Trusted Solaris User's Guide

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

Part No: 805-8006-10
Revision A, July 1997

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.

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

Figures

Tables

Preface

The *Trusted Solaris User's Guide* is a guide to operating in the Trusted Solaris™ environment. As a prerequisite, you should be familiar with the standard Solaris computing environment. You should also be familiar with the security policy of your organization.

Related Materials

The Trusted Solaris documentation set is supplemental to the Solaris 2.5.1 documentation set. You should obtain a copy of both sets for a complete understanding of Trusted Solaris. The Trusted Solaris documentation set consists of:

- *Trusted Solaris Documentation Roadmap* shows all volumes in the documentation set.
- *Trusted Solaris Global Index* provides an index with entries covering the entire Trusted Solaris documentation set.
- *Trusted Solaris Administration Overview* provides an introduction to administration in the Trusted Solaris environment. It *e*xplains basic concepts and terminology commonly used throughout Trusted Solaris.

How This Guide is Organized

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

Chapter 2, “Accessing and Leaving the Trusted Solaris Environment,” presents procedures necessary for accessing and leaving the Trusted Solaris environment.

Chapter 3, “Tour of the Trusted Solaris Environment,” 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, “Elements of the Trusted Solaris Environment,” explains the key elements in the Trusted Solaris environment.

Chapter 5, “Managing Files and Directories,” shows you the basics of managing the security of files and directories in the Trusted Solaris environment.

Ordering Sun Documents

The SunDocs℠ program provides more than 250 manuals from Sun Microsystems, Inc. If you live in the United States, Canada, Europe, or Japan, you can purchase documentation sets or individual manuals using this program.

For a list of documents and how to order them, see the catalog section of the SunExpress™ Internet site at `http://www.sun.com/sunexpress`.

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 `.login` file. Use `ls -a` 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 `rm` *filename*. The *errno* variable is set.
AaBbCc123	Book titles, new words or terms, or words to be emphasized	Read Chapter 6 in *User's Guide*. These are called *class* options. You *must* be root to do this.
Code samples are in `code font` and may display the following:		
`%`	UNIX C shell prompt	`system%`
`$`	UNIX Bourne and Korn shell prompt	`system$`
`#`	Superuser prompt, all shells	`system#`

Introduction to Trusted Solaris 1

This chapter introduces you to Trusted Solaris 2.5, a computer environment with all the advantages of the Solaris 2.5 operating system plus powerful security features to accommodate an organization's security policy.

What is Trusted Solaris?

The Trusted Solaris 2.5 software package is an enhanced version of the Solaris 2.5 environment with special security features. Trusted Solaris 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.

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

How Trusted Solaris Protects against Intruders

Trusted Solaris 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, Trusted Solaris supplies several options for requiring password changes. 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 Trusted Solaris Enforces Access Control Policy" on page 4.

Providing Auditing

Trusted Solaris lets administrators audit all or selected user events 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. Trusted Solaris uses a graphical login and does not allow login from the command line; graphical login is easier to control. Trusted Solaris protects users from hostile spoofing programs by displaying the *Trusted Stripe*, an unmistakable, tamper-proof rectangle at the bottom of the screen which displays a special symbol 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.

Protecting Local Peripheral Devices against Unauthorized Users

Trusted Solaris protects local peripheral devices such as tape drives, floppies, printers, and microphones from unauthorized users. By restricting access to peripheral devices, Trusted Solaris prevents two types of security leaks:

- 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 Trusted Solaris Enforces Access Control Policy

Trusted Solaris 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. If you are unfamiliar with UNIX permission concepts, see "File and Folder Information" in Chapter 2, "File Manager" in *Solaris User's Guide Solaris 2.5*. In traditional UNIX systems, the superuser (root) can override DAC protection; in Trusted Solaris, 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. If you are unfamiliar with how access control lists work, see Chapter 58, "Securing Files" in *System Administration Guide Volume 2* for Solaris 2.5.

Mandatory Access Control

Mandatory access control (MAC) is a system-enforced access control mechanism that uses clearances and sensitivity labels to enforce security policy. Roughly speaking, MAC associates the programs a user runs with the security level (clearance or sensitivity 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 Figure 1-1.

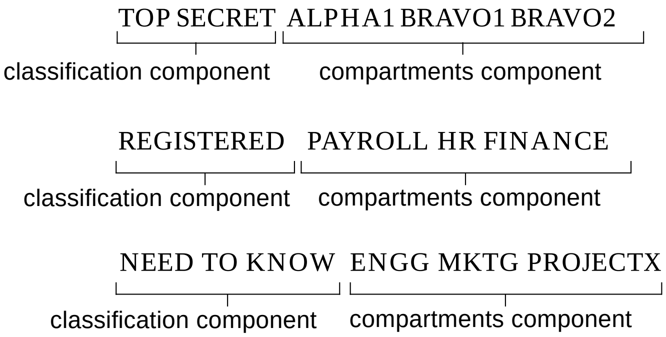


Figure 1-1 Typical Clearances

Sensitivity Labels

Trusted Solaris uses a string called a *sensitivity label (SL)* (related to the clearance level at which you choose to operate) to determine which information you can access. Sensitivity labels may be displayed inside square brackets ([]) in window title bars, in the Trusted Stripe at the bottom of the screen, or not at all, depending on how your system is configured.

All subjects and objects in a system have sensitivity 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 Sensitivity Labels Play in Transactions

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

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

Two labels are said to be *equal* if they have the same classification and the same set of compartments (and markings if information labels). 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 sensitivity label must dominate the object's sensitivity label. This rule ensures that the subject's level of trust meets the requirements for access to the object and that the subject's sensitivity label includes to 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 sensitivity label must dominate the subject’s sensitivity label. This rule prevents the subject from lowering the object’s sensitivity 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 sensitivity 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 Eyes-only	(strictly) dominates	Secret A B Eyes-only
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 sensitivity labels, Trusted Solaris displays a confirmation dialog box if you are permitted to change the sensitivity label or, if you are not permitted, Trusted Solaris 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 sensitivity label, or cancel the transaction altogether.

How Trusted Solaris Protects the Handling of Sensitive Information

Note – If your site does not use information labels, you can skip this section.

Trusted Solaris protects sensitive information by

- Providing information labels
- Monitoring information transactions

Information Labels

Trusted Solaris provides *information labels (ILs)* to indicate the sensitivity and handling of data, processes, and devices. (Some organizations refer to information labels as *advisory labels*.) In contrast to sensitivity labels, the purpose of information labels is advisory and not related to access control. They serve as a reminder of the security levels for subjects and objects. Information labels also can help users decide whether to downgrade the sensitivity label of a file. An information label is composed of

- Classification component
- Compartment component(s)
- Marking component(s) (optional) containing special handling instructions for the data

Some typical information labels are shown in Figure 1-2.

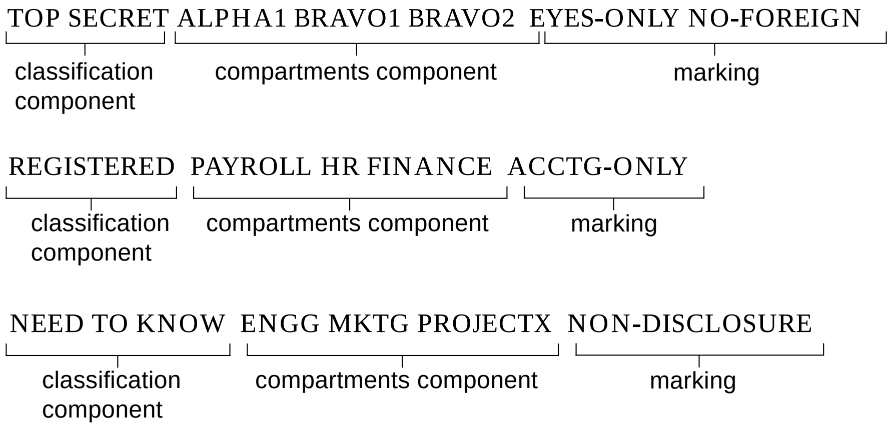


Figure 1-2 Typical Information Labels

Information labels may be displayed in window title bars (with no square brackets so that they can be differentiated from sensitivity labels), in the Trusted Stripe at the bottom of the screen, or not at all, depending on how your system is configured.

CMW Labels

Trusted Solaris combines the sensitivity label and the information label in a string called a *CMW label*; this is what appears in window title bars when you can see both sensitivity labels and information labels. The CMW label merely serves as a container for the two labels and is of interest mainly to system administrators and programmers.

Monitoring Information Transactions

Trusted Solaris monitors transactions to ensure that new and modified documents have appropriate information labels. In a transaction where a subject accesses one or more objects with information labels at different levels, the highest level information label present in the transaction is applied to any resulting objects. This is called *information label floating*; that is, the information label floats to the highest information label classification present in the transaction and combines the compartments of all information labels involved.

For example, pasting a paragraph from a document with a SECRET information label into an document with an information label of UNCLASSIFIED raises the UNCLASSIFIED document's information label to SECRET in order to protect the SECRET information. Another example would be a user with a SECRET information label editing an UNCLASSIFIED document. This raises that document's level to SECRET because the user's editing of the document may increase its sensitivity.

When you perform a drag-and-drop or copy-and-paste operation that could cause an information label to float, Trusted Solaris may display a confirmation dialog box (depending on your configuration) to help you set the information label of the destination file to the proper level.

How Trusted Solaris Keeps Labels Separate

Trusted Solaris helps keep information at different sensitivity labels separate by

- Letting users select single- or multilevel sessions
- Providing labeled workspaces
- Storing files in separate directories according to sensitivity 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 sensitivity label or at multiple sensitivity labels (if you are permitted to). You then set your *session clearance* or *session sensitivity 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 sensitivity 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 sensitivity labels for different workspaces.

Providing Labeled Workspaces

The workspaces in Trusted Solaris are accessed through buttons in the front panel, just as in the standard Solaris operating environment. However, in Trusted Solaris, you can devote a workspace entirely to a single sensitivity label. This is very convenient when you are in a multilevel session and do not wish to move information between files at different sensitivity labels.

Storing Files in Separate Directories by Sensitivity Labels

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

- **multilevel directory (MLD)** – is a special type of directory that transparently stores information by sensitivity 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 sensitivity 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 sensitivity label are visible and accessible. If you keep files at different sensitivity labels in your home directory, for example, you cannot normally view files at sensitivity labels other than your current sensitivity label.

Figure 1-3 illustrates the concept of hidden single-level directories within a multilevel directory. Figure 1-3 (a) shows the contents of a multilevel home directory called `/myHomeDir` from the user's view while working at Confidential A B; Figure 1-3 (b) 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 sensitivity labels associated with the single-level directories are shown in their short form inside parentheses; the sensitivity labels do not actually appear in the directory names.)

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
```

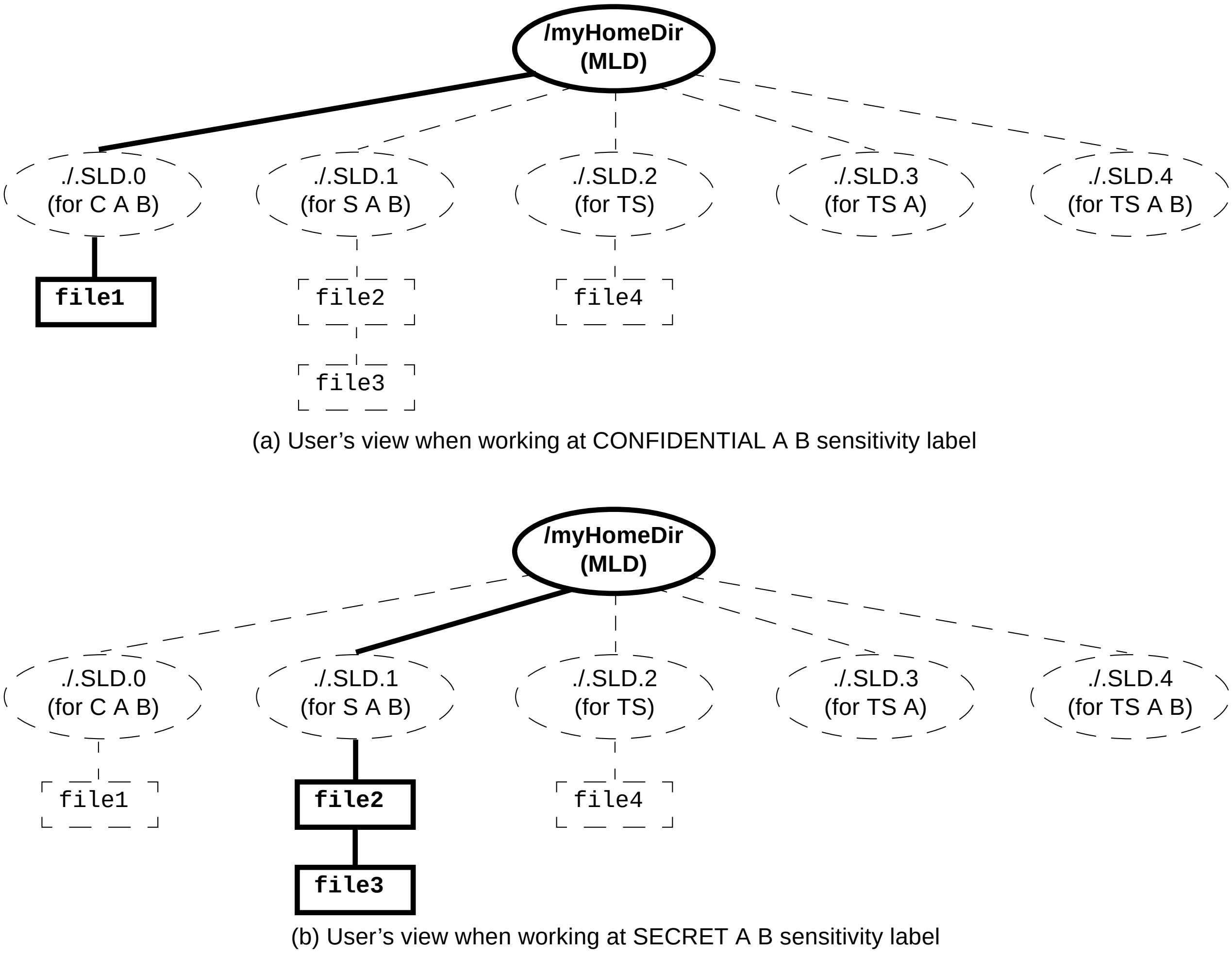


Figure 1-3 Visible and Hidden Files and Directories

Enforcing MAC for Email Transactions

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

Clearing Objects Prior to Reuse

Trusted Solaris 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 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 Trusted Solaris 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 are divided among four predefined 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 Trusted Solaris, 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 you one or more execution profiles. 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.

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, it may be a sign that you are not permitted to use this application. Check with your administrator.

Predefined Roles

By default, Trusted Solaris divides system responsibilities among four predefined roles: *security administrator*, *system administrator*, *root*, and *system operator*. The *security administrator* role is used for security issues, such as assigning sensitivity 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 *root* role is used primarily for installing commercial software. The *system operator* role is used for system backups, printer administration, and mounting removable media. 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 Trusted Solaris

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, "Accessing and Leaving the Trusted Solaris Environment," explains how users log in and out of the Trusted Solaris environment, with numbered steps to show the procedures.
- Chapter 3, "Tour of the Trusted Solaris Environment," is a step-by-step description of a typical Trusted Solaris session.
- Chapter 4, "Elements of the Trusted Solaris Environment," provides detailed descriptions of the major features of the Trusted Solaris environment with step-by-step procedures for the menu commands.
- Chapter 5, "Managing Files and Directories," shows you how to use the File Manager in the Trusted Solaris 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 1-4. 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.

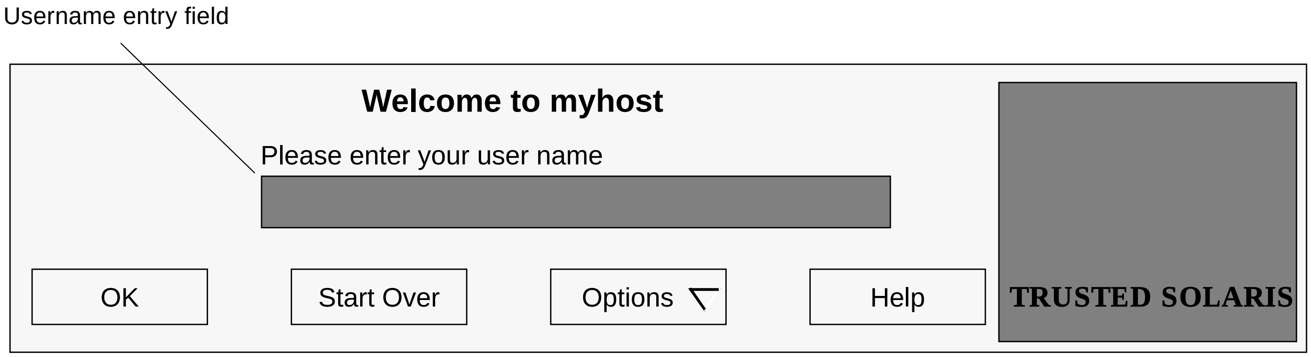


Figure 2-1 Username Dialog Box

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 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.

Figure 1-4 Typical Procedure

Other Useful Manuals

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

Accessing and Leaving the Trusted Solaris Environment

2

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

The Login Process

Before you can use a system, your Trusted Solaris 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. Your initial password is supplied by your Trusted Solaris administrator.

  Successful completion of identification and authentication confirms your right to use the system.
- **Message checking and session type selection** –The Message of the Day 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 sensitivity label. If this is the case, you will not be able to select the type of session in the Message of the Day 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.

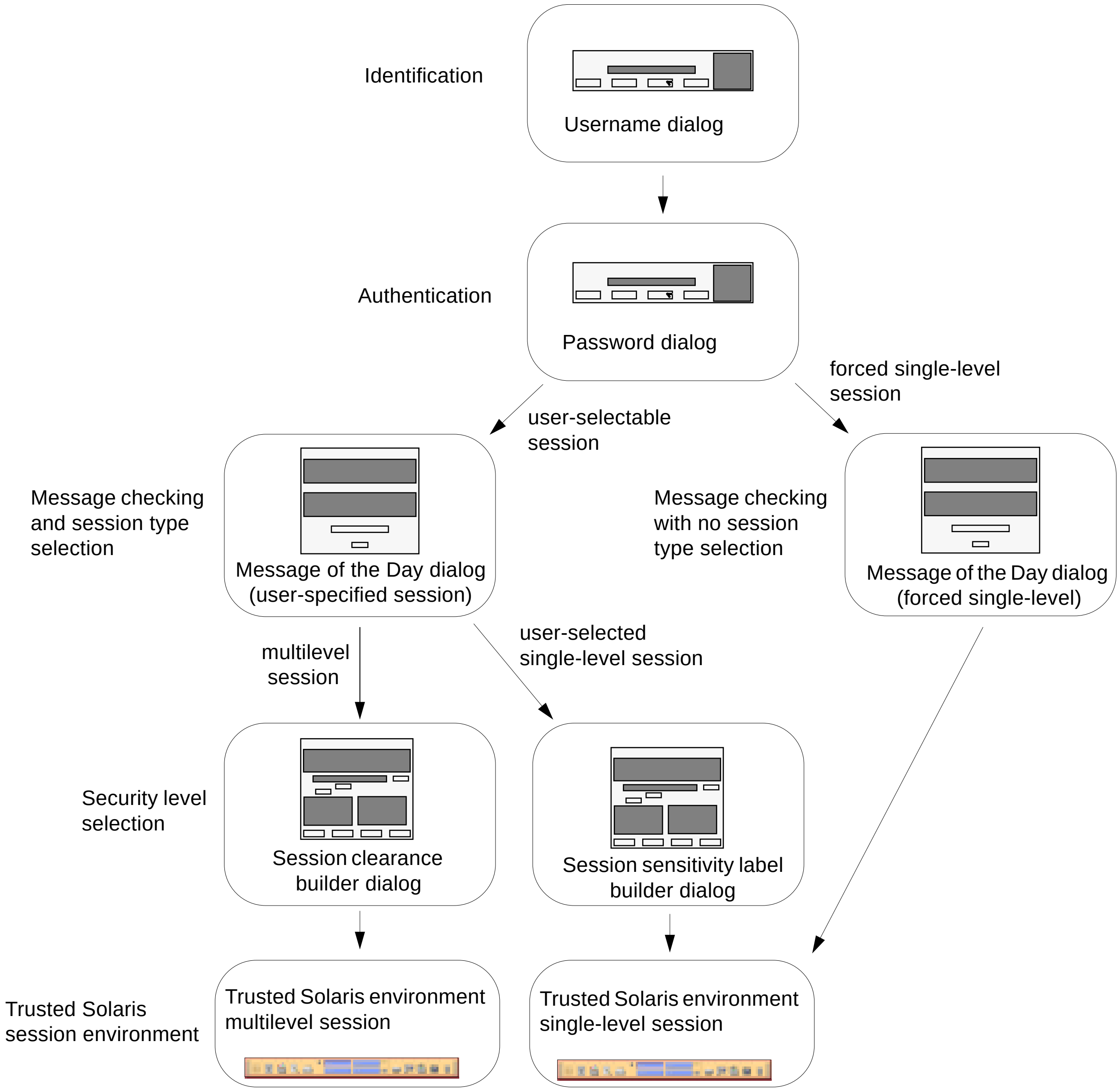

Identification
Username dialog
Authentication
Password dialog
forced single-level session
user-selectable session
Message checking and session type selection
Message of the Day dialog (user-specified session)
Message checking with no session type selection
Message of the Day dialog (forced single-level)
multilevel session
user-selected single-level session
Security level selection
Session clearance builder dialog
Session sensitivity label builder dialog
Trusted Solaris session environment
Trusted Solaris environment multilevel session
Trusted Solaris environment single-level session

Figure 2-1 Trusted Solaris Login Process

Identification

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

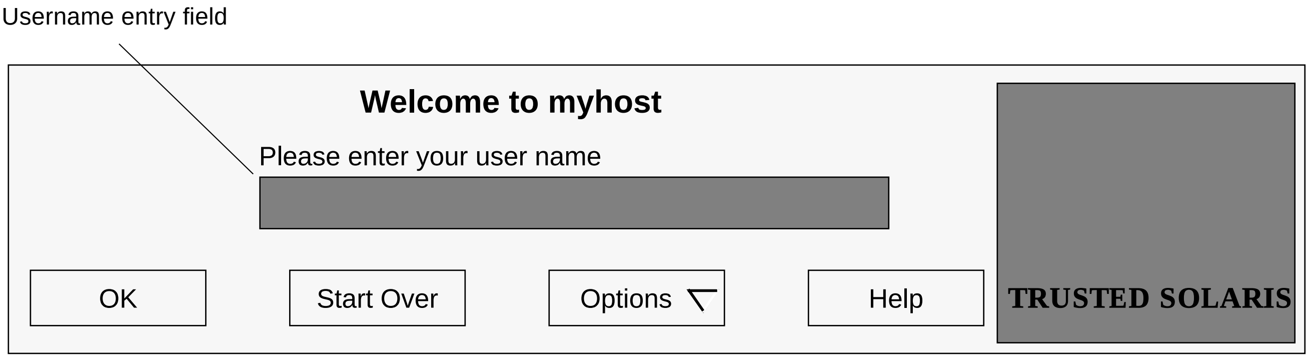


Figure 2-2 Username Dialog Box

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 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.

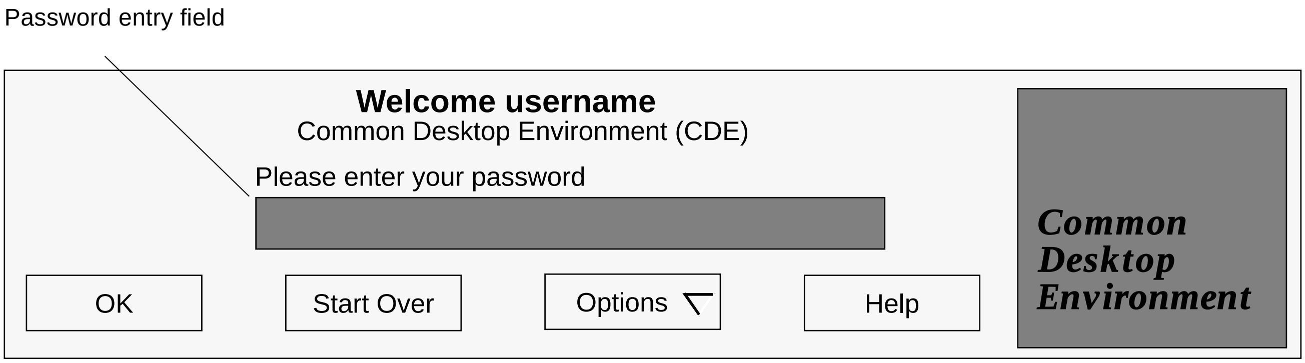
Caution – You should *never* see the Trusted Stripe when the login screen appears. If you ever see the screen stripe while attempting to log in or unlock the screen, do not type your password because there's a chance you are being spoofed, that is, an intruder's program is masquerading as a login program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



Welcome username
Common Desktop Environment (CDE)
Please enter your password

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.
```

The username dialog box then reappears and you should return to Step 1.

Message Checking and Session Type Selection

After you successfully enter your username and password, the Message of the Day dialog box is displayed. It provides status information and, if your site is configured for user-specified sessions, lets you a select a single- or multilevel session. If your site is configured for forced sensitivity label sessions, then you will automatically be in a single-level session.

Single-level Versus Multilevel Sessions

In a *multilevel session*, you can operate at different sensitivity 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 sensitivity label assigned to you by your administrator.

In a *single-level session*, you specify a *session sensitivity label* at which you operate for the entire session. In a single-level session, you can access and write to files at that sensitivity label only. You cannot change the sensitivity label of workspaces in the session. Note that you can assume a role within a single-level session and then operate at any sensitivity 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 sensitivity labels are shown in their short form inside square brackets ([]) and that information labels appear in their long form.

The three columns on the left show the user's session selections at login. Note that users set *session sensitivity 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 is always displayed with the choices permitted).

The four columns on the right show the label values available in the session. The Initial Workspace SL column represents the sensitivity label when the user first enters the Trusted Solaris environment. The Available Sensitivity Labels column lists the sensitivity labels that the user is permitted to switch to in the session. The Initial Input IL column refers to the starting input information label that is applied to data that the user enters from the keyboard or through mouse actions; the system assumes that new data is entered at the lowest information label unless explicitly given a different information label. The Maximum Information Label column refers to the highest information label at which the user can enter or edit data.

Table 2-1 How Session Selections Affect Session Values

User Selections			**Session Label Values**			
Session Type	**Session Sensitivity Label**	**Session Clearance**	**Initial Workspace SL**	**Available Sensitivity Labels**	**Initial Input IL**	**Maximum Information Label**
single-level	[S A]	—	[S A]	[S A]	UNCLASSIFIED	SECRET A with markings
multilevel	—	[S A]	[U]	[U], [C], [C A], [S], [S A]	UNCLASSIFIED	(workspace sensitivity label) with markings

In the first row of the table, the user has selected a single-level session with a session sensitivity label of [S A]. In the Trusted Solaris environment, the user has an initial workspace sensitivity label of [SA] which is also the only sensitivity label at which the user can operate. The user has an initial input information label of UNCLASSIFIED, because the input information label is always set initially to the lowest label in the user's range. The user can reset the input information label to SECRET A with any markings, because that is the highest label in the current session.

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 sensitivity label is set to [U] (that is, a sensitivity label of UNCLASSIFIED), because that is the lowest possible sensitivity label in the user's account sensitivity label range. The user can switch to any sensitivity label between [U], the minimum, and [S A], the session clearance. The initial input information label is UNCLASSIFIED as in the single-level session. The maximum information label is limited to the sensitivity label of the current workspace (or window) and any markings.

▼ To Check Messages and Select Session Type

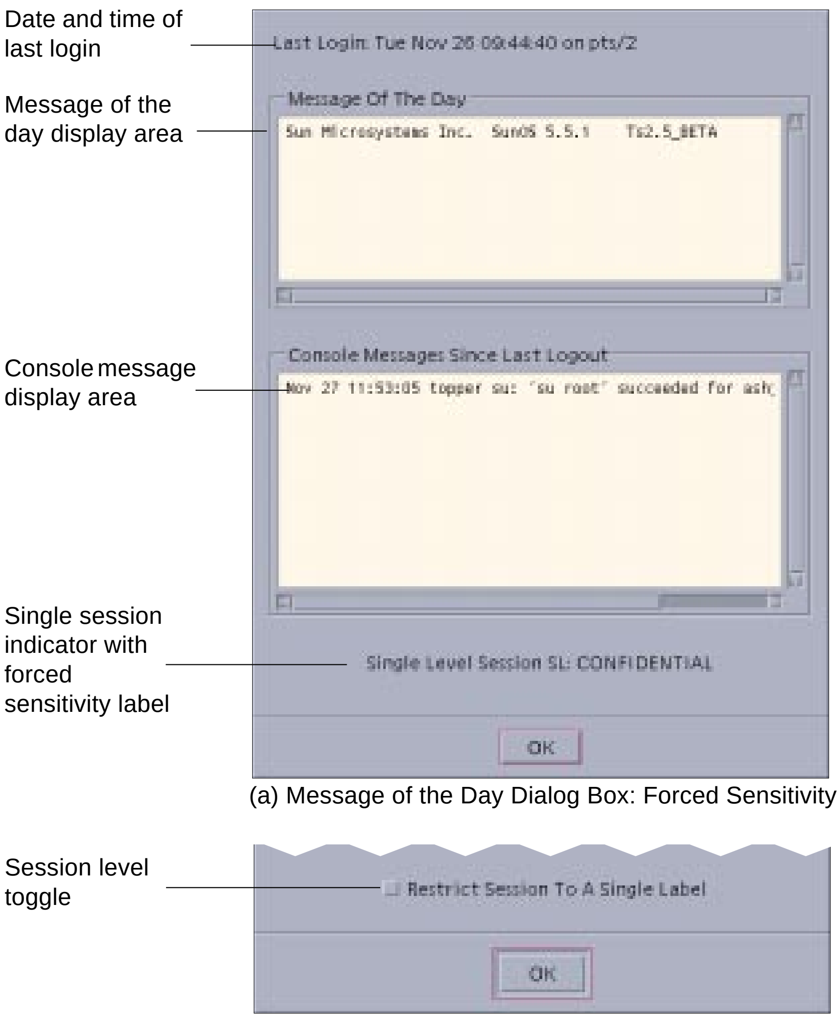
If your system is configured for forced sensitivity label sessions, the Message of the Day dialog box in Figure 2-4 (a) is displayed and you can ignore step 4. If you are permitted to specify single- or multilevel sessions, the Message of the Day dialog box with the session level toggle shown in Figure 2-4 (b) appears.

