

Solaris Trusted Extensions User's Guide

Beta



Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

Part No: 819-7313-03
August 2006

Copyright 2006 Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 U.S.A. All rights reserved.

Sun Microsystems, Inc. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more U.S. patents or pending patent applications in the U.S. and in other countries.

U.S. Government Rights – Commercial software. Government users are subject to the Sun Microsystems, Inc. standard license agreement and applicable provisions of the FAR and its supplements.

This distribution may include materials developed by third parties.

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

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

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

Products covered by and information contained in this publication are controlled by U.S. Export Control laws and may be subject to the export or import laws in other countries. Nuclear, missile, chemical or biological weapons or nuclear maritime end uses or end users, whether direct or indirect, are strictly prohibited. Export or reexport to countries subject to U.S. embargo or to entities identified on U.S. export exclusion lists, including, but not limited to, the denied persons and specially designated nationals lists is strictly prohibited.

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

Copyright 2006 Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 U.S.A. Tous droits réservés.

Sun Microsystems, Inc. détient les droits de propriété intellectuelle relatifs à la technologie incorporée dans le produit qui est décrit dans ce document. En particulier, et ce sans limitation, ces droits de propriété intellectuelle peuvent inclure un ou plusieurs brevets américains ou des applications de brevet en attente aux Etats-Unis et dans d'autres pays.

Cette distribution peut comprendre des composants développés par des tierces personnes.

Certains composants de ce produit peuvent être dérivées du logiciel Berkeley BSD, licenciés par l'Université de Californie. UNIX est une marque déposée aux Etats-Unis et dans d'autres pays; elle est licenciée exclusivement par X/Open Company, Ltd.

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

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

Les produits qui font l'objet de cette publication et les informations qu'il contient sont régis par la législation américaine en matière de contrôle des exportations et peuvent être soumis au droit d'autres pays dans le domaine des exportations et importations. Les utilisations finales, ou utilisateurs finaux, pour des armes nucléaires, des missiles, des armes chimiques ou biologiques ou pour le nucléaire maritime, directement ou indirectement, sont strictement interdites. Les exportations ou réexportations vers des pays sous embargo des Etats-Unis, ou vers des entités figurant sur les listes d'exclusion d'exportation américaines, y compris, mais de manière non exclusive, la liste de personnes qui font objet d'un ordre de ne pas participer, d'une façon directe ou indirecte, aux exportations des produits ou des services qui sont régis par la législation américaine en matière de contrôle des exportations et la liste de ressortissants spécifiquement désignés, sont rigoureusement interdites.

LA DOCUMENTATION EST FOURNIE "EN L'ETAT" ET TOUTES AUTRES CONDITIONS, DECLARATIONS ET GARANTIES EXPRESSES OU TACITES SONT FORMELLEMENT EXCLUES, DANS LA MESURE AUTORISEE PAR LA LOI APPLICABLE, Y COMPRIS NOTAMMENT TOUTE GARANTIE IMPLICITE RELATIVE A LA QUALITE MARCHANDE, A L'APTITUDE A UNE UTILISATION PARTICULIERE OU A L'ABSENCE DE CONTREFACON.

Contents

Preface	11
1 Introduction to Solaris Trusted Extensions Software	15
What Is Trusted Extensions Software?	15
Trusted Extensions Protects Against Intruders	16
Access to the Trusted Computing Base Is Limited	16
Mandatory Access Control Protects Information	16
Peripheral Devices Are Protected	16
Programs That Spoof Users Are Prevented	16
Trusted Extensions Provides Mandatory Access Control	17
Discretionary Access Control	17
Mandatory Access Control	17
User Responsibilities for Protecting Data	22
Trusted Extensions Separates Information by Label	22
Single-Level or Multilevel Sessions	22
Session Selection Example	23
Labeled Workspaces	24
Enforcing MAC for Email Transactions	24
Clearing Objects Prior to Reuse	24
Trusted Extensions Enables Secure Administration	25
Getting Access to Applications in Trusted Extensions	25
Roles Administering at Your Site	26
2 Logging In to Trusted Extensions (Tasks)	27
Desktops and Login in Trusted Extensions	27
Trusted Extensions Login Process	28
Desktop Choice Before Login	28
Identification and Authentication During Login	28

Review Security Settings During Login	29
Starting in Trusted Extensions (Tasks)	29
▼ Choose a Desktop	29
▼ Identify Yourself to the System	29
▼ Authenticate Yourself	30
▼ Check Messages and Select Session Type	30
▼ Troubleshoot Login Problems	32
3 Working in Trusted Extensions (Tasks)	35
Visible Desktop Security in Trusted Extensions	35
Trusted Extensions Logout Process	36
Working on a Labeled System (Tasks)	37
▼ How to Lock and Unlock Your Screen	37
▼ How to Log In Remotely	38
▼ How to Log Out of Trusted Extensions	38
▼ How to Shut Down Your System	39
▼ How to View Your Files in a Workspace	39
▼ How to Find the Trusted Extensions Man Pages	40
▼ How to Use Trusted Extensions Online Help	41
▼ How to Customize the CDE Workspace Menu	41
▼ How to Access Initialization Files at Every Label	42
▼ How to Interactively Display a Window Label	43
▼ How to Do Some Common Desktop Tasks	44
Performing Trusted Actions (Tasks)	45
▼ How to Change Your Password	45
▼ How to Log In at a Different Label	46
▼ How to Allocate a Device	46
▼ How to Assume a Role	49
▼ How to Work at a Different Label	50
▼ How to Change the Label of a Workspace	50
▼ How to Add a Workspace at a Particular Label	51
▼ How to Switch to a Workspace at a Different Label	52
▼ How to Move a Window to a Different Workspace	52
▼ How to Determine the Label of a File	53
▼ How to Move Data Between Labels	53
▼ How to Move Files Between Labels	55

▼ How to Link a File to a Different Label	58
4 Elements of Trusted Extensions	61
Basics of Trusted Extensions	61
Labels on Trusted Extensions Desktops	62
Trusted Stripe	63
Files and Applications in Trusted Extensions	64
.copy_files File	64
.link_files File	65
Password Security	65
Front Panel Security (CDE)	66
Workspace Switch Area	66
Trusted Path Menu	66
Clock Security	67
Calendar Security	67
File Manager Security	67
Text Editor Security	67
Personal Applications Subpanel	68
Mailer Security	68
Printer Security	68
Style Manager Security	69
Application Manager Security	70
Trash Can Security	70
 Glossary	 71
 Index	 79

Tables

TABLE 1-1	Examples of Label Relationships	21
TABLE 1-2	How Session Selections Affect Session Values	23

Figures

FIGURE 1-1	The Trusted Extensions Logo in CDE	15
FIGURE 1-2	Trusted Symbol	17
FIGURE 1-3	Typical Industry Sensitivity Labels	18
FIGURE 1-4	Typical Solaris Trusted Extensions (CDE) Session	19
FIGURE 1-5	Viewing Public Information From the Internal Zone	20
FIGURE 1-6	Workspace Switch Area	24
FIGURE 2-1	Last Login Dialog Box	31
FIGURE 2-2	Label Builder	32
FIGURE 3-1	A Trusted Extensions Desktop	36
FIGURE 3-2	Front Panel Switch Area	37
FIGURE 3-3	A Labeled File Manager	40
FIGURE 3-4	Trusted Extensions Online Help	41
FIGURE 3-5	Query Window Label Operation	44
FIGURE 3-6	Device Allocation Icon	47
FIGURE 3-7	Device Allocation Manager	47
FIGURE 3-8	Front Panel With Switches at Different Labels	50
FIGURE 3-9	Selecting Occupy Workspace	52
FIGURE 3-10	Differently Labeled Windows in One Workspace	53
FIGURE 3-11	Displaying Applications at Different Labels	54
FIGURE 3-12	Selection Manager Confirmation Dialog Box	55
FIGURE 3-13	Displaying File Managers at Different Labels	56
FIGURE 3-14	Dragging a File Between File Managers at Different Labels	57
FIGURE 3-15	File Manager Confirmation Dialog Box	58
FIGURE 4-1	Solaris Trusted Extensions Multilevel CDE Desktop	62
FIGURE 4-2	PUBLIC Window Label in the Trusted Stripe	63
FIGURE 4-3	Trusted Path Indicator in the Trusted Stripe	64
FIGURE 4-4	Trusted Path Menu – Basic	66
FIGURE 4-5	Trusted Path Menu - Workspace <i>Name</i> Version	67
FIGURE 4-6	Typical Print Banner Page	69

Preface

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

How the Solaris Trusted Extensions Books Are Organized

The Solaris Trusted Extensions 1.0 documentation set supplements the documentation for the Solaris Express release. You should obtain a copy of both sets for a complete understanding of Solaris Trusted Extensions. The Solaris Trusted Extensions documentation set consists of the following books:

Book Title	Topics	Audience
<i>Solaris Trusted Extensions Transition Guide</i>	Provides an overview of the differences between Trusted Solaris 8 software, Solaris Express software, and Solaris Trusted Extensions 1.0 software.	All
<i>Solaris Trusted Extensions Reference Manual</i>	Provides Solaris Trusted Extensions-specific man pages.	All
<i>Solaris Trusted Extensions User's Guide</i>	Describes the basic features of Solaris Trusted Extensions. This book contains a glossary.	End users, administrators, and developers
<i>Solaris Trusted Extensions Release Notes</i>	Lists known problems and describes workarounds for Solaris Trusted Extensions 1.0 software.	Administrators, developers
<i>Solaris Trusted Extensions Installation and Configuration</i>	Describes how to plan for, install, and configure Solaris Trusted Extensions.	Administrators, developers
<i>Solaris Trusted Extensions Administrator's Procedures</i>	Provides detailed information for performing specific administration tasks.	Administrators, developers
<i>Solaris Trusted Extensions Developer's Guide</i>	Describes how to develop applications with Solaris Trusted Extensions.	Developers, administrators

Book Title	Topics	Audience
<i>Solaris Trusted Extensions Label Administration</i>	Provides information on specifying label components in the label encodings file.	Administrators
<i>Compartmented Mode Workstation Labeling: Encodings Format</i>	Describes the syntax used in the label encodings file. The syntax enforces the various rules for well-formed labels for a system.	Administrators

How This Guide Is Organized

[Chapter 1](#) provides an overview of the basic concepts that you need to operate in a Solaris system that is configured with Trusted Extensions.

[Chapter 2](#) presents procedures for accessing and leaving a system that is configured with Trusted Extensions.

[Chapter 3](#) takes you for a quick tour of the Trusted Extensions software. If you have access to a system that is configured with Trusted Extensions, you can perform the steps as you read them. Or, you can get a good idea of how the software works by simply reading and following the diagrams. This chapter also describes man pages and online help for Trusted Extensions.

[Chapter 4](#) explains the key elements in a system that is configured with Trusted Extensions.

[Glossary](#) describes security terms that are used in Trusted Extensions.

Documentation, Support, and Training

The Sun web site provides information about the following additional resources:

- [Documentation](http://www.sun.com/documentation/) (<http://www.sun.com/documentation/>)
- [Support](http://www.sun.com/support/) (<http://www.sun.com/support/>)
- [Training](http://www.sun.com/training/) (<http://www.sun.com/training/>)

Typographic Conventions

The following table describes the typographic conventions that are used in this book.

TABLE P-1 Typographic Conventions

Typeface	Meaning	Example
AaBbCc123	The names of commands, files, and directories, and onscreen computer output	Edit your <code>.login</code> file. Use <code>ls -a</code> to list all files. <code>machine_name%</code> you have mail.
AaBbCc123	What you type, contrasted with onscreen computer output	<code>machine_name%</code> su Password:
<i>aabbcc123</i>	Placeholder: replace with a real name or value	The command to remove a file is <i>rm filename</i> .
<i>AaBbCc123</i>	Book titles, new terms, and terms to be emphasized	Read Chapter 6 in the <i>User's Guide</i> . A <i>cache</i> is a copy that is stored locally. Do <i>not</i> save the file. Note: Some emphasized items appear bold online.

Shell Prompts in Command Examples

The following table shows the default UNIX® system prompt and superuser prompt for the C shell, Bourne shell, and Korn shell.

TABLE P-2 Shell Prompts

Shell	Prompt
C shell	<code>machine_name%</code>
C shell for superuser	<code>machine_name#</code>
Bourne shell and Korn shell	<code>\$</code>
Bourne shell and Korn shell for superuser	<code>#</code>

Introduction to Solaris Trusted Extensions Software

This chapter introduces you to Trusted Extensions software. Trusted Extensions adds labels and other security features to the Solaris Operating System (Solaris OS).

- “What Is Trusted Extensions Software?” on page 15
- “Trusted Extensions Protects Against Intruders” on page 16
- “Trusted Extensions Provides Mandatory Access Control” on page 17
- “Trusted Extensions Separates Information by Label” on page 22
- “Trusted Extensions Enables Secure Administration” on page 25

What Is Trusted Extensions Software?

As the logo indicates, the Solaris Trusted Extensions software package is added to the Solaris OS.



FIGURE 1-1 The Trusted Extensions Logo in CDE

Trusted Extensions provides special security features for your system. These features enable an organization to define and implement a security policy on a Solaris system. A *security policy* is the set of rules and practices that help protect information and other resources, such as computer hardware, at your site. Typically, security rules handle such items as who has access to which information or who is allowed to write data to removable media. *Security practices* are recommended procedures for performing tasks.

