

IBM TotalStorage[®] DS6000



Administering

IBM TotalStorage[®] DS6000



Administering

Note:

Before using this information and the product it supports, read the information in "Notices" on page 19.

Twenty-fourth Edition (January 2007)

© Copyright International Business Machines Corporation 2004, 2007. All rights reserved.

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

Contents

Tables	v	Chapter 8. Unlocking an administrative password	17
Notices and publication information	vii	Notices	19
Safety notices	vii	Accessibility	20
Environmental notices.	vii	Trademarks	21
Product recycling and disposal.	vii	Terms and conditions	22
Battery return program	viii	Electronic emission notices	22
How to send your comments	ix	Federal Communications Commission (FCC) statement	23
Chapter 1. Administering user accounts	1	Industry Canada compliance statement	23
Chapter 2. Adding user accounts	3	European community compliance statement	23
Chapter 3. Modifying user accounts.	5	Japanese Voluntary Control Council for Interference (VCCI) class A statement.	24
Chapter 4. Unlocking a user account	7	Korean Ministry of Information and Communication (MIC) statement	24
Chapter 5. Removing user accounts	9	Taiwan class A compliance statement.	24
Chapter 6. Defining password rules	11	Index	25
Chapter 7. User Groups	13		

Tables

1. User Group capabilities 14

Notices and publication information

This section contains information about safety notices that are used in this guide, environmental notices for this product, publication information, and information about sending your comments to IBM.

Safety notices

Complete this task to find information about safety notices.

To find the translated text for a danger or caution notice:

1. Look for the identification number at the end of each danger notice or each caution notice. In the following examples, the numbers **1000** and **1001** are the identification numbers.

DANGER

A danger notice indicates the presence of a hazard that has the potential of causing death or serious personal injury.

1000

CAUTION:

A caution notice indicates the presence of a hazard that has the potential of causing moderate or minor personal injury.

1001

2. Find the number that matches in the *IBM System Storage Solutions Safety Notices for IBM Versatile Storage Server and IBM System Storage Enterprise Storage Server, GC26-7229*.

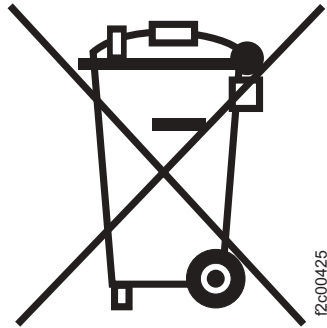
Environmental notices

This section identifies the environmental guidelines that pertain to this product.

Product recycling and disposal

This unit contains recyclable materials.

This unit must be recycled or discarded according to applicable local and national regulations. IBM® encourages owners of information technology (IT) equipment to responsibly recycle their equipment when it is no longer needed. IBM offers a variety of product return programs and services in several countries to assist equipment owners in recycling their IT products. Information on IBM product recycling offerings can be found on IBM's Internet site at <http://www.ibm.com/ibm/environment/products/prp.shtml>.



Notice: This mark applies only to countries within the European Union (EU) and Norway.

Appliances are labeled in accordance with European Directive 2002/96/EC concerning waste electrical and electronic equipment (WEEE). The Directive determines the framework for the return and recycling of used appliances as applicable throughout the European Union. This label is applied to various products to indicate that the product is not to be thrown away, but rather reclaimed upon end of life per this Directive.

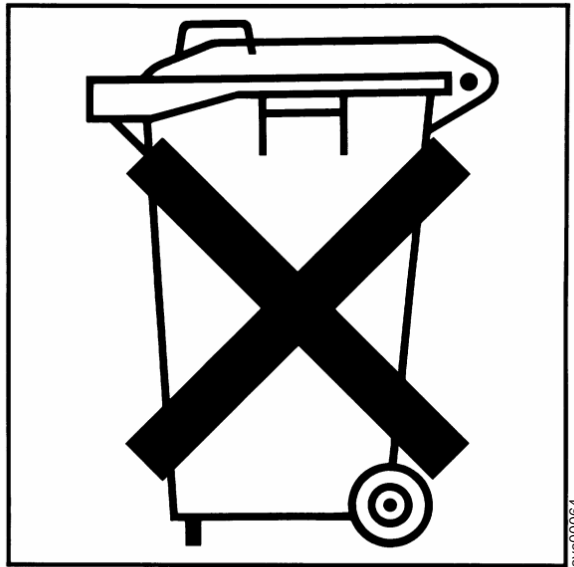
In accordance with the European WEEE Directive, electrical and electronic equipment (EEE) is to be collected separately and to be reused, recycled, or recovered at end of life. Users of EEE with the WEEE marking per Annex IV of the WEEE Directive, as shown above, must not dispose of end of life EEE as unsorted municipal waste, but use the collection framework available to customers for the return, recycling and recovery of WEEE. Customer participation is important to minimize any potential effects of EEE on the environment and human health due to the potential presence of hazardous substances in EEE. For proper collection and treatment, contact your local IBM representative.