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 sensitivity label in your session (user-specified session operation only).**
   In a single-level session, you operate at a single discrete sensitivity label. You can only access and write to files at the same sensitivity label. If you do not click the toggle, you are implicitly selecting a multilevel session and can view data at different sensitivity 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 sensitivity label assigned to you by your administrator.


Date and time of last login
Message of the day display area
Console message display area
Single session indicator with forced sensitivity label
OK
Session level toggle
OK

Last Login: Tue Nov 26 09:44:40 on pts/2

Message Of The Day

```
Sun Microsystems Inc.   SunOS 5.5.1     Ts2.5_BETA
```

Console Messages Since Last Logout

```
Nov 27 11:53:05 topper su: 'su root' succeeded for ash
```

Single Level Session SL: CONFIDENTIAL

(a) Message of the Day Dialog Box: Forced Sensitivity Label Operation

□ Restrict Session To A Single Label

(b) Message of the Day Dialog Box: User-specified Sessions (Lower Portion)

Figure 2-4 Message of the Day Dialog Box

5. **Click OK (or press the Enter or Return key) to close the Message of the Day dialog box.**
   If your system is configured for forced sensitivity label operation, the Trusted Solaris environment is displayed after the Message of the Day dialog box is closed; otherwise you will set the session level next.

Setting the Session Level

Note – If you are configured for forced sensitivity label operation, the Trusted Solaris environment will be displayed after you close the Message of the Day 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 sensitivity label version of the Label Builder dialog box is displayed and you select the sensitivity label for your entire session (see Figure 2-6).

Note – Workstations can be restricted to a limited range of session clearances and sensitivity labels. For example, a workstation in a lobby might be limited to UNCLASSIFIED labels only. If the session clearance or sensitivity 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

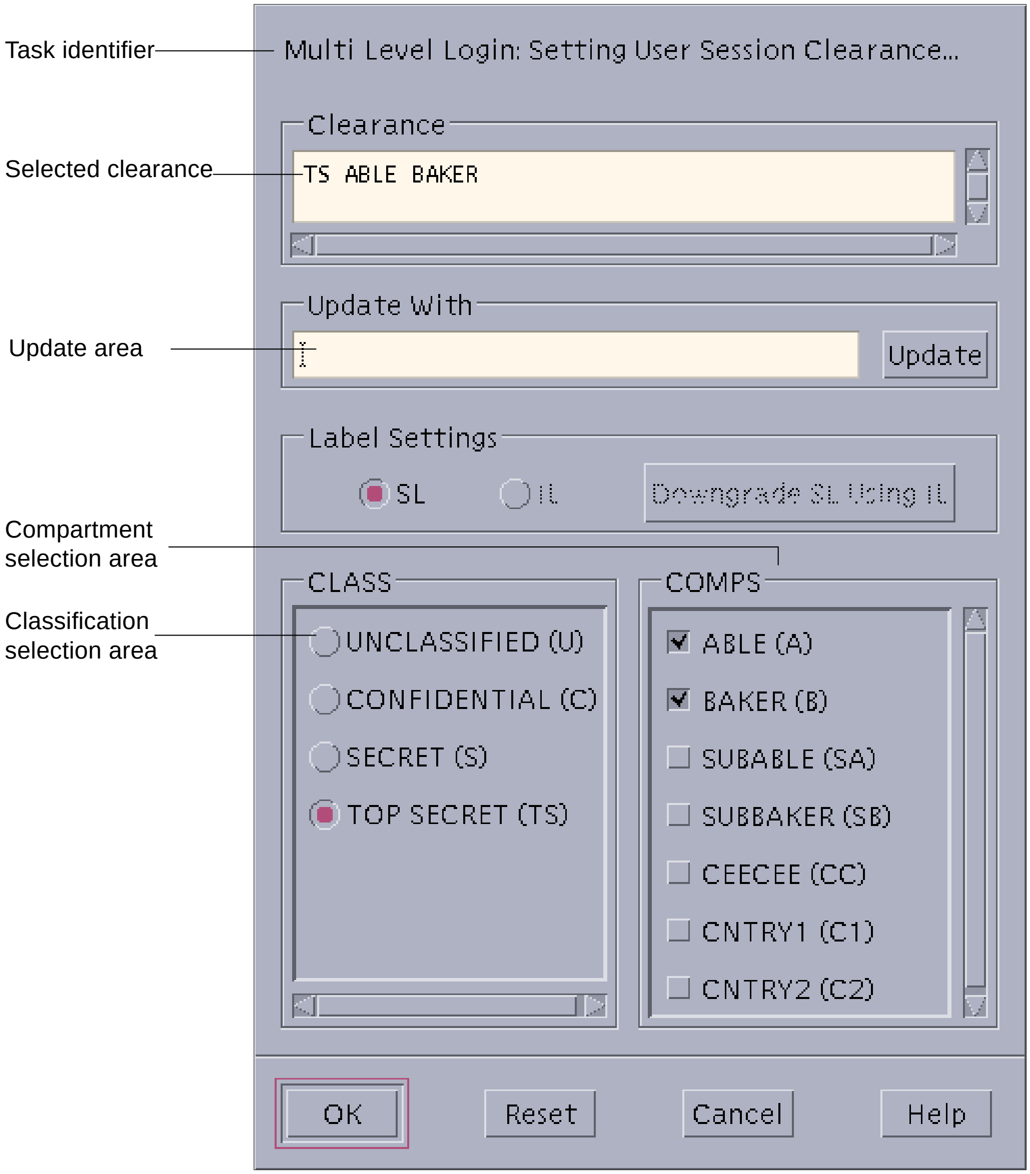
The session clearance sets the top boundary for sensitivity labels of files that you will be able to access in the session. To set the clearance, you use the Clearance Builder dialog box (see Figure 2-5).

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 update area. Click the Update button if it is correct or go back to step 2 to build a different clearance.**



Task identifier

Selected clearance

Update area

Compartment selection area

Classification selection area

Multi Level Login: Setting User Session Clearance...

Clearance: TS ABLE BAKER

Update With:

Label Settings: ● SL ○ IL

CLASS:
○ UNCLASSIFIED (U)
○ CONFIDENTIAL (C)
○ SECRET (S)
● TOP SECRET (TS)

COMPS:
☑ ABLE (A)
☑ BAKER (B)
☐ SUBABLE (SA)
☐ SUBBAKER (SB)
☐ CEECEE (CC)
☐ CNTRY1 (C1)
☐ CNTRY2 (C2)

Figure 2-5 Session Clearance Builder Dialog Box

▼ To Select a Sensitivity Label for a Single-level Session

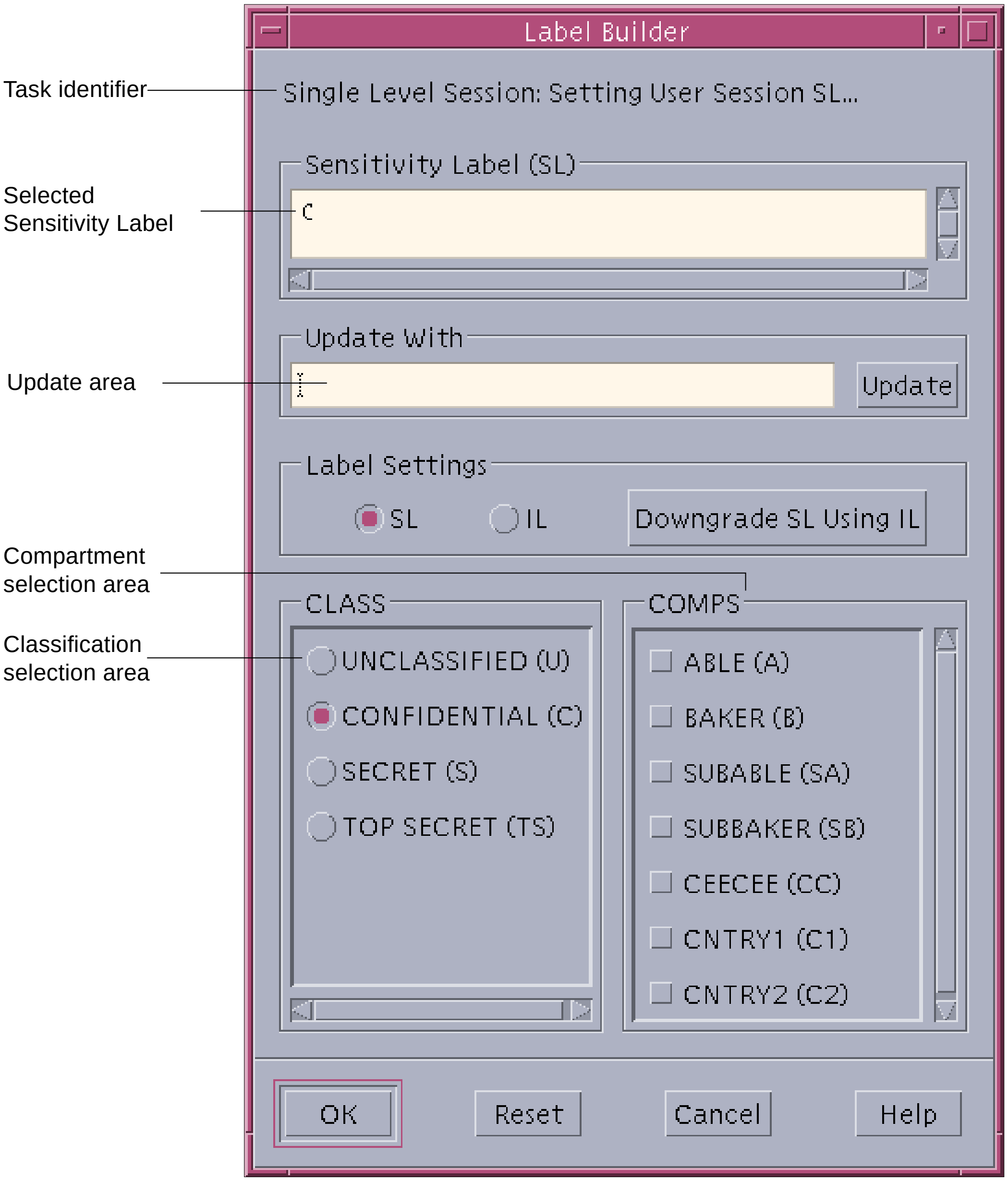
The session sensitivity label sets the sensitivity label at which you intend to operate in this single-level session. To set the session sensitivity label, you use the Single-Level Session Sensitivity Label Builder dialog box shown in Figure 2-6.

1. **To use the default sensitivity label in the Sensitivity Label field, click OK (or press Enter) and wait for the Trusted Solaris environment to be displayed.**
   For a different sensitivity label, go to step 2 to build a new sensitivity 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 sensitivity label you have built in the update area. Click the Update button if it is correct or go back to step 2 to build a different sensitivity label.**



Single Level Session: Setting User Session SL...

Sensitivity Label (SL): C

CLASS:
○ UNCLASSIFIED (U)
● CONFIDENTIAL (C)
○ SECRET (S)
○ TOP SECRET (TS)

COMPS:
□ ABLE (A)
□ BAKER (B)
□ SUBABLE (SA)
□ SUBBAKER (SB)
□ CEECEE (CC)
□ CNTRY1 (C1)
□ CNTRY2 (C2)

Figure 2-6 Single-Level Session Sensitivity Label Builder

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 2-7).**

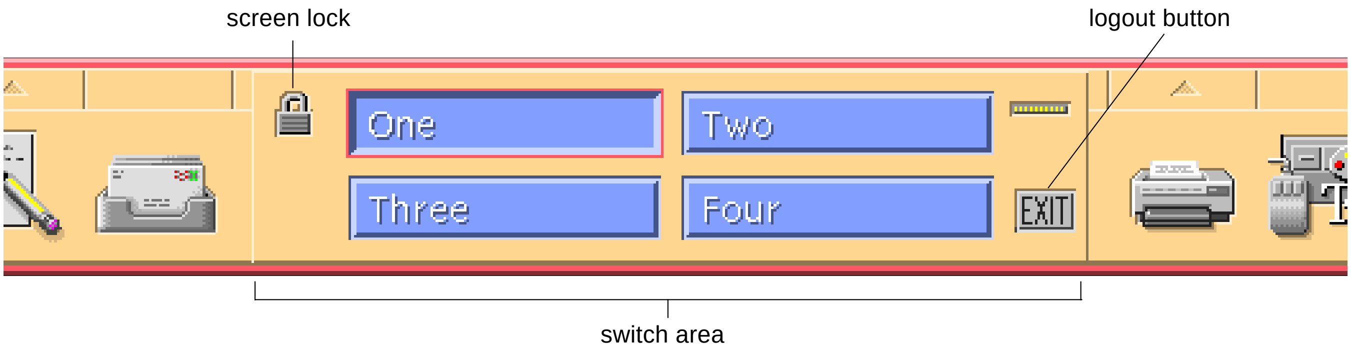
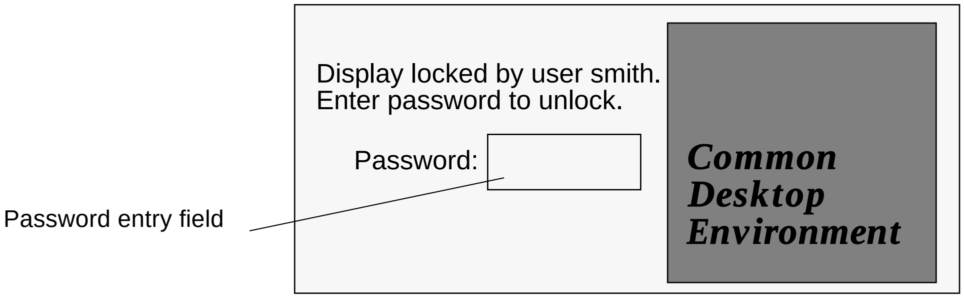


Figure 2-7 Front Panel Switch Area

The screen turns black and the dialog box shown in Figure 2-8 is displayed.



Display locked by user smith.
Enter password to unlock.

Password entry field

Figure 2-8 Lock Screen Dialog Box

Note – The Trusted Stripe does not display when the screen is locked.

---

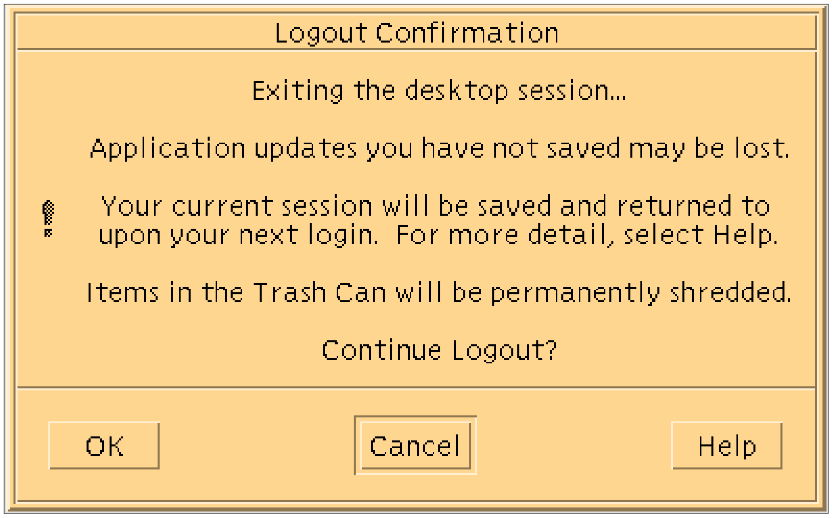
2. **To unlock your screen, type your password in the password entry field and press Enter.**
   This returns you to your session in its previous state.

▼ To Log Out of the Trusted Solaris Environment

1. **Click on the EXIT icon in the switch area of the front panel (see Figure 2-7).**

   The confirmation dialog box shown in Figure 2-9 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.**



Logout Confirmation

Exiting the desktop session...

Application updates you have not saved may be lost.

Your current session will be saved and returned to upon your next login. For more detail, select Help.

Items in the Trash Can will be permanently shredded.

Continue Logout?

Figure 2-9 Logout Confirmation Dialog Box

▼ To Shut Down Your System

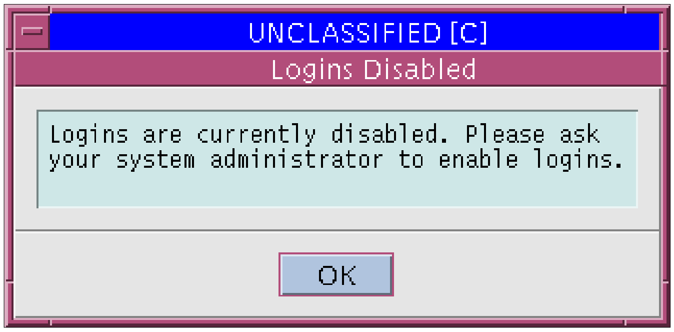
Logging out is the normal way to end a Trusted Solaris session. If you need to turn off your machine, you should use the Shut Down command and then turn off your power. If you do shut down your machine, it may require rebooting by an authorized user depending on your security policy.

1. **Select the Shut Down selection 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.**

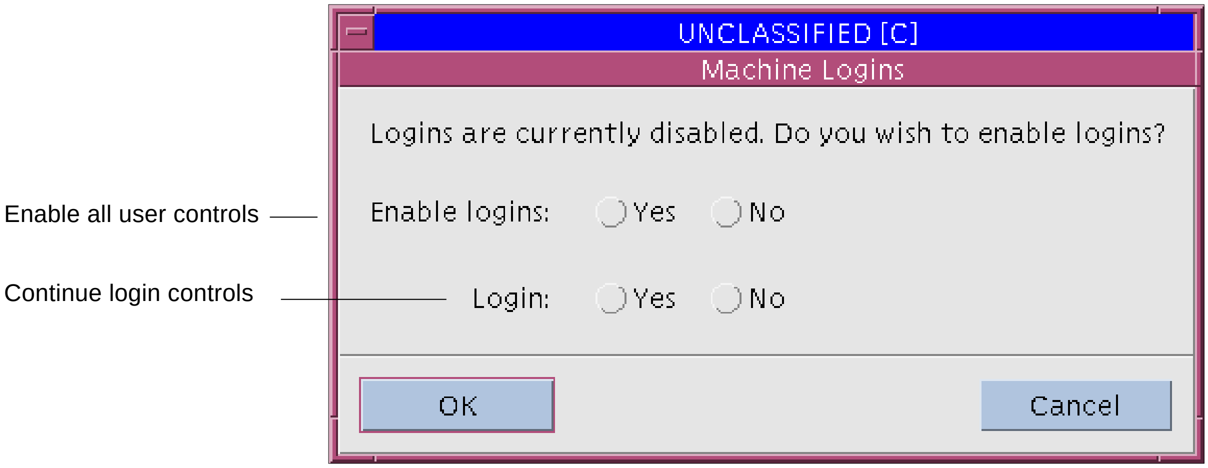
Enabling Logins When Logins Are Disabled

As a security measure, your administrator can configure your site so that all passwords are disabled after a reboot. If a reboot has occurred and you are not authorized to enable logins, the dialog box shown in Figure 2-10 appears; you must notify your Trusted Solaris administrator to help you log in. If you are authorized to enable logins, the dialog box shown in Figure 2-11 appears.



```
Logins are currently disabled. Please ask
your system administrator to enable logins.
```

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



Logins are currently disabled. Do you wish to enable logins?

Enable all user controls

Continue login controls

Figure 2-11 Disabled Logins Dialog Box for Users Authorized to Enable Logins

▼ To Enable Logins After a Reboot

1. Select the appropriate Enable logins button (see Figure 2-11):

a. Click the Yes button to enable logins for all users.
You should first check your site's security policy to ensure that enabling logins does not cause a security breach.

b. Click the No button to leave other logins disabled.
Do this if you are not ready to enable logins.

2. **Select the appropriate Login button:**

   a. **Click the Yes button to log in.**

   b. **Click the No button to enable logins without logging in.**

3. **Click OK to enable 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`, `.dtprofile`, `.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

3

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 chapter discusses these topics:

Tour: Logging In

As in the standard Solaris CDE environment, the Username dialog box is displayed (see Figure 3-1) when the system is waiting for logins. To access the system, you have to identify yourself by your username and authenticate yourself by supplying your password.

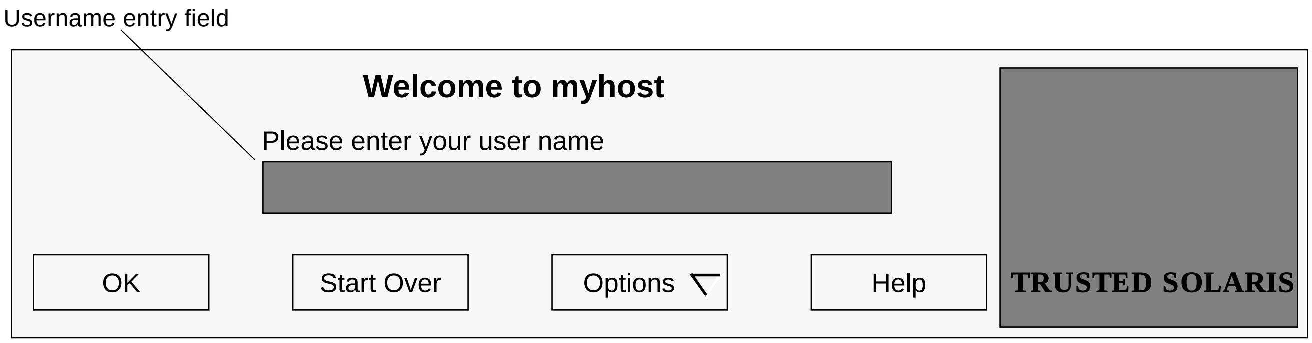


Figure 3-1 Username Dialog Box

1. **In the username dialog box, type your username in the text field and click OK (see Figure 3-1).**
   This step causes the password dialog box (see Figure 3-2) to be displayed.

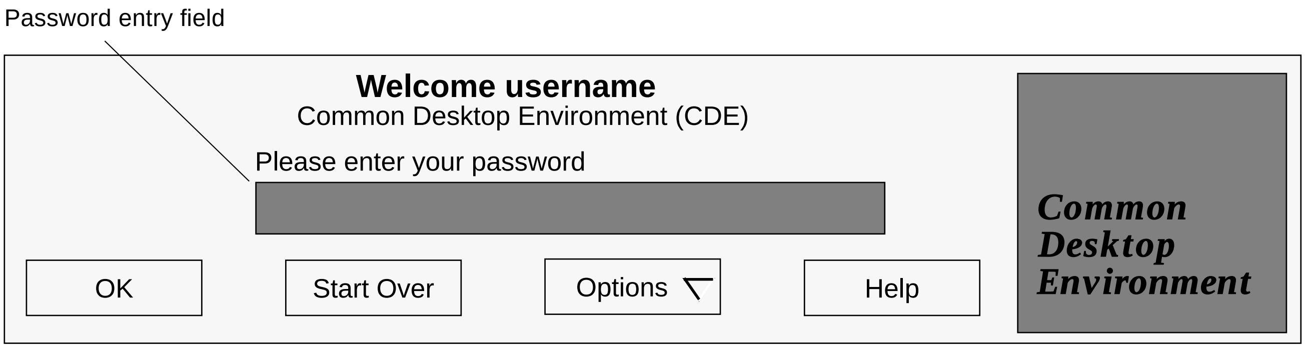

Password entry field
Welcome username
Common Desktop Environment (CDE)
Please enter your password
OK
Start Over
Options
Help
Common Desktop Environment

Figure 3-2 Password Dialog Box

2. **In the password dialog box, type your password and click OK (see Figure 3-2).**
   This step causes the Message of the Day dialog box (see Figure 3-3) to be displayed.

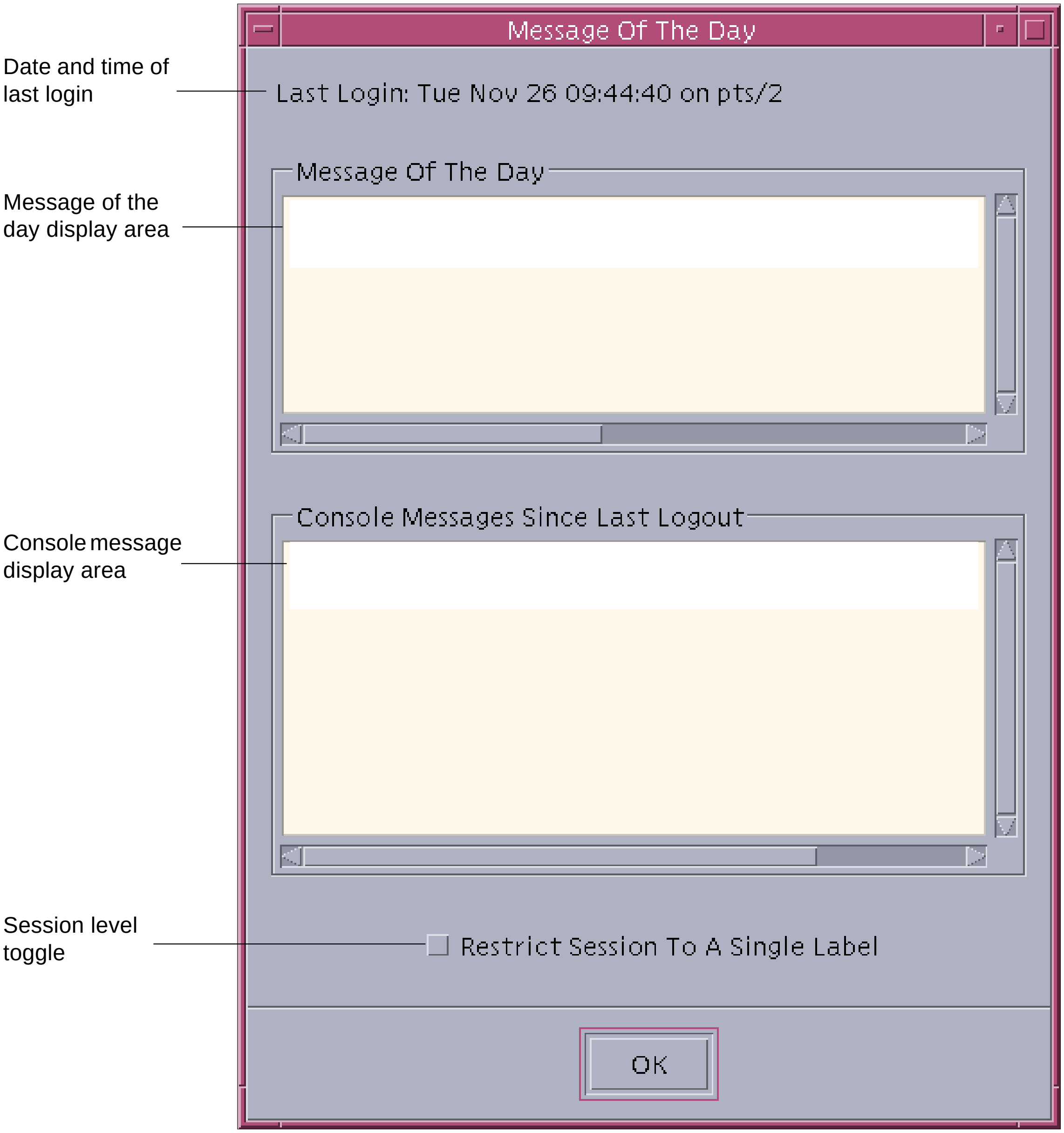
Tour: Setting the Session Type

The Message of the Day dialog box (see Figure 3-3) 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.

3. **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.

4. **Check that the Restrict Session to a Single Label button is not pushed in and then click OK (see Figure 3-3).**
   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 you are configured for forced sensitivity label sessions, 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 this tutorial by skipping to Step 9 and continuing to Step 14.



Message Of The Day
Date and time of last login
Message of the day display area
Message Of The Day
Console message display area
Console Messages Since Last Logout
Session level toggle
□ Restrict Session To A Single Label
OK

Last Login: Tue Nov 26 09:44:40 on pts/2

Figure 3-3 Message of the Day Dialog Box

Tour: Using the Label Builder to Set a Session Clearance

The Session Clearance Builder dialog box (see Figure 3-4) 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, sensitivity label, or information 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.

For the tour, you need to set a session clearance higher than your minimum sensitivity label; this is necessary to demonstrate how multilevel sessions work. If you are not cleared for labels higher than the minimum, enter your clearance; you can participate up to Step 14.

