IBM TS7650G with ProtecTIER
Version 3 Release 4

Software Upgrade Guide V3.4.3

SC27-3643-12

Note:

Before you use this information and the product it supports, read the information in the *Safety and Environmental Notices publication, SC27-4622* and "Notices" sections of this publication.

This edition applies to ProtecTIER version 3.4.3 of the TS7650G ProtecTIER Deduplication Gateway and to all subsequent releases and modifications until otherwise indicated in new editions. This edition replaces SC27-3643-11.

Contents

Figures

Tables

About this guide

This document provides information to customers for upgrading and configuring the ProtecTIER® V3.4.3 software on 3958 DD4, 3958 DD5, and 3958 DD6 servers.

Who should use this guide

This information is intended for use by IBM® customers to upgrade the ProtecTIER V3.4.3 software.

The tasks for upgrading the ProtecTIER software to V3.4.3 are to be done by the customer.

Getting information, help, and service

If you need help, service, technical assistance, or want more information about IBM products, you can find various sources to assist you. You can view the following websites to get information about IBM products and services and to find the latest technical information and support.

- IBM (ibm.com®)
- IBM Support Portal (www.ibm.com/storage/support)
- IBM Directory of Worldwide Contacts (www.ibm.com/planetwide)

Before you call for service

Some problems can be solved without outside assistance, by using the online help, by looking in the online or printed documentation that comes with the TS7650G, or by consulting the support web page. Be sure to also read the information in any README files and release notes that come with the product.

Getting help by telephone

With the original purchase of the IBM System Storage® TS7600 with ProtecTIER, you have access to extensive support coverage. During the product warranty period, you can call the IBM Support Center (1 800 426-7378 in the U.S.) for product assistance covered under the terms of the hardware IBM warranty or the software maintenance contract that comes with product purchase.

Have the following information ready when you call:

- Either machine type and model or software identifier. The software identifier can be either the product name (TS7650 or TS7650G) or the Product Identification (PID) number.
- Either the serial numbers of the components or your proof of purchase.
- Description of the problem.
- Exact wording of any error messages.
- Hardware and software configuration information

If possible, have access to your computer when you call.

In the U.S. and Canada, these services are available 24 hours a day, 7 days a week. In the U.K., these services are available Monday through Friday, from 9:00 a.m. to 6:00 p.m. In all other countries, contact your IBM reseller or IBM marketing representative.

Remote support through Call Home

Remote support is available for the TS7650G through the Call Home capability provided either in the ProtecTIER software or with TSSC. Please note that TSSC with the Call Home feature is not available on the 3958 DD6 server; however, Call Home is supported for 3958 DD6 using native call home tools provided in the ProtecTIER software. The Call Home feature reports failures detected by the ProtecTIER servers. Whenever a failure is detected, Call Home sends detailed error information to IBM (*home*). The IBM Service Representative can then prepare an action plan to handle the problem before traveling to the affected installation. The gateway might also periodically send support information (such as configuration, code versions, and error logs) to IBM. Doing so speeds-up problem determination and fault resolution. When enabled on the gateway, Call Home uses a connection on your Ethernet network to transmit hardware and software problem reports to IBM. Call Home is enabled and tested by IBM Service Representatives during initial system installation.

When the Reliability, Availability, and Serviceability (RAS) software on the ProtecTIER server detects an error condition, Call Home sends detailed error information to IBM (*home*). If the error indicates a problem with a field replaceable unit (FRU), an IBM Service Representative can then prepare an action plan to handle the problem before traveling to your site.

The TS7650Gprovides four Call Home capabilities: Problem Call Home, Heartbeat Call Home, Test Call Home, and User-Initiated Call Home; descriptions follow. RAS sends data files that may be helpful to IBM Support Center personnel for all four types of Call Home. These data files include error logs and configuration information, such as the Machine Reported Product Data (MRPD) log.

Test Call Home
: The IBM Service Representative sends a Test Call Home signal after enabling the Call Home feature during initial installation. You can also send a Test Call Home to ensure that the setup is correct and that the gateway can successfully open a Problem Management Record (PMR) in the IBM Remote Technical Assistance Information Network (RETAIN).

Problem Call Home
: When RAS detects a problem, RAS initiates a Call Home operation to create a PMR in RETAIN. The PMR is a single page of text data that enables the Support Center or the Service Representative to access an action plan and a list of applicable FRU components.

Heartbeat Call Home
: To ensure proper ongoing Call Home functionality, the system sends a Heartbeat Call Home on a regularly-scheduled basis. The heartbeat interval is user-defined.

User-Initiated Call Home
: You can manually initiate Call Home from the TSSC GUI to collect a product engineering (PE) package.

For more information about Electronic Customer Care (ECC) and TSSC, refer to the following topics:

- "Call Home through ECC"
- "Call Home through the TSSC"

Call Home through ECC

Electronic Customer Care (ECC) is an integrated service tool that provides automation of error reporting utilizing the Call Home feature.

Electronic Customer Care is provided as a native tool of ProtecTIER software.

Table 1 presents the capabilities of remote support with a ECC.

Table 1. Remote support capabilities through ECC

Customer site	Call Home events	• Error initiated • Heartbeat (regular interval) • Test
	Support capability	• Error-initiated problem reporting for up to 43 subsystems • Staged, error-specific data gathering • Subsystem and system console heartbeat reporting • Wellness checking • Log file storage (daily) • Code image and documentation repository (from media and RETAIN Fix Distribution Library)
	Remote support service tools	• Code image broadcast • Call home event log review • End-of-call completion report
IBM support	Remote access	• Authenticated, secure remote access • Simultaneous call in and call home • Data transmission (TCP/IP) supported
	IBM call home database	• 24/7 access by IBM support staff • Error analysis and search capability

Call Home through the TSSC

The TSSC is a service tool that **must** be present in an IBM-supported 3958 DD4 or 3958 DD5 TS7650G server. You can either order a TSSC with your appliance or gateway, or use a TSSC already installed at your site.

Note: Please note that TSSC with the Call Home feature is not available on the 3958 DD6 server; Call Home is supported for 3958 DD6 using native call home tools provided in the ProtecTIER software.

Attention: While it is possible to operate a 3958 DD4 or 3958 DD5 without a connected TSSC, note that IBM **does not support** this configuration.

For the TS7650G, FC 2722 provides a new TSSC, while FC 2714 and FC 2715 allow connection of an existing TSSC. For more information on these feature codes, see the *IBM TS7650G ProtecTIER Deduplication Gateway Introduction and Planning Guide*, GA32-0918.

Table 2 presents the capabilities of remote support with a TSSC.

Table 2. Remote support capabilities with a TSSC

Customer site	Call Home events	• Error initiated • Heartbeat (regular interval) • Test
	TSSC support capability	• Error-initiated problem reporting for up to 43 subsystems • Staged, error-specific data gathering • Subsystem and system console heartbeat reporting • Wellness checking • Log file storage (daily) • Code image and documentation repository (from media and RETAIN Fix Distribution Library)
	TSSC and remote support service tools	• Code image broadcast • Call home event log review • End-of-call completion report
IBM support	TSSC remote access	• Authenticated, secure remote access • Simultaneous call in and call home • Data transmission (TCP/IP) supported
	IBM call home database	• 24/7 access by IBM support staff • Error analysis and search capability

Ordering publications

The IBM Publications Center is a worldwide central repository for IBM product publications and marketing material.

The IBM Publications Center (www.ibm.com/shop/publications/order/) offers customized search functions to help you find the publications that you need. Some publications are available for you to view or download at no charge. You can also order publications. The publications center displays prices in your local currency.

Terminology used in this topic

Provides a list of terms used in this document.

TS7650G or Gateway

These are terms for IBM's virtualization solution from the TS7650 family that does not include a disk storage repository, allowing the customer to choose from a variety of storage options. The TS7650G consists of the following:

Server There are five types of server that have been used in the Gateway. The following are the currently supported servers:

3958 DD6

This is a high performance server available since March 2016. The enclosure, or chassis, has space for two controller nodes in the rear, which accommodates a two-node cluster

configuration in a 2u platform and eliminates the external cluster connection kit. In the front, the 3958 DD6 contains 24 SAS drive slots (only 2 of which actually contain SAS drives). The remaining 22 slots are unused by ProtecTIER, do not have any function, and are filled with dummy carriers. The 3958 DD6 also includes redundant power supplies in the rear of the unit.

3958 DD5
This server, which first shipped in May 2012, is based on the IBM System x7143 model. When used as a server in the TS7650G, its machine type and model are 3958 DD5. Use this machine type and model for service purposes.

3958 DD4
This server became available in December 2010 and is based on the IBM System x3850 X5 Type 7145-PBR. When used as a server in the TS7650G, its machine type and model are 3958 DD4. Use this machine type and model for service purposes.

System console
The system console is a TS3000 System Console (TSSC). This document uses the terms *system console* and *TSSC* interchangeably. The TSSC is not available (and does not work) with the 3958 DD6.

Under IBM best practices, the TS7650G also contains the following:

Disk controller
The customer must choose the disk controller for use with the TS7650G. A list of TS7650 compatible controllers can be generated at the IBM System Storage Interoperation Center.

Disk expansion unit
The customer must choose the disk expansion unit for use with the TS7650G. A list of TS7650 compatible expansion units can be generated at the IBM System Storage Interoperation Center.

IBM Tivoli Assist On-site (AOS)
IBM Tivoli Assist On-site (AOS) is a web-based tool that enables a remote support representative in IBM to view or control the management node desktop. More information is located at the Tivoli AOS website.

TS7650
When used alone, this term signifies IBM's family of virtualization solutions that operate on the ProtecTIER platform.

replication
A process that transfers logical objects like cartridges from one ProtecTIER repository to another. The replication function allows ProtecTIER deployment to be distributed across sites. Each site has a single or clustered ProtecTIER environment. Each ProtecTIER environment has at least one ProtecTIER server. The ProtecTIER server that is a part of the replication grid has one or two dedicated replication ports that are used for replication. Replication ports are connected to the customer's WAN and are configured on two subnets as default.

replication grid
A set of repositories that share a common ID and can potentially transmit

and receive logical objects through replication. A replication grid defines a set of ProtecTIER repositories and actions between them. It is configured by using the ProtecTIER Replication Manager. The ProtecTIER Replication Manager is a software component installed on a ProtecTIER server or a dedicated host. The ProtecTIER Replication Manager should be able to recognize all of the members of the entire network that it handles on both replication subnets. The ProtecTIER Replication Manager manages the configuration of multiple replication grids in an organization. An agent on every node in each ProtecTIER server interacts with the server and maintains a table of its grid members.

Note: Customers must license the Replication features on all ProtecTIER systems participating in the replication grid whether the system is sending or receiving data (or both).

replication grid ID
A number from 0 to 63 that identifies a replication grid within an organization.

replication grid member
A repository that is a member in a replication grid.

replication pairs
Two repositories within a replication grid that replicate from one to another.

replication policy
A policy made up of rules that define a set of objects (for example, VTL cartridges) from a source repository to be replicated to a target repository.

repository unique ID (RID)
A number that uniquely identifies the repository. The RID is created from the replication grid ID and the repository internal ID in the grid.

replication timeframe
A scheduled period of time for replication to take place for all policies.

shelf A container of VTL cartridges within a ProtecTIER repository.

virtual tape library (VTL)
The ProtecTIER virtual tape library (VTL) service emulates traditional tape libraries. By emulating tape libraries, ProtecTIER VTL allows you to switch to disk backup without replacing your entire backup environment. Your existing backup application can access virtual robots to move virtual cartridges between virtual slots and drives. The backup application perceives that the data is being stored on cartridges while ProtecTIER actually stores data on a deduplicated disk repository.

visibility switching
The automated process that transfers the visibility of a VTL cartridge from its master to its replica and vice versa. The visibility switching process is triggered by moving a cartridge to the source library Import/Export (I/E) slot. The cartridge will then disappear from the I/E slot and appear at the destination library's I/E slot. To move the cartridge back to the source library, the cartridge must be ejected to the shelf from the destination library. The cartridge will then disappear from the destination library and reappear at the source I/E slot.

server and node
This document uses the terms server and node, interchangeably.

destination and target
This document uses the terms destination and target, interchangeably.

Sending your comments

Your feedback is important in helping IBM provide you with the most accurate and highest quality information.

Procedure

To submit any comments about this publication or any other IBM System Storage TS7600 with ProtecTIER documentation:

- Use the feedback form (http://pic.dhe.ibm.com/infocenter/strhosts/ic/topic/com.ibm.help.strghosts.doc/icfeedback.htm), or
- Send your comments by email to starpubs@us.ibm.com.

What to do next

For either approach, include the following information:

- The publication title and version.
- The publication form number (for example, GC27-3920-02).
- The page, table, or illustration numbers that you are commenting on.
- A detailed description of any information that you would like changed.

Chapter 1. Overview

This document provides instructions for upgrading servers that are running any ProtecTIER version 3.4.x to the latest available of ProtecTIER 3.4 branch. This document also provides instructions for upgrading servers that are running ProtecIER version 3.3.x to the latest available version of ProtecTIER 3.4 branch.

The following is an overview of the steps that might be required to upgrade the ProtecTIER software. Depending on the current status of the ProtecTIER server, you may not need to do all these steps.

- Detaching the TSSC microcode when replacing 3958 DD4 or 3958 DD5 servers with a 3958 DD6 server. See Chapter 2, “Detaching the TSSC,” on page 3.
- Configuring Electronic customer care (ECC) for 3958 DD6 servers. See “Call Home through ECC” on page xi.
- Reimaging the TSSC microcode, if needed. See Chapter 3, “Reimaging the TSSC microcode,” on page 5.
- Upgrading the version of ProtecTIER Manager to version 3.4, on theProtecTIER Manager workstation. See Chapter 4, “Upgrading ProtecTIER Manager,” on page 13.
- Upgrading to Red Hat Linux version 5.11 and ProtecTIER 3.4.x if the server is at ProtecTIER version 3.3.x. SeeChapter 8, “Upgrading Red Hat Linux and ProtecTIER version 3.4.x for servers at version 3.3.x,” on page 31.
- Upgrading ProtecTIER to 3.3.x if the server is at version 3.1.8, or higher. See Chapter 6, “Upgrading the ProtecTIER software to 3.3.x from version 3.1.8 or higher using ProtecTIER Manager,” on page 27.
- Downloading and installing the most current patch update version of ProtecTIER on servers currently running ProtecTIER 3.4.x. See Chapter 9, “Applying fix packs for ProtecTIER systems already at version 3.4,” on page 43.
- For instructions on upgrading ProtecTIER servers running a ProtecTIER version lower than 3.1.8, please refer to a previous version of the IBM TS7650 with ProtecTIER Software Upgrade Guide.

These instructions involve stopping services several times. Read the instructions carefully so you start and stop the services at the appropriate time in the process. Failure to stop the services correctly can result in unnecessary fencing.

If the code upgrade fails, you are directed to go to Chapter 10, “Recovering from a failed upgrade,” on page 51. The topic provides information to troubleshooting your problem and what action to take to resolve the problem.

This document *does not* address the following topics:

- Installation of new 3958 DD6 hardware. Refer to the *IBM TS7650G ProtecTIER Deduplication Gateway Installation Roadmap Guide*, GA32-0921
- Configuration and setup of any recommended hardware components that were not included in the purchase of the TS7650G. Components such as the disk controller and disk expansion modules must be configured and operational before installation of the TS7650G.
- Hardware or software troubleshooting. Refer to the *IBM Problem Determination and Service Guide for the TS7650G ProtecTIER Deduplication Gateway*, GA32-0923.

- Daily use and ongoing maintenance of the ProtecTIER, ProtecTIER Manager, and ProtecTIER Replication Manager, software. Refer to the *IBM ProtecTIER User's Guide for VTL Systems*, GA32-0922.

Notes:

- Upgrading to version 3.4 ProtecTIER software is supported on the existing 3958 DD4 and 3958 DD5 servers.
- Existing 3958 DD3 servers need to be replaced in order to run ProtecTIER V3.4. 3958 DD3 servers support a temporary upgrade for server replacement only. Refer to the*iRPQ 8B3667 Server Replacement 3958 DD3 with 3958 DD6 PN 00VJ479, EC M13702A* for information on replacing 3958 DD3 servers.

Important: A USB keyboard and graphics-capable monitor are required to complete the upgrade. These items are not provided in the ship group; they must be provided by the customer.

Chapter 2. Detaching the TSSC

Before you begin

Important:

1. If you have a ProtecTIER environment with replication you should first use the ProtecTIER Replication Manager to make a Backup before you start the upgrade.
2. You should first upgrade the Hub and then upgrade the spoke or spokes.
3. The ProtecTIER V3.4 release does not support attachment to the TSSC feature on the 3958 DD6 server. Therefore, TSSC must be detached from 3958 DD4 and 3958 DD5 prior to replacing them with the 3958 DD6 system. The 3958 DD4 and 3958 DD5 systems continue to support attachment to the TSSC for the V3.4 ProtecTIER release.

About this task

To detach the TSSC microcode during server upgrade to 3958 DD6, do the following:

Procedure

1. Move the black power switch on the KVM switch to OFF.
2. On the TSSC, press the black power pushbutton on the TSSC display panel. Then, press the white power pushbutton on the front of the TSSC.
3. Power off the server by pressing the white, recessed power-control pushbutton on the server operator panel.

   Note: In a clustered configuration, turn off the top server (Server B) first, wait 30 seconds, and then turn off the bottom server (Server A).
4. Disconnect the cables for the KVM switch and TSSC.

Chapter 3. Reimaging the TSSC microcode

Before you begin

Note: The ProtecTIER V3.4 and above do not support attachment to the TSSC feature on the 3958 DD6 server. The 3958 DD4 and 3958 DD5 systems continue to support attachment to the TSSC for the V3.4 ProtecTIER release.

To ensure compatibility with ProtecTIER 3.4.x, the TSSC must be running microcode version 8.2.14 or higher. A code load and hard disk drive rebuild is necessary to bring the TSSC up to the current level. Use the following instructions to determine the TSSC code version and if an upgrade to the TSSC code is required.

You can have a minimum TSSC code level of 5.12.x installed before you start the upgrade of the ProtecTIER code to 3.4.x. It is better, however, to upgrade the TSSC code to 8.2.14 before you start.

Checking the current version of TSSC microcode

Procedure

Use the following procedure to check the current microcode level:

1. If necessary, power on the TSSC.
2. Go to the **TS3000 System Console Login** screen.

   The code version of the TSSC is displayed at the top of the screen.
3. Take note of the version number. If the current TSSC code level is lower than 8.2.14, contact IBM to schedule an appointment for the microcode reimage.

   Note: Wait until the IBM service representative reimages the microcode on the TSSC before you upgrade the version of ProtecTIER on your servers. Ensuring that you have the current microcode image prevents version incompatibility errors during the ProtecTIER upgrade. The IBM Service Representative uses the following procedure, “Reimaging the TSSC microcode” on page 7.

Reimaging the TSSC microcode

About this task

Attention: Task for IBM Service Personnel

- Use this procedure only if the TSSC code level is lower than 5.11.5.
- There are two discs for reimaging the TSSC microcode - *Product Recovery CD IBM TS3000 System Console Disc 1* and *Product Recovery CD IBM TS3000 System Console Disc 2*
- Rebuilding the TSSC hard disk drive permanently deletes any local data present on the drive. Using the *Product Recovery CD IBM TS3000 System Console Disc 1* and *Product Recovery CD IBM TS3000 System Console Disc 2* returns the console to its "default" state.
- After you complete the following procedure, you need to reload any application software that is specific to the products displayed in the Attached Systems list. Examples of specific products include the TS7650, TS7740, or attached control units. For example, you might have to reload the Storage Manager GUIs, ProtecTIER Manager GUI, and Information Centers for TS7650. The actual applications depend on the systems that are attached to the TSSC. Refer to the *IBM TS3000 System Console (TSSC) Maintenance Information* for additional information. The backup menu option on the TSSC does not back up any of the applications that are mentioned here, only configuration data specific to the TSSC and the physically attached systems.
- Do not load or attempt to use the *Product Recovery CD IBM TS3000 System Console Disc 1* and *Product Recovery CD IBM TS3000 System Console Disc 2* on any machine type other than 4252, 6579, 6792, 7946, 8480, 8482, 8485, 8836, 8849, or 2583. If you use the *Product Recovery CD IBM TS3000 System Console Disc 1* and *Product Recovery CD IBM TS3000 System Console Disc 2* on any other machine type, the installation fails and that machine is unusable.
- Do not attempt to restore configuration settings from a v1.x.x TSSC console onto a v3.x.x or higher console. The files are incompatible. Version 2.x.x files are compatible with v3.x.x or higher.

Procedure

1. Back up the TSSC console configuration.

   Refer to the related topics in the *IBM TS3000 System Console (TSSC) Maintenance Information* (on the *IBM TS7650 with ProtecTIER Publications* CD) for detailed instructions for backing up and restoring configuration data. When the backup completes, a message appears that it was successful or that it failed. Ensure the backup successfully completed before you proceed to the reimageing step, or the data might be unrecoverable.

   Note: For the backup operation, it is useful to have an available USB flash memory drive or key for the configuration backup. It does not overwrite all data on the key. It adds the backup as a file only, so existing flash drive data is not be affected by adding the TSSC backup.
2. Insert the *Product Recovery CD IBM TS3000 System Console Disc 1* CD into the TSSC CD-ROM drive.
3. If you are currently logged in to the TSSC, right-click on the TSSC blue desktop.