Battery return program

This product may contain sealed lead acid, nickel cadmium, nickel metal hydride, lithium, or lithium ion battery. Consult your user manual or service manual for specific battery information. The battery must be recycled or disposed of properly. Recycling facilities may not be available in your area. For information on disposal of batteries outside the United States, go to <http://www.ibm.com/ibm/environment/products/batteryrecycle.shtml> or contact your local waste disposal facility.

In the United States, IBM has established a return process for reuse, recycling, or proper disposal of used IBM sealed lead acid, nickel cadmium, nickel metal hydride, and other battery packs from IBM Equipment. For information on proper disposal of these batteries, contact IBM at 1-800-426-4333. Please have the IBM part number listed on the battery available prior to your call.

In the Netherlands the following applies:



For Taiwan:



Please recycle batteries.

廢電池請回收

How to send your comments

Your feedback is important to help us provide the highest quality information. If you have any comments about this information or any other DS6000™ series documentation, you can submit them in the following ways:

- e-mail

Submit your comments electronically to the following e-mail address:

starpubs@us.ibm.com

Be sure to include the name and order number of the book and, if applicable, the specific location of the text you are commenting on, such as a page number or table number.

- Mail

Fill out the Readers' Comments form (RCF) at the back of this book. Return it by mail or give it to an IBM representative. If the RCF has been removed, you can address your comments to:

International Business Machines Corporation
RCF Processing Department
Department 61C
9032 South Rita Road
TUCSON AZ 85775-4401

Chapter 1. Administering user accounts

The topics in this section provide information related to administering your DS6000 user accounts. If you have administrator level privileges, you can add a new user account, delete an existing user account, or modify the user name, password, and group for a user account. There might be times when users forget the password that they use to access the DS Storage Manager. After going beyond the set number of allowable attempts with the wrong password, the account is locked. The administrator can unlock a user account. If the Admin account is locked, the administrator must use the security recovery utility tool. If you do not have administrator level privileges, your account administration privileges are limited to entering a new password for your own user ID.

Chapter 2. Adding user accounts

You must have Administrator level privileges to add a new user account. If you do not have Administrator level privileges, Add does not display in the **Select Action** drop-down box of the User administration - Main page. You can also add a user account with the **mkuser** DS Command-Line Interface command. See DS CLI documentation for more information.

1. Under **Monitor system**, select **User administration**. In User administration — Main page, select **Add** in the **Select Action** drop-down box. Then click **Go**. The Add user page is displayed.
2. Specify the user name. You can enter up to 16 characters.
3. Specify the user account password. This entry is displayed as asterisks. Passwords must meet the following criteria:
 - Be six to 16 characters long.
 - Must contain five or more letters, and it must begin and end with a letter.
 - Must contain one or more numbers.
 - Cannot contain the user's user ID.
 - Is case-sensitive.
 - Four unique new passwords must be issued before an old password can be reused.
4. Retype the password in the **Confirm password** box. This entry must match the password entry above. Characters in this field appear as asterisks.
5. Assign a group role to the user account by selecting the appropriate group in the **Group assignment** boxes.
6. Click **Ok**. The user ID that you added is available for selection in the User administration — Main Page.

Chapter 3. Modifying user accounts

If you have Administrator level privileges, you can modify the user name, password, and group for a user account. If you do not have Administrator level privileges, you can only enter a new password for your own user ID. You can also modify a user account with the **chuser** DS Command-Line Interface command. See DS CLI documentation for more information.