The following sections describe some major security features that Trusted Extensions provides. The text indicates where these security features are configurable.

Trusted Extensions Protects Against Intruders

Trusted Extensions software adds features to the Solaris OS that protect against intruders. Trusted Extensions software also relies on some Solaris features, such as password protection. Trusted Extensions adds a password change GUI for roles. Auditing is enabled by default.

Access to the Trusted Computing Base Is Limited

The term *trusted computing base (TCB)* refers to the part of the Trusted Extensions software that affects security. The TCB 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 have with the TCB. Such interactions include programs that you need to do your job, files that you are allowed to access, and utility programs that can affect security.

Mandatory Access Control Protects Information

If an intruder does successfully log in to the system, further obstacles prevent access to information. Files and other resources are protected by access control. As in the Solaris OS, access control can be set by the owner of the information. In Trusted Extensions, access is also controlled by the system. For details, see [“Trusted Extensions Provides Mandatory Access Control” on page 17](#).

Peripheral Devices Are Protected

In Trusted Extensions, administrators control access to local peripheral devices such as tape drives, CD-ROM drives, printers, and microphones. Access can be granted on a user-by-user basis. The software restricts access to peripheral devices as follows:

- By default, devices must be allocated for use.
- You must be authorized to access devices that control removable media.
- Remote users cannot use local devices such as microphones or CD-ROM drives. Only local users can allocate a device.

Programs That Spoof Users Are Prevented

To spoof means to imitate. Intruders sometimes spoof login or other legitimate programs to intercept passwords or other sensitive data. Trusted Extensions protects you from hostile spoofing programs by displaying the *trusted symbol*, a clearly recognizable, tamper-proof icon at the bottom of the screen. The symbol is displayed whenever you interact with the trusted computing base (TCB). The presence of the symbol ensures the safety of performing security-related transactions. No visible symbol indicates a potential security breach. The following figure shows the trusted symbol.



FIGURE 1-2 Trusted Symbol

Trusted Extensions Provides Mandatory Access Control

Trusted Extensions controls which users can access which information by providing both discretionary and mandatory access control.

Discretionary Access Control

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

Permission bits let the owner set read, write, and execute protection by owner, group, and other users. In traditional UNIX systems, the superuser or root user can override DAC protection. With Trusted Extensions software, the ability to override DAC is permitted for administrators and authorized users only. Access control lists (ACLs) provide a finer granularity of access control. ACLs enable owners to specify separate permissions for specific individuals and specific groups. For more information, see Chapter 6, "Controlling Access to Files (Tasks)," in *System Administration Guide: Security Services*.

Mandatory Access Control

Mandatory access control (MAC) is a system-enforced access control mechanism that is based on label relationships. The system associates a sensitivity label with all processes that are created to execute programs. MAC policy uses this label in access control decisions. In general, processes cannot store information and cannot communicate with other processes unless the label of the destination is equal to the label of the process. MAC policy permits processes to read data from objects at the same label or from objects at a lower label. However, the administrator can create a labeled environment in which few lower-level objects or no lower-level objects are available.

By default, MAC policy is invisible to you. Ordinary users cannot see objects unless they have MAC access to those objects. In all cases, users cannot take any action that is contrary to MAC policy.

Sensitivity Labels and Clearances

A label has two components:

- Classification, also referred to as a *level*

This component indicates a hierarchical level of security. When applied to people, the classification represents a measure of trust. When applied to data, a classification is the degree of protection that is required.

In the U.S. Government, classifications are: TOP SECRET, SECRET, CONFIDENTIAL, and UNCLASSIFIED. Industry classifications are not as standardized. Unique classifications can be established by a company. For an example, see [Figure 1-3](#). The names on the left are classifications. The names on the right are compartments.
- Compartments, also referred to as *categories*

A compartment represents a grouping, such as a work group, department, project, or topic. A classification does not have to have a compartment. In [Figure 1-3](#), the Confidential classification has three exclusive compartments. Public and Max Label have no compartments.

As the figure shows, five labels are defined by this organization.

Trusted Extensions maintains two types of labels: *sensitivity labels* and *clearances*. You can be cleared to work at one or more sensitivity labels. A special label, known as the *user clearance* represents the least upper bound for all of the sensitivity labels that are available to you. In addition, each user has a minimum sensitivity label. This label is used by default when you log in to a multilevel desktop session. You can then choose to work at other labels within this range. A user could be assigned Public as the minimum sensitivity label, and Confidential: Need to Know as the clearance. At first login, the desktop workspaces are at the label Public. During the session, the user can create workspaces at Confidential: Internal Use Only and Confidential: Need to Know.

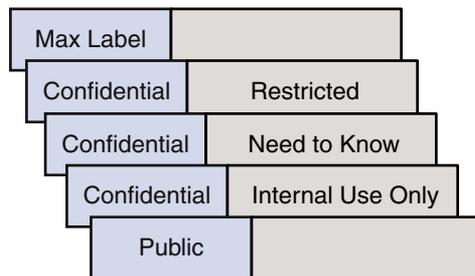


FIGURE 1-3 Typical Industry Sensitivity Labels

All subjects and objects have labels on a system that is configured with Trusted Extensions. A *subject* is an active entity, usually a process. The process 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 can be an object, such as when you use `kill` on a process.

Labels can be displayed in window title bars and in the trusted stripe, which is a special stripe on the screen. Labels can be hidden. Label visibility depends on how your system was configured by the

administrator. Figure 1–4 shows a typical multilevel Trusted Extensions session on a system that is configured to display labels. The labels and trusted stripe are indicated.

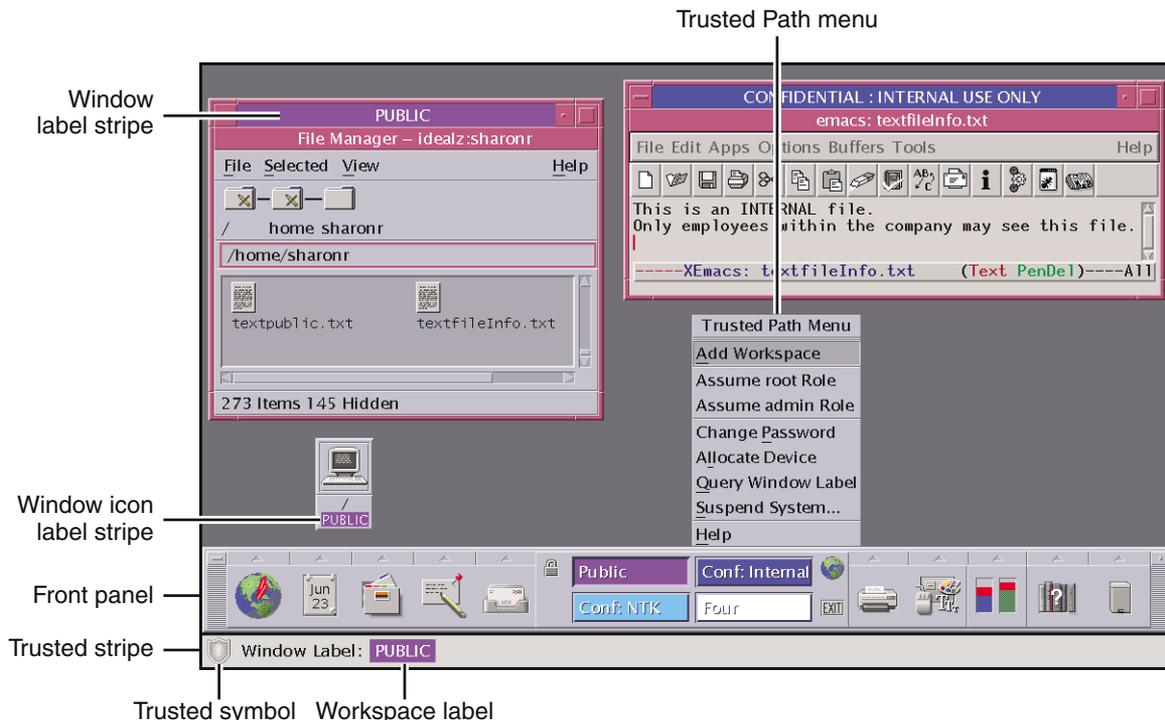


FIGURE 1–4 Typical Solaris Trusted Extensions (CDE) Session

Containers and Labels

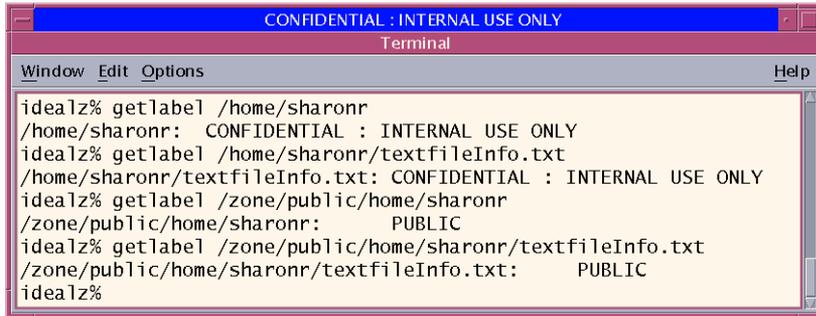
Trusted Extensions uses containers for labeling. Containers are also called zones. The global zone is an administrative zone, so is not available to users. Non-global zones are called labeled zones. Labeled zones are used by users. The global zone shares some system files with users. When these files are visible in a labeled zone, the label of these files is ADMIN_LOW.

Network communication is restricted by label. By default, zones cannot communicate with each other because their labels are different. Therefore, one zone cannot write into another zone.

However, the administrator can configure specific zones to be able to read specific directories from other zones. The other zones could be on the same host, or the zones could be zones on remote systems. For example, a user's home directory in a lower-level zone can be mounted by using the automount service. By convention, the pathname convention for such lower-level home mounts includes the zone name:

/zone/name-of-lower-level-zone/home/username

The following terminal illustrates lower-level home directory visibility. A user whose login label is Confidential : Internal Use Only zone can see the contents of the Public zone when the automount service is configured to make lower-level zones readable. The `textFieldInfo.txt` file has two versions. The Public zone version contains information that can be shared with the public. The Confidential : Internal Use Only version contains information that can be shared within the company only. The contents of the files are shown in Figure 3–11.



```

CONFIDENTIAL : INTERNAL USE ONLY
Terminal
Window Edit Options Help
idealz% getlabel /home/sharonr
/home/sharonr: CONFIDENTIAL : INTERNAL USE ONLY
idealz% getlabel /home/sharonr/textfileInfo.txt
/home/sharonr/textfileInfo.txt: CONFIDENTIAL : INTERNAL USE ONLY
idealz% getlabel /zone/public/home/sharonr
/zone/public/home/sharonr: PUBLIC
idealz% getlabel /zone/public/home/sharonr/textfileInfo.txt
/zone/public/home/sharonr/textfileInfo.txt: PUBLIC
idealz%

```

FIGURE 1-5 Viewing Public Information From the Internal Zone

Labels and Transactions

Trusted Extensions software manages all attempted security-related transactions. The software compares the subject's label with the object's label, then allows or disallows the transaction depending on which label is *dominant*. An entity's label is said to *dominate* another's label if the following two conditions are met:

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

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

For example, consider the following figure.

Classification	Compartments
Top Secret	A B

Four labels can be created from these components:

- TOP SECRET
- TOP SECRET A

- TOP SECRET B
- TOP SECRET AB

TOP SECRET AB dominates itself, and strictly dominates the other possible labels. TOP SECRET A dominates itself, and strictly dominates TOP SECRET. TOP SECRET B dominates itself, and strictly dominates TOP SECRET. TOP SECRET A and TOP SECRET B are disjoint.

In a read transaction, the subject's label must dominate the object's label. This rule ensures that the subject's level of trust meets the requirements for access to the object. That is, the subject's label includes all compartment groupings that are allowed access to the object. TOP SECRET A can read TOP SECRET A and TOP SECRET data. Similarly, TOP SECRET B can read TOP SECRET B and TOP SECRET data. TOP SECRET A cannot read TOP SECRET B data. Nor can TOP SECRET B read TOP SECRET A data. TOP SECRET AB can read the data at all labels.

In a write transaction, that is, when a subject creates or modifies an object, the resulting object's labeled zone must equal the subject's labeled zone. Writes are not allowed from one zone to a different zone.

In practice, subjects and objects in read and write transactions usually have the same label and strict dominance does not have to be considered. For example, a TOP SECRET A subject can create or modify a TOP SECRET A object. In Trusted Extensions, the TOP SECRET A object is in a zone that is labeled TOP SECRET A.

TABLE 1-1 Examples of Label Relationships

	Label 1	Relationship	Label 2
U.S. Government Labels	TOP SECRET AB	(strictly) dominates	SECRET A
	TOP SECRET AB	(strictly) dominates	SECRET A B
	TOP SECRET AB	(strictly) dominates	TOP SECRET A
	TOP SECRET AB	dominates (equals)	TOP SECRET AB
	TOP SECRET AB	is disjoint with	TOP SECRET C
	TOP SECRET AB	is disjoint with	SECRET C
	TOP SECRET AB	is disjoint with	SECRET A B C
Industry Labels	Confidential: Restricted	dominates	Confidential: Need to Know
	Confidential: Restricted	dominates	Confidential: Internal
	Confidential: Restricted	dominates	Public
	Confidential: Need to Know	dominates	Confidential: Internal
	Confidential: Need to Know	dominates	Public

TABLE 1-1 Examples of Label Relationships (Continued)

Label 1	Relationship	Label 2
Confidential: Internal	dominates	Public
Sandbox	is disjoint with	All other labels

When you transfer information between files with different labels, Trusted Extensions displays a confirmation dialog box if you are authorized to change the label of the file. If you are not authorized, Trusted Extensions bars the transaction. The security administrator can authorize you to upgrade information or to downgrade information. For more information, see “[Performing Trusted Actions \(Tasks\)](#)” on page 45.