   The **IBM TS3000 System Console** menu appears.
4. Select **Logout**, then click **OK**.

   You are returned to the login screen.

5. Click **Restart** in the lower-left area of the screen, and then click **OK** when prompted to restart.

   After the restart completes, the following message appears:

   ```
   TSSC Not Installed. Proceed. . .
   This will install the Console onto /dev/sda which will erase everything
   on that device
   Continue? ('yes' or 'no')
   Abort
   ```

6. Type: `y` and press Enter.

   The hard disk drive reimage process begins.

7. When you are prompted, remove disc 1 and insert disc 2.
8. When the reimage is complete, the TSSC restarts automatically and the CD is ejected from the CD-ROM drive.
9. After the initial start up, the software discovers the machine type and model number of the computer, and automatically configures the appropriate drivers and settings. The TSSC is then automatically restarted a second time. During the second restart, the start background and text might look slightly different. The second restart displays a login screen. If the software determines that the machine type is not 4252, 6579, 6792, 7946, 8480, 8482, 8485, 8836, or 8849, or 2583 a warning message appears on the screen and the TSSC stops. This continues each time the TSSC is powered on. Similar symptoms occur after software installation if the TSSC is unable to determine its machine type and model.

   Note: If a product with a machine type of 4252, 6579, 6792, 7946, 8480, 8482, 8485, 8836, 8849, or 2583 reports a different machine type during an installation, the BIOS might be corrupted. Restart the server, and make the appropriate selection during the restart to enter BIOS setup. In the BIOS, check the machine type that is configured. If the machine type does not match the specific server, reinstall the system BIOS. Refer to the server documentation to reinstall the BIOS and to set the correct machine type.

10. Restore the TSSC configuration from the backup. Refer to the *IBM TS3000 System Console (TSSC) Maintenance Information* (on the *IBM TS7650 with ProtecTIER Publications* CD) for instructions.
11. After the TSSC configuration is successfully restored, the reimage process is complete.

Rebuilding the disk and restoring the TSSC microcode configuration

The preferred method to rebuild a hard disk drive and configure the TSSC microcode is to combine both tasks into a single process. The combined process takes less time and does one less restart of the TSSC than does configuring the microcode separately.

About this task

Attention: Task for IBM Service Personnel

- Rebuilding the TSSC hard disk drive permanently deletes any local data present on the drive. Using the *IBM TS3000 System Console Product Recovery CD* will return the console to its "as shipped" state.
- After performing the procedure below, you will need to reload the Storage Manager GUIs, ProtecTIER Manager GUI, and Information Centers for TS7650. The actual applications depend on the systems that are attached to the TSSC. Refer to the *IBM TS3000 System Console (TSSC) Maintenance Information* for additional information. The backup menu option on the TSSC does not back up any of the mentioned applications listed above, only configuration data specific to the TSSC and the physically attached systems.

Procedure

1. Before you start, perform a back up the **IBM TS3000 System Console**.

   Note: The backup to the **IBM TS3000 System Console** is a precautionary step. The TSSC configuration and settings are retained during the upgrade.
2. Log in to the **IBM TS3000 System Console** with a username of `service` and a password of `service`.
3. From the main screen, right click on the desktop to display the IBM **TS3000 System Console** menu.
4. From the menu, select **System Console Actions** > **Disk Rebuild and Restore Config**.

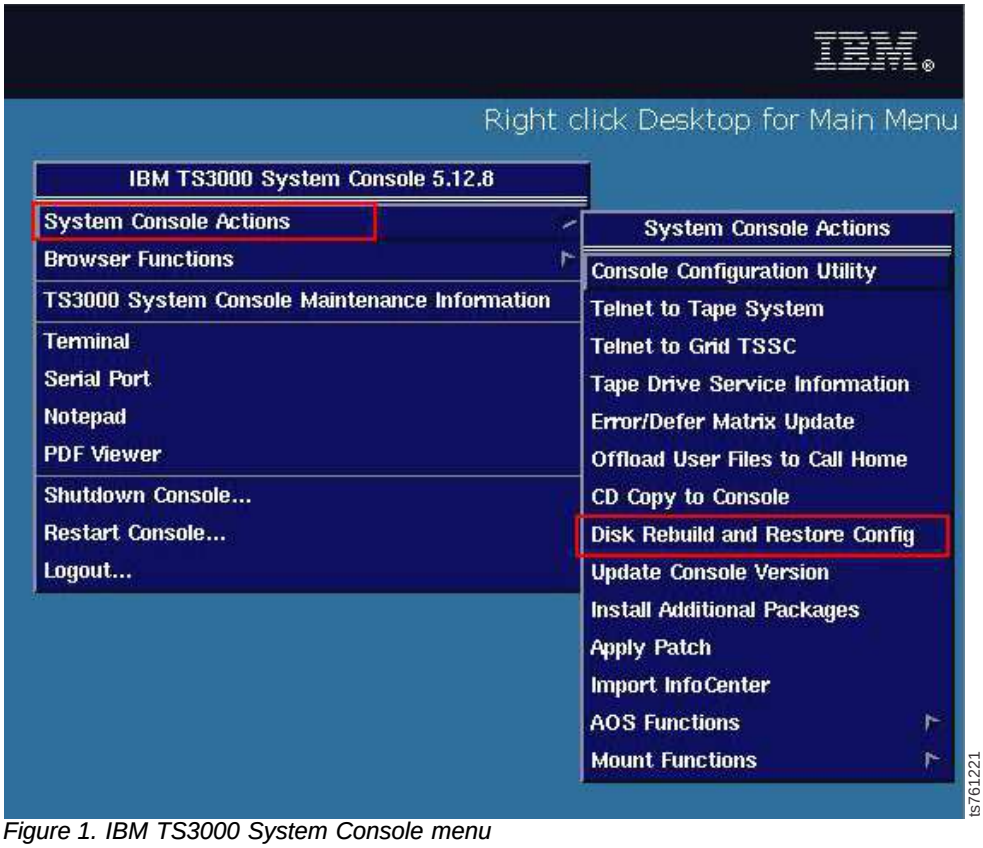


Figure 1. IBM TS3000 System Console menu

5. Go to the TSSC, open the CD-ROM drive bay, and insert the *Product Recovery CD IBM TS3000 System Console Disc 1*, then press Enter to start.

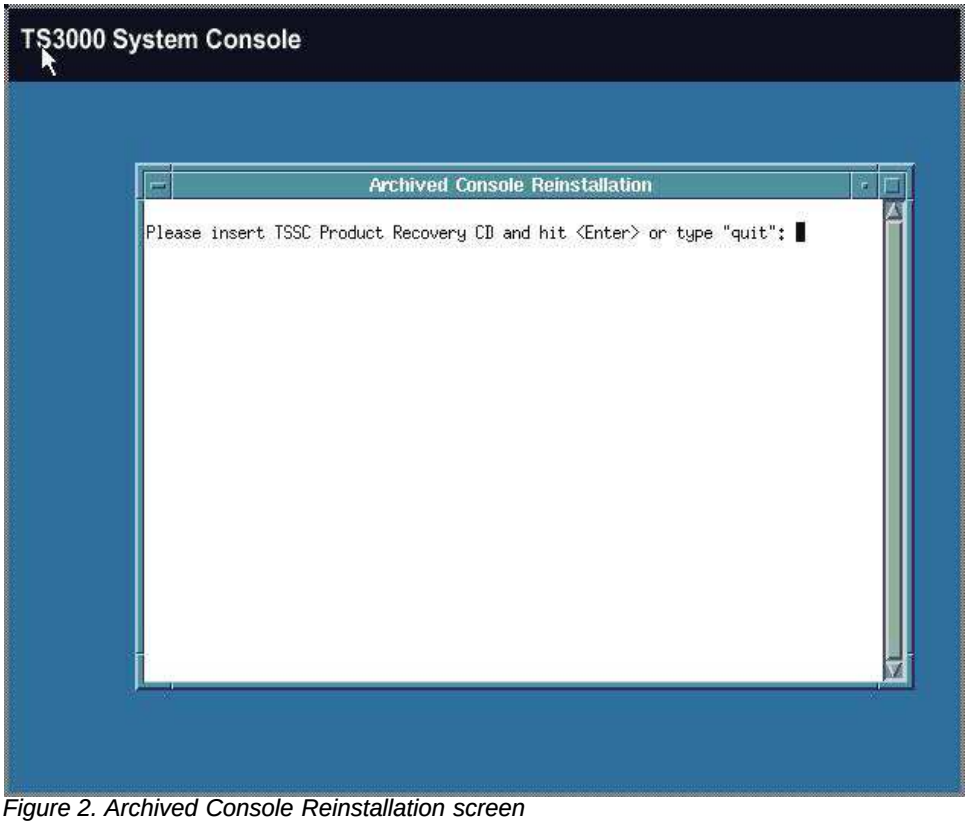


Figure 2. Archived Console Reinstallation screen

6. Pressing Enter dislays the following screen and starts the disk rebuild and restore configuration.

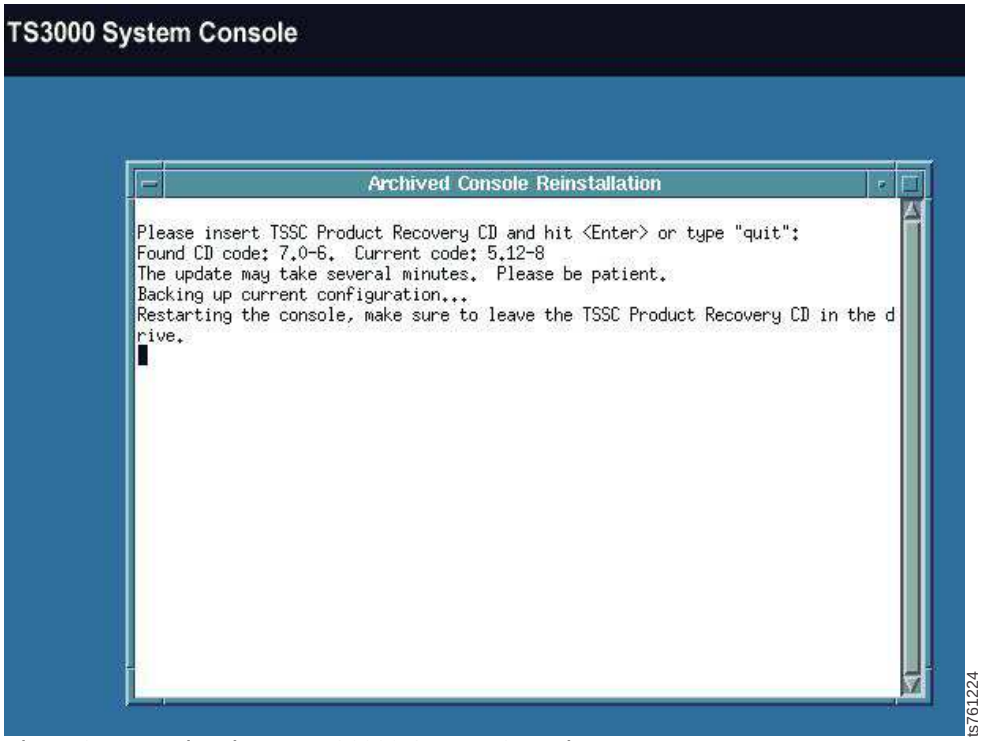


Figure 3. Restarting the IBM TS3000 System Console

7. Wait approximately 5 minutes for the system to reboot automatically.
8. Wait for the following message to ensure that the reboot is complete.

```
This will install the Console onto /dev/sda which will erase everything
 on that device
 Continue? ('yes' or 'no')
```

Figure 4. Message to confirm that reboot is complete

9. Type yes at the prompt, then press Enter. This action starts the rebuild and configuration restore process. The process takes approximately 10 minutes to complete.
10. When you are prompted, remove *Product Recovery CD IBM TS3000 System Console Disc 1* and insert *Product Recovery CD IBM TS3000 System Console Disc 2*.

    Note: When the process is complete, the *Product Recovery CD IBM TS3000 System Console Disc 2* will eject automatically and will display the **IBM TS3000 System Console** log in screen.
11. Log in to the **IBM TS3000 System Console**.

Figure 5. IBM TS3000 System Console login screen for TSSC code 7.0.x

Chapter 4. Upgrading ProtecTIER Manager

Use these procedures to upgrade the version of ProtecTIER Manager on the TSSC or ProtecTIER Manager workstation.

About this task

Note: TSSC is not supported on 3958 DD6 servers.

The current ProtecTIER Manager installer is provided on the *IBM ProtecTIER Manager* DVDand can also be downloaded from Fix Central. Because different ProtecTIER Manager installers are provided for Windows and Linux, make sure that the installer you use is correct for the operating system on your ProtecTIER Manager workstation:

- If you are installing the ProtecTIER Manager upgrade on a workstation that is running Windows, see "Upgrading ProtecTIER Manager on Windows" on page 14.
- If you are installing ProtecTIER Manager upgrade on a workstation that is running Linux, see "Upgrading ProtecTIER Manager on Linux" on page 16.

Important: Before you start the upgrade, make sure the current ProtecTIER Manager application is closed.

Upgrading ProtecTIER Manager on the TSSC

Use this procedure to upgrade the version of ProtecTIER Manager on the TSSC.

About this task

► IBM Service Task ◄

This task is to be completed by IBM service personnel.

To upgrade the version of ProtecTIER Manager on the TSSC, complete the following steps.

Important: Before you start the upgrade, make sure the current ProtecTIER Manager application is closed.

Procedure

1. If the TSSC is not already powered-on, do so now.
2. If prompted for login information, enter the user name `service` and the password `service`.

   The blue TSSC desktop is displayed.
3. Right-click on the blue TSSC desktop.

   The **IBM TS3000 System Console** menu is displayed.
4. Select **Browser Functions** > **ProtecTIER Manager Functions** > **Upgrade GUI**. The TSSC DVD drive opens and a window appears and instructs you to insert the DVD and press Enter.
5. Insert the *IBM ProtecTIER Manager* DVD. The following message is displayed:

   `Installation may last a few moments. Please be patient.`

6. When the ProtecTIER Manager installation wizard starts, follow the on-screen instructions to complete the installation.

   For detailed information about using the ProtecTIER Manager wizard, refer to steps 3 through 9 on page 16 in "Upgrading ProtecTIER Manager on Windows."

   When the installation is complete and ProtecTIER Manager is installed successfully, the **Install Complete** message appears.
7. Click **Done**.

   The ProtecTIER Manager installation wizard closes and the ProtecTIER Manager upgrade is complete.
8. Remove the *IBM ProtecTIER Manager* DVD and close the CD-DVD drive.

Upgrading ProtecTIER Manager on Windows

Use the following procedure to upgrade the version of ProtecTIER Manager on a Windows workstation.

Procedure

To upgrade the version of ProtecTIER Manager on a Windows workstation, complete the following steps:

Important: Before you start the upgrade, make sure the currently installed ProtecTIER Manager application is closed.

1. Set the resolution to 1280 x 1024 or higher.

   The minimum optimal resolution for viewing ProtecTIER Manager is 1280 x 1024.
2. Insert the *IBM ProtecTIER Manager* DVD into the CD-DVD drive of the designated ProtecTIER Manager workstation or run the installer downloaded from Fix Central.
   - If the ProtecTIER Manager Autorun starts the installation, go to step 3.
   - If the ProtecTIER Manager Autorun does not automatically start the installation, do the following tasks:

   a. On the Windows taskbar, click: **Start** > **Run**. The **Run** dialog box opens.
   b. In the **Open** field, type: **D:** (where D: is the CD-DVD drive)
   c. Click **OK**. The contents of the *IBM ProtecTIER Manager* DVD display.
   d. From the list of files, locate the **ProtecTIER Manager for Windows** installation file (`install.exe`). Select the correct file for your environment, either 32 bit or 64 bit. Using the incorrect file can cause the installation to fail.
   e. Double-click the file to start the installation.
3. Read the **Introduction** window, and then click **Next**. Two **License Agreement** windows open.
4. Read and accept the terms of each license agreement, and then click **Next**.

   The **Choose Install Folder** window opens. See Figure 6 on page 15.

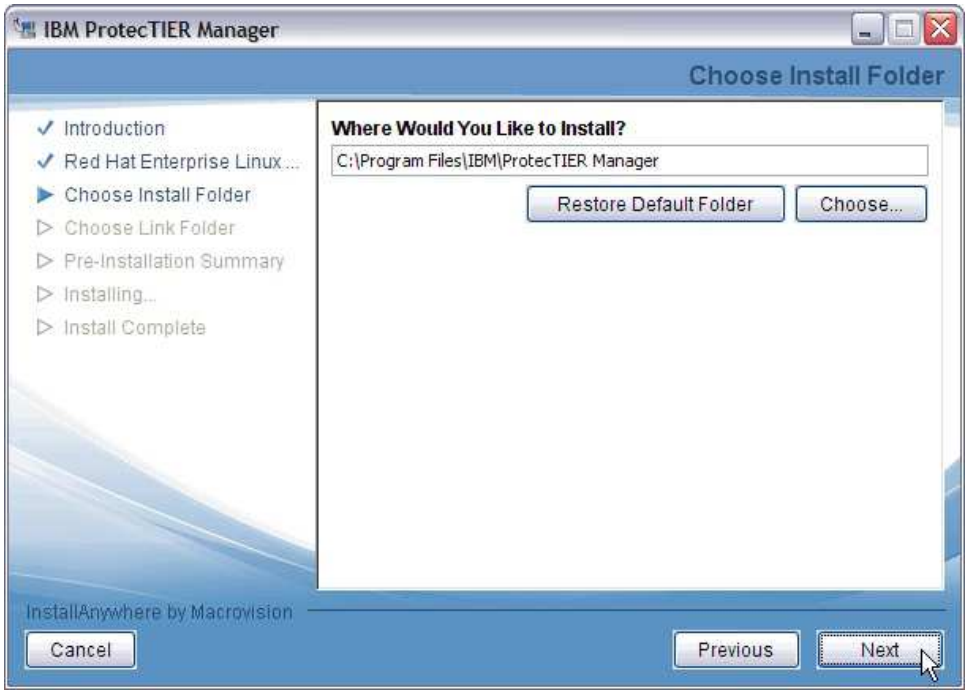


Figure 6. Choose **Install Folder** *window*

5. Specify the folder where you want the ProtecTIER Manager program files to be installed, and then click **Next**.

   The **Choose Shortcut Folder** window opens. See Figure 7.

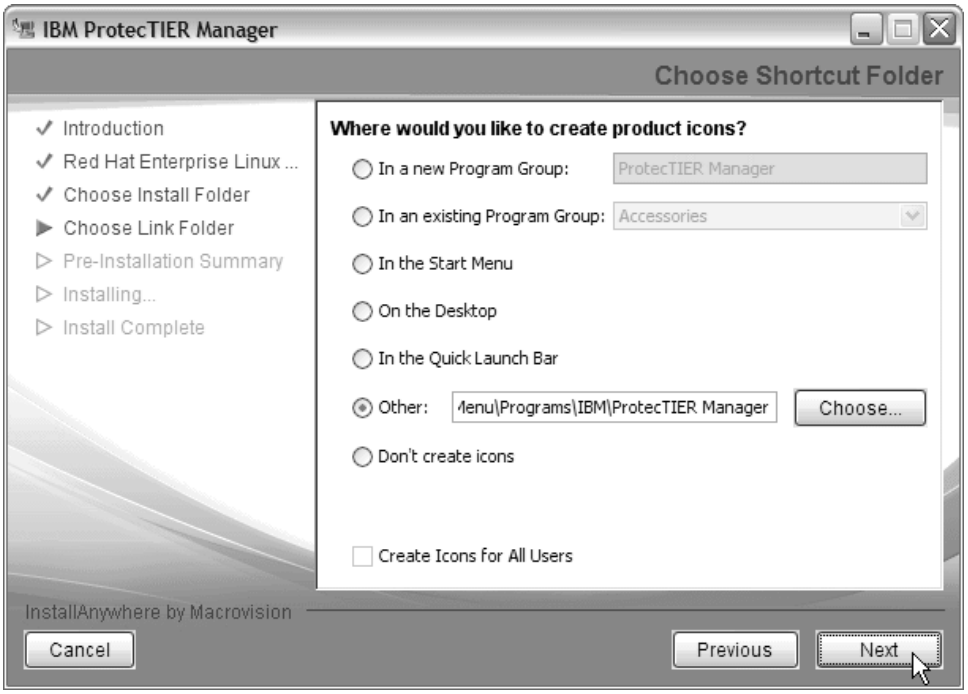


Figure 7. Choose **Shortcut Folder** *window*

6. Select the location where you want the program icons created:

- **In a new Program Group**: Adds the shortcut to a new program group in the Program list of the **Start** menu.
- **In an existing Program Group**: Adds the shortcut to an existing program group in the Program list of the **Start** menu.
- **In the Start Menu**
- **On the Desktop**
- **In the Quick Launch Bar**
- **Other**: Enter a path location for the shortcut, or to browse for a location by clicking **Choose**.
- **Don't create icons**: No shortcuts are created.

  Note: When relevant, you can select **Create Icons for All Users** to create a shortcut in the defined location for all user accounts on the workstation.

7. Click **Next**.

   The **Pre-Installation Summary** window opens.
8. Review the **Summary** window, and then click **Install** to start the installation.

   The Installing ProtecTIER Manager window opens.

