environment, re-install the base IBM Tivoli Monitoring language pack and then install the Fix Pack 003 Language Pack Fix Pack (6.1.0-ITM-LP-FP0003.zip or 6.1.0-ITM-LP-FP0003.tar). For information about installing the language packs, see the "Installing the language packs" section of Chapter 5, "Installing IBM Tivoli Monitoring" in the *IBM Tivoli Monitoring Installation and Setup Guide*.

Installing the fix pack for the i5/OS monitoring agent

The procedure for installing the agent fix pack for the i5/OS monitoring agent differs from the other OS agents. Use the instructions in this section to install the i5/OS agent fix pack.

Note: Remember to install the application support files for the i5/OS agent on the monitoring server, portal server, and portal desktop client, as outlined in the installation checklists for those components.

Special instructions

Sign on as QSECOFR or with a profile with an equivalent special authority (SPCAUT) *ALLOBJ, *AUDIT, *IOSYSCFG, *JOBCTL, *SAVSYS, *SECADM, *SERVICE, *SPLCTL

Special note on User Authority: If object authority to OMA objects was granted or changed, the authorities will be lost when the new fix pack is installed. The following steps will allow the authorities to be restored.

Before installing the agent fix pack:

Note all user profiles that have been granted special authority to OMA objects. Example of finding special authority to one OMA object:

```
DSPOBJAUT OBJ(QAUTOMON/STROMA) OBJTYPE(*CMD) -
```

Repeat for other OMA objects that might have user profile authority granted.

Create a savefile for the security data to be saved. Example:

```
CRTSAVF FILE(yourlib/SECDTA)
```

Save the security data for the user profiles found. Example:

```
SAVSECDTA DEV(*SAVF) SAVF(yourlib/SECDTA)
```

After installing the agent fix pack:

Restore the saved user profiles. Example:

```
RSTUSRPRF DEV(*SAVF) USRPRF(user1 user2) SAVF(yourlib/SECDTA)
```

Use the RSTAUT command to restore authority to ALL objects that listed user profiles have had special authority granted. Example:

```
RSTAUT USRPRF(user1 user2)
```

Verify that the special authorities have been restored.

Installing the i5/OS agent fix pack

Use the following steps to install the fix pack:

1. Copy the fix pack tar file (6.1.0-TIV-ITM_i5OS-FP0003.tar) to a computer with ftp access to the i5/OS agent system.
2. Extract the fix pack tar file. This creates a directory structure that includes the save file for the updated i5/OS agent, a4520cma.sav.
3. On the i5/OS agent's system command line, create a CCCINST library, if this library doesn't already exist:

   ```
   CRTLIB  LIB(CCCINST)
   ```

4. Determine which version of the agent, if any, is currently installed using the **DSPSFWRSC** command. If product 0KA4430, 0KA4440, or 0KA4610 are listed then an agent is already installed.

   If 0KA4430, 0KA4440, or 0KA4610 is already installed, skip to Step 5. If no agent was previously installed, skip to Step 9.
5. Enter `GO OMA` to display the Tivoli Monitoring: i5/OS Agent panel. Use option 4, Configuration, and record the CMS Server values and port numbers. Use F12 to exit without updating the existing configuration.
6. Use **GO OMA** option 3 to end the agent and then use F3 to exit the OMA Menu. Make sure that no other users are displaying the Tivoli Monitoring: i5/OS Agent panel.
7. Create a save file on the target i5/OS computer and save the existing agent if desired. Saving the current agent enables you to restore it if you later choose to remove the new version. This step is optional.

   ```
    CRTSAVF   yourlib/PREFP03KA4
   SAVLICPGM LICPGM(0KA4yyy) DEV(*SAVF) SAVF(yourlib/PREFP03KA4)
   ```

   where *yyy* can be 430, 440, or 610
8. Use command **DLTLICPGM 0KA4430** if product 0KA4430 exists on the system, or use command **DLTLICPGM 0KA4440** if product 0KA4440 exits on the system. It is not required to delete product 0KA4610, although you may choose to do so using command **DLTLICPGM 0KA4610**.
9. Create a save file on the target i5/OS for the fix pack:

   ```
   CRTSAVF   CCCINST/A4520CMA  TEXT('ITM 6.1 Fix Pack 3')
   ```
10. FTP the agent save file to the target system. Use the following commands:

    ```
    ftp <target computer>
    login <i5/OS user profile and password>
    bin
    put c:\temp\a4520cma.sav CCINST/A4520CMA.savf
    quit
    ```
11. Load the fix pack from the save file:
    a. If you are installing the product on a computer that has English upper and lower case as the primary language (language ID 2924), run the following command:

       ```
       RSTLICPGM LICPGM(0KA4610) DEV(*SAVF) SAVF(CCCINST/A4520CMA)
       ```
    b. If you are installing on a computer that does not have English ID 2924 as the primary language, then run the following two commands:

       ```
       RSTLICPGM LICPGM(0KA4610) DEV(*SAVF) RSTOBJ(*PGM) SAVF(CCCINST/A4520CMA)

       RSTLICPGM LICPGM(0KA4610) DEV(*SAVF) RSTOBJ(*LNG) LNG(2924)  /
             SAVF(CCCINST/A4520CMA) LNGLIB(QKA4LNG)
       ```
12. Optionally delete the installation library, which is no longer needed:

    ```
    DLTLIB CCCINST
    ```
13. Configure the agent, then start it. Use **GO OMA**, option 4 to configure the agent. Use the values you recorded in Step 5. Use **GO OMA**, option 2 to start the agent.

Uninstalling the fix pack

Use the following steps to uninstall the fix pack:

1. Save the configuration file QAUTOTMP/KMSPARM(KBBENV) to create a backup of the current settings.
2. Stop the agent by using **GO OMA** Option 3.

Make sure the agent stopped by looking at WRKACTJOB. The subsystem QAUTOMON should not be running and all the jobs in QAUTOMON subsystem must be ended.

3. Exit out of the **GO OMA** menu completely.
4. Create a save file on the target i5/OS and save the existing agent if desired.

   Saving the current agent enables you to restore it if you later choose to remove the new version. This step is optional and the save file name can be any 10 character string.

   ```
    CRTSAVF   yourlib/FP03KA4BKP
   SAVLICPGM LICPGM(0KA4610) DEV(*SAVF) SAVF(yourlib/FP03KA4BKP)
   ```

   Note: Step 1 is required even if the existing agent saved. When you install using the saved file, it creates a new QAUTOTMP/KMSPARM(KBBENV) and it does not have any previous configurations.
5. Enter the following command to uninstall the agent:

   ```
   DLTLICPGM 0KA4610
   ```
6. Delete Authorization list QAUTOMON in QSYS:

   ```
   DLTAUTL QSYS/QAUTOMON
   ```
7. Delete short term history files.

   Short term history files exist in the location set for CTIRA_HIST_DIR in QAUTOTMP/KMSPAR(KBBENV). The default location is /QIBM/USERDATA/IBM/ITM/HIST Save the files in this directory and delete the files and the directory. There is no need to save these files if warehousing is configured. These files are warehoused at every 24 hours interval.

Installing the IBM Tivoli Enterprise Console event synchronization fix pack

The following sections provide information about installing the IBM Tivoli Enterprise Console event synchronization fix pack on your Tivoli Enterprise Console event server:

- "Fix pack prerequisites"
- "Notes about rule bases"
- "Important information for Windows customers" on page 43
- "Installation instructions" on page 43
- "Verifying the installation of the event synchronization fix pack" on page 47
- "Uninstalling the IBM Tivoli Enterprise Console event synchronization" on page 47

Fix pack prerequisites

Before you can install this fix pack, you must have installed either the base event synchronization available with the GA level of IBM Tivoli Monitoring or IBM Tivoli Monitoring & Tivoli Enterprise Console Event Synchronization Fix Pack 1 on your event server.

Notes about rule bases

With this fix pack, the install wizard provides the capability to back up the targeted rule base.

If you have multiple rule bases that are using IBM Tivoli Monitoring and Tivoli Enterprise Console Event Synchronization, you can run the fix pack installation to

update each rule base. After you finish the first rule base, restart the fix pack installer and supply the targeted next rule base you want to update.

The rule bases targeted by the installer are upgraded and recompiled.

If the targeted rule base is the currently active rule base, it is reloaded. You must stop and restart the Tivoli Enterprise Console Server to make the reloaded version of the rule base the current rule base.

If the targeted rule base is not the currently active rule base, it is NOT reloaded. You must load the targeted rule base and then stop and restart the Tivoli Enterprise Console Server to make the targeted rule base current.

Use the **wrb -lscurrb** command from a bash command prompt (on Windows systems) or command prompt (on UNIX systems) to determine the current rule base.

Use the **wrb -loadrb <***rule base name***>** command from a bash command prompt (on Windows systems) or command prompt(on UNIX systems) to load a new rule base

Use the **wstopesvr** command from a bash command prompt (on Windows systems) or command prompt (on UNIX systems) to stop the Tivoli Enterprise Console Server.

Use the **wstartesvr** command from a bash command prompt (on Windows systems) or command prompt (on UNIX systems) to start the Tivoli Enterprise Console Server.

Any customer modifications to the targeted rule base's original omegamon.rls file must be manually migrated to the updated rule base's omegamon.rls file. Then the rule base must be compiled and loaded. After the rule base is loaded the Tivoli Enterprise Console Server must be stopped and restarted.

Note that this fix pack creates a backup copy of the original omegamon.rls file that is named omegamon.rls.bac in the <*rulebase_directory*>/TEC_RULES directory.

Important information for Windows customers

For a Windows event server, any existing rule base that was created with a relative (not absolute) path cannot be found unless you move the fix pack installer to the drive where the rule base exists. To verify that your existing rule base uses an absolute path, run the following command from a bash environment on your server:

```
wrb -lsrb -path
```

If the returned path includes text similar to hostname:\<*rulebase_directory*>, with no drive letter (such as C:\), you must copy the fix pack executable (setupwin32fp3.exe) file from the download directory to the drive where the rule base exists and run the fix pack installation from that location.

Installation instructions

There are three options for installing the event synchronization fix pack:

- "Installing from a wizard" on page 44
- "Installing from the command line" on page 44
- "Installing from the command line using a silent install" on page 46

Before you start the installation, download the 6.1.0-TIV-ITM_TEC-FP0003.tar file and extract the contents to a temporary location on your event server.

Installing from a wizard

Use the following steps to install event synchronization from the installation wizard:

1. On the event server, launch the event synchronization installation:

   On Windows, double-click the setupwin32fp3.bin file in the temporary directory where you extracted the fix pack files.

   On Linux or UNIX, run the following command:

   ```
   setup<operating_system>fp3.bin
   ```

   where <*operating_system*> is the operating system you are installing on. For example, run the following command on an AIX computer:

   ```
   setupAixfp3.bin
   ```

2. Click **Next** on the Welcome window.
3. Select **I accept the terms in the license agreement** and click **Next**.
4. Complete the following fields and click **Next**:

Table 15. IBM Tivoli Enterprise Console event synchronization configuration fields

Field	Description
Rule base name	The name of the rule base to be updated with the fix pack information.
Backup rule base name	If you want the install wizard to back up your rule base, provide a name for the back up version.
Backup rule base path	Type a path for the back up version of the rule base.

5. Click **Next**.
6. Click **Next** on the pre-installation summary panel.

   The installation begins.
7. When the installation and configuration steps are finished, you are given the option to automatically stop and restart the event server. If you want to have the wizard stop and restart your event server, select this option and click **OK**. Otherwise, click **OK** (you will have to manually stop and restart your event server).
8. Click **Finish** on the Summary Information window.

   Note: If any configuration errors occurred during installation and configuration, you are directed to a log file that contains additional troubleshooting information.

Installing from the command line

Use the following steps to install the event synchronization from the command line on your event server:

1. Run the following command to launch the installation:

   On Windows:

   ```
   setupwin32fp3.bin -console
   ```

   On UNIX:

   ```
   setup<operating_system>fp3.bin -console
   ```

where <*operating_system*> is the operating system you are installing on. For example, run the following command on an AIX computer:

```
setupAixfp3.bin -console
```

The following prompt is displayed:

```
Press 1 for Next, 3 to Cancel or 4 to Redisplay [1]
```

2. Type 1 to start the installation and press Enter.

   The following prompt is displayed:

   ```
   Software Licensing Agreement:
   Press Enter to display the license agreement on your screen. Please
   read the agreement carefully before installing the Program. After
   reading the agreement, you will be given the opportunity to accept it
   or decline it. If you choose to decline the agreement, installation
   will not be completed and you will not be able to use the Program.
   ```

3. Press Enter to display the software license agreement.
4. Type 1 and press Enter to accept the license.

   The following prompt is displayed:

   ```
   Press 1 for Next, 2 for Previous, 3 to Cancel, or 4 to Redisplay [1]
   ```

5. Type 1 and press Enter to continue.

   The following prompt is displayed:

   ```
   Rule base Name []
   ```

6. Type the name for the rule base and press Enter.

   The following prompt is displayed:

   ```
   If you want the installer to back up the rule base indicated above before
   modifying the rule base, please provide a backup rule base name.

   Backup rule base name []
   ```

7. Type the backup rule base name, if you want to use one, and press Enter. If you do not want to create a backup rule base, leave this option blank and press Enter.

   The following prompt is displayed:

   ```
   If you have provided a backup rule base name you must provide a backup rule
   base path. NOTE: We append the backup rule base name to the backup rule base
   path for clarity and easy look-up.

   Backup rule base path []
   ```

8. Type the path for the backup rule base and press Enter.

   Note: If you are creating a backup rule base, you *must* provide this path. If you are not creating a backup rule base, leave this option blank and press Enter.

   The following prompt is displayed:

   ```
   Press 1 for Next, 2 for Previous, 3 to Cancel, or 4 to Redisplay [1]
   ```

9. Type 1 and press Enter to continue.

   The following prompt is displayed:

   ```
   IBM Tivoli Monitoring
   Press 1 for Next, 2 for Previous, 3 to Cancel, or 4 to Redisplay [1]
   ```

10. Type 1 and press Enter to continue. The event synchronization is installed.

    The following prompt is displayed:

    ```
    Installation and Configuration has completed.
    Please stop and restart the Tivoli Enterprise Console Server.

    Press 1 for Next, 2 for Previous, 3 to Cancel, or 4 to Redisplay [1]
    ```

11. Type 1 and press Enter to continue.

    The following prompt is displayed:

    ```
    Installation and configuration has completed.
    Please restart the Tivoli Enterprise Console server for the changes to take
    effect.
    Mark appropriately below to restart the Tivoli Enterprise Console server.
    [ ] 1 - Restart the Tivoli Enterprise Console server to make changes effective

    To select an item enter its number, or 0 when you are finished: [0]
    ```

12. Type 0 and press Enter to continue.

    The following prompt is displayed:

    ```
    Press 3 to Finish, or 4 to Redisplay [1]
    ```

13. Type 3 to finish and press Enter.

You must stop and restart the event server for these changes to take effect.

Installing from the command line using a silent install

Use the following steps to install the event synchronization using a silent installation from the command line on your event server. This installation method runs silently, so you will not see status messages during the actual installation.

1. Run the following command to generate the configuration file:

   On Windows:

   ```
   setupwin32fp3.bin -options-template filename
   ```

   where *filename* is the name of the configuration file to create, for example, es_silentinstall.conf.

   On UNIX:

   ```
   setup<operating_system>fp3.bin -options-template filename
   ```

   where <*operating_system*> is the operating system you are installing on. For example, run the following command on an AIX computer:

   ```
   setupAixfp3.bin -options-template filename
   ```

2. Edit the output file to specify the **rulebasePanel.rbName** variable. Define the name of a rule base that has Tivoli Enterprise Console Event Synchronization installed. This is the rule base that will be updated.

   Notes:

   a. If you do not specify a rule base name, the installation will fail.
   b. Remove the pound signs (###) from the beginning of any value that you want to specify.
   c. Do not enclose any values in quotation marks (").
   d. If you do not specify any of the other values, the default values are used.
   e. If you specify values, ensure that the value you specify meets the minimum required values. Otherwise, the installation stops and an error is written to the log file.

3. Save the file.
4. Run the following command:

   On Windows:

   ```
   setupwin32fp3.bin -options filename -silent
   ```

   where *filename* is the name of your configuration file.

   On UNIX:

```
setup<operating_system>fp3.bin -options filename -silent
```

where <*operating_system*> is the operating system you are installing on. For example, on AIX, run the following command:

```
setupAixfp3.bin -options filename -silent
```

You must stop and restart the event server for these changes to take effect. (Stopping and restarting the event server can be done by the silent install wizard by marking the appropriate field).

When installation is complete, the results are written to the itm_tec_event_sync_install.log file. On UNIX, this log file is always created in the /tmp directory. For Windows, this file is creates in the directory defined by the %TEMP% environment variable. To determine where this directory is defined for the current command line window, run the following command:

```
echo %TEMP%
```

Verifying the installation of the event synchronization fix pack

To verify that the IBM Tivoli Monitoring and Tivoli Enterprise Console Event Synchronization fix pack has been successfully installed, do one of the following, depending on the operating system of the computer where your event server is running.

- **HP-UX:** Run the following command:

  ```
  swlist -v TecEvntSyncInstaller
  ```

  Verify that the displayed values for the parameter ismp_key has a value of 1.0.0.3, which indicates that Fix Pack 3 is applied.
- **Windows:** Review the vpd.properties file, located in the c:/Windows or c:/Winnt subdirectory. Locate the TecEvntSyncInstaller string and review the text for the |1|0|3|0|1.0.0.3 string, which indicates that Fix Pack 3 is applied.
- **AIX:** Review the vpd.properties file, located in the /usr/lib/objrepos directory. Locate the TecEvntSyncInstaller string and review the text for the |1|0|3|0|1.0.0.3 string, which indicates that Fix Pack 3 is applied.
- **Linux:** Review the vpd.properties file, located in the / or /root directory. Verify that the TecEvntSyncInstaller string reflects the string |1|0|3|0|1.0.0.3, which indicates that Fix Pack 3 is applied.
- **Solaris:** Run the following command:

  ```
  pkginfo -l ISitmTecE
  ```

  Verify that the displayed values for the parameter Version include a value of 1.0.3.0.DSP=1.0.0.3, which indicates that Fix Pack 3 is applied.