The password and its use must meet the following criteria:

- Be six to 16 characters long.
 - Must contain five or more letters, and it must begin and end with a letter.
 - Must contain one or more numbers.
 - Cannot contain the user's user ID.
 - Is case-sensitive.
 - Four unique new passwords must be issued before an old password can be reused.
1. Under **Monitor system**, select **User administration**. In User administration — Main page, select **Modify** in the **Select Action** drop-down box. Then click **Go**. The Modify user page is displayed.
 2. To modify the user name, enter up to 16 characters. If you do not have Administrator level privileges, your user name appears in the **User name** box by default and you are not able to modify it.
 3. Specify the user account password. Passwords must contain at least 5 alphabetic characters, and at least one numeric character, with an alphabetic character in the first and last positions. Passwords are limited to a total of 16 characters. The user name can not be part of the password. The minimum number of unique new passwords that must be used before an old password can be reused is four. This entry will appear as asterisks.
 4. Retype the password in the **Confirm password** box. This entry must match the password entry above. Characters in this field appear as asterisks.
 5. Assign a group role to the user account by selecting the appropriate group in the **Group assignment** box.
 6. Click **Ok**. The properties for the user account are immediately modified.

Chapter 4. Unlocking a user account

There might be times when users forget the password that they use to access the DS Storage Manager. Beyond the set number of allowable attempts with the wrong password, the account is locked. To unlock a user's account, the administrator can use the unlock user process. If the Administrator account is locked, the Administrator must use the security recovery utility tool. You can also unlock a user account with the **chuser** DS Command-Line Interface command. See DS CLI documentation for more information.

You must have administrator-level privileges to unlock a user's account. If you do not have administrator-level privileges, you cannot unlock a user account or use the security recovery tool to unlock the Administrator account.

Note: This task only explains how to use the unlock user process. The Unlocking an administrative password task describes how to use the security recovery utility tool to unlock the Administrator account.

1. Under **Monitor system**, select **User administration**. In User administration — Main page, select the user ID to unlock.
2. Select **Unlock user** in the **Select Action** drop-down box. Then click **Go**. A confirmation message is displayed.
3. Click **OK**. The Account Status column updates accordingly.

Chapter 5. Removing user accounts

If you have Administrator level privileges, you can remove an existing user account. If you do not have Administrator level privileges, Delete does not display in the **Select Action** drop-down box of the User administration — Main page. You can also remove a user account with the **rmuser** DS Command-Line Interface command. See DS CLI documentation for more information.

1. Under **Monitor system**, select **User administration**. In User administration — Main page, select the user ID to remove.
2. Select **Delete** in the **Select Action** drop-down box. Then click **Go**. A confirmation message is displayed.
3. Click **Ok**. The user ID is removed immediately.

Chapter 6. Defining password rules

Complete this task to set the length of time that passwords are valid and the maximum allowed failed logins.

You must have administrator-level privileges to define password rules. If you do not have administrator-level privileges, Password settings does not display in the **Select Action** drop-down menu of the User administration — Main page.

The password and its use must meet the following criteria:

- Be six to 16 characters long.
 - Must contain five or more letters, and it must begin and end with a letter.
 - Must contain one or more numbers.
 - Cannot contain the user's user ID.
 - Is case-sensitive.
 - Four unique new passwords must be issued before an old password can be reused.
 - Allowable characters are: a-z, A-Z, 0-9.
1. Under **Monitor system**, select **User administration**. In User administration — Main page, select **Password settings** in the **Select Action** drop-down box. Then click **Go**. The Password settings page is displayed.
 2. Specify the number of days after that a password expires in the **Password expires (days)** field. An entry of 0 will result in passwords never expiring.
 3. Specify the number logins after which no more attempts are allowed in the **Failed logins allowed** field. An entry of 0 will allow an unlimited number of attempts.
 4. Click **Ok**. The password setting are immediately applied.

Chapter 7. User Groups

User groups (or roles) are a level of access that is assigned by the administrator, which allows users to perform certain functions. User groups are created using the DS Storage Manager or the CLI.

When a user account is created, the administrator must specify an initial password for the account. This initial password expires immediately which means that the account users must change the password before they are allowed to perform any other actions. This is also true for all account roles, including Administrators.

The user must be assigned to at least one group or role. Users can be assigned to multiple groups or combinations of groups. Groups with the label No Access (only) cannot be selected in combination with another group.

Administrators can make the following user group assignments (Table 1 on page 14 provides specific capabilities for each user group):

Administrator (only)

Must be the only assigned group. This user group has the highest level of authority. It allows a user to add or remove user accounts. This group has access to all service functions and DS6000 resources.

Physical operator (only)

Must be the only assigned group. This user group allows access to resources that are related to physical configuration, including storage complex, storage unit, storage image, management console, arrays, ranks, and extent pools. The physical operator group does not have access to security functions.

Logical operator

Can be assigned in combination with the Copy Services operator group, but not in combination with any other group. This group has access to service functions and resources that relate to logical volumes, hosts, host ports, logical subsystems, and volume groups, excluding security functions.