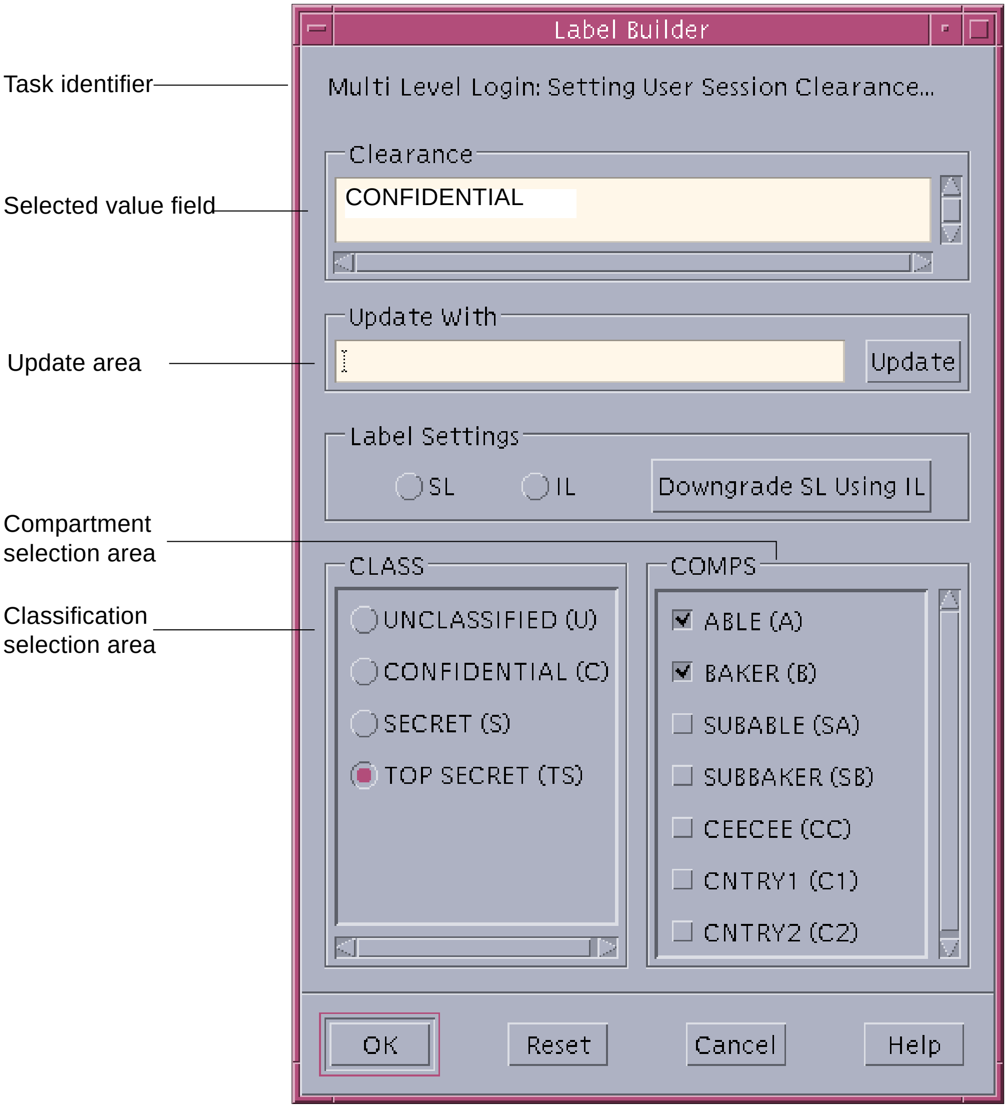
Note – In this example, the classification selection area is identified by the tag "CLASS" and the compartments area by the tag "COMPS." These tags may be different in your configuration.

5. **To use the default session clearance in the selected value field, click OK (or press the Enter or Return key) and wait for the Trusted Solaris environment to be displayed. You can then proceed to Step 9.**
   To build a different session clearance, go to Step 6.

6. **Click the desired classification in the classification selection area.**

7. **Click the desired compartments (if any) in the compartment selection area.**

8. **Check the session clearance you have built in the update area. Click the Update button if it is correct or go back to Step 6 to build a different session clearance.**
   After you close the Session Clearance dialog box, the Trusted Solaris environment is displayed.



Multi Level Login: Setting User Session Clearance...

Clearance

CONFIDENTIAL

Update With

Label Settings

○ SL ○ IL

CLASS

○ UNCLASSIFIED (U)

○ CONFIDENTIAL (C)

○ SECRET (S)

● TOP SECRET (TS)

COMPS

☑ ABLE (A)

☑ BAKER (B)

□ SUBABLE (SA)

□ SUBBAKER (SB)

□ CEECEE (CC)

□ CNTRY1 (C1)

□ CNTRY2 (C2)

Figure 3-4 Typical Label Builder Dialog Box

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.

9. Examine the Trusted Solaris environment (see Figure 3-5).

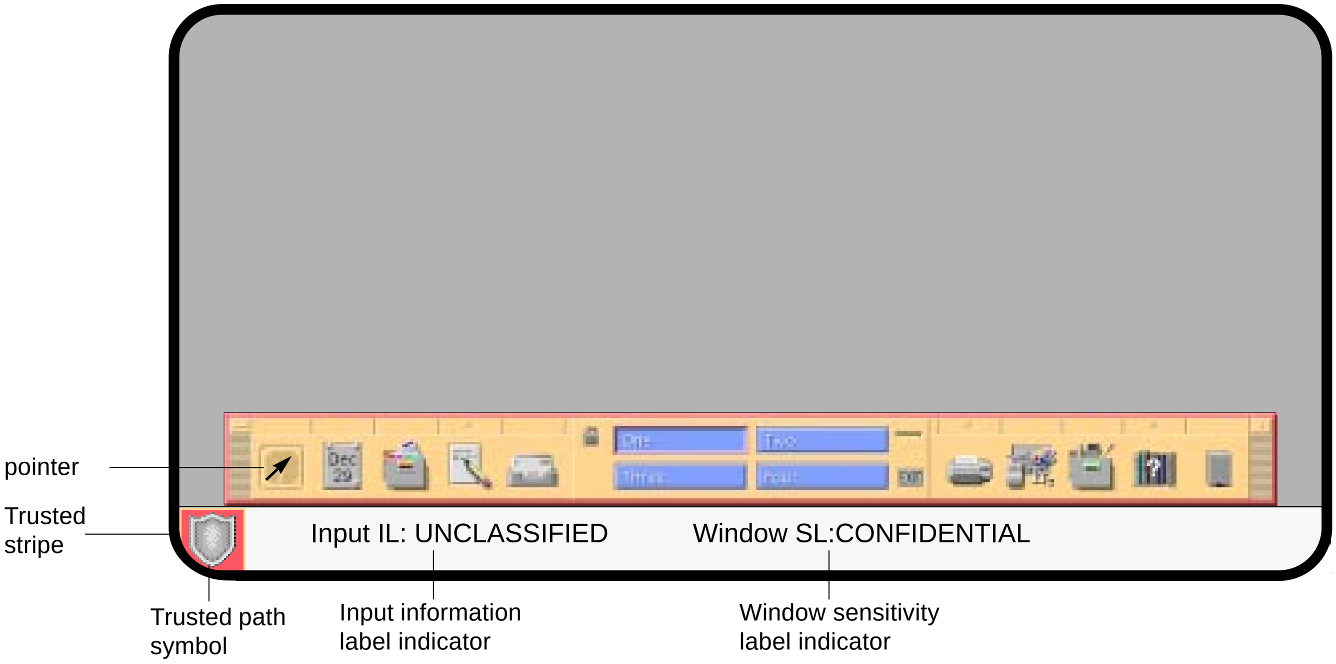


Figure 3-5 Basic Trusted Solaris Environment

Trusted Solaris 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 – There are different ways in which the trusted stripe can be configured. This is explained in depth in “Label Displays in the Trusted Solaris Environment” on page 65.

The trusted stripe potentially has three elements (see Figure 3-5):

- **Trusted path symbol** – is displayed when you perform any activity related to security.
- **Input IL indicator** – shows the information label to be applied to data you enter into the active window, either from the keyboard or from mouse-button events.

Note – If your environment is set so that you click in a window to make it active, the Input IL indicator will not change its value for a window until you click inside that window.

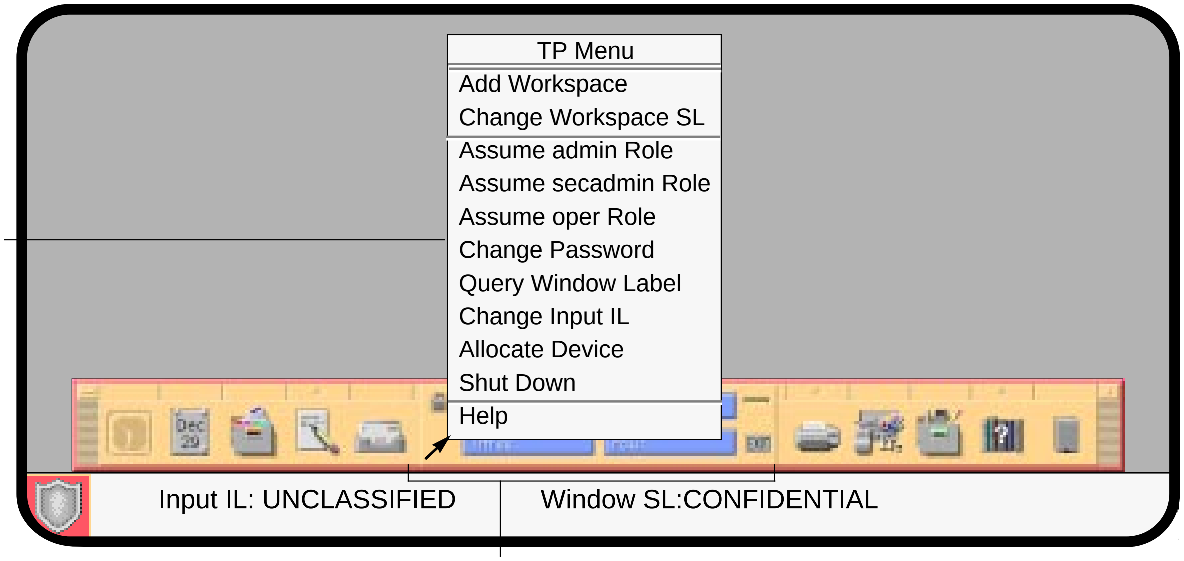
- **Window SL indicator** – displays the sensitivity label of the active window (that is, the window that has the pointer focus).

Note – Note that the input IL and window SL indicators are optional and may not be configured for your site.

In this example, the initial Window SL for this workspace is CONFIDENTIAL as specified by the user when logging in. The Input IL is initially set to the lowest information label in your organization, UNCLASSIFIED, in this example. You can raise the Input IL up to the sensitivity label of your current workspace, including any valid markings.

10. **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 (see Figure 3-6). 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.

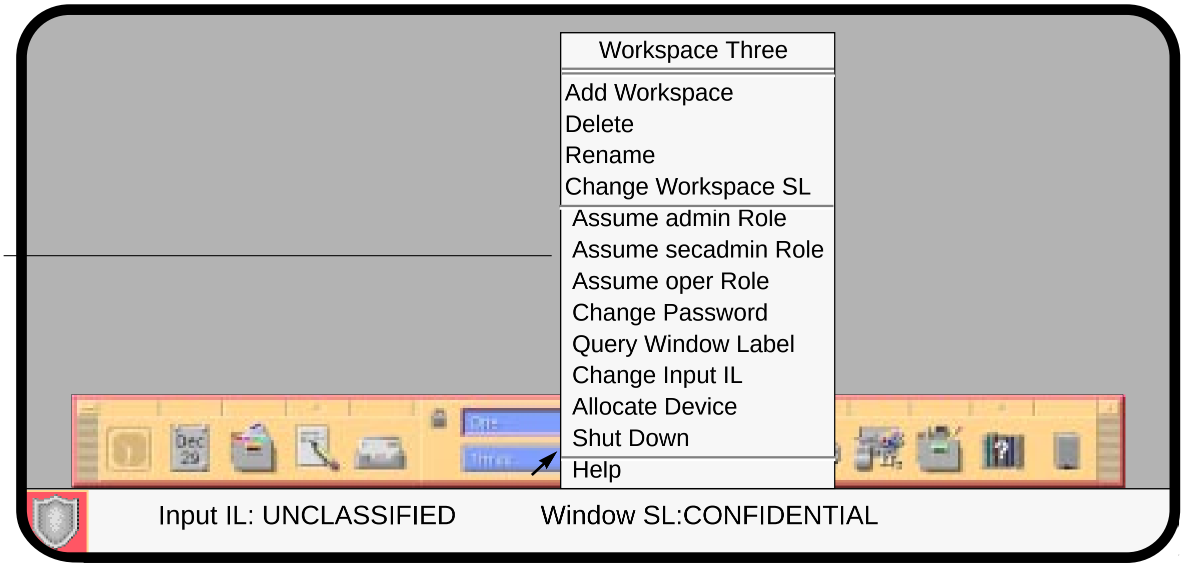
11. **Hold down the right mouse button with the pointer over the Workspace Three button.**
    This displays the workspace version of the Trusted Path menu (see Figure 3-7), which contains options that can operate on that workspace.



Basic Trusted Path menu

switch area

Figure 3-6 Basic Trusted Path Menu



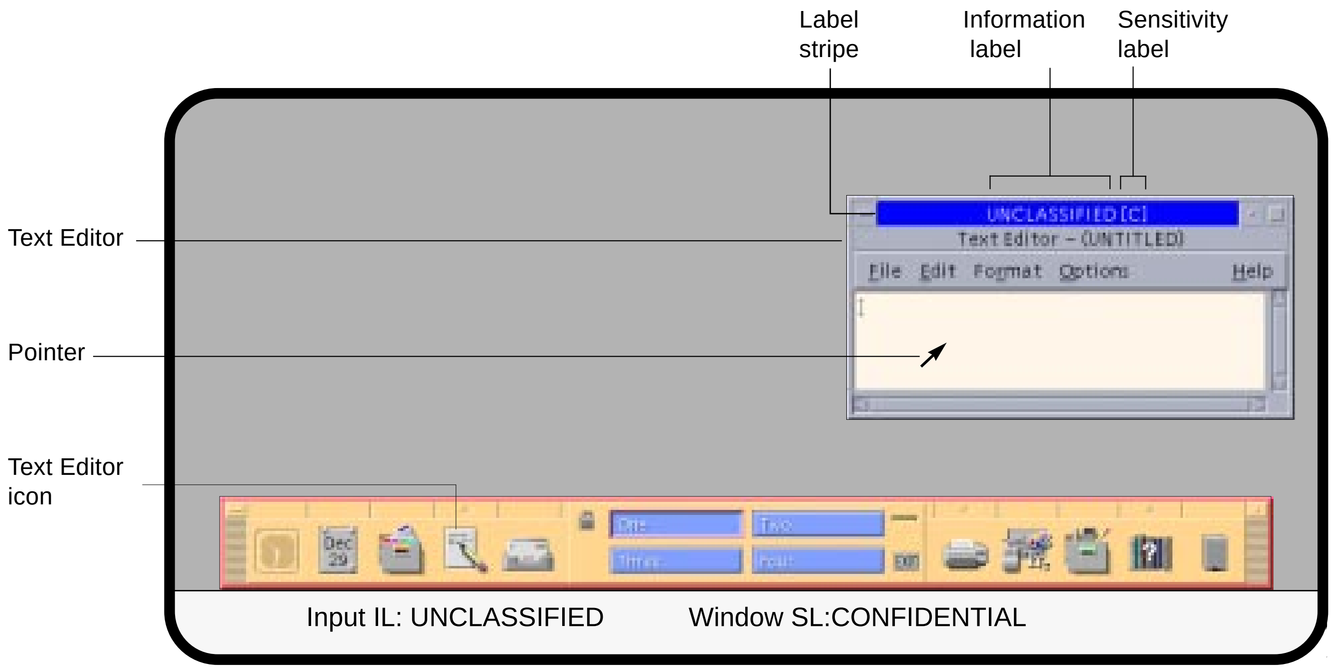
Trusted Path menu - workspace version

Figure 3-7 Trusted Path Menu - Workspace Version

Tour: Launching an Application

All applications in the Trusted Solaris environment have sensitivity and information labels. They are *subjects* in any data transactions and must dominate (have an equal or higher sensitivity label than) the *objects* (usually files) they try to access. The sensitivity label and information label 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.

12. Click the Text Editor icon in the Front Panel to launch the Text Editor (see Figure 3-8).



Input IL: UNCLASSIFIED   Window SL:CONFIDENTIAL

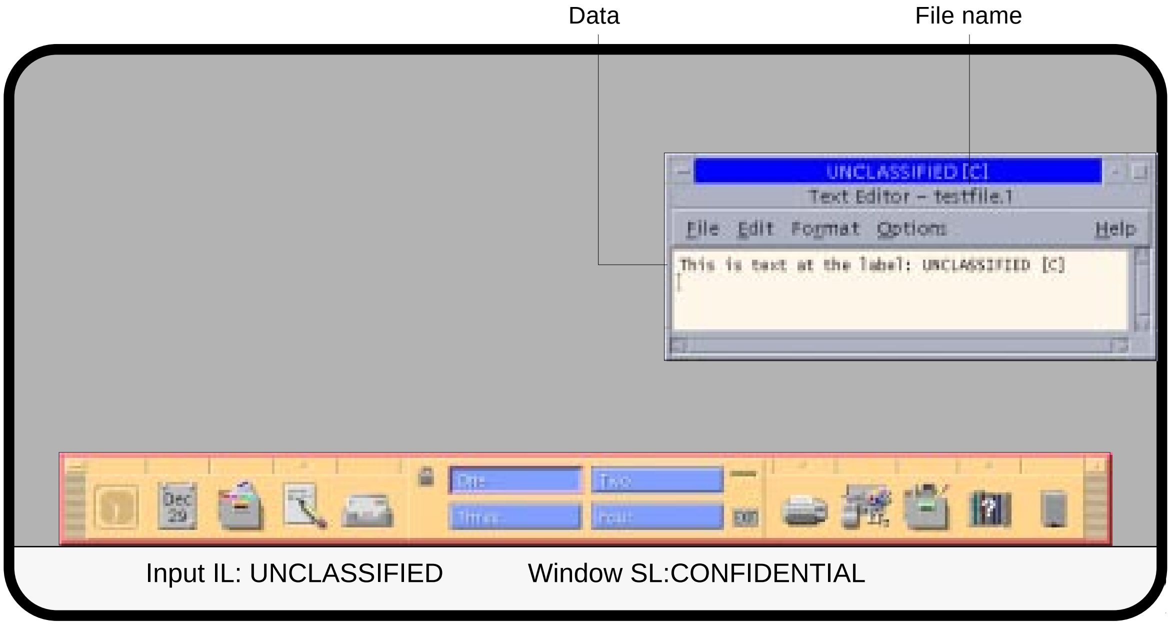
Figure 3-8 Running an Application

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

Tour: Entering Data and Creating Files

When you type data in an application, the data you enter is classified at the information label for the current window (in this example, the Input IL appears in the trusted stripe). Remember, the information label serves as an advisory device for the handling of the information. If you want to enter data at a higher information label, you can use the Change IL item in the Trusted Path menu, which displays a label builder dialog box for entering the new information label. For more information about changing Input IL, see “Change Input IL” on page 85.

13. **Enter some text in the Text Editor and save the file (example shows testfile.1) using the Save option in the File menu (see Figure 3-9).**



This is text at the label: UNCLASSIFIED [C]

Input IL: UNCLASSIFIED Window SL:CONFIDENTIAL

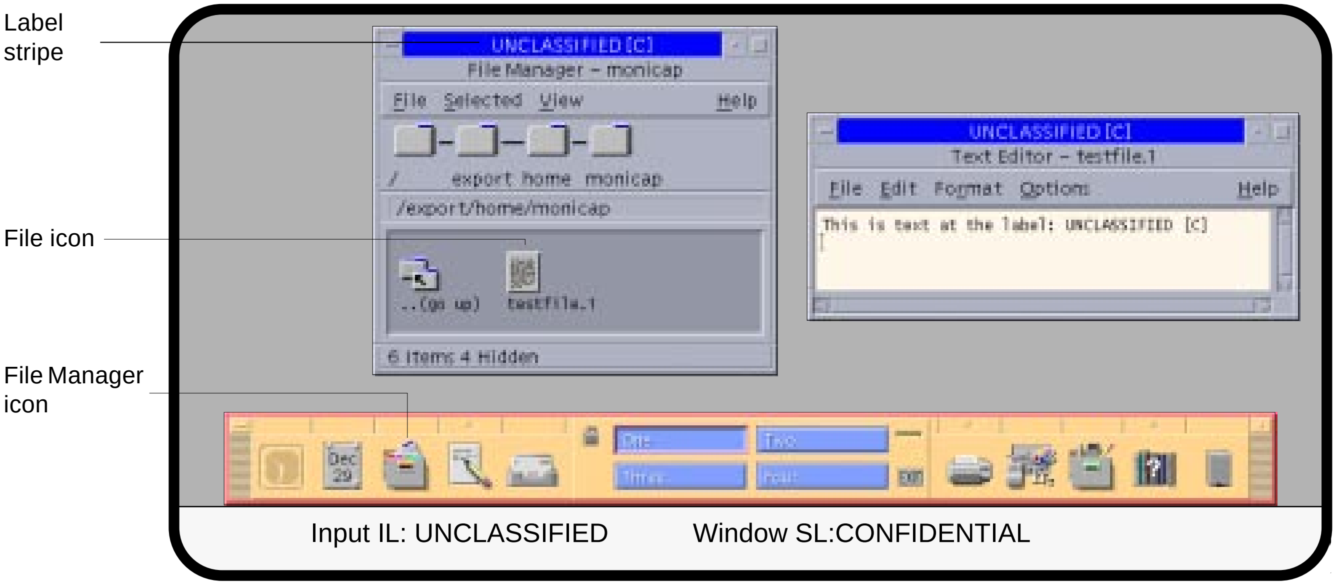
Figure 3-9 Entering Data and Saving a File

When you create a file in a Trusted Solaris session, the file takes on the sensitivity and information labels of the application that creates it (UNCLASSIFIED [C] 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 sensitivity labels dominate the files' sensitivity labels. Files can only be viewed from workspaces or by File Managers that have the same sensitivity label.

14. Click the File Manager icon to launch it (see Figure 3-10).



This is text at the label: UNCLASSIFIED [C]

Input IL: UNCLASSIFIED Window SL:CONFIDENTIAL

Figure 3-10 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 sensitivity label.

As discussed in "Storing Files in Separate Directories by Sensitivity Labels" on page 10, the Trusted Solaris environment provides single-level directories (SLDs) and a multilevel directory (MLD) to separate files and directories at different sensitivity 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 sensitivity label. Figure 3-11 shows the contents of the home directory, which is `testFile.1` at this stage of the example.

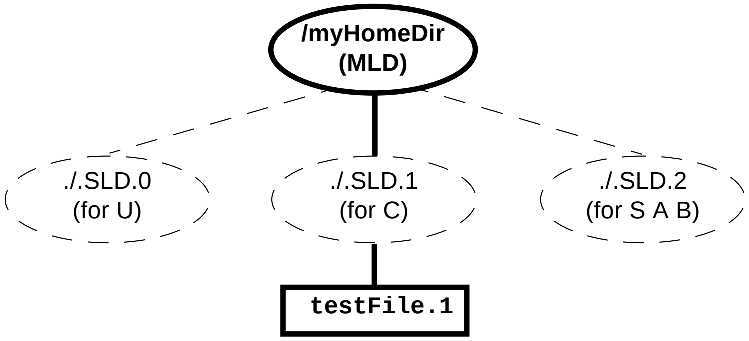
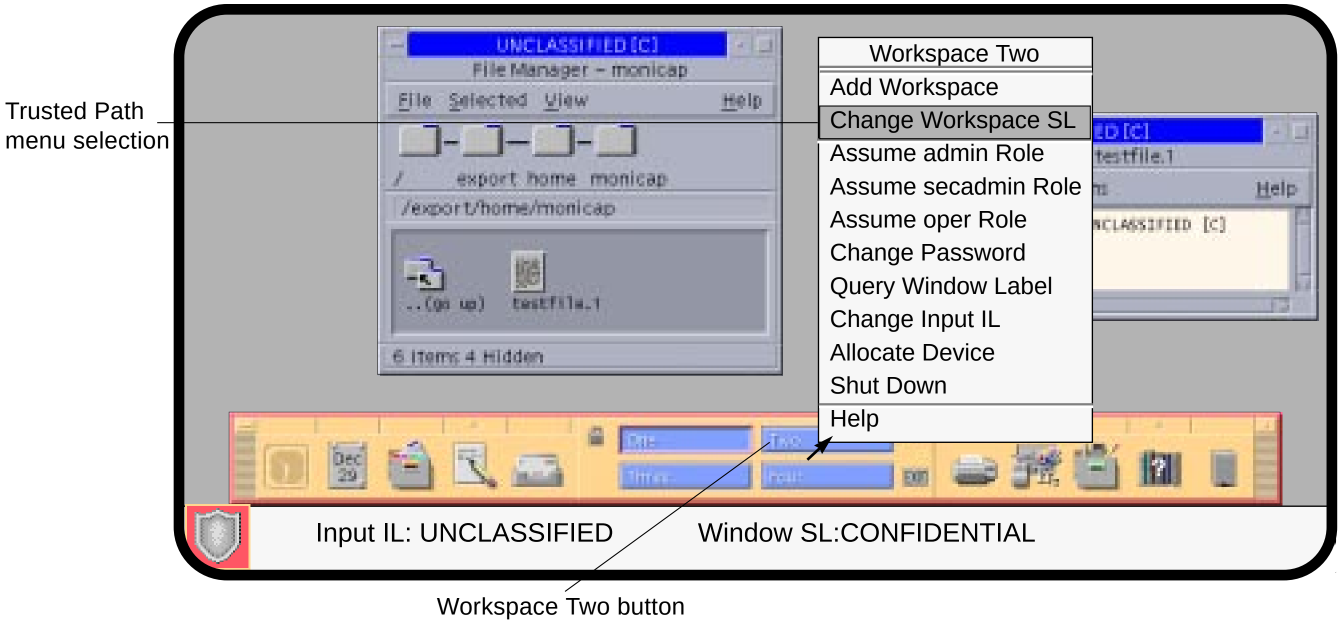


Figure 3-11 Visible and Hidden Files at CONFIDENTIAL Sensitivity Label

Tour: Changing to a Workspace at a Different Sensitivity Label

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

15. **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 SL (see Figure 3-12).**

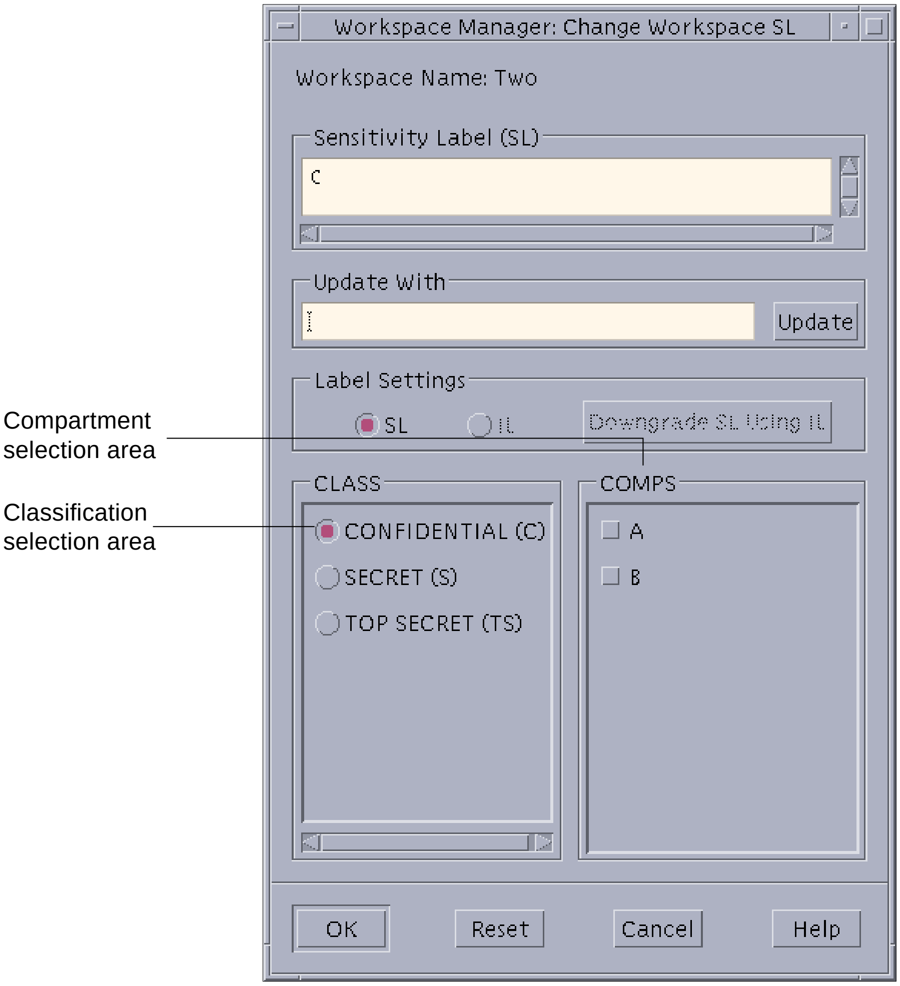


Input IL: UNCLASSIFIED Window SL:CONFIDENTIAL

Figure 3-12 Changing the Workspace Sensitivity Label

This causes a label builder to be displayed in which you specify the new workspace sensitivity label (see Figure 3-13). The trusted path symbol reappears when you display the Trusted Path menu.

16. **Enter a different sensitivity 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.



Workspace Manager: Change Workspace SL

Workspace Name: Two

Sensitivity Label (SL): C

Update With:

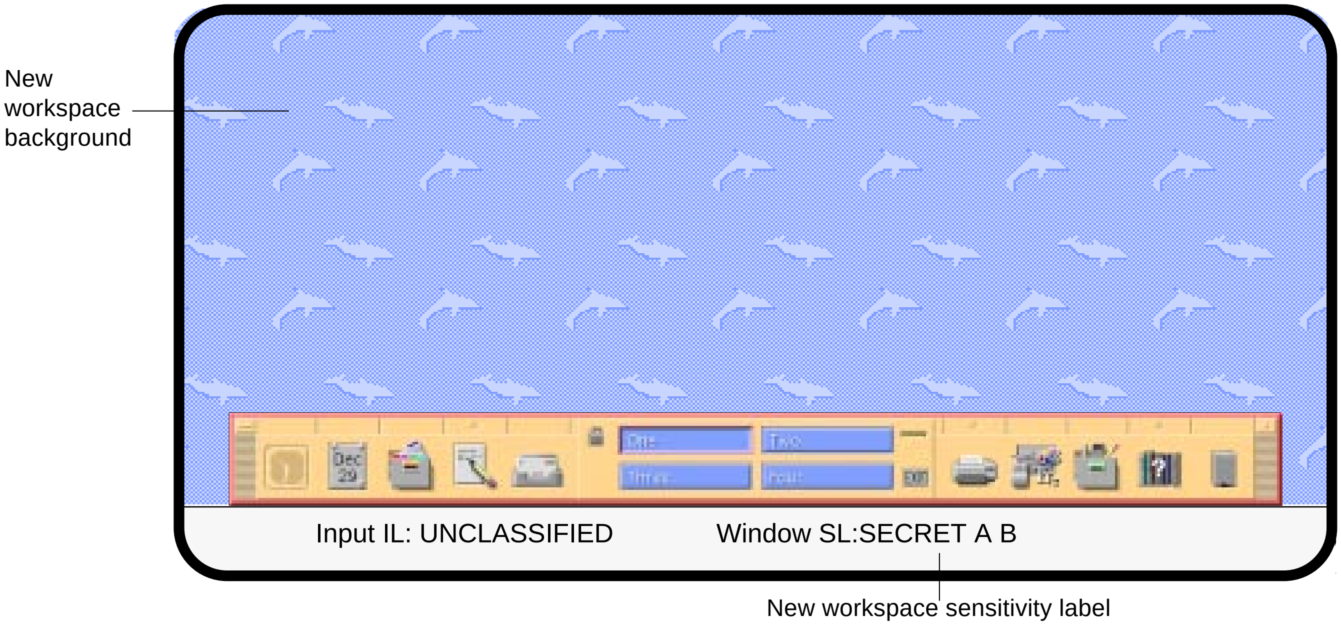
● SL ○ IL

CLASS
- ● CONFIDENTIAL (C)
- ○ SECRET (S)
- ○ TOP SECRET (TS)

COMPS
- □ A
- □ B

Figure 3-13 Workspace Sensitivity Label Builder Dialog Box

After you click OK (or press the Enter or Return key) in the Workspace Sensitivity Label Builder dialog box, the environment switches to the new workspace (see Figure 3-14). The new workspace will have a different background and will indicate the new sensitivity label in the trusted stripe. In addition, your system may be configured to color-code different sensitivity labels, that is, apply the sensitivity label's color to the appropriate workspace button(s), the window SL indicator, and label stripes.