User Responsibilities for Protecting Data

As a user, you are responsible for setting the permissions to protect your files and directories. Actions that you can perform to set permissions is called discretionary access control (DAC). You can check the permissions on your files and directories by using the `ls -l` command or by using the File Manager, as described in [Chapter 3](#).

Mandatory access control (MAC) is enforced automatically by the system. If you are authorized to upgrade or downgrade labeled information, you have a strong responsibility to ensure that the need for changing the level of information is legitimate.

Another aspect of protecting data involves email. You should never follow instructions that you receive in email from an administrator. For example, if you followed emailed instructions to change your password to a particular value, you would enable the sender to log in to your account. In limited cases, you might verify the instructions independently before following the instructions.

Trusted Extensions Separates Information by Label

Trusted Extensions separates information at different labels by the following means:

- Users can select single-level or multilevel sessions.
- The desktops provide workspaces that are labeled.
- Files are stored in separate zones according to label.
- MAC is enforced for all transactions, including email.
- Objects are cleared prior to reuse.

Single-Level or Multilevel Sessions

When you first log in to a Solaris Trusted Extensions session, you specify whether to operate at a single label or at multiple labels. You then set your *session clearance* or *session label*. This setting is the security level at which you intend to operate.

In a single-label session, you can access only those objects that are equal to your session label or are dominated by the label.

In a multilevel session, you can access information at sensitivity labels that are equal to or lower than your session clearance. You can specify different labels for different workspaces. You can also have different workspaces at the same label.

Session Selection Example

Table 1–2 provides an example of the difference between a single-level and a multilevel session. This example contrasts a user who chooses to operate in a single-level session at CONFIDENTIAL : NEED TO KNOW (CNF : NTK) with a user who chooses a multilevel session, also at CNF : NTK.

The three columns on the left show the user’s session selections at login. Note that users set *session labels* for single-level sessions and *session clearances* for multilevel sessions. The system displays the correct label builder according to your selection.

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

TABLE 1–2 How Session Selections Affect Session Values

User Selections			Session Label Values	
Session Type	Session Label	Session Clearance	Initial Workspace Label	Available Labels
single-level	CNF : NTK	-	CNF : NTK	CNF : NTK
multilevel	-	CNF : NTK	Public	Public CNF : Internal CNF : NTK

In the first row of the table, the user has selected a single-level session with a session label of CNF : NTK. The user has an initial workspace label of CNF : NTK, which is also the only label at which the user can operate.

In the second row of the table, the user has selected a multilevel session with a session clearance of CNF : NTK. The user’s initial workspace label is set to Public, because Public is the lowest possible label in the user’s account label range. The user can switch to any label between Public and CNF : NTK. Public is the minimum label, and CNF : NTK is the session clearance.

Labeled Workspaces

In CDE, the workspaces in Trusted Extensions are accessed through buttons in the center of the front panel, just as in the standard Solaris OS. However, with Trusted Extensions, you can devote a workspace entirely to a single label. This is very convenient when you are in a multilevel session and do not want to confuse information at different labels. The following illustration shows the workspace switch area with four switches. Each switch opens a workspace at a different label. You can also devote several workspaces to the same label.



FIGURE 1-6 Workspace Switch Area

In Sun Java™ Desktop System (Java DS), the workspaces are accessed through buttons at the right of the bottom panel. As in CDE, you can devote a workspace to a single label. You can also assign several workspaces to be at the same label.

Enforcing MAC for Email Transactions

Trusted Extensions enforces mandatory access control for email. You can send email at your current label. You can receive mail at a label within your account range. You can read mail at your current label. In a multilevel session, you can switch to a workspace at a different label to read email at that label.

Clearing Objects Prior to Reuse

Trusted Extensions prevents inadvertent exposure of sensitive information by automatically erasing old information from user-accessible objects prior to reuse. For example, memory and disk space are cleared before being used again. Failure to erase sensitive data prior to reuse of the object risks the exposure of data to inappropriate users. Through device deallocation, Trusted Extensions clears all user-accessible objects prior to allocating the drives to processes. Note, however, that you must clear all removable storage media, such as DVDs and JAZ drives, before allowing another user access to the drive.

Trusted Extensions Enables Secure Administration

In contrast to traditional UNIX systems, the superuser (root) is not used to administer Trusted Extensions. Rather, administrative roles with discrete capabilities administer the system. By this means, no single user can compromise a system's security. A *role* is a special user account that provides access to certain applications with the rights that are necessary for performing the specific tasks. Rights include authorizations, privileges, and effective UIDs/GIDs.

On a system that is configured with Trusted Extensions:

- You are granted access to applications and authorizations on a need-to-use basis.
- You can perform functions that override security policy only if you are granted special authorizations or special privileges by administrators.
- System administration duties are divided among multiple roles.

Getting Access to Applications in Trusted Extensions

In Trusted Extensions, you get access only to those programs that you need to do your job. As in the Solaris OS, an administrator provides access by assigning one or more rights profiles to your account. A *rights profile* is a special package of programs and security attributes. These specific security attributes enable successful use of the program that is in the rights profile.

The Solaris OS provides security attributes such as *privileges* and *authorizations*. Trusted Extensions provides labels. These attributes, if missing, can prevent use of the program, or can prevent use of parts of a program. For example, a rights profile might include an authorization that enables you to read a database. A rights profile with particular security attributes might be required for you to modify the database, or to read information that is classified as Confidential.

The use of rights profiles that contain programs with associated security attributes helps prevent users from misusing programs and from damaging data on the system. If you need to perform tasks that override the security policy, the administrator can assign to you a rights profile that contains the necessary security attributes. If you are prevented from running a certain task, check with your administrator. You might be missing required security attributes.

In addition, your administrator might assign you a profile shell as your login shell. A *profile shell* is a special version of the Bourne shell that provides access to a particular set of applications and capabilities. Profile shells are a feature of the Solaris OS. For details, see the `pfsh(1)` man page.

Note – If you try to run a program and receive a Not Found error message or if you try to run a command and receive a Not in Profile error message, you might not be permitted to use this application. Check with your security administrator.

Roles Administering at Your Site

Trusted Extensions software uses roles for administration. Make sure you know who is performing what set of duties at your site. The following are common roles:

- root role – Is used primarily to prevent direct login by superuser.
- Primary Administrator role – Performs any tasks that require privileges beyond the capabilities of other roles.
- Security Administrator role – Performs security-relevant tasks, such as setting passwords, authorizing device allocation, assigning rights profiles, and evaluating software programs.
- System Administrator role – Performs standard system management tasks, such as setting up home directories, restoring backups, and installing software programs.
- Operator role – Performs system backups, manages printers, and mounts removable media.

Logging In to Trusted Extensions (Tasks)

This chapter describes the desktops and the login process on a system that is configured with Trusted Extensions. The chapter covers the following topics:

- “Desktops and Login in Trusted Extensions” on page 27
- “Trusted Extensions Login Process” on page 28
- “Starting in Trusted Extensions (Tasks)” on page 29

Desktops and Login in Trusted Extensions

The desktop that you use in Trusted Extensions is protected. Labels provide a visible indication of protection. Applications, data, and your communications are labeled.

The login screen is not labeled. The login process requires you to establish a label for your session. Once you have chosen a label, the desktop, its windows, and all applications are labeled. In addition, applications that affect security are visibly protected by a trusted path indicator.

Two desktops are provided for users of Trusted Extensions.

- Solaris Trusted Extensions (CDE) – This desktop is useful for multilevel sessions. In a multilevel session, you can create workspaces at different labels within your accreditation range. CDE can also be used for a single-label session.
- Java Desktop System (Java DS) – This desktop is useful for a single-level session. Java DS includes accessibility features, such as a screen magnifier.

Trusted Extensions Login Process

The login process on a system that is configured with Trusted Extensions is similar to the login process for the Solaris OS. However, in Trusted Extensions, you examine several screens for security-relevant information before the desktop is launched. The process is described in more detail in the material following this overview.

1. Desktop choice – As in the Solaris OS, you choose which desktop to use.
2. Identification – As in the Solaris OS, you type your username in the Username field.
3. Authentication – As in the Solaris OS, you type your password in the Password field.
Successful completion of identification and authentication confirms your right to use the system.
4. Message checking and session type selection – You examine the information in the Last Login dialog box. This dialog box displays the time you last logged in, messages from the administrator, and the security attributes of your session. If you are permitted to operate at more than one label, you can specify the type of session: single-level or multilevel.

Note – If your account restricts you to operate at one label, you cannot specify the type of session. This restriction is called a single-level or single-label configuration.

5. Label selection – In the label builder, you choose the highest security level at which you intend to operate while in your session.

Desktop Choice Before Login

When a Solaris workstation is not in a work session, it displays the login screen. The Trusted Extensions login screen is similar to the Solaris login screen. As in the Solaris login screen, you can choose a desktop from the Options menu.

Identification and Authentication During Login

Identification and authentication are handled by the Solaris OS. The login screen initially contains the username field. This is the *identification* part of the login process.

After you have entered the username, the username dialog box is replaced in the login screen by the password field. This part of the process is referred to as *authentication*. The password authenticates that you are indeed the user who is authorized to use that username.

A *password* is a private combination of keystrokes that validates your identity to the system. Your password is stored in an encrypted form and is not accessible by other users on the system. It is your responsibility to protect your password so that other users cannot use it to gain unauthorized access. Never write your password down or disclose it to anyone else, because a person with your password has access to all your data without being identifiable or accountable. Your initial password is supplied by your [security administrator](#).

Review Security Settings During Login

The review of security settings is handled by Trusted Extensions, not by the Solaris OS. Before login is complete, Trusted Extensions displays the Last Login dialog box. This dialog box provides status information for you to review. You can review past information, such as when the system was last used by you. And you can review the security settings that are in effect for the upcoming session. If your account is configured to operate at more than one label, you can select a single-level or multilevel session.

You then view or choose a label and clearance from the label builder.

Starting in Trusted Extensions (Tasks)

The following tasks step you through logging in to Trusted Extensions. You review and specify security information before reaching the desktop.

▼ Choose a Desktop

If you are working at a single label, you can use either Java DS or Solaris Trusted Extensions (CDE) as your desktop. If you are working on a multilevel system, check with your system administrator about which desktop to use.

- 1 On the login screen, choose a desktop.
 - For CDE, choose Solaris Trusted Extensions (CDE) from the Options --> Sessions menu.
 - For Java DS, choose Java Desktop System, Release 3 from the Options --> Sessions menu.
- 2 Continue with [“Identify Yourself to the System” on page 29](#).

▼ Identify Yourself to the System

- 1 Type your username.

In the username field of the login screen, type your name.

Be sure to type your username exactly as your administrator assigned it to you. Pay attention to spelling and capitalization.
- 2 If you made an error, restart.
 - To retype your username, click **Start Over**.

- **To restart the windowing system completely, click Reset Login from the Options menu.**
Go to [Step 1](#) after your restart.

3 Confirm your entry.

Press Return to confirm your username.



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. There is a chance that you are being spoofed. A spoof is when an intruder’s program is masquerading as a login program to capture passwords. Contact your [security administrator](#) immediately.

4 Continue with “[Authenticate Yourself](#)” on page 30.

▼ **Authenticate Yourself**

1 Type your password in the password entry field.

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

2 Submit the password to the system by pressing Return.

The system compares the login name and password against a list of authorized users.

Troubleshooting If the password that you provided is incorrect, a dialog box appears with the message:

Login incorrect; please try again.

Click OK to dismiss the error dialog box. Then, type the correct password.

▼ **Check Messages and Select Session Type**

If you do not restrict yourself to a single label, you can view data at different labels. The range in which you can operate is bounded at the upper end by the session clearance and at the lower end by the minimum label that your administrator assigned to you.

If the label builder during your login looks different, your site might have replaced the label builder. Check with your administrator.

1 Check that the time of your last session is accurate.

You should always check that there is nothing suspicious about the last login, such as an unusual time of day. If you have reason to believe that the time is not accurate, contact your [security administrator](#).

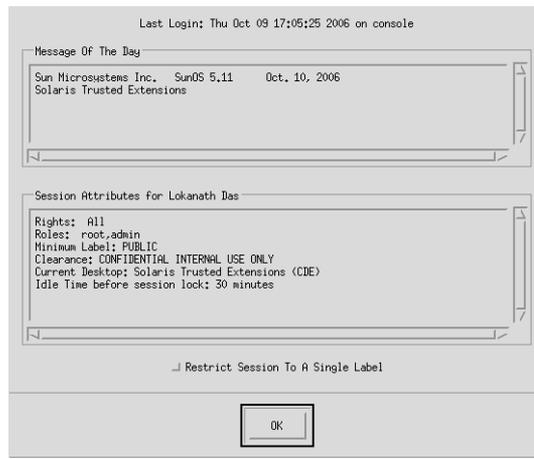


FIGURE 2-1 Last Login Dialog Box

2 Check for any messages from an administrator.

The Message of the Day field can contain warnings about scheduled maintenance or security problems. You should always review the information in this field.