Uninstalling the IBM Tivoli Enterprise Console event synchronization

Use the following steps to uninstall the event synchronization from your event server:

Note: You cannot uninstall just the event synchronization fix pack - if you use these steps, you will uninstall the entire event synchronization package from your event server.

1. Run the following uninstallation program:
   - On Windows: %*BINDIR*%\TME\TEC\OM_TEC_uninst\uninstaller.exe

- On UNIX: *$BINDIR*/TME/TEC/OM_TEC/_uninst/uninstaller.bin

2. Follow the prompts in the uninstallation program.

You can also run this uninstallation program in silent mode (by running the program from the command line with the **-silent** parameter) or in console mode (by using the **-console** parameter).

You must stop and restart the event server for these changes to take effect. (Stopping and restarting the event server can be done by the uninstallation wizard by marking the appropriate field).

If your event server is running on an HP-UX computer, ensure that the $BINDIR/TME/TEC/OM_TEC/_uninst and $BINDIR/TME/TEC/OM_TEC/_jvm directories are successfully removed by the uninstallation program. If they are not, manually delete these directories.

Note: InstallShield can create a second _uninst directory called _uninst2 (InstallShield can also continue this out to _uninstX - where X is 2, 3, 4, 5, ...). This occurs when InstallShield finds an existing _uninst directory and another process has access to it. If this happens on the customer machine, the customer when uninstalling must use the uninstaller found in the latest directory. Using the uninstaller in the most recently created directory will properly uninstall the product.

Additional installation information

Be sure to review the following important additional installation information.

Installing on a computer with no previous IBM Tivoli Monitoring component

When you are installing the full product media, which has been updated to include the Fix Pack 003 changes and related agent fix packs, there are no other special installation instructions except what is noted in this file.

Note that, on Windows computers, you can choose to install into any directory, such as "c:\Program Files," when performing a full product media installation. The default installation directory is still c:\IBM\ITM. If you want to install into a different directory, you must alter the default directory.

Uninstalling the GA level of code

The following items describe how to uninstall the GA (general availability) version of IBM Tivoli Monitoring after applying a fix pack, if you choose to do so:

- If you install the GA code, you uninstall it with the GA code uninstaller. Use the Add/remove programs function on your computer or the silent setup.exe uninstallation option from the GA CD.
- If you install the GA code, and then run the fix pack installer, you still uninstall with the GA code uninstaller. Use the Add/remove programs function on your computer or the silent setup.exe uninstallation option from the GA CD.

Upgrading your GA level of code

You *cannot* upgrade an installed product with the full image refresh CD. The CD install replaces all components, overwriting any configuration and customization you have performed.

Adding agents to a patched environment

If you plan to add monitoring agents (both OS and non-OS agents) to your monitoring environment after you have applied Fix Pack 003 and you want to use the remote deploy function (instead of installing locally), you must use the **tacmd createNode** command (for OS agents) or **tacmd addSystem** command (for non-OS agents) to deploy the *GA* level of the agent and then upgrade that agent to the fix pack level using the **tacmd updateAgent** command.

You cannot have both the Fix Pack 003 full image and the Fix Pack 003 update image in the agent depot. If your agent depot already contains the full image, you can use the **tacmd removeBundles** command to remove the image from the depot. For example, to remove the AIX 5.3 UNIX OS agent full image bundle, run the following command:

```
tacmd removeBundles –i /mnt/bundles –t ux –p aix513 –v 06100301
```

For more information about the **tacmd removeBundles** command, see the ″Command Reference″ appendix in the *IBM Tivoli Monitoring Installation and Setup Guide*.

About the GA versions IBM Tivoli Monitoring V6.1 agent CDs for Windows platforms

The General Availability (GA) versions of the IBM Tivoli Monitoring V6.1 agent CDs for the Windows operating system must *NOT* be installed into an IBM Tivoli Monitoring V6.1 Fix Pack 003 environment or be used to populate a Tivoli Enterprise Monitoring Server depot. The IBM Tivoli Monitoring V6.1 agent CDs have been refreshed for use with Fix Pack 003.

A problem with the installer on the GA version of the IBM Tivoli Monitoring V6.1 agent CDs for the Windows operating system will cause a currently installed Fix Pack 003 Tivoli Enterprise Monitoring agent framework component to be replaced by the older GA version. When this occurs, the IBM Tivoli Monitoring V6.1 Fix Pack 002 Windows OS agent fails. The problem exists only on the Windows version of the IBM Tivoli Monitoring V6.1 agent CDs.

The IBM Tivoli Monitoring V6.1 agent CDs for the Windows operating system have been refreshed with an updated agent installer as well as a Fix Pack 1 level of the Tivoli Enterprise Monitoring agent framework component. In case a GA version of an IBM Tivoli Monitoring V6.1 agent CD was used to install an agent on a Windows operating system after installing IBM Tivoli Monitoring V6.1 Fix Pack 002 Windows OS agent, running the installer from the refreshed IBM Tivoli Monitoring V6.1 agent CD allows the previous version of Tivoli Enterprise Monitoring agent framework component to be restored to the Fix Pack 002 version. The agent version is *NOT* updated. The agents remain at the GA version.

It is important to note that when the Tivoli Enterprise Monitoring agent framework is overlaid by the GA version on computers where the IBM Tivoli Monitoring V6.1 Fix Pack 002 Windows OS agent has been installed, there is no way to administer the system remotely because the Windows OS agent is the prerequisite to all remote administration capabilities. The local installation procedure described above is the only recovery mechanism.

You need to replace your GA version of the IBM Tivoli Monitoring V6.1 agent CD images for the Windows operating system with the refreshed agent CD images. In addition, non-OS agents must also be recreated in the agent depot. If the GA

version of non-OS agents has been placed in the agent depot, the agent bundle must be removed before it can be added back to the depot using the refreshed IBM Tivoli Monitoring V6.1 agent CDs.

See Appendix A in the *IBM Tivoli Monitoring Administrator's Guide* for more information about using the **tacmd removeBundles** and **tacmd addBundles** commands to remove agents from and add agents to the agent depot.

Identifying a refreshed version of IBM Tivoli Monitoring agent CD images

Identify the refreshed IBM Tivoli Monitoring V6.1 agent CD images by examining the KGLWICMA.ver file in the VERFiles directory of the CD image. The KGLWICMA.ver file indicates a VRMF value of 06100301 under the [COMPONENT INFO] tag as shown in the following example:

```
[COMPONENT INFO]
Product Code=GL
Desc=Tivoli Enterprise Monitoring Agent Framework
ComponentID=KGLWICMA
PlatformCode=WI
DPlatformCode=Windows
VRMF=06100301
```

To identify a refreshed agent image in an agent depot, the same KGLWICMA.ver exists in the VERFILES directory of the depot as shown in the following example:

```
C:\IBM\ITM\cms\Depot\Packages\WINNT\KUD\061000000\VERFILES
```

Summary of this section

Every General Availability (GA) version of the IBM Tivoli Monitoring V6.1 agent for Windows operating system CD and installation image must be replaced with the refreshed version. Every GA version of the IBM Tivoli Monitoring V6.1 agent bundle for the Windows operating system installed in a depot must be replaced with the refreshed version before it can be deployed into an IBM Tivoli Monitoring V6.1 Fix Pack 003 environment. You will encounter this scenario only when you install a GA-level application agent *AFTER* you have deployed the Fix Pack 001 or Fix Pack 002 OS agent.

Notes:

1. After you update the GA version of the IBM Tivoli Monitoring V6.1 agent bundle with the refreshed version, that agent bundle *cannot* be used to remotely uninstall the GA version of the agent from an endpoint system.
2. If you install the Fix Pack 002 version of the Windows OS agent on a computer that already contains a GA version agent, you must update that GA version agent with the refreshed version. If you install the Fix Pack 002 Windows OS agent on a computer, you must make sure that any other agents installed on that same computer are updated with that agent's refreshed version. All Windows application agents were refreshed with the updated version of the installation code when Fix Pack 001 was released.
3. If you install the Fix Pack 002 Windows OS agent after installing the GA version of the application agent, the agent framework is updated to the refreshed version. However, if you modify the GA version of the application agent installation by adding another agent from the same image, the KGLWICMA.ver file will no longer be accurate and it will appear as if the agent framework is at the unrefreshed GA version.
4. Do *not* use the **tacmd updateAgent** command to update a GA version of an IBM Tivoli Monitoring V6.1 agent on Windows with a refreshed version. If you do, you can cause the installation of the refreshed agent to create a duplicate

entry in the Add/Remove Programs list on the computer that you are updating. If this occurs, delete the duplicate entry by running a local uninstall of the agent after you remove the refreshed version of the IBM Tivoli Monitoring V6.1 agent.

Instead, you can use the **tacmd updateAgent** command to update a GA version of the agent with the agent *fix pack* image (and not the full image).

Chapter 3. Known problems and limitations

The following problems might occur during the use of this fix pack. Where available, workaround solutions are provided for the problems.

- Users cannot login to the Tivoli Enterprise Portal with mixed-case or lower-case user IDs that existed before applying Fix Pack 03 if your configuration includes a hub monitoring server running on one of the supported UNIX operating systems *and* Security Validation is turned on. Configurations that run the hub monitoring server on Windows or z/OS do not experience this problem. User IDs that are all upper-case do not experience this problem, nor do configurations where Security Validation is turned off. This problem will be addressed in Interim Fix 6.1.0.3-TIV-ITM_TEPS-IF0001 and is documented in APAR IY89043.
- The workspace migration utility can fail during an upgrade to Fix Pack 03 which results in some workspaces being back-leveled. A dialog is shown and indicates that the workspace is back-leveled with following message:

  ```
  KFWITM376W Workspace: Windows OS is back-leveled.

  Version found: 0, Version required: 1

  The Workspace will be rendered, but the Workspace Links will not be functional.
  ```

  If the workspace is modified and saved as new workspace, the dialog is not displayed. All workspaces that need to be migrated were not brought back to the client by the Tivoli Enterprise Portal Server.

  One of the possible causes of this problem in a UDB environment is the VERSION column in the KFWWORKSPACE table is missing.

  1. Open the DB2 control center on the computer where the portal server is installed.
  2. List the tables under the TEPS database.
  3. Select the properties for the KFWWORKSPACE table. After Fix Pack 03 is applied there should be a new column added to the end of the table called ″VERSION″ If the VERSION column is missing from the table execute the following to fix the issue:
     a. From the command prompt, change to the \ibm\itm\cnps\sqllib directory and run the following command.

        ```
        del *done*
        ```

     b. Go back one directory and run the buildpresentation.bat script.
     c. When the script completes go back into the UDB control center and check the KFWWORKSPACE table for the existence of a column named VERSION.
     d. If the VERSION column is present, then the portal server can be started and the workspace version issue should be resolved.
     e. If the VERSION column is not created, then collect the following logs and send them to IBM Software Support:

        \ibm\itm\logs*.log
        \ibm\itm\cnps\workspacemigrationutility.log
        \ibm\itm\cnps\buildpresentation.txt
        \ibm\itm\cnps\buildpresentationErr.txt
        \ibm\itm\cnps\sqllib\migrate.log

This problem will be addressed in Interim Fix 6.1.0.3-TIV-ITM_TEPS-IF0002.

- On Windows, updating application support files for the monitoring server, portal server, and portal client using the Application Support Installer (ASI) might fail if the installation path has spaces, such as ″C:\Program Files\IBM\ITM.″ To address this issue, for Windows installations where these components are installed into a path with spaces, if an agent is based on a fix pack prior to Fix Pack 003, copy the 6.1.0-TIV-ITM_INST-FP0003/ASI/setup.jar and 6.1.0-TIV-ITM_INST-FP0003/ASI/libwinjni.dll from the Fix Pack 003 INST component fix pack to the CD-ROM directory of the Fix Pack 002 location.
- If your workspace views display historical data across multiple pages, data is only displayed on the first page (and not displayed on subsequent pages).
- The command line interfaces to import and export workspaces have the following limitations:
  - Custom queries are not exported or imported by the **tacmd exportWorkspaces** and **tacmd importWorkspaces** commands. When you export a workspace that utilizes custom queries and import that workspace into a different server, the workspace will not work correctly unless you manually recreate the custom query on the server onto which you imported the workspace.
  - Custom situations are not exported or imported by the **tacmd exportWorkspaces** and **tacmd importWorkspaces** commands. Situation definitions, both predefined and custom, are stored on the Tivoli Enterprise Monitoring Server. When you export a workspace that uses custom situations and import that workspace into a Tivoli Enterprise Portal Server that connects to a different monitoring server than the portal server that you exported the workspace from, you must also export the situations from the original monitoring server to the new monitoring server. You can use the **tacmd viewSit** and **tacmd createSit** commands to export and import situations from one monitoring server to another; refer to the *IBM Tivoli Monitoring User's Guide* for more information about the **tacmd viewSit** and **tacmd createSit** commands.
  - When you export a workspace from one portal server to another (for example from a test environment to a production environment), that workspace will not be available from the logical view in the new portal server unless you have the exact same navigator items in the view. You cannot create these items manually but must instead migrate them from one environment to another. To ensure that you have the *exact* same items, use the following process for setting up your environment and migrating the workspaces:
    1. Create the logical view on the portal server in the test environment.
    2. Run the migrate-export utility to migrate the portal server information to an SQL file. For information on this migration utility, see the ″Tivoli Enterprise Portal Migration″ chapter in the *IBM Tivoli Monitoring Administrator's Guide*, located at http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/index.jsp?toc=/com.ibm.itm.doc/toc.xml.
    3. Move the SQL file created by the migrate-export utility to the portal server in the production environment.
    4. Run the migrate-import utility to replicate the logical view on the production portal server.
    5. On the portal server in the test environment, create your workspaces and customize as desired.
    6. Use the **tacmd exportWorkspace** command to export the workspaces from the test environment. See "tacmd exportWorkspaces" on page 107 for more information.

7. Use the **tacmd importWorkspace** command to import the workspaces in the production environment. See "tacmd importWorkspaces" on page 110 for more information.

Note: You must use the above process to create the navigator items in the new environment. You cannot manually create the navigator items.

- The **tacmd createNode** command might time out and generate the following Java exception in the trace_cn.log file:

```
<Exception><![CDATA[java.lang.StringIndexOutOfBoundsException: String index out
     of range: 1
     at java.lang.String.charAt(String.java(Compiled Code))
     at com.ibm.tivoli.remoteaccess.UNIXProtocol.getPerms(Unknown Source)
     at com.ibm.tivoli.remoteaccess.UNIXProtocol.putFile(Unknown Source)
     at com.ibm.tivoli.itm.install.remote.CreateNodeImage.distributeFiles
          (CreateNodeImage.java:2615)
     at com.ibm.tivoli.itm.install.remote.CreateNodeImage.install
          (CreateNodeImage.java:831)
     at com.ibm.tivoli.itm.install.remote.CreateNodeClient.main
          (CreateNodeClient.java:1607)
]]>
```

  This is a StringIndexOutOfBounds exception, which is caused by a lack of memory available. The solution is to free system memory and try again.

- If you are running the OMEGAMON XE for Messaging agent (a 32-bit agent) on a Linux or UNIX computer, you must install the 32-bit agent framework to support the application agent. Use the following steps to install the 32-bit framework:

  1. In the directory where you extracted the base IBM Tivoli Monitoring V6.1 installation files, run the following command:

     ```
     ./install.sh
     ```

  2. When prompted for the IBM Tivoli Monitoring home directory, press Enter to accept the default (/opt/IBM/ITM) or type the full path to a different directory.
  3. If the installation directory does not already exist, you are asked if you want to create it. Type `y` to create this directory and press Enter.
  4. The following prompt is displayed:

     ```
     Select one of the following:
     1) Install products to the local host.
     2) Install products to depot for remote deployment (requires TEMS).
     3) Exit install.

     Please enter a valid number:
     ```

     Note: This prompt might vary depending on the installation image from which you are installing.

     Type 1 to start the installation and press Enter.
  5. Type the number that corresponds to the language in which you want to display the software license agreement in and press Enter.
  6. Press Enter to display the agreement.
  7. Type 1 to accept the agreement and press Enter.
  8. Type a 32 character encryption key and press Enter. This key should be the same as the key that was used during the installation of the monitoring server to which this monitoring agent connects.

     A numbered list of available operating systems is displayed.

9. Type the number for the *32-bit version* of the operating system that you are installing on. So, if you are installing on a 64-bit AIX V5.3 computer, type the number that corresponds to 32-bit AIX V5.3. The default value is your current operating system. Press Enter.
10. Type `y` to confirm the operating system and press Enter.

    A numbered list of available components is displayed.
11. Type the number that corresponds to "Tivoli Enterprise Services User Interface V06.10.02.00" and press Enter.

    A list of the components to install is displayed.
12. Type `y` to confirm the installation.

    The installation begins.
13. After all of the components are installed, you are asked whether you want to install components for a different operating system. Type `n` and press Enter.

You can now install the OMEGAMON XE for Messaging agent.

- In some instances when upgrading custom workspaces from OMEGAMON® 350 to IBM Tivoli Monitoring V6.1 Fix Pack 003, depending on how the workspace was saved in OMEGAMON 350, the original default workspace might not be displayed for some users. The default workspace is still available under the list of workspaces returned under Enterprise Workspace.

  You can access the original default workspace and reset it as the default by doing the following steps:

  1. In the Enterprise Workspace, select the original default workspace.
  2. Click **Properties** in the toolbar.
  3. Under **Workspace Options**, select **Assign as default for this Navigator item**.
  4. Click **Apply** and **OK**.
  5. Close the portal. When you are asked if you want to save the changes you have made, click **Yes**.
  6. When you reopen the portal, the default workspace should be correctly displayed.
- In the Tivoli Enterprise Portal, a user with Administrator authority (including the new Workspace Administration permission) can only see global workspaces; that user cannot see workspaces created by individual users. Only the user who created a custom workspace can see it in the Navigation tree.
- Help or Expert Advice pages might not load in a Simplified Chinese language environment when using the browser client for the portal. This is related to a Java problem, which you can correct by setting the **-Dibm.stream.nio=true** Java Runtime parameter.