Input IL: UNCLASSIFIED

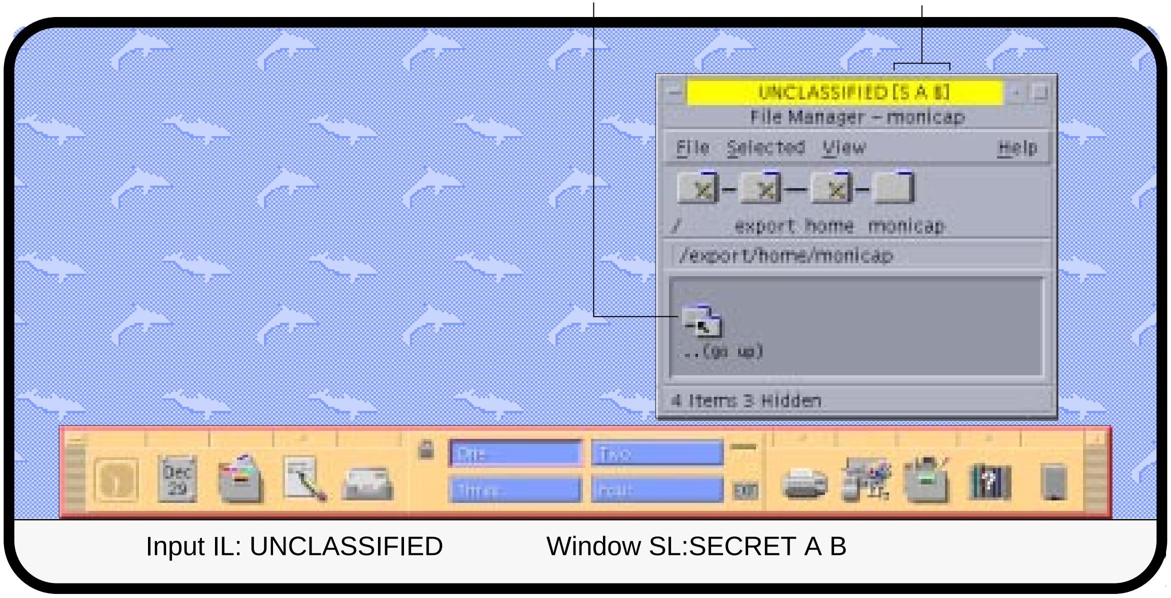
Window SL:SECRET A B

Figure 3-14 Entering a Workspace with a New Sensitivity Label

Tour: Working in a Workspace at a Different Sensitivity Label

A very major difference to note on entering a workspace with a different sensitivity 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.

17. **Click the File Manager icon to view the contents of your home directory (see Figure 3-15).**


Empty home directory

New sensitivity label

Input IL: UNCLASSIFIED

Window SL:SECRET A B

Figure 3-15 Examining Home Directory Contents in a Workspace with a New Sensitivity Label

At this sensitivity level, the file you created in Step 13 is not visible. As shown in Figure 3-16 the file created at the previous sensitivity label cannot be viewed from the workspace at the new sensitivity label.

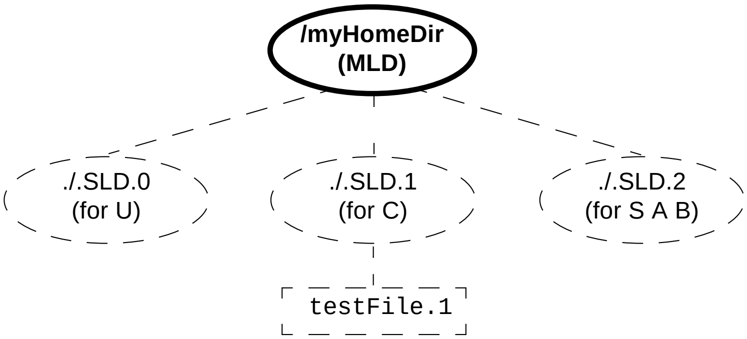
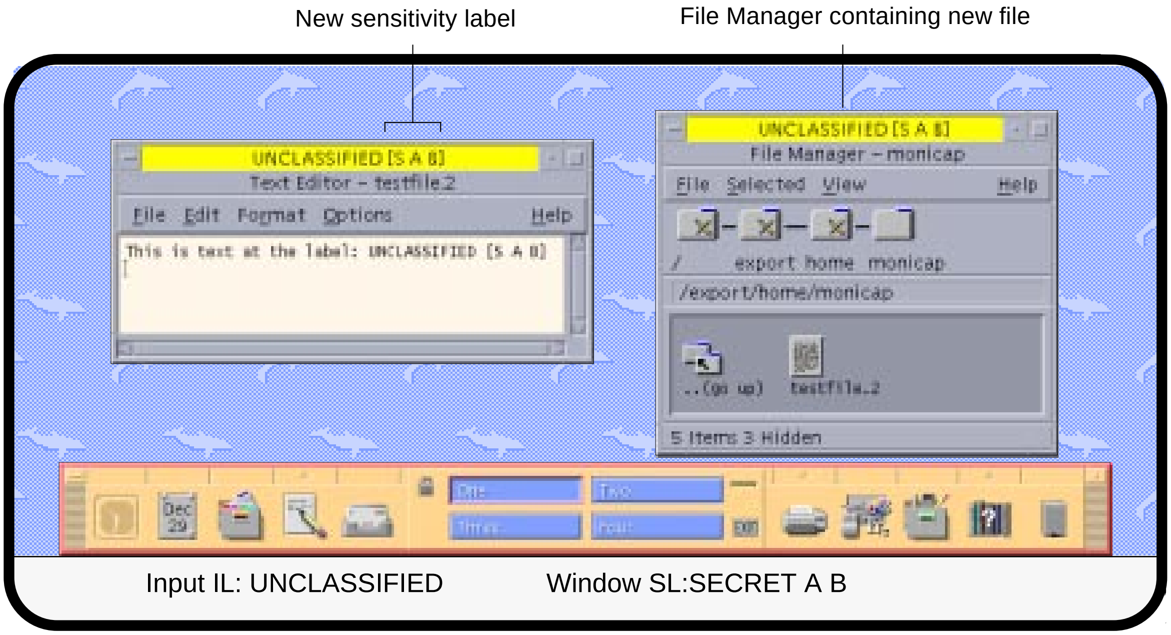


Figure 3-16 Visible and Hidden Files Initially at SECRET A B Sensitivity Label

18. **Create a new file (testfile.2 in example) using the Text Editor as in Step 12 and Step 13 (see Figure 3-17).**
    The new text file has an information label of UNCLASSIFIED and a sensitivity label of SECRET A B.



This is text at the label: UNCLASSIFIED [S A B]

Figure 3-17 Creating a File in a Workspace with a New Sensitivity Label

19. **Use the File Manager to view the contents of the home directory now.** The new file created at SECRET A B (`testFile.2`) is visible and the file created at CONFIDENTIAL (`testFile.1`) cannot be viewed (see Figure 3-18).

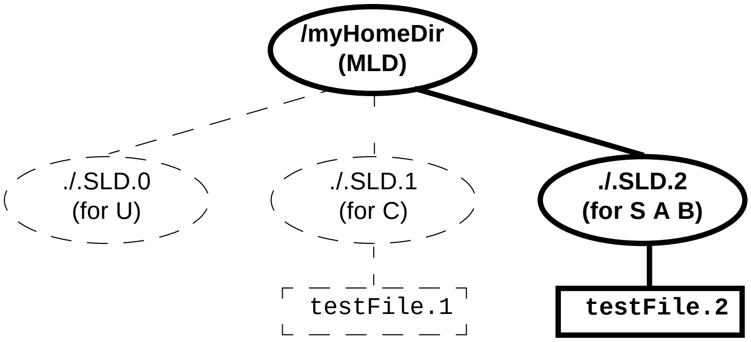
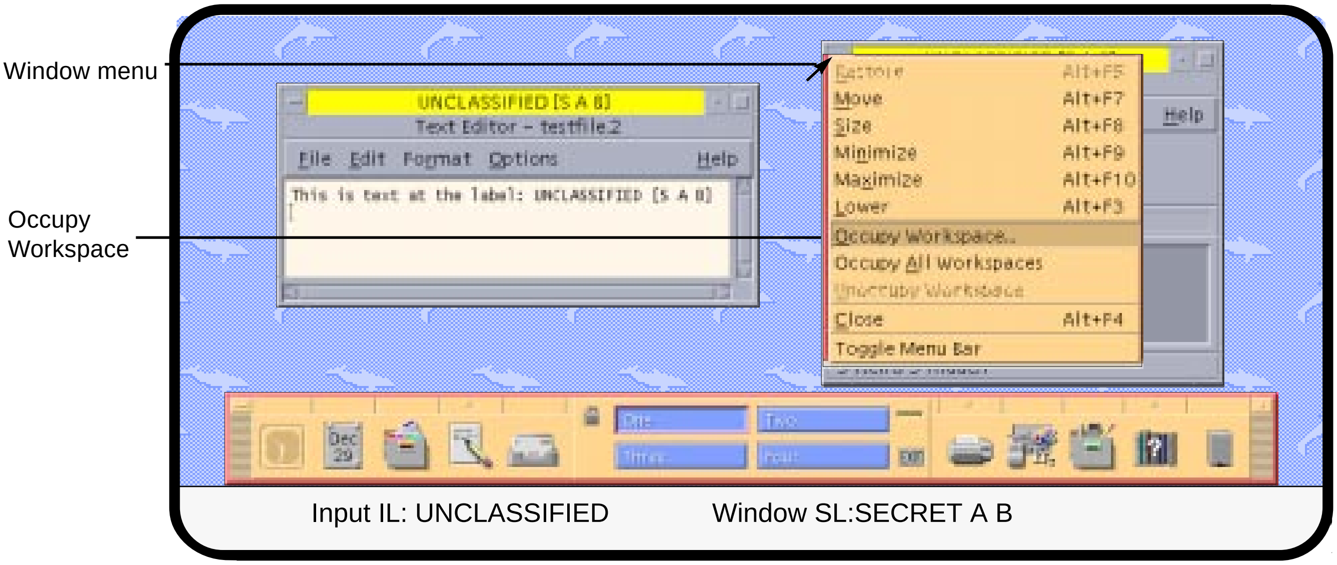


Figure 3-18 Visible and Hidden Files at SECRET A B Sensitivity Label After Creation of New File

Tour: Occupying Workspaces with Applications at Different Sensitivity Labels

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

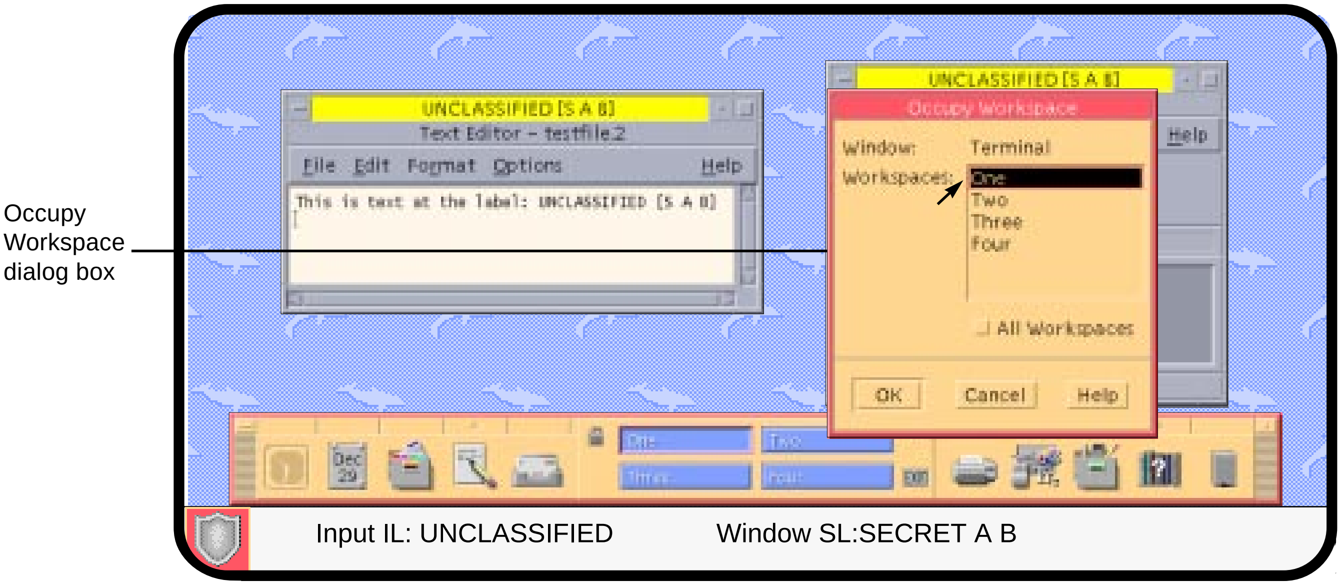
20. **From the window menu in the File Manager, select Occupy Workspace (see Figure 3-19).** This causes the Occupy Workspace dialog box to be displayed (see Figure 3-20).



This is text at the label: UNCLASSIFIED [S A B]

Input IL: UNCLASSIFIED Window SL:SECRET A B

Figure 3-19 Selecting Occupy Workspace



This is text at the label: UNCLASSIFIED [S A B]

Window: Terminal

Workspaces: One

Input IL: UNCLASSIFIED Window SL:SECRET A B

Figure 3-20 Selecting Occupy Workspace

21. **Choose the workspace that you used at the beginning of the tour and click OK.**
    This moves the File Manager running at the current sensitivity 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.

22. **Repeat Step 20 and Step 21 for the Text Editor window.**
    This moves the Text Editor window containing the current file to the previous workspace.

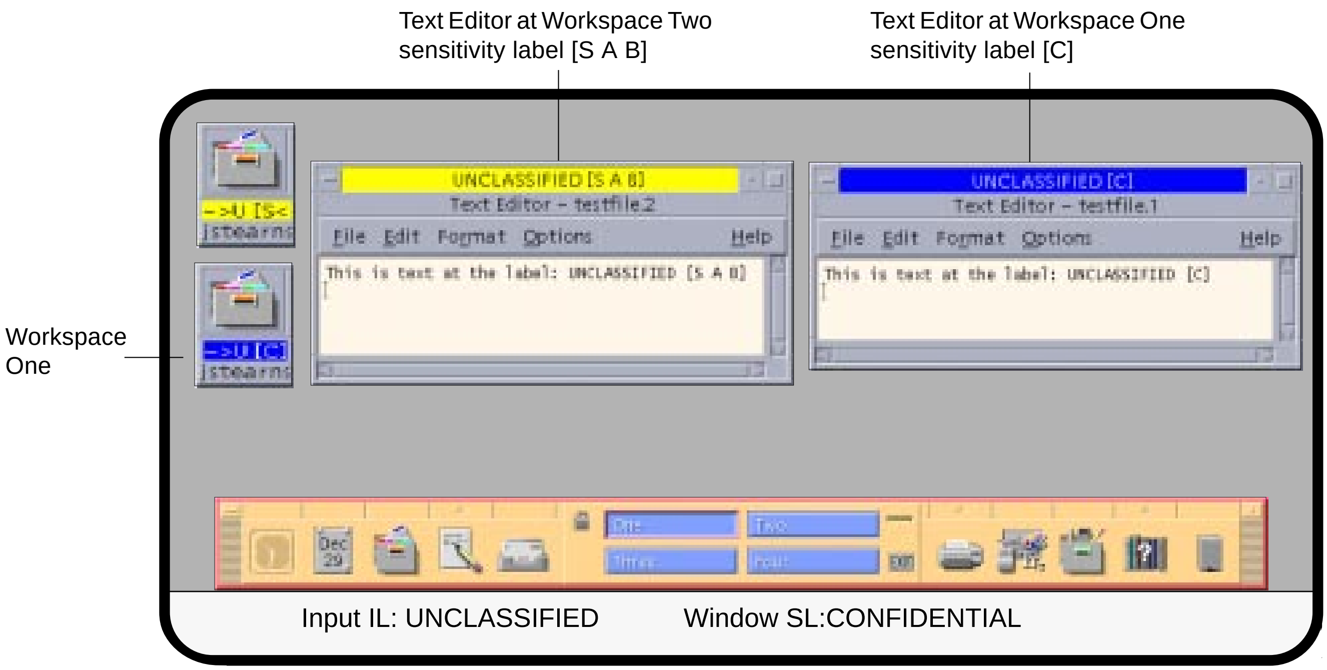
23. **Click the Workspace One button to return to the previous workspace.**
    There should be four windows visible, the Text Editor and File Manager from Workspace One running at UNCLASSIFIED [C] and the Text Editor and File Manager from Workspace Two running at UNCLASSIFIED [S A B].

Tour: Moving Data Between Windows with Different Sensitivity 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 information. If your site's security policy permits this type of transfer, a confirmation dialog box for specifying the information label of the transferred data and confirming the transaction will be displayed; otherwise, the transfer will be prevented.

The preferred method of moving data between windows is to select it with the left mouse button and copy it with the middle mouse button. Although you can do this across workspaces, it is much more convenient if both windows occupy the same workspace.

24. **Minimize the File Manager windows for the time being.**
    The two Text Editor windows should be visible as in Figure 3-21.

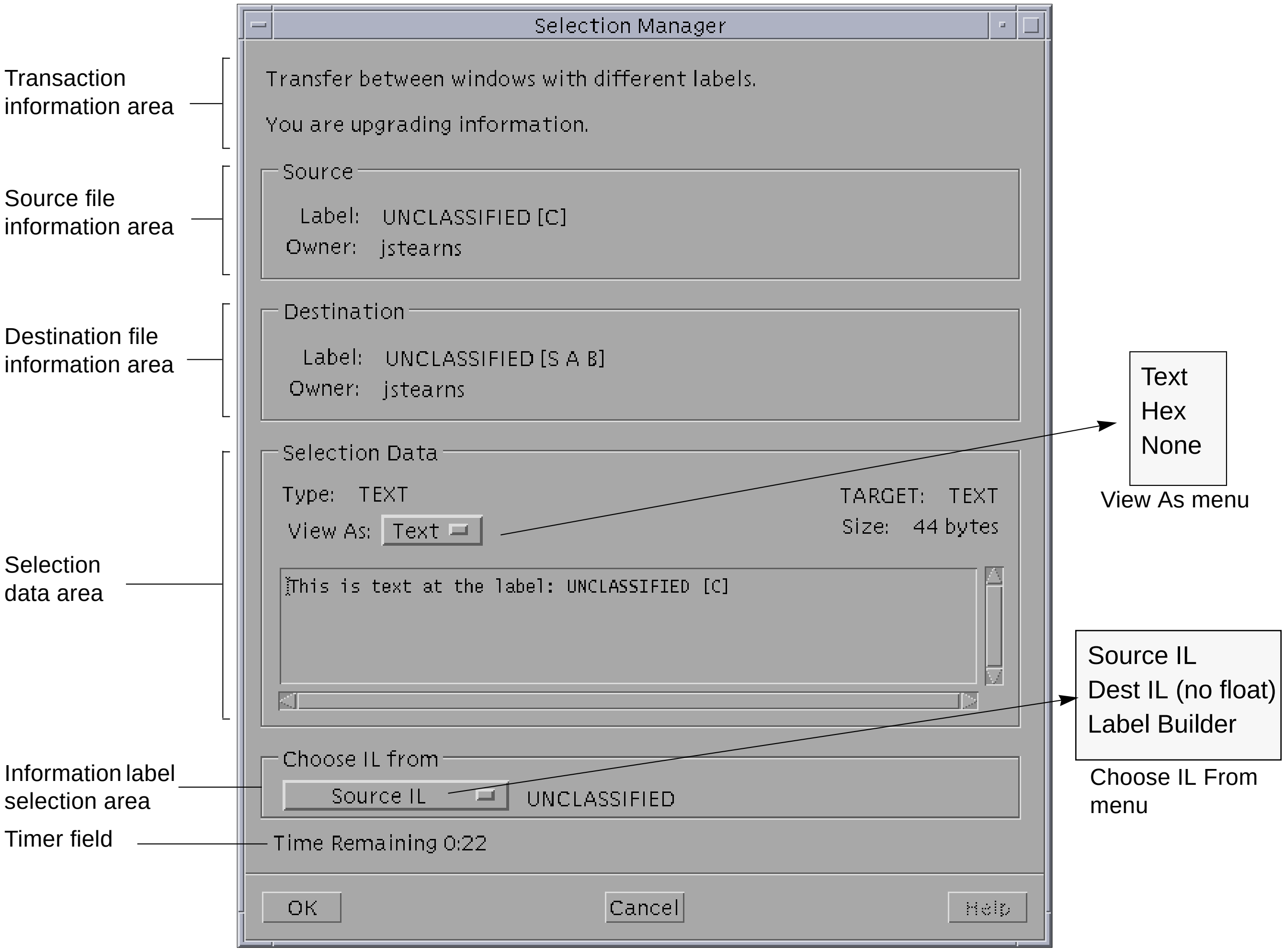


This is text at the label: UNCLASSIFIED [S A B]

This is text at the label: UNCLASSIFIED [C]

Figure 3-21 Displaying Applications at Different Sensitivity Labels

25. **Highlight the text in the UNCLASSIFIED [C] Text Editor window and click the middle mouse button in the UNCLASSIFIED [S A B] to paste the data.**
If this transaction is completed, the sensitivity label of the transferred data will be upgraded and its information label can be set to the level you choose. Before the transfer occurs, the Selection Manager Confirmation dialog box shown in Figure 3-22 is displayed.



Selection Manager

Transfer between windows with different labels.

You are upgrading information.

Source
Label: UNCLASSIFIED [C]
Owner: jstearns

Destination
Label: UNCLASSIFIED [S A B]
Owner: jstearns

Selection Data
Type: TEXT
TARGET: TEXT
View As: Text
Size: 44 bytes

```
This is text at the label: UNCLASSIFIED [C]
```

Choose IL from
Source IL UNCLASSIFIED

Time Remaining 0:22

Figure 3-22 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 information label and sensitivity label in combined form and the owner of the source file.
- **Destination file information area** – identifies the information label, sensitivity 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. Resetting the View As menu affects the displays of subsequent transfers. Choosing None is useful for selections that consist of unreadable data, such as a bitmap.
- **Information label selection area** – lets you specify the information label of the data to be transferred. You select the information label from the Choose IL From menu. The menu choices are: the source information label, the destination information label, or the label builder for setting a different information label. The selected information label is displayed to the right of the menu. If your site is configured to float information labels, the resulting information label will use the highest classification in the transaction and will combine any compartments and markings.
- **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.

26. **Click OK to complete the transfer of the data from the UNCLASSIFIED [C] Text Editor window to the UNCLASSIFIED [S A B] Text Editor window.**
    The transferred data is now in the text file with the label UNCLASSIFIED [S 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 Sensitivity Labels

The Trusted Solaris environment lets you change a file's sensitivity 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 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 sensitivity 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 sensitivity 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 sensitivity 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 sensitivity label from which the file was originally linked to change that file.

27. **Close both Text Editor windows and open the File Manager windows.**
    The file whose sensitivity 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 sensitivity label. At this point, the workspace should appear as shown in Figure 3-23.

File Manager at Workspace One sensitivity label

File Manager at Workspace Two sensitivity label

Workspace One

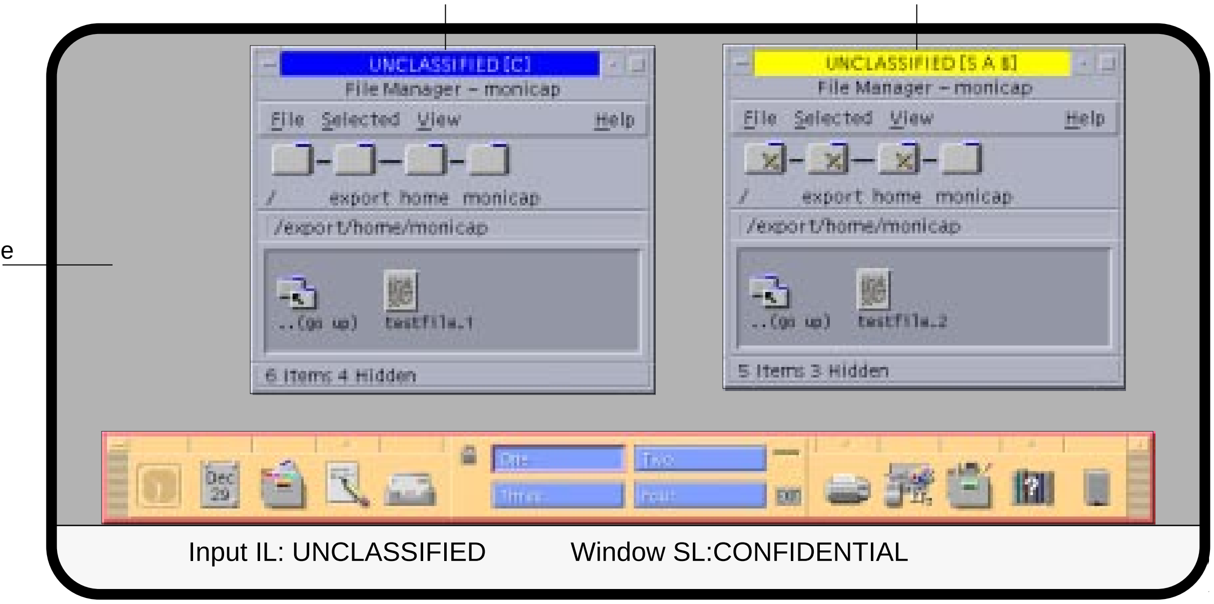
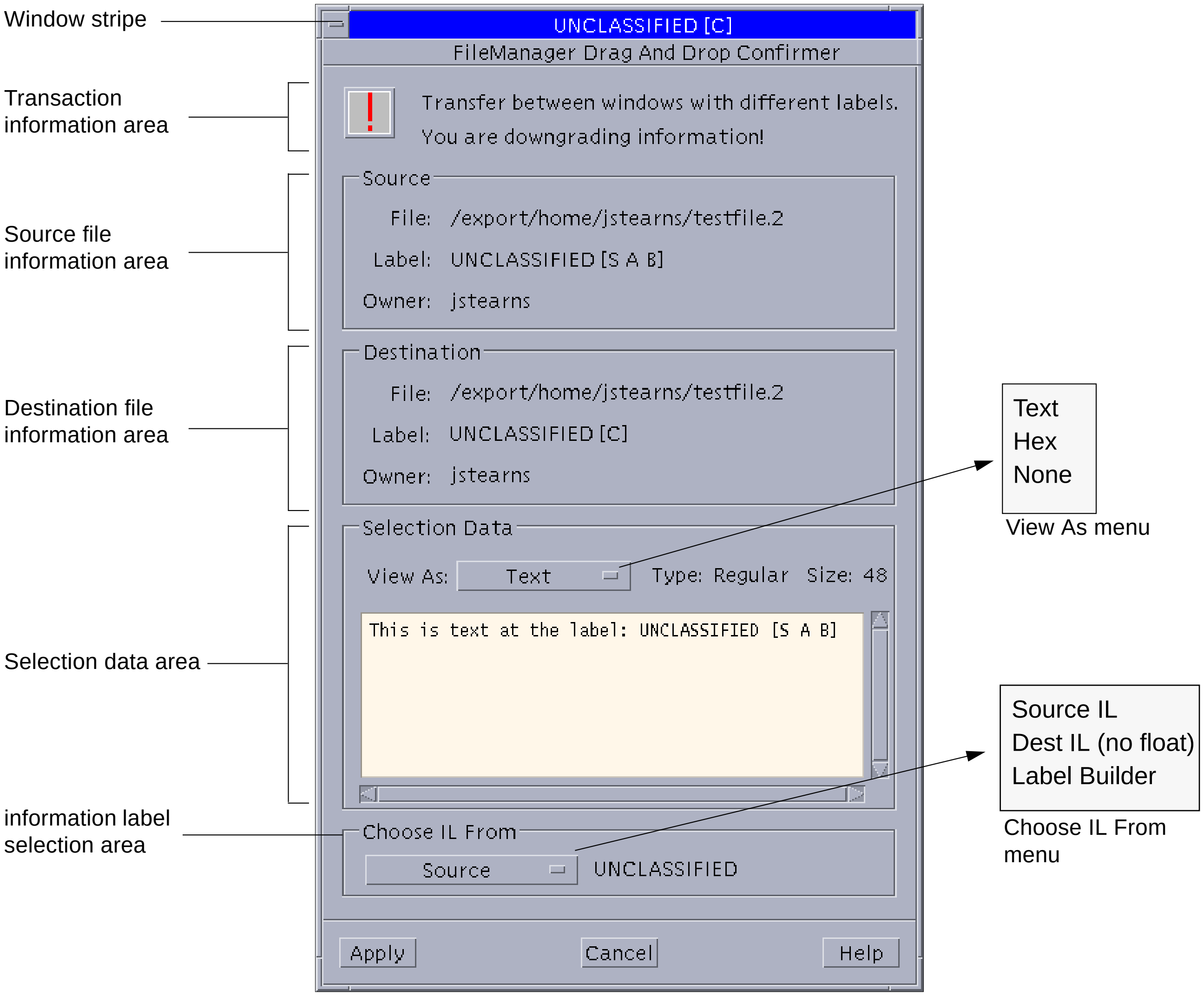


Figure 3-23 Displaying File Managers at Different Sensitivity Labels

28. **Select textfile.2 in the File Manager at UNCLASSIFIED [S A B], drag it to the File Manager at UNCLASSIFIED [C], and drop it.**
    This causes the File Manager Confirmation dialog box in to be displayed (see Figure 3-24).