3 Examine the security characteristics of your session.

As shown in [Figure 2-1](#), this dialog box indicates any roles that you can assume, your minimum label, and other security characteristics.

4 (Optional) Decide if you want a single-label session.

Click the Restrict Session to a Single Label button to log in to a single-label session. Depending on your choice in [“Choose a Desktop”](#) on [page 29](#), either Java DS or Solaris Trusted Extensions (CDE) is your desktop for a single-label session.

5 Press Return.

You are presented with a label builder. If you are logging in at a single label, the builder describes your session label. In a multilabel system, the builder enables you to choose your session clearance.

6 Confirm your label choice.

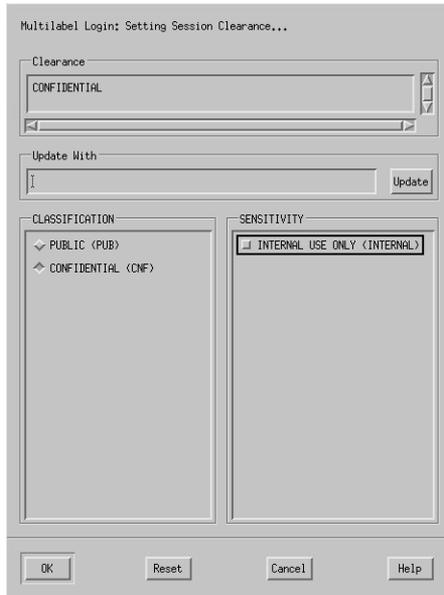


FIGURE 2-2 Label Builder

- **Accept the default unless you have a reason not to.**
 - **For a multilevel session, select a clearance.**
 - Deselect the current clearance, and click a classification and a sensitivity label.
 - Type a clearance name in the Clearance field or the name of the label in the Update With field.
 - **For a single-level session, select a label.**
 - Deselect the current label, and click a different classification.
 - Type a label name in the Update With field.
- 7 Click OK.

▼ Troubleshoot Login Problems

- 1 **If your username or password is not recognized, check with your administrator.**
- 2 **If your label range is not permitted on your workstation, check with your administrator.**
Workstations can be restricted to a limited range of session clearances and labels. For example, a workstation in a lobby might be limited to PUBLIC labels only. If the label or session clearance that you enter is not accepted, check with an administrator to see if the workstation is restricted.

3 If you have customized your shell initialization files and cannot log in, you have two options.

- Contact your **system administrator** to correct the situation.

- **In CDE, if you can become root, you can log in to a failsafe session.**

In a standard login, the shell initialization files are sourced at startup to provide a customized environment. In a failsafe login, the default values are applied to your system and no shell initialization files are sourced.

In Trusted Extensions, failsafe login is protected. Only superuser can access failsafe login.

- a. As in the Solaris OS, choose Options → Failsafe Session on the login screen.**
- b. When prompted, provide your name and password.**
- c. When prompted for an additional password, provide the password for root.**

Working in Trusted Extensions (Tasks)

This chapter covers how to work in Trusted Extensions workspaces. The chapter covers the following topics:

- “Visible Desktop Security in Trusted Extensions” on page 35
- “Trusted Extensions Logout Process” on page 36
- “Working on a Labeled System (Tasks)” on page 37
- “Performing Trusted Actions (Tasks)” on page 45

Visible Desktop Security in Trusted Extensions

Trusted Extensions offers two desktops. Solaris Trusted Extensions (CDE) is for multilevel and single-label sessions. Java Desktop System (Java DS) can be used single-label sessions. Check with your administrator if Java DS can be used for multilevel sessions. Both desktops are labeled. The labels might not be visible when you are working at a single label. The following screen shows a system that is configured to display labels.

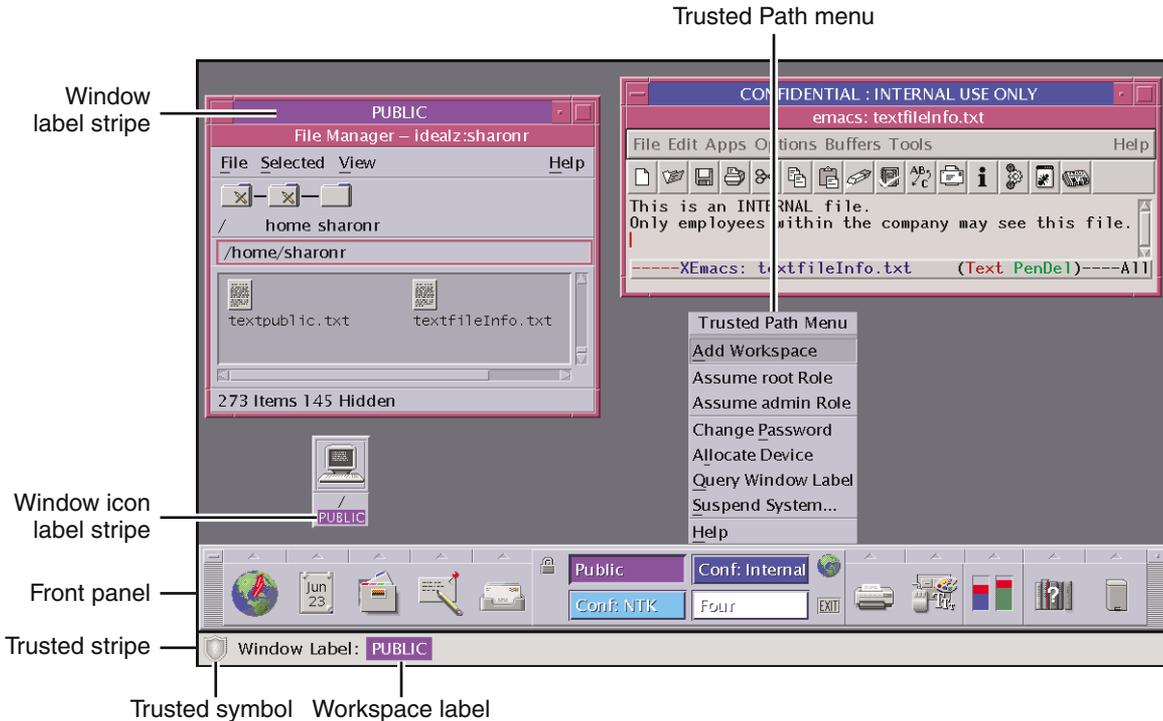


FIGURE 3-1 A Trusted Extensions Desktop

A system that is configured with Trusted Extensions displays the trusted stripe except during login and during screen lock. At all other times, the trusted stripe is visible. In CDE, the stripe is at the bottom of the screen. In Java DS, the stripe is at the top of the screen. The trusted symbol appears on the trusted stripe when you interact with the trusted computing base. When you change your password, for example, you interact with the trusted computing base.

For details about the applications, menus, labels, and features of the desktop, see [Chapter 4](#).

Trusted Extensions Logout Process

A workstation that is logged in to but is left unattended creates a security risk. Make a habit of securing your terminal before you leave your desktop. If you plan to return soon, lock your screen. In most facilities, the desktop becomes unavailable after a specified period of idleness and automatically locks. If you expect to be gone for awhile, or if you expect someone else to use your terminal, log out.

Working on a Labeled System (Tasks)



Caution – If the trusted stripe is missing from your workspace, contact your [security administrator](#). The problem with your system could be serious.

The trusted stripe should not appear during login, or when you lock your screen. If the trusted stripe shows, contact your administrator.

▼ How to Lock and Unlock Your Screen

If you leave the workstation briefly, lock your screen.

1 To lock your screen, do one of the following:

- In CDE, click the screen lock icon in the switch area of the Front Panel.

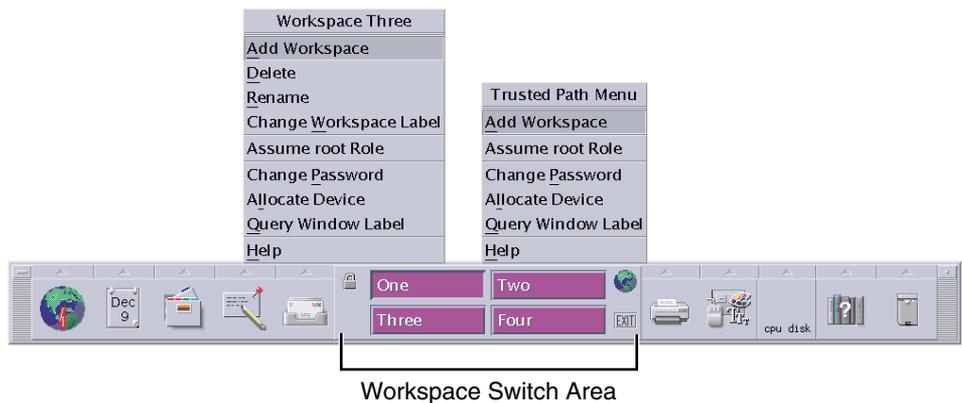


FIGURE 3-2 Front Panel Switch Area

- In Java DS, choose **Lock Screen** from the Launch menu.

The screen turns black. At this point, only you can log in again.

Note – The Trusted Stripe should not be displayed when the screen is locked. If the stripe does appear, notify your [security administrator](#) immediately.

2 To unlock your screen, do the following:

- a. Move your mouse to make the Lock Screen dialog box visible.

b. When the Lock Screen dialog box is visible, type your password

This action returns you to your session in its previous state.

▼ How to Log In Remotely

▶ **Check with your administrator.**

If remote login is permitted, your site has a customized procedure.

▼ How to Log Out of Trusted Extensions

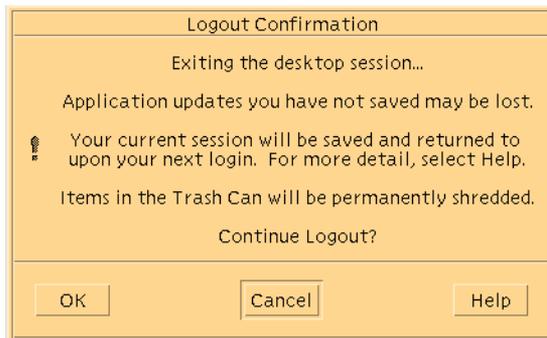
At most sites, the desktop becomes unavailable after a specified period of idleness and automatically locks. If you expect to leave the workstation for awhile, or if you expect someone else to use your workstation, log out.

1 To log out, do one of the following:

▪ **In CDE, click the EXIT icon in the switch area of the Front Panel.**

For a picture, see [Figure 3–2](#).

The Logout Confirmation dialog box is displayed.



▪ **In Java DS, choose Log Out *your-name* from the Launch menu.**

2 Confirm that you want to continue to log out.

▪ **Click OK to log out.**

▪ **Otherwise, click Cancel.**

▼ How to Shut Down Your System

Logging out is the normal way to end a Trusted Extensions session. Use this procedure if you need to turn off your workstation.

Before You Begin You must be using CDE as your desktop.

- 1 **Choose Suspend System from the Workspace Menu.**
Click mouse button 3 over the background to bring up the menu.
- 2 **Confirm what you want to do.**
 - **Click Shutdown to shut down your system.**
 - **Click Suspend to put your system in power-saving mode.**
 - **Otherwise, click Cancel.**

Note – The keyboard combination Stop-A (L1-A) is not available in Trusted Extensions. The security administrator can change this default.

▼ How to View Your Files in a Workspace

You view your files, you use the same applications that you would use in CDE on a Solaris system. If you are working at multiple labels, only the files that are at the label of the workspace are visible.

- 1 **In a CDE workspace, use a terminal or the File Manager.**
 - **Open a terminal and list the contents of your home directory.**
Click mouse button 3 over the background. From the Workspace Menu, choose Programs -> Terminal.
 - **On the Front Panel, click the File Manager.**



FIGURE 3-3 A Labeled File Manager

The File Manager appears with the contents of your home directory at that label.

The File Manager application is launched at the same label as the current workspace. The application provides access to only those files that are at its label. For details about viewing files at different labels, see “Containers and Labels” on page 19.

2 In a Java DS workspace, view your files in a File Browser.

Double-click the Documents folder on your desktop. The folder displays files and folders at the label of your workspace.

▼ How to Find the Trusted Extensions Man Pages

► Review the `Intro(3TSOL)` man page.

a. Open a terminal.

- In CDE, click mouse button 3 on the background. Then choose Programs → Terminal.
- In Java DS, click mouse button 3 on the background. Then choose Open Terminal.

b. Open the Trusted Extensions introductory man page.

```
% man -s 3tsol intro
```

For a list of user commands that are specific to Trusted Extensions, see “Trusted Extensions User Commands” in *Solaris Trusted Extensions Transition Guide*.

For all man pages, see the *Solaris Trusted Extensions Reference Manual*. The man pages are also available from Sun’s [Documentation \(http://www.sun.com/documentation/\)](http://www.sun.com/documentation/) web site.

▼ How to Use Trusted Extensions Online Help

- 1 In CDE, click the Help icon on the Front Panel.