  On Windows computers, do the following to set this parameter:

  1. On the Control Panel, double-click the icon for the Java Plug-in.
  2. On the **Advanced** tab, type the following in the **Java Runtime Parameters** text box: `-Dibm.stream.nio=true`
  3. Click **Apply**.

  On Linux computers, do the following to set this parameter:

  1. From a command line, change to the jre/bin directory:

     ```
     cd ../../jre/bin directory
     ```
  2. Run the following command:

     ```
     ./JavaPluginControlPanel
     ```

3. On the **Advanced** tab, type the following in the **Java Runtime Parameters** text box: `-Dibm.stream.nio=true`
4. Click **Apply**.

- In some upgraded environments (for example in environments using a double-byte character set), you might need to re-install your Java for the Tivoli Enterprise Portal browser client, despite already having Java installed. This is because the portal server fix pack upgraded the level of Java available.
- If you are using the migration utility (migratewarehouse) to migrate your Tivoli Data Warehouse database, when the source database contains a large table (over 2 million rows of data), the default parameter for the Java Virtual Machine is not sufficient and will cause the utility to exceed available memory. To prevent this from occurring, prune the data in the database that you are migrating.
- APAR IY85582 changed the command entry syntax to accept a \: sequence to represent a :. While this corrected the original truncation problem, the saved command will not execute because the extra \ causes a syntax error on the underlying operating system.

Chapter 4. Changes and additions to the environment configuration variables

The following sections provide information about the changes made to environment variables within IBM Tivoli Monitoring. Changes were made both to support new functions (such as the ability to attach files to events) and to address product problems.

Controlling the number of log in attempts

You can specify the number of attempts a user can make to log into the Tivoli Enterprise Portal by setting the following environment variable in the KFWENV file (on Windows) or cq.ini (on Linux or AIX):

```
KFW_AUTHORIZATION_MAX_INVALID_LOGIN=0
```

Specify a value between 0 and 15. The default value, 0, indicates that there is no limit to the number of failed attempts a user can make before they are locked out.

Notes:

1. For Linux and AIX portal servers, you will need to add the above variable to the cq.ini file.
2. This configuration setting is only effective when you have enabled security through the monitoring server (the **Security: Validate User** option). On Linux and UNIX monitoring servers, you must also enable the Login Lockout feature by adding the following line to the monitoring server configuration file:

   ```
   KDS_VALIDATE_EXT=Y
   ```

   The monitoring server configuration files, <*node*>_ms_<*server*>.config and ms.ini, are located in the *ITMinstall_dir*/config directory, where *ITMinstall_dir* is the location where you installed IBM Tivoli Monitoring.

If a user is locked out, you have two options to restore their access to the Tivoli Enterprise Portal:

- You can edit the user from inside the user administration window in the portal and select the **Logon Permitted** option.
- You can run the following command line utility to enable or disable access:

  On Windows:

  ```
  KfwAuthorizationAccountClient.exe ENABLE|DISABLE user_name
  ```

  where *user_name* is the name of the user.

  On Linux:

  ```
  cd ITMinstall_dir/platform/cq/bin
  . ITMinstall_dir/config/cq.config
  . pathsetup.sh
  ./KfwAuthorizationAccountClient ENABLE | DISABLE user_name
  ```

Note that you can also use either of the above procedures to disable a user from accessing the portal, regardless of the KFW_AUTHORIZATION_MAX_INVALID_LOGIN setting.

Event management configuration

The following sections provide information about how to control event information in the IBM Tivoli Monitoring environment:

- "Event pruning"
- "Controlling the size of event attachments"

Event pruning

One of the new enhancements to the way that events are handled within IBM Tivoli Monitoring is that event information is now stored in the KFW tables in the portal server database. Because this information can grow in the amount of space it consumes, it is automatically pruned.

By default, closed events are removed from the database one day after they are closed, within the hours of 12:00 AM and 4:00 AM on the local portal server.

You can control the pruning of this data by changing the following environment variables in the KFWENV configuration file:

KFW_PRUNE_START = *hh:mm*
: The time of day to start pruning data, specified in 24-hour notation. For example, to begin pruning data at 11:00 PM, specify `23:00`.

KFW_PRUNE_END = *hh:mm*
: The time of day to stop pruning data, specified in 24-hour notation. For example, to end pruning data at 1:00 AM, specify `01:00`.

KFW_EVENT_RETENTION = *d*
: The number of days to keep a closed event. For example, to prune an event 2 days after it is closed, specify `2`.

Controlling the size of event attachments

You can control the size of file attachments for events either at the individual client level, by changing client interface variables, or at the monitoring environment level, by changing environment variables in the KFWENV configuration file.

Note: Settings made at the client level take precedence over those at the monitoring environment level. If you have specified a setting at the client level, the KFWENV variables are ignored. If you have not specified a setting at the client level, the KFWENV variables are used. If you have not specified any settings, the default values are used.

By default, the maximum file attachment size is 10 MB, while the maximum segment size (the size of segments of information into which the attachment is broken up to send across the network) is 1 MB.

Changing the client interface variables

Use the following steps to change the client interface variables:

1. In the Manage Tivoli Enterprise Monitoring Services utility (on Windows) or Manage Candle Services (on Linux), right-click **Tivoli Enterprise Portal - Desktop** or **Tivoli Enterprise Portal - Browser** and click **Reconfigure**.
2. Double-click one of the following variables:

   cnp.attachment.total.maxsize
   : Specify the new maximum file attachment size. The default value is 10 MB.

cnp.attachment.segment.maxsize
Specify the new maximum size for file segments. The default value is 1 MB.

3. Click **OK** to close the configuration window.
4. Start the portal server to make the changes take effect.

Changing the KFWENV environment variables

To change the attachment configuration variables at the monitoring environment level, edit the KFWENV configuration file and edit the following variables:

KFW_ATTACHMENT_MAX = *n*
Specify the new maximum file attachment size. The default value is 10 MB.

KFW_ATTACHMENT_SEGMENT_MAX = *n*
Specify the new maximum size for file segments. The default value is 1 MB.

Save and close the file.

Change to enablement of HTTP proxy server on browser client

Environments that use an HTTP proxy server require additional Tivoli Enterprise Portal client configuration to enable URL access within the browser view. For the desktop client, this reconfiguration is done through Manage Tivoli Enterprise Monitoring Services. However, if you use the same method for the Tivoli Enterprise Portal browser client or edit applet.html directly, the change has no effect. Users receive the error message, ″Server refuses to serve document″ when attempting to launch a URL in the browser view.

The HTTP proxy server parameters have been removed from the Configure Tivoli Enterprise Portal Browser window, and the instructions in the Administrator's Guide to Enable the HTTP Proxy Server for the browser client are no longer valid. Please use the following procedure to enable the HTTP proxy server for the browser client through the Java plug-in. For your convenience the desktop client method, which has not changed, is included here.

Enabling the HTTP proxy server

Environments that use an HTTP proxy server require additional client configuration to enable URL access from the Tivoli Enterprise Portal browser view. The method is different for the browser client and desktop client.

Browser client

For the Tivoli Enterprise Portal browser client, enable the HTTP proxy server through the Java plug-in control panel as described here. This must be done on every computer where access to the Tivoli Enterprise Portal is through the browser.

1. Select **Java Plug-in** from the Windows Control Panel.

   If you have multiple versions of Java running be sure this is the one used for the Tivoli Enterprise Portal: The Cache tab identifies the cache location, which should include an IBM subdirectory; and the About tab identifies the Java version.
2. Click the **Advanced** tab
3. Select the IBM JRE from the Java Runtime Environment list.
4. Enter the following HTTP proxy arguments in the Java Runtime Parameters field.

They would normally be added after the required Java heap memory settings (`-Xms128m -Xmx256m`) that are required for the browser client.

```
-Dhttp.proxyHost=myProxyHost -Dhttp.proxyPort=myProxyPort
```

where `myProxyHost` is the DNS identifier or the IP address of the proxy host to use for the HTTP protocol and `myProxyPort` is 80 (default port number) or a different number used by the proxy host.

5. If your configuration uses the IBM integrated HTTP (Web) server, enter the following HTTP non-proxy arguments for the browser client:

   ```
   -Dhttp.nonProxyPorts=1920
   ```

   where `1920` is the default port number of the integrated Web server.

   If, however, your configuration uses an external HTTP server because of, say, a NAT firewall configuration for portal client access to the portal server, you will need to complete the next step to specify a host name instead.

6. If your portal server uses an external HTTP server instead of the integrated HTTP server or you want to bypass the proxy server for certain Web sites being accessed from the Tivoli Enterprise Portal browser view or both, enter the following HTTP non-proxy arguments:

   ```
   -Dhttp.nonProxyHosts=hostname|hostname|hostname|...
   ```

   where `hostname` is a URL, separated from the next URL by a `|` vertical line. If your portal server uses an external HTTP server instead of the integrated HTTP server, this is the host name or IP address of the computer where the portal server is installed.

7. If the Web sites that bypass the HTTP proxy server should use a different port than what is specified for the portal server, add the port to the `-Dhttp.nonProxyPorts` arguments, separated by a `|` vertical line (`-Dhttp.nonProxyPorts=port|port`). Example:

   ```
    -Xms 128m -Xmx256m -Dhttp.proxyHost=9.50.105.115 -Dhttp.proxyPort=80
   -Dhttp.nonProxyPorts=1920 -Dhttp.nonProxyHosts=*ibm.com|usps.gov
   ```

   These parameters set the Java heap memory, the IP address 9.50.105.115 and listening port 80 for the proxy server, and indicate that all http requests to port 1920 (those routed to the TEPS integrated HTTP server) and any requests to *ibm.com or usps.gov bypass the proxy server.

Desktop client

The HTTP proxy server for the desktop client is enabled through Manage Tivoli Enterprise Monitoring Services.

1. Start Manage Tivoli Enterprise Monitoring Services from the system where the Tivoli Enterprise Portal desktop client is installed:
   - Windows: Start → Programs → IBM Tivoli Monitoring→ Manage Tivoli Enterprise Monitoring Services.
   - UNIX: Change the directory to install_dir/bin and enter **./itmcmd manage.**
2. Right-click Tivoli Enterprise Portal - Desktop and select **Reconfigure**.
3. In the Configure Application Instance window that opens, select the **Enable HTTP Proxy Server** check box.
4. In the **PS Host** field, enter the domain name system (DNS) identifier or the IP address of the proxy host to use for the HTTP protocol.
5. In the **PS Port** field, either:
   - Leave 80 as the default port number of the HTTP proxy host
   - If the proxy host uses another port number, enter it here.

6. If you want to bypass the proxy server for certain Web sites being accessed from the Tivoli Enterprise Portal browser view:
   a. Double-click http.nonproxyhosts in the parameters list.
   b. In the Value field, enter the server names, separated with a vertical line (|), and surround the list in double-quotes (").

   For example, if you want the requests to *.ibm.com and usps.gov servers to not go through the proxy, the list reads:

   "*ibm.com|usps.gov"
7. If your proxy server requires a different identity for the IBM integral browser before it will allow Internet access from the browser view:
   a. Double-click http:agent in the parameters list.
   b. Enter a one-word name for the browser.

   It can be any name so long as it is not rejected by the proxy server. You normally would not need to add an http name definition unless users get an error when they attempt to access the Internet through a Tivoli Enterprise Portal browser view.
8. Select **In Use** and click **OK**.

Chapter 5. Installing and configuring the portal server on AIX

Fix Pack 003 adds support for installing the Tivoli Enterprise Portal Server on an AIX computer. Follow the instructions in this chapter to install and configure the portal server and portal client on an AIX computer.

Important:

- To install the portal server, you must install from the full image refresh (available from Passport Advantage), and not from the fix pack image (available from the IBM Software Support Web site).
- Run these installation and configuration procedures as either the root user or as the DB2® administrator. After you have installed and configured the portal server, you can use a different user to run the portal server, as long as that user has access to the binaries used by the portal server.
- DB2 is the only database supported for an AIX portal server. See Table 5 on page 8 for information about the operating systems and database levels supported on AIX.
- There is no unique 64-bit version of the portal server installation for a 64-bit AIX operating system. Instead, use the 32-bit installation image for the portal server; it will operate in 32-bit mode on the 64-bit operating system.
- Regardless of the bit level of your AIX operating system (32-bit vs. 64-bit), you must use a 32-bit DB2 instance.
- To install the application support files for the portal server on AIX for OS agents, use the original OS agent CD. To install application support files for the following agents, use the supplemental CD, *Agent Support for Tivoli Enterprise Portal server on AIX*.
  - IBM Tivoli Monitoring for Applications - mySAP Agent V6.1
  - IBM Tivoli Monitoring for Messaging and Collaboration V6.1
  - IBM Tivoli Monitoring V6.1 Active Directory Monitoring Option
  - IBM Tivoli Monitoring for Databases V6.1
  - IBM Tivoli Monitoring for Virtual Servers V6.1
  - IBM Tivoli Monitoring for Cluster Managers V6.1
  - IBM Tivoli Composite Application Manager for WebSphere V6.0
  - IBM Tivoli Composite Application Manager for Transaction Tracking V6.0
  - IBM Tivoli Monitoring Agent for z/NetView V5.2.5
  - IBM Tivoli Composite Application Manager for Response Time Tracking V6.1
  - IBM Tivoli Composite Application Manager for Service-Oriented Architecture V6.0

Installing the portal server

Use the following steps to install the portal server:

1. In the directory where you extracted the installation files, run the following command:

   ```
   ./install.sh
   ```

2. When prompted for the IBM Tivoli Monitoring home directory, press Enter to accept the default (/opt/IBM/ITM) or type the full path to a different directory.

3. If the installation directory does not already exist, you are asked if you want to create it. Type `y` to create this directory and press Enter.
4. The following prompt is displayed:

   ```
   Select one of the following:
   1) Install products to the local host.
   2) Install products to depot for remote deployment (requires TEMS).
   3) Exit install.

   Please enter a valid number:
   ```

   Type 1 to start the installation and press Enter.
5. Type the number that corresponds to the language in which you want to display the software license agreement in and press Enter.
6. Press Enter to display the agreement.
7. Type 1 to accept the agreement and press Enter.
8. Type a 32 character encryption key and press Enter. This key should be the same as what was used during the installation of the monitoring server to which this portal server will connect.

   A numbered list of available operating systems is displayed.
9. Type the number for the operating system that you are installing on. The default value is your current operating system. Press Enter.
10. Type `y` to confirm the operating system and press Enter.

    A numbered list of available components is displayed.
11. Type the number that corresponds to the portal server and press Enter.

    A list of the components to install is displayed.
12. Type `y` to confirm the installation.

    The installation begins.
13. After all of the components are installed, you are asked whether you want to install components for a different operating system. Type `y` and press Enter.
14. Type the number that corresponds to ″Tivoli Enterprise Portal Browser Client support″ and press Enter.
15. Type `y` to confirm and press Enter.

    A list of the components to install is displayed.
16. Type the number that corresponds to ″all of the above″ and press Enter.
17. Type `y` to confirm the installation.

    The installation begins.
18. When you are asked whether you want to install components for a different operating system, type `y` and press Enter.
19. Type the number that corresponds to ″Tivoli Enterprise Portal Server support″ and press Enter.
20. Type `y` to confirm and press Enter.

    A list of the components to install is displayed.
21. Type the number that corresponds to ″all of the above″ and press Enter.
22. Type `y` to confirm the installation.

    The installation begins.
23. After all of the components are installed, you are asked whether you want to install components for a different operating system. Type `n` and press Enter.

Configuring the portal server

Use the following steps to configure the portal server.

Note: You can also use this procedure to reconfigure the AIX portal server, if needed.

1. At the command line change to the *ITMinstall_dir*/bin directory, where *ITMinstall_dir* is the directory where you installed the product.
2. Run the following command:
   ```
   ./itmcmd config -A cq
   ```
3. Press Enter when you are asked if the agent connects to a monitoring server.
4. Type the host name for the hub monitoring server and press Enter.
5. Type the protocol that you want to use to communicate with your hub monitoring server. You have four choices: ip, sna, ip.pipe, or ip.spipe.
6. If you want to set up a backup protocol, enter that protocol and press Enter. If you do not want to use backup protocol, press Enter without specifying a protocol.
7. Depending on the type of protocol you specified, provide the following information when prompted:

Table 16. UNIX monitoring server protocols and values

Protocol	Value	Definition
IP.UDP	IP Port Number	The port number for the monitoring server. The default is 1918.
SNA	Net Name	The SNA network identifier for your location.
	LU Name	The LU name for the monitoring server. This LU name corresponds to the Local LU Alias in your SNA communications software.
	Log Mode	The name of the LU6.2 LOGMODE. The default value is ″CANCTDCS.″
IP.PIPE	IP.PIPE Port Number	The port number for the monitoring server. The default is 1918.
IP.SPIPE	IP.SPIPE Port Number	The port number for the monitoring server. The default is 3660.

8. Press Enter when you are asked if you want to configure the connection to a secondary monitoring server. The default value is no.
9. Press Enter to accept the default for the Optional Primary Network Name (none).
10. Press Enter to accept the default setting for SSL between the portal server and clients (`N`). By default, SSL is disabled. To enable SSL, type `y` and press Enter.
11. Type the DB2 instance name. The default value is ″db2inst1.″ Press Enter.
12. Type the DB2 administrator ID. The default is ″db2inst1.″ Press Enter.
13. Type the password for the DB2 administrator ID and press Enter.

14. Confirm the password for the DB2 administrator ID by typing it again. Press Enter.
15. Type the name of the database for the portal server. The default is ″TEPS.″ Press Enter.
16. Type the name (or ″login″) of the database user that the portal server will use to access the database. The default is ″itmuser.″ Press Enter.
17. Type the password for the database user and press Enter.
18. Confirm the password for the database user by typing it again. Press Enter.
19. You are asked if it is okay to create the DB2 login user if it does not exist. Type y and press Enter.
20. Type the name of the database that the Tivoli Data Warehouse will use. The default is ″WAREHOUS.″ This database must be cataloged locally if the warehouse database resides on a remote computer. Press Enter.

