



Trusted Solaris User's Guide

Sun Microsystems, Inc.
901 San Antonio Road
Palo Alto, CA 94303-4900
U.S.A.

Part Number 805-8115-10
December 2000

Copyright 2000 Sun Microsystems, Inc. 901 San Antonio Road, Palo Alto, California 94303-4900 U.S.A. All rights reserved.

This product or document is protected by copyright and distributed under licenses restricting its use, copying, distribution, and decompilation. No part of this product or document may be reproduced in any form by any means without prior written authorization of Sun and its licensors, if any. Third-party software, including font technology, is copyrighted and licensed from Sun suppliers.

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California. UNIX is a registered trademark in the U.S. and other countries, exclusively licensed through X/Open Company, Ltd.

Sun, Sun Microsystems, the Sun logo, docs.sun.com, AnswerBook, AnswerBook2, Trusted Solaris, and Solaris are trademarks, registered trademarks, or service marks of Sun Microsystems, Inc. in the U.S. and other countries. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.

The OPEN LOOK and Sun™ Graphical User Interface was developed by Sun Microsystems, Inc. for its users and licensees. Sun acknowledges the pioneering efforts of Xerox in researching and developing the concept of visual or graphical user interfaces for the computer industry. Sun holds a non-exclusive license from Xerox to the Xerox Graphical User Interface, which license also covers Sun's licensees who implement OPEN LOOK GUIs and otherwise comply with Sun's written license agreements.

Federal Acquisitions: Commercial Software – Government Users Subject to Standard License Terms and Conditions

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Copyright 2000 Sun Microsystems, Inc. 901 San Antonio Road, Palo Alto, Californie 94303-4900 Etats-Unis. Tous droits réservés.

Ce produit ou document est protégé par un copyright et distribué avec des licences qui en restreignent l'utilisation, la copie, la distribution, et la décompilation. Aucune partie de ce produit ou document ne peut être reproduite sous aucune forme, par quelque moyen que ce soit, sans l'autorisation préalable et écrite de Sun et de ses bailleurs de licence, s'il y en a. Le logiciel détenu par des tiers, et qui comprend la technologie relative aux polices de caractères, est protégé par un copyright et licencié par des fournisseurs de Sun.

Des parties de ce produit pourront être dérivées du système Berkeley BSD licenciés par l'Université de Californie. UNIX est une marque déposée aux Etats-Unis et dans d'autres pays et licenciée exclusivement par X/Open Company, Ltd.

Sun, Sun Microsystems, le logo Sun, docs.sun.com, AnswerBook, AnswerBook2, et Solaris sont des marques de fabrique ou des marques déposées, ou marques de service, de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays. Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux Etats-Unis et dans d'autres pays. Les produits portant les marques SPARC sont basés sur une architecture développée par Sun Microsystems, Inc.

L'interface d'utilisation graphique OPEN LOOK et Sun™ a été développée par Sun Microsystems, Inc. pour ses utilisateurs et licenciés. Sun reconnaît les efforts de pionniers de Xerox pour la recherche et le développement du concept des interfaces d'utilisation visuelle ou graphique pour l'industrie de l'informatique. Sun détient une licence non exclusive de Xerox sur l'interface d'utilisation graphique Xerox, cette licence couvrant également les licenciés de Sun qui mettent en place l'interface d'utilisation graphique OPEN LOOK et qui en outre se conforment aux licences écrites de Sun.

CETTE PUBLICATION EST FOURNIE "EN L'ETAT" ET AUCUNE GARANTIE, EXPRESSE OU IMPLICITE, N'EST ACCORDEE, Y COMPRIS DES GARANTIES CONCERNANT LA VALEUR MARCHANDE, L'APTITUDE DE LA PUBLICATION A REpondre A UNE UTILISATION PARTICULIERE, OU LE FAIT QU'ELLE NE SOIT PAS CONTREFAISANTE DE PRODUIT DE TIERS. CE DENI DE GARANTIE NE S'APPLIQUERAIT PAS, DANS LA MESURE OU IL SERAIT TENU JURIDIQUEMENT NUL ET NON AVENU.



Contents

Preface	13
1. Introduction to Trusted Solaris	17
What is Trusted Solaris 8?	17
How the Trusted Solaris environment Protects against Intruders	18
Limiting Access to the Trusted Computing Base	18
Making Theft of Passwords More Difficult	18
Protecting Information on the System through Access Control	18
Providing Auditing	19
Preventing Spoofing Programs	19
Protecting Local Peripheral Devices against Unauthorized Users	19
How the Trusted Solaris environment Enforces Access Control Policy	20
Discretionary Access Control	20
Mandatory Access Control	20
User Responsibilities for Protecting Data	23
How the Trusted Solaris environment Keeps Labeled Information Separate	24
Letting Users Select Single- or Multilevel Sessions	24
Providing Labeled Workspaces	24
Storing Files in Separate Directories by Labels	25
Enforcing MAC for Email Transactions	27

Clearing Objects Prior to Reuse	27
How the Trusted Solaris environment Enables Secure Administration	27
Authorizations and Privileges	28
Accessing Applications and Authorizations	28
Predefined Roles	29
To Learn More about the Trusted Solaris environment	29
Also in this Manual	29
How to Use Procedures in this Manual	30
Other Useful Manuals	31
2. Accessing and Leaving the Trusted Solaris Environment	33
The Login Process	33
Identification	35
Authentication	37
Message Checking and Session Type Selection	38
Setting the Session Level	41
Related Access Procedures	43
Leaving the Trusted Solaris Environment	43
Enabling Logins When Logins Are Disabled	46
Fixing a Bad Desktop Profile	47
3. Tour of the Trusted Solaris Environment	49
Tour: Logging In	49
Tour: Setting the Session Type	50
Tour: Using the Label Builder to Set a Session Clearance	52
Tour: Exploring the Basic Trusted Solaris Environment	54
Tour: Launching an Application	57
Tour: Looking at Files with the File Manager	59
Tour: Changing to a Workspace at a Different Label	61
Tour: Working in a Workspace at a Different Label	62

Tour: Occupying Workspaces with Applications at Different Labels	65
Tour: Moving Data Between Windows with Different Labels	66
Tour: Moving Files Between File Managers with Different Labels	69
4. Elements of the Trusted Solaris Environment	73
Basic Trusted Solaris Environment	73
Label Displays in the Trusted Solaris Environment	74
Trusted Stripe	76
Trusted Path Symbol	76
Window Label Indicator	77
Front Panel	77
Workspace Switch Area	77
Clock	78
Calendar	78
File Manager	78
Text Editor	79
Personal Applications Subpanel	79
Mailer	79
Printer	80
Desktop Style Manager	81
Application Manager	82
Trash Can	82
Trusted Path Menu	82
Add Workspace	83
Delete	83
Rename	83
Change Workspace Label	83
Role Assumption Selections	83
Change Password	84

Allocate Device	89
Query Window Label	91
Shut Down (for authorized users only)	92
Help	92
Other Trusted Solaris Environment Features	92
Lock	92
Exit	92
Occupy Workspace Commands	93
5. Managing Files and Directories	95
Setting Permissions and Access Control Lists	95
Basic Permissions	98
Access Control Lists	99
Viewing or Changing Permissions and ACL Entries	100
Manipulating File Labels	108
Viewing and Changing Labels with the File Manager	108
Copying and Linking Files to Different Labels by Default	112
A. Supplementary Documentation	113
Using Man Pages	113
Man Page Paths	114
Specifying Man Pages by Section Number	114
Accessing Online Documentation and Help	114
Glossary	115
Index	129

Tables

TABLE P-1	Typographic Conventions	15
TABLE 1-1	Examples of Label Relationships	23
TABLE 2-1	How Session Selections Affect Session Values	38
TABLE 4-1	Device Name Abbreviations	90
TABLE 5-1	ACL Types and Application	99

Figures

Figure 1-1	Trusted Symbol	19
Figure 1-2	Typical Clearances	21
Figure 1-3	Typical Environment with Labels Displayed	22
Figure 1-4	SLD Subdirectories	26
Figure 1-5	Typical Procedure	30
Figure 2-1	The Trusted Solaris Environment Login Process	35
Figure 2-2	Username Dialog Box	36
Figure 2-3	Password Dialog Box	37
Figure 2-4	Workstation Information Dialog Box	40
Figure 2-5	Session Clearance Builder Dialog Box	42
Figure 2-6	Front Panel Switch Area	44
Figure 2-7	Lock Screen Dialog Box	44
Figure 2-8	Logout Confirmation Dialog Box	45
Figure 2-9	Disabled Logins Dialog Box for Users Unauthorized to Enable Logins	46
Figure 2-10	Disabled Logins Dialog Box for Users Authorized to Enable Logins	46
Figure 3-1	Workstation Information Dialog Box	51
Figure 3-2	Typical Label Builder Dialog Box	53
Figure 3-3	Basic Trusted Solaris Environment	55
Figure 3-4	Basic Trusted Path Menu	56

Figure 3-5	Trusted Path Menu - Workspace Version	57
Figure 3-6	Running an Application	58
Figure 3-7	Entering Data and Saving a File	59
Figure 3-8	Using the File Manager	60
Figure 3-9	Visible and Hidden Files at CONFIDENTIAL Label	60
Figure 3-10	Entering a Workspace with a New Label	62
Figure 3-11	Examining Home Directory Contents in a Workspace with a New Label	63
Figure 3-12	Visible and Hidden Files Initially at SECRET A B Label	63
Figure 3-13	Creating a File in a Workspace with a New Label	64
Figure 3-14	Visible and Hidden Files at SECRET A B Label After Creation of New File	64
Figure 3-15	Selecting Occupy Workspace	65
Figure 3-16	Displaying Applications at Different Labels	67
Figure 3-17	Selection Manager Confirmation Dialog Box	68
Figure 3-18	Displaying File Managers at Different Labels	70
Figure 3-19	File Manager Confirmation Dialog Box	71
Figure 4-1	Basic Trusted Solaris Environment	74
Figure 4-2	Window Labels in the Trusted Solaris Environment	75
Figure 4-3	Trusted Stripe with Labels Suppressed	76
Figure 4-4	Mail Notifier Icons in the Mail Subpanel	79
Figure 4-5	Typical Print Banner Page	81
Figure 4-6	Role Password Dialog Box	84
Figure 4-7	Change Password Dialog Box	85
Figure 4-8	Change Password Confirmation Dialog Box	86
Figure 4-9	Change Password Reconfirmation Dialog Box	86
Figure 4-10	Password Generator Dialog Box	87
Figure 4-11	Device Allocation Manager	89
Figure 4-12	Query Window Label Operation	91

Figure 5-1	File Properties: Permissions Mode — Hide ACLs	96
Figure 5-2	File Properties: Permissions Mode — Show ACLs	97
Figure 5-3	File Properties: Information Mode	98
Figure 5-4	Special File Manager Icons	98
Figure 5-5	Selecting Change Properties from the File Manager Popup Menu	101
Figure 5-6	File Manager Basic Information Dialog Box	102
Figure 5-7	File Manager: Displaying ACL Entries	103
Figure 5-8	File Manager Add ACL Dialog Box	104
Figure 5-9	File Manager Change ACL	106
Figure 5-10	File Manager Delete Access List Entry Dialog Box	107
Figure 5-11	File Manager Change Label Dialog Box in Label Mode	109
Figure 5-12	Dragging a File between File Managers at Different Labels	110
Figure 5-13	File Manager Confirmation Dialog Box	111

Preface

The Trusted Solaris User's Guide is a guide to operating in the Trusted Solaris 8™ environment. As a prerequisite, you should be familiar with the Solaris 8 operating environment and the Common Desktop Environment (CDE). You should also be familiar with the security policy of your organization.

Related Materials

The Trusted Solaris 8 documentation set is supplemental to the Solaris 8 documentation set. You should obtain a copy of both sets for a complete understanding of the Trusted Solaris 8 operating environment. The Trusted Solaris documentation set consists of:

- *Trusted Solaris 8 Release Notes* (805-8117-10) provides help for getting started with and using the Trusted Solaris 8 version of the software. It lists known problems and describes workarounds (primary audience: administrators; secondary audience: developers).
- *Trusted Solaris Installation and Configuration* (805-8114-10) describes how to install the Trusted Solaris operating environment at networked or non-networked sites (primary audience: administrators, secondary audience: developers).
- *Trusted Solaris 8 Reference Manual* (805-8124-10) provides a book version of all Trusted Solaris man pages in four volumes (primary audience: all).
- *Trusted Solaris User's Guide* (805-8115-10) describes the basic features of the Trusted Solaris 8 environment from the end user's point of view. Although it is aimed at end users, it explains basic concepts which are of importance to administrators and application developers as well. It provides a glossary of terms covering the entire product (primary audience: end users, administrators, secondary audience: developers).

- *Trusted Solaris Administration Overview* (805-8119-10) explains the concepts of administration in the Trusted Solaris operating environment and provides an overview of administrative tools and commands (primary audience: administrators, secondary audience: developers).
- *Trusted Solaris Administrator's Procedures* (805-8120-10) provides detailed information for performing specific administration tasks and some detailed tables in the appendices useful for troubleshooting (primary audience: administrators, secondary audience: developers).
- *Trusted Solaris Audit Administration* (805-8121-10) describes the auditing system (primary audience: administrators, secondary audience: developers).
- *Trusted Solaris Label Administration* (805-8122-10) provides information on specifying label components in the label encodings file (primary audience: administrators).
- *Trusted Solaris Developer's Guide* (805-8116-10) describes how to develop applications for the Trusted Solaris 8 environment (primary audience: developers, secondary audience: administrators).
- *Compartmented Mode Workstation Labeling: Encodings Format* (805-8123-10) describes the syntax used in the label encodings file for enforcing the various rules concerning well-formed labels for a system (primary audience: administrators, secondary audience: developers).
- *Trusted Solaris 8 Transition Guide* (805-8118-10) provides an overview of the differences between the Trusted Solaris 8 and Trusted Solaris 7 environments (primary audience: administrators, developers, secondary audience: end users).

How This Guide is Organized

Chapter 1 provides an overview of the basic concepts needed to operate in the Trusted Solaris environment.

Chapter 2 presents procedures necessary for accessing and leaving the Trusted Solaris environment.

Chapter 3 takes you for a quick tour of the Trusted Solaris environment. If you have access to a Trusted Solaris system, you can perform the steps as you read them; or you can get a good idea of the environment simply by reading and following the diagrams.

Chapter 4 explains the key elements in the Trusted Solaris environment.

Chapter 5 shows you the basics of managing the security of files and directories in the Trusted Solaris environment.

Appendix A discusses man pages, online documentation, and online help in the Trusted Solaris operating environment.

Ordering Sun Documents

For a list of Trusted Solaris and other Sun Microsystems, Inc. documents and how to order them, refer to <http://www.fatbrain.com/>.

Typographic Changes and Symbols

The following table describes the type changes and symbols used in this book.

TABLE P-1 Typographic Conventions

Typeface or Symbol	Meaning	Example
AaBbCc123	The names of commands, files, and directories; on-screen computer output	Edit your <code>.login</code> file. Use <code>ls -a</code> to list all files. system% You have mail.
AaBbCc123	What you type, contrasted with on-screen computer output	system% su Password:
AaBbCc123	Command-line placeholder or variable name. Replace with a real name or value	To delete a file, type <code>rm filename</code> . The <i>errno</i> variable is set.
AaBbCc123	Book titles, new words or terms, or words to be emphasized	Read Chapter 6 in <i>User's Guide</i> . These are called <i>class</i> options. You <i>must</i> be root to do this.
Code samples are in code font.		
%	UNIX C shell prompt	system%

Introduction to Trusted Solaris

This chapter introduces you to Trusted Solaris 8, a computer environment with all the advantages of the Solaris 8 operating environment plus powerful security features to accommodate an organization's security policy.

- “How the Trusted Solaris environment Protects against Intruders” on page 18
- “How the Trusted Solaris environment Enforces Access Control Policy” on page 20
- “User Responsibilities for Protecting Data” on page 23
- “How the Trusted Solaris environment Keeps Labeled Information Separate” on page 24
- “How the Trusted Solaris environment Enables Secure Administration” on page 27
- “To Learn More about the Trusted Solaris environment” on page 29

What is Trusted Solaris 8?

The Trusted Solaris 8 software package is an enhanced version of the Solaris 8 operating environment (including the Common Desktop Environment (CDE)), with special security features. The Trusted Solaris environment lets an organization define and implement a security policy for a single Sun workstation or a network of Sun workstations. A *security policy* is the set of rules and practices that help protect information and other resources (such as computer hardware) in your system. Typically, rules deal with such items as who has access to which information or who is allowed to write files to tape; practices are recommended procedures for performing tasks.

Here are some major security features that Trusted Solaris 8 provides. (Note that your site may not implement all of these features.)

How the Trusted Solaris environment Protects against Intruders

The Trusted Solaris environment protects against intruders by

- Limiting access to the trusted computing base
- Making theft of passwords more difficult
- Protecting information on the system through access control
- Providing auditing
- Preventing spoofing programs
- Protecting local peripheral devices against unauthorized users

Limiting Access to the Trusted Computing Base

The term *trusted computing base* or *TCB* refers to the part of the Trusted Solaris environment that affects security; it includes software, hardware, firmware, documentation, and administrative procedures. Utility programs and application programs that can access security-related files are all part of the trusted computing base. Your administrator sets limits on all potential interactions that you can make with the TCB, regarding programs that you need to do your job, files that you are allowed to access, and utility programs that can affect security.

Making Theft of Passwords More Difficult

Because intruders generally break into systems by guessing passwords, the Trusted Solaris environment supplies several options for tightening password security. Users may be required to change passwords with certain intervals or by set expiration dates. In addition, there is a password generator that creates random, non-language passwords. Check with your administrator to see which of these options are used at your site.

Protecting Information on the System through Access Control

If an intruder does successfully log into the system, there are further obstacles to getting surreptitious access to information. Files and other resources are protected by both access control set by the owner of the information and access control enforced

by the system. See “How the Trusted Solaris environment Enforces Access Control Policy” on page 20.

Providing Auditing

The Trusted Solaris environment lets administrators audit all or selected user actions and run reports by user ID, file, date, and time. You are accountable for your actions in a Trusted Solaris system, particularly those actions that may affect security or sensitive files. User activity can be recorded in an audit trail so that administrators can detect suspicious actions on the system.

Preventing Spoofing Programs

Intruders sometimes spoof, that is, imitate login or other legitimate programs to intercept passwords or other sensitive data. The Trusted Solaris environment protects users from hostile spoofing programs by displaying the *Trusted Symbol*, an unmistakable, tamper-proof icon at the bottom of the screen that is displayed whenever you interact with the trusted computing base (TCB). Its presence ensures the safety of performing security-related transactions. Its absence indicates a potential security breach. The following figure shows the trusted symbol.



Figure 1-1 Trusted Symbol

Protecting Local Peripheral Devices against Unauthorized Users

In the Trusted Solaris environment, administrators can assign access to local peripheral devices such as tape drives, floppies, printers, and microphones on a user-by-user basis. The Trusted Solaris 8 environment restricts access to peripheral devices as follows:

- Remote users cannot tap into local devices such as microphones or tape drives; users must be logged in locally to use a special device allocation tool.
- Only users with special authorization can access devices with removable media.

How the Trusted Solaris environment Enforces Access Control Policy

The Trusted Solaris environment controls which users can access which information by providing

- Discretionary access control
- Mandatory access control

Discretionary Access Control

Discretionary access control (DAC) is a software mechanism for controlling users' access to files and directories. It leaves setting protections for files or directories to the owner's discretion. The two forms of DAC are the traditional UNIX permission bits and Access Control Lists (ACLs).

Permission bits let the owner set read, write, and execute protection by owner, group, and other users. In traditional UNIX systems, the superuser (root) can override DAC protection; in the Trusted Solaris environment, the ability to override DAC is permitted for administrators and authorized users only. Access Control Lists (ACLs) provide a finer granularity of access control, letting owners specify separate permissions for specific individuals and groups.

Mandatory Access Control

Mandatory access control (MAC) is a system-enforced access control mechanism that uses clearances and labels to enforce security policy. Roughly speaking, MAC associates the programs a user runs with the security level (clearance or label) at which the user chooses to work in the session and permits access to information, programs, and devices at the same or lower level only. MAC also prevents users from writing to files at lower levels. MAC is enforced according to your site's security policy and cannot be overridden without special authorization or privileges.

Clearances

As part of your site's security policy, your security administrator assigns a *user clearance* to everyone at your site. The user clearance represents the degree of security with which a user is entrusted. It has two components:

- classification – indicates a (hierarchical) level of security. Applied to people, the classification represents a measure of trust; applied to data, it is the degree of

protection required. In government, classifications are: TOP SECRET, SECRET, CONFIDENTIAL, and UNCLASSIFIED. Industry is not as standardized; a hypothetical classification hierarchy might be PUBLIC, INTERNAL, NEED TO KNOW, and REGISTERED.

- compartment – represents a grouping, such as a work group, department, project, or topic. Access to compartments is granted on a need-to-know basis.

Some typical clearances are shown in the following figure.

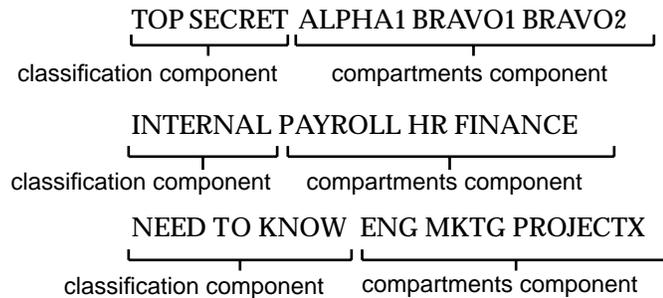


Figure 1-2 Typical Clearances

Labels

The Trusted Solaris environment uses a string called a *label* (containing a classification and compartments in similar fashion to clearances) to determine which information you can access. (Labels are also referred to as *sensitivity labels* or *SLs*, for short.) Labels may be displayed inside square brackets ([]) in window title bars, in the trusted stripe (a special area at the bottom of the screen), or not at all, depending on how your system is configured. Figure 1-3 shows a configuration configured to display labels; the labels and trusted stripe are indicated.

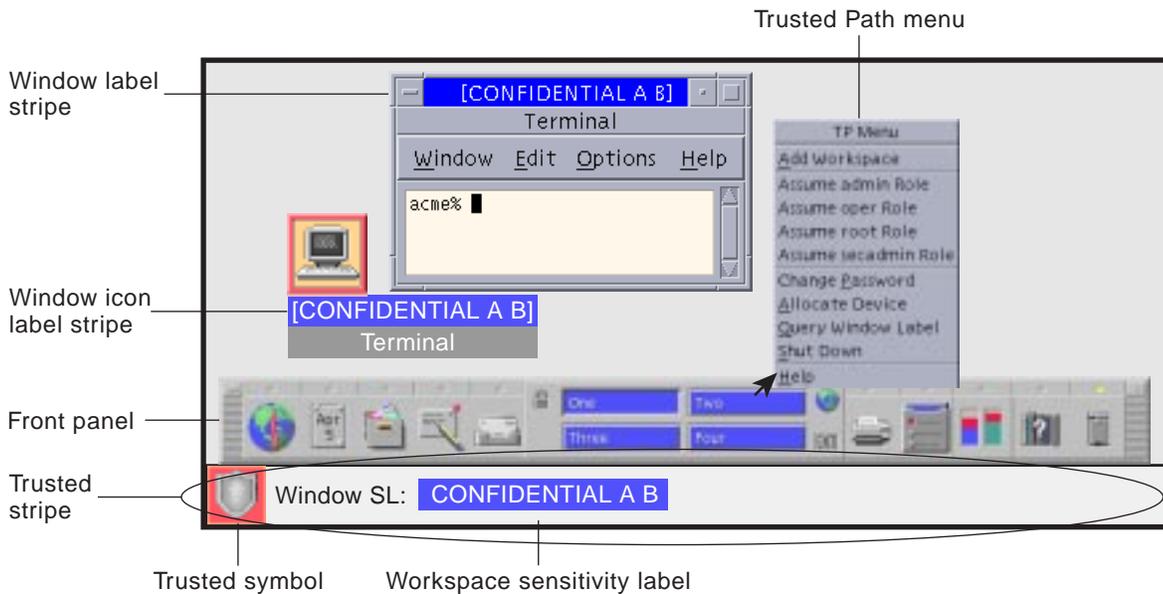


Figure 1-3 Typical Environment with Labels Displayed

All subjects and objects in a system have labels. A *subject* is an active entity, usually a process (running program), that causes information to flow among objects or changes the system state. An *object* is a passive entity that contains or receives data, such as a data file, directory, printer, or other device. In some cases, a process may be an object, such as when you use `kill` on a process.

The Part Labels Play in Transactions

The Trusted Solaris environment mediates all attempted security-related transactions. It compares the subject's label with the object's label and permits or disallows the transaction depending on which label is *dominant* (as described below). An entity's label is said to *dominate* another's if the following two conditions are met:

- The classification component of the first entity's label is equal to or outranks the object's classification.
- All compartments in the second entity's labels are included in the first entity's label.

Two labels are said to be *equal* if they have the same classification and the same set of compartments. If they are equal, they dominate each other so that access is permitted. If one label has a higher classification or includes all of the second label's compartments or both, the first label is said to *strictly dominate* the second label. Two labels are said to be *disjoint* or *noncomparable* if neither label dominates the other.

In a read transaction, the subject's label must dominate the object's label. This rule ensures that the subject's level of trust meets the requirements for access to the object

and that the subject's label includes all compartment groupings that are allowed access to the object.

In a write transaction, that is, when a subject creates or modifies an object, the resulting object's label must dominate the subject's label. This rule prevents the subject from lowering the object's label.

Users sometimes refer to the acronym WURD (write up / read down) to remind themselves of the permitted directions in mandatory access control. In practice, subjects and objects in read and write transactions usually have the same label and strict dominance does not have to be considered.