Note – If your system is not configured to permit upgrading or downgrading sensitivity labels, the dialog box will not be displayed and the icon will reject placement in the second File Manager window.



UNCLASSIFIED [C]

FileManager Drag And Drop Confirmer

Transfer between windows with different labels.
You are downgrading information!

Source

File: /export/home/jstearns/testfile.2
Label: UNCLASSIFIED [S A B]
Owner: jstearns

Destination

File: /export/home/jstearns/testfile.2
Label: UNCLASSIFIED [C]
Owner: jstearns

Selection Data

View As: Text Type: Regular Size: 48

```
This is text at the label: UNCLASSIFIED [S A B]
```

Choose IL From

Source UNCLASSIFIED

Figure 3-24 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** – reflects the label of the destination File Manager (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, the original CMW label, 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 sensitivity label to the single-level directory at the destination sensitivity label.

- **Selection data area** – identifies the type of file selected for the sensitivity label change, how you wish to view it, 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. Resetting the View As menu affects the displays of subsequent transfers. Choosing None is useful for selections that consist of unreadable data.
- **Information label selection area** – lets you specify the information label of the file when its sensitivity label is changed. You select the information label from the Choose IL From menu by selecting the source information label, the destination information label, or the label builder for setting a different information label. The selected information label is displayed to the right of the menu.

29. Click the Apply button in th 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, “Elements of the Trusted Solaris Environment,” for detailed descriptions of the features in the Trusted Solaris environment.

Elements of the Trusted Solaris Environment

4

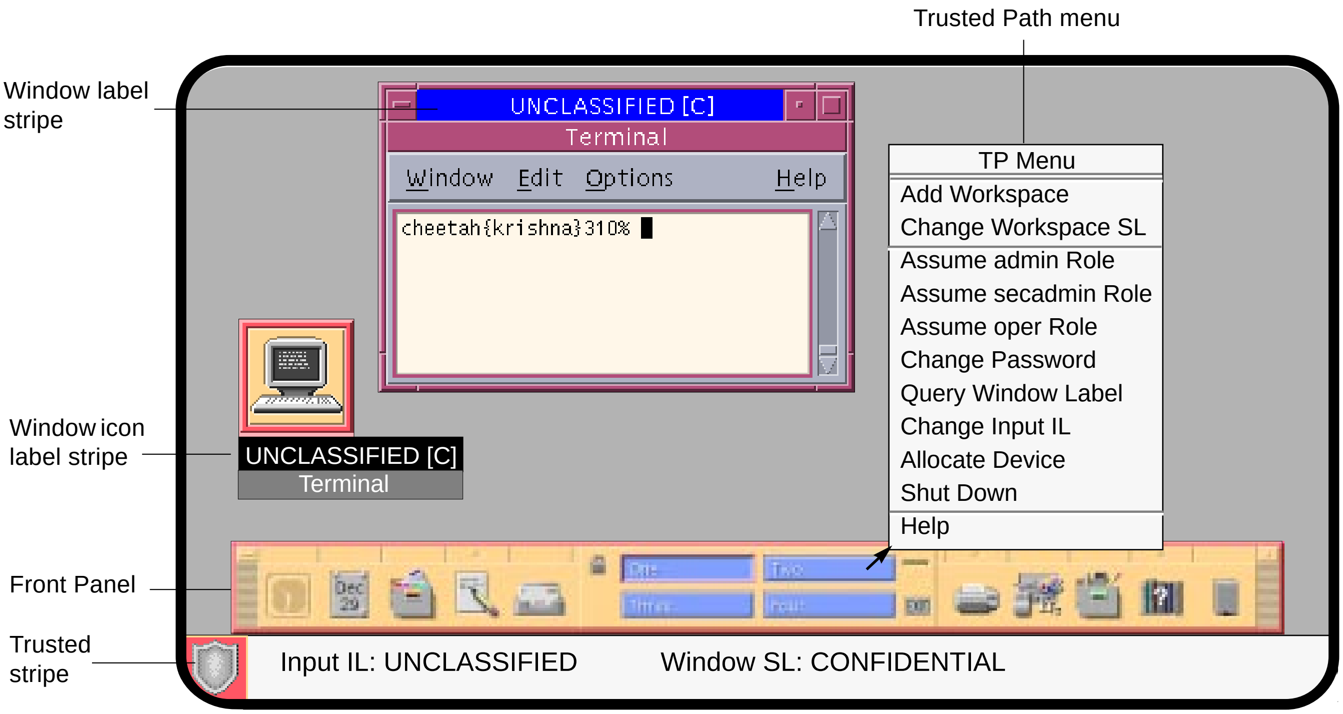
After you have successfully completed the login process, you can work within the Trusted Solaris environment, subject to the restrictions of your clearance, authorizations, and your choice of a single-level or multilevel session. This chapter explains the key elements in the Trusted Solaris environment.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

4

Basic Trusted Solaris Environment

There are four major differences between the Trusted Solaris environment (see Figure 4-1) and the standard Solaris environment:

- **Label displays** – All windows, workspaces, files, and applications have a sensitivity label and optionally an information label 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 environment.
- **Trusted Path menu** – The switch area in the Front Panel lets you access the Trusted Path popup menu for performing security-related tasks.



```
cheetah{krishna}310%
```

Input IL: UNCLASSIFIED   Window SL: CONFIDENTIAL

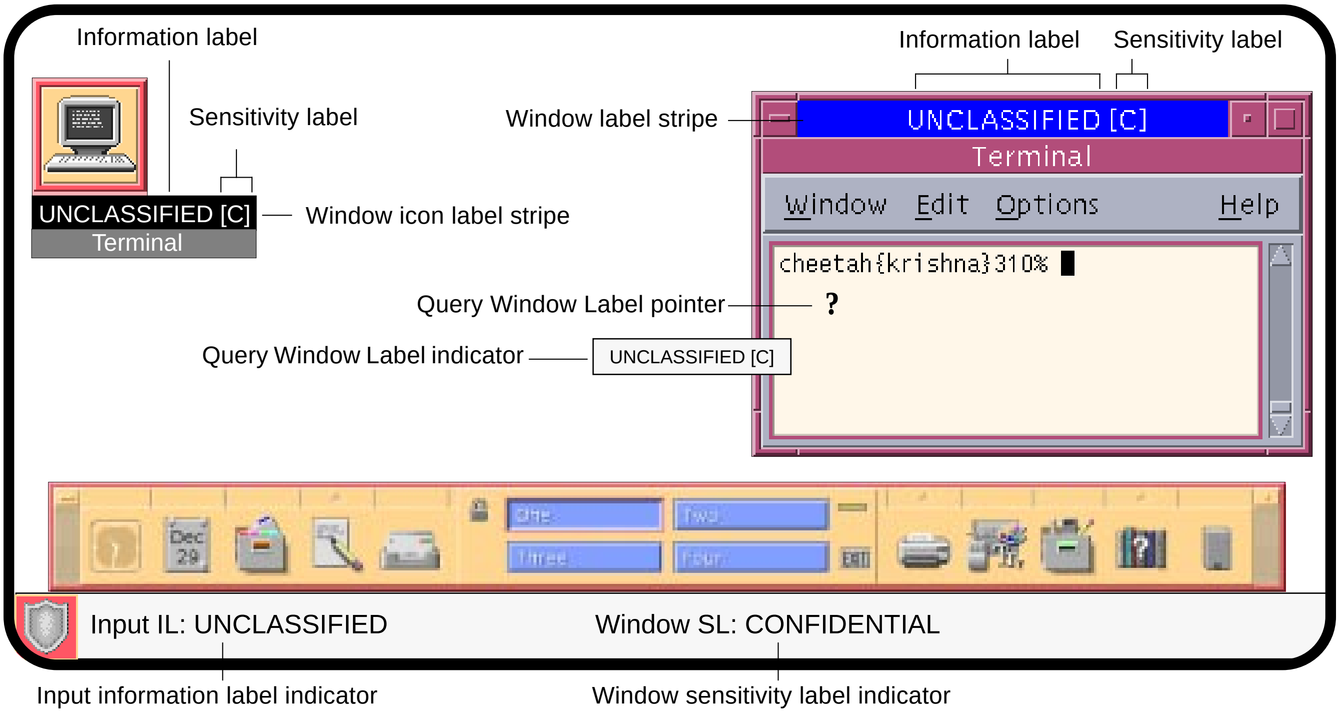
Figure 4-1 Basic Trusted Solaris Environment

Label Displays in the Trusted Solaris Environment

As discussed in “Mandatory Access Control” on page 5, all applications and files in the Trusted Solaris environment have sensitivity labels and potentially information labels 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 Input IL and the Window SL indicators
- **Query window label indicator** – Trusted Path menu operation that displays the label of the window or icon specified by the pointer location

Figure 4-2 shows how labels display in an environment configured to display sensitivity and information labels. It also shows the pointer and indicator when you select Query Window. (When both sensitivity labels and information labels are displayed, the sensitivity labels appear inside square brackets ([]).)



```
cheetah{krishna}310%
```

Figure 4-2 Window Labels in the Trusted Solaris Environment

Different sites have different needs regarding the use and display of labels; the display of labels and the Trusted Stripe is configurable on a site-wide basis. The examples in this manual illustrate a full configuration, that is, both sensitivity labels and information labels are used and displayed. Your Trusted Solaris environment may be configured differently. There are four possible label configurations (see Figure 4-3 through Figure 4-6):

- **Sensitivity labels and information labels displayed** – Both the sensitivity label and the information label are displayed. The information label appears in its long form and the sensitivity label appears in its short form inside square brackets (see Figure 4-3).
- **Sensitivity labels only displayed** – Only sensitivity labels are displayed. They appear in their long form inside square brackets. The Input IL indicator is suppressed from the Trusted Stripe (see Figure 4-4).
- **Information labels only displayed** – Only information labels are displayed. They appear in their long form and the Window SL indicator is suppressed from the Trusted Stripe (see Figure 4-5).
- **Sensitivity labels and information labels suppressed** – Both the sensitivity label and the information label are suppressed. The Trusted Stripe appears as small rectangle in the lower left corner. There are no label stripes or indicators in the Trusted Stripe; the only way to determine labels is by choosing the Query Window Label item in the Trusted Path menu (see Figure 4-6).

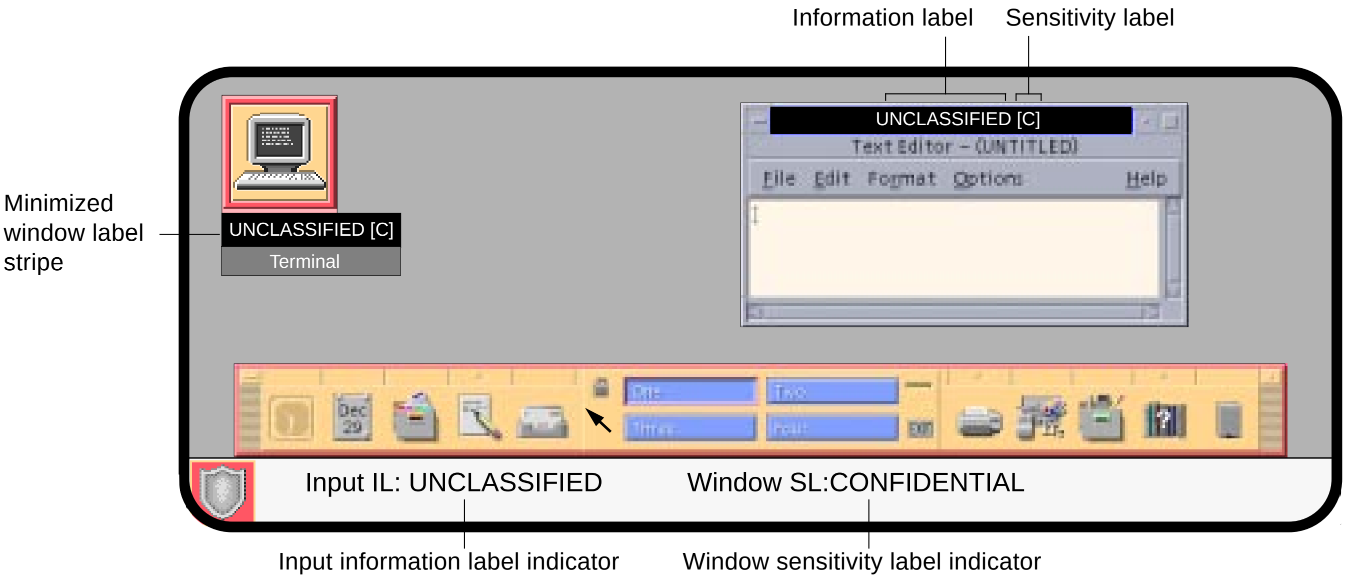


Figure 4-3 Full Trusted Stripe Displaying Information Labels and Sensitivity Labels

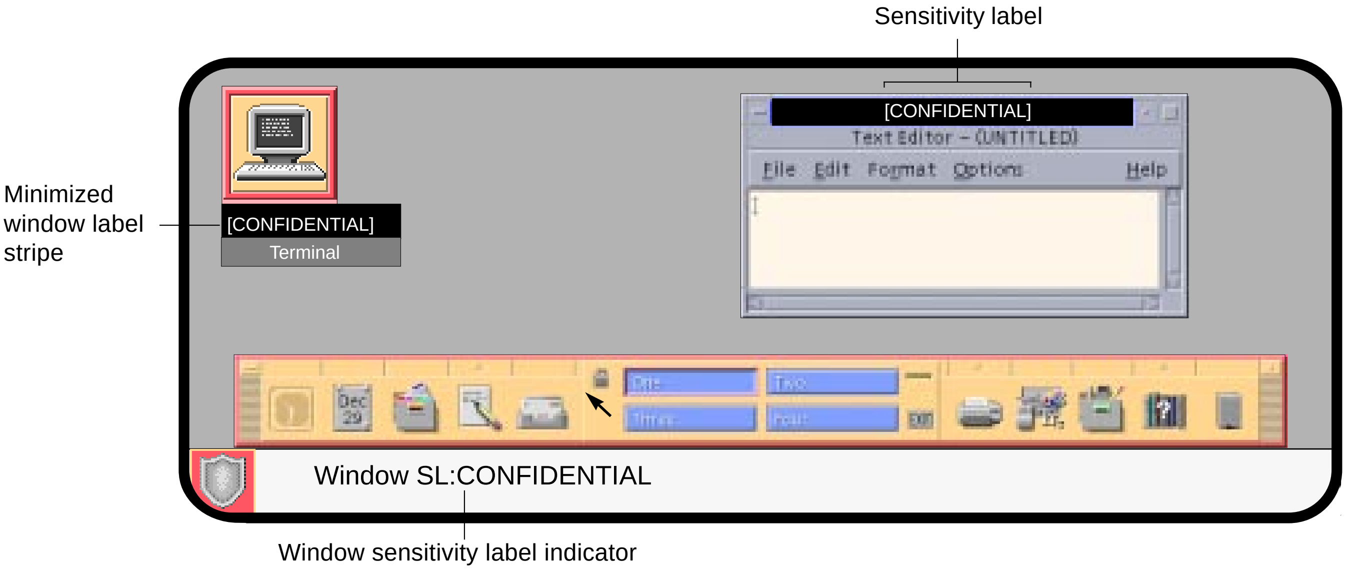


Figure 4-4 Trusted Stripe with Sensitivity Labels Only Displayed

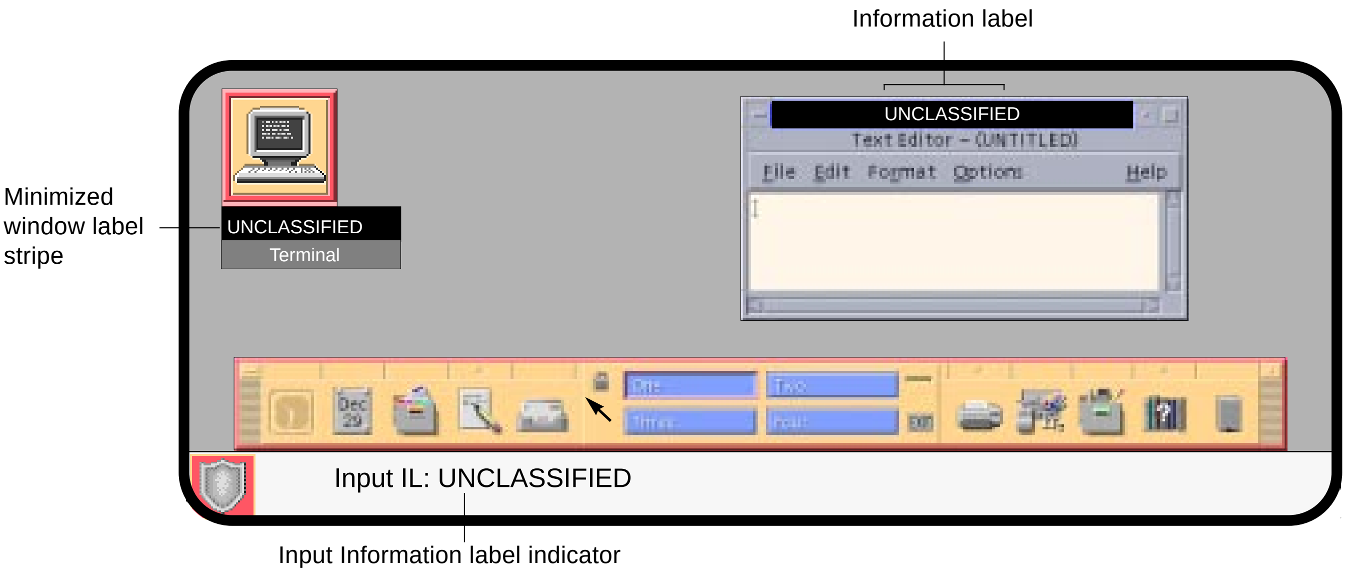


Figure 4-5 Trusted Stripe with Information Labels Only Displayed

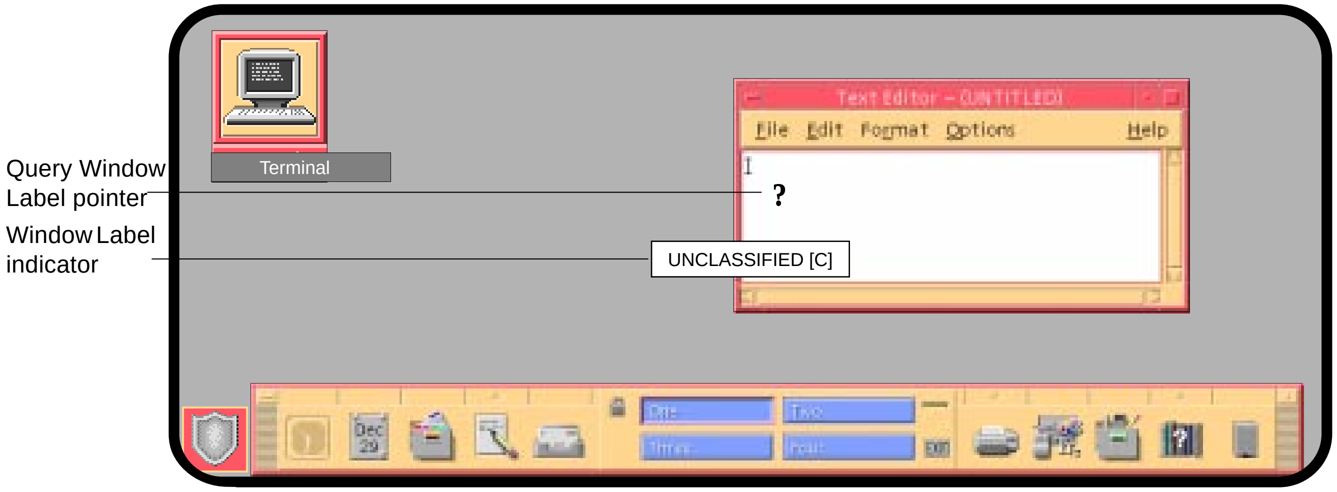


Figure 4-6 Trusted Stripe with Information Labels and Sensitivity Labels Suppressed

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 three elements of the trusted stripe (depending on your site configuration):

- The trusted path symbol is required.
- The Input IL is optional.
- The Window SL is optional.

Figure 4-3 through Figure 4-6 show the four ways in which the trusted stripe can be configured.

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 both the Input IL and Window SL, then the trusted path symbol appears with the trusted stripe to the left of the Front Panel as shown in Figure 4-7.) 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.

Window SL Field

The *Window SL* field displays the sensitivity label of the active window (that is the window that has the pointer focus). If you are working at one sensitivity label at a time, this may be stating the obvious. However, in a multilevel session, it is possible to have windows with different sensitivity labels in the same workspace. For an example, see “Tour: Occupying Workspaces with Applications at Different Sensitivity Labels” on page 53.

Input IL Field

The *Input IL* field indicates the information label to be applied to data you enter into the active window, either from the keyboard or from mouse-button events. The Input IL is initially set to the lowest information label in your organization, UNCLASSIFIED, for example. You can raise the Input IL up to the sensitivity label of your current workspace, including any valid markings. For more information on changing Input IL, see “Change Input IL” on page 85.

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 in your environment. The major operational difference is that clicking the right mouse button anywhere in the switch area causes a special pop-up menu called the Trusted Path (TP) menu to be displayed. Figure 4-7 shows the Trusted Solaris front panel and identifies the elements that are different in the Trusted Solaris environment.

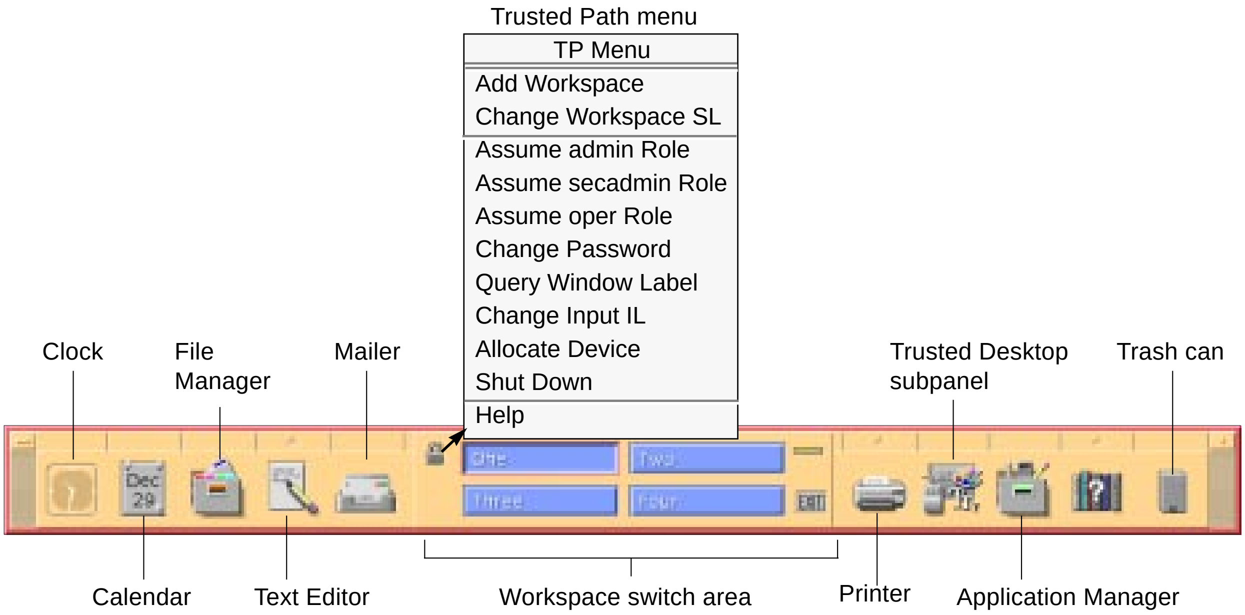


Figure 4-7 Trusted Solaris Front Panel

Workspace Switch Area

In the Trusted Solaris environment, the workspace buttons not only define separate workspaces but let you work at different sensitivity labels if you are conducting a multilevel session (in a single-level session, you can only operate at one sensitivity label). When you begin a multilevel session, each workspace is set to the lowest sensitivity 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 sensitivity label, you click the right mouse button over the workspace button and select Change Workspace SL. This causes a label builder to be displayed in which you enter the new sensitivity label. You can then click the workspace button to work at the new sensitivity label. Note that the Occupy Workspace and Occupy All Workspaces selections in the window menus let you display windows with different sensitivity labels on the screen at the same time.

Clock

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

Calendar

The calendar shows the appointments for you at the sensitivity label of your current workspace only. To view appointments at a different sensitivity label, you need to change to a workspace at that sensitivity 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 sensitivity label of the current workspace. To operate on (or view) files at more than one sensitivity label at a time, you run the File Manager from workspaces at the different sensitivity 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 sensitivity labels. For more information on the File Manager and its capabilities, see Chapter 5, "Managing Files and Directories.

You can view (but not write to) files and directories that are not at your current workspace sensitivity 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 sensitivity label.

Text Editor

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

Mailer

In the Trusted Solaris environment, the Mailer sorts incoming mail by sensitivity label and displays separate mail notifier icons in its subpanel for each valid sensitivity label in your account range and for each role that you are allowed to assume (see Figure 4-8). This feature lets you focus on important mail at higher labels and defer reading more general mail at the UNCLASSIFIED label. The Mailer operates at one sensitivity label at a time only. Clicking the Mailer icon in the Front Panel opens the Mailer at the sensitivity label of the current workspace; clicking a Mailer icon with a label in the subpanel opens the Mailer at that sensitivity label.

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-sensitivity label feature.

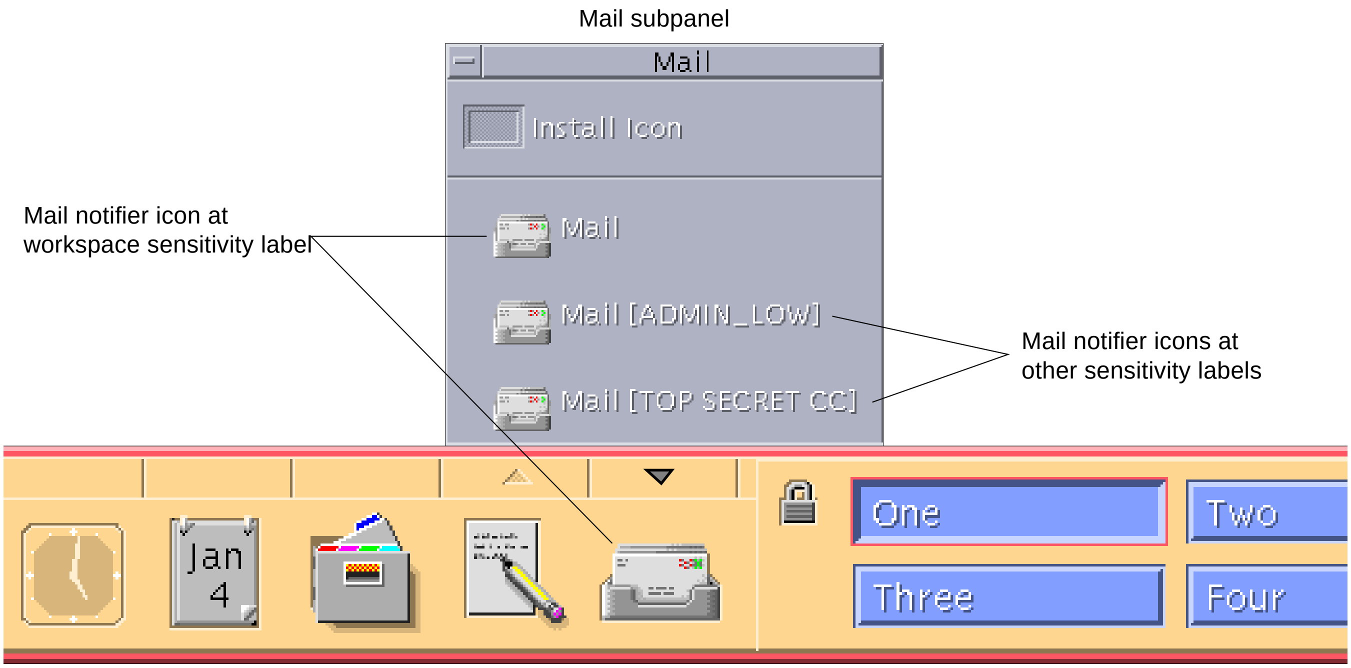

Mail subpanel
Mail
Install Icon
Mail
Mail [ADMIN_LOW]
Mail [TOP SECRET CC]
Mail notifier icon at workspace sensitivity label
Mail notifier icons at other sensitivity labels
Jan 4
One
Two
Three
Four

Figure 4-8 Mail Notifier Icons in the Mail Subpanel

Printer

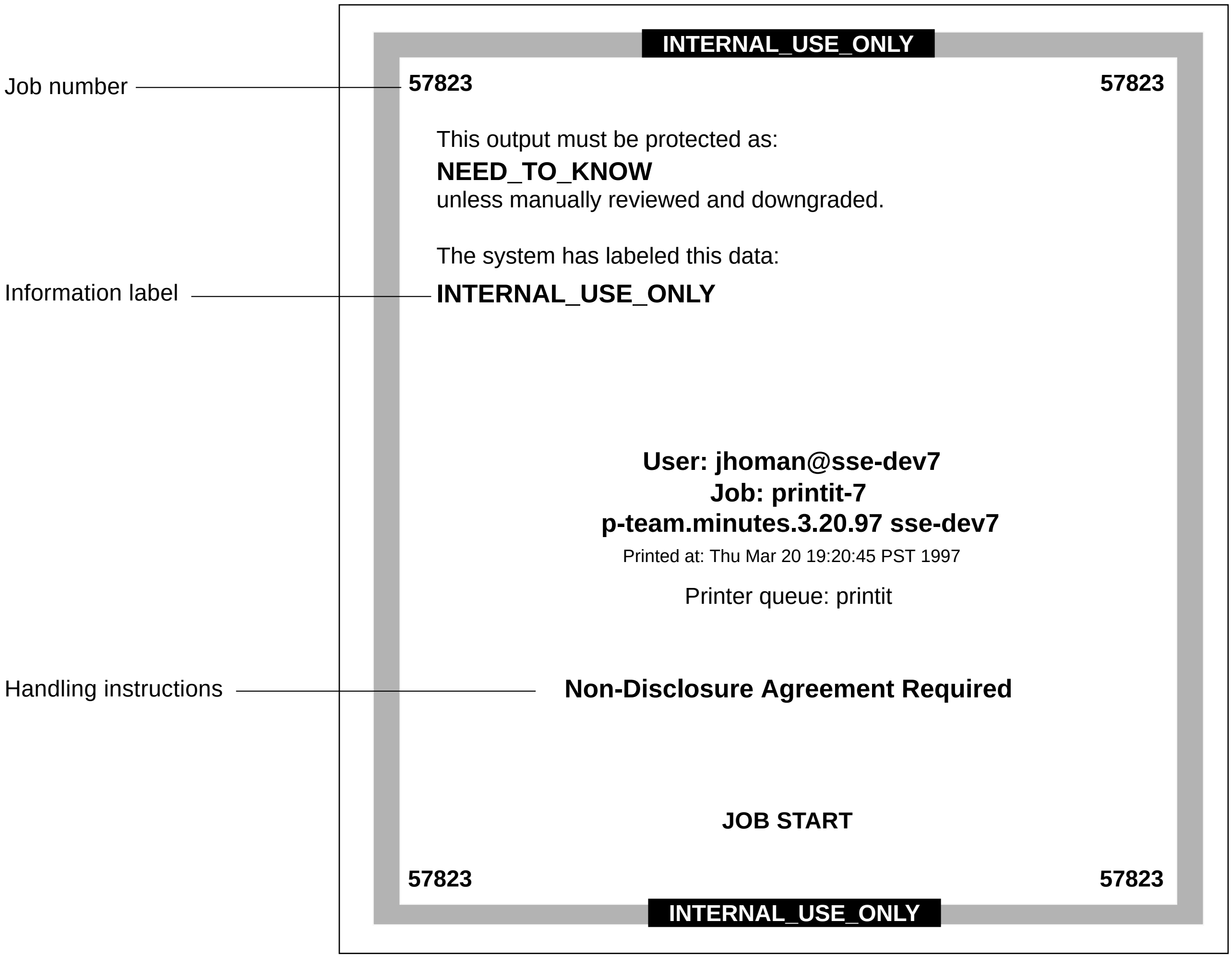
The Printer subpanel displays icons for all printers accredited up to your clearance. However, you can use only those printers accredited to print documents at the sensitivity label of the current workspace.