    Note: If you are using a remote node and database, you must manually configure (catalog) the remote node and the remote database from the AIX DB2 command line. Run the following commands to do this:

    ```
    db2 catalog tcpip node <node_name> remote <host_name> server <port>
    db2 catalog db <db_name> as <dbalias> at node <node_name>
    ```

21. Type the name of the database user that the Tivoli Data Warehouse will use. The default is ″itmuser.″ Press Enter.
22. Type the password for the Warehouse user ID and press Enter.
23. Confirm the password for the Warehouse user by typing it again. Press Enter.

Starting the portal server

From the *ITMinstall_dir*/bin directory, where *ITMinstall_dir* is the directory where you installed IBM Tivoli Monitoring, run the following command to start the portal server:

```
./itmcmd agent start cq
```

Chapter 6. Installing and configuring the Warehouse Proxy on AIX and Linux

Fix Packs 002 and 003 add support for the Warehouse Proxy agent on AIX and Linux computers. The Warehouse Proxy on AIX and Linux uses a JDBC connection to export data collected from IBM Tivoli Monitoring agents to the Tivoli Data Warehouse.

Note: You must install the Warehouse Proxy from the full image refresh and not the fix pack image.

Software prerequisites

The following prerequisite software is required for setting up a Warehouse Proxy on AIX or Linux:

- One of the following relational database management products is required to support the Tivoli Data Warehouse: DB2, Oracle, or Microsoft SQL Server. See "Supported databases for Tivoli Enterprise Portal Server and Tivoli Data Warehouse" on page 8 for information about the supported database versions and operating systems.
- An X Window System is required to configure the Warehouse Proxy on AIX or Linux.

Overview of steps

Perform the following tasks to set up an operational Warehouse Proxy on AIX or Linux:

1. Create the Tivoli Data Warehouse database and a user to connect to the database.
2. Install the Warehouse Proxy agent.
3. Copy or download the JDBC driver files to the computer where the Warehouse Proxy agent is installed.
4. Configure the Warehouse Proxy agent.
5. Start the Warehouse Proxy agent.

Creating the Tivoli Data Warehouse database

To support a Warehouse Proxy on AIX or Linux, you can use an IBM DB2, Oracle, or Microsoft SQL database for the Tivoli Data Warehouse. Refer to your database product documentation for information on how to create a database or have a database administrator create the database for you. For guidance on planning the size and disk requirements for the Tivoli Data Warehouse database, see "Planning considerations for the Tivoli Data Warehouse" in the *IBM Tivoli Monitoring Installation and Setup Guide*.

When you create the database for the Tivoli Data Warehouse, follow these guidelines:

- Create the data warehouse database with UTF-8 encoding.
- Create a name for the data warehouse database, and a user name and password to access the data warehouse. (For Microsoft SQL Server, do *not* use the system

administrator (sa) user to connect to the data warehouse.) Consider using the default values shown in Table 17. The default values are displayed in the fields of the configuration window for the Warehouse Proxy. (See Figure 2 on page 73.)

Table 17. Default values for Tivoli Data Warehouse parameters

Parameter	Default value
Tivoli Data Warehouse database name	WAREHOUS
User name	itmuser
User password	itmpswd1

- Give the user authority to create and update tables, to insert information into the tables, to create indexes for the tables, and to grant public authority to the tables.
  - If you are using a DB2 database, also include *create tablespace* and *create bufferpool* authorities.
  - If you are using Microsoft SQL server, give the user public and db_owner privileges to the Tivoli Data Warehouse database.
- For Microsoft SQL Server 2005, make sure the database is set up to support inbound network TCP/IP connections.
- If you are creating the Tivoli Data Warehouse in DB2 on a UNIX system, ensure that the UNIX server and listener are active. Run the following commands:

```
db2set -i instance_name DB2COMM=tcpip
db2 update dbm cfg using SVCENAME port_number
db2 stop
db2 start
```

  where *instance_name* is the name of the instance in which you created the database and *port_number* is the listening port for the instance. (The port number is specified in the file /etc/services.) For example:

```
db2set -i db2inst1 DB2COMM=tcpip
db2 update dbm cfg using SVCENAME 60000
db2 stop
db2 start
```

Installing the Warehouse Proxy agent

To install the Warehouse Proxy agent on a Linux system, see the section entitled "Linux or UNIX: Installing a monitoring agent" in the *IBM Tivoli Monitoring Installation and Setup Guide*. Follow the instructions within the following subsections:

- "Installing the monitoring agent"
- "Changing the file permissions for agents" (if you used a non-root user to install the Warehouse Proxy)

Note: Do not use the fix pack installer to install the Warehouse Proxy agent.

Installation log files are in the $*ITMinstall_dir*/logs directory:

- C trace : <*hostname*>_hd_<*date*>-0<#>.log
- Java trace: <*hostname*>_hd_java_<*date*>-0<#>.log

There can be 5 files maximum for the C trace and 6 files for the Java trace. The first log file (#1) is always kept; subsequent log files are kept up to the 5th (C

trace) or 6th (Java trace) file. When the maximum number of files is reached, the next file replaces the oldest existing log file (#2).

Copying or downloading the JDBC driver files

The JDBC driver JAR files that come with your database product must be located on the computer where you installed the Warehouse Proxy agent.

- If you are using DB2 for your Tivoli Data Warehouse database, the JDBC driver files are included with the database product installation. If your Tivoli Data Warehouse is located on a remote computer, copy the driver files to the local computer (the computer where you installed the Warehouse Proxy agent).
- If you are using Oracle or Microsoft SQL Server for your Tivoli Data Warehouse database, download the driver files from the company Web site to the computer where you installed the Warehouse Proxy agent.

The following table shows where to obtain the driver files for each database product. Copy or download the files to any directory on the computer where the Warehouse Proxy agent is installed.

Table 18. Where to obtain the JDBC driver files for connecting the Warehouse Proxy on AIX or Linux to the Tivoli Data Warehouse

Database product	**JDBC driver files**
IBM DB2	The DB2 driver files are located with your Tivoli Data Warehouse server installation in the following directories: <*db2installdir*>/java/db2jcc.jar <*db2installdir*>/java/db2jcc_license_cu.jar where <*db2installdir*> is the directory where DB2 was installed. The default DB2 Version 8 installation directory is as follows: • On AIX: /usr/opt/db2_08_01 • On Linux: /opt/IBM/db2/V8.1
Oracle	Obtain the Oracle JDBC Driver from the following Web site: http://www.oracle.com/technology/software/tech/java/sqlj_jdbc/index.html Download the `ojdbc14.jar` file. This file supports JRE 1.4.2 or higher, the required Java Runtime Environment for IBM Tivoli Monitoring.
Microsoft SQL Server	Use the Microsoft SQL Server 2005 Driver to connect to a Tivoli Data Warehouse on either SQL Server 2000 or SQL Server 2005. (The SQL Server 2005 JDBC Driver works with a Tivoli Data Warehouse on SQL Server 2000.) Obtain the 2005 JDBC driver from the following Microsoft Web page: http://msdn.microsoft.com/data/jdbc/default.aspx Download and install the driver to the computer where you installed the Warehouse Proxy agent. Follow the instructions on the Microsoft download page for installing the driver. After you install the driver, the JAR file name and location are as follows: `/sqljdbc_1.0/enu/sqljdbc.jar`

Configuring the Warehouse Proxy agent

After you install the Warehouse Proxy agent and JDBC drivers on an AIX or Linux computer, you are ready to configure the Warehouse Proxy agent. The purpose of configuration is to establish the JDBC connection between the Warehouse Proxy agent and the Tivoli Data Warehouse and to register the Warehouse Proxy agent with the Tivoli Enterprise Monitoring Server.

1. Log on to the computer where the Warehouse Proxy agent is installed.
2. Start the Manage Tivoli Enterprise Monitoring Services utility:
   a. Change to the bin directory:
      `cd install_dir/bin`
   b. Run the following command:
      `./itmcmd manage [-h ITMinstall_dir]`

      where:

Table 19. Parameters for the itmcmd manage command

-h	(optional) An option used to specify the installation directory.
ITMinstall_dir	The directory where the Warehouse Proxy agent is installed. The default installation directory is /opt/IBM/ITM.

      The Manage Tivoli Enterprise Monitoring Services window is displayed.

      Note: Note that the **Platform** column for agents lists the platform that the binary code was built on, not the platform that you are running on.
3. Right-click **Warehouse Proxy**.
4. Click **Configure**.
   The Configure Warehouse Proxy window is displayed.

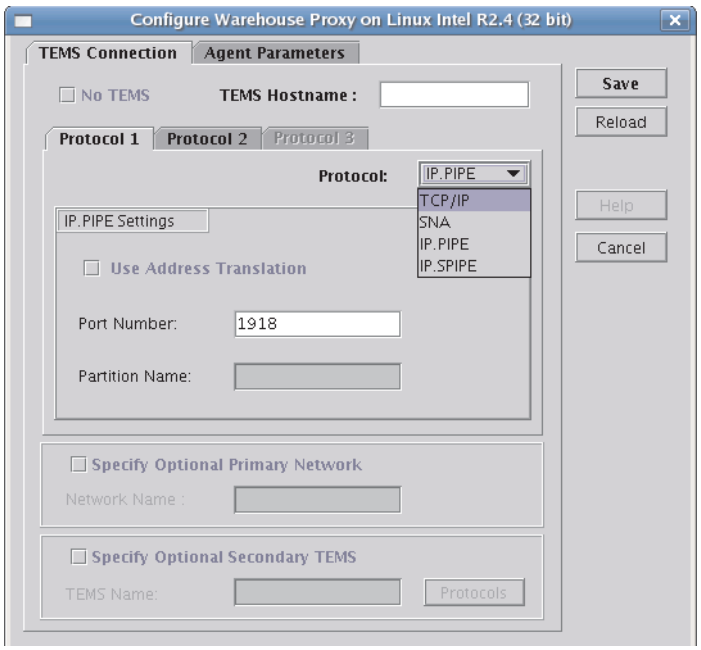


Figure 1. Registering the Warehouse Proxy agent with the Tivoli Enterprise Monitoring Server

5. On the TEMS Connection page, enter information about the Tivoli Enterprise Monitoring Server to which the Warehouse Proxy agent connects:
   - Enter the host name of the monitoring server in the **TEMS Hostname** field. (If the field is not active, clear the **No TEMS** check box.)
   - Select the communications protocol that the monitoring server uses from the **Protocol** drop-down list.
   - Enter the port number of the monitoring server in the **Port Number** field.
6. Click the **Agent Parameters** tab.

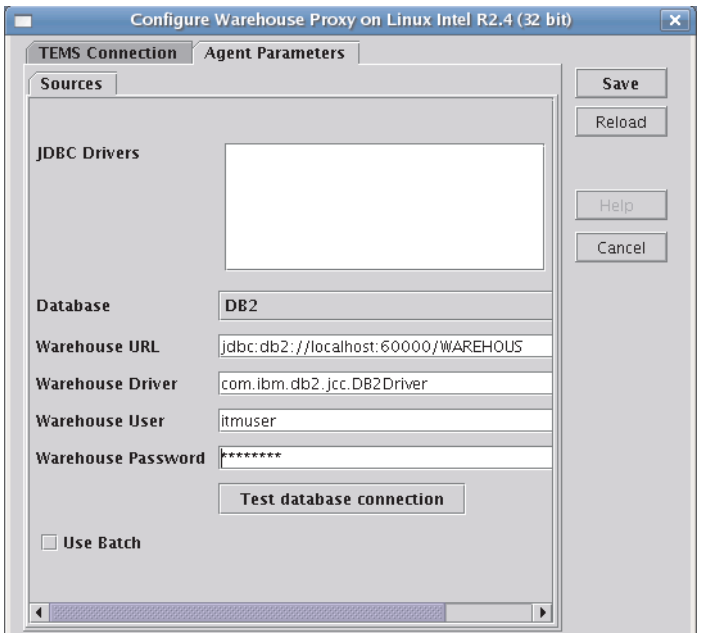


Figure 2. Configuring the JDBC connection for the Warehouse Proxy agent

7. Add the names and directory locations of the JDBC driver JAR files to the **JDBC Drivers** list box:
   a. Use the scroll bar at the bottom of the window to display the **Add** and **Delete** buttons, which are located to the right of the **JDBC Drivers** list box.
   b. Click **Add** to display the file browser window. Navigate to the location of the driver files on this computer and select the driver files for your database product. See Table 18 on page 71 for the names of the driver files to add.
   c. Click **OK** to close the browser window and add the JDBC driver files to the list.

   If you need to delete an entry from the list, select the entry and click **Delete**.
8. In the **Database** drop-down list, select the database product you are using for the Tivoli Data Warehouse.
9. Change the default value displayed in the **Warehouse URL** field if it is not correct. The following table lists the default Tivoli Data Warehouse URLs for the different database products:

Table 20. Tivoli Data Warehouse URLs

Database product	Warehouse URL
IBM DB2	jdbc:db2://localhost:60000/WAREHOUS
Oracle	jdbc:oracle:thin:@localhost:1521:WAREHOUS
Microsoft SQL Server 2000	jdbc:Microsoft:sqlserver://localhost:1433;databaseName=WAREHOUS
Microsoft SQL Server 2005	jdbc:sqlserver://localhost:1433;databaseName=WAREHOUS

   - If the Tivoli Data Warehouse is installed on a remote computer, specify the host name of the remote computer instead of `localhost`.
   - Change the port number if it is different.
   - If the name of the Tivoli Data Warehouse database is not WAREHOUS, replace WAREHOUS with the actual name. (See "Creating the Tivoli Data Warehouse database" on page 69.)
10. Verify the JDBC driver name, which is displayed in the **Warehouse Driver** field. (Note that the **Warehouse Driver** field displays the *driver name*, in contrast to the *driver JAR files* that are listed in the **JDBC Drivers** field.)

    The following table lists the JDBC driver names for each database product:

Table 21. JDBC driver names

Database product	JDBC driver name
IBM DB2	com.ibm.db2.jcc.DB2Driver
Oracle	oracle.jdbc.driver.OracleDriver
Microsoft SQL Server	com.microsoft.sqlserver.jdbc.SQLServerDriver **Note:** This is the name of the recommended 2005 SQL Driver. The name of the 2000 SQL Driver was com.microsoft.jdbc.sqlserver.SQLServerDriver. Note the reversal of the string `jdbc.sqlserver`.

11. If necessary, change the entries in the **Warehouse User** and **Warehouse Password** fields to match the user name and password that were created for

the Tivoli Data Warehouse. (See "Creating the Tivoli Data Warehouse database" on page 69.) The default user name is `itmuser` and the default password is `itmpswd1`.

12. Check the **Use Batch** check box if you want the Warehouse Proxy agent to submit multiple execute statements to the Tivoli Data Warehouse database for processing as a batch.

    In some situations, such as crossing a network, sending multiple statements as a unit is more efficient than sending each statement separately. Batch processing is one of the features provided with the JDBC 2.0 API.

    Note: Select this check box only if you are using a JDBC driver that supports the batch option. The Warehouse proxy agent fails if you select the check box when using a JDBC driver that does not support batch.

13. Click **Test database connection** to ensure you can communicate with the Tivoli Data Warehouse database.

    Note: If you are using DB2 and you receive the following error, you might need to add the path to the DB2 JDBC driver to your PATH environment variable:

    ```
    Database connection failed. The version of the IBM Universal JDBC driver in use
    is not licensed for connectivity to QDB2/NT databases.
    ```

    To address this, add the following statement to the PATH environment variable definition:

    ```
    /usr/opt/db2_08_01/java
    ```

    Stop and restart the Manage Tivoli Enterprise Monitoring Services utility.

14. Click **Save**.

Start the Warehouse Proxy

- To start the Warehouse Proxy agent from the Manage Tivoli Enterprise Services window, right-click **Warehouse Proxy** and select **Start**.
- To start the Warehouse Proxy agent from the command line, enter the following command:

  ```
  ./itmcmd agent start hd
  ```

  where `hd` is the product code for the Warehouse Proxy agent.

Chapter 7. Configuring a Linux portal server to support an Oracle data warehouse

Fix Pack 003 adds support for a Tivoli Data Warehouse on Oracle with a Tivoli Enterprise Portal Server on Linux. See Table 6 on page 9 for information about the supported operating systems and databases.

A JDBC connection is required for communication between a Tivoli Enterprise Portal Server on Linux and a Tivoli Data Warehouse on Oracle. The JDBC driver must reside on the computer where the portal server is installed.

The command line and GUI procedures for configuring the Tivoli Enterprise Portal Server on Linux have been modified to support communication between the portal server and a Tivoli Data Warehouse database on Oracle. The configuration procedures, described in the following sections, include steps for configuring the connection to both the Tivoli Enterprise Portal database and the Tivoli Data Warehouse database:

- The *Tivoli Enterprise Portal Server database* stores user data and information required for graphical presentation on the user interface. A portal server on Linux supports a portal server database on DB2 only. The portal server database is created automatically during configuration of the portal server. The portal server and the portal server database reside on the same computer.

  For Fix Pack 003, the steps in the configuration procedure that pertain to the portal server database have not changed. They are included here for completeness.
- The *Tivoli Data Warehouse database* stores long-term historical data (older than 24 hours) for presentation in historical data views. A portal server on Linux supports a warehouse database on either DB2 or Oracle. The warehouse database can reside on the same computer as the portal server or on a remote computer. The configuration procedures in this chapter include the steps for configuring a connection to a Tivoli Data Warehouse on Oracle only.