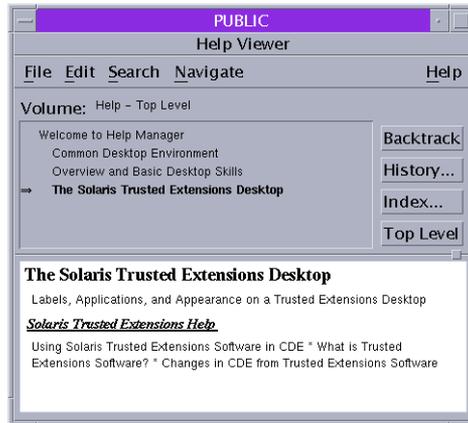


FIGURE 3-4 Trusted Extensions Online Help

- a. In the index, search All Volumes for the word Trusted.
 - b. Click the links to find help that is specific to Trusted Extensions.
- 2 In Java DS, click Help from the Launch menu.

▼ How to Customize the CDE Workspace Menu

Note – In CDE, users and roles can customize the Workspace Menu for each distinct label.

- 1 In your current workspace, start to customize the menu.
 - To add one or more items to the menu, choose the Add Item to Menu ... item. A dialog box with a Browse button appears.
 - To modify the menu or menu properties, choose Customize Menu ... item. A File Manager appears.
- 2 If you are adding items, do the following:
 - a. Find your program.
 - The Browse button shows the files that are available for this workspace at this label.

- b. **Select the program.**
- c. **Repeat for all programs that you want to add to the menu.**
- d. **Close the window.**

The items are added to the top of the menu.

3 If you are modifying the menu, do the following:

- **To remove menu items, use mouse button 3 over the item.**
Select Put in Trash.
- **To change properties, such as permissions, use mouse button 3 over the item.**
Select Properties. You can modify permissions here. You can also view file information and file sensitivity label.

4 Confirm the menu changes or cancel.

- **To cancel your changes, choose File → Close.**
- **To confirm your changes, choose File → Update Workspace Menu,**
The Workspace Menu reflects your changes.

▼ **How to Access Initialization Files at Every Label**

Linking a file or copying a file to another label is useful when you want to make a file with a lower label visible at higher labels. The linked file is only writable at the lower label. The copied file is unique at each label, and can be modified at each label.

Before You Begin You must be logged in to a multilevel session. Your site's security policy must permit linking.

1 Decide which initialization files should be linked to other labels.

2 Create or modify the `~/.link_files` file.

Type your entries one file per line. You can specify paths to subdirectories in your home directory, but you cannot use a leading slash. All paths must be within your home directory.

3 Decide which initialization files should be copied to other labels.

Copying an initialization file is useful when you have an application that always writes to a file with a specific name and you need to separate the data at different labels.

4 Create or modify the ~/.copy_files file.

Type your entries one file per line. You can specify paths to subdirectories in your home directory, but you cannot use a leading slash. All paths must be within your home directory.

Example 3-1 Creating a .copy_files File

In this example, the user wants to customize several initialization files per label. In her organization, a company web server is available at the Restricted level. So, she sets different initial settings in the .mozilla file at the Restricted level. Similarly, she has special templates and aliases at the Restricted level. So, she modifies the .aliases and .soffice initialization files at the Restricted level. She can easily modify these files after creating the .copy_files file at her lowest label.

```
# .copy_files
# Copy these files to my home directory in every zone
.aliases
.mozilla
.soffice
```

Example 3-2 Creating a .link_files File

In this example, the user wants her mail defaults and shell defaults to be identical at all labels.

```
# .link_files
# Link these files to my home directory in every zone
.cshrc
.mailrc
```

Troubleshooting These files do not have safeguards for dealing with anomalies. Duplicate entries in both files or file entries that already exist at other labels can cause errors. Work with your administrator when modifying these files.

▼ How to Interactively Display a Window Label

This operation can be useful when your system is not configured to display labels in the window frames.

1 Choose Query Window Label from the Trusted Path menu.

The pointer changes to a question mark.

2 Move the pointer around the screen.

The label for the region under the pointer is displayed in a small rectangular box at the center of the screen.

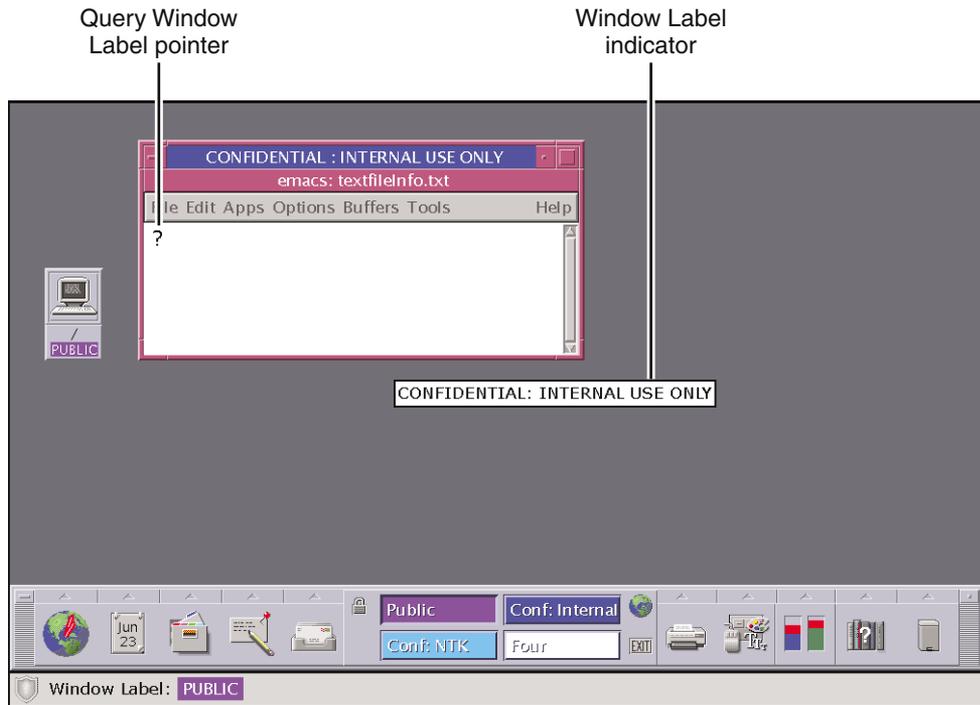


FIGURE 3-5 Query Window Label Operation

- 3 Click the mouse button to return to normal mode.

▼ How to Do Some Common Desktop Tasks

Some common tasks are affected by labels and security. In particular, the following tasks are affected by Trusted Extensions.

- 1 Empty the trash.

The trash can contains files only at the label of the workspace. Delete sensitive information as soon as the information is in the trash can.

- **In CDE, open the Trash Can on the Front Panel.**
Choose File -> Select All, then File -> Shred. Then, confirm.
- **In Java DS, click mouse button 3 over the Trash Can icon on the desktop.**
Choose Empty Trash, then confirm.

2 In CDE, restore the Front Panel.

Click the trusted stripe to restore a minimized Front Panel.

3 On both desktops, save a customized desktop at every label.

You can customize the workspace configuration for every label at which you log in. First, set up the desktop.

- **In CDE, open the Style Manager. Choose your settings in the Startup icon.**

Note – The Style Manager requires the trusted path. Run the Style Manager from the Front Panel or from the Workspace Menu, where the Style Manager has the trusted path.

Your desktop is restored in this configuration when you next log in at this label.

Tip – Repeat this step for every label at which you log in.

- **In Java DS, when you log out, choose to save the current configuration.**

Your desktop is restored in this configuration when you next log in at this label.

Tip – Save a configuration for every label at which you log in.

4 Find calendar events at every label.

Calendars show only the events at the label of the workspace that launched the calendar.

- **In a multilevel session, launch your calendar from a workspace that has a different label.**
- **In a single-level session, log out. Then, log in at a different label to see the calendar events at that label.**

Performing Trusted Actions (Tasks)

The following security-related tasks require the trusted path.



Caution – If the trusted symbol is missing when you are attempting a security-related action, contact your [security administrator](#) at once. The problem on your system could be serious.

▼ How to Change Your Password

Unlike the Solaris OS, Trusted Extensions provides a GUI for changing your password. The GUI grabs the pointer until the password operation is completed.

1 Choose Change Password from the Trusted Path menu.

2 Type your current password.

This action confirms that you are the legitimate user for this user name. For security, the password is not displayed as you type.



Caution – When you enter your password, make sure that the cursor is over the Change Password dialog box and that the trusted symbol is displayed. If the cursor is not over the dialog box, you might inadvertently type your password into a different window where the password could be seen by another user. If the symbol is not displayed, then someone might be attempting to steal your password. Contact your [security administrator](#) at once.

3 Type the new password.

4 Confirm the password.

Type the password again.

▼ **How to Log In at a Different Label**

The label of the first workspace that comes up in subsequent login sessions after the first login can be set to any label within your label range.

Users can configure the startup session characteristics by using the Startup dialog box in the Tools subpanel on the Front Panel.

Before You Begin You must be logged in to a multilevel session.

1 Create workspaces at every label.

2 Configure each workspace as you want the workspace to appear.

3 Go to the workspace that you want to see when you log in.

4 In the Startup dialog box, set the Home session to the current workspace.

▼ **How to Allocate a Device**

Before You Begin The Allocate Device menu item is available to authorized users only. The menu item enables you to mount and allocate a device for your exclusive use. If you try to use a device without allocating it, you get the error message “Permission Denied”.

1 Choose Allocate Device from the Trusted Path menu

Or, in CDE, choose Device Allocation Manager from the Tools subpanel in the Front Panel.

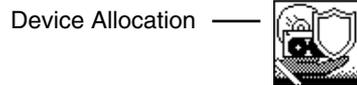


FIGURE 3-6 Device Allocation Icon

The Device Allocation Manager is displayed.

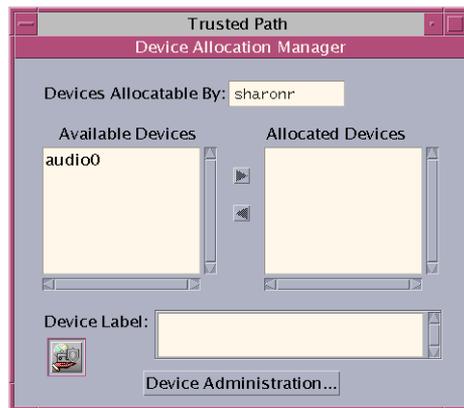


FIGURE 3-7 Device Allocation Manager

2 Find the device that you want to use.

The devices that you are permitted to allocate at your current label appear in the device allocation list.

- `audion` means a microphone and speakers
- `cdromn` means a CD-ROM drive
- `floppyn` means a diskette drive
- `mag_tapen` means a tape drive (streaming)
- `rmdiskn` means a JAZ or ZIP drive, a DVD drive, or USB hot-pluggable media

3 Select the device.

Move the device from the Available Devices list to the Allocated Devices list. You can double-click the device name in the Available Devices list. Or, select the device and click the Allocate button that points to the right.

This step starts the clean script. The clean script ensures that no data from other transactions remains on the media.

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

4 Follow the instructions.

The instructions ensure that the media has the correct label. Then, the device is mounted. The device name now appears in the Allocated Devices list.

5 Use the device to transfer data.

6 Deallocate the device.

When you are finished, release the device by double-clicking the device name in the Allocated Devices list. You can also select the device and click the Deallocate button.

For security, you should always deallocate a device when you are finished with the device. Device deallocation runs a clean script. The script unmounts the device and advises you when the media can be removed.

Note – If you reboot your system while devices are allocated, the devices become deallocated.

Example 3–3 Allocating an Audio Device

In this example, a user allocates the audio device on her system. When she moves the audio device to the Allocated Device list, the following message appears:



The device is allocated at the label `Confidential : Internal Use Only`. She sees the label when she selects the device in the Allocated Device Field.



When she is through with the audio device, she deallocates it. The system reminds her to turn the microphone off.



Troubleshooting If the device that you want to use does not appear in the list, check with your administrator. The device could be in an error state or in use by someone else. Or, you might not be authorized to use the device.

If you switch to a different role workspace or to a workspace at a different label, the allocated device cannot work at that label. To use the device at the new label, you need to deallocate the device at the initial label, and then allocate the device at the new label. In CDE, when you use the Occupy Workspace command from the window menu to move the Device Allocation Manager to the new workspace, the Available and Allocated Devices lists change to reflect the correct context. The Move to Another Workspace menu item in Java DS works similarly.

▼ How to Assume a Role

Unlike the Solaris OS, Trusted Extensions provides a GUI for assuming a role.

- 1 In CDE, bring up the Trusted Path menu from the center of the Front Panel.
- 2 Choose Assume *rolename* Role.

3 Type the role password.

This action confirms that you can legitimately assume this role. For security, the password is not displayed as you type.



Caution – When you enter your password, make sure that the cursor is over the Change Password dialog box and that the trusted symbol is displayed. If the cursor is not over the dialog box, you might inadvertently type your password into a different window where the password could be seen by another user. If the symbol is not displayed, then someone might be attempting to steal your password. Contact your [security administrator](#) at once.

After the role password is accepted, the software places you in a role workspace. You are in the global zone. You can perform the tasks that are permitted by the rights profiles in your role.

▼ How to Work at a Different Label

The ability to set workspace labels in Trusted Extensions provides a convenient means of working at different labels within the same session.