TABLE 1-1 Examples of Label Relationships

Label 1	Relationship	Label 2
Top Secret A B	(strictly) dominates	Secret A
Top Secret A B	(strictly) dominates	Secret A B
Top Secret A B	(strictly) dominates	Top Secret A
Top Secret A B	dominates (equals)	Top Secret A B
Top Secret A B	is disjoint with	Top Secret C
Top Secret A B	is disjoint with	Secret C
Top Secret A B	is disjoint with	Secret A B C

When you perform a drag-and-drop or copy-and-paste operation between files with different labels, the Trusted Solaris environment displays a confirmation dialog box if you are permitted to change the label or, if you are not permitted, the Trusted Solaris environment bars the transaction. You can accept the upgrade of the destination (if you have special authorization), downgrade the information so that the destination will maintain its existing label, or cancel the transaction altogether.

User Responsibilities for Protecting Data

As a user, you are responsible for setting the permissions to protect your files and directories, as part of discretionary access control. You can check the permissions on your files and directories using the `ls(1)` command with the `-l` option or the File Manager, as described in “Viewing or Changing Permissions and ACL Entries” on page 100.

Mandatory access control is enforced automatically by the system. If you are authorized to upgrade or downgrade information protected by labels, you have an extra special responsibility to ensure that there is a legitimate need for the change.

Another aspect of protecting data is that you should never follow emailed instructions from an administrator without verifying that the administrator actually sent the instructions. For example, if you followed emailed instructions to change your password to a particular value, you would enable the sender to log into your account.

How the Trusted Solaris environment Keeps Labeled Information Separate

The Trusted Solaris environment helps keep information at different labels separate by

- Letting users select single- or multilevel sessions
- Providing labeled workspaces
- Storing files in separate directories according to label
- Enforcing MAC for email transactions
- Clearing objects prior to reuse

Letting Users Select Single- or Multilevel Sessions

When you first log into a Trusted Solaris session, you specify whether you will be operating at a single label or at multiple labels (if you are permitted to). You then set your *session clearance* or *session label*, that is, the security level at which you intend to operate.

In a single-level session, you can access only those objects at or dominated by your session label.

In a multilevel session, you can access information at different sensitivity levels, as long as they are at or lower than your session clearance. In the Trusted Solaris environment, you can specify different labels for different workspaces.

Providing Labeled Workspaces

The workspaces in the Trusted Solaris environment are accessed through buttons in the front panel, just as in the standard Solaris operating environment. However, in

the Trusted Solaris environment, you can devote a workspace entirely to a single label. This is very convenient when you are in a multilevel session and do not wish to move information between files at different labels.

Storing Files in Separate Directories by Labels

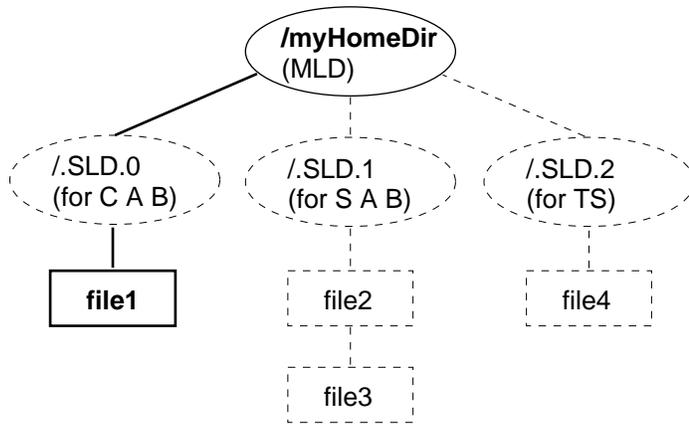
The Trusted Solaris environment provides two special types of directories for storing files and subdirectories with different labels and keeping them separate:

- multilevel directory (MLD) – is a special type of directory that transparently stores information by label in separate subdirectories called single-level directories. Your administrator typically creates your home directory as multilevel directory.
- single-level directory (SLD) – is a hidden subdirectory within a multilevel directory containing files and optionally subdirectories at a single label only.

When you attempt to view or access files in a multilevel directory, (either through an application such as the File Manager or through a shell using standard commands), only those files that are at your current label are visible and accessible. If you keep files at different labels in your home directory, for example, you cannot normally view files at labels other than your current label.

The following figure illustrates the concept of hidden single-level directories within a multilevel directory. The top part of the figure shows the contents of a multilevel home directory called `/myHomeDir` from the user's view while working at Confidential A B; the lower part of the figure shows the user at Secret A B. Hidden directories and files are indicated with dashed lines and unbolded text; the solid lines and bolded text indicate visible ones. (Note that the labels associated with the single-level directories are shown in their short form inside parentheses; the labels do not actually appear in the directory names.)

(a) User's View While at C A B label



(b) User's View While at S A B label

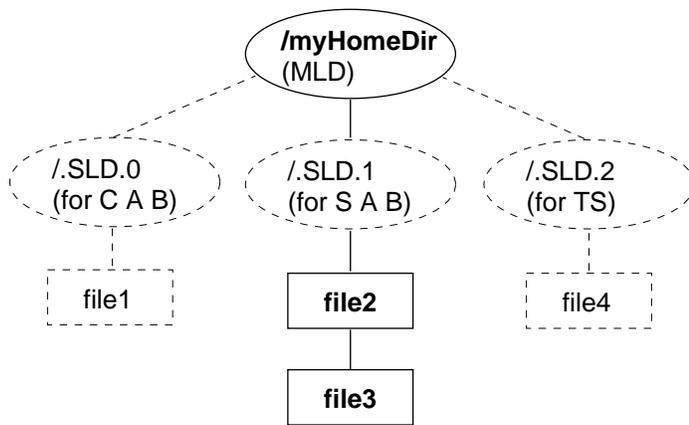


Figure 1-4 SLD Subdirectories

While working at Confidential A B, the user has the following results when trying to list the contents of the /myHomeDir directory:

```
% pwd
/myhomedir
% ls
file1
```

At Secret A B, the user sees these results:

```
% pwd
/myhomedir
% ls
file2  file3
```

Enforcing MAC for Email Transactions

The Trusted Solaris environment enforces mandatory access control whenever you use email. When you send email, the Trusted Solaris environment prevents users with insufficiently high clearance from receiving it. On the receiving end, email is sorted by the labels within your account range. Your current label must be at the same level as the email message you intend to read; otherwise you must change your current label.

Clearing Objects Prior to Reuse

The Trusted Solaris environment prevents inadvertent exposure of sensitive information by automatically clearing (erasing) user-accessible objects, such as memory and disk space, prior to reuse. Processes on the system continuously allocate, deallocate, and reuse objects, such as memory and disk space. Failure to erase sensitive data prior to reuse of the object risks exposing the data to inappropriate users. Through device deallocation, Trusted Solaris 8 clears all user-accessible objects prior to allocating them to processes. Note, however, you must clear any removable storage medium (floppy disk, magnetic tape, etc.) before another user can have access to it.

How the Trusted Solaris environment Enables Secure Administration

In contrast to traditional UNIX systems, the superuser (root) is not all-powerful in the Trusted Solaris environment. Rather, the ability to override protections is broken into discrete capabilities and assigned to administrative roles so that no single user can compromise the system's security. A *role* is a special user account that gives the user access to certain applications with the authorizations, privileges, and effective UIDs/GIDs necessary for performing the specific tasks.

In the Trusted Solaris environment,

- Users can only perform functions that override security policy if they are granted special authorizations or privileges by administrators.
- Users are granted access to applications and authorizations on a need-to-use basis.

- System administration duties can be divided among multiple roles.

Authorizations and Privileges

There are usually cases for every security policy when a control must be overridden. In conventional UNIX systems, the superuser has the ability to override *all* security policy. In the Trusted Solaris environment, there is a software mechanism called an *authorization* that gives an individual user the right to override a *specific* security control. There is also a mechanism for overriding controls called a *privilege* that is associated with software programs and permitted for specific users only. If you are prevented from running a certain task to which you think you are entitled, check with your administrator to see if an authorization is required for that application.

Accessing Applications and Authorizations

In the Trusted Solaris environment, you get access to only those applications you need to do your job. The administrator provides access by assigning one or more execution profiles to your account. An *execution profile* is a special package of CDE actions, commands, and authorizations. This restriction helps prevent users from misusing applications and harming data on the system. If you need to perform tasks that override the security policy, the administrator will grant you access to either an execution profile containing the necessary authorization or to a role with the authorization to run the program.

Note - If you have access to a special version of a command that can override security policy, you should make sure that your path is set to find this version first; otherwise, you will not be able to take advantage of the security overrides.

In addition, your administrator may assign you a profile shell as the default shell when you log in or assume a role. A *profile shell* is a special version of the Bourne shell that provides access to a restricted set of applications and capabilities. If you are assigned a profile shell, you can determine which commands are permitted by using the `clist` command at the command line. The `clist` command lists all commands available in the profile shell.

Note - If you try to run an action and receive a “Not Found” error message or if you try to run a command and receive a “Not in Profile” error message, it may be a sign that you are not permitted to use this application. Check with your administrator.

Note - If you attempt to execute a command in the profile shell, you may see the message: `Warning: command operating outside of trusted path.` This means that although you are working in a profile shell and the trusted symbol is being displayed, the current command is not interacting with the trusted computing base.

Predefined Roles

Trusted Solaris 8 provides five predefined roles: *root*, *security administrator*, *primary administrator*, *system administrator*, and *system operator*. The *root* role is used primarily for initial installation. The *security administrator* role is used for security issues, such as assigning labels or auditing user activity. The *system administrator* role is used to perform standard system management tasks such as setting up the non-security-relevant portions of user accounts. The *system operator* role is used for system backups, printer administration, and mounting removable media. The *primary administrator* role is used to perform any tasks requiring privileges beyond the capabilities of the other roles. If your site uses the predefined administration roles, make sure you know who is performing each set of duties.

Note - No role can configure its own features. For example, the system administrator role is used to set up a user's access to the security administrator role and the security administrator role is used to set a user's access to the system administrator role.

To Learn More about the Trusted Solaris environment

This section describes the rest of this manual and other useful manuals.

Also in this Manual

These Trusted Solaris features are covered in greater depth in the remaining chapters in this manual, as follows:

- Chapter 2, explains how users log in and out of the Trusted Solaris environment, with numbered steps to show the procedures.
- Chapter 3, is a step-by-step description of a typical Trusted Solaris session.

- Chapter 4, provides detailed descriptions of the major features of the Trusted Solaris environment with step-by-step procedures for the menu commands.
- Chapter 5, shows you how to use the File Manager in the Trusted Solaris environment.
- Appendix A, discusses man pages, online documentation, and online help in the Trusted Solaris operating environment.

How to Use Procedures in this Manual

All procedures are identified by a heading with a down-pointing triangle. A typical procedure appears in Figure 1-5. Procedures contain numbered steps, typically with accompanying descriptions, and often include a figure showing a typical screen. In some cases, you can actually follow the procedures and get the same results; other cases may use hypothetical examples, useful for demonstrating the process.

▼ **To Identify Yourself to the System**

1. Type your username in the text field in the username dialog box (see Figure 2-1).
Be sure to type it exactly as your administrator assigned it to you with regard to spelling and upper and lower case.

Username entry field



Figure 2-1 Username Dialog Box

2. Click the OK button (or press Enter) to confirm your entry of the username or select one of the other options if you are not ready to log in.
If you are not ready to login, you can choose one of these options:

- Click the Start Over button to re-enter your username.
- Click Reset login in the Options menu to restart the windowing system.
- Click Help to get information on using the login username dialog box.

Figure 1-5 Typical Procedure

Other Useful Manuals

For an overview of the administration aspects of the Trusted Solaris environment, refer to the *Trusted Solaris Administration Overview*. The programming aspects of the Trusted Solaris environment are covered in the *Trusted Solaris Developer's Guide*.

Accessing and Leaving the Trusted Solaris Environment

This chapter presents procedures necessary for accessing and leaving the Trusted Solaris environment.

- “The Login Process” on page 33
- “To Identify Yourself to the System” on page 36
- “To Authenticate Yourself ” on page 37
- “To Check Messages and Select Session Type” on page 39
- “To Select a Clearance for a Multilevel Session” on page 41
- “To Select a Label for a Single-level Session” on page 43
- “To Lock and Unlock Your Screen” on page 44
- “To Log Out of the Trusted Solaris Environment” on page 44
- “To Enable Logins After a Reboot” on page 46
- “To Perform a Failsafe Login” on page 47

The Login Process

Before you can get access to the environment, your Trusted Solaris 8 system administrator and security administrator must set up a user account for you. The account gives you permission to use some of the computer facilities and contains identifying information, such as the username assigned to you and your user ID (UID). The username in conjunction with your password lets you log into the system. The user ID identifies all of your transactions as well as the files and directories that you own.

An overview of the login process is shown in Figure 2-1. The process is described in more detail in the material following the overview figure. The steps in the process include:

- Identification – entering your username in the Username dialog box
- Authentication – entering your password in the Password dialog box. A *password* is a private combination of keystrokes that validates your identity to the system. Since it is stored in an encrypted form, your password is not accessible by other users on the system. It is your responsibility to protect your password so that other users cannot use it to gain unauthorized access. Never write your password down or disclose it to anyone else, because a person with your password has access to all your data without being identifiable or accountable. Your initial password is supplied by your Trusted Solaris 8 administrator.

Successful completion of identification and authentication confirms your right to use the system.

- Message checking and session type selection –The Workstation Information dialog box displays the message of the day, provides account access information (so that you can check for any possible security breaches), and lets you specify the type of session: single-level or multilevel.

Note - Your account may be configured such that you always operate at the same label (a single-label configuration). If this is the case, you will not be able to select the type of session in the Workstation Information dialog box or set a security level.

- Security level selection – setting the highest security level at which you intend to operate while in your session.

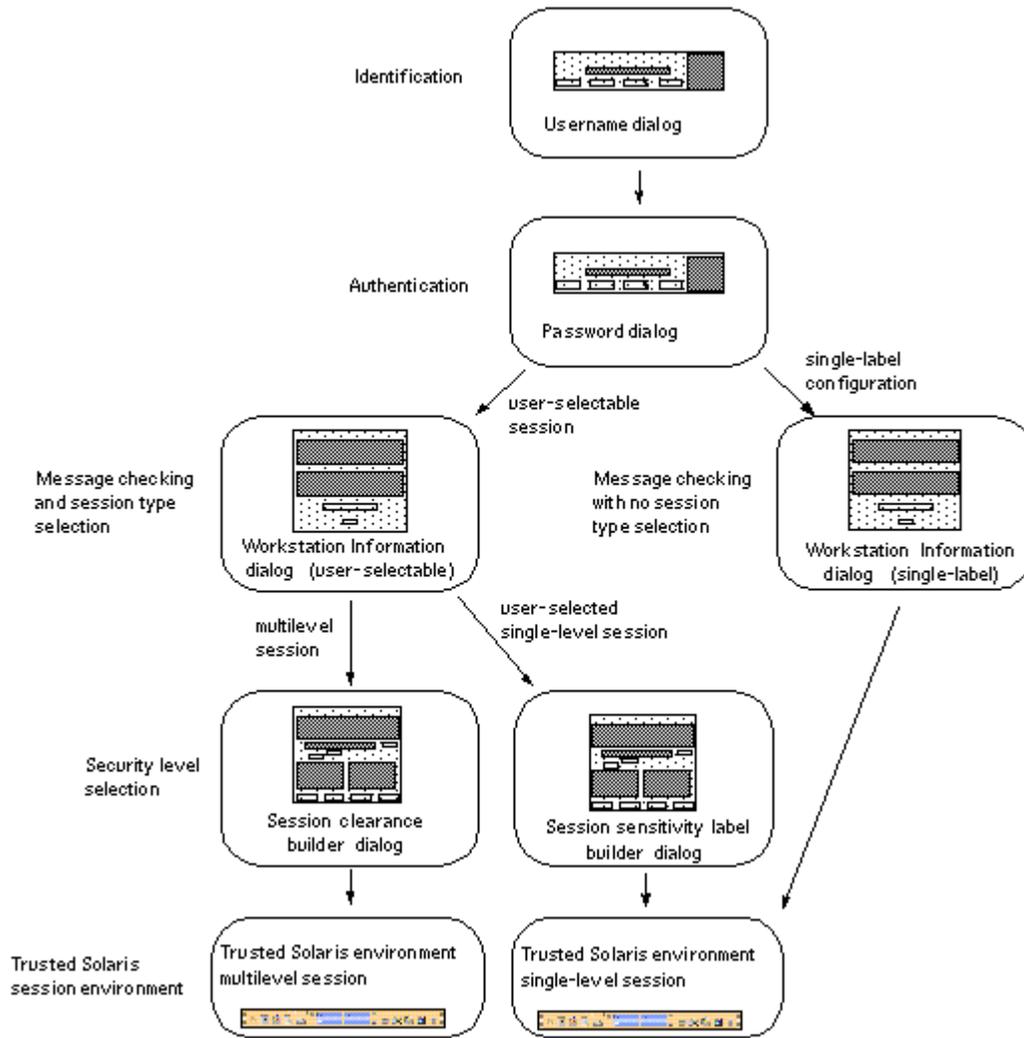


Figure 2-1 The Trusted Solaris Environment Login Process

Identification

When a Trusted Solaris 8 workstation is not in a work session, it displays the login screen. The login screen initially contains the username dialog box, which enables the next user to enter his or her username (see Figure 2-2). This is the identification part of the login process.

To Identify Yourself to the System

1. **You can log in remotely by selecting Remote Login from the Options menu in the username dialog box (see following figure) and selecting Enter Host Name or Choose Host From List; otherwise, go to the following step to log in locally.**

A dialog box for direct host entry or a list dialog box is displayed. The host you specify must be running a compatible version of the Trusted Solaris environment. In either case, after host selection, another username dialog is displayed with the name of the remote host.

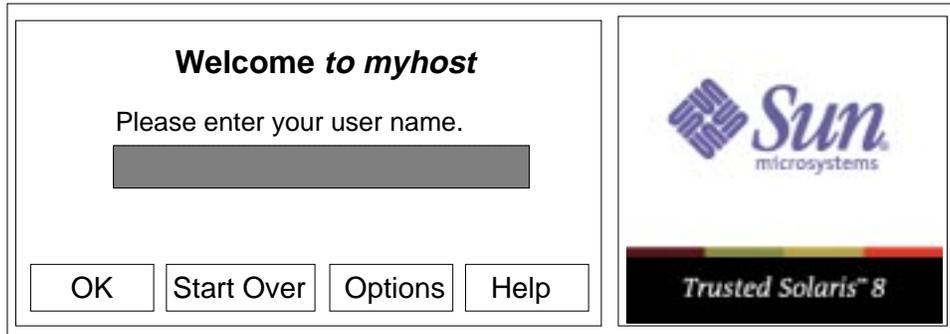


Figure 2-2 Username Dialog Box

2. **Type your username in the text field in the username dialog box.**

Be sure to type it exactly as your administrator assigned it to you with regard to spelling and upper and lower case.

3. **Click the OK button (or press Enter) to confirm your entry of the username or select one of the other options if you are not ready to log in.**

If you are not ready to log in, you can choose one of these options:

- Click the `Start Over` button to re-enter your username.
- Click `Reset login` in the Options menu to restart the windowing system.
- Click `Help` to get information on using the login username dialog box.



Caution - You should *never* see the Trusted Stripe when the login screen appears. If you ever see the screen stripe while attempting to log in or unlock the screen, do not type your password because there's a chance you are being spoofed, that is, an intruder's program is masquerading as a login program to capture passwords.

Authentication

After you have entered the username, the username dialog box is replaced in the login screen by the password dialog box (see Figure 2-3). This part of the process is referred to as *authentication*, that is, authenticating that you are indeed the user authorized to use that username.

To Authenticate Yourself

1. Type your password in the password entry field.

For security purposes, the characters do not actually display in the field.

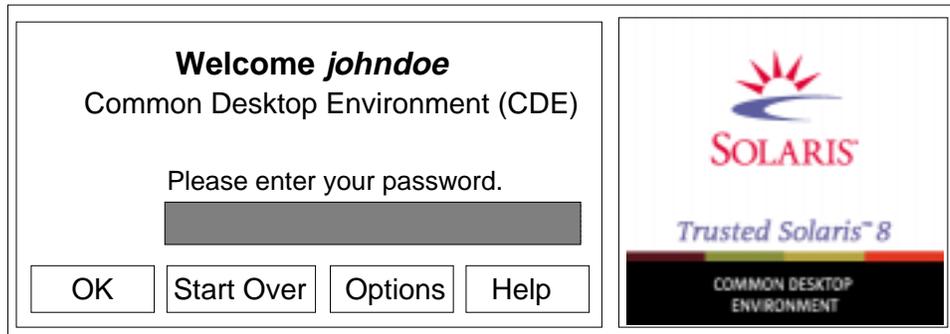


Figure 2-3 Password Dialog Box

2. Click the OK button (or press Enter) to confirm your entry of the password or select one of the other options if you are not ready to log in.

If you are ready to log in, click **OK** or press **Enter**. Otherwise, you have these options:

- Click the **Start Over** button to re-enter your username.
- Click **Reset login** in the **Options** menu to restart the windowing system.
- Click **Help** to get information on using the login username dialog box

The system compares the entered login name and password against a list of authorized users. If you have entered your password incorrectly, a message dialog box appears displaying the message:

```
Login incorrect; please try again.
```

Click **OK** to dismiss the error dialog box and return to Step 1 on page 37.

Message Checking and Session Type Selection

After you successfully enter your username and password, the Workstation Information dialog box is displayed. It provides status information and, if your account is configured for user-specified sessions, lets you select a single- or multilevel session. If your account is set up for a single-label configuration, then there will be no option for selecting a session level.

Single-level Versus Multilevel Sessions

In a *multilevel session*, you can operate at different labels. The range in which you operate is bounded at the upper end by the *session clearance* you specify and at the lower end by the minimum label assigned to you by your administrator.

In a *single-level session*, you specify a *session label* at which you operate for the entire session. In a single-level session, you can access and write to files at that label only. You cannot change the label of workspaces in the session. Note that you can assume a role within a single-level session and then operate at any label available to that role.

Session Selection Example

Table 2-1 provides an example of the difference between a single- and multilevel session. It contrasts a user choosing to operate in a single-level session at SECRET A against the user selecting a multilevel session, also at SECRET A. Note that labels are shown in their long form inside square brackets ({}).

The three columns on the left show the user's session selections at login. Note that users set *session labels* for single-level sessions and *session clearances* for multilevel sessions. (This is a minor distinction that is taken care of by the system; the correct label builder dialog box is always displayed with the choices permitted.)

The two columns on the right show the label values available in the session. The Initial Workspace label column represents the label when the user first enters the Trusted Solaris environment. The Available Labels column lists the labels that the user is permitted to switch to in the session.

TABLE 2-1 How Session Selections Affect Session Values

User Selections			Session Label Values	
Session Type	Session Label	Session Clearance	Initial Workspace Label	Available Labels
single-level	[S A]	—	[S A]	[S A]
multilevel	—	[S A]	[C]	[C], [C A], [S], [S A]

In the first row of the table, the user has selected a single-level session with a session label of [S A]. In the Trusted Solaris environment, the user has an initial workspace label of [S A] which is also the only label at which the user can operate.

In the second row of the table, the user has selected a multilevel session with a session clearance of [S A]. The user's initial workspace label is set to [U], that is, a label of [UNCLASSIFIED], because that is the lowest possible label in the user's account label range. The user can switch to any label between [U], the minimum, and [S A], the session clearance.

To Check Messages and Select Session Type

A typical Workstation Information dialog box appears in the following figure. Note that because this account is configured for multilevel operation, there is a toggle for restricting the session to a single level; single-level accounts do not get this option.



Figure 2-4 Workstation Information Dialog Box

1. Check the date and time of the last login.

This field indicates when your system was last used. You should always check that there is nothing suspicious about the last login, such as an unusual time of day, and report such occurrences to your security administrator.

2. Read any messages in the Message of the Day field.

This field contains messages from your administrator. Since this message may contain warnings about scheduled maintenance or security problems, you should always read it.

3. Read any console messages since last logout.

Typically, these system messages contain messages concerning cron (batch) jobs, but you should check that there are no messages indicating suspicious activity or other problems.

4. Click the session level toggle if you intend to work at only one label in your session (not available in single-label configurations).

In a single-level session, you operate at a single discrete label. You can only access and write to files at the same label. If you do not click the toggle, you are implicitly selecting a multilevel session and can view data at different labels. The range in which you can operate is bounded at the upper end by the session clearance that you select in the session clearance dialog box and at the lower end by the minimum label assigned to you by your administrator.

5. Click OK (or press Enter) to close the Workstation Information dialog box.

If your account is configured for single-label operation, the Trusted Solaris environment is displayed after the Workstation Information dialog box is closed; otherwise you will set the session level next.

Setting the Session Level

Note - If your account is set up for a single-label configuration, the Trusted Solaris environment will be displayed after you close the Workstation Information dialog box and you have no need to read further in this section.

If you do not select Restrict Session to a Single Level, the Clearance Builder version of the Label Builder dialog box is displayed so that you can specify the session clearance (see Figure 2-5).

If you select Restrict Session to a Single Level, the user session label version of the Label Builder dialog box is displayed and you select the label for your entire session.

Note - Workstations can be restricted to a limited range of session clearances and labels. For example, a workstation in a lobby might be limited to UNCLASSIFIED labels only. If the session clearance or label you enter is not accepted, check with an administrator to see if the workstation is restricted.

To Select a Clearance for a Multilevel Session

The session clearance sets the top boundary for labels of files that you will be able to access in the session. To set the clearance, you use the Clearance Builder dialog box (see Figure 2-5).

1. To use the default clearance in the Clearance field, click OK (or press Enter) and wait for the Trusted Solaris environment to be displayed.

For a different clearance, go to step 2 to build a new clearance.

2. Click the desired classification in the classification selection area.

3. Click the desired compartments (if any) in the compartments selection area.

4. Check the clearance you have built in the selected clearance field. Click OK or press Enter if it is correct or go back to step 2 to build a different clearance.