Copy Services Operator

Can be assigned in combination with the Logical operator group, but not in combination with any other group. This group has access to all Copy Services service functions and resources, excluding security functions.

Monitor (only)

Must be the only assigned group. This group has access to all read-only, nonsecurity service functions and all DS6000 resources.

Service Operator

This group has access to all service related DS6000 service functions and resources (for example, performing a code load, and retrieving problem logs). This user group inherits all authority of the Monitor group.

No Access (only)

The default selection. Must be the only assigned group. This group has no access to any service functions or DS6000 resources. This is the user group that is assigned to a user account that is not associated with any other user group.

Table 1. User Group capabilities

Capability	Administrator	Physical Operator	Logical Operator	Copy Services Operator	Monitor	Service Operator	No Access
User account management	X						
Access audit log	X						
Update storage complex	X	X					
Power on/off storage image	X	X					
Update storage unit	X	X					
Update storage image	X	X					
Warmstart storage image	X	X					
Manage arrays, ranks, extent pools	X	X					
I/O port configuration	X	X					
Configuration recovery services (unfence volumes, discard pinned tracks, repair ranks,...)	X	X					
Host configuration	X	X	X				
Logical subsystem configuration	X	X	X				
Volume configuration	X	X	X				
Add or remove volume group	X	X	X				
Assign or unassign volume group to host connection	X	X	X				
Add or remove volumes to volume group	X	X	X				
Manage Copy Services (FlashCopy, PPRC, Global Mirror)	X	X		X			
Set Copy Services timeout values	X	X		X			

Table 1. User Group capabilities (continued)

Capability	Administrator	Physical Operator	Logical Operator	Copy Services Operator	Monitor	Service Operator	No Access
Update user account password	X	X	X	X	X	X	
Query FRUs and enclosures	X	X	X	X	X	X	
Query configuration	X	X	X	X	X	X	
Query Copy Services	X	X	X	X	X	X	
FRU management	X	X				X	
Problem management	X	X				X	
Validate communication paths	X	X				X	
Activate code load	X	X				X	
Create a new PE package	X	X				X	
Manage storage unit IP addresses	X						

Chapter 8. Unlocking an administrative password

There might be times when administrative users forget the password that they use to access the DS Storage Manager. Beyond the set number of allowable attempts with the wrong password, the account is locked. If the administrative account is locked, the administrator must use the security recovery utility tool to reset the password to the default (administrative). You cannot unlock an administrative password using the DS Command-Line Interface. The administrative user is forced to establish a new password. Using the **chuser** command, you can specify a password that expires after the initial use, and then create a new password. See DS CLI documentation for more information.

Notes:

1. This security recovery utility tool only unlocks the administrative account on the DS Storage Manager on which the tool is run.
 2. This task only explains how to use the security recovery utility tool to unlock the administrative account. The topic "Unlocking a user account" describes how to unlock a non-administrative user account.
 3. The security recovery utility tool is a script that is installed in a file directory. You run the script from the directory.
1. Open a command prompt and navigate to the C:\Program Files\IBM\dsniserver\bin\ directory where the recovery tool (script) has been installed.
 2. Type the script name, securityRecoveryUtility.bat -r
 3. Press the **Enter** key. The script runs and the administrative account is unlocked. The password is reset to the default (admin).

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.

Accessibility

Accessibility features provide users who have disabilities with the ability to successfully access information and use technology.

Accessibility features help a user who has a physical disability, such as restricted mobility or limited vision, to use software products successfully.

Features

These are the major accessibility features in the IBM System Storage[™] DS6000 information:

- You can use screen-reader software and a digital speech synthesizer to hear what is displayed on the screen. IBM Home Page Reader version 3.0 has been tested.
- You can operate features using the keyboard instead of the mouse.

Navigating by keyboard

You can use keys or key combinations to perform operations and initiate menu actions that can also be done through mouse actions. You can navigate the IBM System Storage DS6000 information from the keyboard by using the shortcut keys for your browser or Home Page Reader. See your browser Help for a list of shortcut keys that it supports. See the following Web site for a list of shortcut keys supported by Home Page Reader: http://www-306.ibm.com/able/solution_offerings/keyshort.html

Accessing the publications

You can find HTML versions of the IBM System Storage DS6000 information at the following Web site: <http://www.ehonet.ibm.com/public/applications/publications/cgi-bin/pbi.cgi>

You can access the information using IBM Home Page Reader 3.0.