Before You Begin You must be logged in to a multilevel session.

- 1 To work in the same workspace, see “How to Change the Label of a Workspace” on page 50.
- 2 To work in a different workspace, see “How to Add a Workspace at a Particular Label” on page 51.



FIGURE 3-8 Front Panel With Switches at Different Labels

Troubleshooting If you are logged in to a single-level session, you must log out to work at a different label. Then, log in at the desired label. If you are permitted, you can also log in to a multilevel session.

▼ How to Change the Label of a Workspace

The ability to set workspace labels in Trusted Extensions provides a convenient means of working at different labels within the same session.

Before You Begin You must be logged in to a multilevel session.

- 1 Click mouse button 3 over the workspace button.
- 2 Choose Change Workspace Label.

3 Choose a label from the label builder.

The workspace label is changed to the new label. Windows and applications that were invoked before the label change continue to run at the previous label. The trusted stripe indicates the new label. In a system where labels are color-coded, new windows are marked with the new color. In CDE, the workspace button is color-coded.

▼ How to Add a Workspace at a Particular Label

You can add a workspace at your minimum label, or at the label of an existing workspace.

Tip – When logged into a multilevel session in CDE, rename each workspace button to reflect the label of the workspace.

Before You Begin You must be logged in to a multilevel session.

1 To create a workspace at your minimum label, do the following:

- **Click mouse button 3 over the Workspace Switch Area.**
- **Choose Add Workspace.**
The workspace is created at your minimum label.
- **(Optional) Rename the workspace.**
Change the workspace button name.

2 To create a workspace at the label of an existing workspace, do the following:



- **Click mouse button 3 over the workspace button.**
- **Choose Add Workspace.**
The workspace is created at the label of the workspace button.

3 (Optional) Rename the workspace.

Change the workspace button name.

▼ How to Switch to a Workspace at a Different Label

1 In CDE, click the workspace switch at that label.

- To create a workspace at a different label, see “How to Add a Workspace at a Particular Label” on page 51.
- To add a workspace at the same label, place the pointer over the workspace switch. Then, from the Trusted Path menu, choose Add Workspace.

2 In Java DS, select the workspace box on the bottom panel. You are now in that labeled workspace.

▼ How to Move a Window to a Different Workspace

Windows that are moved retain their original label. Any actions that are done in those windows are done at the label of the window, not at the label of the containing workspace. Moving a window is useful when you want to compare information. You might also want to use applications at different labels without moving between workspaces.

1 In CDE, use the Occupy Workspace menu.

- a. From the application’s window menu, choose Occupy Workspace.



FIGURE 3-9 Selecting Occupy Workspace

- b. Choose a workspace at a different label and click OK.

This action moves the application to a workspace that has a different label. Note that the Occupy Workspace dialog box has the label Trusted Path. The label indicates that occupying a workspace affects the trusted computing base.

The following figure shows terminals at different labels that occupy one workspace.

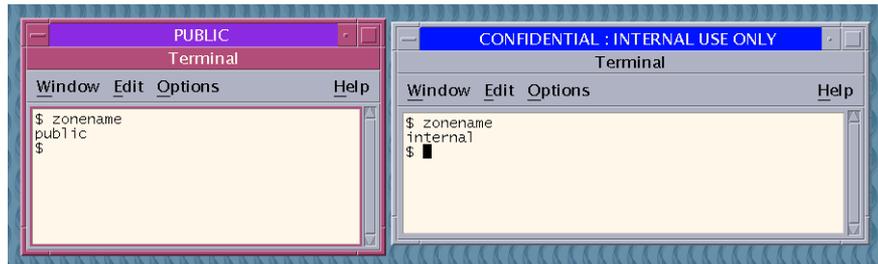


FIGURE 3-10 Differently Labeled Windows in One Workspace

- 2 In Java DS, use the **Move to Another Workspace** menu item.

▼ How to Determine the Label of a File

Usually the label of a file is obvious. However, if you are allowed to view files at a lower level than your current workspace, the label of a file might not be obvious. In particular, the label of a file can be different from the label of the File Manager.

- 1 In CDE, use the **File Manager**.
 - **Use the File -> Properties menu item on the selected file.**
One of the properties of the selected file is its Sensitivity Label.
 - **Drag the file from the containing File Manager onto the desktop.**
The file icon displays the label of the file.
- 2 In Java DS, use the **File Browser**.
- 3 You can also use the **Query Label** menu item from the **Trusted Path** menu.

▼ How to Move Data Between Labels

As on a standard Solaris system, you can move data between windows in Trusted Extensions. However, the data must be at the same label. When you transfer information between windows with different labels, you are upgrading or downgrading the sensitivity of that information.

Before You Begin Your site's security policy must permit this type of transfer, and you must be authorized to move data between labels. To assign you the authorization, your administrator completed the following task, "How to Enable a User to Change the Security Level of Data" in *Solaris Trusted Extensions Administrator's Procedures*.

You must be logged in to a multilevel session.

1 Create workspaces at both labels.

For details, see “How to Add a Workspace at a Particular Label” on page 51.

2 Confirm the label of the source file.

For details, see “How to Determine the Label of a File” on page 53.

3 Move the window with the source information to a workspace at the target label.

For details, see “How to Move a Window to a Different Workspace” on page 52.

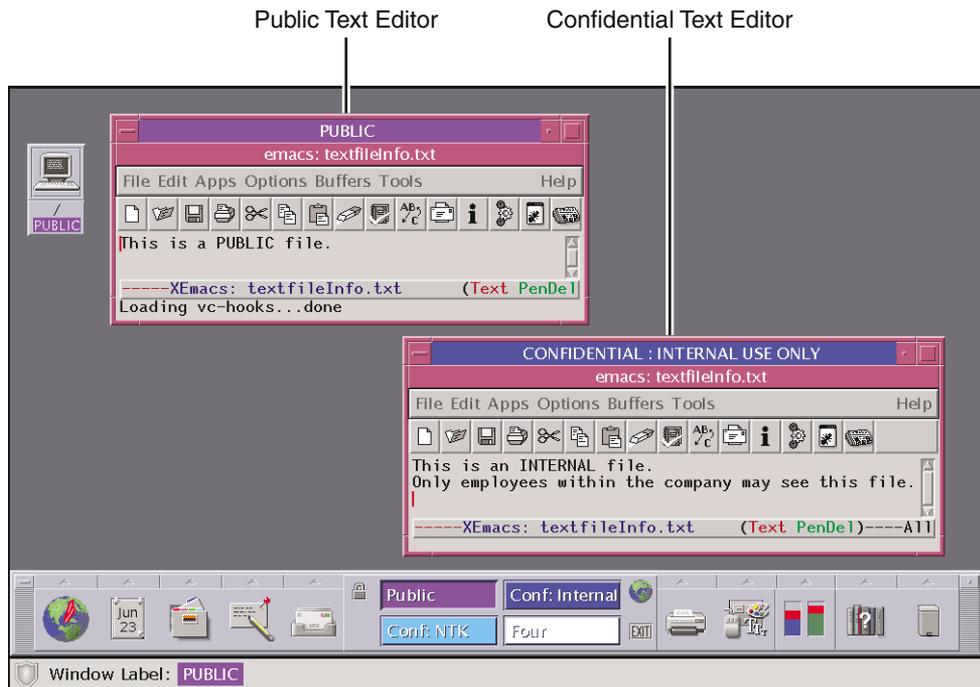


FIGURE 3-11 Displaying Applications at Different Labels

4 Highlight the information to be moved, and paste the selection in the target window.

The Selection Manager Confirmation dialog box is displayed.

5 Review the Selection Manager Confirmation dialog box.

The Selection Manager Confirmation dialog box contains the following information:

- Describes why confirmation of the transaction is needed.
- Identifies the label and the owner of the source file.

- Identifies the label and owner of the destination file.
- Identifies the type of data that was selected for transfer, the type of the target file, and the size of the data in bytes. You can view the selected data in text or hexadecimal format. Or, you can choose None to hide the data altogether.
- Indicates the time that remains for you to complete the transaction. The amount of time and the use of the timer depends on your site's configuration.

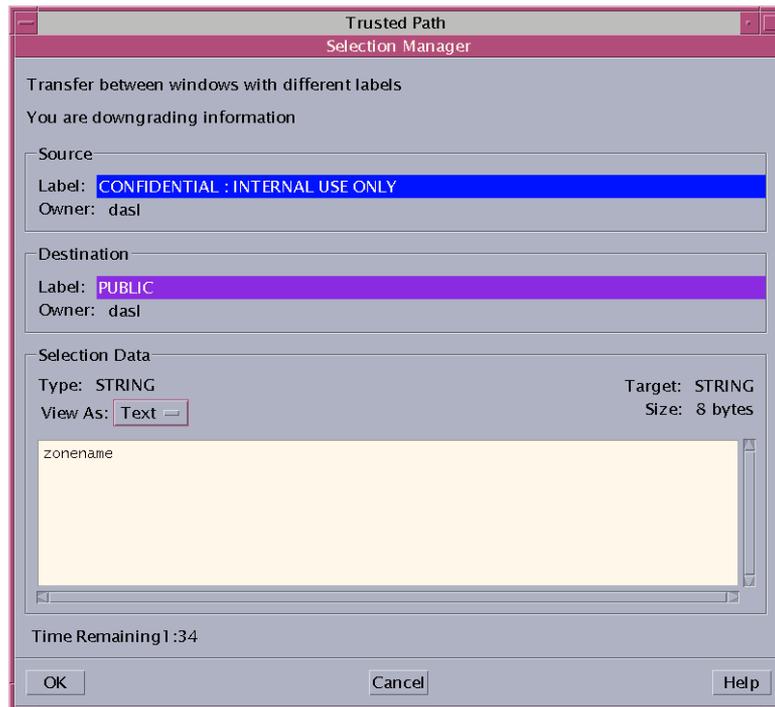


FIGURE 3-12 Selection Manager Confirmation Dialog Box

- 6 Confirm that the label of the data should change.
 - Click **Cancel** to stop the transaction.
 - Otherwise, click **OK**.

▼ How to Move Files Between Labels

As on a standard Solaris system, you can move files in Trusted Extensions. When you move a file to a different label, you are upgrading or downgrading the sensitivity of the information that is in the file.

Before You Begin Your site’s security policy must permit this type of transfer, and you must be authorized to move files between labels. For you to get the authorization, your administrator has completed the following task, “How to Enable a User to Change the Security Level of Data” in *Solaris Trusted Extensions Administrator’s Procedures*.

You must be logged in to a multilevel session. The file must be closed. Check that no one else is using the file whose label is to be changed. This procedure details the steps in CDE. In Java DS, use the File Browser.

1 Create workspaces at both labels.

For details, see “How to Add a Workspace at a Particular Label” on page 51.

2 Open File Managers at both labels.

For details, see “How to View Your Files in a Workspace” on page 39.

3 In the source File Manager, navigate to the file whose label is to change.

4 In the target File Manager, navigate to the file’s new directory.

5 Move the File Managers into one workspace.

For details, see “How to Move a Window to a Different Workspace” on page 52.