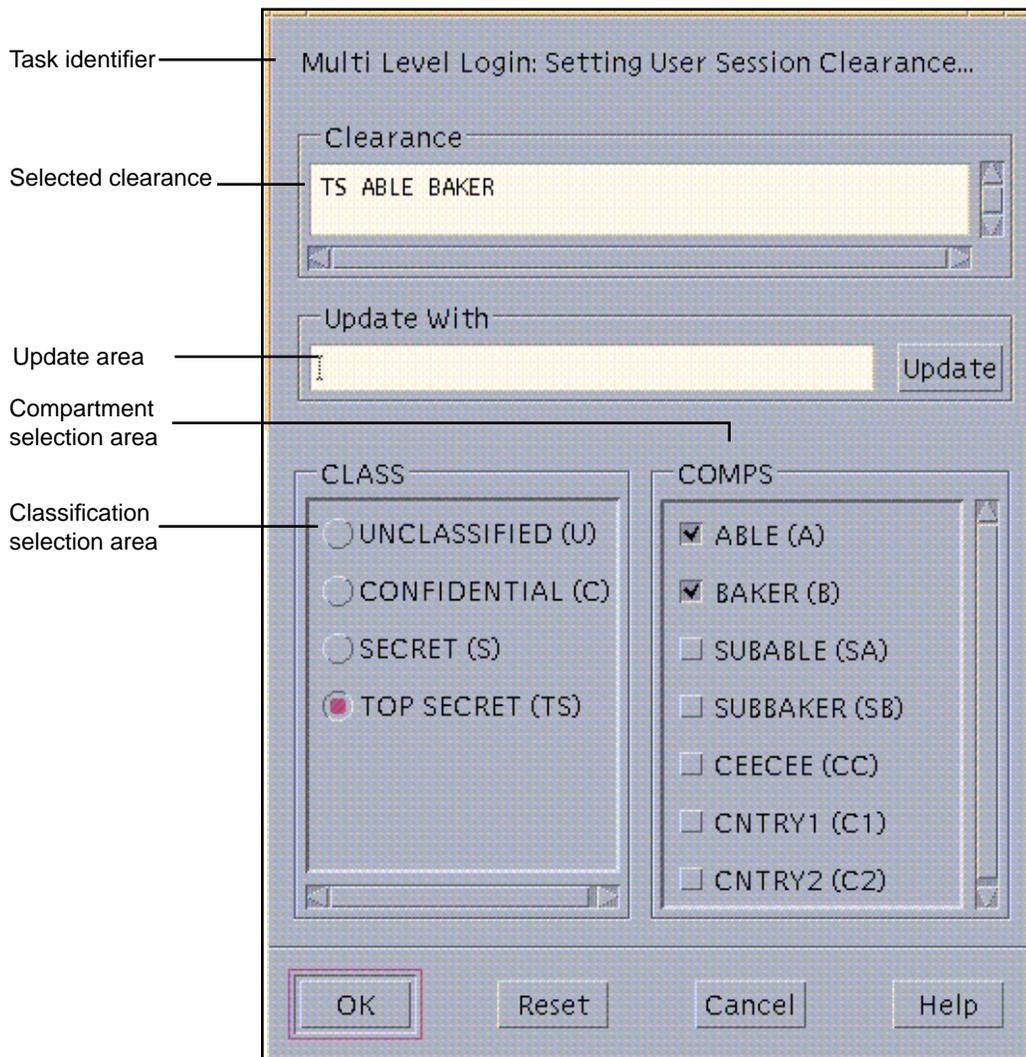


Figure 2-5 Session Clearance Builder Dialog Box

To Select a Label for a Single-level Session

The session label sets the label at which you intend to operate in this single-level session. To set the session label, you use the Single-Level Session Label Builder dialog box, which is similar to dialog box shown in Figure 2-5 except that the task identifier indicates a single-level session.

1. **To use the default label in the Label field, click OK (or press Enter) and wait for the Trusted Solaris environment to be displayed.**

For a different label, go to step 2 to build a new label.

2. **Click the desired classification in the classification selection area.**
3. **Click the desired compartments (if any) in the compartments selection area.**
4. **Check the label you have built in the selected label field. Click OK or press Enter if it is correct or go back to step 2 to build a different label.**

Related Access Procedures

This section provides other procedures related to accessing the Trusted Solaris environment, concerning:

- Leaving the Trusted Solaris environment
- Changing passwords
- Enabling logins when logins are disabled

Leaving the Trusted Solaris Environment

If you leave your logged-on terminal unattended, you create a security risk. Make a habit of securing your terminal before leaving it; either lock the screen or log out. If you plan to return shortly, lock your screen. In most facilities, the screen times out after a specified period of idleness and automatically locks. If you expect to be gone for a while or you expect someone else to use your terminal, log out.

To Lock and Unlock Your Screen

1. To lock your screen, click on the screen lock icon in the switch area of the front panel (see Figure 2-6).

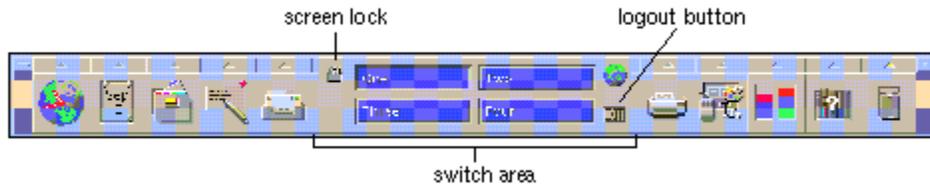


Figure 2-6 Front Panel Switch Area

The screen turns black and the dialog box shown in Figure 2-7 is displayed.

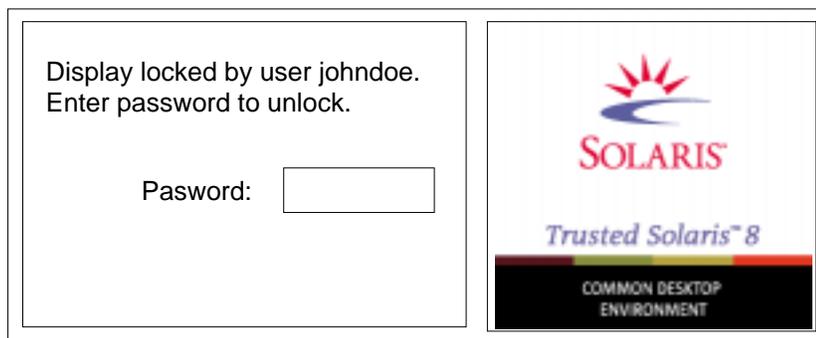


Figure 2-7 Lock Screen Dialog Box

Note - The Trusted Stripe should not be displayed when the screen is locked. If it does appear, notify your security administrator immediately.

2. To unlock your screen, type your password in the password entry field and press Enter.

This returns you to your session in its previous state.

To Log Out of the Trusted Solaris Environment

1. Click on the EXIT icon in the switch area of the front panel (see Figure 2-6).

The confirmation dialog box shown in Figure 2–8 is displayed. It tells you to save application updates, reminds you that the current session will be saved, and warns you that any items in the Trash Can will be permanently shredded.

2. **Click OK to continue the logout process.**

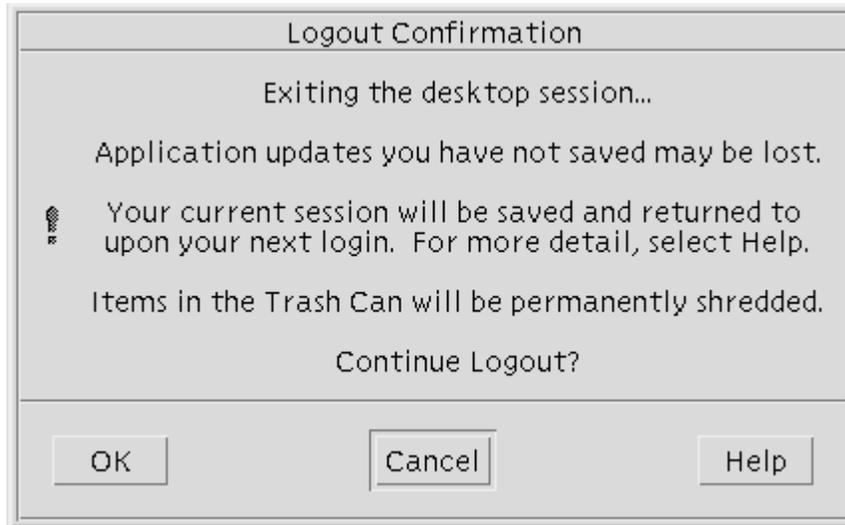


Figure 2–8 Logout Confirmation Dialog Box

To Shut Down Your System (for authorized users only)

Logging out is the normal way to end a Trusted Solaris session. If you need to turn off your machine (and you are authorized for shutting down your system), you should use the Shut Down command and then turn off your power. If you do shut down your machine, it may require rebooting by an user with additional authorization depending on your security policy.

1. **Select Shut Down from the Trusted Path menu.**
This causes a confirmation dialog box to be displayed.
2. **Select OK if you definitely want to shut down your system or Cancel if you want to reconsider.**

Note - The keyboard combination Stop-A (L1-A) is not available in the Trusted Solaris environment unless specially configured by your security administrator.

Enabling Logins When Logins Are Disabled

As a security measure, your administrator can configure your site so that all logins are disabled after a reboot. If a reboot has occurred and you are not authorized to enable logins, the dialog box shown in Figure 2-9 appears; you must notify your Trusted Solaris 8 administrator to help you log in. If you are authorized to enable logins, the dialog box shown in Figure 2-10 appears.



Figure 2-9 Disabled Logins Dialog Box for Users Unauthorized to Enable Logins

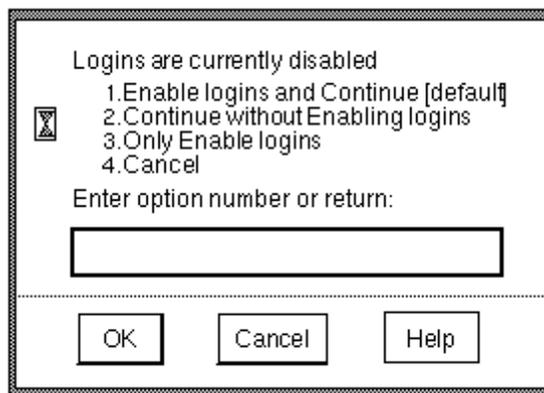


Figure 2-10 Disabled Logins Dialog Box for Users Authorized to Enable Logins

To Enable Logins After a Reboot

1. Enter the appropriate Enable logins option (see Figure 2-10):
 - a. Enter 1 to enable logins for all users and then log in, or 3 to enable logins for all users without logging in.
You should first check your site's security policy to ensure that enabling logins does not cause a security breach.
 - b. Enter 2 to leave other logins disabled and then log in, or 4 to leave other logins disabled and not log in.

Do this if you are not ready to enable logins.

2. **Click OK to enable or leave disabled the logins as specified or click Cancel to leave logins in their current state.**

Both options dismiss the dialog box and reset logins as specified.

Fixing a Bad Desktop Profile

If you have customized your shell initialization files (`.cshrc`, `.login`, etc.) and cannot log in, you can use the failsafe login feature to log in and correct the situation. In a standard login, the shell initialization files are sourced at startup to provide features customized for your environment. In a failsafe login, the default values are applied to your environment and no shell initialization files are sourced. This guarantees your ability to log in and permits you to fix any problems in shell initialization files.

To Perform a Failsafe Login

1. **Type your username in the text field in the username dialog box (see Figure 2-2).**
2. **Click the Options button and choose Failsafe Session from the Session submenu.**
3. **Click the OK button (or press Enter) and perform the rest of the steps in a standard login.**
4. **Edit the shell initialization file(s) where you think the problem may be occurring.**

Tour of the Trusted Solaris Environment

This chapter takes you for a quick tour of the Trusted Solaris environment. If you have access to a Trusted Solaris system, you can perform the steps as you read them; or you can get a good idea of the environment simply by reading and following the diagrams. The user account in the example is cleared for multilabel operation and is configured to display labels. The chapter discusses these topics:

- “Tour: Logging In” on page 49
- “Tour: Setting the Session Type” on page 50
- “Tour: Using the Label Builder to Set a Session Clearance” on page 52
- “Tour: Exploring the Basic Trusted Solaris Environment” on page 54
- “Tour: Launching an Application” on page 57
- “Tour: Looking at Files with the File Manager” on page 59
- “Tour: Changing to a Workspace at a Different Label” on page 61
- “Tour: Working in a Workspace at a Different Label” on page 62
- “Tour: Occupying Workspaces with Applications at Different Labels” on page 65
- “Tour: Moving Data Between Windows with Different Labels” on page 66

Tour: Logging In

As in the standard Solaris CDE environment, the Username dialog box is displayed when the system is waiting for logins (see figure below). To access the system, you have to identify yourself by your username and authenticate yourself by supplying your password.

1. **In the username dialog box, type your username in the text field and click OK (or press Enter).**

This step causes the password dialog box to be displayed.

2. **In the password dialog box, type your password and click OK (or press Enter).**

This step causes the Message of the Day dialog box to be displayed.

Tour: Setting the Session Type

The Workstation Information dialog box (see the following figure) displays the date and time of the last login, the message of the day from your administrator, and console messages (which you should inspect for possible security breaches). It also lets you specify the type of session: single-level or multilevel.

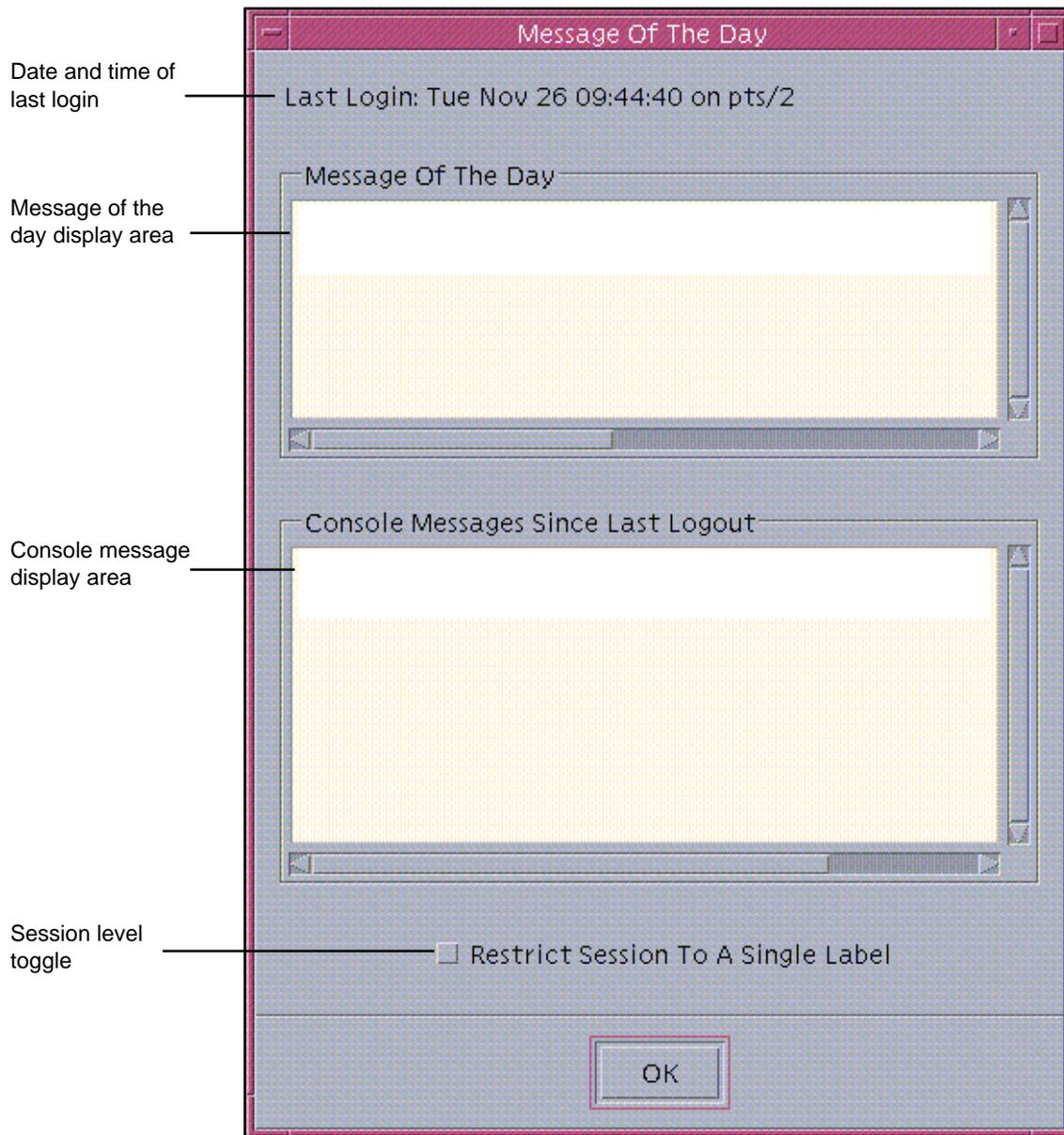


Figure 3-1 Workstation Information Dialog Box

1. Examine the date and time of last login, the Message of the Day, and the console message area.

This is good practice for preventing security problems.

2. Check that the **Restrict Session to a Single Label** button is not pushed in and then click **OK**.

The Session Level button indicates whether you are selecting a single- or multilevel session. Clicking **OK** sets the session type and causes the Message of the Day dialog box to be replaced by the Session Clearance Builder dialog box.

Note - If your account is configured for single-label operation, you cannot conduct multilevel sessions and the Session Clearance Label Builder dialog box will not be displayed on your system. However, you can participate in the following sections of this tutorial: “Tour: Exploring the Basic Trusted Solaris Environment” on page 54, “Tour: Launching an Application” on page 57, “Tour: Looking at Files with the File Manager” on page 59.

Tour: Using the Label Builder to Set a Session Clearance

The Session Clearance Builder dialog box (see figure below) is a typical label builder dialog box. Label builder dialog boxes are used throughout the Trusted Solaris environment whenever you have to enter a clearance or a label. Each label builder dialog box presents only those label combinations appropriate to your immediate situation and provides a default value in the selected value field.

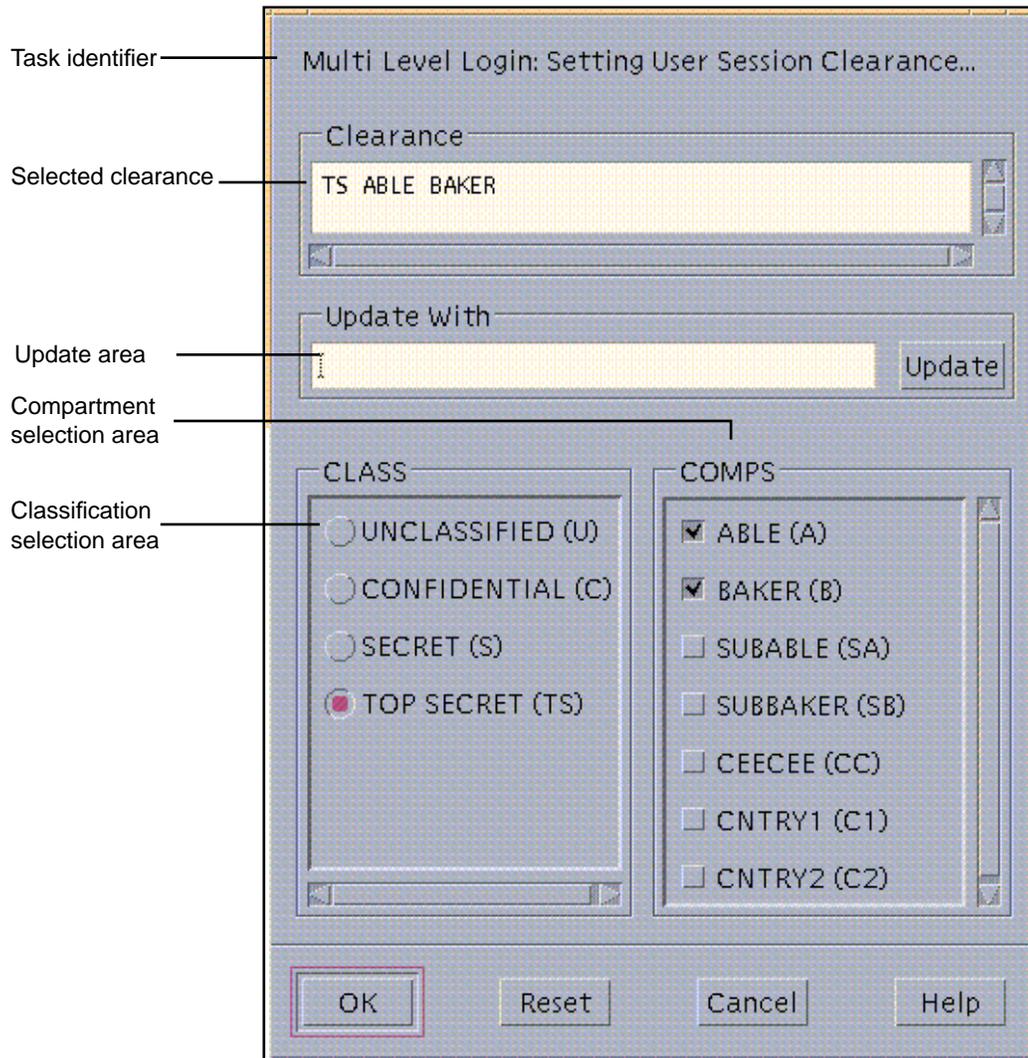


Figure 3-2 Typical Label Builder Dialog Box

For the tour, you need to set a session clearance higher than your minimum label; this is necessary to demonstrate how multilevel sessions work.

Note - In this example, the classification selection area is identified by the tag `CLASS` and the compartments area by the tag `COMPS`. These tags may be different in your configuration.

1. To use the default session clearance in the selected value field, click **OK** (or press **Enter**) and wait for the Trusted Solaris environment to be displayed. You can then proceed to the following section.

To build a different session clearance, go to the next step.

2. **Click the desired classification in the classification selection area.**
3. **Click the desired compartments (if any) in the compartment selection area.**
4. **Check the session clearance you have built in the Clearance field. Click the OK button (or press Enter) if it is correct or select a new classification and compartment(s) to build a different session clearance.**

After you close the Session Clearance dialog box, the Trusted Solaris environment is displayed.

Tour: Exploring the Basic Trusted Solaris Environment

This part of the tour looks at the basic elements of the Trusted Solaris environment before any applications are run or windows displayed. Note that this example environment is configured to display labels.

1. **Examine the Trusted Solaris environment.**

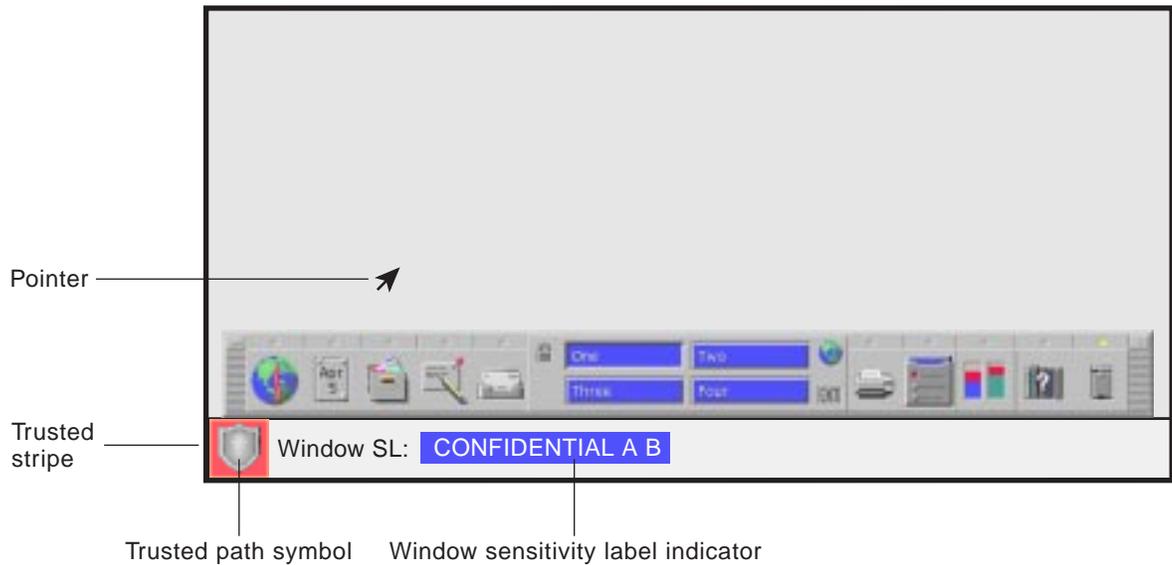


Figure 3-3 Basic Trusted Solaris Environment

The Trusted Solaris environment displays the trusted stripe at all times at the bottom of the screen and displays the trusted path symbol when you are interacting with the trusted computing base. (In this figure, the trusted path symbol appears because the pointer is in the Front Panel area and the Front Panel contains applications that can interact with the trusted computing base.) If the trusted stripe is missing from your window environment (other than when you lock your screen), notify your Trusted Solaris administrator at once; there is a serious problem with your system.

Note - The trusted stripe can be configured in different ways. This is explained in depth in “Label Displays in the Trusted Solaris Environment” on page 74.

The trusted stripe (see Figure 3-3) potentially has two elements:

- Trusted path symbol – is displayed when you perform any activity related to security.
- Window Label indicator – displays the label of the active window (that is, the window that has the pointer focus). In this example, the initial Window label for this workspace is CONFIDENTIAL A B, which is the minimum label for

this user. The window label indicator is optional and may not appear in your configuration.

Note - Note that the Window Label indicator is optional and may not be configured for your site.

2. **Hold down the right mouse button with the pointer in the workspace switch area but not over a workspace button.**

This displays the basic version of the Trusted Path menu.