Configuring the portal server from the command line

To use the command line for configuring a Linux portal server to support a Tivoli Data Warehouse on Oracle, follow these steps:

1. Log on to the computer where the Tivoli Enterprise Portal Server is installed.
2. At the command line change to the *ITMinstall_dir*/bin directory, where *ITMinstall_dir* is the directory where you installed the product.
3. Run the following command to start configuring the Tivoli Enterprise Portal Server:

   ```
   ./itmcmd config -A cq
   ```

   where cq is the product code for the portal server.
4. Press Enter when you are asked if the agent connects to a monitoring server. (Although the prompt refers to an *agent*, this command is used to configure the portal server.)
5. Configure the connection between the portal server and the hub monitoring server:
   a. Type the host name for the hub monitoring server and press Enter.

b. Type the protocol that the hub monitoring server uses to communicate with the portal server. You have four choices: IP.UDP, SNA, IP.PIPE, or IP.SPIPE.
c. If you want to set up a backup protocol, enter that protocol and press Enter. If you do not want to use backup protocol, press Enter without specifying a protocol.
d. Depending on the type of protocol you specified, provide the following information when prompted:

Table 22. Hub monitoring server protocols and values

Protocol	Value	Definition
IP.UDP	IP Port Number	The port number for the monitoring server. The default is 1918.
SNA	Net Name	The SNA network identifier for your location.
	LU Name	The LU name for the monitoring server. This LU name corresponds to the Local LU Alias in your SNA communications software.
	Log Mode	The name of the LU6.2 LOGMODE. The default value is `CANCTDCS`.
IP.PIPE	IP.PIPE Port Number	The port number for the monitoring server. The default is 1918.
IP.SPIPE	IP.SPIPE Port Number	The port number for the monitoring server. The default is 3660.

e. Press Enter when you are asked if you want to configure the connection to a secondary monitoring server. The default value is no.
f. Press Enter to accept the default for the Optional Primary Network Name (none).
g. Press Enter to accept the default setting for SSL between the portal server and clients (`N`). By default, SSL is disabled. To enable SSL, type `y` and press Enter.

6. Configure the connection between the Tivoli Enterprise Portal Server and the Tivoli Enterprise Portal Server database:
   a. Type the DB2 instance name. The default value is `db2inst1`. Press Enter.
   b. Type the DB2 administrator ID. The default is `db2inst1`. Press Enter.

      Note: The DB2 Administrator account was created during DB2 installation.
   c. Type the password for the DB2 administrator ID and press Enter.
   d. Confirm the password for the DB2 administrator ID by typing it again. Press Enter.
   e. Type the name of the portal server database. The default is `TEPS`. Press Enter.
   f. Type the login name of the database user that the portal server will use to access the database. The default is `itmuser`. Press Enter.
   g. Type the password for the database user and press Enter.
   h. Confirm the password for the database user by typing it again. Press Enter.

i. You are asked if it is okay to create the DB2 login user if it does not exist. Type `y` and press Enter.

7. Configure the connection between the Tivoli Enterprise Portal Server and the Tivoli Data Warehouse database on Oracle:
   a. You are asked if you are using DB2 or Oracle for the Warehouse. The default is Oracle. Press Enter to accept the default.
   b. Type the name of the Tivoli Data Warehouse database. The default is `WAREHOUS`. Press Enter.
   c. Type the name of the Warehouse user. This is the user ID that the portal server will use to access the database. The default is `itmuser`. Press Enter.
   d. Type the password for the Warehouse user ID and press Enter.
   e. Confirm the password for the Warehouse user by typing it again. Press Enter.
   f. Type the full path name of the Oracle JDBC driver JAR file as follows:
      dir_path`/ojdbc14.jar`

      where *dir_path* is the full directory location of the JDBC driver JAR file on this computer. Press Enter.
   g. Type the following JDBC driver name and press Enter:
      `oracle.jdbc.driver.OracleDriver`
   h. Type the JDBC driver URL and press Enter. This is the Oracle-defined URL that identifies the locally or remotely installed Oracle instance used for the Tivoli Data Warehouse. The following entry is an example:
      `jdbc:oracle:thin:@localhost:1521:oracle`
   i. Type any user-defined attributes that are used to customize the behavior of the driver connection. Use semi-colons (;) to delimit the attributes. Press Enter to finish the configuration.

Configuring the portal server from the GUI

To use the GUI interface for configuring a Linux portal server to support a Tivoli Data Warehouse on Oracle, follow these steps:

1. Log on to the computer where the Tivoli Enterprise Portal Server is installed.
2. Start the Manage Tivoli Enterprise Monitoring Services utility:
   a. Change to the bin directory:
      `cd` *`install_dir`*`/bin`
   b. Run the following command:
      `./itmcmd manage [-h` *`ITMinstall_dir`*`]`

      where:

Table 23. Parameters for the itmcmd manage command

-h	(optional) An option used to specify the installation directory.
ITMinstall_dir	The directory where the portal server is installed. The default installation directory is /opt/IBM/ITM.

   The Manage Tivoli Enterprise Monitoring Services window is displayed.
3. Right-click **Tivoli Enterprise Portal Server** and click **Configure**.

The Configure Tivoli Enterprise Portal Server window is displayed.

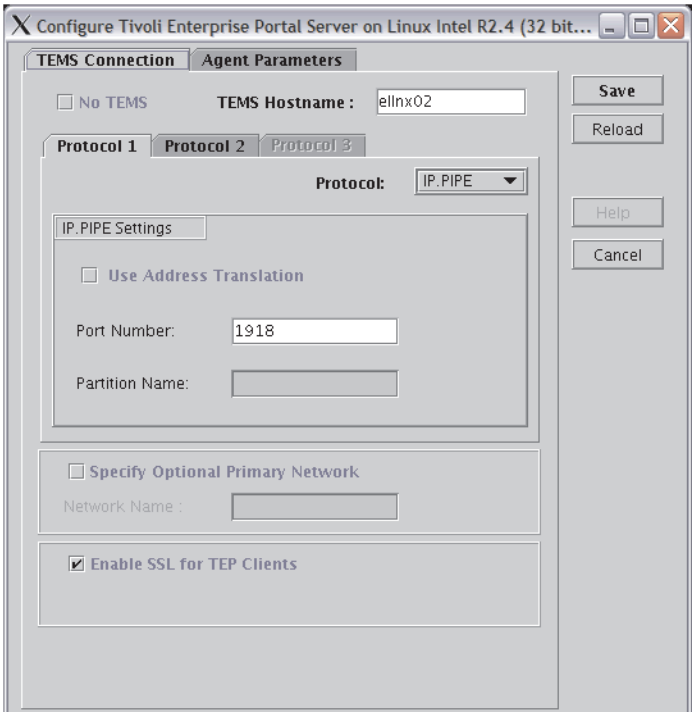


Figure 3. Registering the Linux portal server with the Tivoli Enterprise Monitoring Server

4. On the TEMS Connection page, enter information about the Tivoli Enterprise Monitoring Server to which the Tivoli Enterprise Portal Server connects:
   - Enter the host name of the monitoring server in the **TEMS Hostname** field. (If the field is not active, clear the **No TEMS** check box.)
   - Select the communications protocol that the monitoring server uses from the **Protocol** drop-down list.
     - If you select SNA, enter information in the **Net Name**, **LU Name**, and **LOG Mode** fields.
     - If you select IP.UDP, IP.PIPE, or IP.SPIPE, enter the port number of the monitoring server in the **Port Number** field.

     For information about these fields, refer to Table 22 on page 78.
5. Click the **Agent Parameters** tab.

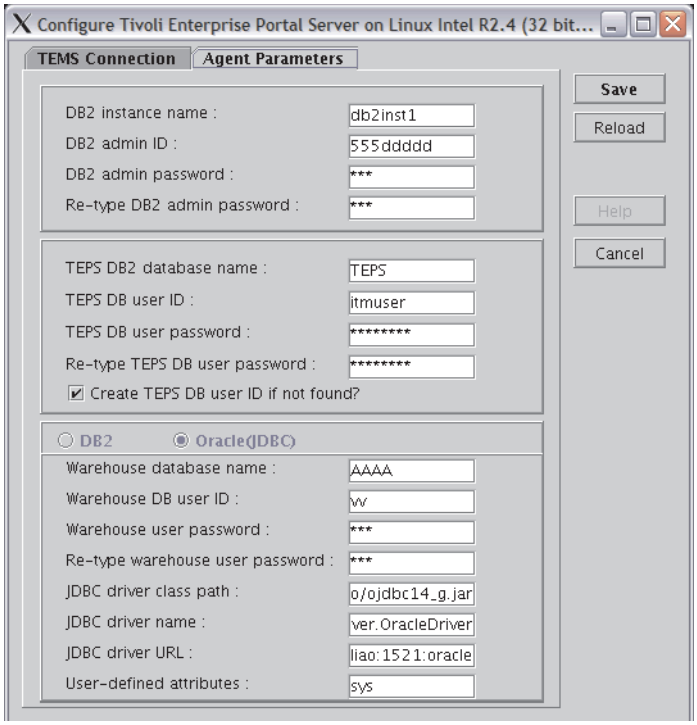


Figure 4. Configuring database connections for the portal server

6. Configure the connection between the Tivoli Enterprise Portal Server and the Tivoli Enterprise Portal Server database by entering information in the fields described in the following table:

Table 24. Configuration information for the Tivoli Enterprise Portal Server database

Field	Default value	Description
DB2 instance name	db2inst1	The DB2 instance name.
DB2 admin ID	db2inst1	The DB2 Administrator ID. The DB2 Administrator account was created during DB2 installation.
DB2 admin password	(no default)	The password for the DB2 Administrator ID.
Re-type DB2 admin password	(no default)	The password for the DB2 Administrator ID.
TEPS DB2 database name	TEPS	The Tivoli Enterprise Portal Server database name.
TEPS DB user ID	itmuser	The login name of the database user that the portal server will use to access the database.
TEPS DB user password	(no default)	The password for the database login user.
Re-type TEPS DB user password	(no default)	The password for the database login user.
Create TEPS DB user ID if not found?	yes	This check box is selected by default. If the database login account (user ID and password) that you specified in the preceding fields does not exist, it is created.

7. Select **Oracle (JDBC)** to configure a connection to a data warehouse on Oracle.

8. Configure the connection between the Tivoli Enterprise Portal Server and the Tivoli Data Warehouse database on Oracle by entering information in the fields described in the following table:

Table 25. Configuration information for the Tivoli Data Warehouse

Field	Default value	Description
Warehouse database name	WAREHOUS	The name of the Tivoli Data Warehouse database.
Warehouse DB user ID	itmuser	The database login user that the portal server uses to access the Tivoli Data Warehouse database.
Warehouse user password	(no default)	The password for the warehouse database user.
Re-type Warehouse user password	(no default)	The password for the warehouse database user.
JDBC driver class path	(no default)	Enter the full path name of the Oracle JDBC driver JAR file as follows: *dir_path*/ojdbc14.jar where *dir_path* is the full directory location of the JDBC driver JAR file on this computer.
JDBC driver name	(no default)	The JDBC driver name. Enter the following: oracle.jdbc.driver.OracleDriver
JDBC driver URL	(no default)	The Oracle-defined URL that identifies the locally or remotely installed Oracle instance used for the Tivoli Data Warehouse. The following entry is an example: jdbc:oracle:thin:@localhost:1521:oracle
User-defined attributes	(no default)	Enter any user-defined attributes that are used to customize the behavior of the driver connection. Use semi-colons (;) to delimit the attributes.

Chapter 8. Using the Tivoli Monitoring Services Discovery Library adapter

The Tivoli Monitoring Services Discovery Library adapter (DLA) scans the IBM Tivoli Monitoring environment and identifies the managed systems in the environment. You can then feed this information (an XML output file) into IBM Tivoli Change and Configuration Management Database or another CMDB. The DLA identifies all distributed and mainframe agents, as well as logical groupings defined through the Tivoli Enterprise Portal.

The DLA gathers information by querying the hub monitoring server for all managed systems and mapping them to Common Data Model resources based on the agent product code and managed system name format. For example, ″IMN1:SYS1:IMS″ is the managed system name for an OMEGAMON XE for IMS agent. The DLA discovers the following:

- A z/OS computer named ″IMN1″
- An IMS subsystem named ″SYS1″
- A relationship between the SYS1 z/OS computer and IMN1 IMS

For agents that use IP, IP.PIPE, or IP.SPIPE, the DLA can discover the IP address where the agent is running. The DLA also discovers the operating system for the computer where the agent is running, regardless of whether an OS monitoring agent is running on that computer.

The DLA also queries the Tivoli Enterprise Portal Server for information regarding logical groupings in the environment. For logical groupings, the following components are discovered:

- Logical views
- Aggregate objects
- Managed system objects

Note: The monitoring servers and portal server must be running for these queries. The managed systems can be running or not running.

The DLA is run from the command line on the computer where the portal server is installed. The command is located in the \IBM\ITM\CNPS subdirectory. Use the following command and syntax:

KfwTmsDla [/?] [/b] [/d] [/l] [/o *orgname***] [/s] [/x** *outputfile***]**

where:

/? Displays the syntax help information.

/b Open a browser with which to view the output of the adapter.

/d Creates a diagnostic file during the discovery process. You can use this file for debugging.

/l Indicates to discover logical views.

/o *orgname*
Sets the Organization GlobalName.

/s Indicates to discover HTTPS URL instead of HTTP URL.

/x *outputfile*
Indicates the name of the XML output file.

The following is a sample XML output file:

```
<cdm:app.db.db2.Db2Instance id="DB2:PTHTIV25:UD-Db2Instance"
              sourceToken="managed_system_name=DB2:PTHTIV25:UD&
                           object_id=p@DB2:PTHTIV25:UD">
     <cdm:Name>DB2<cdm:Name>
     <cdm:ManagedSystemName>DB2:PTHTIV25:UD<cdm:ManagedSystemName>
<cdm:app.db.db2.Db2Instance>

<cdm:runsOn source="DB2:PTHTIV25:UD-Db2Instance"
      target="pthtiv25.au.ibm.com-ComputerSystem" />
<cdm:monitors source="DB2:PTHTIV25:UD-TMSAgentô
        target="DB2:PTHTIV25:UD-Db2Instance" />
```

In the above sample, `DB2:PTHTIV25:UD` identifies the resource class and attributes of the managed system, while the information identified by `cdm:runsOn` and `cdm:monitors` identify the relationship.

By default, the DLA generates the XML output file in the \TMSDLA subdirectory on the portal server. The name of this file follows the standard Discovery Library file name format, such as TMSDISC100.systemA.ibm.com.2006-05-22T23.35.06Z.refresh.xml. To use this information in the CMDB, you must transfer the XML file to the Discovery Library File Store and then use the Discovery Library Bulk Loader.

In addition to discovering resources and relationships, the TMS DLA discovers information that the IBM Tivoli Change and Configuration Management Database uses to provide a context sensitive launch to the Tivoli Enterprise Portal. You can also view the status of the discovered managed systems while in IBM Tivoli Change and Configuration Management Database.

For more information about IBM Tivoli Change and Configuration Management Database, see the product information center at http://publib.boulder.ibm.com/infocenter/tivihelp/v10r1/index.jsp?toc=/com.ibm.ccmdb.doc/ccmdb_ic.xml.

Chapter 9. Using the secureMain utility

If you use a non-root user to initially install IBM Tivoli Monitoring on a Linux or UNIX computer, the file permissions for many files and directories are set to a very low level, 777. You can use the new secureMain utility to change these permissions.

Note: You do not need to be logged in as a root user to run this utility, but you are prompted for the root password when it is required.

The secureMain utility has the following syntax:

```
secureMain [-h install_dir] lock|unlock
```

where:

-h *install_dir*
The directory path for the IBM Tivoli Monitoring installation. If this parameter is not supplied, then the script attempts to determine the installation directory.

lock Tightens the directory tree permissions. The permissions are set to 750.

If certain products or components that require access by multiple user IDs are installed, a basic permission model of 755 is used. Some specific files and directories will still remain at 777 permissions.

unlock
Loosens the directory tree permissions.

Note that the **unlock** parameter does not restore permissions to exactly what they were before **secureMain lock** was run. It sets most files and directories back to 777 permissions but not all files and directories. Permissions on the common directories shared by applications, and on the server components (monitoring server, portal server, and portal client) are set to 777. Permissions on most application specific directories are not reset.

Chapter 10. Monitoring agent enhancements

Linux File and Directory monitoring

The Linux OS agent has added Linux File and Directory monitoring, file information attributes to refer to file information characteristics. The File Information workspace shows a list of files and directories on your file system. The default directory shown is the / directory.

To create a situation using attributes from this table for a directory, the situation must specify the fully qualified directory using the Path attribute. To create a situation using attributes from this table for a file, the situation must specify the fully qualified directory and file name, using both the Path and File attributes.

The following attributes have been added:

Attribute	Description
Access	The access rights of the file expressed as 4 digit octal number.
Group	The logical group to which the file belongs.
Last Accessed Time	The date and time of the last file access.
Last Changed Time	The date and time of the last change to a file.
Link Name	The name of the file for which this file is a symbolic link. If this field is blank, the file is not a link.
Links	The number of links to a file.
File Name	The name of file or directory. If the file is a symbolic link, the link name is shown in Link_Name attribute.
Path Name	The full path containing a particular file or directory.
Owner	The name of the file owner.
Path	The full path containing a particular file or directory.
Size MB	The size, in MB, of the file.
System Name	The managed system name of system being monitored.
Timestamp	The date and time the agent collects information as set on the monitored system.
Type	The type of file. Possible values are Dir (= directory), File (= file), Sock (= socket), Link (= Link), Spec (= Special file).

UNIX OS agent enhancements

The following new functions have been added to the UNIX OS agent:

- The UNIX OS agent adds support for AIX printer queue monitoring for AIX V5.1, V5.32, and V5.3 computers using the AIX Printing system. A table has been added to support the printer queue support.

  Note: System V printing is not supported and will return ″Not Collected″ (N/C) to the user.
- Megabytes and gigabytes were added for very large disk attributes currently represented using kilobytes.

To support these functions, a new table, UNXPRINTQ, has been added and the UNIXDISK has been modified.

UNXPRINTQ has the following attributes:

Attribute	Description
Print Queue Name	The name of the print queue.
Device Name	The name of a device associated with this queue.
Print Queue Status	The status of the print queue.
Print_Queue_Depth	The number of jobs in the print queue.
Total Size of Jobs in Queue	The number of kilobytes in the print queue, including copies.