   When the installation is complete and ProtecTIER Manager is successfully installed, the Install Complete window opens.
9. Click **Done**.

   The ProtecTIER Manager installation wizard closes and the upgrade process is complete.

Upgrading ProtecTIER Manager on Linux

Use this procedure to upgrade the version of ProtecTIER Manager on a Linux workstation.

Before you begin

Important: This procedure assumes that the workstation on which ProtecTIER Manager is being installed has a Linux graphical user interface (GUI). A GUI is required for ProtecTIER Manager operation on Linux.

Procedure

To upgrade the version of ProtecTIER Manager on a Linux workstation, complete the following steps:

Important: Before you start the upgrade, make sure the currently installed ProtecTIER Manager application is closed.

1. Set the resolution to 1280 x 1024 or higher.

   The optimal resolution for viewing ProtecTIER Manager.
2. Insert the *IBM ProtecTIER Manager* DVD into the CD-DVD drive of the designated ProtecTIER Manager workstation.
3. Run the ProtecTIER Manager installer. For example if you are using the DVD, complete the following steps:
   a. From the **Linux** desktop, double-click the **CD-DVD** icon, and then double-click the installation folder for the version of Linux you are using. Select the correct file for your environment, either 32 bit or 64 bit. Using the incorrect file can cause the installation to fail.

b. From the installation folder, select the `InstallLinuxXX.bin` file (where *XX* is 64 bit or 32 bit, depending on the folder you are in). Drag the file onto the desktop.

c. Close any open windows.

d. Right-click on any open area of the desktop, and from the displayed menu, click **Open Terminal**. The terminal window opens.

e. At the terminal command prompt, change to the **Desktop** directory. Enter the following command:

```
cd Desktop
```

and press Enter.

Note: This command is case-sensitive. Type it using a capital "D" in "Desktop."

f. From the Desktop directory on the Terminal Window, run the ProtecTIER Manager installer. In all commands below, *XX* is 64 bit or 32 bit.

Type `./InstallLinuxXX.bin` and press Enter

If the message: `Permission Denied` appears, enter the following commands:

```
chmod +x InstallLinuxXX.bin
./InstallLinuxXX.bin
```

and press Enter.

The **IBM ProtecTIER Manager Wizard Introduction**

4. Click **Next**. Two sequential **Software License Agreement** screens display.
5. Read the terms for each license agreement, indicate your acceptance, and then click **Next**. The **Choose Install Folder** screen displays.
6. Specify the location for the ProtecTIER Manager program files. To do so, do one of the following steps:
   - Enter the path to the location where you want the ProtecTIER Manager program files to be installed.
   - Click **Choose** to browse for a location.

   Note: Click **Restore Default Folder** to revert to the default installation path.
7. Click **Next**.

   The **Choose Link Folder** screen displays. See Figure 8 on page 18.

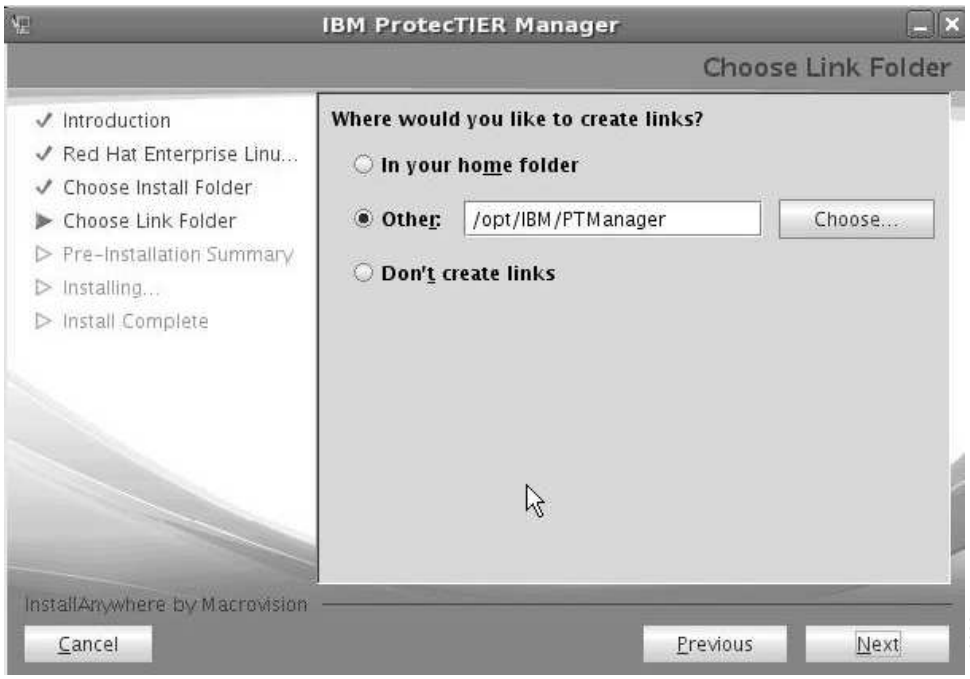


Figure 8. Choose Link folder

8. Select the location where the program links are created:
   - **In your Home folder**: Creates the links in the directory where the users files are typically stored. For example: `/home/bill`.
   - **Other**: Creates the links in the default location, such as `/opt/IBM/PTManager`. To specify a different location, click **Choose** and select a directory on the workstations hard disk.
   - **Don't create links**: No links are created.
9. Click **Next**. The **Pre-Installation Summary** screen displays.
10. Click **Install**.

    The **Installing ProtecTIER Manager** window is displayed and ProtecTIER Manager is installed.

    When the installation finishes, the **Install Complete** screen displays.
11. Click **Done**.

    The ProtecTIER Manager installation wizard closes and the upgrade process is complete.

Chapter 5. Upgrading the ProtecTIER software to 3.4.x from version 3.3.x using ProtecTIER Manager

This information helps you use the ProtecTIER Manager to upgrade ProtecTIER servers to version 3.4.x from version 3.3.x.

Before you begin

About this task

Important Notes:

- Although there are no specific caveats about going from any ProtecTIER version 3.3.x to any ProtecTIER version 3.4.x, the recommendation is that the repository is at ProtecTIER version 3.3.7 and then upgraded to ProtecTIER version 3.4.x.
- ProtecTIER Manager must be at version 3.4.x before this procedure can be used. To determine which version of ProtecTIER Manager is installed, click **Help > About ProtecTIER Manager**. For instructions about how to upgrade ProtecTIER Manager see Chapter 4, "Upgrading ProtecTIER Manager," on page 13.
- If your ProtecTIER Manager is in a version below 3.4.x and you do not want to upgrade it, you can use the ProtecTIER service menu to run the upgrade. See Chapter 7, "Upgrading the ProtecTIER software to 3.4.x from version 3.3.x using the ProtecTIER Service Menu," on page 29.
- If you are upgrading a dual node cluster ProtecTIER configuration, it is recommended that both nodes are online and active when running the upgrade.

  Note: If it happens that one of the nodes is offline, complete the upgrade in the online node. Once it finishes and the offline node is recovered, you must perform a special procedure known as single node upgrade, which is only available from the Service Menu.
- During an upgrade, the ProtecTIER server is not available for configurations or operations. The ProtecTIER Manager displays information about the upgrade that you are running.
- If your code upgrade fails, go to Chapter 10, "Recovering from a failed upgrade," on page 51.
- The upgrade procedure is not concurrent in a clustered environment. Complete the Red Hat and the ProtecTIER software upgrades on Server A first, then the Red Hat and the ProtecTIER software upgrades on Server B. The software upgrade process includes stopping and restarting services on each node.
- Verify that any attached storage is problem free. If any problems are present, such as failed DDM's or other errors, you must resolve them before you continue with the ProtecTIER upgrade.

Table 3. Preparing the servers for the ProtecTIER 3.4.x upgrade

Tasks	Procedure
Check the version of ProtecTIER running on each server to verify that the servers are at ProtecTIER version 3.3.x. ProtecTIER Manager must be at version 3.3.x or higher.	Appendix B, "Checking the ProtecTIER version for servers at ProtecTIER version 3.1.8 or higher," on page 57
Upgrade ProtecTIER Manager to the latest version 3.4.x if necessary.	Chapter 4, "Upgrading ProtecTIER Manager," on page 13

Table 3. Preparing the servers for the ProtecTIER 3.4.x upgrade (continued)

Tasks	Procedure
Download the desired ProtecTIER version 3.4.x software package from Fix Central.	See "Downloading the ProtecTIER 3.4.x fix pack" on page 43 for instructions about how to download ProtecTIER software and fixes.
Upgrade Red Hat Linux from V5.6 to V5.11	See Chapter 8, "Upgrading Red Hat Linux and ProtecTIER version 3.4.x for servers at version 3.3.x," on page 31
Upgrade ProtecTIER 3.3.x to version 3.4.x using ProtecTIER Manager.	"Upgrading from ProtecTIER 3.3.x to 3.4.x using ProtecTIER Manager on the ProtecTIER servers"

Upgrading from ProtecTIER 3.3.x to 3.4.x using ProtecTIER Manager on the ProtecTIER servers

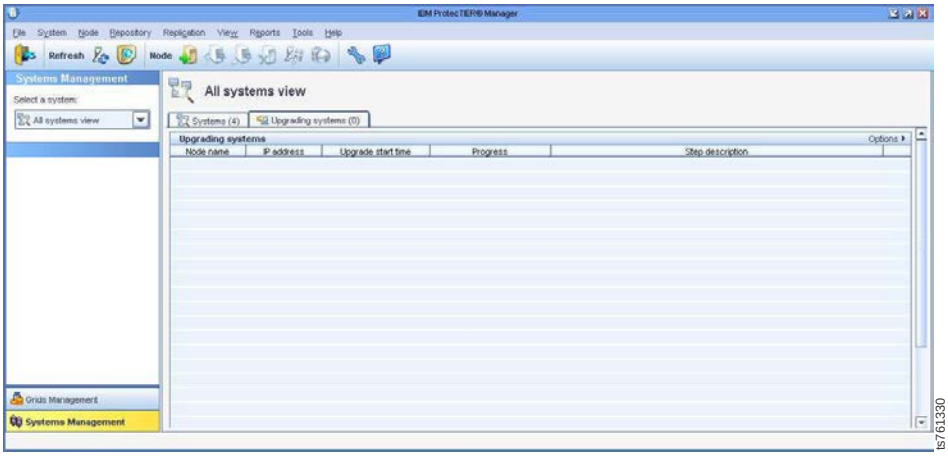
Use these procedures to upgrade from ProtecTIER 3.3.x to 3.4.x using the graphical user interface.

Procedure

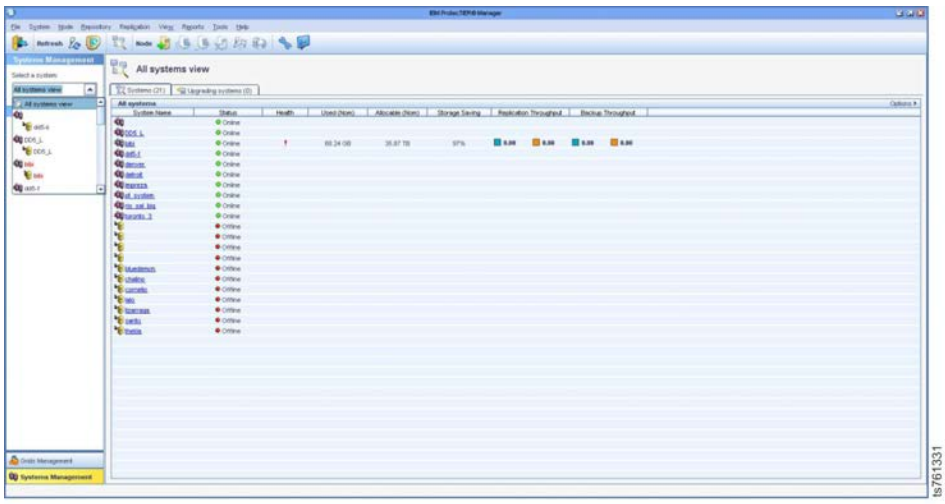
1. Open the ProtecTIER Manager. This action displays the ProtecTIER Manager splash screen and a message that the nodes are initializing.
2. After the nodes initialize, ensure that the **All systems view** is selected from the selection menu on the left.

   When you start the ProtecTIER Manager, the content page for **All systems view** does not display any system, which is normal. The systems appear on the display after you log in. The column headings in the **All systems view** also change after you log in. Instructions for logging in appear later in this procedure.

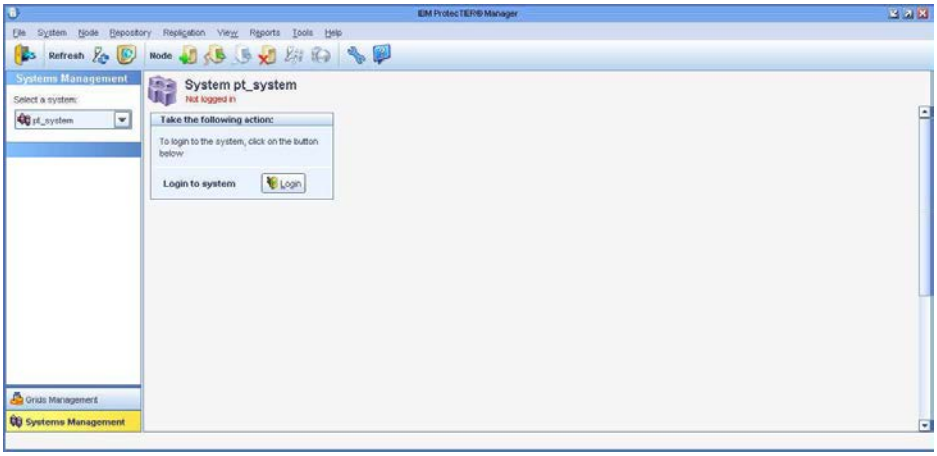
   Note: For a more detailed explanation of the **All systems view**, see the *IBM ProtecTIER User's Guide for VTL Systems, GA32-0922*.



3. From the selection menu on the left, select the system that you want to upgrade. Ensure that the column headings for System Name, Status, Health, Used (Nom), Allocable (Nom), Storage Saving, Replication Throughput, and Backup Throughput display after you log in.

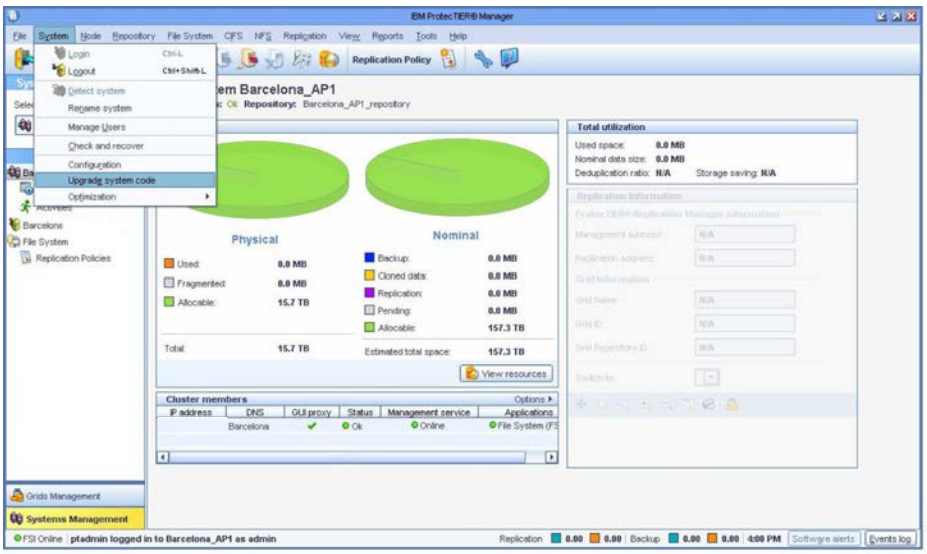


4. After you select your system, click **Login**.



5. Log in to ProtecTIER Manager.
   a. In the **User name** field, type `ptadmin`.
   b. In the **Password** field, type `ptadmin`.

6. Select the option you want to use to install the upgrade by use of the GUI. There are two ways to upgrade through the GUI.
   - From CD/DVD (either the one you received from IBM, or the one you created after downloading the code in the previous task). Continue with 7
   - From the upgrade file you downloaded from Fix Central to your PC. Continue with 10 on page 22
7. Insert the DVD/CD. Ensure that the DVD-ROM tray is closed.
8. From the ProtecTIER menu, select **System** > **Upgrade system code**.



9. Enter the `User name` and `Password`. Continue with 12
10. Locate the directory that contains the `PT_MD5_TS76XXXX_V3.4.x.x.x86_64.tar` file. You have two choices of how to access the upgrade files.
    - Leave the upgrade files on the PC where you downloaded them.
    - Copy the `PT_MD5_TS76XXXX_V3.4.x.x.x86_64.tar` file directly to the ProtecTIER server you are upgrading. Ensure that you copy the file to the `/install/new` directory on the server.

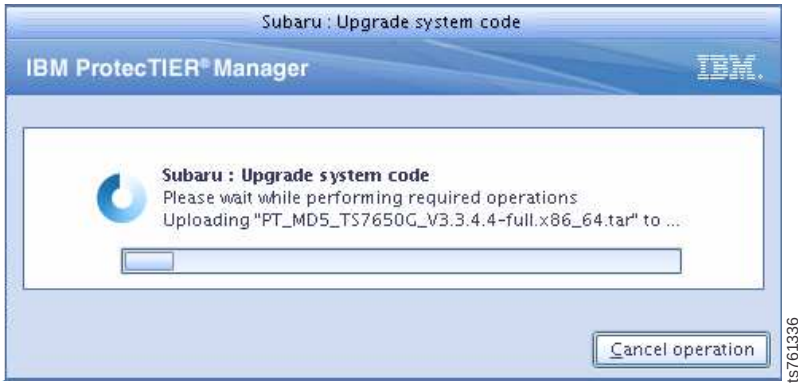
    When you start the upgrade process, the ProtecTIER GUI requests the path to the installation file.
11. If you are prompted for a password for root access, type `admin`.

```
scp <ProtecTIER package.tar> root@<ProtecTIER server IP>:/install/new
ls -l /install/new
-rwxr-xr-x 1 root root 873666560
MMM DD HH:MM PT_MD5_TS7650_V3.4.x.x.x86_64.tar
```

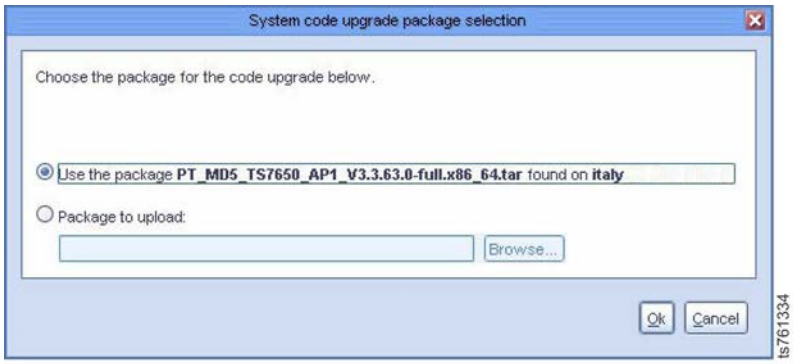
Note: The output of the **`ls -l /install/new`** command is an example of what might be shown. The actual output is determined by the specific code fix package that you are using.

12. The system is unavailable during the code upgrade. When you see the System code upgrade message, click **Yes** to continue.

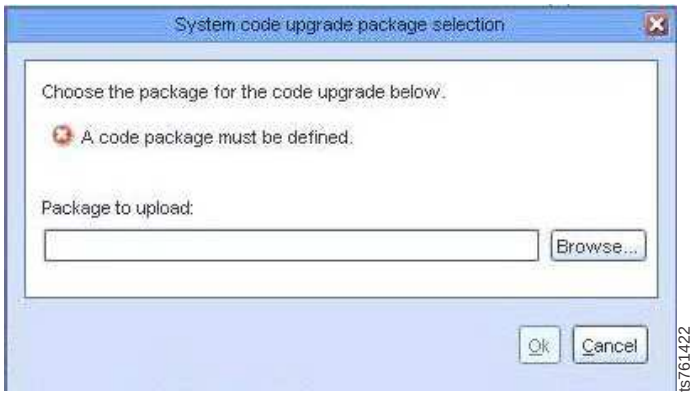
13. Wait approximately 10 minutes while the system performs the required operations, extracts the package, and prepares the server for the code upgrade.



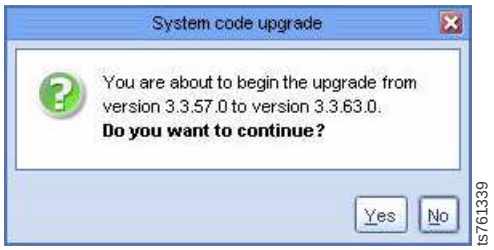
14. Did the window for **Choose the package for the code upgrade** appear?
    - **Yes**. A dialog box similar to the one shown here means that your code upgrade package is on the server. Select the name of the code upgrade package and click **OK**, then go to the next step. Otherwise, go to the **No** branch.