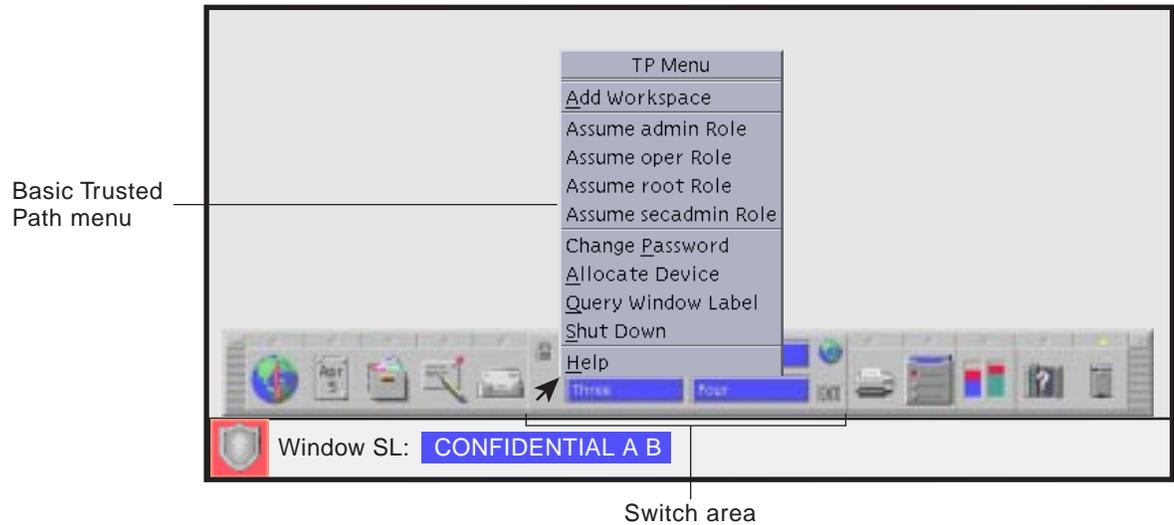


Figure 3-4 Basic Trusted Path Menu

The Trusted Path menu is used primarily to perform general security-related tasks. Notice that the trusted path symbol is displayed when you display the Trusted Path menu or position the pointer over any part of the trusted stripe or Front Panel.

3. **Hold down the right mouse button with the pointer over the Workspace Three button.**

This displays the workspace version of the Trusted Path menu, which contains options that can operate on that workspace. Note that the selections that appear in your menu depend on how your user account has been set up.

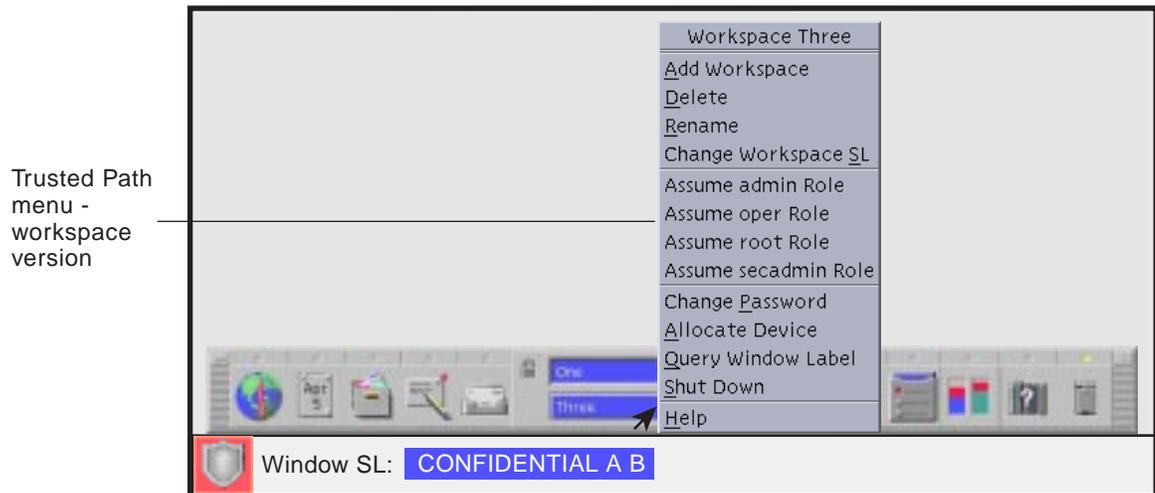


Figure 3-5 Trusted Path Menu - Workspace Version

Tour: Launching an Application

All applications in the Trusted Solaris environment have sensitivity. Applications are *subjects* in any data transactions and must dominate (have an equal or higher label than) the *objects* (usually files) they try to access. The label information for an application is displayed in the window label stripe both when the window is open and when it is minimized). An application's labels also appear in the trusted stripe when the pointer is in its window.

1. Click the Text Editor icon in the Front Panel to launch the Text Editor.

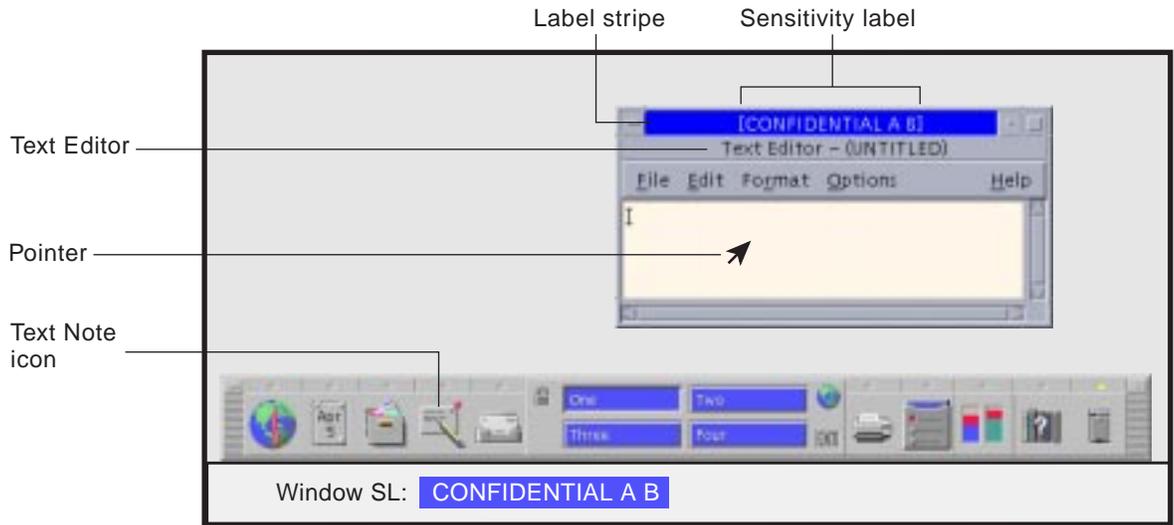


Figure 3-6 Running an Application

In the example, the Text Editor has CONFIDENTIAL A B as its label. All applications launched in this workspace, from either the graphical interface or from a shell window have the same label. The trusted path symbol does not appear in the trusted stripe since you are not accessing the trusted computing base.

- 2. Enter some text in the Text Editor and save the file (example shows textfile.1) using the Save option in the File menu.**

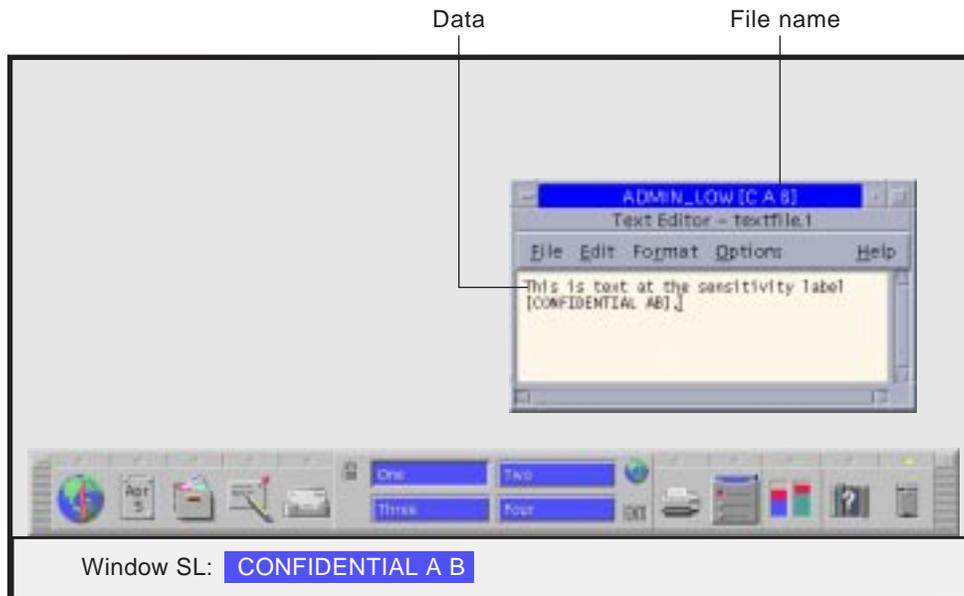


Figure 3-7 Entering Data and Saving a File

When you create a file in a Trusted Solaris session, the file takes on the label of the application that creates it, [CONFIDENTIAL A B] in the example.

Tour: Looking at Files with the File Manager

Files are objects in data transactions in the Trusted Solaris environment and can only be accessed by applications whose labels dominate the files' labels. Files can only be viewed from workspaces or by File Managers that have the same label.

- ◆ Click the File Manager icon to launch it.

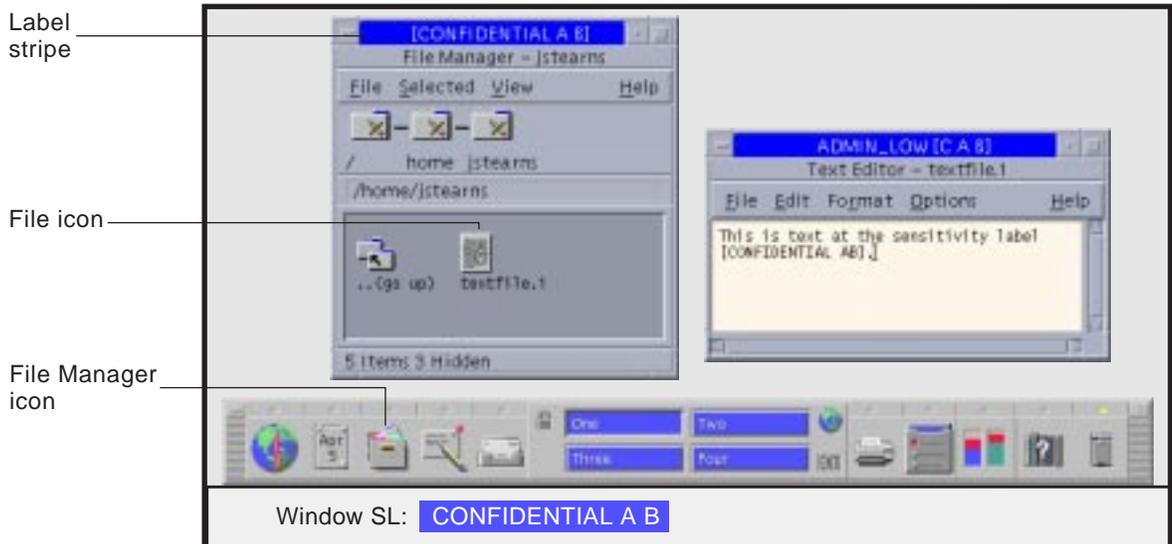


Figure 3-8 Using the File Manager

The File Manager is an application and is launched with the same labels as the current workspace. It provides access to only those files that are at its label.

As discussed in “Storing Files in Separate Directories by Labels” on page 25, the Trusted Solaris environment provides single-level directories (SLDs) and a multilevel directories (MLDs) to separate files and directories at different labels. Whenever you attempt to view or access files within a multilevel directory, you are effectively limited to the contents of the single-level directory at the current label. The following figure shows the contents of the home directory, which is `textfile.1` at this stage of the example.

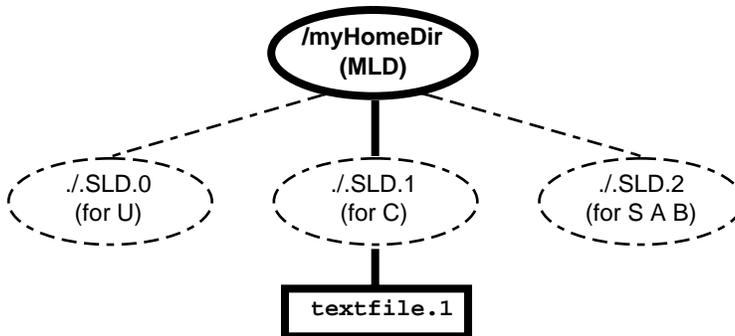


Figure 3-9 Visible and Hidden Files at CONFIDENTIAL Label

Tour: Changing to a Workspace at a Different Label

The ability to set workspace labels in the Trusted Solaris environment provides a safe and convenient means of working at different labels within the same session. To work at a different label you need to change the label on one of the available workspace buttons and then click that button to enter the workspace at the new label.

- 1. Hold down the right mouse button while the pointer is over a different workspace button to display the Trusted Path menu and select Change Workspace Label.**

This causes a label builder to be displayed in which you specify the new workspace label. The trusted path symbol reappears when you display the Trusted Path menu.

- 2. Enter a different label for the new workspace.**

Do this by selecting a classification in the classification area and one or more compartments in the compartments area and then clicking **OK**.

After you click **OK** (or press **Enter**) in the Workspace Label Builder dialog box, the environment switches to the new workspace (see figure below). The new workspace may have a different background and will indicate the new label in the trusted stripe. In addition, your system may be configured to color-code different labels, that is, apply the label's color to the appropriate workspace button(s), the Window Label indicator, and label stripes.



Figure 3-10 Entering a Workspace with a New Label

Tour: Working in a Workspace at a Different Label

A very major difference to note on entering a workspace with a different label is that you have access to a different set of files and no longer have direct access to the files in the workspace you just left.

1. Click the **File Manager** icon to view the contents of your home directory.



Figure 3-11 Examining Home Directory Contents in a Workspace with a New Label

At this sensitivity level, the file you created previously, `textfile.1`, is not visible. As shown in the figure below, the file created at the previous label cannot be viewed from the workspace at the new label.

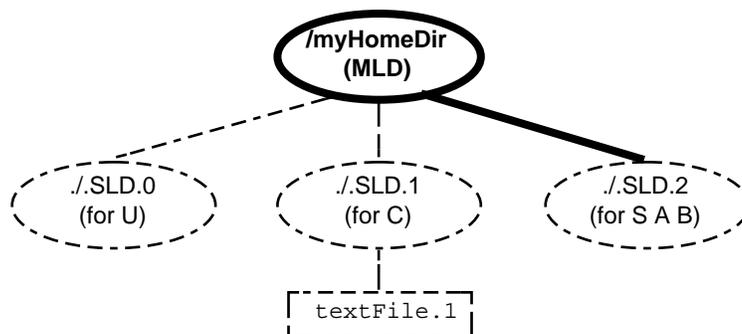


Figure 3-12 Visible and Hidden Files Initially at SECRET A B Label

2. Create a new file (textfile.2 in example) using the Text Editor.

The new text file has a label of SECRET A B.

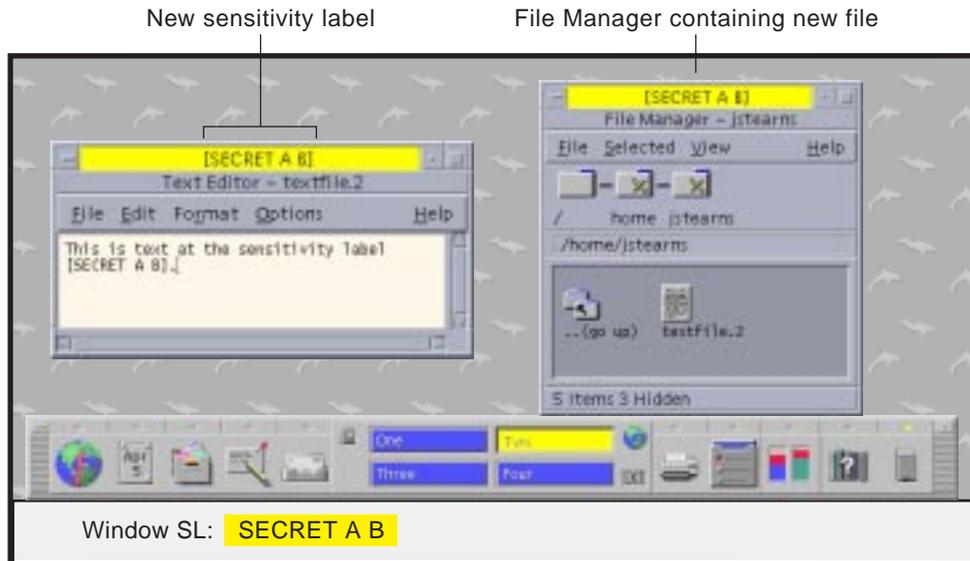


Figure 3-13 Creating a File in a Workspace with a New Label

3. Use the File Manager to view the contents of the home directory now.

The new file created at SECRET A B (textFile.2) is visible and the file created at CONFIDENTIAL (textFile.1) cannot be viewed.

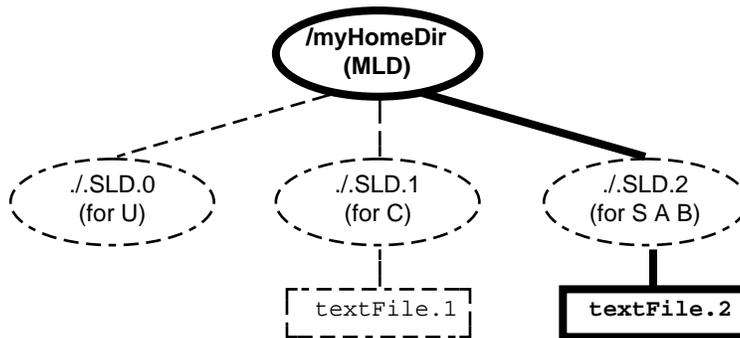


Figure 3-14 Visible and Hidden Files at SECRET A B Label After Creation of New File

Tour: Occupying Workspaces with Applications at Different Labels

Sometimes it is necessary to move an application at one label to a workspace at a different label. To do this, you need to open a workspace at a different label and then use the `Occupy Workspace` or `Occupy All Workspaces` command from a `Window` menu to place the window in another workspace.

Note - The `Occupy Workspace` commands do not let you occupy administrative role workspaces from a normal user workspace.

1. **From the window menu in the File Manager, select `Occupy Workspace`.**
This causes the `Occupy Workspace` dialog box to be displayed (see below).

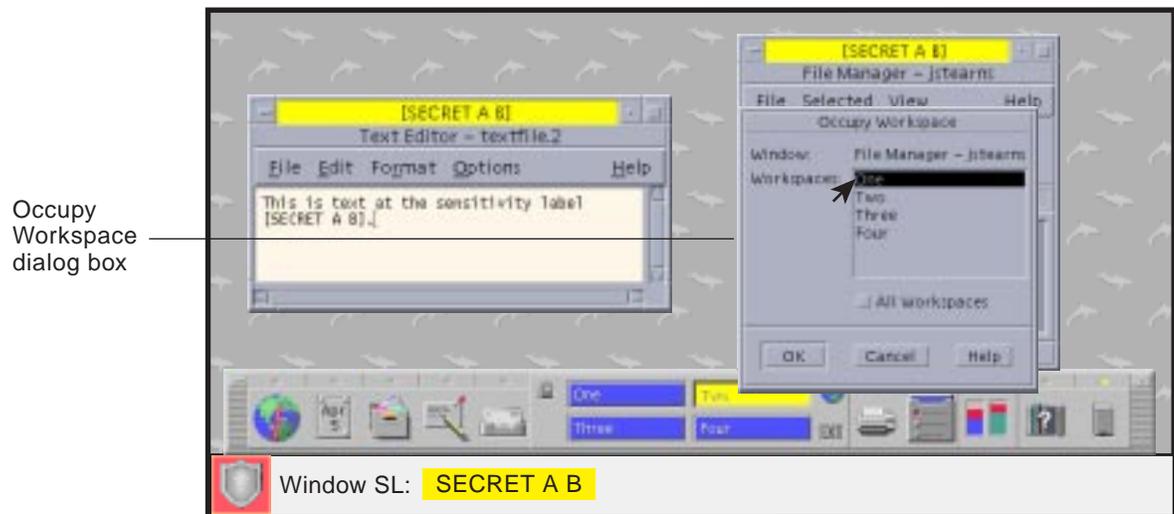


Figure 3-15 Selecting `Occupy Workspace`

2. **Choose the workspace that you used at the beginning of the tour and click `OK`.**
This moves the File Manager running at the current label [S A B] to the previous workspace, which is set to [C]. Note that the trusted path symbol reappears when the pointer is in the `Occupy Workspace` dialog box, because occupying a workspace has a potential effect on the trusted computing base.

3. **Repeat Step 1 on page 65 and Step 2 on page 65 for the Text Editor window.**
This moves the Text Editor window containing the current file to the previous workspace.
4. **Click the Workspace One button to return to the previous workspace.**
There should be four windows visible, the Text Editor and File Manager from Workspace One running at [CONFIDENTIAL A B] and the Text Editor and File Manager from Workspace Two running at [SECRET A B].

Tour: Moving Data Between Windows with Different Labels

As in standard Solaris, you can move data between windows in the Trusted Solaris environment. If you attempt to transfer information between windows with different labels or user UIDs, you are potentially upgrading or downgrading the label for that information. If your site's security policy permits this type of transfer and your account is authorized, a confirmation dialog box for confirming the transaction will be displayed; otherwise, the transfer will be prevented.

There are two methods for moving data between windows: (1) select it with the left mouse button and copy it with the middle mouse button or (2) Copy and Paste using menu commands, keyboard shortcuts, or function keys. Although you can move data across workspaces, it is much more convenient if both windows occupy the same workspace. Drag-and-drop operations do not work across windows with different labels.

1. **Minimize the File Manager windows for the time being.**

The two Text Editor windows should be visible as in the figure below.

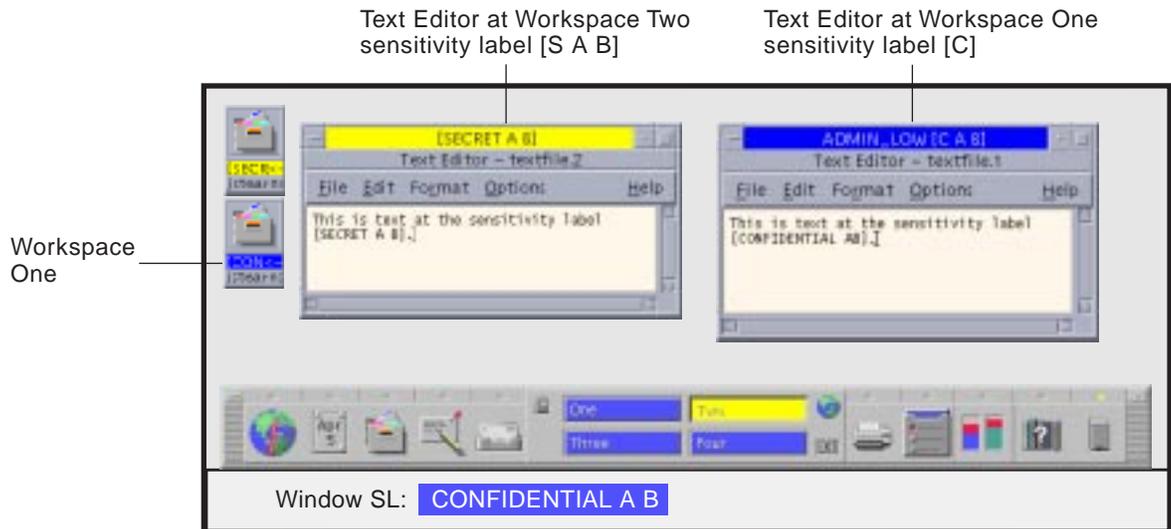


Figure 3-16 Displaying Applications at Different Labels

2. **Highlight the text in the [CONFIDENTIAL A B] Text Editor window and click the middle mouse button in the [SECRET A B] Text Editor window to paste the data.**

If this transaction is completed, the label of the transferred data will be upgraded. Before the transfer occurs, the Selection Manager Confirmation dialog box shown below is displayed.