UNIXDISK has the following attributes:

Attribute	Description
Size_MB	The total size of a file system, expressed in megabytes.
Size_GB	The total size of a file system, expressed in gigabytes.
Space_Used_MB	The amount of disk space currently in use on a file system, expressed in megabytes.
Space_Used_GB	The amount of disk space currently in use on a file system, expressed in gigabytes.
Space_Available_MB	The amount of disk space currently available to non-superusers on a file system, expressed in megabytes.
Space_Available_GB	The amount of disk space currently available to non-superusers on a file system, expressed in gigabytes.

Support for SSL communication with the i5/OS monitoring agent

Fix Pack 003 adds support for the i5/OS agent to communicate with the monitoring server using the SSL communication protocol.

In IBM Tivoli Monitoring, SSL communication is managed through the use of digital certificates. You have two options for managing certifications:

- iKeyman, a Java-based utility available as part of IBM iSeries Client Encryption licensed program. Key ring files to hold certificates can be created using the iKeyman GUI. Both Server and Client certificates can be created and stored in key ring files.
- Digital Certificate Manager (DCM), a free iSeries feature, to centrally manage certificates for applications. DCM enables managing certificates that are obtained from any Certificate Authority (CA). Also, you can use DCM to create and operate your own local CA to issue private certificates to applications and users in your organization.

Current SSL configuration does not use the key ring files on the i5/OS monitoring agent, unlike other OS monitoring agents. Instead, DCM is used to create a local certificate store, if it does not already exist on the system where i5/OS is installed. Local certificates are created in the certificate store. Certificates obtained from a 3rd party Certificate authority also can be imported to the local certificate store. Steps

provided below are for configuring the SSL for i5/OS agent using the Application Identifier to associate certificates to the i5/OS agent application and SSL services provided by iSeries.

The following procedure provides the high-level summary of the steps to configure this support:

1. Install the i5/OS agent on System i.
2. Open the Configure Tivoli Monitoring: i5/OS screen by running the **GO OMA** command and selecting Option 4.
3. Set the monitoring server DNS or IP address using the **TEMS IP.SPIPE Address** parameter.
4. Set the port number using the **TEMS IP.SPIPE Port Number** parameter. 3660 is the default port.
5. Configure the Certificate and Application ID using the steps in "Configuring DCM" on page 90.
6. Occasionally, agents might have connection problems on some V5R3 systems. In that case, set the KDEBE_PROTOCOL to SSL_VERSION_3 in QAUTOTMP/KMSPARM(KBBENV) file on System i. This is not necessary if i5/OS PTFs MF40084 and PTF MF39703 are installed.
7. Configure the monitoring server to communicate with the IP.SPIPE protocol on the port set in step 4. You can set this communication protocol in the Monitoring Tivoli Enterprise Monitoring Services utility.
8. Start the monitoring server and the i5/OS agent.

If there are connection problems, first configure the agent to communicate using the IP.PIPE protocol. If that is successful, then try with the SPIPE protocol.

If the agent does not connect, to troubleshoot the problem, set the agent trace as follows:

1. Add the line KDE_DEBUG=A somewhere in QAUTOTMP/KMSPARM(KBBENV)
2. Recycle the agent to generate more trace.
3. FTP the file QAUTOTMP/KA4AGENT01 to a PC and send to IBM Software Support.

Prerequisites

The documentation on the SSL and DCM are taken from the iSeries Information Center Web site. Refer to the iSeries documentation for more details on these topics. iSeries documentation can be obtained using the following link: http://publib.boulder.ibm.com/iseries/v5r2/ic2924/index.htm. Search for *DCM* or *SSL*.

The following are prerequisites for the SSL support on i5/OS:

- IBM Digital Certificate Manager (DCM), option 34 of OS/400 (5722-SS1)
- TCP/IP Connectivity Utilities for iSeries (5722-TC1)
- IBM HTTP Server for iSeries (5722-DG1)
- If you are trying to use the HTTP server to use the DCM, be sure you have the IBM Developer Kit for Java(TM) (5722-JV1) installed, or the HTTP admin server will not start.
- The IBM Cryptographic Access Provider product, 5722-AC3 (128-bit). The bit size for this product indicates the maximum size of the secret material within

the symmetric keys that can be used in cryptographic operations. The size allowed for a symmetric key is controlled by the export and import laws of each country. A higher bit size results in a more secure connection.

Optional: You might also want to install cryptographic hardware to use with SSL to speed up the SSL handshake processing. As of release V5R2M0, the following cryptographic hardware options are available to you, for use with your iSeries server:

- 2058 Cryptographic Accelerator (Hardware Feature code 4805)
- 4758 Cryptographic Coprocessor (Hardware Feature codes 4801 or 4802)

If you want to install cryptographic hardware, you must also install Option 35, the Cryptographic Service Provider.

Configuring DCM

The following sections provide the steps to configure DCM.

Starting DCM

Before you can use any of its functions, you need to start Digital Certificate Manager (DCM). Complete these tasks to ensure that you can start DCM successfully:

- Install 5722 SS1 Option 34. This is Digital Certificate Manager (DCM).
- Install 5722 DG1. This is the IBM HTTP Server for iSeries.
- Install 5722 AC3. This is the cryptography product that V5R2 DCM uses to generate a public-private key pair for certificates, to encrypt exported certificate files, and decrypt imported certificate files.

Use the following steps to start DCM:

1. Use the iSeries Navigator to start the HTTP Server *ADMIN instance:
   a. Start iSeries Navigator.
   b. Double-click your iSeries server in the main tree view.
   c. Double-click **Network**.
   d. Double-click **Servers**.
   e. Double-click **TCP/IP**.
   f. Right-click **HTTP Administration** and click **Start**.
2. Start your Web browser and go to the iSeries Tasks page on your system at http://*your_system_name*:2001.
3. Select **Digital Certificate Manager** from the list of products on the iSeries Tasks page to access the DCM feature.

Setting up certificates for the first time

The left frame of Digital Certificate Manager (DCM) is the task navigation frame. You can use this frame to select a wide variety of tasks for managing certificates and the applications that use them. Which tasks are available depends on which certificate store (if any) you have opened and your user profile authority. Most tasks are available only if you have *ALLOBJ and *SECADM special authorities.

When you use Digital Certificate Manager (DCM) for the first time, no certificate stores exist (unless you have migrated from a previous version of DCM). Consequently, the navigation frame displays only these tasks when you have the necessary authorities:

- Manage User Certificates.

- Create New Certificate Store.
- Create a Certificate Authority (CA). (Note: After you use this task to create a private CA, this task no longer appears in the list.)
- Manage CRL Locations.
- Manage PKIX Request Location.

Even if certificate stores already exist on your system (for example, you are migrating from an earlier version of DCM), DCM displays only a limited number of tasks or task categories in the left navigation frame. You must first access the appropriate certificate store before you can begin working with most certificate and application management tasks. To open a specific certificate store, click Select a Certificate Store in the navigation frame.

Certificates can be obtained using either public internet Certificate Authority (CA), such as VeriSign or certificates can issued from the local private Certificate Authority. The steps below primarily applicable to certificates issued using the local CA. iSeries or other documentation need to be considered for the steps to obtain certificates from public CA.

Creating a new certificate store

Perform the steps in this section if *SYSTEM certificate store does not exist already. This section should be skipped if *SYSTEM certificate store already created on the system. “Select Certificate Store” button in the task navigation frame can be used to verify if *SYSTEM certificate store already created or not. “*SYSTEM” will be listed if there is one already.

1. Click **Create New Certificate Store** in the task navigation frame.
2. Select ***SYSTEM** and click **Continue**.
3. Select **No – Do not create a certificate in the certificate store** and click **Continue**.
4. Provide the password and click **Continue**.
5. Click **OK** to complete the step.

Selecting the *SYSTEM certificate store

This step is prerequisite for performing the steps in the sections below.

1. Click **Select a Certificate Store** in the task navigation frame.
2. Choose ***SYSTEM** and click **Continue**.
3. Provide the password and click **Continue**.

A screen will be displayed indicating *SYSTEM as the current certificate store and also showing the **Certificate store path and filename**: `/QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KDB` (if the default certificate store path is chosen).

Authorizing QAUTOMON to use certificate store files

The i5/OS agent needs to be installed on the System i (iSeries) before completing this step. These steps require that the QAUTOMON user profile is available on the system for authorizing QAUTOMON to the certificate store files.

Authority on ’/qibm/userdata/icss/Cert/Server ’ directory: On System i 5120 session, run the following command:

```
wrklnk '/qibm/userdata/icss/Cert/Server'
```

If the certificate store files were created in a path other than the default, provide the correct path instead of the default used above.

Type 9 in the **Opt** field next to the directory **Server**. Option 9 is not displayed by default. Use `F23=More options` to display `9=Work with authority`.

In the next screen, type 1 in **Opt** field, `QAUTOMON` in **User** and `*RX` in the **Data Authority** fields. The screen will look like the following. Press Enter.

```
Data     --Object Authorities--
     Opt    User            Authority  Exist  Mgt  Alter  Ref
      1     QAUTOMON        *RX
            *PUBLIC         *EXCLUDE
            QSYS            *RWX         X     X     X     X
```

Perform the above steps for all the directories in the /qibm/userdata/icss/Cert path if *PUBLIC or QAUTOMON does not have *RX authority.

Authority on DEFAULT.KDB & DEFAULT.RDB files: On System i 5120 session, run the following command:

```
wrklnk '/qibm/userdata/icss/Cert/Server'
```

If the certificate store files were created in a path other than the default, provide the correct path instead of the default used above.

Two files DEFAULT.KDB, DEFAULT.RDB are listed. Perform the following steps for both files.

Type 9 in the **Opt** field next to the directory **Server**. Option 9 is not displayed by default. Use `F23=More options` to display `9=Work with authority`.

In the next screen, type 1 in **Opt** field, `QAUTOMON` in **User** and `*RW` in the **Data Authority** fields. The screen will look like the following. Press Enter.

```
Data     --Object Authorities--
      Opt     User              Authority  Exist  Mgt  Alter  Ref
        1     QAUTOMON          *RW
              *PUBLIC           *EXCLUDE
              QSYS              *RW          X     X     X     X
```

This step provides sufficient authority for QAUTOMON to access certificate store files.

Creating the local Certificate Authority

The steps below can be followed if Local Certificate Authority does not exist already. Use the Select Certificate Store task to verify if a local Certificate Authority exists. If one exists, **Local Certificate Authority (CA)** is listed.

1. Click **Create a Certificate Authority** in the task navigation frame.
2. Complete the following fields for the certificate and click **OK**.

Field	Value
Key size	1024
Certificate store password	Type the password for your certificate store. This field is required.
Confirm password	Type the password again.
Certificate Authority (CA) name	LOCAL_CERTIFICATE_AUTHORITY (1). This field is required.
Organization unit	
Organization name	Specify the company name. This field is required.

Field	Value
Locality or city	
State or province	Specify the state. This field is required.
Country or region	Specify the country. This field is required.
Validity period of Certificate Authority (CA) (2-7300)	1095 days

3. The next screen provides the option to install the certificate on your browser. This is an optional step and is not required for i5/OS. To install the certificate on your browser, click **Install Certificate**. Choose to **Open** or **Save** the certificate in local directory. If you choose to save the certificate, click on it after saving to open the certificate. Several screens are displayed to install the certificate.
4. Click **Continue** on the Install Local Certificate screen.
5. Click **Yes** for **Allow creation of user certificates** on the Certificate Authority (CA) Policy Data screen.
6. Click **Continue**.
7. Click **Continue** or **OK** on the next screen to complete the creation of local Certificate Authority.

Creating certificates using the local Certificate Authority

DCM provides a guided task path that can be used for creating a CA and using it to issue certificates to your applications. After clicking the button, a screen will be displayed with the list of Certificate Stores. Make sure *SYSTEM is the current certificate store. Use “Select a Certificate Store” button to select *SYSTEM certificate store.

1. Click **Create Certificate**.
2. Select **Server or Client Certificate**.
3. 3. Select **Local Certificate Authority**.
4. Enter the details for the certificate as listed below:

Certificate type	Server or client
Certificate store	*SYSTEM

5. Complete the form to create the certificate. Use the following values:

Field	Value
Key size	1024
Certificate label	IBM_Tivoli_Monitoring_Agent_Certificate
Common name	IBM Tivoli Monitoring Agent Self Signed Certificate
Organization unit	Type the organization name. This field is required.
Locality or city	
State or province	Type the state or province. This field is required.
Country or region	Type the country. This field is required.
IP version 4 address	

Field	Value
Fully qualified domain name (host_name.domain_name)	
E-mail address (user_name@domain_name)	

6. Click **Continue** and **OK** on the next screens. No need to choose any applications at this time.

This will complete the steps to create a Server or Client Certificate. You can view the details of the certification using the **View Certificate** task.

Creating an application ID

To create an application definition, follow these steps:

1. In DCM, click **Select a Certificate Store** and select the appropriate certificate store. (This should be *SYSTEM certificate store for creating SSL application definition for either a server application or client application.)
2. When the Certificate Store and Password page displays, provide the password that you specified for the certificate store when you created it and click **Continue**.
3. In the navigation frame, select **Manage Applications** to display a list of tasks.
4. Select **Add application** from the task list to display a form for defining the application.

   Note: If you are working in the *SYSTEM certificate store, DCM will prompt you to choose whether to add a server application definition or a client application definition. Choose to create Client application definition for this purpose.
5. Complete the form and click **Add**. The information that you can specify for the application definition varies based on the type of application that you are defining.

   Below are the current properties for the default Application ID created for IBM Tivoli Monitoring for the i5/OS agent.

Field	Default value
Application type	Client
Application ID	QIBM_ITM_KA4_AGENT
Exit program	CT_AGENT
Exit program library	QAUTOMON
Threadsafe	Yes
Multithread job action	Run program and send message
Application user profile	QAUTOMON
Define the CA trust list	Yes
Certificate revocation processing	No
Application description	ITM 6.1 Monitoring Agent for i5/OS Agent

Associating the certificate with the application ID

Use the following steps to associate the certificate with the application ID:

1. Click **Assign Certificate** under Manage Certificates in the task navigation frame.

2. Select the certificate from the list.
3. Click **Assign to Applications**.
4. Select the application definition you want to associate with the certificate and click **Continue**.

Defining the CA Trust list

Use the following steps to define the CA Trust list:

1. Click **Define CA Trust list** under **Manage Applications**.
2. Select **Client - Add or remove a Certificate Authority (CA) certificate from a client application CA trust list**.
3. Select **ITM 6.1 Monitoring Agent for i5/OS Agent** and click **Define CA Trust List**.
4. Click **Trust All** and click **OK**.

Configuring the i5/OS agent

Four new environment variables have been introduced for SSL configuration on the agent.

- KDEBE_APPLICATIONID
- KDC_PORTSSL
- IP_SPIPE
- KDEBE_PROTOCOL

You can set the KDEBE_OS400_APP_ID and KDEBE_PROTOCOL variables by editing the QAUTOTMP/KMSPARM(KBBENV) file. You can set the IP_PIPE and KDC_PORTSSL variables using the configuration screen provided using **GO OMA**, Option 4.

KDEBE_APPLICATIONID
: Required for identifying the Application Identifier used to establish the SSL communication handshake between the i5/OS agent and the monitoring server. The value for this variable depends on the Application Identifier name that is created using DCM. The default value is QIBM_ITM_KA4_AGENT for the i5/OS monitoring agent. If the default Application Identifier is not used, you must update the KDEBE_APPLICATIONID value in the KBBENV configuration file with the correct Application ID.

IP_SPIPE
: Used to store the monitoring server's SPIPE Address. This can be either the DNS name or IP address. This value can be set using the configuration screen available from the main menu (**GO OMA** Option 4). You do not need to edit the KBBENV environment variable file for this variable.

KDC_PORTSSL
: Used to store the monitoring server's SPIPE port number. This value can be set using the configuration screen available from the main menu (**GO OMA** Option 4). You do not need to edit the KBBENV environment variable file for this variable.

KDEBE_PROTOCOL
: Used to set the SSL Version protocol that the agent computer uses to connect to the monitoring server computer. If a monitoring agent on a V5R3 computer fails to connect to the monitoring server, set the **KDEBE_PROTOCOL=SSL_VERSION_3** variable to circumvent connection problems using SPIPE configuration.

KDEBE_PROTOCOL has the following characteristics:

- KDEBE_PROTOCOL=SSL_VERSION_3 (SSL 3 only). This causes an override of the available cipher suites to preclude the use of AES and to circumvent the i5/OS defects of AES not tolerated in cipher suite. This circumvents the connection problems on V5R3 systems.

  System i PTFs for SSL Layer (PTF MF40084, PTF MF39703), available in August of 2006, will fix these defects. These PTFs are installed on the V5R3 system, KDEBE_PROTOCOL can be set to SSL_VERSION_CURRENT to take advantage of all the ciphers supported.
- KDEBE_PROTOCOL=SSL_VERSION_CURRENT (TLS with SSL 3 and 2 compatibility)
- KDEBE_PROTOCOL=SSL_VERSION_2 (SSL 2, not recommended, weak) KDEBE_PROTOCOL=TLSV1_SSLV3 (TLS with SSL 3 compatibility)

Chapter 11. Installing and configuring multiple Warehouse Proxy agents

Fix Pack 003 introduces support for multiple warehouse proxies within a single hub monitoring server environment. The provision for multiple warehouse proxies provides for greater scalability and performance in historical data collection.

About multiple Warehouse Proxy support

The support for multiple warehouse proxies has the following important features:

- All Warehouse Proxy agents within a single hub monitoring server environment export data to a single Tivoli Data Warehouse.
- Each Warehouse Proxy agent is associated with a subset of monitoring server instances that you specify when you configure the proxy agent. Each warehouse proxy exports data only for monitoring agents that report to one of the monitoring servers on the specified list.