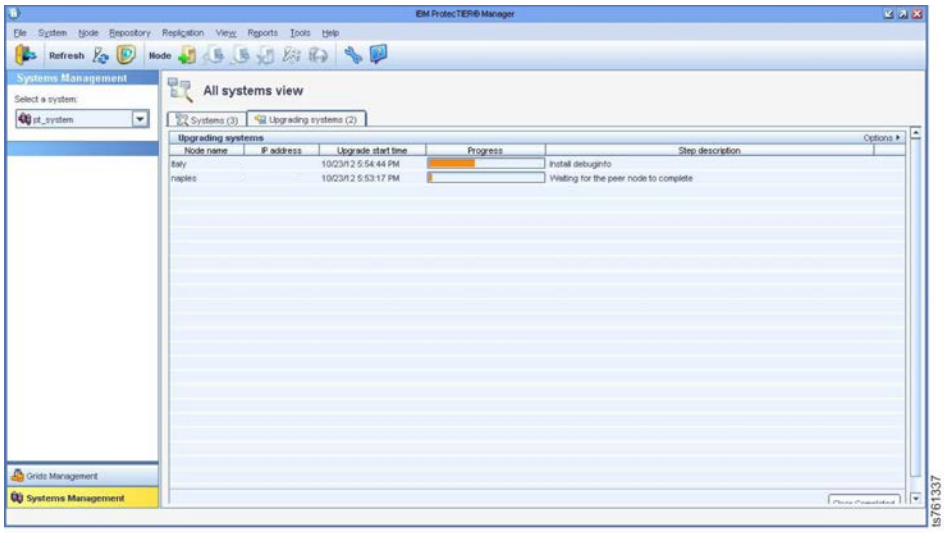
    - **No**. A dialog box similar to the one shown here appears if your code upgrade package is in a location other than the server. Click **Browse**, then navigate to the directory in which you saved the code upgrade package, then click **OK**.



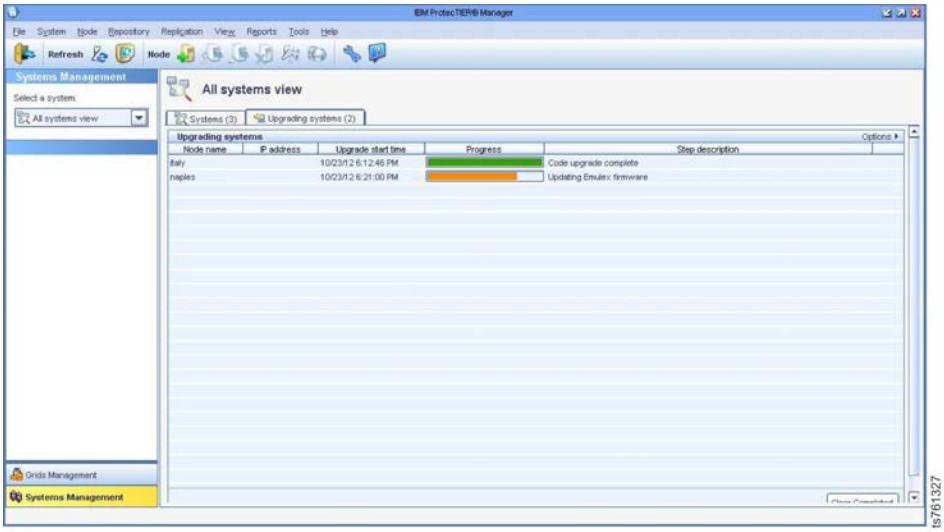
15. You are ready to start the code upgrade. Click **Yes** to continue or **No** to abort.



16. It takes approximately 20 - 30 minutes for each node to install the code upgrade package. Other variables, such as connection speed, can increase the amount of time.
    a. Monitor the progress bar periodically. To view the progress, ensure that you selected the tab for **Upgrading systems**.
    b. During the code upgrade, services stop, the system restarts automatically, and the **All systems view** appears.

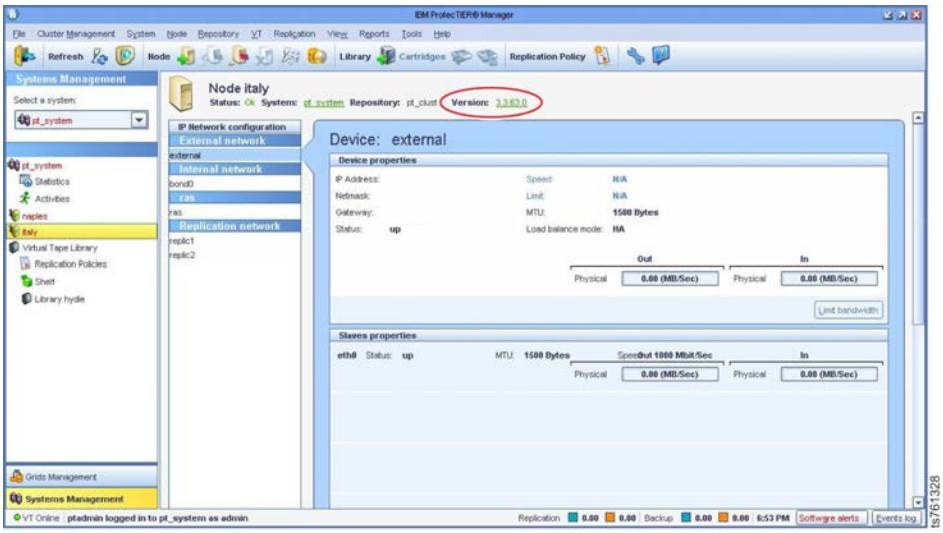


17. Wait until the progress bar turns green and that you see a message that the code upgrade is complete.



Note: If the code upgrade completes successfully and you see an alert message that the BOM check failed, disregard the message and continue.

18. To confirm that you upgraded the ProtecTIER to the correct version, click the name of the system which you upgraded, then locate the words and link for **Version**.



19. If you want to see detailed information about the release version (of the code), the ProtecTIER model, Linux RPM version, DTC Emulex RPM version, ProtecTIER Replication Manager Version, machine type model, and machine serial number, click the link for **Version**.

20. If the code upgrade failed, go to Chapter 10, “Recovering from a failed upgrade,” on page 51.

Chapter 6. Upgrading the ProtecTIER software to 3.3.x from version 3.1.8 or higher using ProtecTIER Manager

This information helps you use the ProtecTIER Manager to upgrade ProtecTIER servers to version 3.3.x from version 3.1.8 or higher.

About this task

Important Notes:

- The upgrade procedure is not concurrent in a clustered environment. In a clustered environment, complete the ProtecTIER software upgrade on Server A first (if a Red Hat kernel upgrade is required, it will be done automatically by the ProtecTIER software upgrade). Next, complete the ProtecTIER software upgrade on Server B (if a Red Hat kernel upgrade is required, it will be done automatically by the ProtecTIER software upgrade). The software upgrade process includes stopping and restarting services on each node.
- During an upgrade, the ProtecTIER server is not available for configurations or operations. The ProtecTIER Manager displays information about the upgrade that you are running.
- ProtecTIER Manager must be at version 3.3.x before this procedure can be used. For instructions about how to upgrade ProtecTIER Manager see Chapter 4, "Upgrading ProtecTIER Manager," on page 13..
- If ProtecTIER Manager is at a version below 3.3.x and you do not want to upgrade it, you can use the ProtecTIER **Service Menu** to complete the ProtecTIER software upgrade. See Chapter 7, "Upgrading the ProtecTIER software to 3.4.x from version 3.3.x using the ProtecTIER Service Menu," on page 29
- These procedures are for servers already at ProtecTIER version 3.1.8 or higher. ProtecTIER Versions 3.1.8 or higher include a Red Hat Linux kernel update as part of the upgrade, but do not require a full Red Hat Linux upgrade.
- If you are upgrading a dual node cluster ProtecTIER configuration, it is recommended that both nodes are online and active when running the upgrade.

  Note: If it happens that one of the nodes is offline, complete the upgrade in the online node. When the upgrade finishes, recover the offline node. Use the single node upgrade procedure, which is only available from the Service Menu, to upgrade the second node.
- Verify that any attached storage is problem free. If any problems are present, such as failed DDM's or other errors, you must resolve them before you continue with the ProtecTIER upgrade.

Table 4. Preparing the servers for the ProtecTIER 3.3.x upgrade

Tasks	Procedures
Check the version of ProtecTIER running on each server to verify that the servers are at ProtecTIER version 3.1.8 or higher. ProtecTIER Manager must be at version 3.3.x or higher.	Appendix B, "Checking the ProtecTIER version for servers at ProtecTIER version 3.1.8 or higher," on page 57
Upgrade ProtecTIER Manager to version 3.3.x, if necessary.	Chapter 4, "Upgrading ProtecTIER Manager," on page 13

Table 4. Preparing the servers for the ProtecTIER 3.3.x upgrade (continued)

Tasks	Procedures
Upgrade ProtecTIER 3.1.8 or higher to version 3.3.x using ProtecTIER Manager.	Follow the same instructions as described in Chapter 5, "Upgrading the ProtecTIER software to 3.4.x from version 3.3.x using ProtecTIER Manager," on page 19

Chapter 7. Upgrading the ProtecTIER software to 3.4.x from version 3.3.x using the ProtecTIER Service Menu

You can use the **ProtecTIER service menu** to upgrade ProtecTIER servers to version 3.4.x from version 3.3.x.

Before you begin

About this task

Important Notes:

- If you are upgrading a dual node cluster ProtecTIER configuration, it is recommended that both nodes are online and active when running the upgrade.

  Note: If it happens that one of the nodes is offline, complete the upgrade in the online node. When the upgrade finishes, recover the offline node. Use the single node upgrade procedure, which is only available from the Service Menu, to upgrade the second node.
- During an upgrade, the ProtecTIER server is not available for configurations or operations. The ProtecTIER Manager displays information about the upgrade that you are running.
- If your code upgrade fails, go to Chapter 10, "Recovering from a failed upgrade," on page 51.
- The upgrade procedure is not concurrent in a clustered environment. Complete the Red Hat and the ProtecTIER software upgrades on Server A first, then the Red Hat and the ProtecTIER software upgrades on Server B. The software upgrade process includes stopping and restarting services on each node.
- Verify that any attached storage is problem free. If any problems are present, such as failed DDM's or other errors, you must resolve them before you continue with the ProtecTIER upgrade.

Table 5. Preparing the servers for the ProtecTIER 3.4.x upgrade

Tasks	Procedure
Check the version of ProtecTIER running on each server to verify that the servers are at ProtecTIER version 3.3.x. ProtecTIER Manager must be at version 3.3.x or higher.	Appendix B, "Checking the ProtecTIER version for servers at ProtecTIER version 3.1.8 or higher," on page 57
Upgrade ProtecTIER Manager to the latest version 3.4.x if necessary.	Chapter 4, "Upgrading ProtecTIER Manager," on page 13
Download the desired ProtecTIER version 3.4.x software package from Fix Central.	See "Downloading the ProtecTIER 3.4.x fix pack" on page 43 for instructions about how to download ProtecTIER software and fixes.
Upgrade Red Hat Linux from V5.6 to V5.11.	Chapter 8, "Upgrading Red Hat Linux and ProtecTIER version 3.4.x for servers at version 3.3.x," on page 31
Upgrade ProtecTIER 3.3.x to version 3.4.x using the ProtecTIER Service menu.	Follow the same instructions as described in Chapter 9, "Applying fix packs for ProtecTIER systems already at version 3.4," on page 43

Chapter 8. Upgrading Red Hat Linux and ProtecTIER version 3.4.x for servers at version 3.3.x

This information provides instructions for upgrading Red Hat Linux and ProtecTIER on existing servers at ProtecTIER version 3.3.x.

About this task

Important:

- For the 3958 DD6 neither an external DVD ROM nor the micro HDMI to VGA adapter is part of the IBM ship group. These need to be supplied by the customer.
- Before you can upgrade the ProtecTIER software to V3.4.x from 3.3.x, you must first upgrade to Red Hat Enterprise Linux 5.11. Do not try to start the upgrade from the `PT_MD_TS7650G_v3.4.x.x.x86_64.tar` packet before you complete the upgrade to Red Hat Enterprise Linux, or you get the following error message:

  ```
  The kernal version check found kernal 2.6.18-238.40.1.el5
  This version of ProtecTIER requires kernel 2.6.18-398.el5 to be installed.

  Please upgrade to RH5.11 with latest PT iso retry
  ```

- Due to licensing and copyright restrictions Red Hat Enterprise Linux version 5.11 is only available to registered customers via the Entitled Systems Support site. http://www-304.ibm.com/servers/eserver/ess/OpenServlet.wss.

  To download the Red Hat Enterprise Linux software, register at the above link by supplying your software customer number or ProtecTIER system serial number. For help registering or downloading the software please refer to the "Contacts" page at the website for assistance (http://www-304.ibm.com/servers/eserver/ess/OpenServlet.wss?NO_SCRIPT=YES&show_page=ess_contact_info.jsp&command=ShowPageCommand).
- The upgrade procedure is not concurrent. You must complete the Red Hat Linux version 5.11 first, and then complete the ProtecTIER version 3.4.x upgrade. In a dual node cluster environment, both software upgrades must be completed on Server A, then completed on Server B.
- The upgrade of Red Hat Linux version 5.11 and ProtecTIER version 3.4.x can take up to four hours total to complete in a dual node cluster environment.
- You can run the upgrade procedure on existing servers with ProtecTIER version 3.3.x. If your server is at a ProtecTIER version 3.2.x or earlier, you need to upgrade it to version 3.3.x before you can continue. See Chapter 6, “Upgrading the ProtecTIER software to 3.3.x from version 3.1.8 or higher using ProtecTIER Manager,” on page 27.
- If your server is at a ProtecTIER version earlier than 2.4, you need to upgrade it to version 2.4 before you can continue. Use the *IBM System Storage TS7650 ProtecTIER V2.4 Software Upgrade and Replication Enablement Guide*, IBM form number GC53-1196 to run this upgrade.
- Verify that any attached storage is problem free. If any problems are present, such as failed DDM’s or other errors, you need to resolve them before you can continue with the ProtecTIER upgrade.

Attention: If your code upgrade fails, you are directed when to go to Chapter 10, "Recovering from a failed upgrade," on page 51, which provides instructions on how to troubleshoot and resolve your problems with the code upgrade.

Procedure

1. Log in to the server on which you plan to upgrade Red Hat Enterprise Linux v5.11. In a dual node cluster environment, the first time through these steps work with Server A

   Important:

   - In a dual node cluster environment, run all procedures for both the upgrade to Red Hat Enterprise Linux version 5.11 and the upgrade to ProtecTIER version 3.4 on Server A (the bottom server) first. Then, repeat these procedures on Server B. To avoid complications, including unnecessary system restarts, you must start with Server A.
   - In a dual node cluster environment, when you are upgrading Server A power off Server B. If Server B is still powered on during the ProtecTIER code upgrade on Server A, the automatic restart on Server A also restarts Server B. Restarting Server B with a lower version of Red Hat Enterprise Linux results in a failure.

2. Restart node A and insert the IBM System Storage ProtecTIER Maintenance and Recovery Disk (which includes Linux Red Hat V5.11) into the DVD/CD-ROM drive.
3. Log in to Server B by typing `ptconfig` at the logon prompt and pressing Enter. At the password prompt, type `ptconfig` and press Enter. The system displays the ProtecTIER Service menu:

```
--------------------------------------------------------------------------------
   ProtecTIER Service Menu running on rasap 1
--------------------------------------------------------------------------------
   1) ProtecTIER Configuration (...)
   2) Manage ProtecTIER services (...)
   3) Health Monitoring (...)
   4) Problem Alerting (...)
   5) Version Information (...)
   6) Generate a service report
   7) Generate a system view
   8) Update ProtecTIER code
   9) ProtecTIER Analysis (...)

   E) Exit
   ------------------------------------------------------------------------------
   >>> Your choice?
```

4. From the ProtecTIER Service menu, select **Manage ProtecTIER services (...)**. The system displays the Manage ProtecTIER services (...) menu:

```
-------------------------------------------------------------------
 ProtecTIER Service Menu running on rasap 1
 Manage ProtecTIER Services (...)
-------------------------------------------------------------------
  1) Display services status
  2) Start all services
  3) Stop all services
  4) Stop ProtecTIER services only (including GFS)
  5) Stop VTFD service only
  6) Poweroff This Node
  7) Reboot This Node

  B) Back
  E) Exit
--------------------------------------------------------------------------------
>>> Your choice?
```

5. From the Manage ProtecTIER Services (...) menu, select **Poweroff This Node**. When the power off process is complete, the power LED on the server's front panel flashes steadily to indicate that the server is in standby node.

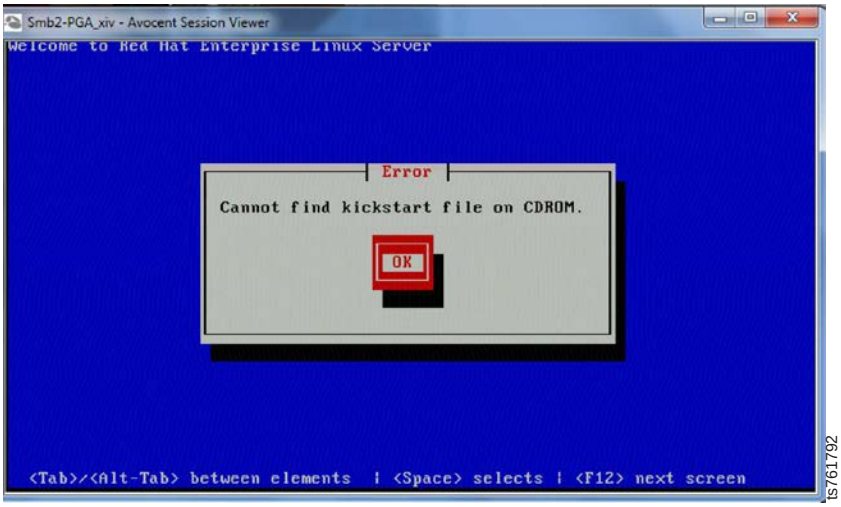
6. Log in to Server A by typing `ptconfig` at the logon prompt and pressing Enter. At the password prompt, type `ptconfig` and press Enter. The system displays the ProtecTIER Service menu:

```
--------------------------------------------------------------------------
 ProtecTIER Service Menu running on rasap 1
--------------------------------------------------------------------------
  1) ProtecTIER Configuration (...)
  2) Manage ProtecTIER services (...)
  3) Health Monitoring (...)
  4) Problem Alerting (...)
  5) Version Information (...)
  6) Generate a service report
  7) Generate a system view
  8) Update ProtecTIER code
  9) ProtecTIER Analysis (...)

  E) Exit
--------------------------------------------------------------------------
>>> Your choice?
```

7. From the ProtecTIER Service menu, select **Manage ProtecTIER services (...)**. The system displays the Manage ProtecTIER services (...) menu:

```
--------------------------------------------------------------------------
 ProtecTIER Service Menu running on rasap 1
           Manage ProtecTIER Services (...)
--------------------------------------------------------------------------
  1) Display services status
  2) Start all services
  3) Stop all services
  4) Stop ProtecTIER services only (including GFS)
  5) Stop VTFD service only
  6) Poweroff This Node
  7) Reboot This Node

  B) Back
  E) Exit
--------------------------------------------------------------------------
>>> Your choice?
```

8. From the Manage ProtecTIER Services menu, select **Stop all services**.
9. After the services are stopped (which can take up to an hour or more), select **Reboot This Node** to restart the server.
   a. When the IBM logo screen appears during the start sequence, press the F12 key to open the Select one time Boot Device window. The selection window looks similar to the screen:



   b. Select the CD/DVD ROM drive as the Boot Device.

10. Select Option 2 to upgrade your version of Red Hat.
    a. Follow the prompts on the screen.

       ```
       ATTENTION:
                This is an UPGRADE. The information stored on the local
                hard drive will not be overwritten.

       If this is what you intended to run,
       please type YES and [Enter] to continue (NO to poweroff):
       ```

    b. Type: YES and press Enter. Upgrading Red Hat takes about 30 minutes and you may receive progress information such as

       ```
       Checking dependencies in packages selected for installation...
       ```

       The server restarts automatically at the end of the Red Hat upgrade.
    c. When prompted to accept the software license agreement, press Enter to view the license agreement. Press Enter to read the next page, repeating until you reach the end of the license agreement. Type yes to accept the license agreement. Press Enter to continue.
11. The Red Hat Enterprise Linux upgrade begins. The upgrade takes approximately 15 minutes to an hour to complete.

Attention: If a server power loss interrupts the Red Hat Linux v5.11 upgrade before it is completed, the upgrade fails. To recover from the failed upgrade and prevent problems in future Red Hat Linux v5.11 upgrades, take the following steps:

a. Allow the server to restart normally from the power loss on the server to recover the server from the failed Red Hat Linux v5.6 upgrade.

b. When the server is back online, go to step 12

12. The server restarts automatically at the end of the upgrade process. Remove the *IBM ProtecTIER Maintenance and Recovery Disk* from the DVD drive during the restart. If you see any Buffer I/O error messages, they are not critical errors and you can continue with the procedure.