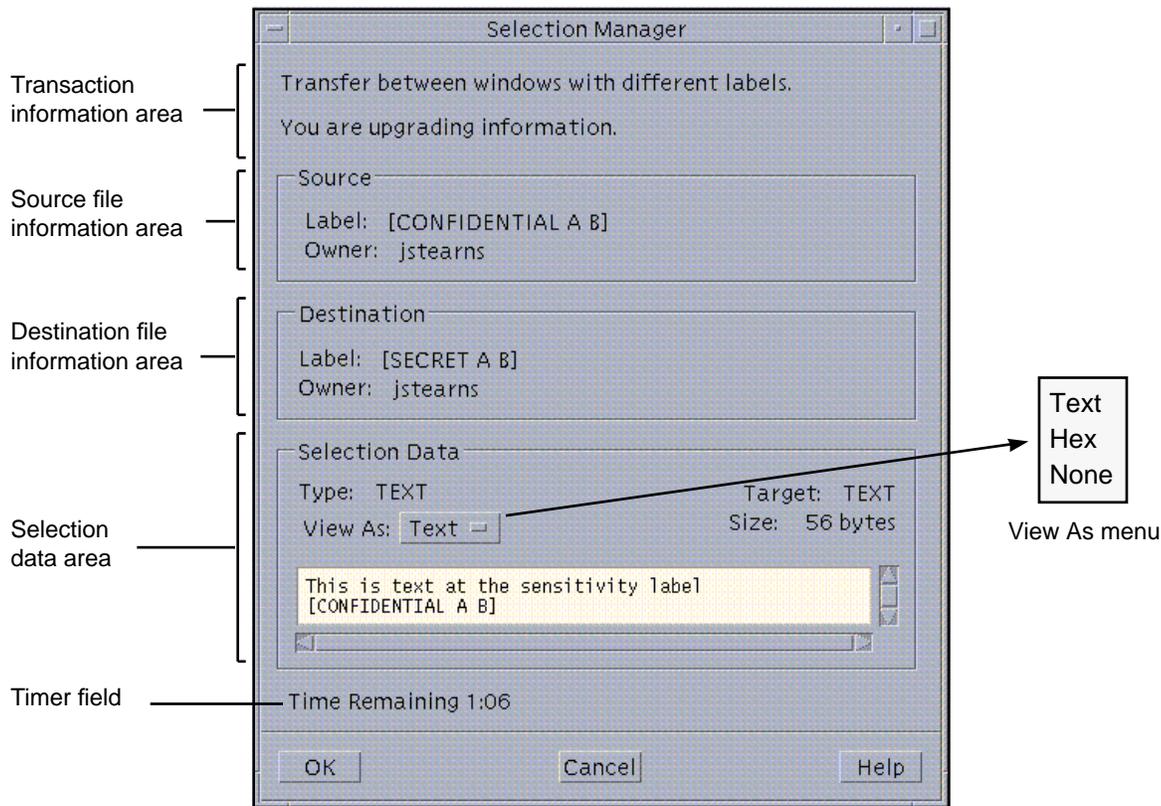


Figure 3-17 Selection Manager Confirmation Dialog Box

The Selection Manager Confirmation dialog box has these areas:

- Transaction information area – describes why confirmation of the transaction is needed.
- Source file information area – identifies the label and the owner of the source file.
- Destination file information area – identifies the label and owner of the destination file.
- Selection data area – identifies the type of data selected for transfer, the type of the target file, and its size in bytes. You can view the selected data in text or hexadecimal format in the scrollable display field or choose None and hide it altogether.
- Timer field – reminds you of the time left to complete the transaction. The amount of time and the use of the timer depends on your site's configuration.

3. Click OK to complete the transfer of the data from the [CONFIDENTIAL A B] Text Editor window to the [SECRET A B] Text Editor window.

The transferred data is now in the text editor with the label [SECRET A B]. If you had decided against the transaction, you could have clicked the `Cancel` button to stop the transaction.

Tour: Moving Files Between File Managers with Different Labels

The Trusted Solaris environment lets you change a file's label, provided you have the proper authorizations and are permitted to work in multilevel sessions. To make a file available in a different workspace you need to (1) make sure it is not in use, (2) display both the source and destination File Managers with different labels in the same workspace, and (3) use drag-and-drop techniques as follows:

- **Copying files** – To copy a file, drag it from one File Manager to the other while pressing the left mouse button and the `Control` key. This creates a new copy of the file in the second File Manager. Copying files is useful when you need files with the same name at different labels. For example, you could have an application that writes to a file with a specific name and you need to keep separate copies of the file.
- **Moving files** – To move a file, drag it from the source File Manager to the destination File Manager with the left mouse button. The file will only be available in the destination File Manager. Moving files is useful when you need to change the label of a file.
- **Linking files** – To link a file, drag it from the source File Manager to the destination File Manager while pressing the left mouse button, the `Control` key, and `Shift` keys. The file will be available in both File Managers but will use the label of the source File Manager. In general, you should link from a lower label to a higher label. A process at the higher label will be able to read the file but cannot write to it. Linking files is useful when you need to share a file that you access from different workspaces, for example the `.dtprofile` and `.login` files. Remember that you will have to work at the same label from which the file was originally linked to change that file.

1. Close both Text Editor windows and open the File Manager windows.

The file whose label is to be modified should be closed when you make the change—this is a good practice whenever you are changing a file's label. At this point, the workspace should appear as shown below.



Figure 3-18 Displaying File Managers at Different Labels

2. **Select `testfile.2` in the File Manager at [SECRET A B], drag it to the File Manager at [CONFIDENTIAL A B], and drop it.**

This causes the File Manager Confirmation dialog box in to be displayed (see figure below).

Note - If your system is not configured to permit upgrading or downgrading labels, a dialog box will be displayed stating that the transfer is not authorized.

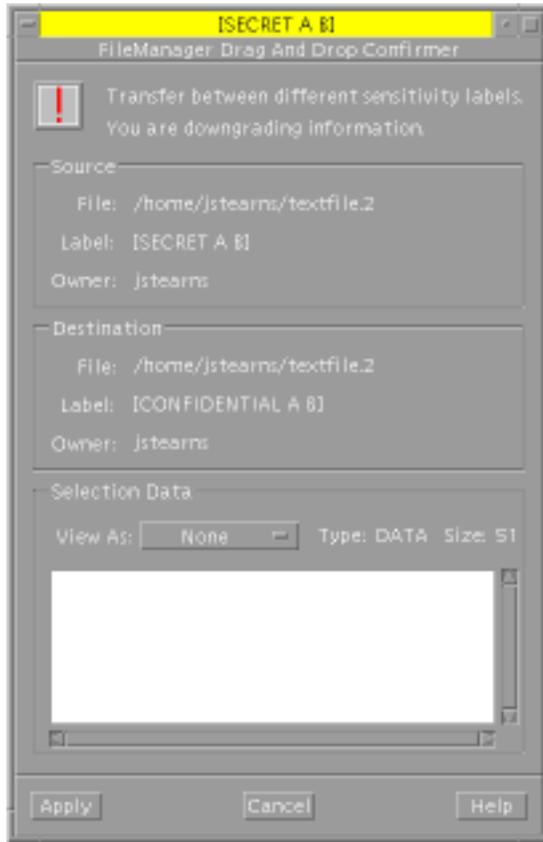


Figure 3-19 File Manager Confirmation Dialog Box

This dialog box is similar but not the same as the Selection Manager Confirmation dialog box. It has the following areas:

- Window stripe – contains the label which dominates in a comparison of the destination File Manager and the transferred data (there is no window stripe on the Selection Manager Confirmation dialog box).
- Transaction information area – describes why confirmation of the transaction is needed.
- Source file information area – identifies the path to the file, label information, and the owner of the source file (the Selection Manager does not identify a source file).
- Destination file information area – identifies the path to the file, the potential CMW label, and the owner of the destination file (the Selection Manager does not identify a destination file).

Note - Although the File Manager Confirmation dialog box does not display the single-level directory name in either the source or destination paths, the file will actually move from the single-level directory at the source label to the single-level directory at the destination label.

- Selection data area - identifies the type of file selected for the label change, how you wish to view it, and its size in bytes. You can view the file's data in text or hexadecimal format in the scrollable display field or choose `None` and hide it altogether. Resetting the `View As` menu affects the displays of subsequent transfers. Choosing `None` is useful for selections that consist of unreadable data.

3. Click the Apply button in the File Manager Confirmation Dialog Box to confirm your choice and close the dialog box.

This is the end of the regular tour. See Chapter 4, for detailed descriptions of the features in the Trusted Solaris environment.

Elements of the Trusted Solaris Environment

After you have successfully completed the login process, you can work within the Trusted Solaris environment, subject to the restrictions of your clearance, authorizations, and your choice of a single-level or multilevel session. This chapter explains the key elements in the Trusted Solaris environment. The chapter discusses these topics:

- “Basic Trusted Solaris Environment” on page 73
- “Label Displays in the Trusted Solaris Environment” on page 74
- “Trusted Stripe” on page 76
- “Front Panel” on page 77
- “Trusted Path Menu” on page 82
- “Other Trusted Solaris Environment Features” on page 92

Basic Trusted Solaris Environment

There are four major differences between the Trusted Solaris environment (see figure below) and the standard Solaris environment:

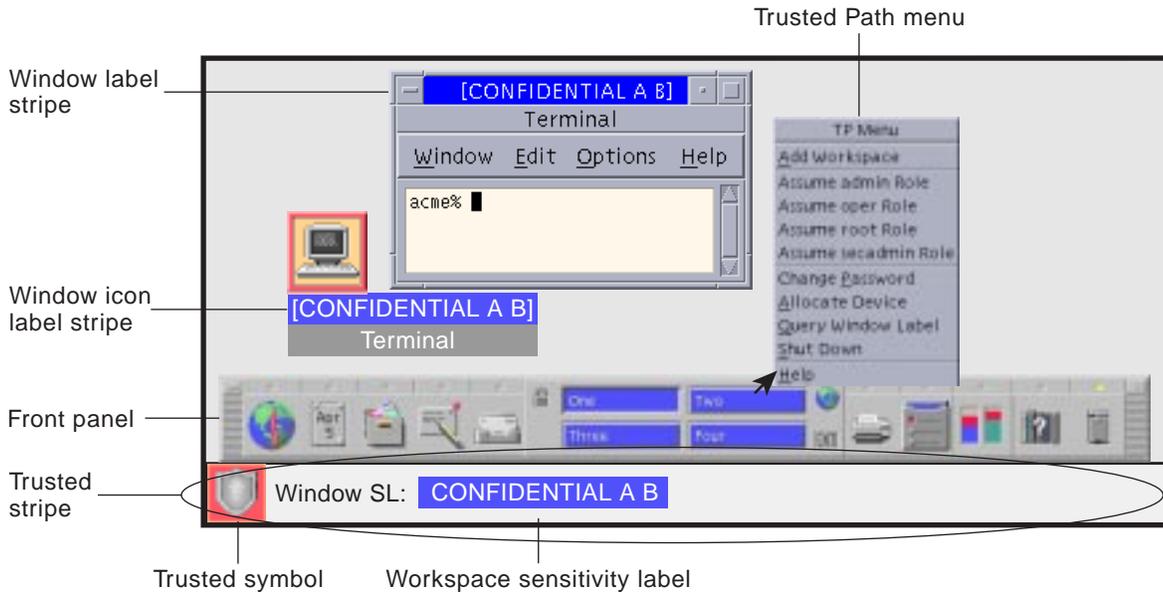


Figure 4-1 Basic Trusted Solaris Environment

- Label displays – All windows, workspaces, files, and applications have a label (which may be visible or hidden) associated with them. The graphical interface provides stripes and other indicators for viewing an entity’s labels.
- Trusted stripe – A special graphical security mechanism called the *trusted stripe* is always displayed at the bottom of the screen.
- Limited access to applications from Front Panel – The Front Panel provides access to only those applications permitted in your user account.
- Trusted Path menu – The switch area in the Front Panel lets you access the Trusted Path popup menu for performing security-related tasks.

Label Displays in the Trusted Solaris Environment

As discussed in “Mandatory Access Control” on page 20, all applications and files in the Trusted Solaris environment have labels (which may be hidden or visible) associated with them. The Trusted Solaris environment displays these labels in:

- window label stripes – above the window title bar
- window icon label stripes – under the minimized window
- the trusted stripe – in the Window Label indicator

- Query window label indicator – Trusted Path menu operation that displays the label of the window or icon specified by the pointer location

The following figure shows how labels display in an environment configured to display labels. It also shows the pointer and indicator when you select Query Window. (Labels appear inside square brackets ([]) .)

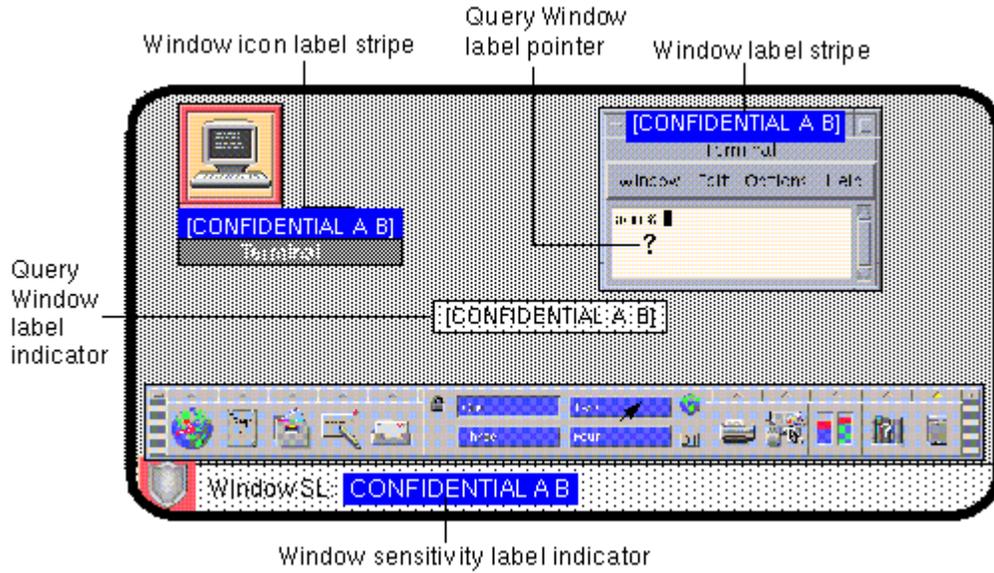


Figure 4-2 Window Labels in the Trusted Solaris Environment

A site can also be configured to hide labels, as shown in the following figure.

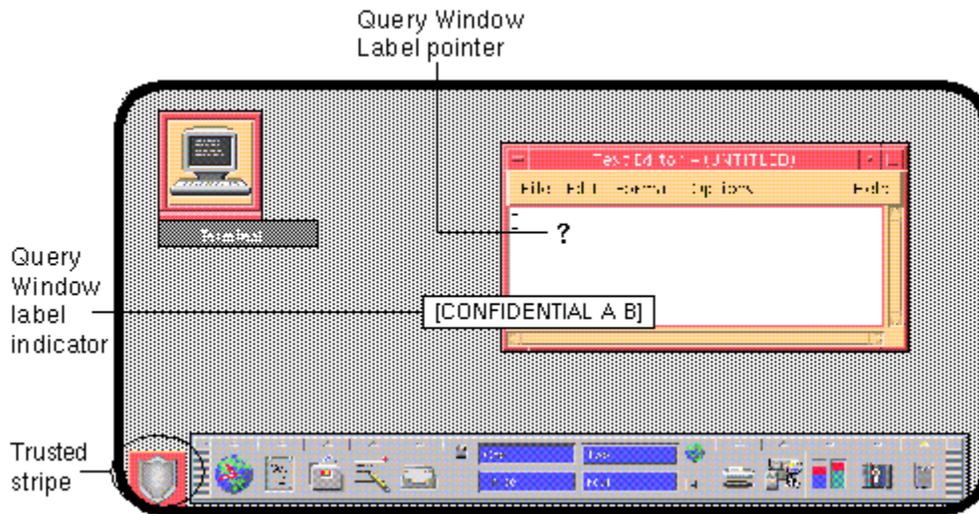


Figure 4-3 Trusted Stripe with Labels Suppressed

Trusted Stripe

The *trusted stripe* appears in a reserved area at the bottom of the screen in all Trusted Solaris sessions. Its purpose is (1) to give you a visual confirmation that you are in a legitimate Trusted Solaris session, (2) to let you know when you are interacting with the trusted computing base, and (3) to indicate the labels of your current workspace and window. The trusted stripe cannot be moved or obscured by other windows or dialog boxes. There are potentially two elements of the trusted stripe (depending on your site configuration):

- The trusted path symbol is required.
- The Window Label is optional.

Trusted Path Symbol

Whenever you access any portion of the trusted computing base, the *trusted path symbol* appears at the left of the trusted stripe area. (If your configuration suppresses labels, then the trusted path symbol appears with the trusted stripe to the left of the Front Panel as shown in the previous figure.) The trusted path symbol is not displayed when the pointer is focused in a window or area of the screen that does not affect security. The trusted path symbol cannot be forged; if you see it, you can be sure that you are safely interacting with the trusted computing base.



Caution - If the trusted stripe is missing from your window environment (other than when you lock your screen) or if the trusted path symbol is missing when you are attempting a security-related action, notify your Trusted Solaris administrator at once; there is a serious problem with your system. If the trusted stripe is visible when you lock your screen, this may be a problem as well.

Window Label Indicator

The *Window Label* indicator displays the label of the active window (that is the window that has the pointer focus). If you are working at one label at a time, this may be stating the obvious. However, in a multilevel session, it is possible to have windows with different labels in the same workspace. For an example, see “Tour: Occupying Workspaces with Applications at Different Labels” on page 65.

Front Panel

The Trusted Solaris front panel is very similar to the one used in standard CDE. It is more limited in that it provides access to only those applications, files, and utilities permitted that you are allowed to use. The major operational difference is that clicking the right mouse button anywhere in the workspace switch area causes a special pop-up menu called the Trusted Path (TP) menu to be displayed. Another difference is that before you can access a device through the Removable Media Manager, that device must be allocated using the Device Allocation Manager. The Device Allocation Manager is accessed from the Tools subpanel, which is above the Style Manager icon in the Front Panel.

If you minimize the front panel, you can restore it by clicking anywhere in the Trusted Stripe, double-clicking the minimized front panel icon, or selecting `Minimize/Restore Front Panel` from the Workspace menu.

In the Trusted Solaris environment, Install Icon dropsites are limited to applications and files permitted in your user account and subject to any limitations on the particular application. For example, an application may not be operational below a set label.

Workspace Switch Area

In the Trusted Solaris environment, the workspace buttons not only define separate workspaces but let you work at different labels if you are conducting a multilevel

session (in a single-level session, you can only operate at one label). When you begin a multilevel session, each workspace is set to the lowest label assigned to you. If your administrator has color-coded workspace buttons by classification, the workspace buttons will appear in the appropriate color.

To change to a workspace at a different label, you click the right mouse button over the workspace button and select `Change Workspace Label`. This causes a label builder to be displayed in which you enter the new label. You can then click the workspace button to work at the new label. Note that the `Occupy Workspace` and `Occupy All Workspaces` selections in the window menus let you display windows with different labels in the same workspace.

Clock

The clock works exactly the same as in the standard CDE environment. In the Trusted Solaris environment, however, only an administrator can change the date and time for your workstation.

Calendar

The calendar shows the appointments for you at the label of your current workspace only. To view appointments at a different label, you need to change to a workspace at that label if you are in a multilevel session or log out and back in if you are in a single-level session.

File Manager

In the Trusted Solaris environment, the File Manager has certain limitations on the files (and folders) that it can display. The File Manager displays files at the label of the current workspace. To operate on (or view) files at more than one label at a time, you run the File Manager from workspaces at different labels and then use the `Occupy Workspace` command to display the different File Managers in the same workspace.

The File Manager lets you change a file or folder's basic permissions, access control list (ACL), and information. You can also move, copy, or link files between File Managers at different labels. For more information on the File Manager and its capabilities, see Chapter 5.

You can view (but not write to) files and directories that are not at your current workspace label by specifying a pathname with adornments, as in `/ .MLD.myHomeDir/ .SLD.0`. However, you can only write to files and directories dominated by your current workspace label.

Text Editor

The Text Editor can edit files at the label of the current workspace only. If you need to move data from a Text Editor to a file at a different label, you change a workspace label, open the Text Editor at the second label, and copy the text in one Text Editor and paste it in the other.

Personal Applications Subpanel

The default applications in the personal applications operate basically the same as in the standard CDE environment. The terminal icon launches the default shell assigned to you by your administrator. When you use a web browser, the label of the browser must be the same as the label of the web server.

Mailer

In the Trusted Solaris environment, all mail messages are assigned a label. The Mailer sorts incoming mail by label and role and displays separate mail notifier icons in its subpanel (see figure below). This feature lets you focus on mail at labels of interest to you and defer reading mail at other labels. The Mailer operates at one label at a time only. Clicking the Mailer icon in the Front Panel opens the Mailer at the label of the current workspace; clicking a Mailer icon with a label in the subpanel opens the Mailer at that label.



Figure 4-4 Mail Notifier Icons in the Mail Subpanel

When you send mail, the mail will go out at the label of the mail tool in which you compose the message. Only hosts and users that are cleared for that label will receive this mail.

If you need to use the vacation message option in the Mailer, you must explicitly enable vacation message replies for each label at which you typically receive mail. Check with your security administrator for your site's security policy for vacation messages.

The CDE Mailer is supplied by default. If you prefer a different mail application, contact your administrator to ensure that your preferred mail application is installed properly. Although you can install a different mail application by dropping its icon on the Install Icon dropsite in the subpanel, you will lose the notification-by-label feature.

Printer

The Print Manager in the Personal Printers subpanel displays icons for all printers accredited up to your clearance. However, you can use only those printers accredited to print documents at the label of the current workspace.

A typical print job in the Trusted Solaris environment includes:

- banner page at the beginning of the print job – identifying the print job, handling instructions and labels appropriate to the site
- labeled pages – with labels in the heading and footer
- trailer page at the end of the print job – signalling the end of the job

A typical banner page appears in the following figure. The words “JOB START” indicate the banner page.

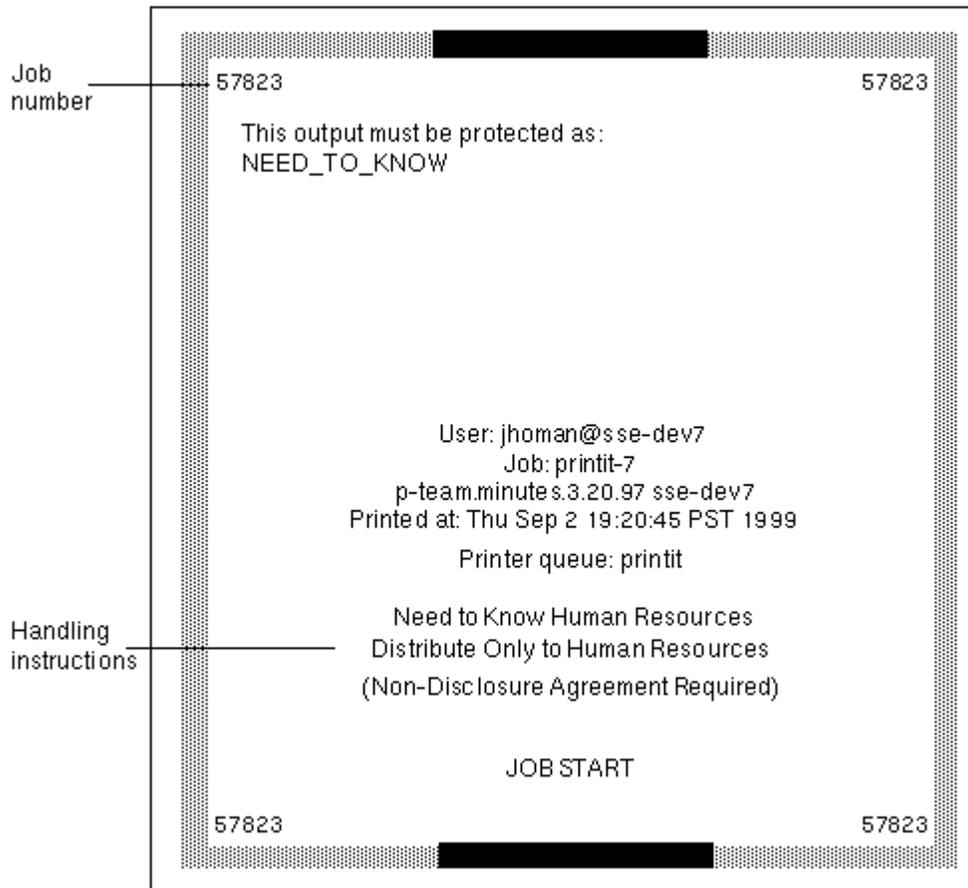


Figure 4-5 Typical Print Banner Page

For the exact security information regarding printing at your site, please see your administrator.

Desktop Style Manager

The Desktop Style Manager operates in the same manner as in standard Solaris with two exceptions:

- The Screen Blanker and Screen Lock options are limited. Your administrator specifies the maximum amount of time that your system can be idle prior to being secured. You can reduce the idle time but cannot increase it above the maximum. You can still choose a pattern for when the screen is locked. See your administrator if you are not familiar with the policy at your site.

- The Startup control sets your startup session settings according to the label or clearance that you specify at login. Thus, you can have a different session defined for each label in your account label range.

Application Manager

The Application Manager provides access to only those applications and utilities that have been assigned to you by your administrator. If you can assume a role, you will have access to a different set of applications and capabilities. Remember that the ability of a function to operate on a file depends on the label of the current workspace.

Similarly, although you can add applications to the Personal Application submenu by dropping icons onto the Install Icon dropsite, you can only run them if your administrator has assigned these applications to you.

Trash Can

In the Trusted Solaris environment, the trash can stores files to be deleted by label. Although you can drop files at any label in the trash can, it displays files at the current label only. You cannot view files that are in the trash can at other labels. It is good practice to use the Shred selection from the File menu in the trash can window to delete sensitive information as soon as you put it in the trash can.

Trusted Path Menu

The Trusted Path (TP) menu can be accessed by holding down the right mouse button in the switch area of the Front Panel. The Trusted Path menu adds the following menu items in addition to the normal switch menu items:

- **Change Workspace Label**—changes the label of a workspace so that you can work at a different label (only displayed when the pointer is over a workspace button).
- **Assume *role* Role**—lets you assume a role assigned to your user account.
- **Change Password**—lets you change passwords in accordance with your site's security policy.
- **Allocate Device**—displays the Allocation Manager so that you can allocate a device for use.
- **Query Window Label**—lets you determine the label of the next window you click in.

- **Shutdown**—lets you reboot the system if you are permitted by your site's security policy.

Add Workspace

`Add Workspace` lets you add another button to the switch area for accessing another workspace. This operates similarly to the standard version of CDE, except that the new workspace button takes on the security characteristics of the workspace under the pointer or, if the pointer is not over a workspace button, the characteristics of your minimum label.

Delete

`Delete` lets you remove a workspace from the switch area just as in standard Solaris CDE. It is good practice to quit all applications in a workspace prior to closing it; otherwise these applications may continue to run invisibly or in a different workspace.

Rename

`Rename` lets you rename a workspace from the switch area just as in standard Solaris CDE. The text in the workspace button becomes editable and lets you enter a new name.