The following sequence of events explains how the monitoring agents, which collect the data for historical reports, know which Warehouse Proxy agent to use:

1. When a Warehouse Proxy agent starts, it registers with the global location broker on the hub monitoring server, sending it the list of monitoring servers that it is configured to serve. This registration process is repeated every hour.
2. Each monitoring server queries the global location broker at regular intervals to determine which warehouse proxy it is associated with. The monitoring server then sends the address of this warehouse proxy to all of its child monitoring agents to use during historical data exports. You can change the default query interval of 60 minutes to some other value.

When a Warehouse Proxy agent registers with the global location broker, it is registered as the default proxy agent if no other proxy agent is already configured as the default. When a monitoring server queries the global location broker for its associated warehouse proxy, the default proxy agent is used if that monitoring server is not on the list of servers for any proxy agent.

Installing and configuring the proxy agents

Use the following procedure to install and configure each Warehouse Proxy agent:

1. Install each proxy agent using the procedures described in the *IBM Tivoli Monitoring V6.1 Installation and Setup Guide*. To set up a proxy agent on AIX or Linux, see Chapter 6, "Installing and configuring the Warehouse Proxy on AIX and Linux," on page 69.

   The procedure for installing a proxy agent into an environment with multiple proxy agents is the same as the procedure for installing a single proxy agent.
2. Associate each proxy agent with the list of monitoring servers that you want the proxy agent to serve:
   a. Open the environment file for the proxy agent:
      - (Windows) *ITMinstall_dir*\TMAITM6\KHDENV
      - (Linux) *ITMinstall_dir*/config/hd.ini

      where *ITMinstall_dir* is the directory where you installed the product.

b. Add the environment variable KHD_WAREHOUSE_TEMS_LIST to the file and set it to specify a space-delimited list of monitoring server instance names. For example:

```
KHD_WAREHOUSE_TEMS_LIST=REMOTE_TEMS1 REMOTE_TEMS2
```

The name of a monitoring server is specified when the server is installed. The default name of a monitoring server is HUB_*host_name* (for a hub monitoring server) or REMOTE_*host_name* (for a remote monitoring server), where *host_name* is the short host name.

3. Optionally modify the interval at which a monitoring server queries the global location broker to find out which warehouse proxy it is associated with:
   a. Open the environment file for the monitoring server:
      - (Windows) *ITMinstall_dir*\CMS\KBBENV
      - (UNIX or Linux) *ITMinstall_dir*/config/ms.ini

      where *ITMinstall_dir* is the directory where you installed the product.
   b. Change the following entry to specify a different query interval:

```
KPX_WAREHOUSE_REGCHK=60
```

      The query interval is specified in minutes. The default value is 60 minutes.
4. Start the Warehouse Proxy agent:
   - To start a Warehouse Proxy agent on Windows or Linux from the Manage Tivoli Enterprise Services window, right-click **Warehouse Proxy** and select **Start**.
   - To start a Warehouse Proxy agent on Linux from the command line, enter the following command:

```
./itmcmd agent start hd
```

     where `hd` is the product code for the Warehouse Proxy agent.

Verifying the configuration

Use the following trace settings to verify the configuration:

- To verify that a warehouse proxy is registering with the hub monitoring server and placing the correct entries into the global location broker:
  1. Open the environment file for the proxy agent:
     - (Windows) *ITMinstall_dir*\TMAITM6\KHDENV
     - (Linux) *ITMinstall_dir*/config/hd.ini

     where *ITMinstall_dir* is the directory where you installed the product.
  2. Add the following entry to the KBB_RAS1 trace setting:

```
KBB_RAS1=ERROR(UNIT:khdxrpcr STATE)
```

     This setting prints the value of KHD_WAREHOUSE_TEMS_LIST and shows any errors associated with its components.
- To determine which warehouse proxy a particular monitoring server uses for its agents:
  1. Open the environment file for the monitoring server:
     - (Windows) *ITMinstall_dir*\CMS\KBBENV
     - (UNIX or Linux) *ITMinstall_dir*/config/ms.ini

     where *ITMinstall_dir* is the directory where you installed the product.
  2. Add the following entry to the KBB_RAS1 trace setting:

```
KBB_RAS1=ERROR(UNIT:kprwhpx STATE)
```

This setting prints entries in the RAS log of the monitoring server when a registration change occurs. The entry specifies the name and address of the new Warehouse Proxy agent that the monitoring server is using.

Chapter 12. New tacmd commands

The following commands have been added to IBM Tivoli Monitoring.

Table 26. New tacmd commands

Command name	Description
"tacmd createsystemlist" on page 102	Creates a new managed system list.
"tacmd deletesystemlist" on page 104	Deletes an existing managed system list.
"tacmd editsystemlist" on page 105	Edits a managed system list.
"tacmd exportWorkspaces" on page 107	Exports a workspace.
"tacmd importWorkspaces" on page 110	Imports a workspace.
"tacmd listsystemlist" on page 112	Lists all existing managed system lists.
"tacmd listWorkspaces" on page 113	Lists workspaces available to export.
"tacmd viewsystemlist" on page 115	Displays a managed system list.

tacmd createsystemlist

Description

This command creates a new managed system list.

CLI syntax

tacmd createsystemlist {-l|--list} *listname*
{-m|--system} *system ...*
[{-t|--type} *type***]**

tacmd createsystemlist {-l|--list} *listname*
{-b|--basedOn} *baselistname*
[{-m|--system} *system ...***]**

tacmd createsystemlist {-i|--import} *filename*

where:

-l|--list *listname*
Name of the new managed system list to be created. Specify a string of letters (upper or lower case), numbers, or underscores (_) up to a maximum length of 32 characters.

-m|--system *system ...*
Name or names of the managed systems. Specify a string of letters (upper or lower case), numbers, underscores (_), colons (:), or periods (.). This parameter is required when specifying -t|--type and is optional when specifying -b|--basedOn.

-b|--basedOn *baselistname*
Name of the managed system list on which on which to base the new system list. The new system list is identical to the base system list except the name (LISTNAME) and any systems that are specifically changed. Specify a string of letters (upper or lower case), numbers, underscores (_), or asterisks (*). This parameter is mutually exclusive with -t|--type.

-i|--import *filename*
Import the system list definition. Specify the name of a readable file containing a valid system list definition.

-t|--type *type*
The type of the new system list. Specify a string for the managed system type name or its associated 2 character code. The string may consist of letters (upper or lower case), numbers, underscores (_), slashes (/), left parenthesis "(", right parenthesis ")", or spaces ( ). If not specified, a type of "All Managed Systems" is used. This parameter is mutually exclusive with -b|--basedOn.

CLI example

This example creates a system list testList1 on the server HUB_HDCHASDSTC0420.

```
tacmd createsystemlist -l testList1 -t NT
                       -m Primary:HDCHASDSTC0420:NT HUB_HDCHASDSTC0420
```

Return values

See “Return codes” on page 116.

Related commands

“tacmd editsystemlist” on page 105

“tacmd deletesystemlist” on page 104

“tacmd viewsystemlist” on page 115

“tacmd listsystemlist” on page 112

tacmd deletesystemlist

Description

This command deletes the specified managed system list.

CLI syntax

tacmd deletesystemlist {-l|--list} *listname*
[{-f|--force}]

where:

-l|--list *listname*
Name of the managed system list to be deleted. Specify a string of letters (upper or lower case), numbers, or underscores (_) up to a maximum length of 32 characters.

-f|--force
Do not confirm with the user the managed system list to be deleted. If not specified, the user will prompted for confirmation.

CLI example

This example deletes the managed system list testList1 after prompting the user.

```
tacmd deletesystemlist –l testList1
```

Return values

See “Return codes” on page 116.

Related commands

“tacmd createsystemlist” on page 102

“tacmd editsystemlist” on page 105

“tacmd viewsystemlist” on page 115

“tacmd listsystemlist” on page 112

tacmd editsystemlist

Description

This command is used to add or delete managed systems to or from an existing managed system list on the server. It can also be used to edit (add or delete system list names to/from) an existing managed system list in a file.

CLI syntax

tacmd editsystemlist **{-l|--list}** *listname*
{[{-a|--add} *system ...*] **[{-d|--delete}** *system ...*]}
[{-f|--force}]

tacmd editsystemlist **{-e|--edit}** *filename*
{[{-a|--add} *system ...*] **[{-d|--delete}** *system ...*]}

where:

-l|--list *listname*
Name of the managed system list to be edited. Specify a string of letters (upper or lower case), numbers, or underscores (_) up to a maximum length of 32 characters.

-a|--add *system ...*
Name or names of the managed systems to be added to the managed system list. Specify a string of letters (upper or lower case), numbers, underscores (_), colons (:), or periods (.). Note that at least one of -a|--add or -d|--delete must be specified and both may be used in the same command invocation.

-d|--delete *system ...*
Name or names of the managed systems to be deleted from the managed system list. Specify a string of letters (upper or lower case), numbers, underscores (_), colons (:), or periods (.). Note that at least one of -a|--add or -d|--delete must be specified and both may be used in the same command invocation.

-e|--edit *filename*
Name of the managed system list file to be edited. Specify a valid file name consisting of letters (upper or lower case), numbers, underscores (_), colons (:), periods (.), slashes (/), back slashes (\), or tildes (~).

-f|--force
Do not confirm with the user the managed systems to be added or deleted. If not specified, the user will prompted for confirmation.

CLI example

This example updates the managed system list testList1 on server HDCHASDSTC0422.

```
tacmd editsystemlist -l testList1 -a Primary:HDCHASDSTC0422:NT -f
```

This example updates the managed system list definition file sys200.xml by both adding and entry and deleting entries.

```
tacmd editsystemlist -e sys200.xml
                     -a Primary:HDCHASDSTC0420:NT hdchasdstc0420ASFSdp:UAGENT00
                     -d HDCHASDSTC0420:Warehouse
```

Return values

See “Return codes” on page 116.

Related commands

“tacmd createsystemlist” on page 102

“tacmd deletesystemlist” on page 104

“tacmd viewsystemlist” on page 115

“tacmd listsystemlist” on page 112

tacmd exportWorkspaces

Description

This command exports one or more Tivoli Enterprise Portal Server workspaces to the file *xml_file*.

Notes:

1. When you export a workspace from one portal server and import it to another, the data might appear differently than it did on the first agent. This is related to the context for the portal server. If the environment for the second portal server is different in any way from that of the first portal server, the data varies accordingly.
2. Exporting and importing workspaces have the following known limitations:
   - When you export a workspace from one portal server and import it to another, custom queries and situations are not exported.
   - When you export a workspace from one portal server to another (for example from a test environment to a production environment), that workspace will not be available from the logical view in the new portal server unless you have the exact same navigator items in the view. You cannot create these items manually but must instead migrate them from one environment to another.

   For more information, see Chapter 3, “Known problems and limitations,” on page 53.

CLI syntax

tacmd exportWorkspaces **{-x|--xmlFile}** *xml_file*
[{-s|--server} *host***[:***port***]]**
[{-u|--username} *teps_user***]**
[{-p|--password} *pwd***]**
[{-w|--workspace} *workspace ...***]**
[{-r|--workspaceUser} *userid ...***]**
[{-t|--type} *type ...***]**
[{-f|--force}]

where:

-x|--xmlFile *xml_file*
The name of the XML file accessible to the local file system where the workspace definition or definitions will be exported to. This is the name of a file that can be created or overwritten.

-s|--server *host***[:***port***]**
Specifies a Tivoli Enterprise Portal Server to use. The *host* is a 32 or 64 bit IP address or hostname and *port* is an integer between 1 and 65536. If not specified, *host* defaults to localhost and *port* defaults to 1920.

-u|--username *teps_user*
The identifier of the user to authenticate on the remote Tivoli Enterprise Portal Server. Specify a string valid in the local locale.

Attention: The user must have both ″Workspace Administration Mode″ and ″Workspace Author Mode″ Workspace Administrator permissions enables on the server to run this command. The ″Workspace Administration Mode″ permission is disabled by default for most users.

-p | --password *pwd*
The password of the user to authenticate on the remote Tivoli Enterprise Portal Server. Specify a string valid in the local locale.

-w | --workspace *workspace ...*
The name or names of the workspaces to export. Specify a string (any character except hyphen (-)) up to a maximum length of 72 characters. If not specified, all workspaces will be exported. If the name of the workspace includes spaces, use quotation marks (either single or double) around the name.

-r | --workspaceUser *userid ...*
A Tivoli Enterprise Portal user ID that one or more Tivoli Enterprise Portal workspaces are associated with. Specify a string of letters (upper or lower case) or numbers up to a maximum length of 32 characters. If not specified, workspaces are exported for all users.

-t | --type *type ...*
An IBM Tivoli Monitoring 6.1 application type. Specify a 2 or 3 character string for the managed system type code. If a 2 character type is entered, the letter 'k' will be prefixed automatically to form a 3 character type code. If not specified, all types are exported.

-f | --force
Perform the export without prompting for confirmation first.

CLI example

This example exports all workspaces on the Tivoli Enterprise Portal Server myteps.ibm.com without any filtering arguments (such as workspace name, user ID, or application type).

Note: A large number (over 500) of workspaces may be displayed and exported.

```
tacmd exportWorkspaces –s http://myteps.ibm.com:1920 –u imasample
                       –p mypassword -x all_workspaces.xml
```

This example exports all workspaces on the Tivoli Enterprise Portal Server myteps.ibm.com without any filtering arguments (such as workspace name, user ID, or application type). The **-f** option is used in this example to perform the export operation without prompting for confirmation.

Note: A large number (over 500) of workspaces are likely be exported.

```
tacmd exportWorkspaces –s http://myteps.ibm.com –u imasample
                       –p mypassword -x all_workspaces.xml -f
```

This example exports all workspaces belonging to the *klz* and *knt* application types on the Tivoli Enterprise Portal Server running on the local machine on port 1920 and filtered by application type.

```
tacmd exportWorkspaces –u imasample –p mypassword –t klz knt
                       -x klz_and_knt_workspaces.xml
```

This example is identical to the one above, except that the server credentials (username and password) were omitted at invocation time, and the user is interactively prompted to enter them.

```
tacmd exportWorkspaces –s myteps.ibm.com –t klz knt
```

This example exports all workspaces belonging to (customized for) the *SYSADMIN* user on the Tivoli Enterprise Portal Server myteps.ibm.com and filtered by user name.

Note: In this example no global workspaces are exported.

```
tacmd exportWorkspaces –s myteps.ibm.com –u imasample –p mypassword –r SYSADMIN
```

This example exports only workspaces matching the names *Historical Summarized Availability Daily* or *Historical Summarized Availability Weekly* on the Tivoli Enterprise Portal Server myteps.ibm.com and filtered by workspace name.

```
tacmd exportWorkspaces –s myteps.ibm.com –u imasample –p mypassword
      –w "Historical Summarized Availability Daily"
         "Historical Summarized Availability Weekly"
```

This example exports only workspaces belonging to the *klz* and *knt* application types, workspace names matching the names *Historical Summarized Availability Daily* or *Historical Summarized Availability Weekly* on the Tivoli Enterprise Portal Server myteps.ibm.com, and filtered by both workspace name and application type.

```
tacmd exportWorkspaces –s myteps.ibm.com –u imasample –p mypassword –t klz kux
–w "Historical Summarized Availability Daily"
       "Historical Summarized Availability Weekly"
```

Return values

See “Return codes” on page 116.

Related commands

“tacmd listWorkspaces” on page 113

“tacmd importWorkspaces” on page 110

tacmd importWorkspaces

Description

This command is used to import the workspace or workspaces contained in the file *xml_file* into the Tivoli Enterprise Portal Server.

Notes:

1. When you export a workspace from one agent and import it to another, the data might appear differently than it did on the first agent. This is related to the context for the agent. If the environment for the second agent is different in any way from that of the first agent, the data varies accordingly.
2. Exporting and importing workspaces have the following known limitations:
   - When you export a workspace from one portal server and import it to another, custom queries and situations are not exported.
   - When you export a workspace from one portal server to another (for example from a test environment to a production environment), that workspace will not be available from the logical view in the new portal server unless you have the exact same navigator items in the view. You cannot create these items manually but must instead migrate them from one environment to another.

   For more information, see Chapter 3, "Known problems and limitations," on page 53.

CLI syntax

tacmd importWorkspaces **{-x|--xmlFile}** *xml_file*
[{-s|--server} *host***[:***port***]]**
[{-u|--username} *teps_user***]**
[{-p|--password} *pwd***]**
[{-f|--force}]

where:

-x|--xmlFile *xml_file*
The name of an XML file containing one or more workspace definitions that conform to the workspace XML schema. The file must be accessible by the local file system.

-s|--server *host***[:***port***]**
Specifies a Tivoli Enterprise Portal Server to use. The *host* is a 32 or 64 bit IP address or hostname and *port* is an integer between 1 and 65536. If not specified, *host* defaults to localhost and *port* defaults to 1920.

-u|--username *teps_user*
The name of the user to authenticate on the remote Tivoli Enterprise Portal Server. Specify a string valid in the local locale.

Attention: The user must have both ″Workspace Administration Mode″ and ″Workspace Author Mode″ Workspace Administrator permissions enables on the server to run this command. The ″Workspace Administration Mode″ permission is disabled by default for most users.

-p|--password *pwd*
The password of the user to authenticate on the remote Tivoli Enterprise Portal Server. Specify a string valid in the local locale.

-f|--force
Perform the import without prompting for confirmation first.

CLI example

This example imports workspaces from the file all_lever_workspaces.xml to the server located at myteps.ibm.com.

```
tacmd importWorkspaces –s myteps.ibm.com –u imasample
                       –p mypassword –x all_lever_workspaces.xml
```

This example is the same scenario as above, except that the force flag is used to suppress confirmation prompts.

```
tacmd importWorkspaces –s myteps.ibm.com –u imasample
                       –p mypassword –x all_lever_workspaces.xml -f
```

This example imports workspaces from the file all_lever_workspaces.xml to the server located at myteps.ibm.com on port 1996. The user will be prompted to enter the server username and password.

```
tacmd importWorkspaces –s http://myteps.ibm.com:1996 –x all_lever_workspaces.xml
```

Return values

See “Return codes” on page 116.