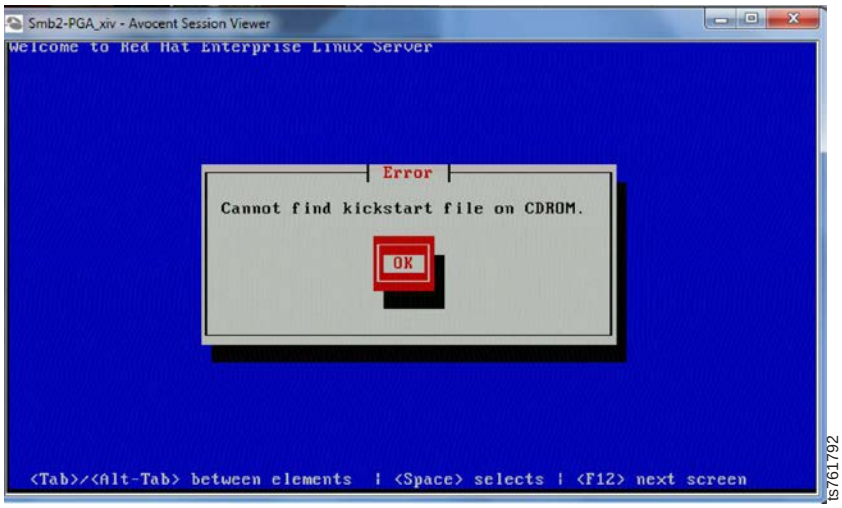
13. At the **login:** prompt, log in to Server A with the ID `ptconfig` and the password `ptconfig`.

What to do if the Red Hat kickstart exec is not found

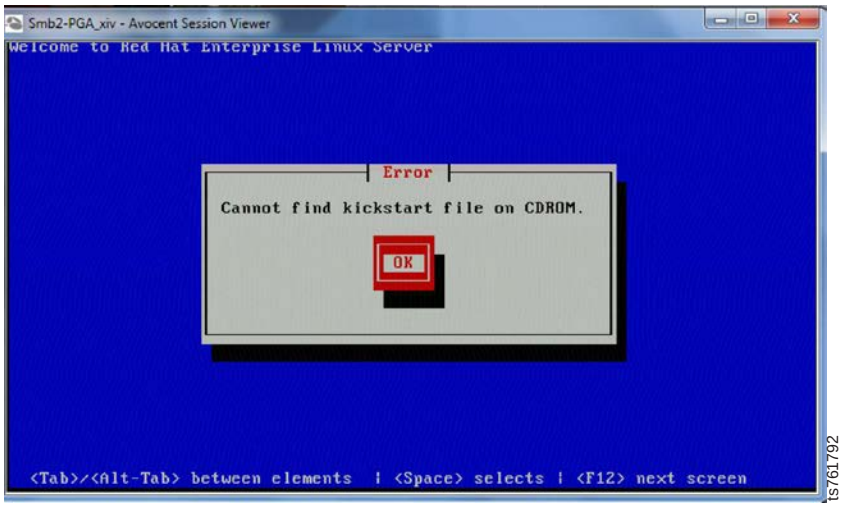
Procedure

1. Depending on how you access the Red Hat Enterprise Linux V5.11 upgrade, you may encounter one of the following messages.
   - If you are using the IBM System Storage ProtecTIER Maintenance and Recovery Disk and the following message appears, click OK to access the

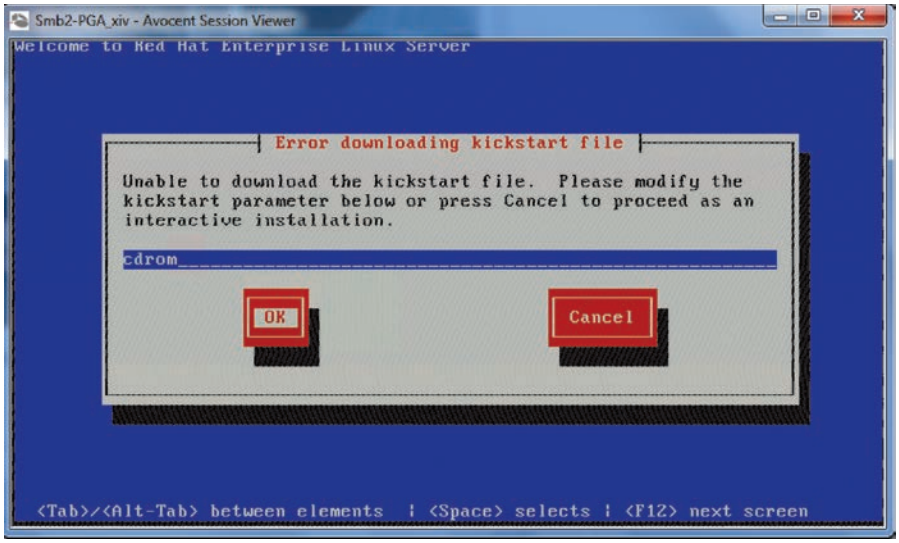
backup software.



- If you downloaded the Red Hat Enterprise Linux v5.11 code from IBM Entitle Systems Support (ESS) site and the following message appears, click OK to access the backup software.



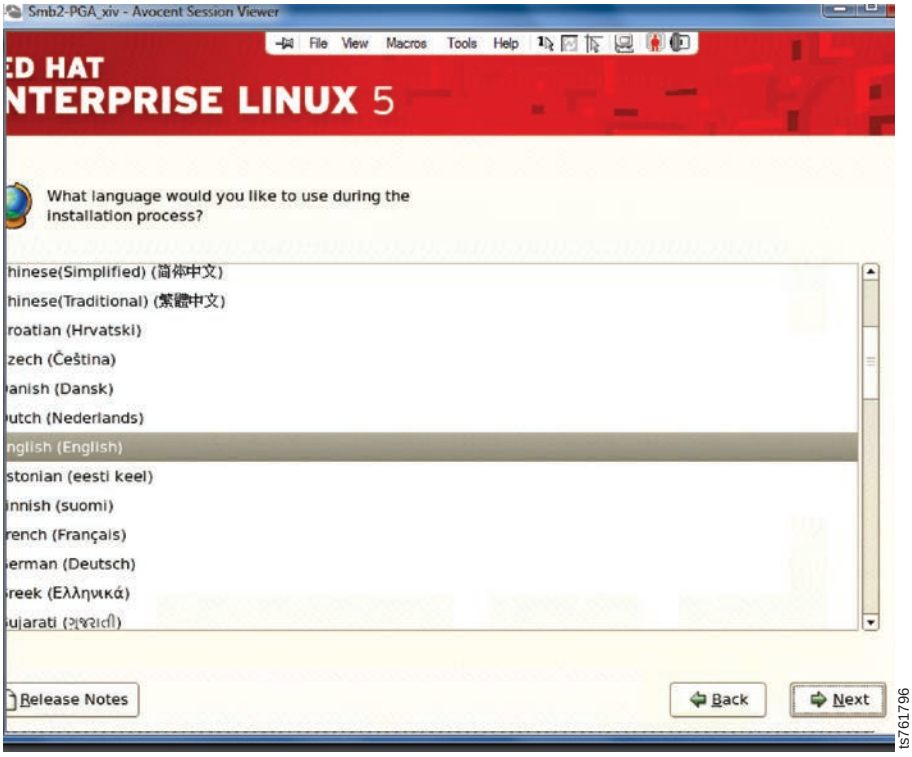
2. In either case, DO NOT cancel out of the menu. If you cancel, any of the following screens might appear. They all mean the upgrade has failed. Stop Red Hat Enterprise Linux installation and start over again.



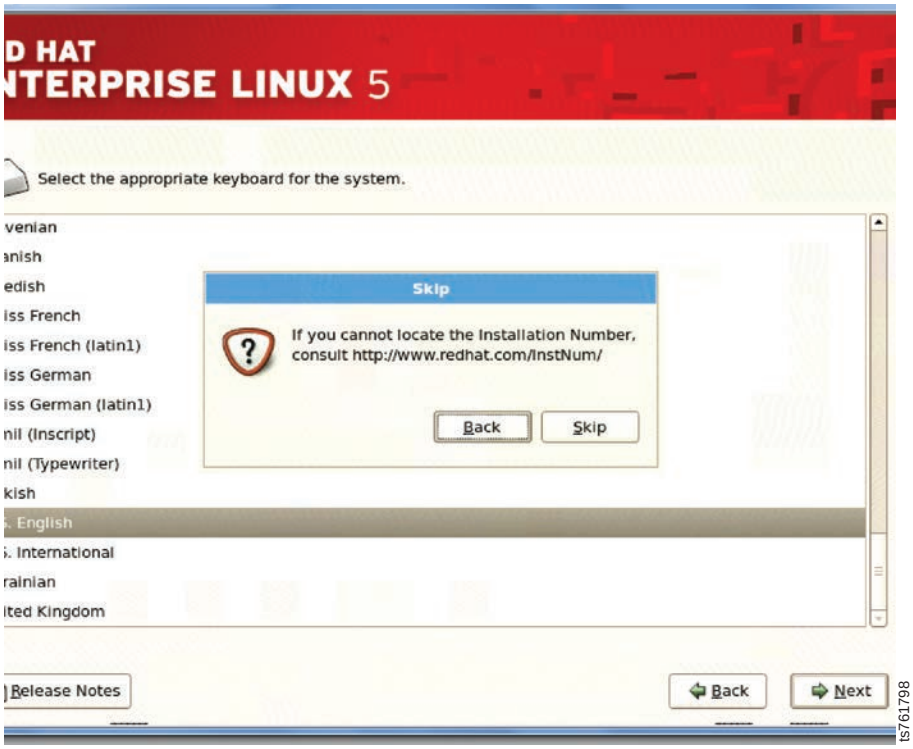
ts761793

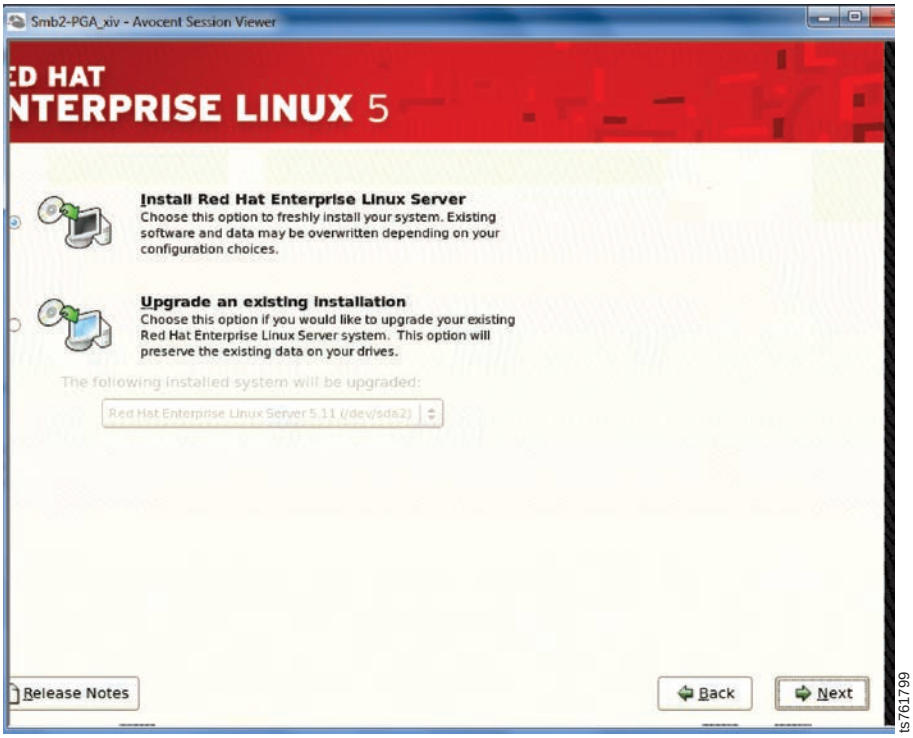
ts761794

ts761795

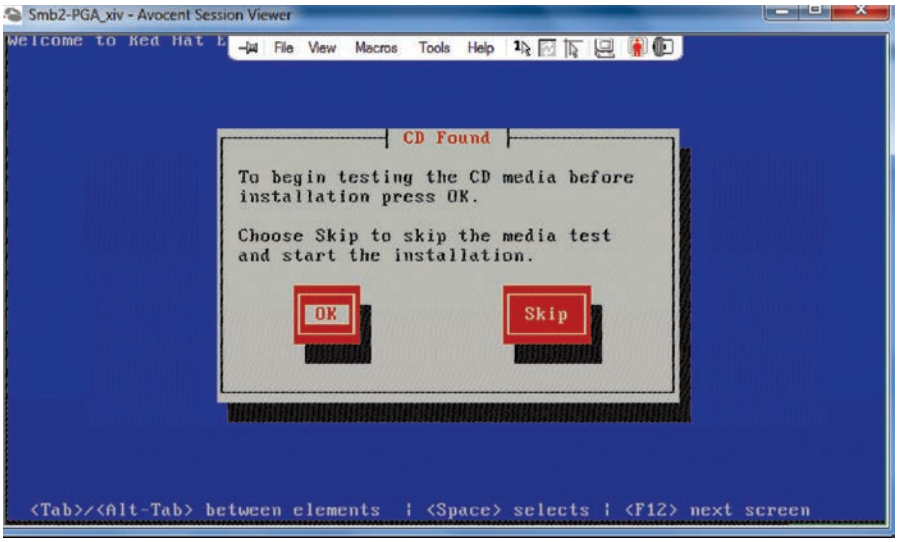


ts761796

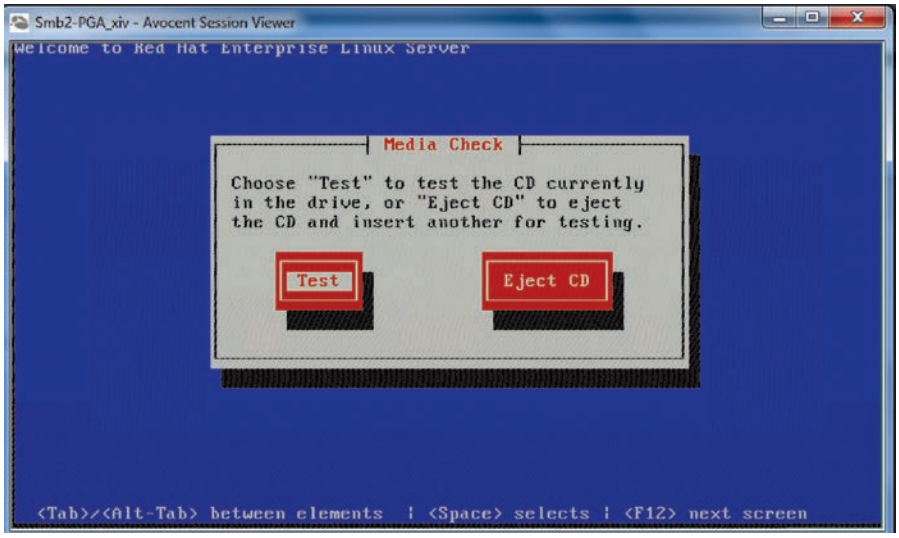

D HAT
NTERPRISE LINUX 5
Select the appropriate keyboard for the system.
venian
anish
edish
iss French
iss French (latin1)
iss German
iss German (latin1)
nil (Inscript)
nil (Typewriter)
kish
. English
. International
rainian
ited Kingdom
Skip
If you cannot locate the Installation Number, consult http://www.redhat.com/InstNum/
Back
Skip
Release Notes
Back
Next
ts761798

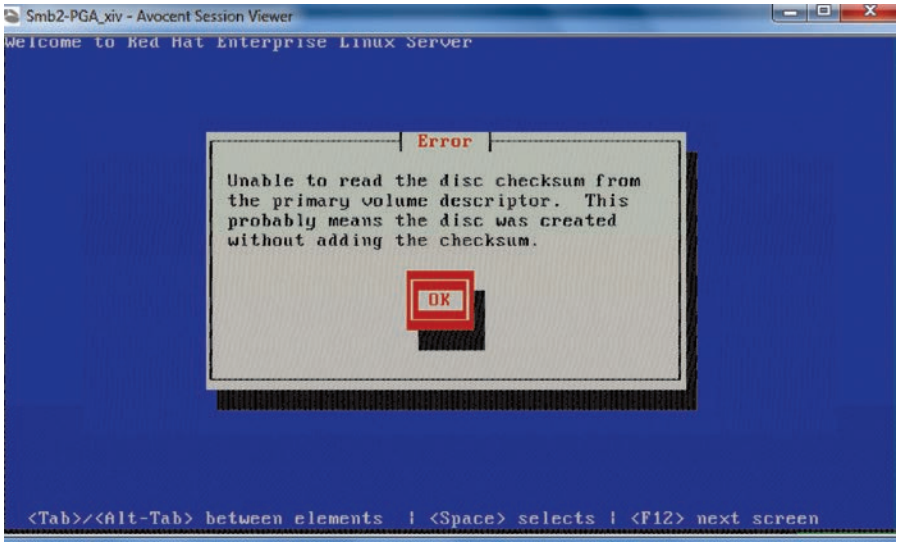


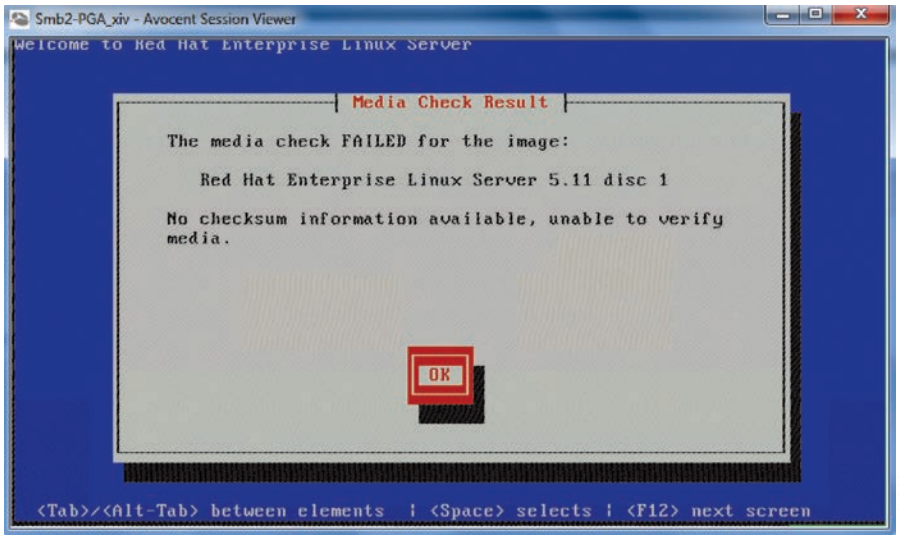
ts761799

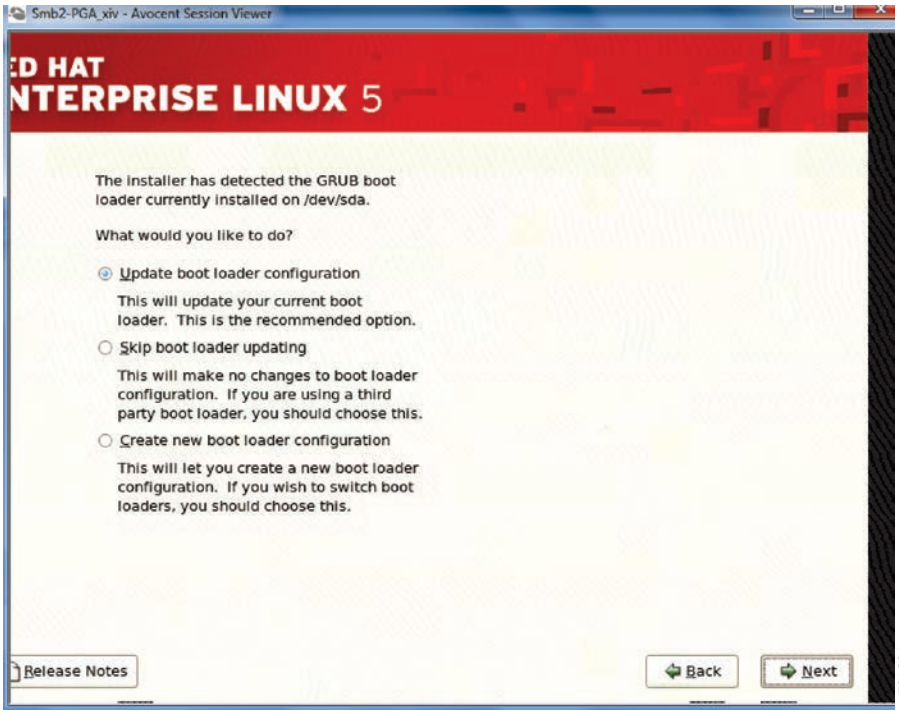


ts761800


Smb2-PGA_xiv - Avocent Session Viewer
Welcome to Red Hat Enterprise Linux Server
Media Check
Choose "Test" to test the CD currently in the drive, or "Eject CD" to eject the CD and insert another for testing.
Test
Eject CD
<Tab>/<Alt-Tab> between elements | <Space> selects | <F12> next screen
ts761801


Smb2-PGA_xiv - Avocent Session Viewer
Welcome to Red Hat Enterprise Linux Server
Error
Unable to read the disc checksum from the primary volume descriptor. This probably means the disc was created without adding the checksum.
OK
<Tab>/<Alt-Tab> between elements | <Space> selects | <F12> next screen
ts761802


Smb2-PGA_xiv - Avocent Session Viewer
Welcome to Red Hat Enterprise Linux Server
Media Check Result
The media check FAILED for the image:
Red Hat Enterprise Linux Server 5.11 disc 1
No checksum information available, unable to verify media.
OK
<Tab>/<Alt-Tab> between elements | <Space> selects | <F12> next screen
ts761803


Smb2-PGA_xiv - Avocent Session Viewer
ED HAT
NTERPRISE LINUX 5
The installer has detected the GRUB boot loader currently installed on /dev/sda.
What would you like to do?
Update boot loader configuration
This will update your current boot loader. This is the recommended option.
Skip boot loader updating
This will make no changes to boot loader configuration. If you are using a third party boot loader, you should choose this.
Create new boot loader configuration
This will let you create a new boot loader configuration. If you wish to switch boot loaders, you should choose this.
Release Notes
Back
Next
ts761804

Chapter 9. Applying fix packs for ProtecTIER systems already at version 3.4

After the ProtecTIER software is upgraded to version 3.4.0 or higher, you might need to install updates to ProtecTIER for fixes and other updates. These instructions are for upgrading to version 3.4.x.