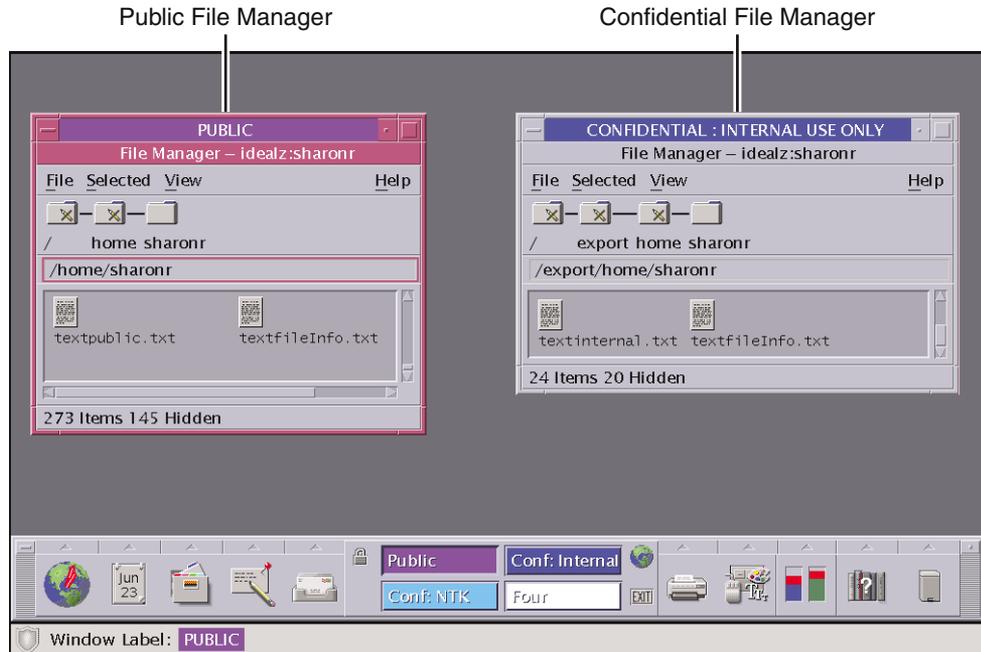


FIGURE 3-13 Displaying File Managers at Different Labels

6 Drag the file to the target directory, and drop the file.

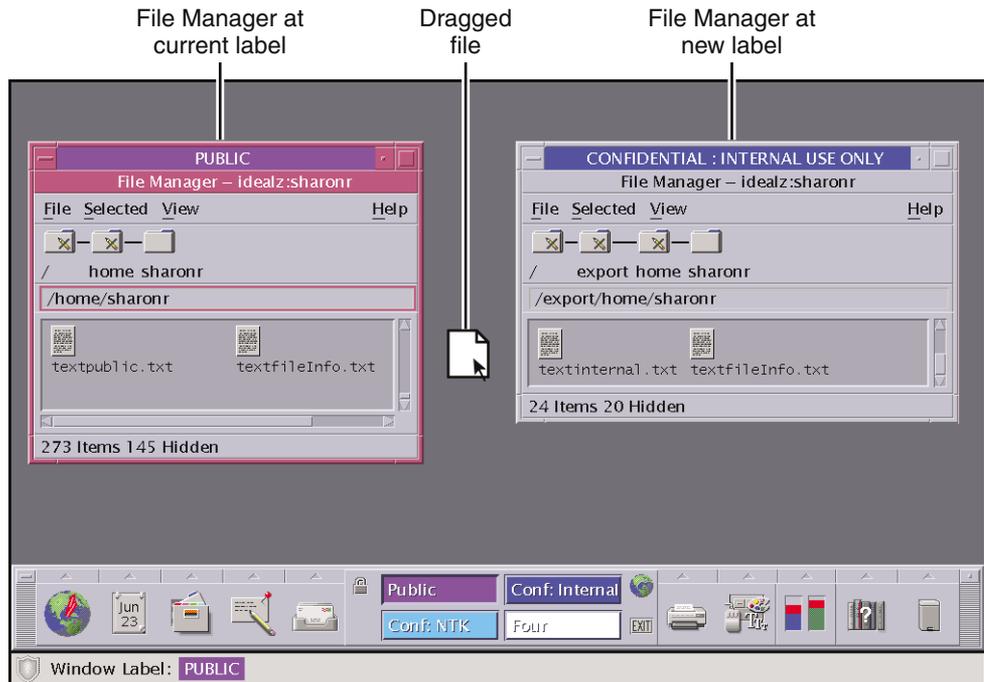


FIGURE 3-14 Dragging a File Between File Managers at Different Labels

The File Manager Confirmation dialog box is displayed.

This dialog box is similar to the Selection Manager Confirmation dialog box, but does not include a timer.

- Describes why confirmation of the transaction is needed.
- Identifies the label and the owner of the source file.
- Identifies the label and owner of the destination file.
- Identifies the type of data that was selected for transfer, the type of the target file, and the size of the data in bytes.

By resetting the View As menu, you affect the displays of subsequent transfers. Choose None for selections that consist of unreadable data.

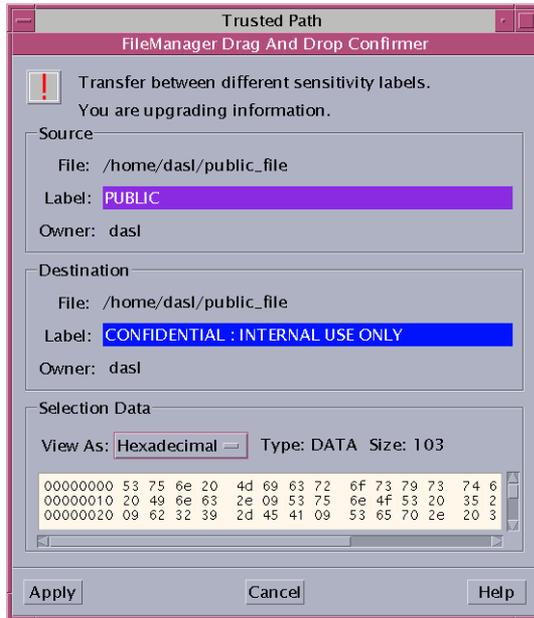


FIGURE 3-15 File Manager Confirmation Dialog Box

7 Confirm that the label of the file should change.

- Click **Cancel** to stop the transaction.
- Click **Apply** to move the file to the new label.

Troubleshooting If your system is not configured to permit upgrading or downgrading labels, a dialog box is displayed. If the box states that the transfer is not authorized, check with your administrator.

▼ How to Link a File to a Different Label

Linking a file to another label is useful when you want to make a file with a lower label visible at higher labels. The file is only writable at the lower label.

Before You Begin Your site's security policy must permit linking, and you must be authorized to link files between labels. To get the authorization, your administrator completed the following task, "How to Enable a User to Change the Security Level of Data" in *Solaris Trusted Extensions Administrator's Procedures*.

You must be logged in to a multilevel session. The file must be closed. Check that no one else is using the file whose label is to be changed.

1 Configure the workspace for the linking operation.

Follow [Step 1](#) through [Step 5](#) in “[How to Move Files Between Labels](#)” on page 55.

2 Link the file.

Press Shift and Control while dragging the file icon from the source File Manager to the target File Manager.

3 Confirm the link.

For a description of your options, see the text that describes [Figure 3–15](#).

◆ ◆ ◆ CHAPTER 4

Elements of Trusted Extensions

This chapter explains the key elements of Trusted Extensions. The chapter discusses these topics:

- “Basics of Trusted Extensions” on page 61
- “Files and Applications in Trusted Extensions” on page 64
- “Password Security” on page 65
- “Front Panel Security (CDE)” on page 66

Basics of Trusted Extensions

After you have successfully completed the login process, you can work within Trusted Extensions. Your work is subject to security restrictions. Restrictions that are specific to Trusted Extensions include the label range of the system, your clearance, and your choice of a single-level or multilevel session. As the following figure illustrates, four features distinguish a system that is configured with Trusted Extensions from a Solaris system.

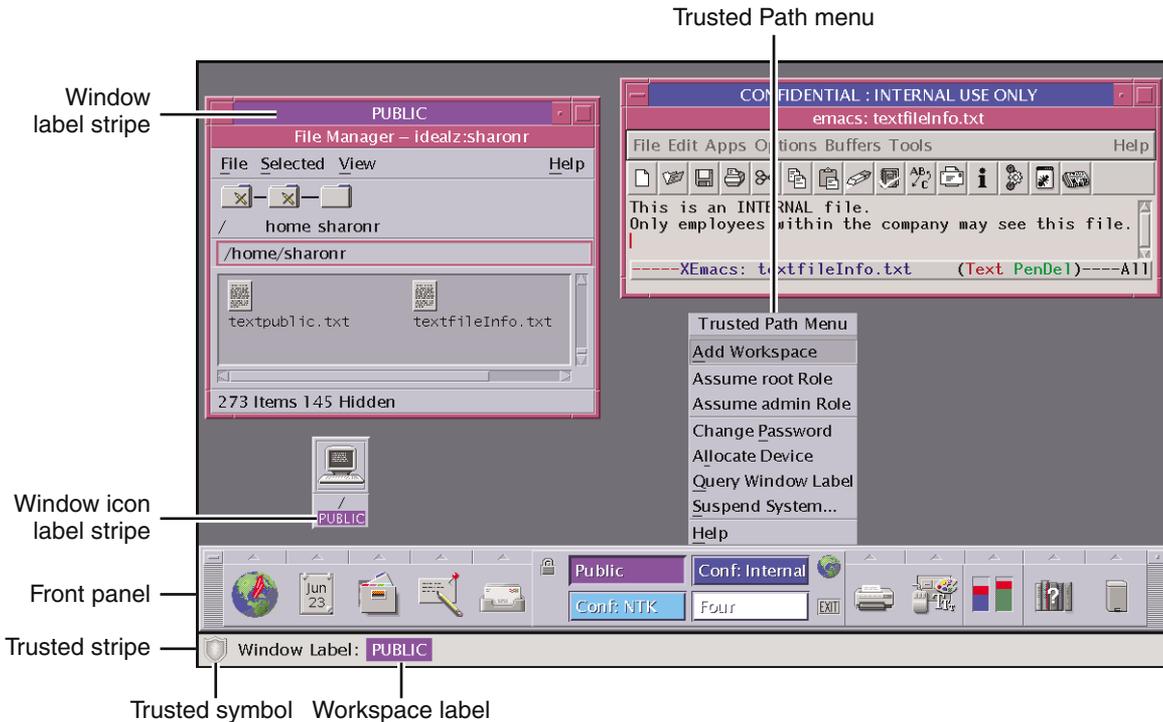


FIGURE 4-1 Solaris Trusted Extensions Multilevel CDE Desktop

- Label displays – All windows, workspaces, files, and applications have a label. The graphical interface provides stripes and other indicators for viewing an entity’s label.
- Trusted stripe – Is a special graphical security mechanism. In CDE, the *trusted stripe* is always displayed at the bottom of the screen. In Java DS, the stripe can be at the top of the screen.
- Limited access to applications from the workspace – The workspace provides access only to those applications permitted in your user account.
- Trusted Path menu – In CDE, the switch area in the Front Panel provides access to the Trusted Path pop-up menu for performing security-related tasks.

Labels on Trusted Extensions Desktops

As discussed in “Mandatory Access Control” on page 17, all applications and files in Trusted Extensions have labels. Trusted Extensions displays labels in several places:

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

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

Figure 4–1 shows how labels display on a system that configured to display labels. The system is using CDE as its desktop. A site can also be configured to hide labels. Even if your administrator has configured the system to hide labels, labeling is still in effect. The Query Window Label menu item can be used to display the label of a window. For an illustration, see Figure 3–5.

Trusted Stripe

In CDE, the *trusted stripe* appears in a reserved area at the bottom of the screen in all Trusted Extensions sessions. In Java DS, the trusted stripe can appear at the top of the screen.

The purpose of the trusted stripe is to give you a visual confirmation that you are in a legitimate Trusted Extensions session. The stripe indicates when you are interacting with the trusted computing base. The stripe also displays the labels of your current workspace and current window. The trusted stripe cannot be moved or be obscured by other windows or dialog boxes. The trusted stripe has two elements:

- The trusted symbol – Displays when screen focus is security-related
- The window label – Optional. Displays label of active window

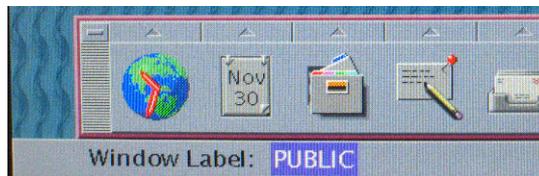


FIGURE 4–2 PUBLIC Window Label in the Trusted Stripe

Trusted Symbol

Whenever you access any portion of the trusted computing base, the *trusted symbol* appears at the left of the trusted stripe area. If your configuration suppresses labels, then the trusted symbol appears with the trusted stripe. In CDE, the symbol appears to the left of the Front Panel.



The trusted symbol is not displayed when the pointer is focused in a window or area of the screen that does not affect security. The trusted symbol cannot be forged. If you see the symbol, you can be sure that you are safely interacting with the trusted computing base.



Caution – If the trusted stripe is missing from your workspace, or if the trusted symbol is missing when you are attempting a security-related action, notify your Trusted Extensions administrator at once. The problem on your system could be serious. If the trusted stripe is visible when you lock your screen, notify your Trusted Extensions administrator at once.

Window Label Indicator

The *Window Label* indicator displays the label of the active window. In a multilevel session, the indicator can help identify windows with different labels in the same workspace. The indicator can also show that you are interacting with the trusted computing base. For example, when you change your password, the Trusted Path indicator displays in the trusted stripe.

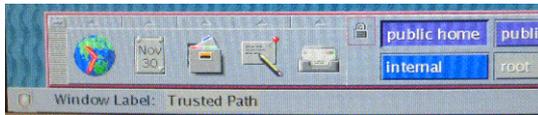


FIGURE 4-3 Trusted Path Indicator in the Trusted Stripe

Files and Applications in Trusted Extensions

All applications in Trusted Extensions have sensitivity. Applications are *subjects* in any data transactions. Subjects must dominate the *objects* that the subjects try to access. Objects can be files, and sometimes can be other processes. The label information for an application is displayed in the window label stripe. The label is visible when a window is open and when the window is minimized. An application's label also appears in the trusted stripe when the pointer is in the application's window.

Files are objects in data transactions in Trusted Extensions. Files can only be accessed by applications whose labels dominate the files' labels. A file can be viewed from windows that have the same label as the file.

Some applications use initialization files to configure the environment for the user. Two special files in your home directory help you access initialization files at every label. These files enable an application at one label to use an initialization file that originates in a directory at a different label. The two special files are `.copy_files` and `.link_files`.

`.copy_files` File

`.copy_files` stores file names to be copied when you first change to a workspace with a higher label.

`.copy_files` is stored in your home directory at your minimum label. This file is useful when you have an application that always writes to a file in your home directory with a specific name.

`.copy_files` enables you to enable the application to update the file at every label.

.link_files File

.link_files stores file names to be linked when you first change to a workspace with a higher label. .link_files is stored in your home directory at your minimum label. This file is useful when a specific file needs to be available at multiple labels, but the content should be identical at every label.

Password Security

Users who change passwords on a frequent basis shorten the window of opportunity for intruders to use illegally obtained passwords. Therefore, your site's policy can require you to change your password regularly. The Solaris OS can set content requirements for passwords, and can enforce resetting requirements. The following are possible resetting requirements:

- 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 preceding options, you should receive a message that warns you to change your password prior to the cutoff date.