A typical printer configuration includes:

- banner page at the beginning of the print job – identifying the print job, handling instructions and labels appropriate to the site
- labelled 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 Figure 4-9. It has been configured to print the information label on a gray border. The words “JOB START” indicate the banner page.

For the exact security information for your site, please see your administrator.


Job number
Information label
Handling instructions

INTERNAL_USE_ONLY

57823 57823

This output must be protected as:
NEED_TO_KNOW
unless manually reviewed and downgraded.

The system has labeled this data:
INTERNAL_USE_ONLY

User: jhoman@sse-dev7
Job: printit-7
p-team.minutes.3.20.97 sse-dev7
Printed at: Thu Mar 20 19:20:45 PST 1997

Printer queue: printit

Non-Disclosure Agreement Required

JOB START

57823 57823

INTERNAL_USE_ONLY

Figure 4-9 Typical Print Banner Page

Trusted Desktop Subpanel

The Trusted Desktop subpanel provides access to the Desktop Style Manager and the Device Manager (see "Allocate Device" on page 88).

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 sensitivity label or clearance that you specify at login. Thus, you can have a different session defined for each sensitivity label in your account sensitivity 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 sensitivity 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 sensitivity label. Although you can drop files at any sensitivity label in the trash can, it displays files at the current sensitivity 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 is displayed with a different set of selections and title depending on the location of the pointer as follows:

- **Over a workspace button** – core entries and Change Workspace SL, Add Workspace, Delete, and Rename for operating on that workspace (see Figure 4-10)
- **Over an area with no controls** – core entries and Add Workspace
- **Over the Exit icon** – core entries and ExitSession for logging out
- **Over the Lock icon** – core entries and Lock Display

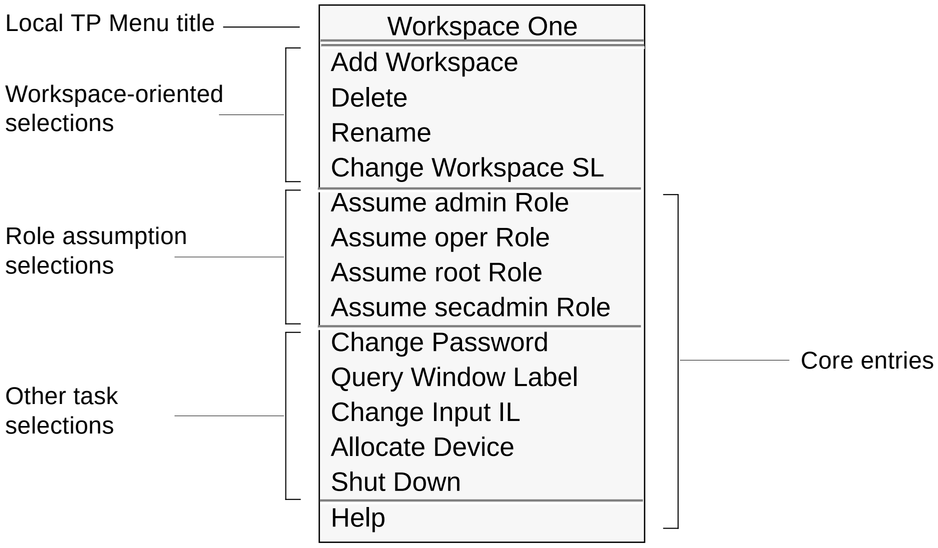


Figure 4-10 The Workspace Version of the Trusted Path Menu

As shown in the left side of the figure, the Trusted Menu selections fall into three major categories:

- workspace-oriented selections
- role assumption selections
- other task selections

The right side of the figure shows the core selections common to all TP menus. Note also that your system may have different selections available due to configuration differences.

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 the current workspace.

Delete

Delete lets you remove a workspace from the switch area just as in standard Solaris CDE. It is good practice to close 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 SL

Change Workspace SL lets you change the sensitivity label of a workspace to any sensitivity label between the minimum sensitivity label assigned to you and your current session clearance (for multilabel sessions only). When you click on the changed workspace button, you enter a session at the new sensitivity label.

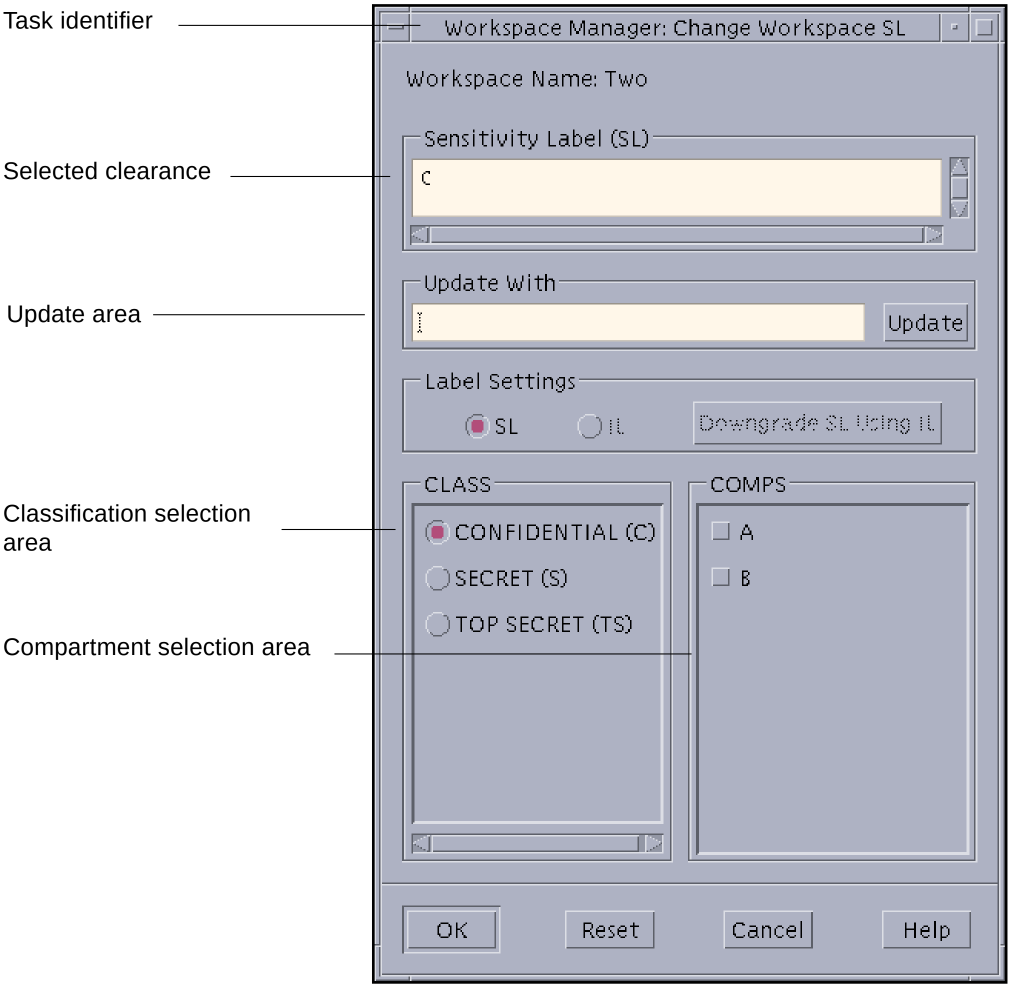
▼ To Change a Workspace Sensitivity Label

1. **Select Change Workspace SL from the Trusted Path menu.**
   The dialog box shown in Figure 4-11 is displayed.

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 sensitivity label you have built in the update area. Click the OK button if it is correct or go back to step 2 to build a different sensitivity label.**



Workspace Manager: Change Workspace SL

Workspace Name: Two

Sensitivity Label (SL): C

Update With:

Label Settings: ● SL ○ IL

CLASS: ● CONFIDENTIAL (C) ○ SECRET (S) ○ TOP SECRET (TS)

COMPS: □ A □ B

Figure 4-11 Change Workspace SL Dialog Box

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 you do not need 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 your password. After successfully entering your 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.

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 (see Figure 4-12).**
   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.

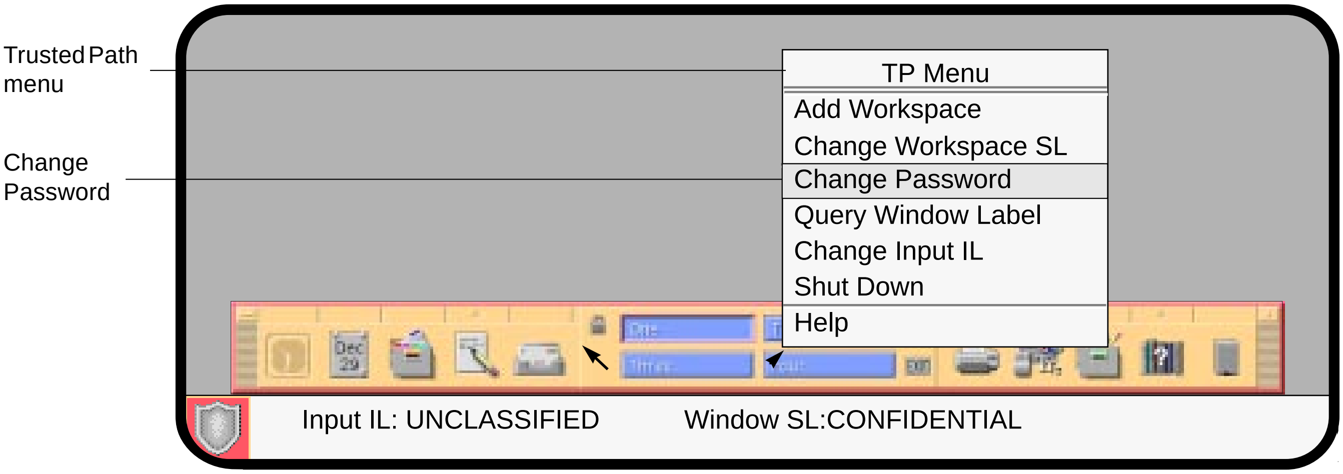
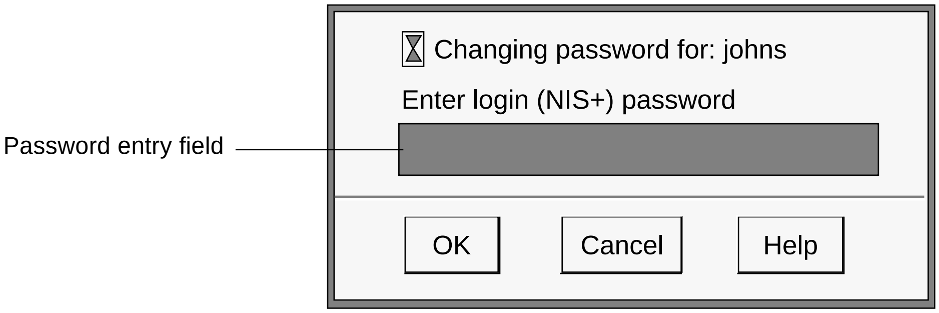


Figure 4-12 Selecting Change Password from the Trusted Path Menu

2. **Choose a new password.**
   It must meet the following criteria:

   - The password must be between 6 and 8 characters in length. (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.)

3. **Type the new password in the Change Password dialog box and click OK (see Figure 4-13).**
   For the sake of security, the password is not displayed as you type it.



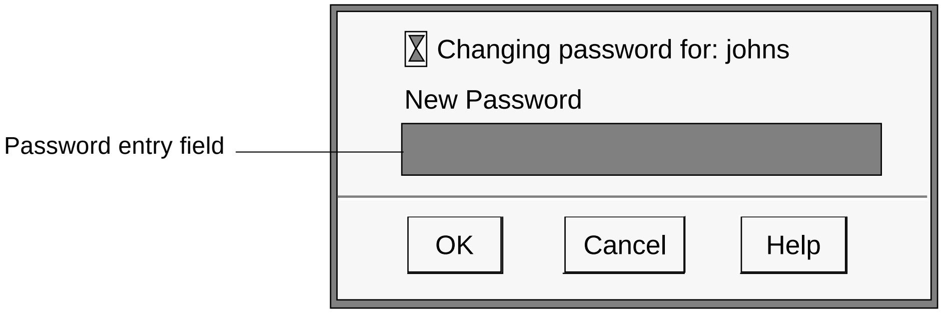
Changing password for: johns

Enter login (NIS+) password

Password entry field

Figure 4-13 Change Password Dialog Box

4. **Type the new password in the Change Password Confirmation dialog box and click OK (see Figure 4-14).**
   This step confirms your choice.



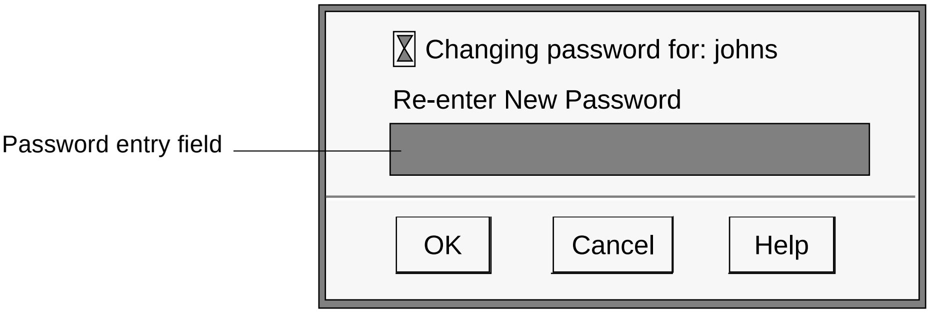
Changing password for: johns

New Password

Password entry field

Figure 4-14 Change Password Confirmation Dialog Box

5. **Type the new password in the Change Password Reconfirmation dialog box and click OK (see Figure 4-15).**
   This step is the final confirmation of your choice.



Changing password for: johns

Re-enter New Password

Figure 4-15 Change Password Reconfirmation Dialog Box

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

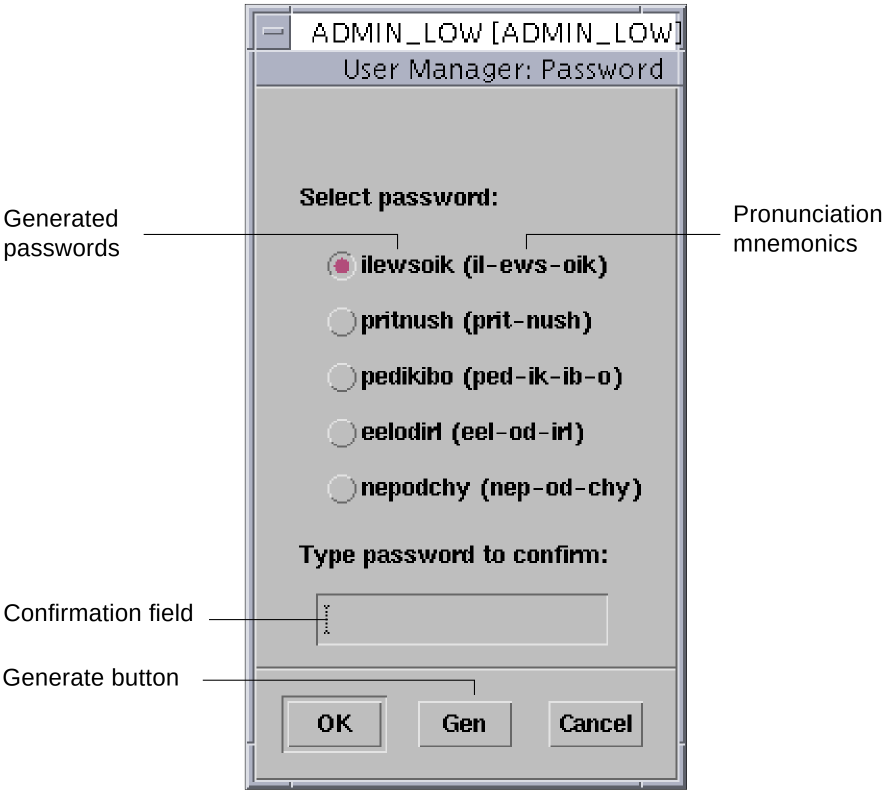
Your administrator has the option to require users to select new passwords from lists of system-generated passwords. Trusted Solaris generates passwords that are pronounceable but difficult for intruders to guess.

1. **Select Change Password from the Trusted Path menu.**
   If your system is configured for system-generated entry, a dialog box similar to the one shown in Figure 4-16 is displayed. 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.

2. **Click the radio button to the left of the password you wish to select or click the Generate button to get five new choices.**

3. **Type the selected password in the confirmation field.**
   This step confirms your choice and gives you practice at entering it.

4. **Click OK (or press Enter) to set your password.**
   This step establishes your choice and closes the dialog box.



ADMIN_LOW [ADMIN_LOW]

User Manager: Password

Select password:

● ilevsoik (il-evs-oik)

○ pritnush (prit-nush)

○ pedikibo (ped-ik-ib-o)

○ eelodirl (eel-od-irl)

○ nepodchy (nep-od-chy)

Type password to confirm:

Generated passwords

Pronunciation mnemonics

Confirmation field

Generate button

Figure 4-16 Password Generator Dialog Box

Query Window Label

Query Window Label changes the pointer to a question mark. As you move the pointer around the screen, the sensitivity label for the region under the pointer is displayed in a small rectangular box at the center of the screen (see Figure 4-17). 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.

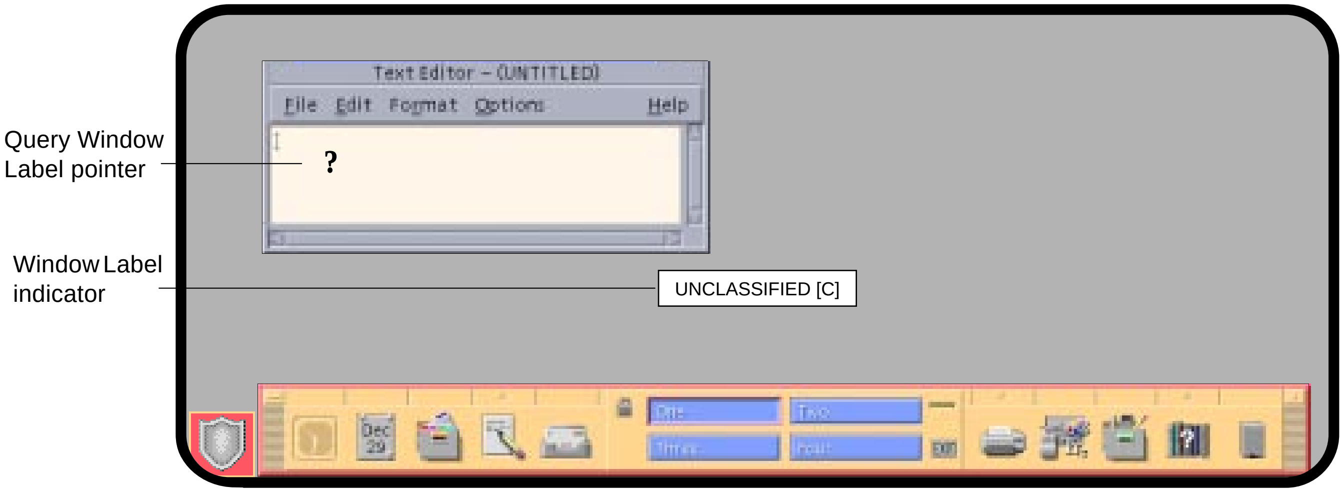


Figure 4-17 Query Window Label Operation

Change Input IL

Change Input IL lets you change the input information label of a window. The *input information label* is applied to data you enter from the keyboard or from similar input devices into the window currently containing the pointer. You can change the information label to any value between the minimum information label at your site and the sensitivity label you are currently working at, including any markings.

▼ To Change Input IL

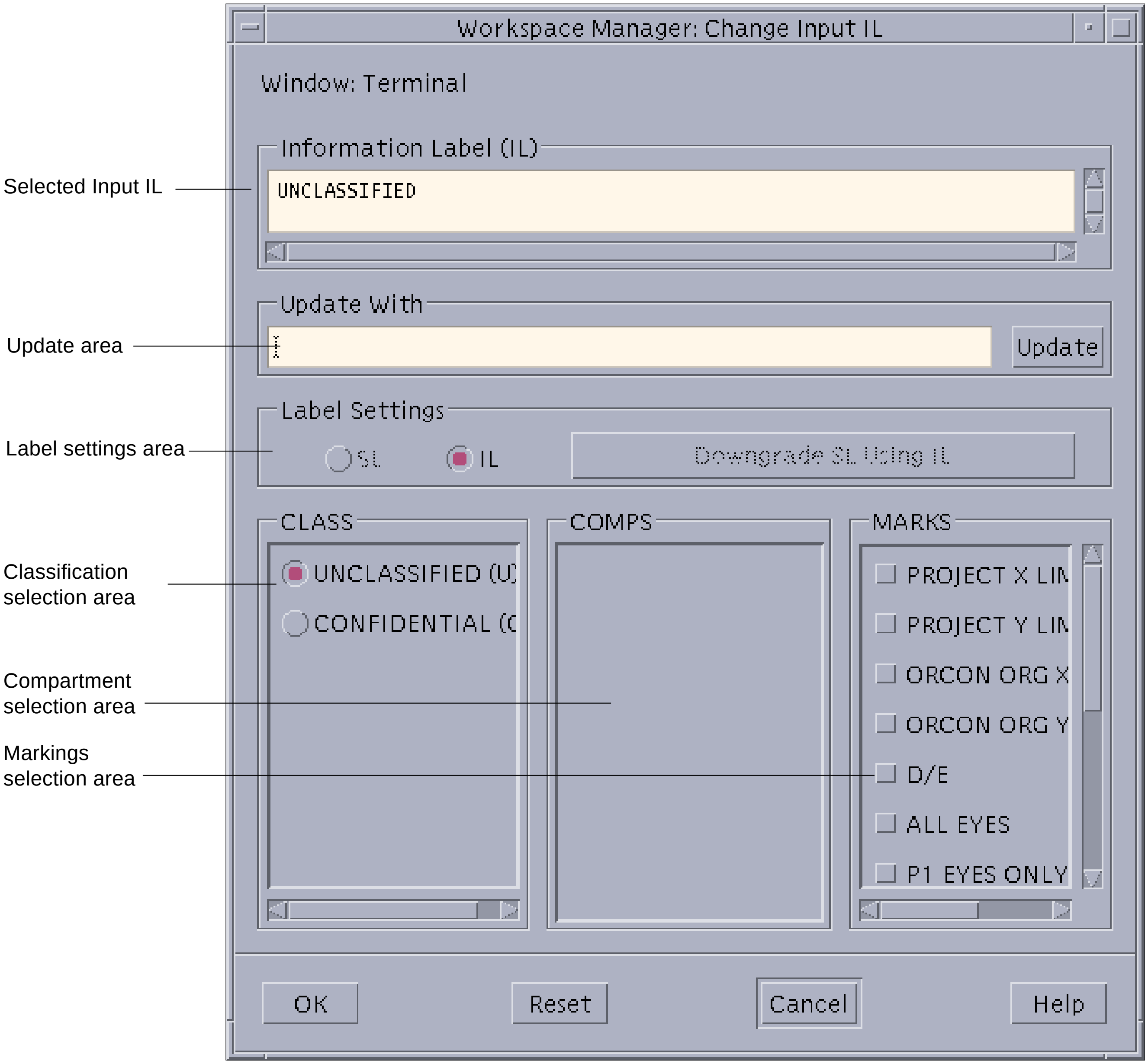
1. **Select Change Input IL from the Trusted Path menu.**
   The dialog box shown in Figure 4-18 is displayed.

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

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

4. **Click the desired markings (if any) in the markings selection area.**

5. **Check the information label you have built in the Selected Input IL field. Click the OK button if it is correct or go back to step 2 to build a different information label.**
   Now any information that you enter by means of the keyboard or mouse will be entered at the new information label. If this can cause a change in a document's information label due to information label floating, the Confirmer dialog box will be displayed so that you can confirm the change in information label or prevent it.



Workspace Manager: Change Input IL

Window: Terminal

Information Label (IL)

UNCLASSIFIED

Update With

Label Settings

○ SL ● IL

CLASS

● UNCLASSIFIED (U)

○ CONFIDENTIAL (C

COMPS

MARKS

□ PROJECT X LIN

□ PROJECT Y LIN

□ ORCON ORG X

□ ORCON ORG Y

□ D/E

□ ALL EYES

□ P1 EYES ONLY

Figure 4-18 Change Input IL Dialog Box

Allocate Device

Allocate Device lets you 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. **Select Allocate Device from the Trusted Path menu.**
   This step causes the Device Manager to be displayed (see Figure 4-20).

   OR

1. **Select Device Manager from the Trusted Desktop subpanel in the Front Panel (see Figure 4-19).**
   This is an alternative step for displaying the Device Manager (see Figure 4-20).

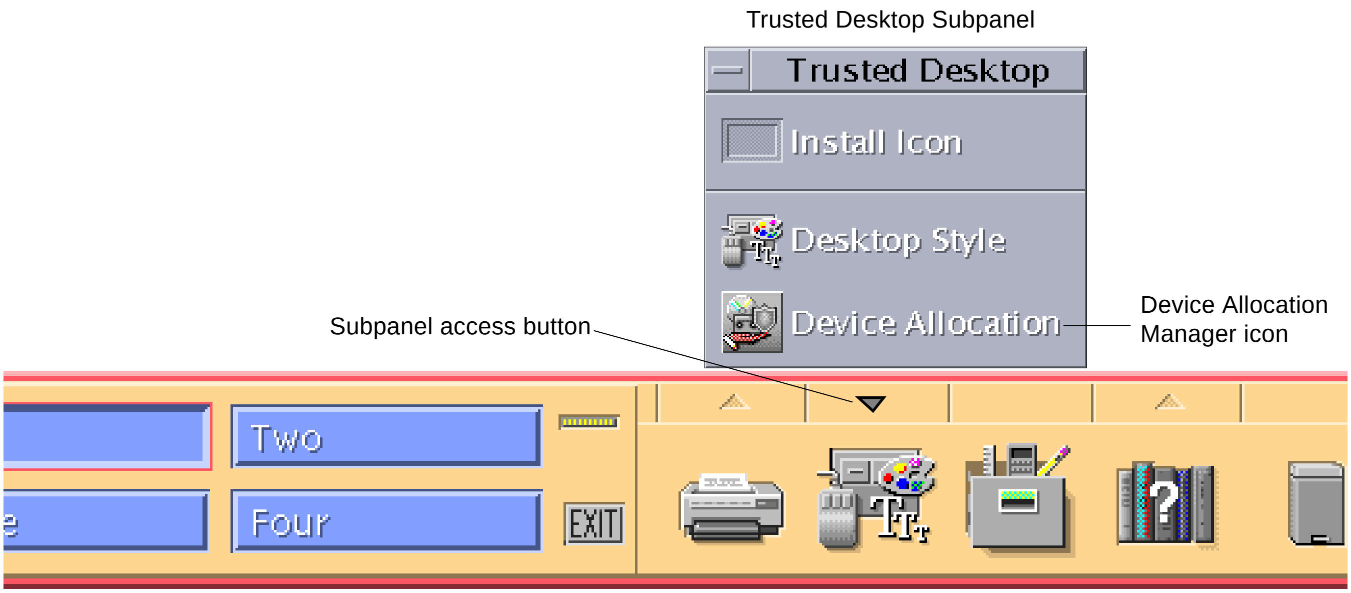
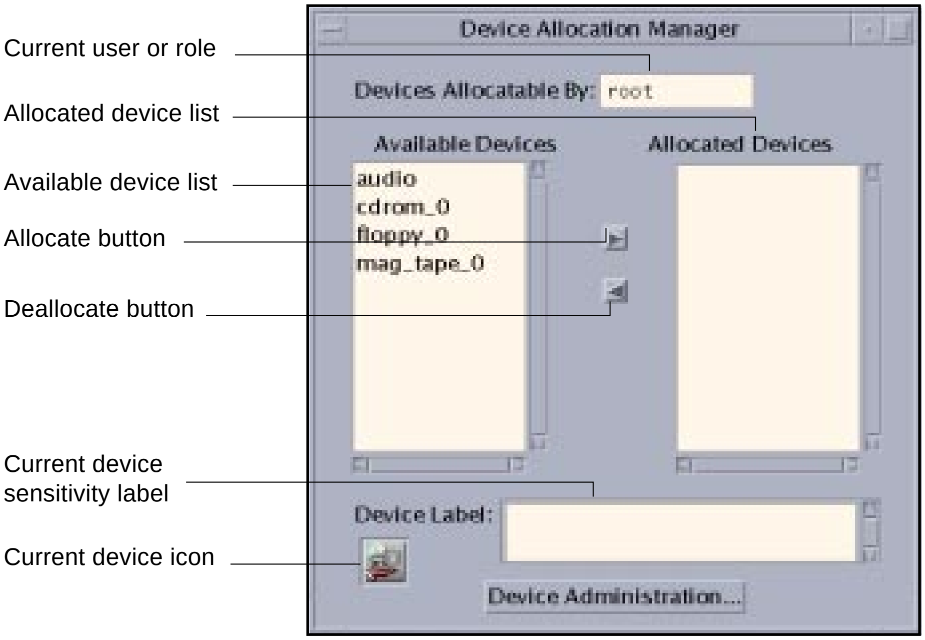


Figure 4-19 Trusted Desktop Subpanel



Devices Allocatable By: root

Figure 4-20 Device 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 sensitivity 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.