Change Workspace Label

`Change Workspace Label` lets you change the label of a workspace to any label between the minimum label assigned to you and your current session clearance (for multilabel sessions only). When you choose `Change Workspace Label`, a label builder dialog box is displayed. After you enter a new label, the label (and if implemented the color) of the workspace button changes. When you click on the workspace button, you enter a session at the new label.

Role Assumption Selections

`Assume <site-specific> Role` lets you change roles. Remember that a role is a special user account that gives you access to certain applications and the authorization(s) you need to run these applications. The administrator at your site assigns roles. If

your account has not been assigned any roles, the assume role selections do not appear in the Trusted Path menu.

When you make a role assumption selection, a dialog box is displayed requesting the password for the role (see figure below). After successfully entering the password, a workspace button with the role name is displayed and you are shifted to this workspace. The role workspace provides you with the special set of applications, privileges, authorizations, and the UID assigned to this role. Remember that for auditing purposes your user account UID is attached to all transactions you make while in this role.

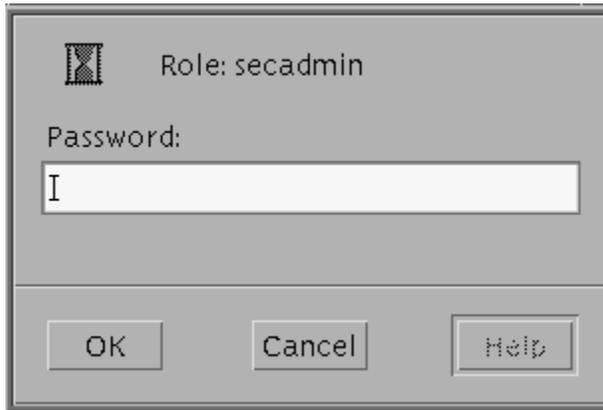


Figure 4-6 Role Password Dialog Box

Change Password

`Change Password` lets you change your password. Frequently changing passwords shortens the window of opportunity for intruders using illegally obtained passwords; thus, your site's policy may require you to change your password regularly. Your administrator has a number of options for changing your password:

- minimum number of days between changes – prevents you or anyone else from changing your password for a set number of days.
- maximum number of days between changes – requires you to change your password after a set number of days.
- maximum number of inactive days – locks your account after the set number of days of inactivity if the password has not been changed
- expiration date – requires you to change your password by a specific date

If your administrator has implemented one of the options requiring you to change your password, you should receive a message warning you to change your password prior to the cutoff date. You will be required to change your password by one of two methods, depending on your site's security policy

- Direct entry
- Choosing from a list of system-generated passwords

To Change Passwords by Direct Entry

1. Select Change Password from the Trusted Path menu.

You access the Trusted Path menu by holding down the right mouse button while the pointer is over the switch area in the Front Panel.

2. Choose a new password.

It must meet the following criteria:

- The password must be 8 characters in length. (More than 8 characters can be entered but only the first 8 characters are significant.)
- The password must contain at least two alphabetic characters and at least one numeric or special character.
- The new password must differ from your previous password; you cannot use a reverse or circular shift of the previous password. (For this comparison, upper case letters and lower case letters are considered to be equal.)
- The new password must have at least three characters different from the old. (For this comparison, upper case letters and lower case letters are considered to be equal.)
- It should be difficult to guess. Do not use a common word or a proper name, as individuals attempting to break into an account occasionally use lists to try to guess users' passwords.

3. Type your old password in the Change Password dialog box and click OK.

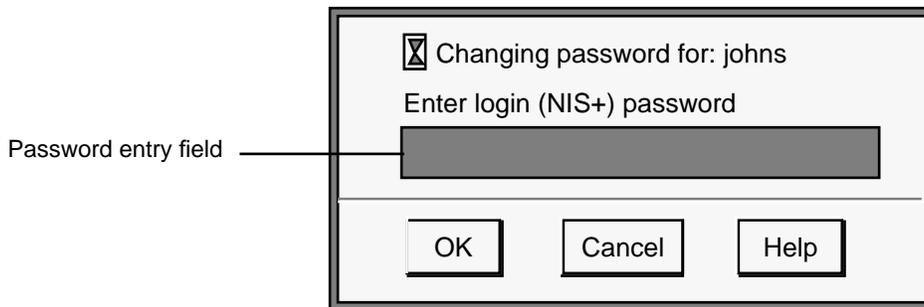


Figure 4-7 Change Password Dialog Box

This confirms that you are the legitimate user associated with this user name. For the sake of security, the password is not displayed as you type it.



Caution - When you enter your password, make sure that the cursor is over the Change Password dialog box and that the trusted path symbol is displayed. If the cursor is not over the dialog box, you can inadvertently type your password into a different window where it could be seen by another user. If the symbol is not displayed, then someone may be attempting to steal your password and you should notify your security administrator at once.

4. Type the new password in the Change Password Confirmation dialog box and click OK.

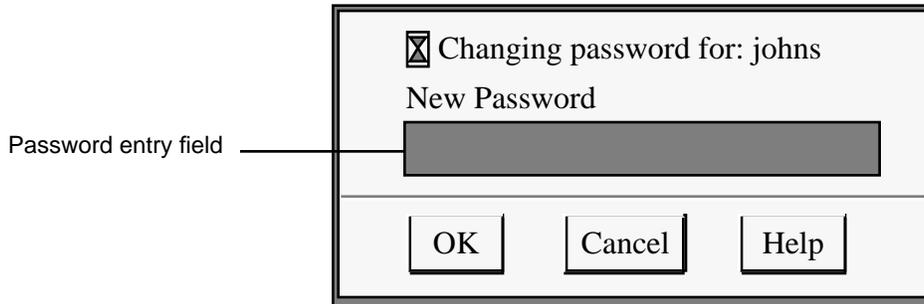


Figure 4-8 Change Password Confirmation Dialog Box

5. Type the new password in the Change Password Reconfirmation dialog box and click OK.

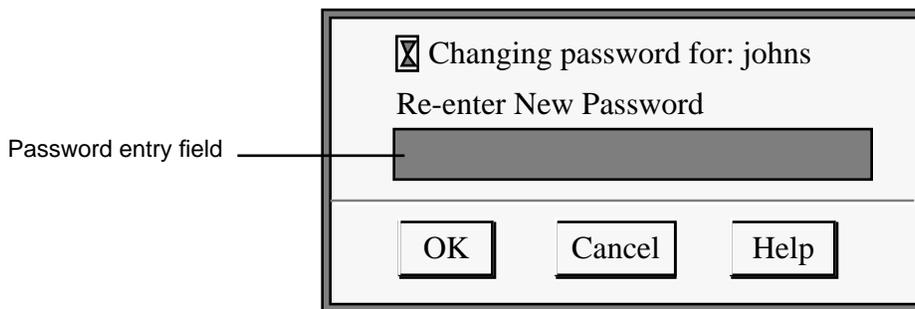


Figure 4-9 Change Password Reconfirmation Dialog Box

This step confirms your choice.

6. Click the OK button in the dialog box (not shown) that notifies you that the change has been made.

To Change Passwords by Choosing from a List

Your administrator has the option to require users to select new passwords from lists of system-generated passwords. Trusted Solaris 8 generates passwords that are pronounceable but difficult for intruders to guess.

1. **Select Change Password from the Trusted Path menu.**

A dialog box requesting your current password is displayed (see Figure 4-7). After you enter your password and click OK, a dialog box similar to the one shown below is displayed (if your system is configured for system-generated entry). The Password Generator dialog box provides you with a choice of five unique system-generated passwords. The pronunciation mnemonic shown in parentheses to the right of each password divides the password into syllables to make it easier to remember.

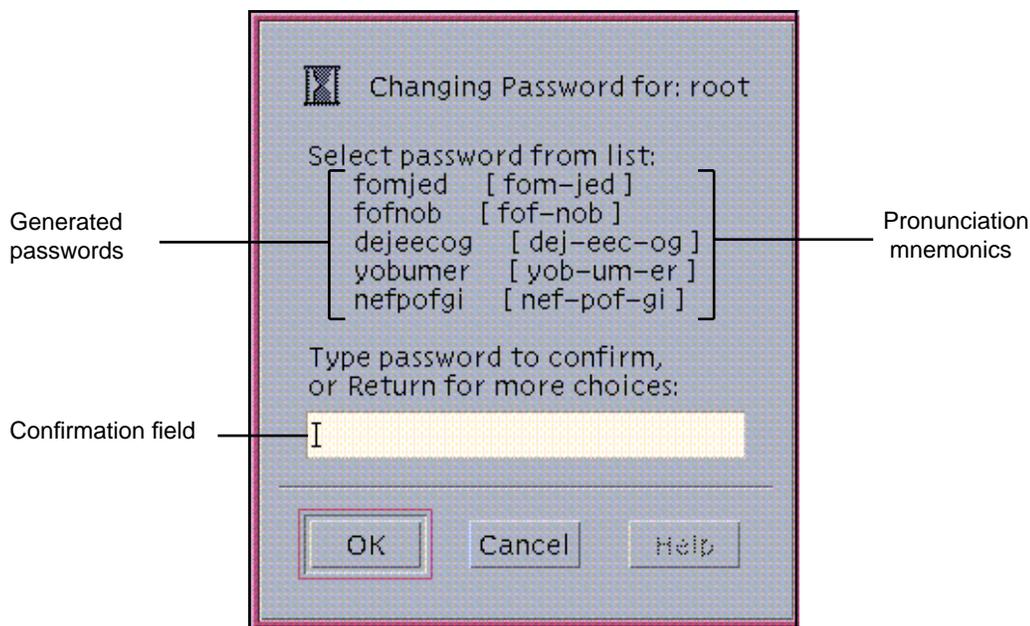


Figure 4-10 Password Generator Dialog Box

2. **Read the five password choices.**
 - a. **If you want to use one of these choices, enter it in the confirmation field and press Enter or click OK.**

This step establishes your choice.

- b. If you want to select from a different set of choices, leave the confirmation field blank and press Enter or click OK.**

This step causes five new selections to be displayed. If one of these selections is suitable, enter that choice and press Return or click OK; otherwise repeat this step to get five new selections.

- 3. After you are prompted for the password again, re-enter your choice in the confirmation field and press Enter or click OK.**

This step confirms the spelling of your choice and gives you practice at entering it. It closes the dialog box.

To Choose a Password from a List at the Command Line

A command line version of the password generator is provided as an alternative to the Password Generator Dialog Box. Note that this version is available to users in administrative roles only.

- 1. Type `passwd`**

A set of five generated password choices as follows.

```
Select password from list:
  rocskovi      [ rocs-kov-i ]
  phuzpeca     [ phuz-pec-a ]
  bephzoba     [ beph-zo-ba ]
  eblircit     [ e-blirc-it ]
  yeaskedo     [ yeas-ke-do ]

Type password to confirm,
or Return for more choices:
```

- 2. Read the five password choices.**

- a. If you want to use one of these choices, enter it and press Enter.**

This step establishes your choice.

- b. If you want to select from a different set of choices, press Enter without making an entry.**

This step causes five new selections to be displayed. If one of these selections is suitable, enter that choice and press Return; otherwise repeat this step to get five new selections.

3. **After you are prompted for the password again, re-enter your choice in the confirmation field and press Enter.**

This step confirms the spelling of your choice and gives you practice at entering it.

Allocate Device

Allocate Device is available to authorized users only. It lets you mount and allocate a device so that you can securely move data on or off the system to another medium. If you try to use a device without allocating it, you will get the error message “Permission Denied.”

To Allocate a Device

1. **A) Select Allocate Device from the Trusted Path menu.**

This step causes the Device Allocation Manager to be displayed.

OR

1. **B) Select Device Allocation Manager from the Tools subpanel in the Front Panel.**

This is an alternative step for displaying the Device Allocation Manager (see below).



Figure 4-11 Device Allocation Manager

2. Look in the available device list for the device you wish to use.

The devices that you are permitted to allocate at your current label appear in this list. Table 4-1 shows some typical device names.

TABLE 4-1 Device Name Abbreviations

Abbreviated Device Name	Long Version of Device Name
audio	microphone and speakers
floppy_0	floppy drive
mag_tape_0	tape drive (streaming)
cdrom_0	CDROM drive

If the device you want to use does not appear in the list, you should check with your administrator to make sure you are properly authorized. It may also be that the device is in an error state or in use by somebody else.

3. Move the device from the Available Devices list to the Allocated Devices list.

You can accomplish this by:

- Double-clicking the device name in the Available Devices list
- Selecting the device and clicking the `Allocate` (right-pointing) button

This step starts the clean script. The clean script ensures that there is no data left over on the medium from other transactions.

Note that the label of the current workspace will be applied to the device. Any data transferred to or from the device's medium must be dominated by this label.

4. Follow the instructions in the clean script dialog boxes to (1) load and make sure the medium has the correct label and (2) mount the device.

At this point, the medium has been cleaned and the device has been mounted and is ready to be used. The device name now appears in the Allocated Devices list.

Note - Until you close the command tool window, the Device Allocation Manager and its label builder windows are disabled. At this point, you will not be able to use the Device Allocation Manager in this workspace or any other.

5. Use the device to transfer data.

At any point, if you switch to a workspace with a different User ID (by assuming a role) or label, you need to make a separate allocation of the device at the label for that workspace. When you use the `Occupy Workspace` command from the window menu to move the Device Allocation Manager to the new workspace, the Available and Allocated Devices lists change to reflect the correct context.

6. Deallocate the device when you are finished.

For the sake of security, you should always deallocate a device when you are finished using it. You can accomplish this by:

- Double-clicking the device name in the Allocated Devices list
- Selecting the device and clicking the Deallocate (left-pointing) button

Deallocating a device runs a clean script that advises unmounts the device and advises you when the media can be removed.

If you reboot your system while devices are allocated, they become deallocated.

Query Window Label

`Query Window Label` changes the pointer to a question mark. As you move the pointer around the screen, the label for the region under the pointer is displayed in a small rectangular box at the center of the screen (see below). When you click the mouse button, you return to normal mode. This operation is mainly useful if your system is not configured to display labels in the window frames.

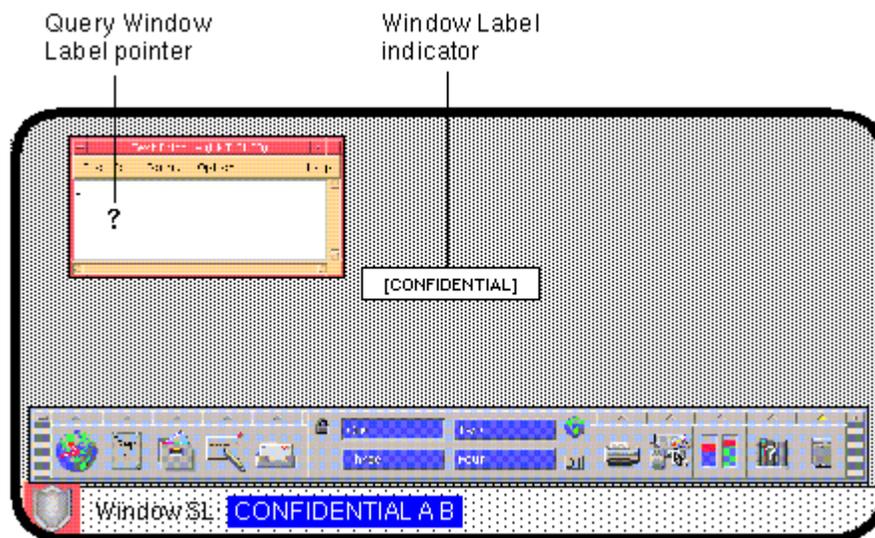


Figure 4-12 Query Window Label Operation

Shut Down (for authorized users only)

`Shut Down` lets you shut down your machine (if you are authorized). This is not the normal way of ending a Trusted Solaris session; the normal logout method is clicking the `Exit` icon in the switch area of the Front Panel. When you select `Shut Down`, you are first queried for confirmation and then permitted to shut down the workstation. If you need to turn off your machine, you should use the `Shut Down` command and then turn off your power.

Note - If you do shut down your machine, rebooting it may require further authorization and extra passwords depending on your site's security policy.

Help

`Help` provides online help information including various topics on elements in the Trusted Solaris environment including a glossary. Individual tools provide specific help directly through `Help` buttons and menus.

Other Trusted Solaris Environment Features

This section describes features in the Trusted Solaris environment not covered in the other sections of this chapter.

Lock

Clicking the `Lock` icon locks your screen so that no one else can use your workstation. To unlock your workstation, you need to supply your password. See "To Lock and Unlock Your Screen" on page 44 for a description of this procedure.

Exit

Clicking the `Exit` icon displays the Exit Session dialog box for exiting the session. See "To Log Out of the Trusted Solaris Environment" on page 44 for a description of this procedure.

Occupy Workspace Commands

The `Occupy Workspace...` and `Occupy All Workspaces` commands have additional security implications in the Trusted Solaris environment. They enable you to occupy a workspace with a window at a different label, which may be convenient for viewing data. The ability to move data from a window at one label to a window at another label must be granted by the security administrator.

Note that the `Occupy Workspace` commands do not let you occupy administrative role workspaces with windows from a normal user workspace.

Managing Files and Directories

This chapter shows you the basics of managing the security of files and directories in the Trusted Solaris environment. The chapter discusses these topics:

- “Setting Permissions and Access Control Lists” on page 95
- “To Display the Properties Dialog Box for a File or Folder” on page 100
- “To View the Basic Information of a File or Folder” on page 101
- “To View or Change a File or Folder’s Basic Permissions” on page 102
- “To View a File or Folder’s ACL Entries” on page 104
- “To Add an ACL Entry” on page 104
- “To Change an ACL Entry” on page 105
- “To Delete an ACL Entry” on page 107
- “To Determine a File’s Label” on page 108
- “To Change a File’s Label (Move Operation)” on page 110
- “To Create a Copy of a File at a Different Label (Copy Operation)” on page 111
- “To Link a File to a Different Label (Link Operation)” on page 112
- “Copying and Linking Files to Different Labels by Default” on page 112

Setting Permissions and Access Control Lists

The File Manager is the main tool for working with files and directories. It has been slightly modified for the Trusted Solaris environment to accommodate mandatory

access control. This section focuses on the basic permissions and access control list (ACL) for files and folders in the Trusted Solaris environment. For other information on the File Manager, refer to the base Solaris documentation.

The File Manager provides the two methods for displaying the Properties dialog box. You can hold down the right mouse button over the specified file and select *Properties...* from the File Manager pop-up menu or you can select the file and choose *Change Properties* from the Selected menu. Both methods cause the Properties dialog box to be displayed. The Properties dialog box can display three types of properties:

- Permissions – by selecting the permissions toggle and Hide Access List (see the permissions mode dialog box below)

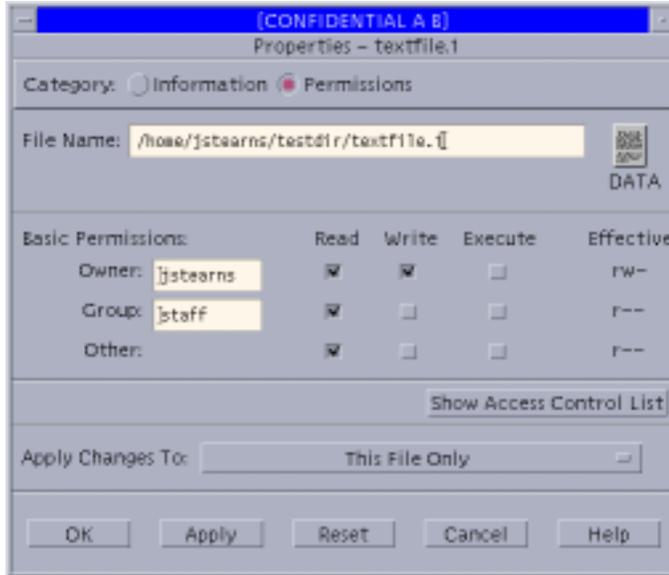


Figure 5-1 File Properties: Permissions Mode — Hide ACLs

- ACLs – by selecting the permissions toggle and Show Access Control List (see the ACLs mode dialog box below)

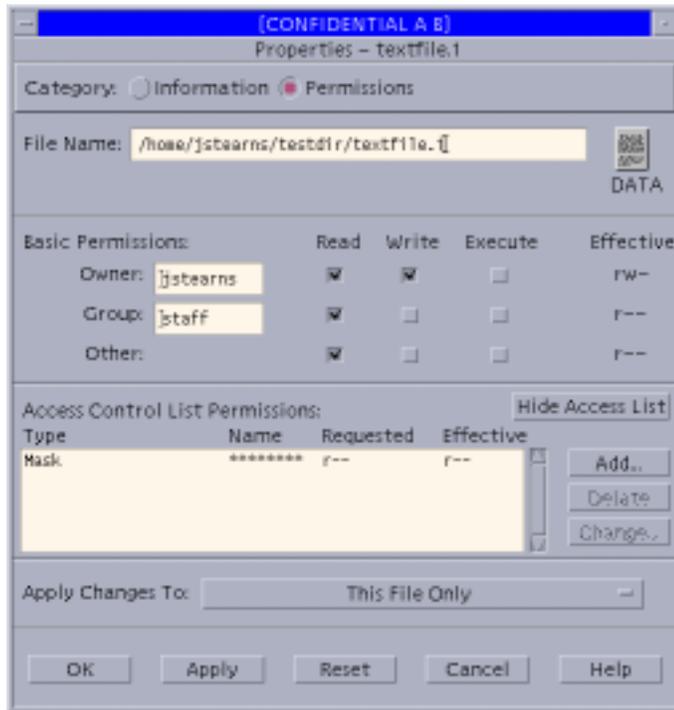


Figure 5-2 File Properties: Permissions Mode — Show ACLs

- Basic information – by selecting the information toggle (see the information mode dialog box below)

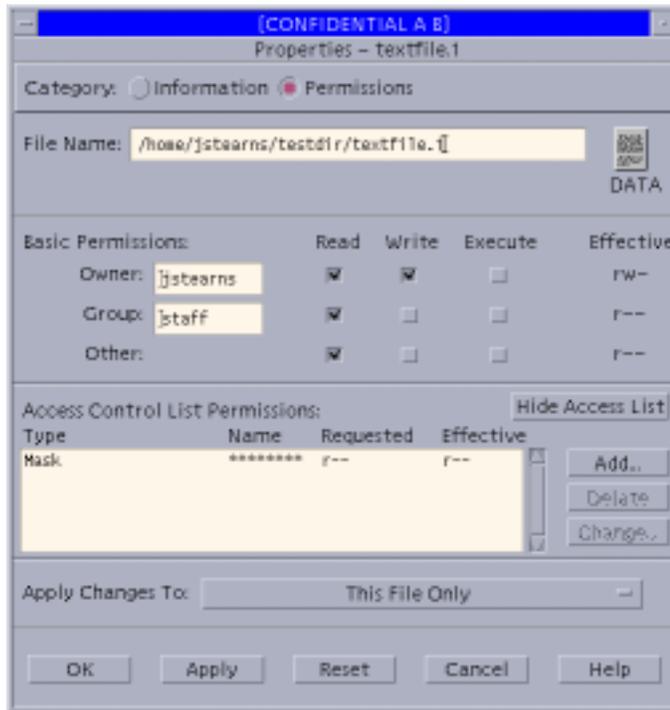


Figure 5-3 File Properties: Information Mode

Basic Permissions

The term *basic permissions* refers to the traditional UNIX scheme for protecting files and folders (directories) regarding three types of access:

- *read* permission – lets a user read the contents of a file or, if a folder, list the files in the folder
- *write* permission – lets a user make changes to a file, or, if a folder, add or delete files
- *execute* permission – lets a user run the file if it is executable or, if a folder, read or search its files

If access to a folder is limited, the File Manager displays special icons to show that a folder is inaccessible or read-only (see figure below).



Figure 5-4 Special File Manager Icons

Permissions are granted according to three classes of user:

- *owner* – the user who created the file or folder (or received ownership through `chown(1)`), usually with the greatest degree of access
- *group* – the set of users to which the owner belongs, with common needs of access to the file or folder
- *other* – all other users that are not the owner or in the owner’s group

Access Control Lists

The *access control list (ACL)* lets you grant individual permissions (referred to as *ACL entries*) to specific users and groups. For example, if you want to grant write permission to your manager, you can create an ACL entry granting him or her write permission.

There are two general categories of ACL entries: access ACL entries and default ACL entries. *Access ACL entries* define who has access to a specific file or directory. *Default access entries* define the permissions to be applied to newly created files or folders with a specified folder.

By definition, every access control list has a special entry called a mask (which cannot be deleted). The *mask* sets the maximum permissions allowed on a file or folder for all groups and any non-owner users. (The mask does not apply to users who fall into the “other” category for basic permissions.) A good use of a mask is to turn off write permission for everyone but yourself when you need to have sole write access to a file.

The ACL entry types are described in the table below.

TABLE 5-1 ACL Types and Application

Entry Type	Applies to	User Category
mask	Files or folders	All users except owner and other.
user	Files or folders	Specified user
group	Files or folders	Specified group
default user	Files created in selected folder	Specified user
default group	Files created in selected folder	Specified group
default owning user	Files created in selected folder	Folder’s owner

TABLE 5-1 ACL Types and Application *(continued)*

Entry Type	Applies to	User Category
default owning group	Files created in selected folder	Owner's group
default other	Files created in selected folder	Users other than the owner and users in the owner's group
default mask	Files created in selected folder	All users except owner and other

Whenever you create any default ACL entry, the following entries are required:

- default owning user
- default owning group
- default other
- default mask

The File Manager creates these default entries automatically, taking its best guess at their permission settings. If you do not want these default permission settings, you are free to change them.

Viewing or Changing Permissions and ACL Entries

All changes to a file or folder's basic permissions and ACL entries are made using the File Manager's Properties dialog box.