Use the procedures in this section to update the ProtecTIER servers to the most current version of ProtecTIER.

Important: The upgrade procedure is not concurrent in a clustered environment. In a clustered environment, complete the Red Hat Enterprise Linux upgrade (if required) and ProtecTIER software upgrade on Server A first then complete the Red Hat Enterprise Linux upgrade (if required) and the ProtecTIER software upgrade on Server B The software upgrade process includes stopping and restarting services on each node.

Table 6. Preparing the servers for the most current update

Tasks	Procedure
Check the version of ProtecTIER running on each server to verify that the servers are at ProtecTIER version 3.4.x. ProtecTIER Manager must be at version 3.4.x or higher.	Appendix B, "Checking the ProtecTIER version for servers at ProtecTIER version 3.1.8 or higher," on page 57
Download the most current version of ProtecTIER (v3.4.x) from the IBM Fix Central Website. Copy the files to a CD or copy the file directly to the appropriate location on the server.	"Downloading the ProtecTIER 3.4.x fix pack"
Install the ProtecTIER fix updates.	"Applying the V3.4.x fix pack to the ProtecTIER servers" on page 44

Downloading the ProtecTIER 3.4.x fix pack

Use these procedures to download the latest or desiredProtecTIER version 3.4.x fix pack from the IBM Fix Central website.

Before you begin

If you already have the desired software package from IBM, skip the following steps and go to Chapter 5, "Upgrading the ProtecTIER software to 3.4.x from version 3.3.x using ProtecTIER Manager," on page 19

About this task

Procedure

Sign in to ibm.com, find the correct fix package, and download the fix update.

1. Go to www.ibm.com.
2. Click the **Sign in** link in the masthead and log in using your IBM user ID. If you do not have an IBM user ID, follow the procedures to create one from any IBM web page.

Note: If you need help with the login, go to the **Help and FAQ authentication** website: https://www.ibm.com/account/profile/.

3. From the **Home** page, click: **Support**. The IBM Support page opens.
4. Select **Downloads** > **Fix central**.
5. Under **Find product**, type `ProtecTIER` in the **Product selector field** and select **TS7650G Deduplication Gateway (3958-DD1-6) ProtecTIER Enterprise Edition**.
6. Select the appropriate version from the **Installed version** drop-down box. A list of available packages appears.
7. Use the check box to select the package that you want to download, then click **Continue**. The **Download options** menu opens.
8. Click the radio button for **Download using bulk FTP**, select the checkbox next to **include prerequisites and co-requisite fixes** and click **Continue**. The **Terms and Conditions** page opens.
9. Read the information and then click **I agree**.

   Depending on the product you selected, the **Opening PT_MD5_TS7650G_V3.4.x.x.x86_64** dialog box, opens.

   Note: The specific file name will depend on the fix package you are downloading.
10. Select **Save file** and click **OK**.

    The ProtecTIER software fix update downloads to the local hard disk drive.
11. Either record the directory into which the software downloaded, or copy the downloaded `PT_MD5_TS7650G_V3.4.x.x.x86_64` file to a DVD and use this disk to perform the fix update
12. Go to "Applying the V3.4.x fix pack to the ProtecTIER servers".

Applying the V3.4.x fix pack to the ProtecTIER servers

This procedure describes how to upgrade the ProtecTIER code using the service menus.

Before you begin

Ensure that you have completed the steps in "Downloading the ProtecTIER 3.4.x fix pack" on page 43 and saved the update package either to a DVD or to the /install/new directory on Server A.

Upgrading the ProtecTIER code through the graphical user interface in "Upgrading from ProtecTIER 3.3.x to 3.4.x using ProtecTIER Manager on the ProtecTIER servers" on page 20 is the preferred method. Use the steps in this section only if you want to upgrade the ProtecTIER using the service menus.

The terms *update file*, *update package*, and *software package* are used interchangeably in this procedure.

About this task

For the 3958 DD6 neither an external DVD ROM nor the micro HDMI to VGA adapter is part of the IBM ship group. These need to be supplied by the customer.

Procedure

1. If you saved the update package to a DVD in step 12 of "Downloading the ProtecTIER 3.4.x fix pack" on page 43, perform the following substeps:
   a. Insert the DVD into the disk drive tray of Server A.
   b. Close the disk drive tray.
2. Start a session on node A to access the ProtecTIER service menus by using either a direct connection, for example, from the terminal to the server, or for a remote connection, using a software tool like PuTTY and the IP address for the ProtecTIER machine.
3. At the **login** prompt, log in with user name `ptconfig` and password `ptconfig`. Press Enter.
4. At the command prompt, type `menu` and press Enter. The **ProtecTIER Service Menu** is displayed.

```
------------------------------------------------------------------------
  ProtecTIER Service Menu running on rasddx
------------------------------------------------------------------------
   1) ProtecTIER Configuration (...)
   2) Manage ProtecTIER services (...)
   3) Health Monitoring (...)
   4) Problem Alerting (...)
   5) Version Information (...)
   6) Generate a service report
   7) Generate a system view
   8) Update ProtecTIER code
   9) ProtecTIER Analysis (...)

   E) Exit
------------------------------------------------------------------------
>>> Your choice?
```

5. From the main menu, select the numeral corresponding to **Update ProtecTIER code** and press Enter. A message that is similar to the following example is displayed.

```
Begin proessing procedure

Going to extract upgrade package

==================================================================
            ptupgrade V3.4 package
            kernel    2.6.18-238.40.1.el5.x86_64
            PT Build  7133.089
==================================================================

Extracting perl modules...
job 805 at 2013-01-04 20:34
job 806 at 2013-01-04 20:34
Going to start installation GUI process
Checking for available packages:                [ Done ]
```

   If older update packages are found, the system prompts you to delete them if desired.

   If you are not prompted to delete older packages, or after you delete them, output similar to the following example displays

```
Upgrade candidates
1. /install/PT_MD5_TS7650G_V3.4.x.x.x86_64.tar (node 1)
2. /install/PT_TS7650_V3.1.8.0.x86_64.tar (node 2)

Which package do you want to install?  (Press 'q' to quit) :
```

6. Type the numeral corresponding to the update package that you want to install and press Enter. Output similar to the following example displays.

```
Extracting new GUI package from upgrade package                  [ Done ]
Checking prequisites conditions for package                      [ Done ]
Gong to upgrade the package
  /mnt/cdrom/PT_MD5_TS7650G_V3.4.x _64.tar
  (build=7234.035, version=3, release=4, minor=1, fix=0
Upgrade method = SEQUENTIAL
Do you want to continue? (yes|no)
```

7. Enter `yes` to continue. Respond to any prompts as required. The installation starts. In case of dual cluster configuration the installation on the peer node starts automatically. The service menu displays the progress. Here you can see an example on a dual cluster node upgrade.

```
Checking progress:

_____________________________________________________________________________
              Local Node                |              Remote Node
________________________________________|____________________________________
[  6% - The peer node is rebooting   ]  | [ 93% - In the middle of reboot pr...]
```

   When the local node is rebooted it means both nodes were updated successfully. Here you can see an example on a dual cluster node upgrade.

```
Checking progress:

_____________________________________________________________________________
              Local Node                |              Remote Node
________________________________________|____________________________________
[100% - The node will now reboot     ]  | [100% - Code upgrade complete        ]
```

8. When the restart cycle completes, the login: prompt is shown. Check the status of the services on the server or servers on which you updated the code.
   a. At the login prompt, log in to the server on which you updated the code with the user name `ptconfig` and the password `ptconfig`.
   b. At the command prompt, type `menu` and press Enter. The ProtecTIER Service main menu is displayed:

```
--------------------------------------------------------------------------
  ProtecTIER Service Menu running on rasddx
--------------------------------------------------------------------------
   1) ProtecTIER Configuration (...)
   2) Manage ProtecTIER services (...)
   3) Health Monitoring (...)
   4) Problem Alerting (...)
   5) Version Information (...)
   6) Generate a service report
   7) Generate a system view
   8) Update ProtecTIER code
   9) ProtecTIER Analysis (...)

   E) Exit
--------------------------------------------------------------------------
>>> Your choice?
```

   c. Select the option to **Manage ProtecTIER services**. The **Manage ProtecTIER services** menu is displayed.

```
--------------------------------------------------------------------------
  ProtecTIER Service Menu running on rasddx
             Manage ProtecTIER Services (...)
--------------------------------------------------------------------------
   1) Display services status
   2) Start all services
   3) Stop all services
   4) Stop ProtecTIER services only (including GFS)
   5) Stop VTFD service only

   B) Back
   E) Exit
--------------------------------------------------------------------------
>>> Your choice?
```

d. Select the option to **Display services status**.

e. The service status is expected to be UP for all services. If a service status is STILL_LOADING, wait and check the service status again until it changes to UP.

```
Service                  Status
=========================================
cman                     UP
clvmd                    UP
gfs                      UP
vtfd                     STILL_LOADING
ptrasd                   UP
ptconfigd                UP
```

9. Verify the ProtecTIER version on the servers on which you performed the upgrade. Use the ProtecTIER Service menu.

a. From the main ProtecTIER Service menu, select the **Version information** option.

b. The **Version information** menu is displayed.

```
--------------------------------------------------------------------------
 ProtecTIER Service Menu running on rasddx
            Version Information (...)
--------------------------------------------------------------------------
  1) Display version information
  2) Display Machine Reported Product Data (MRPD)
  3) Display Firmware Versions

  B) Back
  E) Exit
--------------------------------------------------------------------------
>>> Your choice?
```

c. Select the **Display version information** option. The ProtecTIER version is shown in the first line of output, in the first three digits after the colon. The version information looks similar to the following message:

```
PT version : 3.4.x
```

If the ProtecTIER fix update version is correct, continue to the next step. If the ProtecTIER version is incorrect, the update has failed. Contact IBM Support for assistance.

10. The code update procedure is now complete.

Updating the ProtecTIER 3958 DD6 Firmware

Complete this task to update the 3958 DD6 Firmware

About this task

Important: The firmware upgrade process connects to the Baseboard Management Controller (BMC) to get firmware information. Therefore, it is mandatory to have the BMC configured with an IP address on the same customer network segment before continuing with the procedure.

Procedure

1. If you are updating a single node configuration, connect a USB keyboard and graphics-capable monitor to the server.
2. If you are updating a clustered configuration, verify that both Server A and Server B are running:
   - **Yes**, continue to step 3
   - **No**, power on any servers that are not running, wait for the boot cycle to complete, and then continue to step 3
3. At the **Login** prompt, type the user ID **ptconfig** and the password **ptconfig** press **<enter>**.

   The **ProtecTIER System Menu** displays:

```
--------------------------------------------------------------------------------
 ProtecTIER Service Menu running on rassmx
--------------------------------------------------------------------------------
  1) ProtecTIER Configuration (...)
  2) Manage ProtecTIER services (...)
  3) Health Monitoring (...)
  4) Problem Alerting (...)
  5) Version Information (...)
  6) Generate a service report
  7) Generate a system view
  8) Update ProtecTIER code
  9) ProtecTIER Analysis (...)

  E) Exit
--------------------------------------------------------------------------------
>>> Your choice?
```

4. Select **Protectier Configuration**. Type the corresponding number and press **<enter>**.

   The **ProtecTIER Configuration (...)** screen displays:

```
--------------------------------------------------------------------------------
 ProtecTIER Service Menu running on rassmx
 ProtecTIER Configuration (...)
--------------------------------------------------------------------------------
  1) Configure ProtecTIER node
  2) Recover Configuration for a replaced server
  3) Configure enclosure serial number for a replaced enclosure
  4) Update Time, Date, Timezone & Timeserver(s)
  5) Configure replication (...)
  6) IP Network configuration (...)
  7) Update Firmware
  8) Update the System's name
  9) Validate configuration
 10) Single node - code upgrade (For Support Use ONLY)

  B) Back
  E) Exit
--------------------------------------------------------------------------------
>>> Your choice?
```

5. Select **Update Firmware**. Type the corresponding number and press **<enter>**.

   The **Update Firmware (...)** screen is displayed:

```
--------------------------------------------------------------------------------
 ProtecTIER Service Menu running on rassmx
            ProtecTIER Configuration (...)
            Update Firmware (...)
--------------------------------------------------------------------------------
  1) Update Server Firmware
  2) Display Firmware Version for BMC and GEM Components
  3) Upgrade Firmware Version for BMC and GEM Components

  B) Back
  E) Exit
--------------------------------------------------------------------------------
>>> Your choice?
```

6. Select Upgrade Firmware Version for BMC and GEM Components. Type the corresponding number and press **<enter>**. The current firmware is checked and if an upgrade is needed, a confirmation message is displayed informing that services will be stopped and 1 or 2 reboots are needed during the upgrade process. Select **Yes** and press **<enter>**. Wait for the process to complete:

```
Your Choice? 3
BeginProcessingProcedure [Jan 30 07:47:33]
Checkcurrent Firmware Versions  [ Done ]
In ordertoupdatetheNode's firmware level, alltheserviceswill be stopped.
The firmware upgradeprocesswill requiere 1 reboot
Do youwanttocontinue? (yes|no) yes
Stoppingptrasd  [ Done ]
Stoppingvtfd  [ Done ]
Stoppingptcluster  [ Done ]
Updating BMC firmware                                [ Done ]
Updating CPLD firmware                               [ Done ]
Updating BIOS firmware                               [ Done ]
Machine will be rebooted
```

7. Once the system is online, run the Update Firmware option again to make sure the process completed. If firmware was upgraded successfully the following message is displayed:

```
Your choice? 3
Begin Processing Procedure [Jan 31 11:25:43]

Check current Firmware Versions                      [ Done ]
All firmware versions are up to date.

End Processing Procedure Successfully [Jan 31 11:25:43]
```

Chapter 10. Recovering from a failed upgrade

Use these procedures to upgrade to ProtecTIER version 3.4.x from version 3.3.x using the ProtecTIER graphical user interface (GUI) or ProtecTIER Service menus.

About this task

See Table 7 for failed code upgrade scenarios and what action to take to recover from a failed upgrade.

To determine whether a code upgrade was successful, check the current ProtecTIER version. To check the current version, enter **cat /opt/dtc/app/sys/verinfo** on the command line and press Enter.

Important: If the code upgrade fails, do not start any of the services manually.

What to do next

Table 7. Actions to take to recover from a failed upgrade

Failed code upgrade scenario	Action
The code upgrade failed on a single node environment.	1. Logon to the ProtecTIER Service menus. 2. From the ProtecTIER Service menu, select **Upgrade ProecTIER code**. 3. Follow the displayed prompts. 4. If your code upgrade fails again, do the following: a. Logon to the ProtecTIER service menus. From the menu, select **Generate a service report**. b. Contact IBM support.
The code upgrade failed in a clustered environment and failed on either Server A or Server B.	1. Logon to the server where you upgraded the code successfully. 2. Do you have access to the GUI? • **Yes.** Logon to the GUI, then from the ProtecTIER GUI, run the code upgrade again. • **No.** Logon to the ProtecTIER service menus. From the menu, select **Upgrade ProecTIER code**. 3. Follow the displayed prompts. 4. If your code upgrade fails again, do the following: a. Logon to the ProtecTIER service menus. From the menu, select **Generate a service report**. b. Contact IBM support.

Table 7. Actions to take to recover from a failed upgrade (continued)

Failed code upgrade scenario	Action
The code upgrade was successful on one server, but the other server is in service mode. **Note:** If a server is in service mode, no call home notifications are sent. To determine whether the server is in service mode, select **Health Monitoring** > **Service Mode** from the ProtecTIER service menu. The condition of the service menu is displayed as enabled or disabled. You will also be prompted to enable or disable the service mode.	1. Logon to the server where you upgraded the code successfully. 2. Logon to the ProtecTIER GUI, then run the code upgrade again. 3. Follow the displayed prompts. 4. If your code upgrade fails again, do the following: a. Logon to the ProtecTIER service menus. From the menu, select **Generate a service report**. b. Contact IBM support.
None of the listed scenarios apply.	1. Contact IBM support and request that the person run the following steps: a. Logon to the ProtecTIER Service menus. b. From the ProtecTIER Service menu, select **Upgrade ProecTIER code** > **Single node - code upgrade (for Support Use Only)**. c. **Attention:** Although the option for **Single node - code upgrade (for Support Use Only)** is available on the service menus, do not attempt to use this option to upgrade the code. Only the IBM support desk personnel can use this option to troubleshoot and resolve the problems with your code upgrade.
When you use the GUI to perform the upgrade, it does not show the progress of the upgrade	1. Use one of the following options to follow the progress of the upgrade • SSH to the machine • Run the upgrade on a single node using the menu.

Appendix A. Company information worksheet

IBM service representatives use the information that is provided on the company information worksheet to customize your IBM storage complex. When you use any of the remote support features, the TSSC sends this information to IBM so an IBM service representative can contact you.

Table 8. Company information worksheet

Required information	Description	Your information
Business company name	The full name of your company. IBM service representatives use this information to identify your company when they receive Call Home reports from your IBM storage system. Ensure that the company name provided is consistent with all other machines that correspond to your IBM customer account.	
Customer number	The IBM-assigned customer number for your company. This is provided by the customer.	
Country code	The two-character code that must be used in order to reach your country by phone or fax, from another country. This is **not** the three-digit RETAIN country code. See Table 9 on page 54.	
SMTP Server ID / IP address		
SMTP email address	The email address of the administrator who receives failure alerts for the server. This may or may not be the administrator listed below.	
System administrator information Provide information about your storage system administrator in the following section.		
Administrator name	The name of the individual at your site who IBM service representatives should contact about IBM storage system service matters.	
Administrator email address	The storage system administrator's email address.	
Voice phone number	The primary telephone number that IBM service representatives should use to contact the storage system administrator. Include the area code and the country code, if appropriate.	
Fax number	The primary fax number that IBM service representatives should use to fax documents to the storage system administrator. Include the area code and the country code, if appropriate.	

Table 8. Company information worksheet (continued)

Required information	Description	Your information
Alternate fax number	An alternate fax number that IBM service representatives can use to fax documents to the storage system administrator. Include the area code and the country code, if appropriate.	
Administrator mailing address	The postal mailing address for the storage system administrator. provide the full street address, building (if appropriate), city or locality, state or province, and postal or zip code.	
Storage system information Provide basic information about your storage system and the TSSC in the following section.		
Machine location	The address of the facility where the TS7650 server(s) reside. If different from the administrator mailing address above, provide the full street address, building (if appropriate), city or locality, state or province, and postal or zip code.	
Call back phone number	The phone number of the modem being used for Call Home. Include the area code and the country code, if appropriate.	
Disk array machine type(s) and model number(s)	The machine type(s) and model number(s) for the attached disk array storage subsystem(s). For non-IBM equipment, also provide vendor name(s). Use an additional sheet if necessary.	
Disk array serial number(s)	The serial number(s) for the attached disk array storage subsystem(s).	

Use the information in the following table to convert a country to a code, and use that code as an entry in the **Country code** field of the Table 8 on page 53.