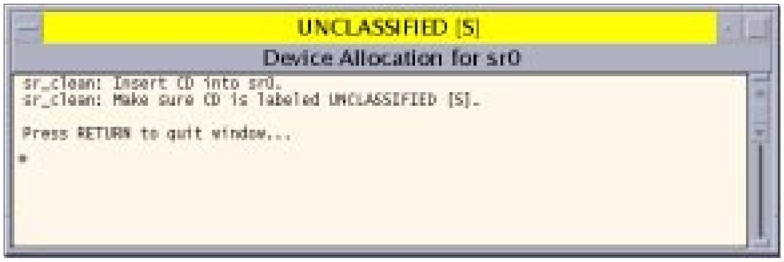
3. **Move the device from the Available Devices list to the Allocated Devices list.**
   You can accomplish this by:

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

   If your session is restricted to a single sensitivity label, that label will apply to the device and you can skip to Step 7. Otherwise, a label builder dialog box will be displayed (see Figure 4-11 on page 79 for an illustration of a similar dialog box). The label builder establishes the sensitivity label for the device you are allocating. Any data you wish to transfer to or from this device's medium must be dominated by this sensitivity label.

4. **Click the desired classification and compartments (if any) in the label builder dialog box.**

5. **Check the sensitivity label you have built in the update area. Click the Update button and then the OK button if it is correct, or go back to step 2 to build a different sensitivity label.**
   This step closes the label builder dialog box and opens a cmdtool window running a clean script (see Figure 4-21). The clean script ensures that there is no data left over on the medium from other transactions.



```
sr_clean: Insert CD into sr0.
sr_clean: Make sure CD is labeled UNCLASSIFIED [S].

Press RETURN to quit window...
■
```

Figure 4-21 Clean Script During Allocation

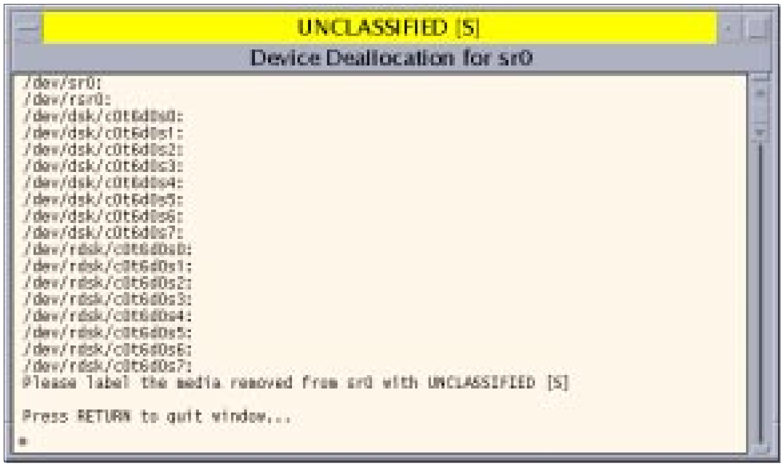
6. **Follow the instructions in the clean script, which are (1) load and label the medium and (2) press return to close the cmdtool window.**
   At this point, the medium has been cleaned and the device is ready to be used. The device name now appears in the Allocated Devices list.

7. **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 sensitivity label, you need to make a separate allocation of the device at the sensitivity label for that workspace. When you use the Occupy Workspace command from the window menu to move the Device manager to the new workspace, the Available and Allocated Devices lists change to reflect the correct context.

8. **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 opens a cmdtool window and runs a clean script that advises you about the labeling of the medium (see Figure 4-22).



```
/dev/sr0:
/dev/rsr0:
/dev/dsk/c0t6d0s0:
/dev/dsk/c0t6d0s1:
/dev/dsk/c0t6d0s2:
/dev/dsk/c0t6d0s3:
/dev/dsk/c0t6d0s4:
/dev/dsk/c0t6d0s5:
/dev/dsk/c0t6d0s6:
/dev/dsk/c0t6d0s7:
/dev/rdsk/c0t6d0s0:
/dev/rdsk/c0t6d0s1:
/dev/rdsk/c0t6d0s2:
/dev/rdsk/c0t6d0s3:
/dev/rdsk/c0t6d0s4:
/dev/rdsk/c0t6d0s5:
/dev/rdsk/c0t6d0s6:
/dev/rdsk/c0t6d0s7:
Please label the media removed from sr0 with UNCLASSIFIED [S]

Press RETURN to quit window...
■
```

Figure 4-22 Clean Script During Deallocation

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

Shut Down

Shut Down lets you shut down your machine. 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 an authorized user depending on your security policy.

Help

Help provides online help information including a glossary for the Trusted Solaris environment in general. Individual tools provide specific help directly through Help buttons and menus.

Other Switch Area Controls

In addition to the workspace buttons and the Trusted Path menu, there are two other controls in the switch area:

- Lock icon
- Exit icon

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 30 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 31 for a description of this procedure.

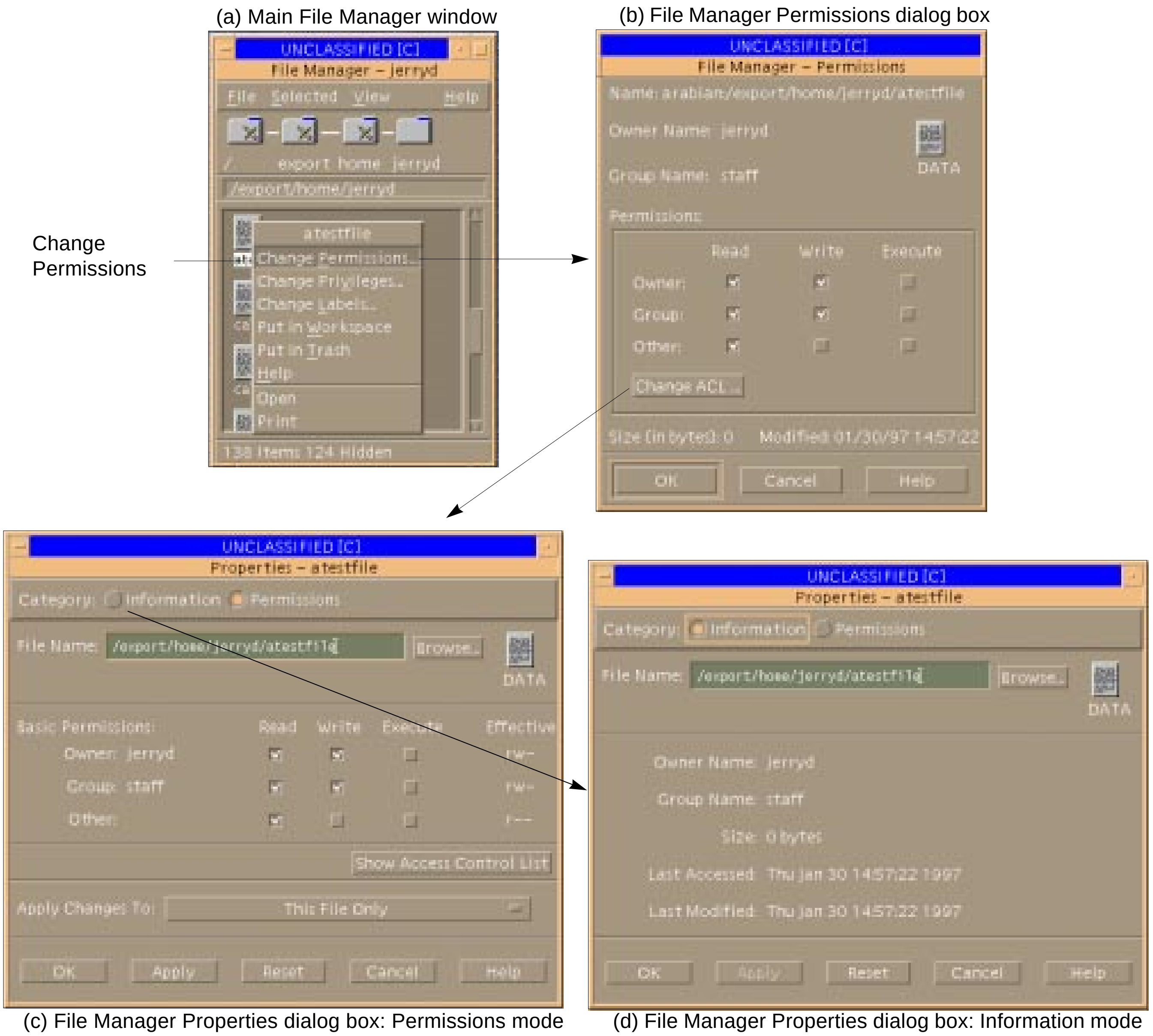
Managing Files and Directories 5

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

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.

Figure 5-1 is an overview of how you navigate to the dialog boxes for basic permissions, ACLs, and basic information. First you need to display the icon of the file to be worked on in the File Manager. When you hold down the right mouse button over the specified file, the File Manager pop-up menu is displayed and you select Change Permissions (see Figure 5-1 (a)). An alternative method is to select the file and choose Change Permissions from the Selected menu. Selecting Change Permissions causes the Permissions dialog box (for changing basic permissions) to be displayed (see Figure 5-1 (b)). Clicking the Change ACLs button in that dialog box causes the Properties dialog box to be displayed in ACL mode (see Figure 5-1 (c)). Clicking the Information button in the category field causes the Properties dialog box to be redisplayed in information mode (see Figure 5-1 (d)).



(a) Main File Manager window

(b) File Manager Permissions dialog box

UNCLASSIFIED [C]

File Manager – Permissions

Name: arabian:/export/home/jerryd/atestfile

Owner Name: jerryd

Group Name: staff

Permissions:

	Read	Write	Execute
Owner:	☑	☑	□
Group:	☑	☑	□
Other:	☑	□	□

Size (in bytes): 0 Modified: 01/30/97 14:57:22

UNCLASSIFIED [C]

Properties – atestfile

Category: ○ Information ● Permissions

File Name: /export/home/jerryd/atestfile

Basic Permissions:	Read	Write	Execute	Effective
Owner: jerryd	☑	☑	□	rw-
Group: staff	☑	☑	□	rw-
Other:	☑	□	□	r--

Apply Changes To: This File Only

UNCLASSIFIED [C]

Properties – atestfile

Category: ● Information ○ Permissions

File Name: /export/home/jerryd/atestfile

Owner Name: jerryd

Group Name: staff

Size: 0 bytes

Last Accessed: Thu Jan 30 14:57:22 1997

Last Modified: Thu Jan 30 14:57:22 1997

(c) File Manager Properties dialog box: Permissions mode

(d) File Manager Properties dialog box: Information mode

Figure 5-1 File Manager Dialog Boxes for Permissions, ACLs, and Basic Information

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 5-2).

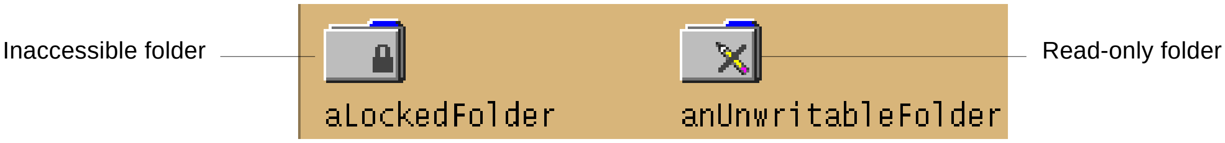


Figure 5-2 Special File Manager Icons

Permissions are granted according to three classes of user:

- *owner* – the user who created the file or folder (or received ownership through `chown(1TSOL)`), 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.

ACL entries can be applied to files, folders, or new files created within a specified folder. You can specify whether the entry applies to the owner, owner's group, others, specific users, specific groups, or to defaults for newly created files and folders.

By definition, every access control list has a special entry called a mask (which cannot be deleted). The *mask* lets you apply permissions to 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. When a file's mask is read-only, the read and write permissions for all ACL entries for users other than the owner are rendered ineffective.

The ACL entry types are described in Table 5-1.

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
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 Permissions dialog box.

▼ To Display the Permissions Dialog Box for a File or Folder

1. **Display the File Manager.**

2. **Place the pointer over the file or folder whose permissions you wish to access and press the right mouse button.**
   See Figure 5-3.

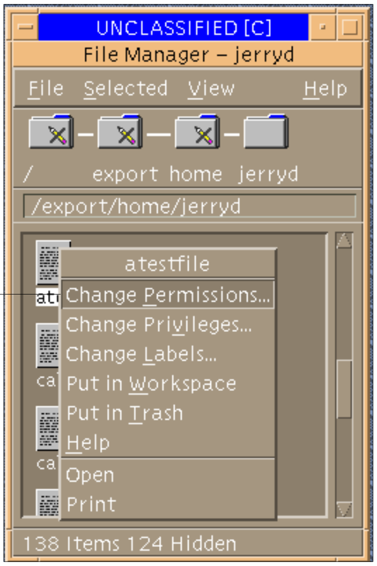


Figure 5-3 Selecting Change Permissions from the File Manager Popup Menu

3. **Select Change Permissions.**
   This step displays the Permissions 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

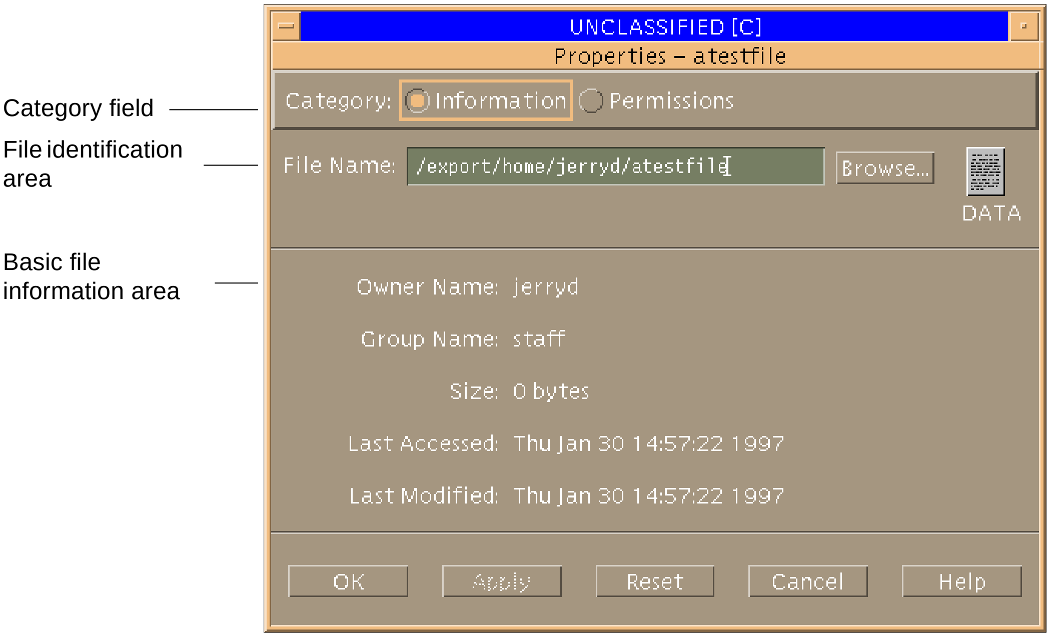
A file or folder's basic information consists of: owner, group, size in bytes, the last access date, and the last modification date.

1. **Display the File Manager Permissions dialog box.**
   See "To Display the Permissions Dialog Box for a File or Folder" on page 98.

2. **Click the "Change ACLs..." button in the File Manager Permissions dialog box.**
   This step causes the Properties dialog box to be displayed (see Figure 5-4).

3. **Click the Information button in the Category field.**
   This step sets the dialog box to basic information mode (see Figure 5-4).

4. **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.



Category: ● Information ○ Permissions

File Name: /export/home/jerryd/atestfile

Owner Name: jerryd

Group Name: staff

Size: 0 bytes

Last Accessed: Thu Jan 30 14:57:22 1997

Last Modified: Thu Jan 30 14:57:22 1997

Figure 5-4 File Manager Basic Information Dialog Box

▼ To View or Change a File or Folder’s Basic Permissions

1. **Display the File Manager Permissions dialog box.**
   See “To Display the Permissions Dialog Box for a File or Folder” on page 98.

2. **Click the Permissions button in the Category field.**
   This step sets the dialog box to permissions mode (see Figure 5-5).

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.**

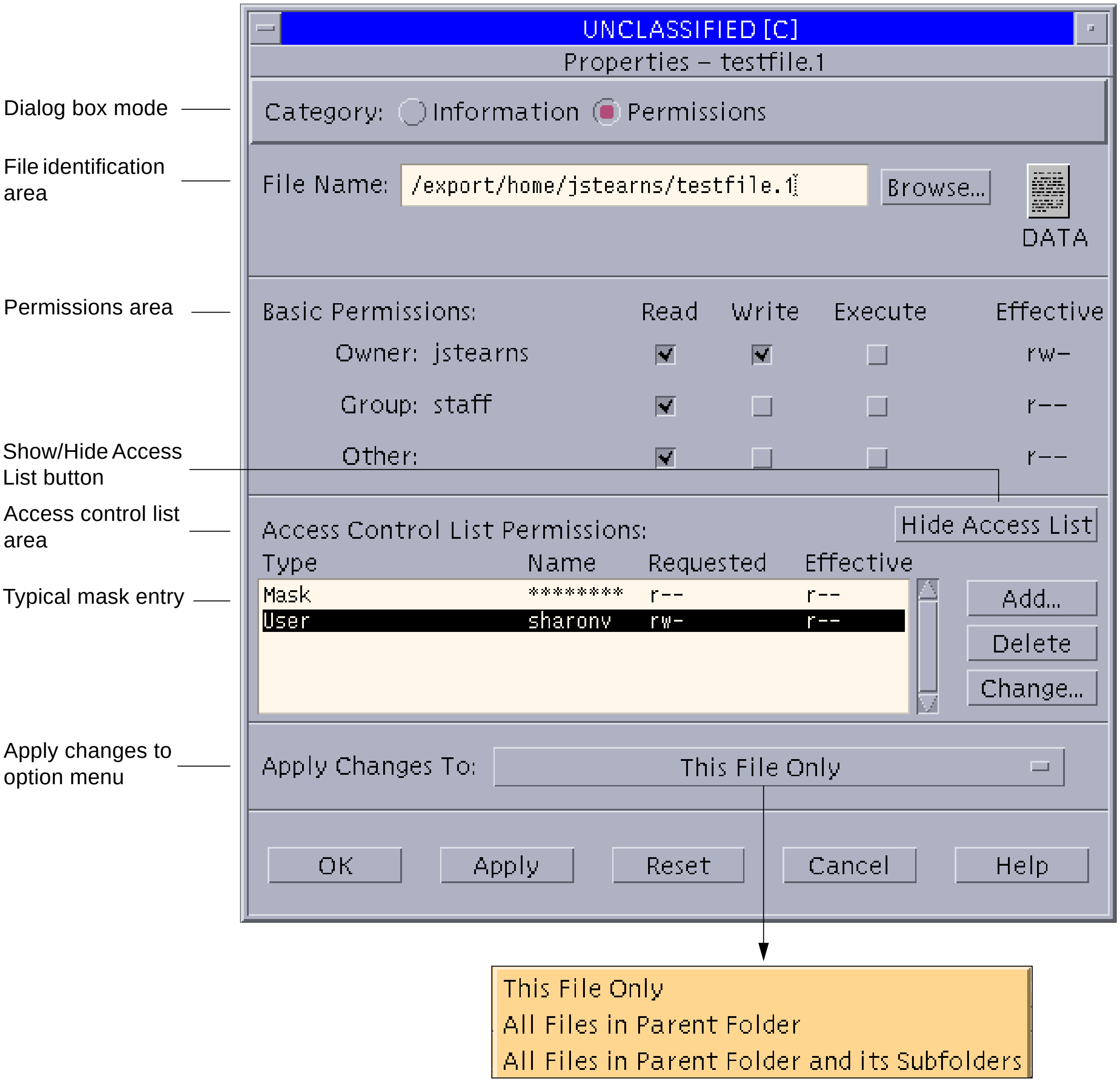
▼ To View a File or Folder’s ACL Entries

1. **Display the File Manager Permissions dialog box.**
   See “To Display the Permissions Dialog Box for a File or Folder” on page 98.

2. **Click the Permissions button in the Category field.**
   This sets the dialog box to permissions mode (see Figure 5-5).

3. **Click the Show Access 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 been applied—the effective permissions reflect the permissions after the mask has been applied.



Properties – testfile.1

Category: ○ Information ● Permissions

File Name: /export/home/jstearns/testfile.1

Basic Permissions:	Read	Write	Execute	Effective
Owner: jstearns	☑	☑	□	rw–
Group: staff	☑	□	□	r––
Other:	☑	□	□	r––

Access Control List Permissions:

Type	Name	Requested	Effective
Mask	********	r--	r--
User	sharonv	rw-	r--

Apply Changes To: This File Only

This File Only
All Files in Parent Folder
All Files in Parent Folder and its Subfolders

Figure 5-5 File Manager: Displaying ACL Entries

▼ To Add an ACL Entry

1. **Display the File Manager Permissions dialog box as described in "To View a File or Folder's ACL Entries" on page 100.**

2. **Click the Add button at the right of the ACL area (see Figure 5-5) to display the Add dialog box.**
   The File Manager Add Access List Entry dialog box is displayed as shown in Figure 5-6.

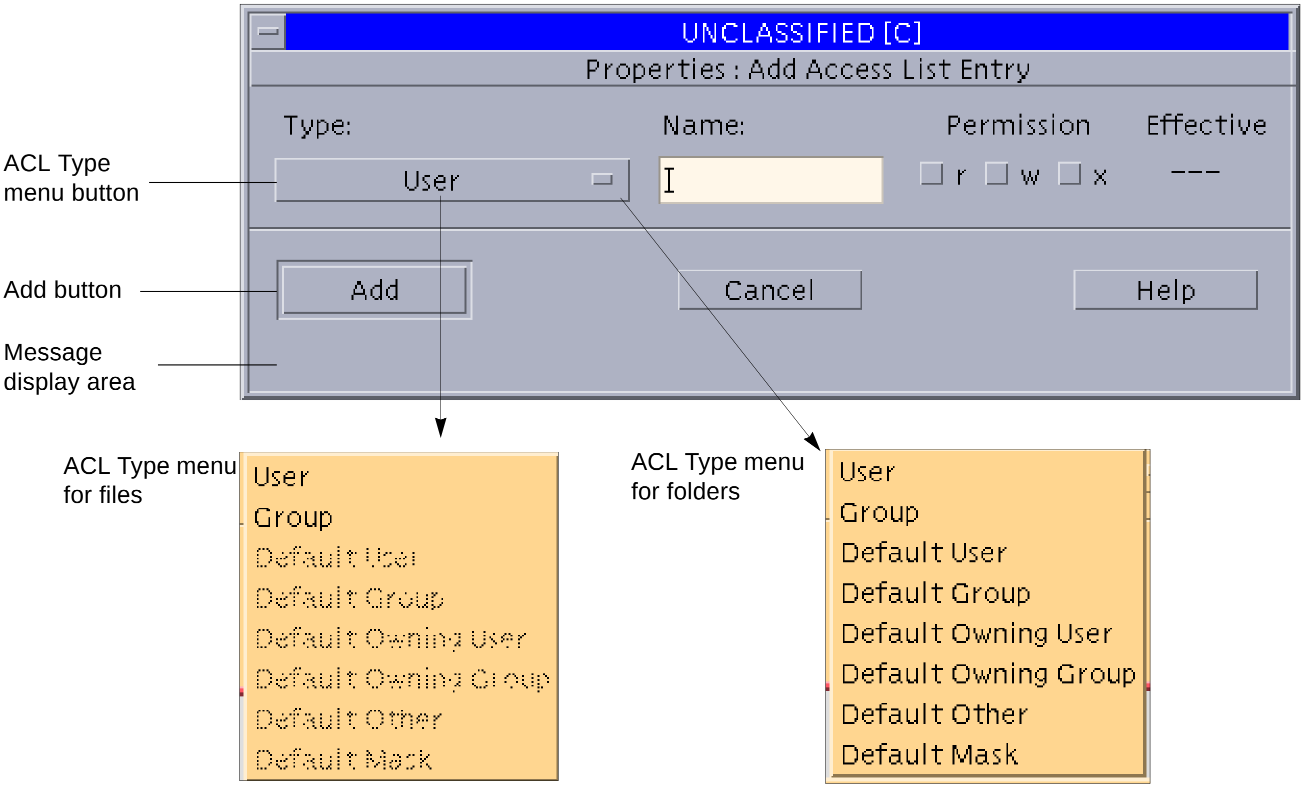


Figure 5-6 File Manager Add Access List Entry Dialog Box with ACL Type Menus

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 on page 97.

   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 Owning User, Default Owning 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 104).

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 (see Figure 5-5).**
   You can select the current file, all files in the parent folder, or all files in the parent folder and its subfolders.

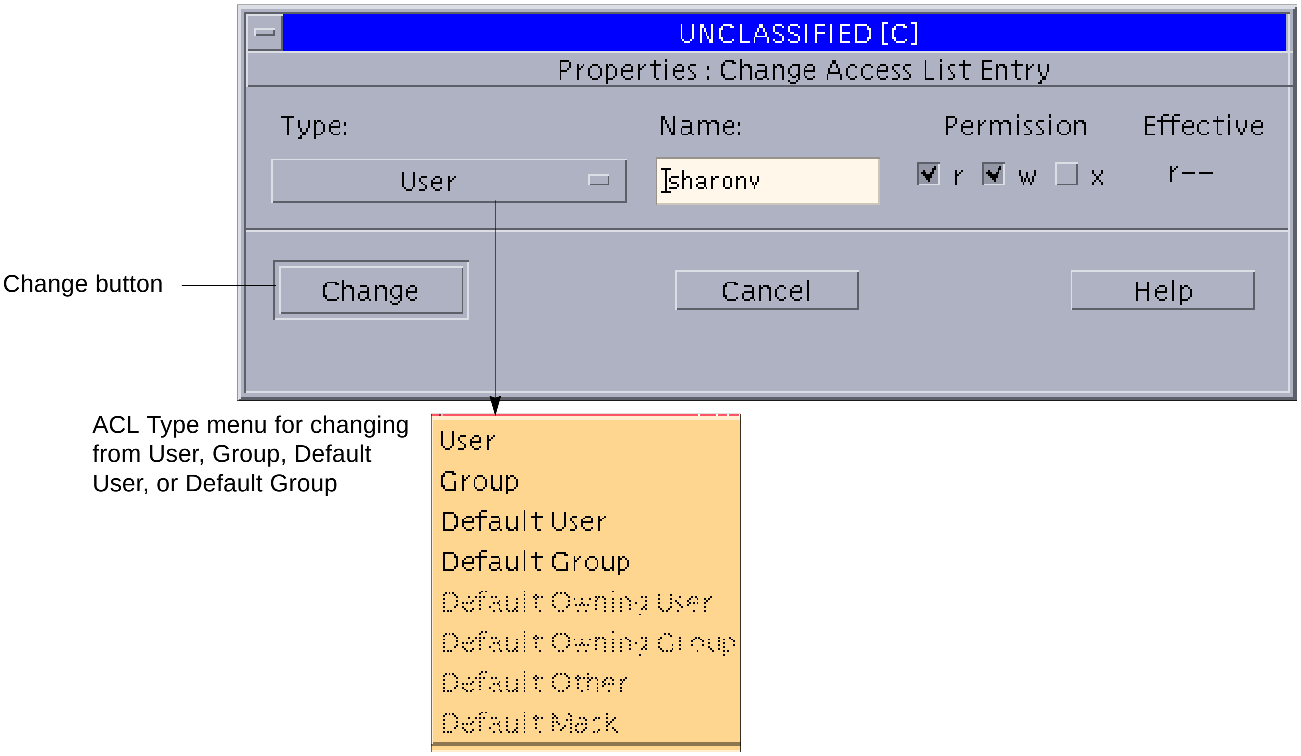
8. **Click OK or Apply to save the ACL entries (and any permissions you have changed).**

To Change an ACL Entry

1. **Display the File Manager Permissions dialog box as described in "To View a File or Folder's ACL Entries" on page 100.**

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 (see Figure 5-5) 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 (see Figure 5-7) and you can change the type. If you select Mask, Default Owning User, Default Owning Group, Default Other, or Default Mask, there is no ACL type menu button and the type is fixed. See Figure 5-8, which is an example of changing a Default Mask entry.