To Display the Properties Dialog Box for a File or Folder

1. **Display the File Manager.**
2. **Place the pointer over the file or folder whose properties you wish to access and press the right mouse button (see figure below).**

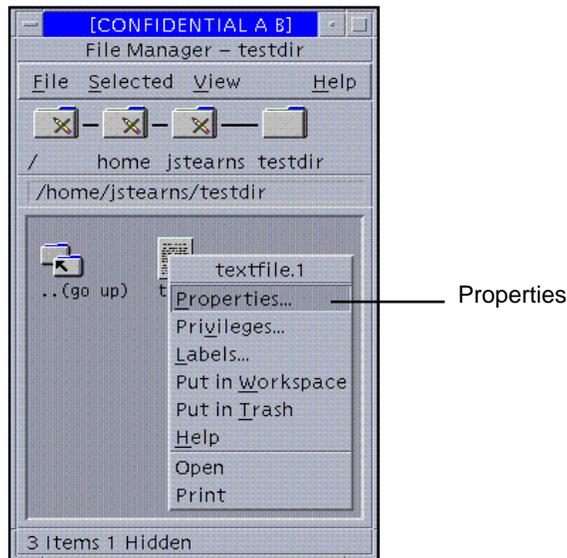


Figure 5-5 Selecting Change Properties from the File Manager Popup Menu

3. Select Properties...

This step displays the Properties dialog box for the selected file or folder. This dialog box lets you:

- View the file or folder's basic information
- View or change the file or folder's basic permissions
- View or change the file or folder's ACL entries
- Browse for other files or folders to be viewed or changed

To View the Basic Information of a File or Folder

A file or folder's basic information consists of: owner, group, size in bytes, the last access date, and the last modification date.

1. Display the File Manager Properties dialog box.

See "To Display the Properties Dialog Box for a File or Folder" on page 100.

2. Click the Information button in the Category field.

This step sets the dialog box to basic information mode.

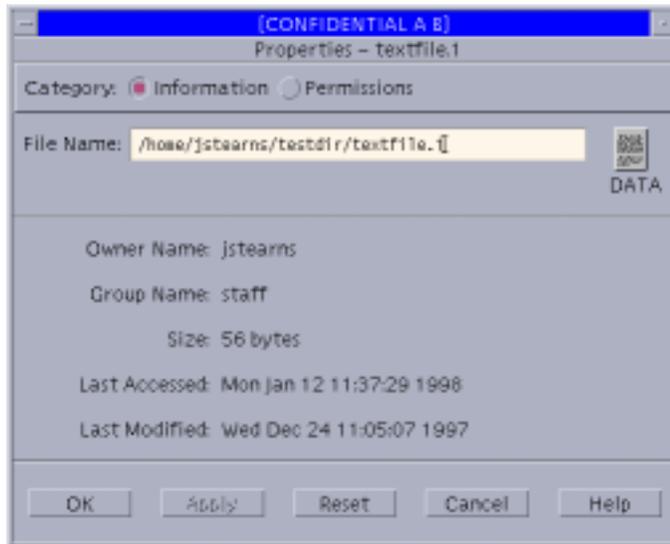


Figure 5-6 File Manager Basic Information Dialog Box

3. Examine the data in the basic file information area.

In addition to the data in the basic file information area, there is an icon at the right of the file identification area that indicates the file or folder's type.

To View or Change a File or Folder's Basic Permissions

1. Display the File Manager Properties dialog box.

See "To Display the Properties Dialog Box for a File or Folder" on page 100.

2. Click the Permissions button in the Category field.

This step sets the dialog box to permissions mode (see below).

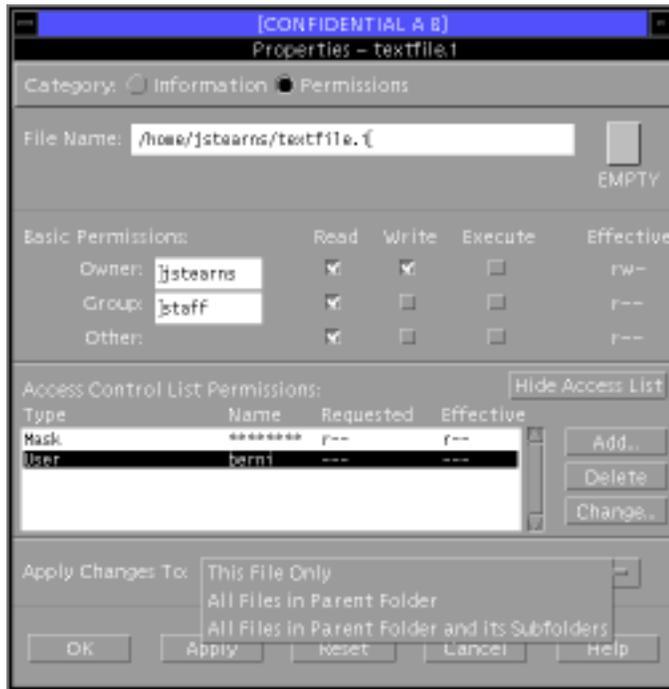


Figure 5-7 File Manager: Displaying ACL Entries

3. Examine the settings in the permissions area.

The owner, group, and other's read, write, and execute permissions are displayed here, along with buttons for making changes. The Effective column (at the right side of the permissions area) displays the permissions after the ACL mask has been applied as the permissions appear in the command line interface.

4. To make changes, click the appropriate read, write, or execute buttons for owner, group, or other.

You can check the result in the Effective column at the right of the area.

5. To specify the target item(s) for these changes, select the appropriate target in the Apply Changes To option menu at the bottom of the window.

You can select the current file, all files in the parent folder, or all files in the parent folder and its subfolders.

6. Click OK or Apply to save the permissions.

To View a File or Folder's ACL Entries

1. **Display the File Manager Properties dialog box.**

See “To Display the Properties Dialog Box for a File or Folder” on page 100.

2. **Click the Permissions button in the Category field.**

This sets the dialog box to permissions mode (see Figure 5-7).

3. **Click the Show Access Control List button if the access control list area is not currently displayed.**

4. **Examine the entries in the access control list area.**

Any existing ACL entries for the item are displayed in the scroll list, including the type of entry, specified name, requested permissions, and effective permissions. The requested permissions are the default permissions before the ACL mask has been applied—the effective permissions reflect the permissions after the mask has been applied.

To Add an ACL Entry

1. **Display the File Manager Properties dialog box as described in “To View a File or Folder's ACL Entries” on page 104.**

2. **Click the Add button at the right of the ACL area (see Figure 5-7) to display the Add dialog box.**

The File Manager Add Access List Entry dialog box with the Type menu displayed is shown below. Note that for folders all menu items are available. For files, only the User and Group menu items are active.

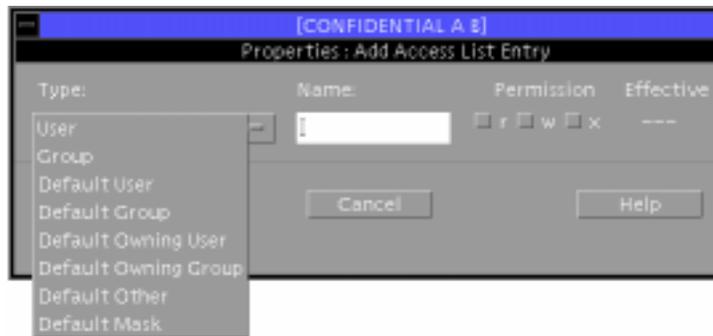


Figure 5-8 File Manager Add ACL Dialog Box

3. Specify the type of ACL entry.

The ACL types enabled in the options menu depend on whether you selected a file or folder. Only the User and Group items are available for files. All entries are enabled for folders. If you need to review the ACL types, see Table 5-1.

In addition, if you select one of the default entries, a message will be displayed at the bottom of the dialog box as a reminder that the default owning user, default owning group, default other, and default mask will be added with their permissions enabled accordingly.

4. Specify the name if enabled.

When you select User, Group, Default User, or Default Group, you must enter a name (or ID).

If you select Default Owing User, Default Owing Group, Default Other, or Default Mask, the name field is disabled, since it is not necessary.

5. Click the permissions you wish to enable (or disable).

A check mark means that the permission is enabled. If you select a permission that will be overridden by the mask, a warning will be displayed in the message display area at the bottom of the dialog box, along with a beep. The effective permissions column will indicate the difference. You are nonetheless allowed to make the entry and it will take effect if the mask is modified to permit it later.

6. Click Add in the dialog box.

This adds the entry, causing it (and any related default entries) to be displayed in the Access Control List area. If you do not like the setting in the default permission settings, you can change them (see “To Change an ACL Entry” on page 105).

7. To specify the target item(s) for the permissions or ACL entries that you specified, select the appropriate target in the Apply Changes To option menu at the bottom of the window.

You can select the current file, all files in the parent folder, or all files in the parent folder and its subfolders.

8. Click OK or Apply to save the ACL entries (and any permissions you have changed).

To Change an ACL Entry

- 1. Display the File Manager Properties dialog box as described in “To View a File or Folder’s ACL Entries” on page 104.**
- 2. Select an entry in the access control list area to be changed.**

3. Click the Change button at the right of the ACL area to display the Change Access List Entry dialog box.

If you have selected an entry of type User, Group, Default User, or Default Group, the dialog box displays a Type menu and you can change the type. If you select Mask, Default Owing User, Default Owing Group, Default Other, or Default Mask, there is no ACL type menu button and the type is fixed. See the figure below, which is an example of changing a Default Mask entry.

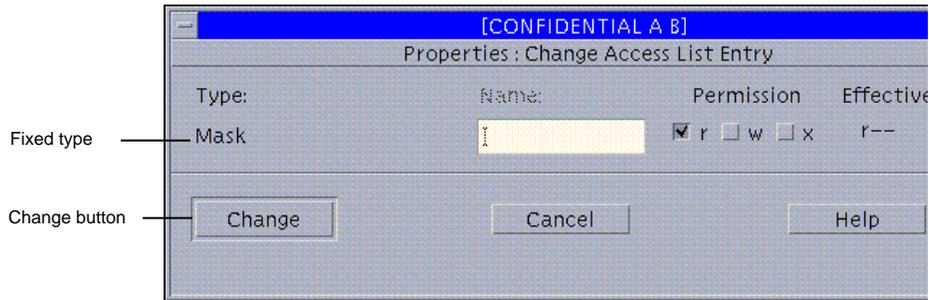


Figure 5-9 File Manager Change ACL

4. Specify the type of ACL entry.

The type will be limited as discussed in Step 3 on page 105.

5. Specify the name (if enabled) and if you wish to change it.

6. Click the permissions you wish to enable (or disable).

A check mark means that the permission is enabled. If you select a permission that will be overridden by the mask, a warning will be displayed in the message display area at the bottom of the dialog box, along with a beep. The effective permissions column will indicate the difference. You are nonetheless allowed to make the entry and it will take effect if the mask is modified later.

7. Click Change in the dialog box.

This modifies the entry, causing the modification to be displayed in the Access Control List area. Remember that if you select Mask, your modifications may change the effectiveness of the entries for specified users and groups and for the owner's group.

8. To specify the target item(s) for the permissions or ACL entries that you specified, select the appropriate target in the Apply Changes To option menu at the bottom of the window (see Figure 5-7).

You can select the current file, all files in the parent folder, or all files in the parent folder and its subfolders.

9. Click **OK** or **Apply** to save the ACL entry changes (and any permissions you have changed).

To Delete an ACL Entry

1. Display the File Manager Properties dialog box as described in “To View a File or Folder’s ACL Entries” on page 104.
2. Select the entry to be deleted in the Access Control List area.
3. Click the **Delete** button at the right of the ACL area to display the Delete dialog box (see figure below).

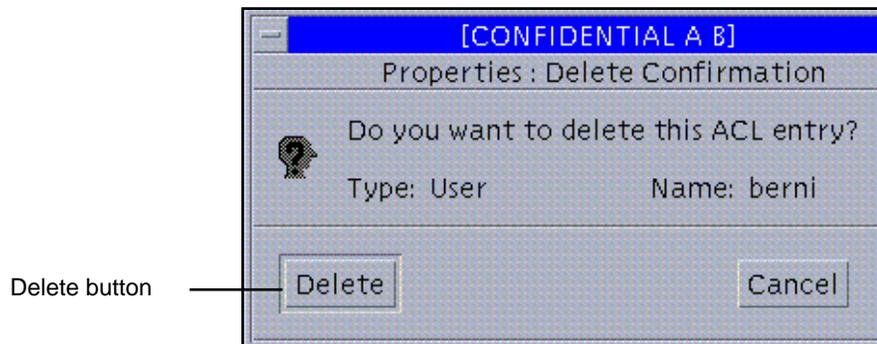


Figure 5-10 File Manager Delete Access List Entry Dialog Box

4. **Confirm that the selected entry is correct and click Delete in the dialog box.**
This removes the entry from the Access Control List area.
5. **To specify the target item(s) for the permissions or ACL entries that you specified, select the appropriate target in the Apply Changes To option menu at the bottom of the window (see Figure 5-7).**
You can select the current file, all files in the parent folder, or all files in the parent folder and its subfolders.
6. Click **OK** or **Apply** to save the current ACL entries (and any permissions you have changed).

Manipulating File Labels

This section focuses on manipulating a file's sensitivity labels.

Note - These procedures are only available to authorized users. You cannot change the label of a file or directory without being authorized by your administrator.

Viewing and Changing Labels with the File Manager

Use the File Manager when you want to view or change a file's labels.

To Determine a File's Label

1. **Display the File Manager and navigate to the directory containing the file.**
2. **Select the file and choose Labels... from either the popup menu or the Selected menu.**

This step causes the Labels dialog box to be displayed (see figure below).

3. **Click Cancel to close the Labels dialog box.**

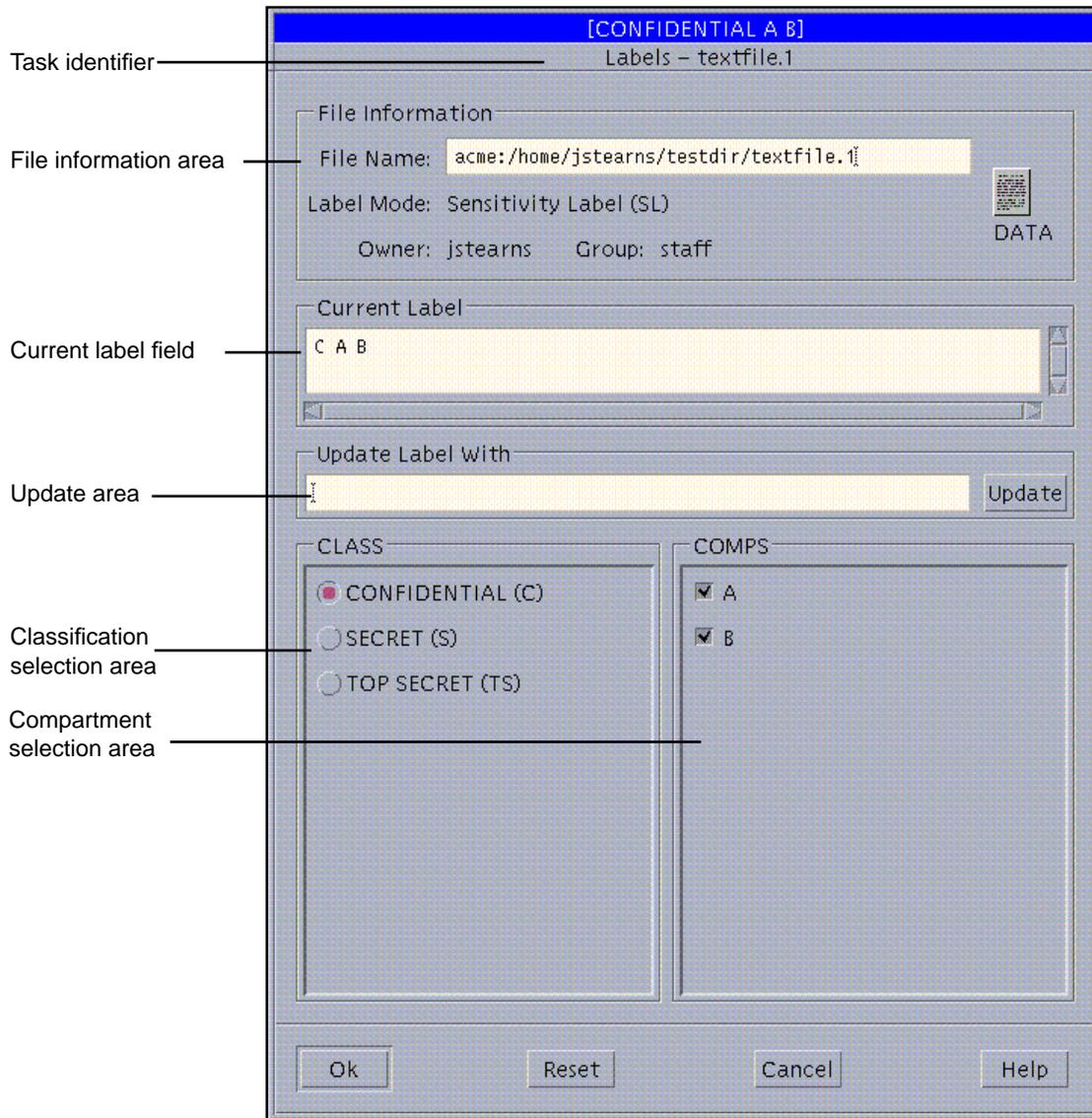


Figure 5-11 File Manager Change Label Dialog Box in Label Mode

The file's label appears in the Current Label field. The label will be a label or CMW label (combined), depending on how your user account is configured.

To Change a File's Label (Move Operation)

1. **Make sure that no one else is using the file whose label is to be changed.**

Changing the label of a file in use can cause serious problems when the other user attempts to save the file.

2. **Display the File Manager at the file's current label and the File Manager at the new label in the same workspace.**

This step entails opening a second workspace at a different label, displaying its File Manager, and occupying the original workspace. For a detailed example of this procedure, see "Tour: Occupying Workspaces with Applications at Different Labels" on page 65.

3. **Drag the file icon from the source File Manager to the File Manager at the new label (see figure below).**

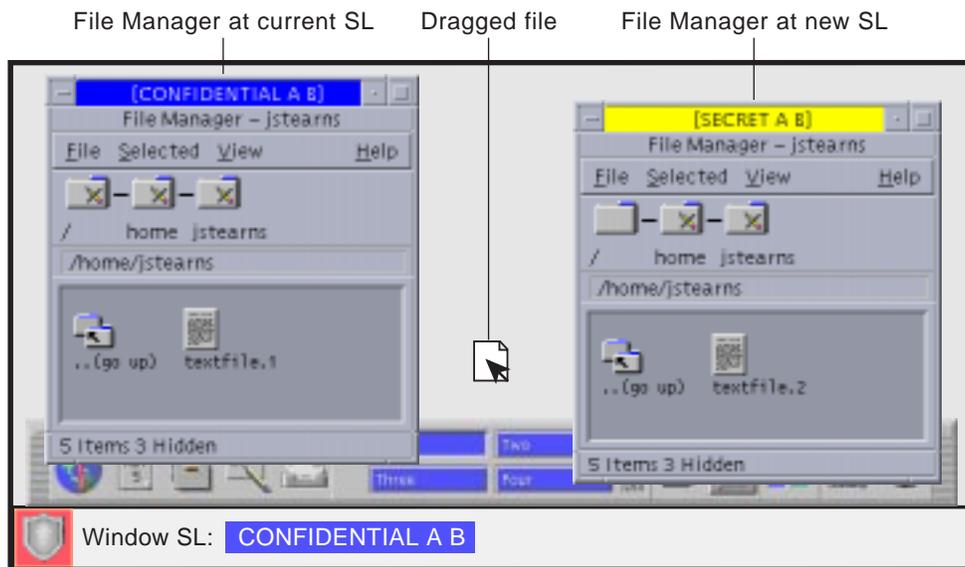


Figure 5-12 Dragging a File between File Managers at Different Labels

This causes the File Manager Confirmation dialog box to be displayed. See figure below.

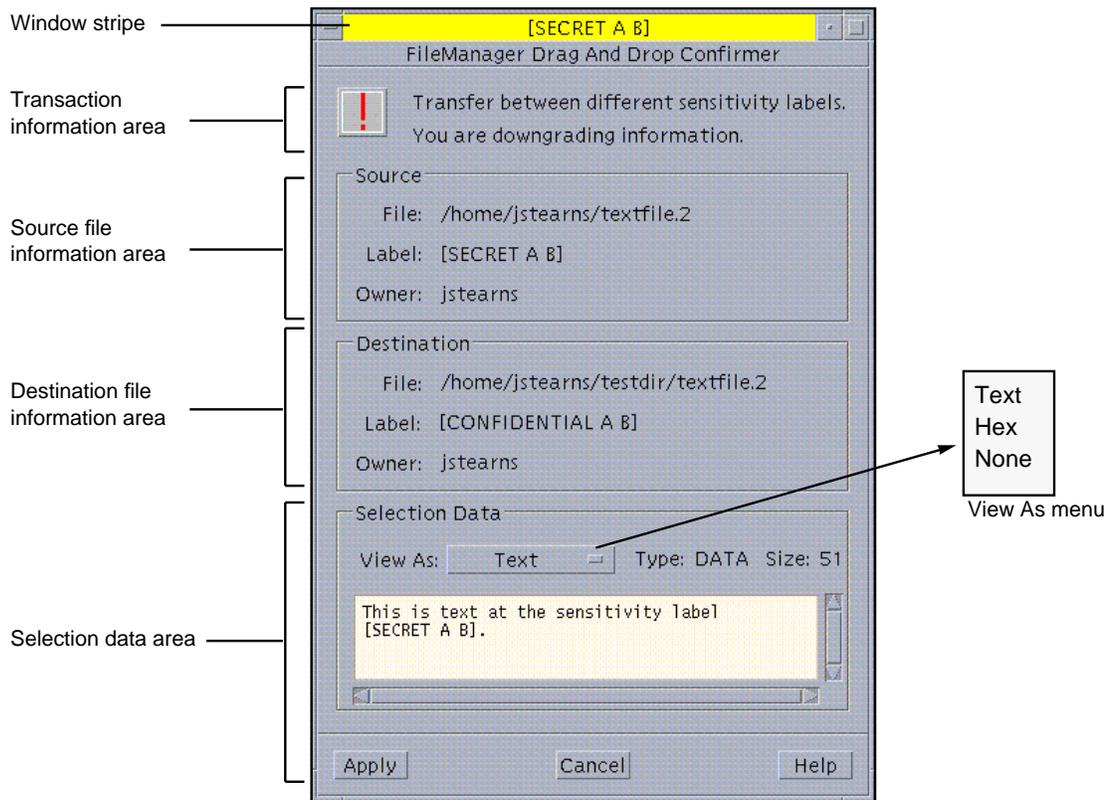


Figure 5-13 File Manager Confirmation Dialog Box

4. Click the **Apply** button in the File Manager Confirmation dialog box to complete the transfer.

To Create a Copy of a File at a Different Label (Copy Operation)

Follow the same instructions as in “To Change a File’s Label (Move Operation)” on page 110 except that you hold down the Control key when dragging the file icon in Step 3 on page 110. Creating a copy of a file at another label is useful when you need to use the same file name although you are editing different versions of the file at different labels.

To Link a File to a Different Label (Link Operation)

Follow the same instructions as in “To Change a File’s Label (Move Operation)” on page 110 except that you hold down both the Shift and the Control keys when dragging the file icon in Step 3 on page 110. Linking a file to another label is useful when you want to make a file with a lower label visible at higher labels. The file is only writable at the lower label.

Copying and Linking Files to Different Labels by Default

There are two special files that can be stored in your home directory for copying and linking files from your home directory at your minimum labels to your home directory at different labels. These files are provided to circumvent such problems as an application at one label that needs a file in a single-level directory at a different label. The files are:

- `.copy_files` – stores file names to be copied when you first change to a workspace with a different label. This is useful when you have an application that always writes to a file with a specific name and you need to separate the data at different labels.
- `.link_files` – stores file names to be linked when you first change to a workspace with a different label. This is useful when a specific file needs to be available at multiple labels but writable at its minimum label only. Two good candidates for the `.link_files` file are `.dtprofile` and `.login`.

Both files store their entries one file per line. You can specify paths to subdirectories in your home directory, but you should never use a leading slash since all paths should be within your home directory.

Note - Your administrator may have already installed a `.copy_files` and `.link_files` file in your home directory; they are at your discretion to modify. Since there are no safeguards for dealing with such anomalies as duplicate entries in both files or file entries that already exist at other labels, it is best to work with your administrator when modifying these files.

Supplementary Documentation

This appendix discusses man pages, online documentation, and online help in the Trusted Solaris operating environment.

- “Using Man Pages” on page 113
- “Accessing Online Documentation and Help” on page 114

Using Man Pages

There is an extensive library of man pages available for the Trusted Solaris environment. For an overview of the system and a complete listing of commands available in the Trusted Solaris environment, see the following man pages:

- Intro(1)
- Intro(1M)
- Intro(2)
- Intro(3)
- Intro(4)
- Intro(5)
- Intro(7)
- Intro(9)
- Intro(9F)

Man Page Paths

The man pages for the Trusted Solaris environment reside in three different directories, which need to be included in your MANPATH environment variable:

- /usr/man
- /usr/openwin/man
- /usr/dt/man

The MANPATH variable can be set individually by users in their shell initialization files or globally by administrators in site-wide shell initialization files in /etc/skel (or alternate skeleton directory) for all users. To set the MANPATH variable, type:

```
setenv MANPATH=' '/usr/dt/man:/usr/openwin/man:/usr/man:$MANPATH''
```

To check a system's current MANPATH setting, type:

```
echo $MANPATH
```

This should display the three paths mentioned above and any other paths to man pages at your site.

Specifying Man Pages by Section Number

To check whether there are different versions of a topic in different sections, type:

```
% man -l topic
```

To specify man pages by section in the Trusted Solaris environment, you type

```
% man -s sectionnumber topic
```

specifying the topic and section number.

Accessing Online Documentation and Help

All Trusted Solaris documentation is available on the *Trusted Solaris 8 AnswerBook CD-ROM* and at the website: <http://www.sun.com/docs> where it can be viewed or downloaded in PDF format. In addition, online help is provided in the Trusted Solaris environment through the Front Panel help icon, help menus, and help buttons.