Table 9. Country codes

Country	Code	Country	Code	Country	Code	Country	Code	Country	Code
Afghanistan	af	Cook Islands	ck	Iceland	is	Nauru	nr	Solomon Islands	sb
Albania	al	Costa Rica	cr	India	in	Nepal	np	Somalia	so
Algeria	dz	Croatia	hr	Indonesia	id	Netherlands	nl	South Africa	za
American Samoa	as	Cuba	cu	Iran	ir	Netherlands Antilles	an	South Korea	kr
Andorra	ad	Cyprus	cy	Iraq	iq	Neutral Zone	nt	Spain	es
Angola	ao	Czech Republic	cz	Ireland	ie	New Caledonia (French)	nc	Sri Lanka	lk
Anguilla	ai	Denmark	dk	Israel	il	New Zealand	nz	Sudan	sd
Antarctica	aq	Djibouti	dj	Italy	it	Nicaragua	ni	Suriname	sr
Antigua and Barbuda	ag	Dominica	dm	Ivory Coast (Cote D'Ivoire)	ci	Niger	ne	Svalbard and Jan Mayen Islands	sj

Table 9. Country codes (continued)

Country	Code	Country	Code	Country	Code	Country	Code	Country	Code
Argentina	ar	Dominican Republic	do	Jamaica	jm	Nigeria	ng	Swaziland	sz
Armenia	am	East Timor	tp	Japan	jp	Niue	nu	Sweden	se
Aruba	aw	Ecuador	ec	Jordan	jo	Norfolk Island	nf	Switzerland	ch
Australia	au	Egypt	eg	Kazakhstan	kz	North Korea	kp	Syria	sy
Austria	at	El Salvador	sv	Kenya	ke	Northern Mariana Islands	mp	Tadjikistan	tj
Azerbaidjan	az	Equatorial Guinea	gq	Kiribati	ki	Norway	no	Taiwan	tw
Bahamas	bs	Eritrea	er	Kuwait	kw	Oman	om	Tanzania	tz
Bahrain	bh	Estonia	ee	Kyrgyzstan	kg	Pakistan	pk	Thailand	th
Bangladesh	bd	Ethiopia	et	Laos	la	Palau	pw	Togo	tg
Barbados	bb	Falkland Islands	fk	Latvia	lv	Panama	pa	Tokelau	tk
Belarus	by	Faroe Islands	fo	Lebanon	lb	Papua New Guinea	pg	Tonga	to
Belgium	be	Fiji	fj	Lesotho	ls	Paraguay	py	Trinidad and Tobago	tt
Belize	bz	Finland	fi	Liberia	lr	Peru	pe	Tunisia	tn
Benin	bj	Former Czechoslovakia	cs	Libya	ly	Philippines	ph	Turkey	tr
Bermuda	bm	Former USSR	su	Liechtenstein	li	Pitcairn Island	pn	Turkmenistan	tm
Bhutan	bt	France	fr	Lithuania	lt	Poland	pl	Turks and Caicos Islands	tc
Bolivia	bo	France (European Territory)	fx	Luxembourg	lu	Polynesia (French)	pf	Tuvalu	tv
Bosnia-Herzegovina	ba	French Guyana	gf	Macau	mo	Portugal	pt	Uganda	ug
Botswana	bw	French Southern Territories	tf	Macedonia	mk	Puerto Rico	pr	Ukraine	ua
Bouvet Island	bv	Gabon	ga	Madagascar	mg	Qatar	qa	United Arab Emirates	ae
Brazil	br	Gambia	gm	Malawi	mw	Reunion (French)	re	United Kingdom	uk
British Indian Ocean Territory	io	Georgia	ge	Malaysia	my	Romania	ro	United States of America	us
Brunei Darussalam	bn	Germany	de	Maldives	mv	Russian Federation	ru	Uruguay	uy
Bulgaria	bg	Ghana	gh	Mali	ml	Rwanda	rw	USA Minor Outlying Islands	um
Burkina Faso	bf	Gibraltar	gi	Malta	mt	S. Georgia & S. Sandwich Isls.	gs	Uzbekistan	uz
Burundi	bi	Great Britain	gb	Marshall Islands	mh	Saint Helena	sh	Vanuatu	vu
Cambodia	kh	Greece	gr	Martinique (French)	mq	Saint Kitts & Nevis Anguilla	kn	Vatican City State	va

Table 9. Country codes (continued)

Country	Code	Country	Code	Country	Code	Country	Code	Country	Code
Cameroon	cm	Greenland	gl	Mauritania	mr	Saint Lucia	lc	Venezuela	ve
Canada	ca	Grenada	gd	Mauritius	mu	Saint Pierre and Miquelon	pm	Vietnam	vn
Cape Verde	cv	Guadeloupe (French)	gp	Mayotte	yt	Saint Tome (Sao Tome) and Principe	st	Virgin Islands (British)	vg
Cayman Islands	ky	Guam (USA)	gu	Mexico	mx	Saint Vincent & Grenadines	vc	Virgin Islands (USA)	vi
Central African Republic	cf	Guatemala	gt	Micronesia	fm	Samoa	ws	Wallis and Futuna Islands	wf
Chad	td	Guinea	gn	Moldavia	md	San Marino	sm	Western Sahara	eh
Chile	cl	Guinea Bissau	gw	Monaco	mc	Saudi Arabia	sa	Yemen	ye
China	cn	Guyana	gy	Mongoliar	mn	Senegal	sn	Yugoslavia	yu
Christmas Island	cx	Haiti	ht	Montserrat	ms	Seychelles	sc	Zaire	zr
Cocos (Keeling) Islands	cc	Heard and McDonald Islands	hm	Morocco	ma	Sierra Leon	sl	Zambia	zm
Colombia	co	Honduras	hn	Mozambique	mz	Singapore	sg	Zimbabwe	zw
Comoros	km	Hong Kong	hk	Myanmar	mm	Slovak Republic	sk		
Congo	cg	Hungary	hy	Namibia	na	Slovenia	si		

Appendix B. Checking the ProtecTIER version for servers at ProtecTIER version 3.1.8 or higher

This appendix describes several ways to check the ProtecTIER version on a ProtecTIER server using the command line interface (CLI), the service menu or the graphical user interface (GUI). After you obtain the ProtecTIER version, verify that the package that you are applying is a higher version than the currently installed ProtecTIER version.

Using the CLI to check the ProtecTIER version

Procedure

Perform this procedure on each server for which you need version information. Make note of the ProtecTIER version for each server to verify that the fix update you are applying is a higher version of ProtecTIER than the version currently installed.

1. Use ssh to log onto the server that you are updating. At the login prompt, log in with the ID `root` and the default password `admin`.
2. On the command prompt enter the following command: **`verinfo`**

   The ProtecTIER version is shown in the first line of the output, in the digits after the colon. The version information looks like the following example:

   ```
   ProtecTIER version : 3.4.x.x
   ```

Using the service menu to check the ProtecTIER version

Procedure

Perform this procedure on each server for which you need version information. Make note of the ProtecTIER version for each server to verify that the fix update you are applying is a higher version of ProtecTIER than the version currently installed.

1. Use ssh to long onto the server that you are updating with the ID `ptconfig` and the default password `ptconfig`. The main **ProtecTIER Service Menu** is displayed.

   ```
   --------------------------------------------------------------------------
     ProtecTIER Service Menu running on rasddx
   --------------------------------------------------------------------------
      1) ProtecTIER Configuration (...)
      2) Manage ProtecTIER services (...)
      3) Health Monitoring (...)
      4) Problem Alerting (...)
      5) Version Information (...)
      6) Generate a service report
      7) Generate a system view
      8) Update ProtecTIER code
      9) ProtecTIER Analysis (...)

      E) Exit
   --------------------------------------------------------------------------
   >>> Your choice?
   ```

2. From the main **ProtecTIER Service menu**, select the **Version information...** option. The **Version information** menu opens.

```
------------------------------------------------------------------------
 ProtecTIER Service Menu running on rasddx
            Version Information (...)
------------------------------------------------------------------------
  1) Display version information
  2) Display Machine Reported Product Data (MRPD)
  3) Display Firmware Versions

  B) Back
  E) Exit
------------------------------------------------------------------------
>>> Your choice?
```

3. Select the **Display version information (...)** option. The ProtecTIER version is shown in the first line of the output, in the digits after the colon. The version information looks like the following example:

   ```
   ProtecTIER version : 3.4.x.x
   ```

Using the GUI to check the ProtecTIER version

Procedure

Perform this procedure on each server for which you need version information. Make note of the ProtecTIER version for each server to verify that the fix update you are applying is a higher version of ProtecTIER than the version currently installed.

1. Start the ProtecTIER Manager.
2. From the **Select a system** drop down box, select the repository on which you want to check the ProtecTIER version.
3. Log in to the server that you selected by using any of the following userIDs and default passwords:
   - `ptadmin` (default password `ptadmin`)
   - `ptoper` (default password `ptoper`
   - `ptuser` (default password `ptuser`)
4. Use the cursor to select a ProtecTIER server on the repository (the GUI menus are contextual, so in order to enable the next step, you have to select a ProtecTIER server).
5. From the GUI menu, select **Node > Show version information**. This action displays a message box, and the ProtecTIER version is shown in the first line as Release version. The version information looks like the following example:

   ```
   Release version : 3.4.x.x
   ```

Appendix C. TS7600 Upgrade Matrix

This topic provides new installation and upgrade information for all releases.

Table 10. New installation compatibility

New installation*					
Configuration / Version	**3.1**	**3.1.8, 3.1.9, 3.1.10**	**3.2**	**3.3**	**3.4**
DD3[2, 6]	No	Yes[4]	Yes[4]	Yes[9]	No
DD4 VTL	Yes[4]	Yes[4]	Yes[4]	Yes	Yes[7]
DD4 OST	Yes[4]	Yes[4]	Yes[4]	Yes	No
DD5 VTL	No	No	Yes	Yes	Yes
DD5 OST	No	No	Yes	Yes	No
DD5 FSI	No	No	Yes	Yes	Yes
SM1VTL	Yes	Yes	Yes	Yes	No
SM1 OST	No	No	No	Yes	No
SM2 VTL	No	No	Yes	Yes	No
SM2 OST	No	No	Yes	Yes	No
SM2 FSI	No	No	Yes	Yes	Yes
AP1 DD3 VTL[6]	No	Yes[4]	Yes[4]	Yes[9]	No
AP1 DD4 VTL	Yes[4]	Yes[4]	Yes[4]	Yes	No
AP1 DD4 OST	Yes[4]	Yes[4]	Yes[4]	Yes	No
Generic	Yes[3, 4]	Yes[3, 4]	Yes[3, 4]	Yes	No

Table 11. Upgrade compatability

Upgrade to version*					
Configuration / Version	**3.1**	**3.1.8, 3.1.9, 3.1.10**	**3.2**[5]	**3.3**	**3.4**[7]
DD3[8]	Yes (must upgrade to 2.4 or 2.5 previously)[1]	Yes (must upgrade to 2.4, 2.5, or 3.1 previously)	Yes (must upgrade to 2.4, 2.5, 3.1, or 3.1.8 previously)	Yes (must upgrade to 3.1.8 previously)	No
DD4 VTL	Yes	Yes	Yes	Yes (must upgrade to 3.1.8 previously)	Yes (must upgrade to 3.3.x previously)
DD4 OST	Yes	Yes	Yes	Yes (must upgrade to 3.1.8 previously)	No
DD5 VTL	No	No	DD5 only used from 3.2	Yes	Yes (must upgrade to 3.3 previously)
DD5 OST	No	No	DD5 only used from 3.2	Yes	No

Table 11. Upgrade compatability (continued)

	Upgrade to version*				
DD5 FSI	No	No	DD5 only used from 3.2, FSI released only from 3.2	Yes	Yes (must upgrade to 3.3 previously)
SM1 VTL	Yes (must upgrade to 2.5 previously)	Yes (must upgrade to 2.5 or 3.1 previously)	Yes (must upgrade to 2.5, 3.1, or 3.1.8 previously)	Yes (must upgrade to 3.1.8 previously)	No
SM1 OST	Yes	Yes	Yes	Yes (must upgrade to 3.1.8 previously)	No
SM2 VTL	No	No	SM2 used only from 3.2	Yes	Yes (must upgrade to 3.3 previously)
SM2 OST	No	No	SM2 used only from 3.2	Yes	No
SM2 FSI	No	No	SM2 used only from 3.2	Yes	Yes (must upgrade to 3.3 previously)
AP1 DD3 VTL	Yes (must upgrade to 2.4 or 2.5 previously)[1]	Yes (must upgrade to 2.4, 2.5, or 3.1 previously)	Yes (must upgrade to 2.4, 2.5, 3.1, or 3.1.8 previously)	Yes (must upgrade to 3.1.8 previously)	No
AP1 DD4 VTL	Yes	Yes	Yes	Yes (must upgrade to 3.1.8 previously)	No
AP1 DD4 OST	Yes	Yes	Yes	Yes (must upgrade to 3.1.8 previously)	No
Generic	Yes (must upgrade to 2.4 or 2.5 previously)[3]	Yes (must upgrade to 2.4, 2.5, or 3.1 previously)[3]	Yes (must upgrade to 2.4, 2.5, 3.1, or 3.1.8 previously)[3]	Yes (must upgrade to 3.1.8 previously)	No

Note:

* In general, use the latest released version as installation issues might have been resolved.

1. RAS cannot be configure on DD3 in 2.5 or 3.1. Either configure RAS on 2.4 before upgrading to a higher version , or upgrade to 3.1.8 or higher and then configure RAS.
2. It is recommended to create repositories under 2.4.
3. Qualified Emulex HBA cards must be provided as per Support Matrix.
4. Use the **ptconfig** (not "menu" but manual ptconfig) option -oldclusterkit when using the old cluster kit on 3.1 and newer versions (FC 3447).
5. The 3.1.8 column in the above tables represents all codes from 3.1.8 and higher (3.1G versions), which are lower than 3.2.

6. ProtecTIER code 3.1.8 or higher requires an upgrade to Red Hat OS version 5.6.
7. ProtecTIER code 3.4 or higher requires an upgrade to Red Hat OS version 5.11.
8. OST isn't supported on DD3, only VTL.
9. The 3958 AP1 appliance or the 3958 DD3 gateway server require a memory upgrade (64GB RAM) to upgrade to ProtecTIER V3.3.x when your system exceeds any of these configuration values.
   a. Installed physical storage greater than 300TB
   b. More than 64 virtual drives
   c. There are 8 or more paths per LUN

General Considerations

Observe the following considerations when upgrading ProtecTIER code.

- Use the latest versions as recommended and available on Fix Central.
- Run the Grid Manager on the ProtecTIER server with the higher code level.
- Ensure that the ProtecTIER Manager level is higher than, or equal to, the ProtecTIER code level where the Grid Manager is running.
- The recommendation to upgrade 3958 DD4 or 3958 DD5 systems to ProtecTIER v3.4.x is to install ProtecTIER v3.3.7.0 first.
- ProtecTIER v3.4.2.0 is not supported for node replacements, use instead a higher version from Fix Central. For more references and information check the iRPQ 8B3667 (DD3 to DD6) and iRPQ 8B3668 (DD4/DD5 to DD6) in the IBM Knowledge Center.
- OST is not supported on ProtecTIER v3.4.
- ProtecTIER v3.4 does not support DD3, AP1 DD3, or AP1 DD4 servers.

Accessibility for publications and ProtecTIER Manager

The publications for this product are in Adobe Portable Document Format (PDF) and should be compliant with accessibility standards. Use these procedures to enable screen-reader compatibility, change the Windows contrast setting, and customize the color palette used in ProtecTIER Manager.

About this task

If you experience difficulties when you use the PDF files and want to request a Web-based format for a publication, send your request to the following address:

International Business Machines Corporation
Information Development
Department GZW
9000 South Rita Road
Tucson, Arizona 85744-001 U.S.A

In the request, be sure to include the publication number and title. When you send information to IBM, you grant IBM a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

About the Windows-based accessibility features

About this task

The accessibility features in ProtecTIER Manager help persons with limited vision use the ProtecTIER Manager installation wizard and software. After preparing the ProtecTIER Manager workstation for accessibility, you can use Windows-based screen-reader software and a digital voice synthesizer to hear what is displayed on the screen.

The installation, configuration, and instructional screens in the Windows versions of the ProtecTIER Manager installation wizard and the ProtecTIER Manager software have been tested with Job Access with Speech (JAWS). However, the associated diagrams and graphs in ProtecTIER Manager and ProtecTIER Replication Manager, do not currently support keyboard navigation or screen-reader use. You can obtain full system statistics (typically provided in the diagrams and graphs) by going to the ProtecTIER Manager toolbar and clicking: **Reports** > **Create long term statistics report**, and downloading the results.

To enable screen-reader compatibility, you must prepare the ProtecTIER Manager workstation by completing these tasks. Instructions are provided in the topics that follow:

Before you install ProtecTIER Manager:

- Download and install the Java Runtime Environment (JRE).
- Download and install the Java Access Bridge (JAB).

After you install ProtecTIER Manager:

- Change the ProtecTIER Manager preferences to enable support of the Windows system settings *(required)*.
- Select a high-contrast color scheme in Windows *(optional)*.
- Customize the color palette used in the ProtecTIER Manager display *(optional)*.

About the Java-based tools

About this task

Complete the following procedures to download and install the Java-based tools that are required to enable full screen-reader compatibility on the ProtecTIER Manager workstation.

Install the Java™ Runtime Environment (JRE) first, and then install the Java Access Bridge (JAB). Both of these tools must be installed before you install the ProtecTIER Manager software.

For simplicity, download the Java-based tools by using the ProtecTIER Manager workstation on which you are installing the JRE and JAB. If this is not possible, try to use another computer that is running Windows.

Installing the Java Runtime Environment

About this task

The JRE includes the Java Virtual Machine (JVM). These tools are necessary for your computer to run Java-based applications.

Procedure

1. Go to http://www.java.com. The Java website opens.

   The java.com website auto-detects the operating system and Internet browser of the computer you use when you access the site.
2. Click **Free Java Download**, and proceed as appropriate:
   - If the **Download Java for Windows** page opens, go on to step 3
   - If the **Download Java for...** page title contains the name of an operating system other than Windows, do the following:
     a. Click the **See all downloads here** link.

        The list of available downloads, categorized by operating system, displays.
     b. In the Windows section, click **Windows 7/XP/Vista/2000/2003/2008 Online**.
3. Review the information provided, and then click **Agree and Start Free Download**.

   The download dialog box opens.
4. Follow the on-screen instructions to save the executable (.exe) installer file to the hard disk drive.
5. After the download is complete, find the installer file on the hard disk drive and write down the full path to the location of the file. For example: *C:\Program Files\Java\jre6\bin\java.exe*. This path is needed during ProtecTIER Manager installation.
6. Proceed as appropriate:

- If you downloaded the installer on the ProtecTIER Manager workstation on which you are installing the JRE, go on to step 7.
- If you downloaded the installer on a PC other than the applicable ProtecTIER Manager workstation, do the following:
  a. Copy the installer file onto a CD, flash memory drive, or other form of removable media.
  b. Copy the installer file from the removable media to the hard disk drive of the ProtecTIER Manager workstation.
  c. Go on to step 7.

7. Double-click the installer file to start the **Java installation wizard**.

   The **Java Setup – Welcome** window opens.
8. Click **Install** and follow the on-screen instructions to complete the installation process.
9. When you have successfully installed the JRE, go on to "Installing the Java Access Bridge."

Installing the Java Access Bridge

About this task

The Java Access Bridge (JAB) makes it possible for you to use Java-based screen readers with the ProtecTIER Manager installation wizard and software.

Procedure

1. Go to: http://www.oracle.com/technetwork/java/javase/tech/index-jsp-136191.html.

   The **Java SE Desktop Accessibility** page of the Oracle website opens.
2. Read the information provided, then click **Access Bridge**.
3. Scroll down to the **Java Access Bridge for Microsoft Windows Operating System x.x.x** (where *x.x.x* is the most recent version listed) section. Click the **Download Java Access Bridge x.x.x** link.

   The **Software License Agreement** page opens.
4. Read the license agreement, and then select the **I agree to the Software License Agreement** check box.

   The **Download Java Access Bridge for Windows Operating System x.x.x** page opens.
5. In the **Required Files** list, click the link to download the **Access Bridge x.x.x, accessbridge-x.x.x.exe** file.

   The download dialog box opens.
6. Follow the on-screen instructions to save the executable (.exe) installer file to the hard disk drive.
7. When the download is complete, locate the installer file on the hard disk drive and proceed as appropriate:
   - If you downloaded the installer by using the ProtecTIER Manager workstation on which you are installing the JAB, go on to step 8 on page 66.
   - If you downloaded the installer by using a PC other than the applicable ProtecTIER Manager workstation, do the following:
     a. Copy the installer file onto a CD, flash memory drive, or other removable media device.

b. Copy the installer file from the removable media device to the hard disk drive of the ProtecTIER Manager workstation.
c. Go on to step 8.

8. On the ProtecTIER Manager workstation, double-click the **accessbridge-x.x.x.exe** installer file.

   A security warning dialog box displays.

9. Click **Run**.

   The **Java Access Bridge – InstallShield Wizard** opens.

10. Read the welcome information, then click **Next** and follow the on-screen instructions to complete the installation.
11. When the installation is complete, restart the workstation as directed.

    You now have the necessary Java tools for compatibility between the ProtecTIER Manager installation wizard and screen reader software.

12. Follow the instructions in "Using a screen reader to install ProtecTIER Manager" to start the ProtecTIER Manager installation wizard by using a screen reader.

Using a screen reader to install ProtecTIER Manager

About this task

Install ProtecTIER Manager according to the following command line-based instructions.

When entering the commands, type them exactly as shown, including any spaces or quotation marks. Any deviation in the procedure can cause the installation to start in the non-accessible mode, or fail completely.

Procedure

1. If your workstation is configured to automatically open DVDs, temporarily disable the Windows **AutoPlay** feature for the CD/DVD device. Use the Windows Help or other Windows documentation for instructions, and then go on to step 2.
2. Insert the *IBM ProtecTIER Manager DVD* into the CD/DVD drive of the ProtecTIER Manager workstation.
3. Access the command prompt on the ProtecTIER Manager workstation:
   a. Click **Start** > **Run...**.

      The **Run** dialog box opens.

4. In the **Open** field, type: **cmd** and click **Ok**.

   The command window opens.

5. Browse to the ProtecTIER Manager installation directory on the DVD. To do so:
   a. At the command prompt, type: **D:** (where D: is the letter assigned to the CD/DVD drive of the workstation) and press **<enter>**.
   b. At the command prompt, list the contents of the DVD. Type: **dir** and press **<enter>**.
   c. Locate the name of the ProtecTIER Manager directory on the DVD. For example: *PT_Manager_V3.3*.
   d. At the command prompt, change to the **ProtecTIER Manager** directory. Type: **cd <directory name>** and press **<enter>**. For example: `cd PT_Manager_V3.3` **<enter>.**

e. At the command prompt, change to the **Windows** directory. Type: **cd windows** and press **<enter>**.

f. At the command prompt, type: **Install.exe LAX_VM "C:\Program Files\Java60\jre\bin\java.exe"** and press **<enter>**, where the path contained within the quotation marks is the same as the path that you noted in step 5 on page 64.