Related commands

“tacmd listWorkspaces” on page 113

“tacmd exportWorkspaces” on page 107

tacmd listsystemlist

Description

This command lists the available managed system lists. You can filter for a specified managed system type or for a list of specified managed system types.

CLI syntax

tacmd listsystemlist [{-d | --delim} *delim*]
[{-t | --type | --types} *type ...*]

where:

-d | --delim *delim*
Use this string to separate the fields. You can specify a delimiter character of a comma (,), colon (:), semicolon (;), asterisk (*), number (#), dollar ($), exclamation (!), or tilde (~). If not specified, use one or more tabs to separate the columns so they line up.

-t | --type | --types *type ...*
One or more managed system types. Specify a string for the managed system type name or its associated 2 character code. The string may consist of letters (upper or lower case), numbers, underscores (_), slashes (/), left parenthesis "(", right parenthesis ")", or spaces ( ). If not specified, list all the managed system lists available.

CLI example

This example lists the manages system list catalog.

```
tacmd listsystemlist
```

Return values

See "Return codes" on page 116.

Related commands

"tacmd createsystemlist" on page 102

"tacmd editsystemlist" on page 105

"tacmd deletesystemlist" on page 104

"tacmd viewsystemlist" on page 115

tacmd listWorkspaces

Description

This command displays a list of the Tivoli Enterprise Portal Server workspaces on the server. The workspace name, product code, and user ID is displayed for each workspace. You can optionally filter the list by workspace names, product codes, or workspace users.

CLI syntax

tacmd listWorkspaces [{-s|--server} *host*[**:***port*]**]**
[{-u|--username} *teps_user*]
[{-p|--password} *pwd*]
[{-w|--workspace} *workspace ...*]
[{-t|--type} *type ...*]
[{-r|--workspaceUser} *user ...*]

where:

-s|--server *host*[**:***port*]
Specifies a Tivoli Enterprise Portal Server to use. The *host* is a 32 or 64 bit IP address or hostname and *port* is an integer between 1 and 65536. If not specified, *host* defaults to localhost and *port* defaults to 1920.

-u|--username *teps_user*
The name of the user to authenticate on the remote Tivoli Enterprise Portal Server. Specify a string valid in the local locale.

Attention: The user must have both ″Workspace Administration Mode″ and ″Workspace Author Mode″ Workspace Administrator permissions enables on the server to run this command. The ″Workspace Administration Mode″ permission is disabled by default for most users.

-p|--password *pwd*
The password of the user to authenticate on the remote Tivoli Enterprise Portal Server. Specify a string valid in the local locale.

-w|--workspace *workspace ...*
The name or names of the workspaces to list. Specify a string (any character except hyphen (-)) up to a maximum length of 72 characters. If not specified, all workspaces will be displayed. If the name of the workspace includes spaces, use quotation marks (either single or double) around the name.

-t|--type *type ...*
An IBM Tivoli Monitoring 6.1 application type. Specify a 2 or 3 character string for the managed system type code. If a 2 character type is entered, the letter ‘k’ will be prefixed automatically to form a 3 character type code. If not specified, all types are displayed.

-r|--workspaceUser *user ...*
A Tivoli Enterprise Portal user ID that one or more Tivoli Enterprise Portal workspaces are associated with. Specify a string of letters (upper or lower case) or numbers up to a maximum length of 32 characters. If not specified, workspaces are displayed for all users.

CLI example

This example displays all workspaces on the Tivoli Enterprise Portal Server myteps.ibm.com without any filtering arguments (such as workspace name, user ID, or application type).

Note: A large number (over 500) of results are likely to be displayed.

```
tacmd listWorkspaces –s myteps.ibm.com –u imasample –p mypassword
```

This example displays all workspaces belonging to the *klz* and *knt* application types on the Tivoli Enterprise Portal Server running on the local machine on port 1920 and filtered by application type.

```
tacmd listWorkspaces –u imasample –p mypassword –t klz knt
```

This example is identical to the one above, except that the portal server credentials (username and password) were omitted at invocation time, and the user is interactively prompted to enter them.

```
tacmd listWorkspaces –t klz knt
```

This example displays all workspaces belonging to the *SYSADMIN* user on the Tivoli Enterprise Portal Server myteps.ibm.com and filtered by user name.

Note: In this example no *global* workspaces are displayed.

```
tacmd listWorkspaces –s http://myteps.ibm.com –u imasample –p mypassword
                     –r SYSADMIN
```

This example displays only workspaces matching the names *Historical Summarized Availability Daily* or *Historical Summarized Availability Weekly* on the Tivoli Enterprise Portal Server myteps.ibm.com and filtered by workspace name.

```
tacmd listWorkspaces –s myteps.ibm.com –u imasample –p mypassword
                     –w "Historical Summarized Availability Daily"
                        "Historical Summarized Availability Weekly"
```

This example displays only workspaces belonging to the *klz* and *knt* application types, workspace names matching the names *Historical Summarized Availability Daily* or *Historical Summarized Availability Weekly* on the Tivoli Enterprise Portal Server myteps.ibm.com on port 1996, and filtered by both workspace name and application type.

```
tacmd listWorkspaces –s myteps.ibm.com:1996 –u imasample –p mypassword –t klz kux
                  –w "Historical Summarized Availability Daily"
                         "Historical Summarized Availability Weekly"
```

Return values

See “Return codes” on page 116.

Related commands

“tacmd importWorkspaces” on page 110

“tacmd exportWorkspaces” on page 107

tacmd viewsystemlist

Description

This command displays the configuration of a managed system list or saves it in an export file.

CLI syntax

tacmd viewsystemlist {-l|--list } *listname*
[{-e|--export} [*filename***]]**

where:

-l|--list *listname*
Name of the managed system list to be viewed or exported. Specify a string of letters (upper or lower case), numbers, underscores (_), or asterisks (*) up to a maximum length of 32 characters.

-e|--export *filename*
Export the managed system list definition to the specified export stream (file). The name of a file can be created or overwritten. If *filename* is not specified, the manage system list will be redirected to the standard output stream.

CLI example

This example displays the details of one of the catalog entries.

```
tacmd viewsystemlist –l Test_All_Managed_Systems
```

This example displays the details of a new manages system list.

```
tacmd viewsystemlist –l testList1
```

This example exports the managed system list testList1 to the specified file apache_httpd.xml.

```
tacmd viewsystemlist –l testList1 –e apache_httpd.xml
```

Return values

See “Return codes” on page 116.

Related commands

“tacmd createsystemlist” on page 102

“tacmd editsystemlist” on page 105

“tacmd deletesystemlist” on page 104

“tacmd listsystemlist” on page 112

Return codes

The following table lists the return codes for the **tacmd** commands.

Table 27. Return Codes for tacmd CLI commands

Code	Category	Description
0	Success	Indicates that the command was successful.
1	Syntax Error or Help	Indicates either that the help command was given or that the syntax used was incorrect.
2	No Permission	Indicates that the user does not have permission to issue the command.
3	Version Mismatch	Indicates that the version of the server is not what was expected.
4	Communication Error	Indicates that an error occurred in the communications with the server.
5	Timeout	Indicates that an operation waiting for data did not receive it within the time it was expected.
6	Input Error	Indicates that the input to the command was not what was expected.
7	Server Exception	Indicates that an error occurred on the server that caused the command to fail.
8	Command Error	Indicates that an internal error occurred while executing the command.
9	Invalid Object	Indicates that a specified object does not exist.

Appendix A. Detailed installation procedures for installing the component fix packs

The following sections provide detailed instructions for installing the component fix packs. Use these sections in conjunction with the installation checklists to complete your installation.

Installing the 6.1.0-TIV-ITM_INST-FP0003 fix pack

Run the following command to install the 6.1.0-TIV-ITM_INST-FP0003 fix pack on all monitoring components:

On Windows, run:

```
cd patch_dir
install_kui.bat
```

where *patch_dir* is the directory where you extracted the fix pack files.

On UNIX or Linux, run:

```
cd patch_dir
./install_kui.sh
```

Installing fix packs using the itmpatch command

Run the following command to install the component fix packs:

```
itmpatch -h ITMinstall_dir -i patch_file
```

where *ITMinstall_dir* is the location where IBM Tivoli Monitoring is installed and *patch_file* is the name and location of the fix pack.

You can also use the **itmpatch** command to generate a report that identifies the actions a fix pack will take. Run the following command to preview a fix pack:

```
itmpatch -h ITMinstall_dir -t patch_file
```

The following example installs the 6.1.0-TIV-ITM_TEMS-FP0003 fix pack on a Windows monitoring server:

```
itmpatch.exe -h c:\ibm\itm -i c:\temp\6.1.0-TIV-ITM_TEMS-FP0003
```

For additional information about the **itmpatch** command, including other parameters for the command, see Appendix B, “Using the fix pack installer,” on page 123.

Installing application support

Use the following steps to install the application support on the monitoring server, portal server, and portal desktop client. Application support files include the situations, policies, and workspaces for an agent. Application support files are located in a subdirectory of the agent fix pack package.

1. Download and extract the agent fix pack file (the 6.1.0-TIV-ITM_*platform*-FP003.tar file, where *platform* identifies the specific operating system, such as ″UNIX″) for each OS agent in your environment

This creates a directory structure that contains fix packs for all of the supported operating systems.

2. Extract the compressed files that contain the application support files for each fix pack. Look for a file named *"pc__tems_teps_tepd_fp0003.tar,"* where *pc* is "k" plus the 2-letter product code for the agent. For example, the file for the UNIX OS agent is kux_tems_teps_tepd_fp0003.tar.

   Note: Extract the application support files for each OS agent to a unique directory; otherwise, files from the different agents will over-write each other.

3. Start the Application Support Installer GUI to install the fix pack. Run the following command from within the fix pack CD-ROM directory:

   ```
   java -jar setup.jar
   ```

   Note that you need to either have the IBM Java JRE v1.4.2 in your path or invoke the JRE executable directly by specifying the path to it on the command line. So, instead of the above command, you'd run:

   ```
   Java_installDir\java -jar setup.jar
   ```

   Note: To determine the location of the JRE on a UNIX computer, run the following command:

   ```
   which java
   ```

   This returns the install location for the Java JRE.

   To ensure that the level of JRE is 1.4.2, run the following command from the directory where the JRE is installed:

   ```
   java -version
   ```

   If it is not 1.4.2, you must download the IBM Java JRE v1.4.2 from the IBM Software Support Web site.

4. Click **Next** on the Welcome window.
5. Type the location where IBM Tivoli Monitoring is installed on your monitoring server. For Windows computers, this location is detected automatically. For UNIX computers, either type the location in or click **Browse** to find the directory.
6. Type the location where the support files that you want to install are located. When you extract the downloaded file, the following directory structure is created:

   CD-ROM
   TEMS
   TEPS
   TEPD
   product.properties

   Type the path to the CD-ROM directory.
7. Click **Next**. A list of applications for which support can be installed is displayed.
8. Select component on which you want to install support (monitoring server, portal server, or portal desktop client) and click **Next**.
9. Select the applications for which you want to install application support and click **Next**.

10. If you are trying to install application support for a component that you have already installed support for, a warning window is displayed. You can choose to continue by simply clicking **Next**. The existing installed support files are overwritten.

    If you do not want to overwrite your existing application files, clear the box next to the application and click **Next**. The application support files for this application are not installed.
11. Review the summary of what is going to be installed and click **Next**.

    This summary tells you what is going to happen to your computer during the installation, such as starting, stopping, and restarting the monitoring server as application support for each application is installed.

    A progress window is displayed to show the installation progress.

    Note: If you are trying to install support for more than one component (monitoring server, portal server, or portal desktop client) and the support files are already installed, you get a warning for each component, enabling you to select which components you want to re-install support for.
12. When the installation is complete, click **Finish.**
13. Exit and then restart any portal clients (desktop or browser).

Using a response file to install the application support files

You can install the application support files on the IBM Tivoli Monitoring components through the silent install method using a response file.

Note: If your UNIX or Linux computer does not have X-Windows, you must use the silent installation method.

Performing a silent install involves the following three steps:

1. "Creating a response file"
2. "Running the silent installation" on page 120
3. "Examining the installation log file" on page 120

Creating a response file

Create a text file called response.txt that contains the following lines:

```
# IBM Tivoli Monitoring installation directory
-W Directories.itmhome="/opt/ibm"

# Directory where the application support media is located
-W Directories.mediaLocation="/opt/appsupport"

# Select "true" to install monitoring server support files
-W ComponentSelectionPanel.temsSelected="true"

# Select "true" to install portal server support files
-W ComponentSelectionPanel.tepsSelected="true"

# Select "true" to install portal desktop client support files
-W ComponentSelectionPanel.tepdSelected="true"

# Comma-separated list of directories with the application media location to
# install. These are directories that contain the product support files and
# are sub-directories under the specified media location
-W ProductSelectionPanel.products="kqf-v1.0,kqc-v1.0"

# Set this flag to "true" if you want to re-install if the
# specified product is already installed.  This overwrites
```

```
# any previously installed support files for this product.
-W ProductSelectionPanel.reinstall="true"

# Setting this flag to "true" confirms that you have purchased
# an OMEGAMON DE license.  If any product requires a DE LICENSE
# and this flag is "false" installation will fail
-W ProductSelectionPanel.deLicense="false"
```

Running the silent installation

Run the installation from the command-line interface by running the following command:

```
java -jar setup.jar -silent -options response.txt
```

Examining the installation log file

The log file, named ITM_AppSupport_Install.log, is written to the /tmp directory on Linux and UNIX computers and on Windows, in the directory defined by the TEMP environment variable. Review the contents of this file to determine if the installation succeeded.

Adding fix packs to the agent depot

You can remotely deploy the following fix packs:

- 6.1.0-TIV-ITM_INST-FP0003 -- IBM Tivoli Monitoring Global-common Component
- 6.1.0-TIV-ITM_TEMA-FP0003 -- ITM Shared Libraries
- 6.1.0-TIV-ITM_i5OS-FP0003 – i5/OS OS Agent (A4)
- 6.1.0-TIV-ITM_LINUX-FP003 – Linux OS monitoring agent (LZ)
- 6.1.0-TIV-ITM_UA-FP0003 -- Universal Agent (UM)
- 6.1.0-TIV-ITM_UNIX-FP0003 -- UNIX OS monitoring agent (UX)
- 6.1.0-TIV-ITM_UXLOG-FP0003 – UNIX Log Agent (UL)

Run the following command from the fix pack directory to add the fix packs to the agent depot on the monitoring server:

ITMinstall_dir/bin/tacmd addBundles -i *patch_file* -n

where *ITMinstall_dir* is the directory where you installed IBM Tivoli Monitoring and *patch_file* is the location of the fix pack.

Repeat this step for each agent fix pack.

For example, to add the 6.1.0-TIV-ITM_TEMA-FP0003 fix pack to the depot, run the following command:

ITMinstall_dir/bin/tacmd addBundles -i D:\FP2_IMAGES\6.1.0-TIV-ITM_TEMA-FP0003 -n

For additional information about the **tacmd addbundles** command, see the *IBM Tivoli Monitoring Installation and Setup Guide*.

Deploying fix packs to remote agents

Run the following command from the monitoring server to remotely deploy the agent fix packs (which you previously added to the agent depot):

ITMinstall_dir/bin/tacmd updateAgent -t *pc* -n *node_name*

where:

pc Indicates the two-letter product code for the agent (such as ″UM″ for the Universal Agent)

node_name
Indicates the name of the computer and OS agent to which you want to deploy the update. For example, ″Primary:*host_name*:NT″ is the node name for a Windows OS agent. You can use the **tacmd listSystems** command to determine the node name.

Repeat this step on each agent in your environment for each agent fix pack you want to deploy.

Note: If you have a large number of monitoring agents to which to deploy updates, consider using the itmpatchagents script, available as a sample from the IBM Tivoli Open Process Automation Library (http://www-18.lotus.com/wps/portal/topal). This script enables the automatic deployment of updates across your monitoring environment.

Appendix B. Using the fix pack installer

The fix pack installer runs as a standalone command-line interface (CLI) that you can run locally or remotely using the remote deployment function. The fix pack installer performs the following functions:

- Determines the set of products that are running in your environment so that it can restart products that might have been stopped to apply a fix pack
- Preserves file permissions when a fix pack updates files
- Delivers cumulative interim fix packs
- Installs agent components such as Java Runtime Environments and Global Security Kit (GSKit, which is used for Secure Socket Layer TCP/IP connections using public key encryption/decryption methodologies)
- Installs agent fix packs locally
- Can be used with remote deployment to remotely install agent fix packs

The Patch Installer creates and maintains a file called patches.hist, which is located in the *ITMinstall_dir*/patchlogs directory, that records each fix pack installation attempt. This file includes the following information:

- Which fix packs were installed
- Which components were fix packs installed against
- The date and time the fix pack was installed
- If the fix pack installation was successful or aborted because of an error.

Important: Each line in the patches.hist file corresponds to a fix pack installation attempt. This file is not rolled back and must never be deleted.

The **itmpatch** command has the following syntax:

itmpatch -h *ITMinstall_dir* **{-i | -t} {** *patch_file_directory* **|** *patch_file* **}**

where:

-h *ITMinstall_dir*
Defines the installation directory for IBM Tivoli Monitoring.

-i Specifies the path to the directory or fix pack file to be installed.

-t Generates a report of the actions that will be performed by the fix pack. This option does *not* install the fix pack. Use this option to preview the fix pack.

The following example creates a report about a fix pack on a UNIX computer:

```
ITMinstall_dir/bin/itmpatch -h ITMinstall_dir -t $PATCH
```

The following example installs a fix pack on a Windows computer:

```
itmpatch.exe -h %CANDLE_HOME% -i %PATCH%
```

Appendix C. 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.

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.

Trademarks

IBM, the IBM logo, AIX, DB2, i5/OS, iSeries, OMEGAMON, OS/400, pSeries, Tivoli, the Tivoli logo, Tivoli Enterprise, Tivoli Enterprise Console®, z/OS, and zSeries are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

Intel is a trademark of Intel Corporation in the United States, other countries, or both.

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

Microsoft is a registered trademark 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.

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

Printed in USA