Trademarks

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

- AIX
- DB2
- DFSMS/MVS
- DFSMS/VM
- DS4000
- DS6000
- DS8000
- e (logo)
- Enterprise Storage Server
- ES/9000
- ESCON
- FICON
- FlashCopy
- Graphically Dispersed Parallel Sysplex
- HACMP
- i5/OS
- IBM
- IntelliStation
- MVS/ESA
- Netfinity
- NetVista
- Operating System/400
- OS/400
- RS/6000
- S/390
- Seascape
- SNAP/SHOT
- SP
- System/390
- System p5
- System Storage
- Versatile Storage Server
- Virtualization Engine
- VSE/ESA
- z/Architecture
- z/OS
- z/VM
- zSeries

Java and all Java-based trademarks are trademarks of Sun Microsystems, 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 trademark of Linus Torvalds in the United States, other countries, or both.

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

Terms and conditions

Permissions for the use of these publications is granted subject to the following terms and conditions.

Personal Use: You may reproduce these Publications for your personal, non commercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these Publications, or any portion thereof, without the express consent of IBM.

Commercial Use: You may reproduce, distribute and display these Publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these Publications, or reproduce, distribute or display these Publications or any portion thereof outside your enterprise, without the express consent of IBM.

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the Publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the Publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED “AS-IS” AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Electronic emission notices

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

Federal Communications Commission (FCC) statement

This equipment has been tested and complies 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 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 users 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 community compliance statement

This product is in conformity with the protection requirements of EC Council Directive 89/336/EEC 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 nonrecommended modification of the product, including the fitting of non-IBM option cards.

Germany only

Zulassungsbescheinigung laut Gesetz ueber die elektromagnetische Vertraeglichkeit von Geraeten (EMVG) vom 30. August 1995.

Dieses Geraet ist berechtigt, in Uebereinstimmung mit dem deutschen EMVG das EG-Konformitaetszeichen - CE - zu fuehren.

Der Aussteller der Konformitaetserklaeung ist die IBM Deutschland.

Informationen in Hinsicht EMVG Paragraph 3 Abs. (2) 2:

Das Geraet erfuehlt die Schutzanforderungen nach EN 50082-1 und EN 55022 Klasse A.

EN 55022 Klasse A Geraete beduerfen folgender Hinweise:

Nach dem EMVG:

"Geraete duerfen an Orten, fuer die sie nicht ausreichend entstoert sind, nur mit besonderer Genehmigung des Bundesministeriums fuer Post und Telekommunikation oder des Bundesamtes fuer Post und Telekommunikation

betrieben werden. Die Genehmigung wird erteilt, wenn keine elektromagnetischen Störungen zu erwarten sind." (Auszug aus dem EMVG, Paragraph 3, Abs.4)

Dieses Genehmigungsverfahren ist nach Paragraph 9 EMVG in Verbindung mit der entsprechenden Kostenverordnung (Amtsblatt 14/93) kostenpflichtig.

Nach der EN 55022:

"Dies ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funkstörungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Massnahmen durchzuführen und dafür aufzukommen."

Anmerkung:

Um die Einhaltung des EMVG sicherzustellen, sind die Geräte wie in den Handbüchern angegeben zu installieren und zu betreiben.

Japanese Voluntary Control Council for Interference (VCCI) class A statement

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラス 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。

Korean Ministry of Information and Communication (MIC) statement

Please note that this device has been certified for business use with regard to electromagnetic interference. If you find this is not suitable for your use, you may exchange it for one of residential use.

Taiwan class A compliance 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。

VS07171L

Index

A

- accessibility 20
- account setup
 - adding user accounts 3
 - administering user accounts 3
 - unlocking a user account 7
 - unlocking an administrative password 17
- adding
 - users 3

D

- deleting
 - user accounts 9

K

- keyboards
 - accessibility features 20

L

- legal
 - terms and conditions 22

M

- modifying user accounts 5

P

- passwords
 - defining rules 11
 - use criteria 3

R

- removing
 - user accounts 9

S

- security
 - defining user groups 13

T

- Trademarks 21

U

- user administration
 - adding user accounts 3
 - administering user accounts 3
 - defining password rules 11

- user administration (*continued*)
 - deleting user accounts 9
 - modifying user accounts 5
 - unlocking a user account 7
 - unlocking an administrative password 17
- users
 - adding 3
 - defining access 13
 - deleting user accounts 9
 - modifying user accounts 5
 - removing user accounts 9
 - user groups 13



Printed in USA