Glossary

ACL	See access control list.
access control list	Also referred to as ACL, a software mechanism for discretionary access control that uses a list of permission specifications (referred to as ACL entries) to be applied to specific users and groups. The advantage of an ACL is that it allows finer-grained control than provided by the standard UNIX permissions.
access permission	The right of a user to read, write, execute, or view the name of a file or directory. See also discretionary access control and mandatory access control.
account label range	The set of labels assigned by the security administrator to a user or role account for working in the Trusted Solaris environment. It is defined at the upper end by the user clearance , at the lower end by the user's minimum label, and is limited to well-formed labels.
accreditation range	A set of labels that are approved for a class of users or resources. See also system accreditation range, user accreditation range , label encodings file, and network accreditation range.
action	An application that can be accessed from the CDE (Common Desktop Environment) graphical user interface. An action is represented by an icon and consists of one or more commands and optional user prompts. In the Trusted Solaris environment, an action is only available to a user if the security administrator has included it in an execution profile assigned to the user's account. Similarly certain functions of the action may be available only if the security administrator has assigned the appropriate authorizations and privileges in that execution profile.
administrative labels	Two special labels intended for administrative files only: ADMIN_LOW and ADMIN_HIGH. ADMIN_LOW is the lowest

label in the system with no compartments; it is strictly dominated by all labels in the system. Information at ADMIN_LOW can be read by all but can only be written by a user in a role working at the ADMIN_LOW label. ADMIN_HIGH is the highest label in the system with all compartments; it strictly dominates all labels in the system. Information at ADMIN_HIGH can only be read by users in roles operating at ADMIN_HIGH. These labels can be used as labels or clearances. See also dominating label.

adorned name	The complete name (including the strings .MLD. or .SLD.) for a single-level directory or multilevel directory. A single-level directory contains files at a single <i>label</i> and uses the name .SLD. <i>n</i> where .SLD. is the adornment string and <i>n</i> is an identifying number. A multilevel directory contains single-level directories; it uses the adornment .MLD. as a prefix to the name you specify. An example of a single-level directory within a multilevel directory would be / .MLD.myHomeDir/ .SLD.0.
allocatable device	A device with controlled access, capable of importing or exporting data from the system. Devices are allocatable to a single user at a time. The security administrator determines which users may access which allocatable devices. Allocatable devices include tape drives, floppy drives, audio devices, and CD-ROM devices. (See device allocation.)
allowed privilege	A privilege in the set of privileges specified by the security administrator to be potentially available for an application. If a privilege is not in an application's allowable set, it will never be available to users executing that application. Allowed privileges are assigned to the application's executable file using the File Manager.
audit ID	The UID representing the actual user, as opposed to a role, used to identify the user for auditing purposes. The audit ID always represents the user for auditing even when the user assumes roles or acquires effective UIDs/GIDs. Also referred to as AUID. See also user ID.
auditing	The process of capturing user activity and other events on the system, storing this information in a set of files called an <i>audit trail</i> , and producing system activity reports to fulfill site security policy.
audit trail	See auditing.
authorization	Permission granted to a user to perform an action that would be otherwise prohibited by security policy. The security administrator assigns authorizations to execution profiles which in turn are

assigned to user or role accounts. Some commands and actions will not function fully unless the user has the necessary authorizations. See also privilege.

CDE action	See action.
classification	A component of a clearance or a label that indicates a hierarchical level of security, for example, TOP SECRET or UNCLASSIFIED.
clearance	A label defining the upper boundary of a label range. There are two components to a clearance: a classification and zero or more compartments. A clearance need not be a well-formed label; it defines a theoretical boundary, not necessarily an actual label. See also user clearance , session clearance, and label encodings file.
CMW label	A label indicating the security level of a file or window in those Trusted Solaris environments configured to display information labels and sensitivity labels. It is composed of an information label (information labels are no longer supported in the Trusted Solaris environment) and a label shown in brackets. CMW labels appear in a stripe at the top of open windows and in a stripe under minimized windows. See also label encodings file.
Common Desktop Environment	Also referred to as CDE, the graphical environment on which standard Solaris and Trusted Solaris are based. It includes the login manager, the session manager, the window manager, and various desktop tools.
compartment	A nonhierarchical component of a label used with the classification component to form a clearance or a label. A compartment represents a group of users with a potential need to access this information, such as an engineering department or a multidisciplinary project team.
compartmented mode workstation	Also referred to as CMW, a computing system that fulfills the government requirements for a trusted workstation stated in Security Requirements for System High and Compartmented Mode Workstations, DIA document number DDS-2600-5502-87. Specifically, it defines a trusted, X-window system-based operating environment for UNIX workstations.
covert channel	Communication channel that is not normally intended for data communication and that allows a process to transfer information indirectly in a manner that violates the intent of the security policy.
DAC	See discretionary access control.

deallocated device	Device no longer assigned (allocated) to a user. See also device allocation.
device	See allocatable device .
device allocation	A mechanism for protecting the information on an allocatable device from access by anybody except the user who allocates the device. When the device is deallocated, device clean scripts are run to clean information from the device before the device may be accessed again by another user.
discretionary access control	Also referred to as DAC, an access control mechanism that allows the owner of a file or directory to grant or deny access to other users. The owner assigns read, write, and execute permissions to the owner, the user group to which the owner belongs, and a category called other, which refers to all other unspecified users. The owner can also specify an access control list, which lets the owner assign permissions specifically to additional users and groups. Contrast with mandatory access control.
disjoint label	See dominating label.
dominating label	In a comparison of two labels, the label whose classification component is higher than or equal to the second label's classification and whose compartment components include all of the second label's compartment components. If the components are the same, the labels are said to dominate each other and are <i>equal</i> . If one label dominates the other and the labels are not equal, it is said to <i>strictly dominate</i> the other. Two labels are <i>disjoint</i> if they are not equal and neither label is dominant.
downgraded label	A label of an object that has been changed to a value that does not dominate the previous value of the label.
effective privilege	A privilege available for use by a process and currently enabled.
effective UIDs/GIDs	A user ID that overrides a user's real user ID when necessary to run a particular program or an option of a program. The security administrator assigns an effective UID to a command or action in an execution profile when that command or action must be run by a specific user, most often when the command must be run as root. Effective group IDs are used in the same fashion. Note that using <code>setuid</code> as in conventional UNIX systems does not work due to the need for privileges.

evaluatable configuration	A computer system that meets a set standard of government security requirements. See also extended configuration.
execution profile	A mechanism that allows a site's security administrator to bundle authorizations, commands, CDE actions, and any inheritable privileges, label ranges, and effective UIDs/GIDs necessary for the commands and actions. An execution profile generally contains related tasks. It can be assigned to users and roles.
extended configuration	A computer system that is no longer an evaluatable configuration due to modifications that have broken security policy.
fallback mechanism	A shortcut method for specifying IP addresses in the <code>tnrhttp(4)</code> file. The fallback mechanism recognizes 0 as a wildcard in the rightmost byte(s) of the IP addresses.
forced privilege	A privilege in a set of privileges specified by the security administrator to be enabled unconditionally when the application is executed by any user with access to an execution profile containing that application. If the privilege is not in the application's allowed privilege set for the execution profile, it will not be available in the forced privilege set. Forced privileges are assigned to the application's executable file using the File Manager.
gateway	A Trusted Solaris host having more than one network interface and used to connect two or more networks.
group ID	Also referred to as GID, an integer used to identify a group of users that have common access permissions. Group ID is a security attribute in the Trusted Solaris environment. See also discretionary access control.
host	A computer attached to a network.
host template	A record in the <code>tnrhttp(4)</code> file used to define the security attributes of a class of hosts that are permitted access to the network.
host type	A classification of a host used in network communications and stored in the <code>tnrhttp(4)</code> database. The host type determines which network protocol is used to communicate with other hosts on the network. <i>Network protocol</i> refers to the rules for packaging communication information.
information system security officer	Also referred to as ISSO, an alternate term for security administrator, no longer used in the Trusted Solaris system.

inheritable privilege	A privilege that is granted to a process when the application is run by a user permitted to use the execution profile containing the application. An inheritable privilege can be passed on to child processes created by the application. The security administrator assigns inheritable privileges to commands or actions in an execution profile using the Profile Manager. See also allowed privilege and forced privilege.
install	The name of a special user with root capabilities responsible for configuring the Trusted Solaris system.
label	Also referred to as a sensitivity label or SL, a string indicating the security level of an entity (file, directory, process, device, or network interface) used to determine whether access should be permitted in a particular transaction. There are two components to a label: a classification indicating the hierarchical level of security, and zero or more compartments for defining who has a need to access the entity given a sufficiently high classification. See also label encodings file.
label encodings file	A file managed by the security administrator that contains the definitions for all valid clearances and labels as well as defining the system accreditation range, user accreditation range, and labeling of hardcopy reports for the site.
label range	Any set of labels bounded on the upper end by a clearance or maximum label, on the lower end by a minimum label, and consisting of well-formed labels. Label ranges are used to enforce mandatory access control. See also label encodings file, account label range, accreditation range, network accreditation range, session range, system accreditation range, and user accreditation range.
label view	A security feature that displays the administrative labels or substitutes unclassified placeholders for the administrative labels. For example, if it is against security policy to expose the labels ADMIN_HIGH and ADMIN_LOW, the labels REGISTERED and PUBLIC may be substituted.
labeled workspace	The Trusted Solaris version of CDE workspaces, which confines the activity in a workspace to a label. There are two exceptions. (1) Authorized users can move a window at a different label into the workspace using the <code>Occupy Workspace</code> or <code>Occupy All Workspaces</code> command. (2) Certain applications, such as the Mail Tool, permit operation at multiple labels from a labeled workspace.
least privilege	See principle of least privilege.

MAC	See mandatory access control.
mandatory access control	Also referred to as MAC, a system-enforced access control mechanism that uses clearances and labels to enforce security policy. MAC associates the programs a user runs with the security level (clearance or label) at which the user chooses to work in the session and permits access to information, programs, and devices at the same or lower level only. MAC also prevents users from writing to files at lower levels. MAC cannot be overridden without special authorizations or privileges. Contrast with discretionary access control.
minimum label	<p>A label assigned to a user as the lower bound of the set of labels at which that user may work. The minimum label is the user's initial label by default when the user first begins a Trusted Solaris session. The user can optionally reset the value for the initial label if desired by changing the home session.</p> <p>Also, the lowest label permitted to any non-administrative user. It is assigned by the security administrator and it defines the bottom of the user accreditation range .</p>
MLD	See multilevel directory.
multilevel directory	Also referred to as MLD, a special type of directory that transparently stores information by label in separate subdirectories called single-level directories. When users access multilevel directories through the command line or use the File Manager, they see information at their current label only. Note; if permitted by the security policy, a user may access information at other labels by explicitly specifying the adorned names of directories in the path. See also single-level directory.
network accreditation range	The set of labels within which Trusted Solaris hosts are permitted to communicate on a network.
normal user	A user who holds no special authorizations that allow exceptions from the standard security policies of the system; not an assumer of an administrative role.
object	A passive entity that contains or receives data, such as a data file, directory, printer, or other device, and is acted upon by subjects. In some cases, a process may be an object, such as when you send a signal to a process.

permissions	A set of codes that indicate which users are allowed to read, write, or execute the file or directory (folder). Users are classified as owner, group (the owner's group), and other (everyone else). Read permission (indicated by <i>r</i>) lets the user read the contents of a file or, if a directory, list the files in the folder. Write permission (<i>w</i>) lets the user make changes to a file or, if a folder, add or delete files. Execute permission (<i>e</i>) lets the user run the file if it is executable or, if a directory, read or search its files. Also referred to as UNIX permissions or permission bits.
principle of least privilege	The security principle that restricts users to only those functions necessary to perform their jobs. It is applied in Trusted Solaris systems by making privileges available to programs on an as-needed basis and enabling the privileges on an as-needed basis for specific purposes only.
privilege	A permission granted to a program by the security administrator to override some aspect of security policy. To be usable by the program, the privilege must be (1) in the allowed privilege set assigned to the program's executable file and (2) either in the forced privilege set assigned to the executable file or in the process's inheritable privilege set. The term effective privilege refers to privileges that are currently enabled. See also authorization and privilege set.
privilege bracketing	The coding technique of enabling a privilege only while it is needed for a specific function. This is in keeping with the principle of least privilege.
privilege set	A group of allowed privileges, forced privileges, inheritable privileges, effective privileges, or saved privileges. Privilege set is a useful term for describing how privileges are assigned and made available to programs. Allowed and forced privileges are assigned by the security administrator to executable files through the File Manager. Inheritable privileges are assigned by the security administrator to commands and actions in execution profiles through the Profile Manager. Effective and saved privileges are mainly of use to developers and are determined by the system.
privileged process	A process that has privileges available to it.
process	A running program. In the Trusted Solaris environment, processes have security attributes, such as user ID, group ID, the user's audit ID, privileges, the process clearance, the label of the current workspace.

process clearance	A clearance equal to the session clearance that sets a boundary on the highest label at which the process can write information.
profile	See execution profile.
profile shell	A version of the Bourne shell that lets a user run a command with the privileges, label ranges, and effective UIDs/GIDs assigned to the command in the execution profile.
public object	A file that contains read-only information, is not modifiable by normal users, and has no implications on security, such as the system clock. There is little need to perform auditing on public objects.
reading down	The ability of a subject to view an object whose label it dominates. Security policy generally allows reading down. For example, a text editor program running at Secret can read Confidential data. See also mandatory access control and reading up.
reading up	The ability of a subject to view an object at a label that dominates the subject's label. Due to mandatory access control, reading up is generally prohibited unless the subject has the appropriate privilege. For example, a text editor program running at Confidential cannot normally read Secret data. See also reading down.
role	A special user account that gives the user assuming the role access to certain applications with the authorizations, privileges, and effective UIDs/GIDs necessary for performing the specific tasks.
root	In the Trusted Solaris environment, the role assigned to the user or users responsible for installing commercial software. The Trusted Solaris version of root does not have the all-powerful capabilities of root in standard UNIX systems.
saved privilege	(This is mainly of use to developers.) A privilege set inherited by a process when its parent process performs an <code>execve(2)</code> . The saved privileges become invalid if the process changes its effective user ID but are re-enabled on a return to the prior user ID.
security administrator	In the Trusted Solaris environment, the role assigned to the user or users responsible for defining and enforcing the site security policy. The security administrator can work at any label in the system accreditation range and potentially has access to all information at the site. The security administrator configures the security attributes for all users and equipment. See also label encodings file.

security attribute	A property of an entity (file, directory, process, device, or network interface) in the Trusted Solaris environment related to security. Security attributes include identification values such as user ID and group ID, different types of clearances, and all types of labels and label ranges. Note that only certain security attributes apply to a particular type of entity.
security policy	In the Trusted Solaris environment, the set of DAC, MAC, and label rules that define how information may be accessed and by whom. At a customer site, the set of rules that defines the sensitivity of the information being processed at that site and the measures that are used to protect the information from unauthorized access.
sensitivity label	See label.
session	The time between logging into and out from a Trusted Solaris host. The trusted stripe appears in all Trusted Solaris sessions to confirm that users are not being spoofed by a counterfeit environment.
session clearance	A clearance set at login that defines the upper boundary of labels for a Trusted Solaris session. If the user is permitted to set the session clearance, the user can specify any value within the user's account label range. If the user's account is configured for forced single-level sessions, the session clearance is set to the default value specified by the security administrator. See also clearance.
session range	The set of labels available to a user during a Trusted Solaris session. It is bounded at the upper boundary by the user's session clearance and at the lower end by the minimum label.
single-label configuration	A user account that has been configured for operation at a single label only.
single-level directory	Also referred to as SLD, a subdirectory within a multilevel directory containing files and optionally subdirectories at a single label only. Single-level directory names are created by the Trusted Solaris operating system; it uses the .SLD. prefix followed by a number indicating the sequence in which they were created. When a user changes to a multilevel directory, the user actually goes to the single-level directory matching the user's current label. See also adorned name.
SLD	See single-level directory.

spoof	To counterfeit a software program in order to get access or information on a system illegally.
strict dominance	See dominating label.
subject	An active entity in the Trusted Solaris environment, usually a process running on behalf of a user or role, that causes information to flow among objects or changes the system state.
system accreditation range	The set of all valid labels for a site including the administrative labels available to the site's security administrators and system administrators. The system accreditation range is defined in the label encodings file.
system administrator	In the Trusted Solaris environment, the role assigned to the user or users responsible for performing standard system management tasks such as setting up the non-security-relevant portions of user accounts. See also security administrator.
system operator	In the Trusted Solaris environment, the role assigned to the user or users responsible for backing up systems.
trusted application	An application that has been granted one or more privileges.
trusted computing base	Also referred to as TCB, the part of the Trusted Solaris environment that affects security; it includes software, hardware, firmware, documentation, and administrative procedures. Utility programs and application programs that can access security-related files are all part of the trusted computing base.
trusted facilities management	All activities associated with system administration in a conventional UNIX environment, plus all of the administrative activities necessary to maintain the security of a distributed system and the data it contains.
trusted path	Refers to the mechanism for accessing actions and commands permitted to interact with the trusted computing base. See also trusted path menu, trusted path symbol, and trusted stripe.
trusted path menu	A menu of Trusted Solaris operations that is displayed by holding down the right mouse button over the switch area of the front panel at the bottom of the screen. The menu selections fall into three categories: workspace-oriented selections, role assumption selections, and security-related tasks.

trusted path symbol	The symbol (the letters <i>TP</i>) that appears at the left of the trusted stripe area. It is displayed whenever the user accesses any portion of the trusted computing base.
trusted stripe	A rectangular graphic in a reserved area at the bottom of the screen that appears in all Trusted Solaris sessions. Its purpose is to confirm valid Trusted Solaris sessions. Depending on a site's configuration, the trusted stripe has one or two components: (1) a mandatory trusted path symbol to indicate interaction with the trusted computing base and (2) an optional label to indicate the label of the current window or workspace.
upgraded label	A label of an object that has been changed to a value that dominates the previous value of the label.
upgraded name	The name of a file or directory whose label has been upgraded and thus dominates the label of the directory that contains it. The security administrator can configure a system so that upgraded names are displayed or hidden from users by default.
user accreditation range	The largest set of labels that the security administrator can potentially assign to a user at a specific site. The user accreditation range excludes the administrative labels and any label combinations available to administrators only. It is defined in the label encodings file.
user clearance	A clearance assigned by the security administrator that defines the upper boundary of a user's account label range; it determines the highest label at which the user is permitted to work in a Trusted Solaris environment. See also clearance and session clearance.
user ID	Also referred to as UID, an integer used to identify a user for the purposes of discretionary access control, mandatory access control, and auditing. User ID is a security attribute in the Trusted Solaris environment. See also access permissions.
well-formed label	A label that is permitted by all applicable rules in the label encodings file to be included in a range.
workspace	See labeled workspace.
writing down	The ability of a subject to write to an object whose label is strictly dominated by the subject's label. Due to mandatory access control, writing down is not permitted without the appropriate privilege. For example, a text editor program running at Secret cannot write

Confidential data without the right privilege. Note that writing between subjects and objects at equal labels is permitted and is the norm. See also mandatory access control and writing up.

writing up

The ability of a subject to write to an object whose label dominates (or is equal to) the subject's label. For example, a text editor program running at Confidential can write Secret data (if its session clearance is at SECRET or higher). See also mandatory access control and writing down.

Index

A

access control lists, *see* ACLs

accounts

roles 27

users 33

ACLs

(access control lists) 17

adding entries 104, 105

changing entries 105, 107

defined 99, 100

deleting entries 107

displaying entries 104

introduction 20

Add Workspace menu item

described 83

admin role, *see* system administrator

Allocate Device menu item

described 89, 91

Application Manager

differences in the Trusted Solaris
environment 82

auditing

introduction 19

authentication

defined 34

procedure 37

authorizations 17

defined 28

C

calendar

differences in the Trusted Solaris
environment 78

CDE actions, *see* actions

Change Password menu item

described 84, 89

Change Workspace Label menu item

described 83

example 61

classification label component

defined 21

clearances

see also labels

defined 20

setting session 41, 42

clock

differences in the Trusted Solaris
environment 78

CMW labels 17

(compartmented mode workstation
labels) 17

compartment label component

defined 21

compartmented mode workstation labels, *see*
CMW labels

copy-and-paste

effect on labels 23

example 66, 69

.copy_files file

described 112

D

DAC

- (discretionary access control) 17
- defined 20
- default groups
 - ACL entry 99
- default masks
 - ACL entry 100
- default others
 - ACL entry 100
- default owning groups
 - ACL entry 100
- default owning users
 - ACL entry 99
- default users
 - ACL entry 99
- Delete menu item
 - described 83
- devices
 - allocation
 - description 89, 91
 - introduction 19
 - clearing prior to reuse 27
- discretionary access control, *see* DAC
- dominance of labels
 - overview 22
 - strict dominance 23
- drag-and-drop
 - effect on labels 23

E

- email
 - in the Trusted Solaris environment 27
- execution profiles
 - defined 28
- Exit control 92

F

- failsafe login
 - defined 47
- File Manager
 - ACLs 100, 107
 - adding ACL entries 104, 105
 - changing ACL entries 105, 107
 - changing file labels 112
 - changing labels 110
 - changing permissions 102
 - deleting ACL entries 107

- determining labels 108
- differences in the Trusted Solaris
 - environment 78
- displaying ACL entries 104
- displaying basic information 101
- labels 108, 112
- overview for users 96, 112
- permissions 100, 108
- viewing SLD contents 10, 63, 64

files

- ACLs 96, 107
- copying between File Managers 111
- copying to other labels with
 - .copy_files 112
- linking between File Managers 112
- linking to other labels with
 - .link_files 112
- moving between File Managers 110
- permissions 96, 107

Front Panel

- differences in the Trusted Solaris
 - environment 77, 82

G

- groups
 - ACL entry 99

H

- Help menu item
 - described 92

I

- identification
 - defined 34
 - procedure 35, 37

IDs

- see also* audit IDs
- see also* UIDs

ILs

- determining with File Manager 108

L

- labels 17
 - see also* clearances

- changing 110, 112
 - by copying 69
 - by linking 69
 - by moving 69
 - example 69
- defined 21
- determining by window query 91
- determining with File Manager 108
- displayed in Trusted Solaris
 - environment 74, 75
- dominance 22
- relationships 22
- setting session labels 41, 43
- .link_files file
 - described 112
- lock control 43, 44
- Lock control 92
- login
 - disabled 46
 - enabling 46, 47
 - example 49, 50
 - failsafe 47
 - fixing initialization problems 47
 - procedure 33, 43
- logout
 - procedure 9, 45

M

- MAC
 - defined 20
 - (mandatory access control) 17
- mail
 - differences in the Trusted Solaris
 - environment 79
- mandatory access control, *see* MAC
- masks
 - ACL entry 99
- MLDs
 - see also* SLDs
 - defined 25
 - example 10, 62, 64
 - (multilevel directories) 17
- multilevel directories, *see* MLDs
- multilevel sessions
 - defined 24

O

- object
 - defined 22
- object-reuse
 - introduction 27
- Occupy Workspace
 - example 65, 66
- occupying workspaces
 - Trusted Solaris environment 93
- oper role, *see* system operator

P

- passwords
 - changing 84, 89
 - entry procedure 37, 38
 - expiration 84
 - introduction 18
- permission bits
 - changing 102
 - defined 98
 - introduction 20
- pfsh command, *see* profile shell
- policy, *see* security policy
- Printer tool
 - differences in the Trusted Solaris
 - environment 80
- privileges
 - see also* authorizations
 - defined 28
- profile shell
 - defined 28
- profiles, *see* execution profiles

Q

- Query Window Label menu item
 - described 91

R

- read access
 - overview 23
- Rename menu item
 - described 83
- roles
 - assuming 84
 - defined 27

- root
 - defined 29
- S**
- screen locking 43, 44
- secadmin role, *see* security administrator
- security administrator
 - defined 29
- security policy
 - defined 17
- Selection Manager
 - Confirmation dialog box example 68
- sensitivity labels, *see* SLs
- session clearances
 - defined 24
 - setting 9, 52, 53
- sessions
 - setting level 9, 43, 50, 53
- Shut Down menu item
 - described 92
- single-level directories, *see* SLDs
- single-level sessions
 - defined 24
- SLDs
 - see also* MLDs
 - defined 25
 - example 10, 62, 64
 - (single-level directories) 17
- SLs
 - see also* labels
 - (sensitivity labels) 17
- spoofing
 - defined 19
- strict dominance
 - defined 23
- subject
 - defined 22
- subpanels
 - differences in the Trusted Solaris environment 77
- system administration
 - in the Trusted Solaris environment 27, 29
- system administrator
 - defined 29
- system operator
 - defined 29

- T**
- TCB
 - defined 18
 - (trusted computing base) 17
- Text Editor
 - differences in the Trusted Solaris environment 79
- Trash Can
 - differences in the Trusted Solaris environment 82
- Trusted Computing Base, *see* TCB
- trusted networks, *see* networks
- Trusted Path menu
 - described 82
 - example 56
- trusted path symbol
 - described 76
 - example 55, 56
- Trusted Solaris environment
 - basic features 10, 73, 74
 - guided tour 54, 73
 - overview 17, 29
- trusted stripe
 - defined 74
 - described 76
 - example 55, 56

- U**
- UIDs
 - and roles 84
 - (user IDs) 17
- user accounts
 - see also* accounts
- user clearances
 - defined 20
- user IDs, *see* UIDs
- users
 - ACL entry 99

- W**
- Window Label indicator
 - described 77
- windows
 - moving data between 66, 69

- workspace switch area
 - controls 92
 - differences in the Trusted Solaris environment 78
- workspaces
 - changing 10, 61, 62
- Workstation Information dialog box
 - example 9, 50, 51
- introduction 34
- procedure 9, 38, 40
- write access
 - overview 23
- WURD
 - defined 23