Type: User

Name: sharonv

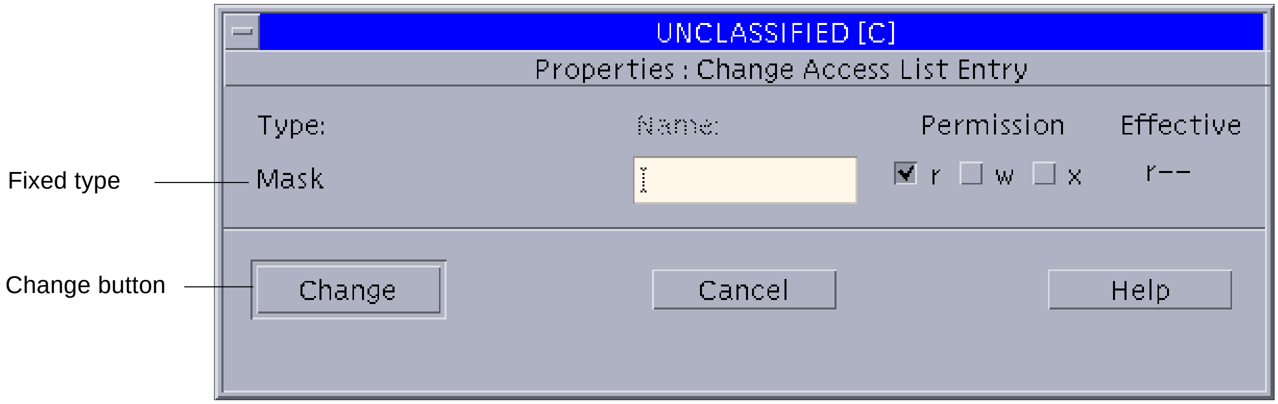
Permission: ☑ r ☑ w □ x

Effective: r--

Change button

ACL Type menu for changing from User, Group, Default User, or Default Group

Figure 5-7 File Manager Change Access List Entry Dialog Box for User, Group, Default User, or Default Group



Type: Mask

Name:

Permission: ☑ r □ w □ x

Effective: r--

Figure 5-8 File Manager Change Access List Entry Dialog Box for Default Mask

4. **Specify the type of ACL entry.**
   The type will be limited as discussed in Step 3.

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 5-5).**
   You can select the current file, all files in the parent folder, or all files in the parent folder and its subfolders.

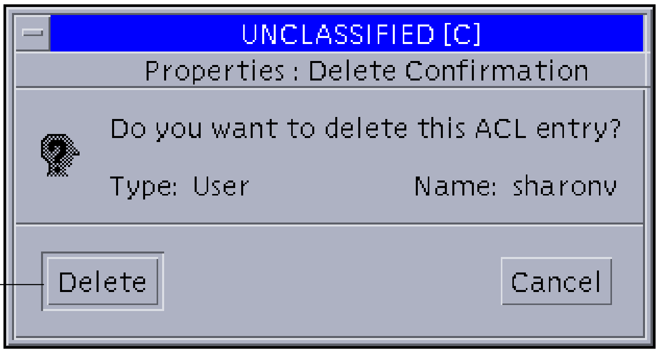
9. **Click OK or Apply to save the ACL entry changes (and any permissions you have changed).**

▼ To Delete an ACL Entry

1. **Display the File Manager Permissions dialog box as described in "To View a File or Folder's ACL Entries" on page 100.**

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 5-9).**



Do you want to delete this ACL entry?

Type: User Name: sharonv

Figure 5-9 File Manager Delete Access List Entry Dialog Box

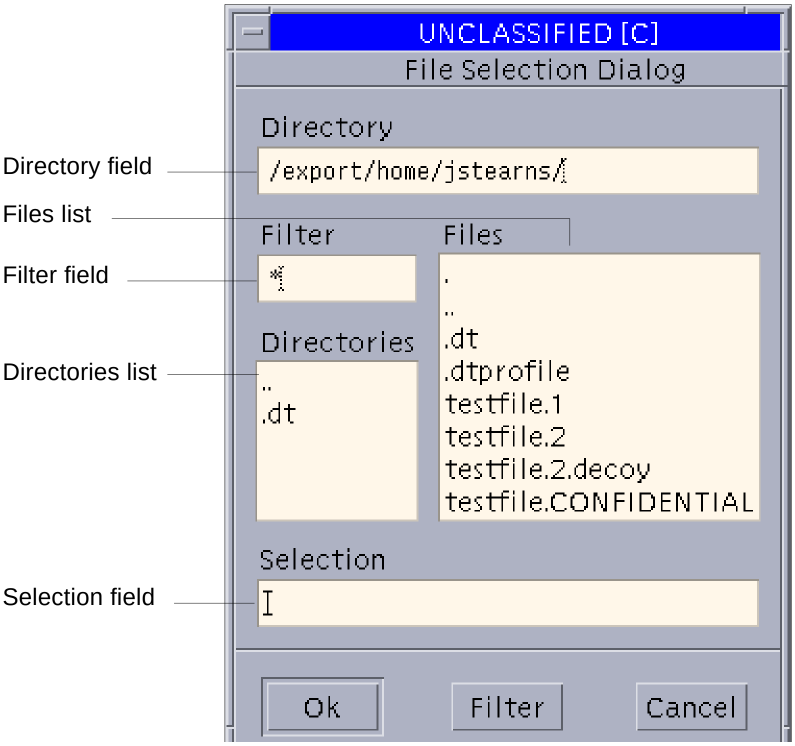
4. **Confirm that the selected entry is correct and click Delete in the dialog box.**
   This removes the entry from the Access Control List area.

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 5-5).**
   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).**

▼ To View or Change Permissions or ACLs for Other Files or Folders

1. **Click the Browse button at the right of the file identification area.**
   This causes the dialog box in Figure 5-10 to be displayed.



Directory: /export/home/jstearns/

Filter: *

Files:
.
..
.dt
.dtprofile
testfile.1
testfile.2
testfile.2.decoy
testfile.CONFIDENTIAL

Directories:
..
.dt

Figure 5-10 File Browser Dialog Box

2. **Specify the directory either by typing directly in the Directory field or by navigating in the Directories list.**

3. **To filter the files and folders in the Files list, enter a regular expression (with a wild card) in the Filter field and click the Filter button.**
   This causes those files and folders in the current directory that match the expression to be displayed in the Files list.

4. **Double-click the file or folder in the Files list whose permissions or ACLs you wish to examine.**
   Your choice appears in the Selection field.

5. **Click OK to complete your selection.**
   The file or folder you chose now appears in the File Manger Permissions dialog box (see Figure 5-5). Its type is identified by the icon at the right of the file identification area.

Manipulating File Labels

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

Viewing and Changing Labels with the File Manager

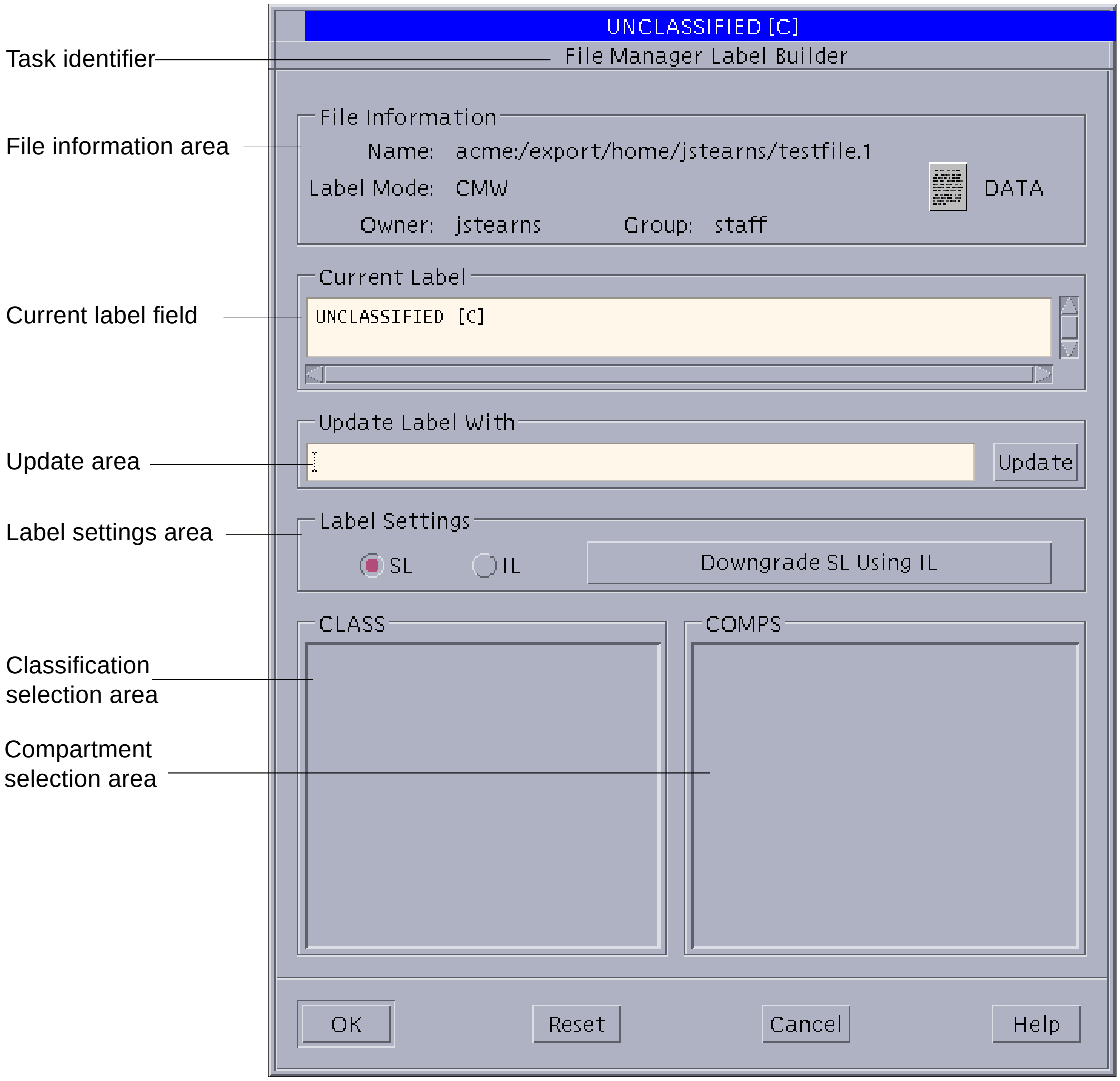
Use the File Manager when you want to view or change a file's labels.

▼ To Determine a File's CMW Label

1. **Display the File Manager and navigate to the directory containing the file.**
2. **Select the file and choose Change Labels from either the popup menu or the Selected menu.**
   You are NOT actually going to change the label; simply view its current CMW label (typically it requires special authorization or an administrator to change a file's sensitivity label using the File Manager). This step causes the Change Labels dialog box to be displayed (see Figure 5-11). The file's CMW label appears in the current label field.
3. **Click Cancel to close the Change Labels dialog box.**

▼ To Change a File's Information Label

1. **Make sure that no one else is using the file whose information label is to be changed.**
   Changing the information label of a file in use can cause serious problems when the other user attempts to save the file.
2. **Display the File Manager and navigate to the directory containing the file.**
3. **Select the file and choose Change Labels from either the popup menu or the Selected menu.**
   This step causes the Change Labels dialog box to be displayed (see Figure 5-11).



UNCLASSIFIED [C]

File Manager Label Builder

File Information

Name: acme:/export/home/jstearns/testfile.1

Label Mode: CMW

Owner: jstearns Group: staff

DATA

Current Label

UNCLASSIFIED [C]

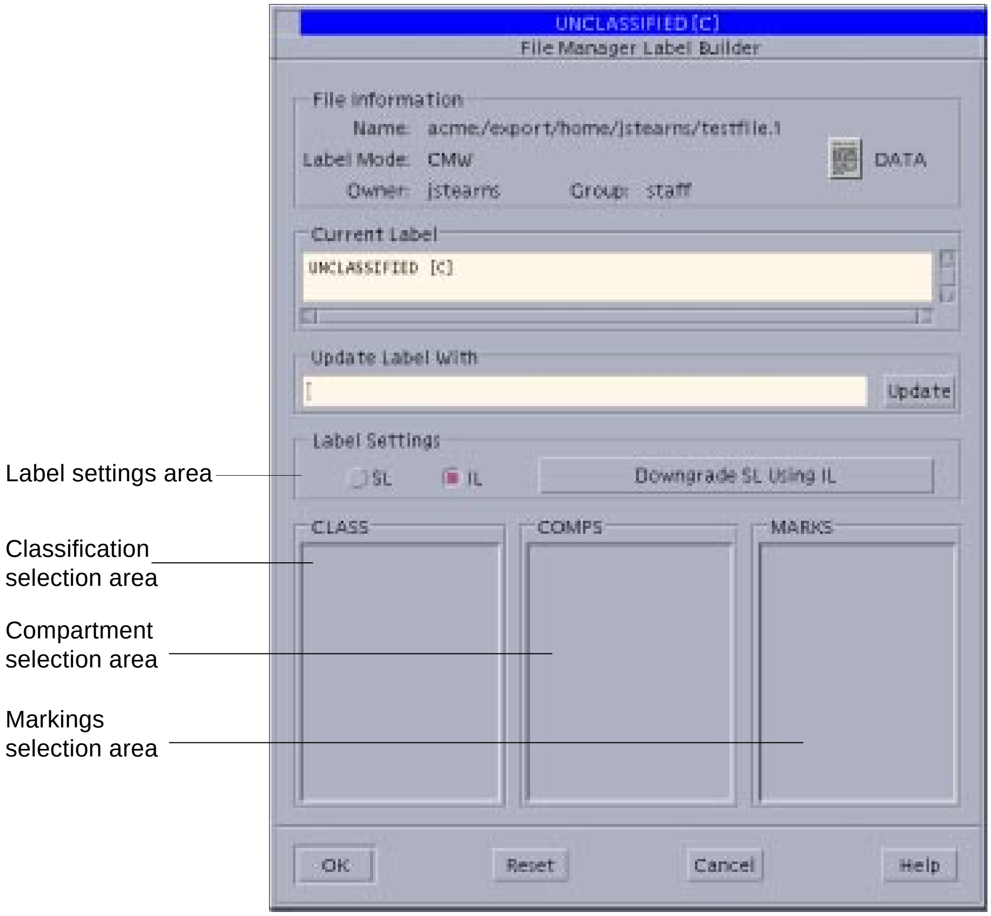
Update Label With

Label Settings

● SL ○ IL

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

4. **Click the IL button in the label settings area.**
   This switches the Change Labels dialog box to IL mode. A third column for markings now appears to the right of the compartment selection area (see Figure 5-12).



UNCLASSIFIED [C]

File Manager Label Builder

File Information

Name: acme:/export/home/jstearns/testfile.1

Label Mode: CMW

Owner: jstearns Group: staff

DATA

Current Label

UNCLASSIFIED [C]

Update Label With

Label Settings

○ SL ● IL

Figure 5-12 File Manager Change Label Dialog Box in IL Mode

5. **Select the components of the new information label from the classification, compartment, and markings selection areas.**

6. **Click OK to save the new information label and close the Change Labels dialog box.**

▼ To Change a File’s Sensitivity Label (Move Operation)

1. **Make sure that no one else is using the file whose sensitivity label is to be changed.**
   Changing the sensitivity label of a file in use can cause serious problems when the other user attempts to save the file.

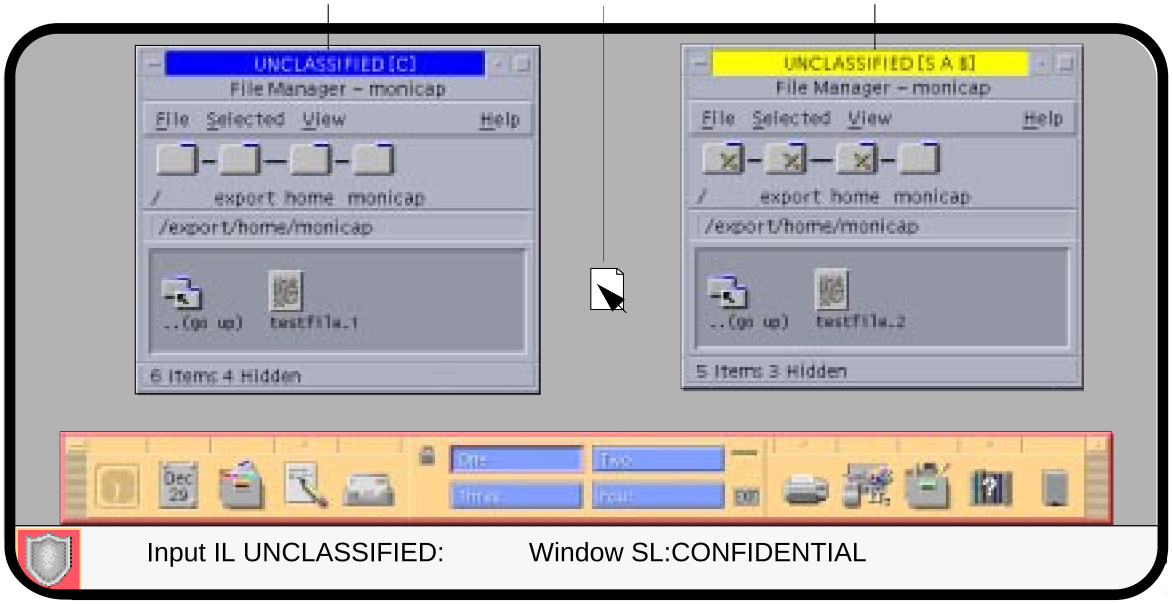
2. **Display the File Manager at the file’s current sensitivity label and the File Manager at the new sensitivity label in the same workspace.**
   This step entails opening a second workspace at a different sensitivity label, displaying its File Manager, and occupying the original workspace. For a detailed example of this procedure, see “Tour: Occupying Workspaces with Applications at Different Sensitivity Labels” on page 53.

3. **Drag the file icon from the source File Manager to the File Manager at the new sensitivity label (see Figure 5-13).**
   This causes the File Manager Confirmation dialog box to be displayed (see Figure 5-14).

File Manager at current SL

Dragged file

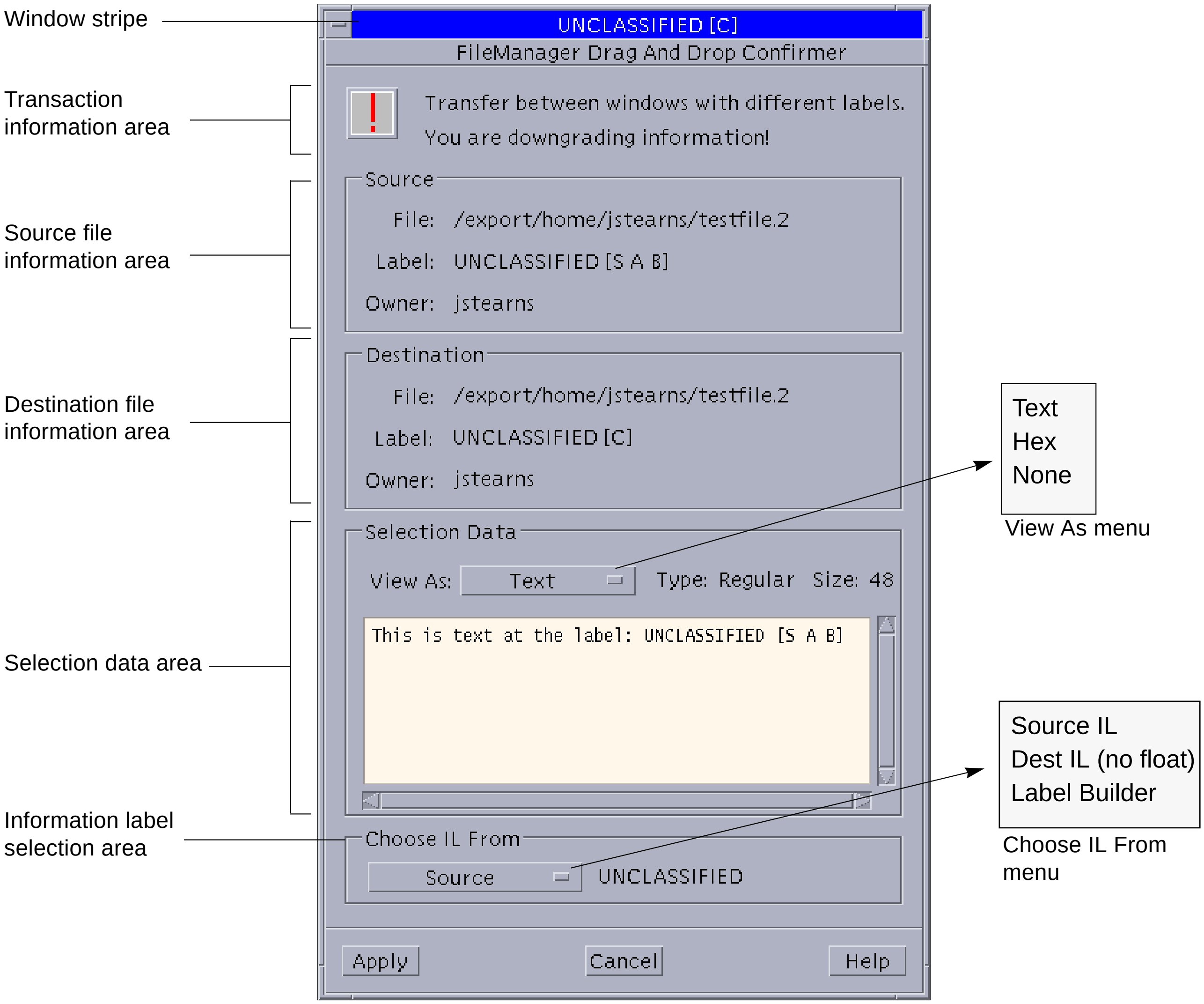
File Manager at new SL



Input IL UNCLASSIFIED: Window SL:CONFIDENTIAL

Figure 5-13 Dragging a File between File Managers at Different Sensitivity Labels

4. **Check the information label to see if it needs to be changed when the sensitivity label changes.**
   Quite often a change of sensitivity label can affect the information label.



UNCLASSIFIED [C]

FileManager Drag And Drop Confirmer

Transfer between windows with different labels.
You are downgrading information!

Source
File: /export/home/jstearns/testfile.2
Label: UNCLASSIFIED [S A B]
Owner: jstearns

Destination
File: /export/home/jstearns/testfile.2
Label: UNCLASSIFIED [C]
Owner: jstearns

Selection Data
View As: Text Type: Regular Size: 48

```
This is text at the label: UNCLASSIFIED [S A B]
```

Choose IL From
Source UNCLASSIFIED

Figure 5-14 File Manager Confirmation Dialog Box

5. **If you need to change the information label, use the Choose IL From menu in the information label selection area to choose a new information label.**
   The Source IL selection is the default. The Destination IL selection sets the new information label to the sensitivity label of the destination File Manager. The Label Builder selection displays a label builder dialog box so that you can explicitly choose the new information label.

6. **Click the Apply button in the File Manager Confirmation dialog box to complete the transfer.**
   At this point, the file icon disappears in the source File Manager window and reappears in the destination File Manager window.

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

Follow the same instructions as in "To Change a File's Sensitivity Label (Move Operation)" on page 111 except that you hold down the Control key when dragging the file icon in Step 3. Creating a copy of a file at another sensitivity label is useful when you need to use the same file name although you are editing different versions of the file at different sensitivity labels.

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

Follow the same instructions as in "To Change a File's Sensitivity Label (Move Operation)" on page 111 except that you hold down both the Shift and the Control keys when dragging the file icon in Step 3. Linking a file to another sensitivity label is useful when you want to make a file with a lower sensitivity label visible at higher sensitivity labels. The file is only writable at the lower sensitivity label.

Copying and Linking Files to Different Sensitivity 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 sensitivity labels to your home directory at different sensitivity labels. These files are provided to circumvent problems due to the storage of files in separate single-level directories within your home directory. The files are:

- **.copy_files** – stores file names to be copied when you first change to a workspace with a different sensitivity 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 sensitivity labels.
- **.link_files** – stores file names to be linked when you first change to a workspace with a different sensitivity label. This is useful when a specific file needs to be available at multiple sensitivity labels but writable at its minimum sensitivity 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. Keep in mind that there are no safeguards for dealing with such anomalies as duplicate entries in both files or file entries that already exist at other sensitivity labels.

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, or execute a file or directory. See also *discretionary access control* and *mandatory access control*.

account label range

The set of *sensitivity 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 sensitivity label*, and is limited to *well-formed labels*.

accreditation range

A set of sensitivity 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 are 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 sensitivity 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 *sensitivity labels*, *clearances*, or *information labels*. 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 *sensitivity label* and uses the name .SLD.*n* where .SLD. is the adornment string and *n* is an identifying number. A multilevel directory contains single-level directories; it uses the adornment .MLD. as a prefix to the name you specify.

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 *role*s 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 *audit trail*, 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*, a *sensitivity label*, and an *information 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 the Trusted Solaris environment. It is composed of an *information label* and a *sensitivity 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*, *sensitivity label*, or *information 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 system 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* and optionally *marking* components include all of the second label's compartment and marking components. If the components are the same, the labels are said to dominate each other and are *equal*. If one label dominates the other and the labels are not equal, it is said to *strictly dominate* the other. Two labels are *disjoint* if they are not equal and neither label is dominant.

downgraded label

A *sensitivity label* or *information labels* 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 setuid 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 `tnrhdb(4TSOL)`file. The fallback mechanism recognizes 0 as a wildcard in the rightmost byte(s) of the IP addresses.

floating

See *information label floating*.

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 `tnrhtp(4TSOL)`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 `tnrhtp(4TSOL)`database. The host type determines which network protocol is used to communicate with other hosts on the network. *Network protocol* refers to the rules for packaging communication information.

IIL

See *input information label*.

IL

See *information label*.

information label

Also referred to as IL, a *label* indicating the security level of a file, directory, process, device, or network interface. Information labels advise users how the information should be handled regarding exposure to others. An information label has three components: a *classification*, zero or more *compartments*, and zero or more *markings* with handling instructions. See also *sensitivity label* and *label encodings file*.

information label floating

An optional security feature that ensures that in a transaction where information is changed, the resulting *information label's classification* is raised to the highest information label classification in the transaction, the *compartments* include all compartments involved and the *markings* include all markings involved.

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*.

input information label

Also referred to as IIL, an *information label* applied to data that the user enters through the keyboard or other character entry device. Users can set the value of the input information label through the Trusted Path menu. The default input information label is ADMIN_LOW.

install

The name of a special user with root capabilities responsible for configuring the Trusted Solaris system.

label

A security indicator assigned to an entity in the Trusted Solaris environment indicating the level to which it should be protected. All labels have at least two components: a *classification* indicating the hierarchical level of security, and zero or more *compartments* for defining who has a need to access to the entity given a sufficiently high classification. See also *clearance*, *sensitivity label*, *information label*, and *CMW label*.

label encodings file

A file managed by the *security administrator* that contains the definitions for all valid *clearances*, *sensitivity labels*, and *information labels*, as well as defining the *system accreditation range*, *user accreditation range*, and labelling of hardcopy reports for the site.

label range

Any set of *sensitivity label*s bounded on the upper end by a *clearance* or maximum sensitivity label, on the lower end by a minimum sensitivity 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 *sensitivity label*. There are two exceptions. (1) Authorized users can move a window at a different sensitivity label into the workspace using the Occupy Workspace or Occupy All Workspaces 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 *sensitivity labels* to enforce security policy. MAC associates the programs a user runs with the security level (clearance or sensitivity 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*.

marking

The codewords, handling warnings, control and release instructions and other information used to specify how information should be handled with regard to exposure to others. Examples include COMPANY USE ONLY and NOFORN (not for dissemination to non-U.S. nationals). A marking is a part of an *information label*.

minimum sensitivity label

A *sensitivity label* assigned to a user as the lower bound of the set of sensitivity labels at which that user may work. The minimum sensitivity label is the user's initial sensitivity label by default when the user first begins a Trusted Solaris session. The user can optionally reset the value for the initial sensitivity label if desired by changing the home session.

Also, the lowest sensitivity label permitted to any non-administrative user. It is assigned by the *security administrator* and it defines the bottom of the *user accreditation range*.

MLD

See *multilevel directory*.

multilevel directory

Also referred to as MLD, a special type of directory that transparently stores information by *sensitivity 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 sensitivity label only. Note; if permitted by the security policy, a user may access information at other sensitivity labels by explicitly specifying the *adorned name*s of directories in the path. See also *single-level directory*.

network accreditation range

The set of *sensitivity labels* within which Trusted Solaris hosts are permitted to communicate on a network.

normal user

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 *r*) lets the user read the contents of a file or, if a directory, list the files in the folder. Write permission (*w*) lets the user make changes to a file or, if a folder, add or delete files. Execute permission (*e*) 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*. See also *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 *sensitivity label* of the current workspace, and an *information label*.

process clearance

A *clearance* equal to the *session clearance* that sets a boundary on the highest *sensitivity 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 range*s, 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 *sensitivity 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 *sensitivity label* that dominates the subject’s sensitivity 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 `execve(2TSOL)`. 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 sensitivity 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

Also referred to as SL, a *label* 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 sensitivity label: a *classification* and zero or more *compartments*. See also *information label* and *label encodings file*.

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 *sensitivity 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 sensitivity 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 sensitivity label*.

single-level directory

Also referred to as SLD, a subdirectory within a *multilevel directory* containing files and optionally subdirectories at a single sensitivity 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 sensitivity 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 *TP*) 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 between one and three components: (1) a mandatory *trusted path symbol* to indicate interaction with the *trusted computing base*, (2) an optional *sensitivity label* to indicate the sensitivity label of the current window or workspace, and (3) an optional *input information label* indicator to show the information label that will be applied to text data entered from the keyboard.

upgraded label

A *sensitivity label* or *information labels* 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 *sensitivity label* has been upgraded and thus dominates the sensitivity 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 sensitivity 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 *sensitivity label* or *information 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 a *subject* to write to an *object* whose *sensitivity label* is strictly dominated by the subject's sensitivity 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 sensitivity labels is permitted and is the norm. See also *mandatory access control* and *writing up*.

writing up

The ability of a a *subject* to write to an *object* whose *sensitivity label* dominates (or is equal to) the subject's sensitivity 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