The screen-reader-enabled ProtecTIER Manager installation wizard starts.

g. Follow the spoken prompts to compete the installation.

6. When the installation completes, proceed as appropriate:
   - If you **do not** want to enable the Windows High Contrast option or customize the color palette, resume your regular use of ProtecTIER Manager.
   - To change the contrast mode for ProtecTIER Manager, go to "Enabling the Windows High Contrast option." To customize the color palette, go to "Customizing the color palette" on page 71.

Enabling the Windows High Contrast option

About this task

To make it possible for ProtecTIER Manager to display in high contrast, you must first enable the **Use High Contrast** option in Windows.

Procedure

1. On the ProtecTIER Manager workstation, go to **Windows** > **Control Panel** > **Accessibility Options**.

   The **Accessibility Options** dialog box opens.

2. Select the **Display** tab.
3. In the **High Contrast** area of the **Display** tab, select the **Use High Contrast** check box, as shown in Figure 9 on page 68:

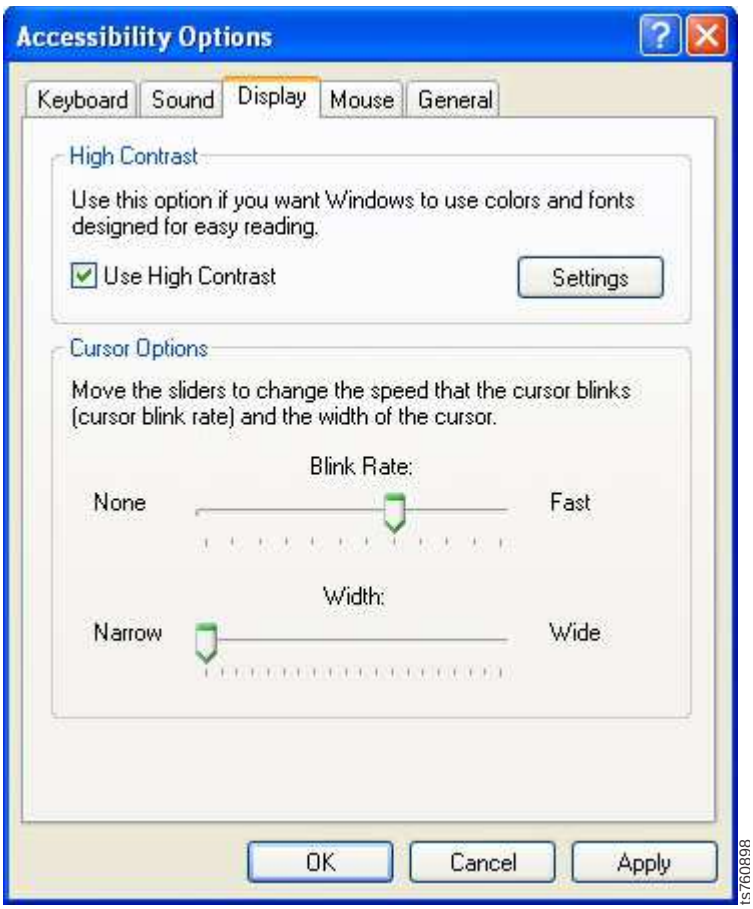


Figure 9. Display tab

4. Click **Settings**.

   The **Settings for High Contrast** dialog box displays, as shown in Figure 10 on page 69:

Figure 10. Settings for High Contrast

By default, the **High Contrast Black (large)** scheme is selected.

5. Do one of the following:
   - To use the default, **High Contrast Black (large)**, scheme:
     a. Click **Ok** to close the **Settings for High Contrast** dialog box.
     b. Click **Ok** to close the **Accessibility Options** dialog box.
        After a few moments, the display changes to the new color scheme.
     c. Go on to "Using the Windows high contrast scheme with ProtecTIER Manager."
   - To use a different high contrast scheme:
     a. Click the arrow to show the list of available color schemes.
     b. Select the high contrast scheme that you want to use.
     c. Click **Ok** to close the **Settings for High Contrast** dialog box.
     d. Click **Ok** to close the **Accessibility Options** dialog box.
        After a few moments, the display changes to the new color scheme.
     e. Go on to "Using the Windows high contrast scheme with ProtecTIER Manager."

Using the Windows high contrast scheme with ProtecTIER Manager

About this task

Now that you have changed the contrast scheme in Windows, you must enable the **Support system settings** option in ProtecTIER Manager.

Procedure

1. Launch **ProtecTIER Manager**:

a. Click: **Start** > **All Programs** > **IBM** > **ProtecTIER Manager** > **IBM ProtecTIER Manager**.

The ProtecTIER Manager window opens, as shown in: Figure 11.

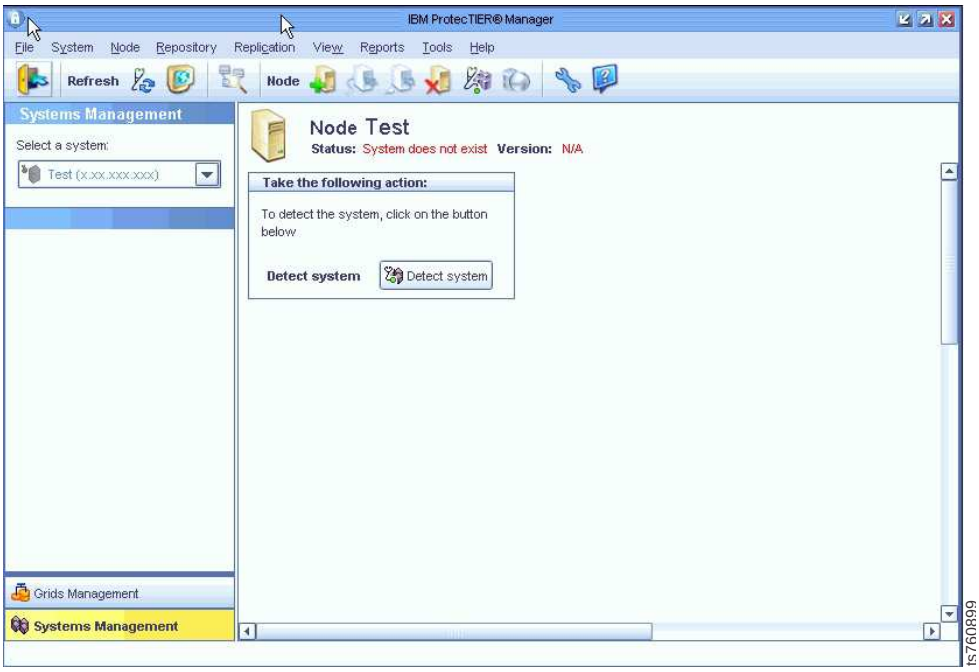


Figure 11. ProtecTIER Manager window

2. On the toolbar, click: **Tools** > **Preferences**.

   The **Preferences** dialog box opens with the **Appearance** tab selected, as shown in Figure 12:

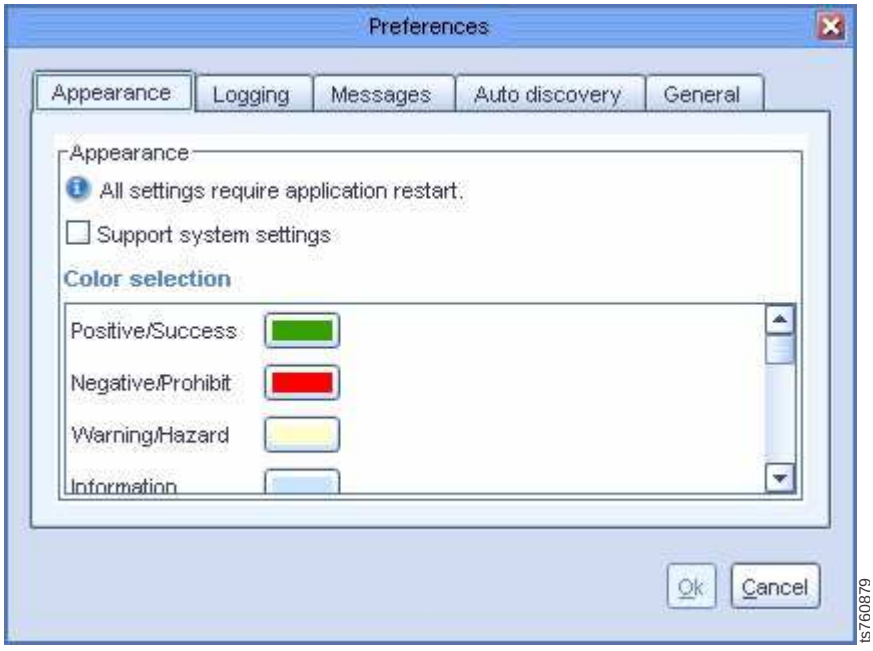


Figure 12. Preferences dialog box

3. On the **Appearance** tab, select the **Support system settings** check box.
   You are returned to the **ProtecTIER Manager** window.
4. Exit and restart ProtecTIER Manager so the contrast settings take effect:
   a. On the **ProtecTIER Manager** toolbar, click: **File** > **Exit**.
      The **ProtecTIER Manager** window closes.
   b. Click: **Start** > **All Programs** > **IBM** > **ProtecTIER Manager** > **IBM ProtecTIER Manager**.
      When the ProtecTIER Manager window opens, the display reflects the contrast change, as shown in: Figure 13.

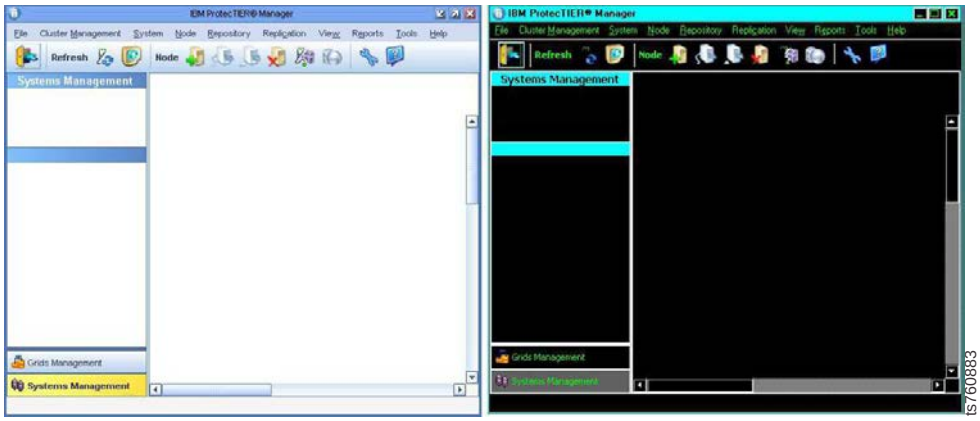


Figure 13. Normal contrast versus high contrast

5. Proceed as appropriate:
   - If you want to change one or more of the colors used in the ProtecTIER Manager display, continue to "Customizing the color palette."
   - If you **do not** want to customize the color palette, resume your regular use of ProtecTIER Manager.

Customizing the color palette

About this task

Use this procedure to customize the color palette for ProtecTIER Manager to improve visibility in the display, or to suit your personal preferences.

Procedure

1. If necessary, start ProtecTIER Manager as described in step 1 on page 69.
2. Open the **Preferences** dialog box, as described in 2 on page 70.
3. Scroll down (if necessary) to see the entire **Color selection** list, and then select the color you want to change.
   The **Color selection** dialog box opens, with the **Swatches** tab selected, as shown in Figure 14 on page 72:

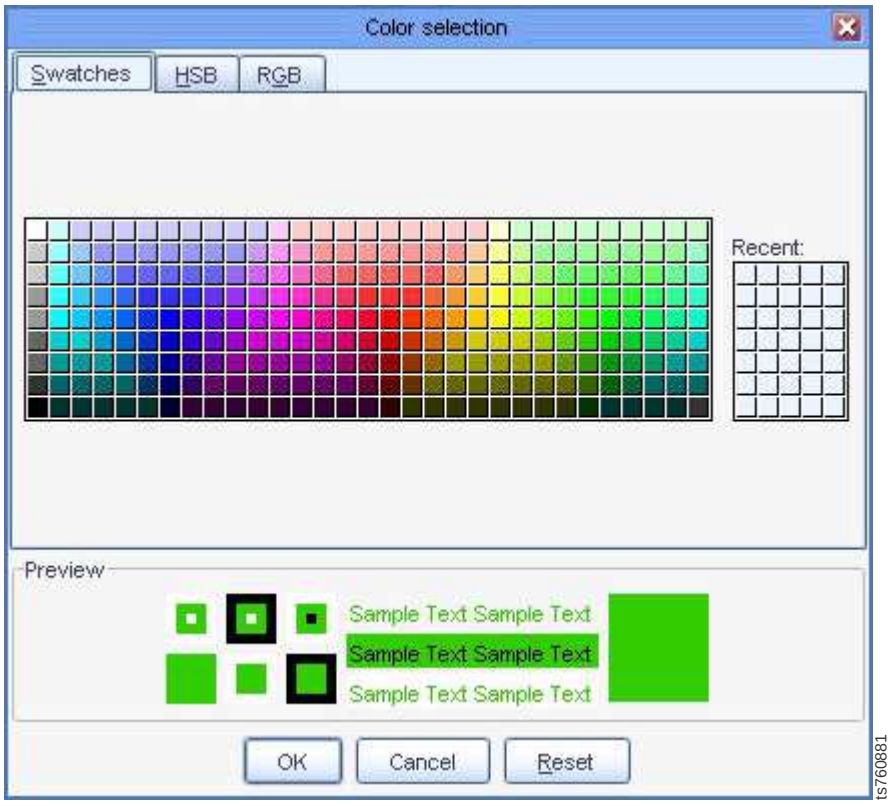


Figure 14. Color selection, Swatches tab

The color that is currently defined for your selection is shown in the **Preview** pane.

4. Select a new color from the color palette.

   You can also specify a new color by using the Hue/Saturation/Brightness (HSB) or Red/Green/Blue (RGB) color models. To do so, click the tab for the model you want to use and enter the required values.

5. When you have finished selecting or specifying the new color, click **Ok**.

   You are returned to the **Appearance** tab.

6. To change another color, repeat steps 3 on page 71 through 5.
7. When you are finished making changes in the **Appearance** tab, click **Ok**.

   You are returned to the ProtecTIER Manager window.

8. Exit and restart ProtecTIER Manager (as described in step 4 on page 71) so the color palette changes take effect.

   After you log in to ProtecTIER Manager and add a node, the display reflects your custom color selections.

   An example of the default color versus a custom color for **Allocable** resources, is shown in: Figure 15 on page 73

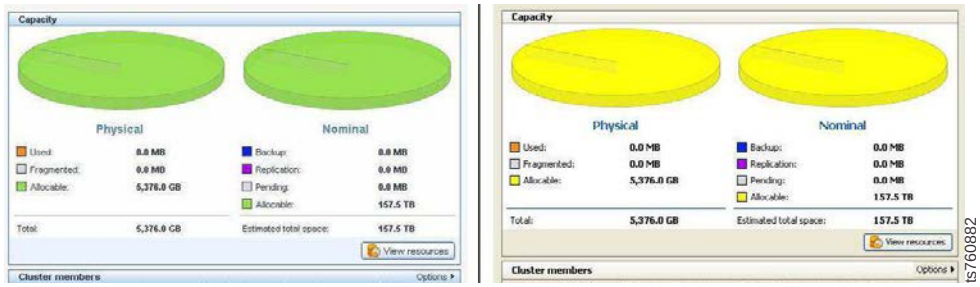


Figure 15. Default color versus custom color

9. Proceed as appropriate. Return to the task from which you were sent to these instructions or resume your regular use of ProtecTIER Manager.

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.

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 PUBLICATIONS "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 may not apply to you.

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

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

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

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been

estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

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

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

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

Red Hat Notice

IBM delivers patches (including security fixes) for Red Hat Enterprise Linux (RHEL) based on the Red Hat Enterprise Linux Life Cycle policy. As stated in the Red Hat policy, fixes are not provided for all vulnerabilities on all RHEL versions, which means that IBM cannot deliver security fixes for some RHEL issues.

When security and other related updates are available from Red Hat, IBM delivers those updates in software packages that can be downloaded and applied to ProtecTIER. IBM may also publish Security Bulletins with additional information for security related updates. Customers should subscribe to My Notifications to be notified of important ProtecTIER support alerts.

Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

- AIX®
- DS4000®
- Enterprise Storage Server®
- ESCON
- FICON®
- i5/OS™
- iSeries
- IBM
- ProtecTIER
- pSeries
- S/390®
- ServeRAID
- System x

- System Storage
- TotalStorage
- Wake on LAN
- z/OS®
- zSeries

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol ((R) or (TM)), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at http://www.ibm.com/legal/copytrade.shtml.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Java and all Java-based trademarks are trademarks of Oracle, Inc. in the United States, other countries, or both.

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

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

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

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

Red Hat is a registered trademark of Red Hat, Inc. in the United States, other countries, or both.

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

Electronic emission notices

This section contains the electronic emission notices or statements for the United States and other regions.

Federal Communications Commission statement

This explains the Federal Communications Commission's (FCC) statement.

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is

operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, might cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. IBM is not responsible for any radio or television interference caused by using other than recommended cables and connectors, or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device might not cause harmful interference, and (2) this device must accept any interference received, including interference that might cause undesired operation.

Industry Canada compliance statement

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conform à la norme NMB-003 du Canada.

European Union Electromagnetic Compatibility Directive

This product is in conformity with the protection requirements of European Union (EU) Council Directive 2004/108/EC on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the fitting of non-IBM option cards.

Attention: This is an EN 55022 Class A product. In a domestic environment this product might cause radio interference in which case the user might be required to take adequate measures.

Responsible Manufacturer:

International Business Machines Corp.
New Orchard Road
Armonk, New York 10504
914-499-1900

European community contact:

IBM Deutschland GmbH
Technical Regulations, Department M372
IBM-Allee 1, 71139 Ehningen, Germany
Tele: +49 7032 15 2941
e-mail: lugi@de.ibm.com

Australia and New Zealand Class A Statement

Attention: This is a Class A product. In a domestic environment this product might cause radio interference in which case the user might be required to take adequate measures.

Germany Electromagnetic compatibility directive

Deutschsprachiger EU Hinweis: Hinweis für Geräte der Klasse A EU-Richtlinie zur Elektromagnetischen Verträglichkeit

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2004/108/EG zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der EN 55022 Klasse A ein.

Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von der IBM empfohlene Kabel angeschlossen werden. IBM übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung der IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung der IBM gesteckt/eingebaut werden.

EN 55022 Klasse A Geräte müssen mit folgendem Warnhinweis versehen werden:

"Warnung: Dieses ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funk-Störungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Mabnahmen zu ergreifen und dafür aufzukommen."

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

Dieses Produkt entspricht dem "Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG)." Dies ist die Umsetzung der EU-Richtlinie 2004/108/EG in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) (bzw. der EMC EG Richtlinie 2004/108/EG) für Geräte der Klasse A

Dieses Gerät ist berechtigt, in übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen.

Verantwortlich für die Einhaltung der EMV Vorschriften ist der Hersteller:

International Business Machines Corp.
New Orchard Road
Armonk, New York 10504
914-499-1900

Der verantwortliche Ansprechpartner des Herstellers in der EU ist:

IBM Deutschland GmbH
Technical Regulations, Abteilung M372

IBM-Allee 1, 71139 Ehningen, Germany
Tele: +49 7032 15 2941
e-mail: lugi@de.ibm.com

Generelle Informationen:

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 Klasse A.

People's Republic of China Class A Electronic Emission statement

中华人民共和国“A类”警告声明

声 明
此为A级产品，在生活环境中，该产品可能会造成无线电干扰。在这种情况下，可能需要用户对其干扰采取切实可行的措施。

Taiwan Class A Statement

警告使用者:
這是甲類的資訊產品，在
居住的環境中使用時，可
能會造成射頻干擾，在這
種情況下，使用者會被要
求採取某些適當的對策。 taiemi

Taiwan contact information

This topic contains the product service contact information for Taiwan.

```
IBM Taiwan Product Service Contact Information:
IBM Taiwan Corporation
3F, No 7, Song Ren Rd., Taipei Taiwan
Tel: 0800-016-888
```

台灣IBM 產品服務聯絡方式：
台灣國際商業機器股份有限公司
台北市松仁路7號3樓
電話：0800-016-888

f2c00790

Japan Voluntary Control Council for Interference (VCCI) Class A Statement

この装置は、クラス A 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI-A

Japan Electronics and Information Technology Industries Association (JEITA) Statement (less than or equal to 20 A per phase)

高調波ガイドライン適合品 jieta1

Korean Electromagnetic Interference (EMI) Statement

This explains the Korean Electromagnetic Interference (EMI) statement.

이 기기는 업무용 환경에서 사용할 목적으로 적합성평가를 받은 기기로서

가정용 환경에서 사용하는 경우 전파간섭의 우려가 있습니다.

Russia Electromagnetic Interference (EMI) Class A Statement

ВНИМАНИЕ! Настоящее изделие относится к классу А.
В жилых помещениях оно может создавать
радиопомехи, для снижения которых необходимы
дополнительные меры rusemi

Index

Printed in USA

SC27-3643-12