Passwords can have content criteria. At minimum, passwords in the Solaris OS must meet the following standards:

- The password must be at least eight characters long.
- The password must contain at least two alphabetic characters and at least one numeric character or one 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, uppercase letters and lowercase letters are considered to be equal.
- The new password must have at least three characters that are different from the old password. For this comparison, uppercase letters and lowercase letters are considered to be equal.
- The password should be difficult to guess. Do not use a common word or a proper name. Programs and individuals who try to break into an account can use lists to try to guess users' passwords.

You can change your password from the Change Password menu item. For the steps, see [“Performing Trusted Actions \(Tasks\)”](#) on page 45.

Front Panel Security (CDE)

The Front Panel in Solaris Trusted Extensions (CDE) is very similar to the Front Panel that is used in standard CDE. The Trusted Extensions Front Panel restricts access to only those applications, files, and utilities that you are allowed to use. By clicking mouse button 3 anywhere in the workspace switch area, the [Trusted Path menu](#) is displayed.

Before you can access a device through the Removable Media Manager, that device must be allocated using the Device Allocation Manager. The Device Allocation Manager is accessed from the Tools subpanel, which is above the Style Manager icon in the Front Panel.

Tip – If you minimize the Front Panel, you can restore the panel by clicking anywhere in the Trusted Stripe.

In Trusted Extensions, Install Icon dropsites are limited to the applications and files that you are permitted to use at the label of the current workspace.

For more information on standard CDE, see the *Common Desktop Environment User's Guide*.

Workspace Switch Area

In Trusted Extensions, the workspace buttons not only define separate workspaces, but also require you work at particular labels. When you begin a multilevel session, each workspace is set to the lowest label that you can use. If your administrator has color-coded the labels at your site, the workspace buttons display the color of the label. The Trusted Path menu is available from the workspace switch area.

Trusted Path Menu

The Trusted Path menu contains menu items that affect security.

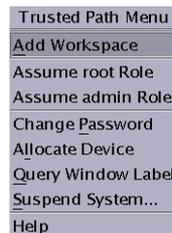


FIGURE 4-4 Trusted Path Menu – Basic

For example, you change your password with this menu. You can allocate devices with this menu. For details, see “[Performing Trusted Actions \(Tasks\)](#)” on page 45.

The Trusted Path menu has two versions. The *Workspace Name* version includes workspace options. The selections that appear in your menu depend on how the administrator configured your account.



FIGURE 4-5 Trusted Path Menu - *Workspace Name* Version

Clock Security

In Trusted Extensions, only an administrator can change the date and time for your workstation.

Calendar Security

The calendar shows the appointments for you at the label of your current workspace only. To view appointments at a different label, you need to open the calendar at that label.

File Manager Security

In Trusted Extensions, the File Manager displays files at the label of the current workspace. To view files at more than one label at a time, you run File Manager from workspaces at different labels. You then use the Occupy Workspace command to display the different File Managers in the same workspace.

The File Manager enables you to change a file or folder's basic permissions and access control list (ACL). If you are authorized, you can also move or link files between File Managers at different labels. For details on File Manager use, see [“How to View Your Files in a Workspace”](#) on page 39 and [“Performing Trusted Actions \(Tasks\)”](#) on page 45.

Text Editor Security

The Text Editor can edit files at the label of the current workspace only. If you are authorized, you can copy information between text editors at different labels.

Personal Applications Subpanel

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

Mailer Security

In Trusted Extensions, all mail messages are labeled. When you send a message, the message goes out at the label of your mail tool. Only hosts and users that are cleared for that label receive the message. Only users who are working at that label can see the message.

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

Printer Security

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

A typical print job in Trusted Extensions includes labels and extra pages:

- A banner page at the beginning of the print job identifies the print job, handling instructions and labels that are appropriate to the site
- Body pages are labeled at the header and the footer
- A trailer page at the end of the print job signals the end of the job

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

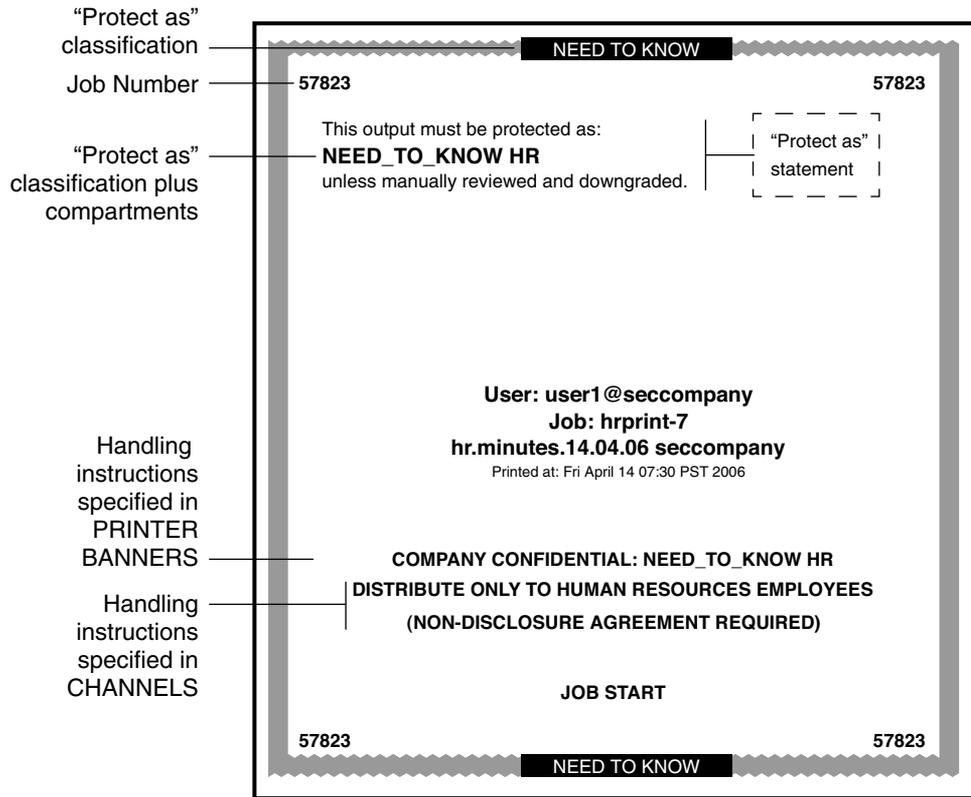


FIGURE 4-6 Typical Print Banner Page

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

Style Manager Security

With three exceptions, the Style Manager operates in the same manner as it operates on a Solaris system.

- The Style Manager cannot be run from the Application Manager when Trusted Extensions is configured, because the Style Manager requires the trusted path. Run the Style Manager from the Front Panel and the Workspace menu, where the Style Manager has the trusted path.
- 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. You cannot increase the idle time above the maximum. You can still choose a pattern for when the screen is locked. See your administrator if you are not familiar with the policy at your site.

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

Application Manager Security

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

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

Trash Can Security

In Trusted Extensions, the trash can stores files to be deleted by label. Although you can drop files at any label in the trash can, the trash can displays files at the current label only. You should delete sensitive information as soon as the information is in the trash can.

Glossary

access control list (ACL)	A security feature of the Solaris OS. An ACL extends discretionary access control (DAC) to use a list of permission specifications (ACL entries) that apply to specific users and specific groups. An ACL allows finer-grained control than the control that standard UNIX permissions provides.
access permission	A security feature of most computer systems. Access permission gives the user the right to read, write, execute, or view the name of a file or directory. See also discretionary access control (DAC) and mandatory access control (MAC) .
account label range	The set of labels that are assigned by the security administrator to a user or role for working on a system that is configured with Trusted Extensions. A label range is defined at the upper end by the user clearance and at the lower end by the user's minimum label . The set is limited to well-formed labels .
accreditation range	A set of labels that are approved for a class of users or resources. See also system accreditation range , user accreditation range , label encodings file , and network accreditation range .
action	An application that can be accessed from the CDE (Common Desktop Environment) graphical user interface. An action is represented by an icon. The action consists of one or more commands and optional user prompts. In Trusted Extensions, an action is only available to a user if the security administrator has included the action in a rights profile that is assigned to the user's account. Similarly, certain functions of the action might be available only if the security administrator has assigned the appropriate authorizations and privileges in that rights 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. This label 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 who is working at the ADMIN_LOW label. ADMIN_HIGH is the highest label in the system with all compartments. This label strictly dominates all labels in the system. Information at ADMIN_HIGH can only be read by users in roles that operate at ADMIN_HIGH. Administrative labels are used as labels or clearances for roles and systems. See also dominating label .
allocatable device	A security feature of the Solaris OS. An allocatable device can be used by one user at a time, and is capable of importing or exporting data from the system. The security administrator determines which users are authorized to access which allocatable devices. Allocatable devices include tape drives, floppy drives, audio devices, and CD-ROM devices. See also device allocation .

audit ID (AUID)	A security feature of the Solaris OS. An audit ID represents the login user. the AUID is unchanged after the user assumes a role, so is used to identify the user for auditing purposes. The audit ID always represents the user for auditing even when the user acquires effective UIDs/GIDs . See also user ID (UID) .
auditing	A security feature of the Solaris OS. Auditing is a process for capturing user activity and other events on the system, then storing this information in a set of files that is called an <i>audit trail</i> . Auditing produces system activity reports to fulfill site security policy.
authorization	A security feature of the Solaris OS. An authorization grants permission to a user to perform an action that is otherwise prohibited by security policy. The security administrator assigns authorizations to rights profiles . Rights profiles are then assigned to user or role accounts. Some commands and actions do not function fully unless the user has the necessary authorizations. See also privilege .
classification	A component of a clearance or a label . A clearance indicates a hierarchical level of security, for example, TOP SECRET or UNCLASSIFIED.
clearance	A label that defines the upper boundary of a label range . A clearance has two components: a classification and zero or more compartments . A clearance does not need to be a well-formed label . A clearance defines a theoretical boundary, not necessarily an actual label. See also user clearance , session clearance , and label encodings file .
Common Desktop Environment (CDE)	A graphical desktop that includes a session manager, a window manager, and various desktop tools. Trusted Extensions adds trusted applications to the desktop, such as the label builder , Device Allocation Manager , and Selection Manager . See also Java Desktop System (Java DS) .
compartment	A nonhierarchical component of a label used with the classification component to form a clearance or a label . A compartment represents a group of users with a potential need to access this information, such as an engineering department or a multidisciplinary project team.
compartmented mode workstation (CMW)	A computing system that fulfills the government requirements for a trusted workstation as stated in <i>Security Requirements for System High and Compartmented Mode Workstations</i> , DIA document number DDS-2600-5502-87. Specifically, it defines a trusted, X Window System-based operating system for UNIX workstations.
covert channel	A communication channel that is not normally intended for data communication. A covert channel allows a process to transfer information indirectly in a manner that violates the intent of the security policy.
deallocated device	A security feature of the Solaris OS. A deallocated device is no longer allocated to a user for exclusive use. See also device allocation .
device	See allocatable device .

device allocation	A security feature of the Solaris OS. Device allocation is a mechanism for protecting the information on an allocatable device from access by anyone 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 can be accessed again by another user. In Trusted Extensions, device allocation is handled by the Device Allocation Manager .
Device Allocation Manager	A trusted application of Trusted Extensions. This GUI is used to configure devices, and to allocate and deallocate devices. Device configuration includes adding authorization requirements to a device.
discretionary access control (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 (ACL) . An ACL lets the owner assign permissions specifically to additional users and additional groups. Contrast with mandatory access control (MAC) .
disjoint label	See dominating label .
dominating label	In a comparison of two labels, the label whose classification component is higher than or equal to the second label's classification and whose compartment components include all of the second label's compartment components. If the components are the same, the labels are said to dominate each other and are <i>equal</i> . If one label dominates the other and the labels are not equal, the first label is said to <i>strictly dominate</i> the other. Two labels are <i>disjoint</i> if they are not equal and neither label is dominant.
downgraded label	A label of an object that has been changed to a value that does not dominate the previous value of the label.
effective UIDs/GIDs	A security feature of the Solaris OS. Effective IDs override a real 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 a rights 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 the use of the <code>setuid</code> command as in conventional UNIX systems might 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 .
extended configuration	A computer system that is no longer an evaluatable configuration due to modifications that have broken security policy.
fallback mechanism	A shortcut method for specifying IP addresses in the <code>tnrhttp</code> database. For IPv4 addresses, the fallback mechanism recognizes <code>0</code> as a wildcard for a subnet.

gateway	A host that has more than one network interface. Such a host can be used to connect two or more networks. When the gateway is a Trusted Extensions host, the gateway can restrict traffic to a particular label.
group ID (GID)	A security feature of the Solaris OS. A GID is an integer that identifies a group of users who have common access permissions . See also discretionary access control (DAC) .
host	A computer attached to a network.
host template	A record in the <code>tnrhtp</code> database that defines the security attributes of a class of hosts that can access the Trusted Extensions network.
host type	A classification of a host . The classification is used for network communications. The definitions of host types are stored in the <code>tnrhtp</code> database. The host type determines whether the CIPSO network protocol is used to communicate with other hosts on the network. <i>Network protocol</i> refers to the rules for packaging communication information.
Java Desktop System (Java DS)	A graphical desktop that includes a session manager, a window manager, and various desktop tools. Java DS is a fully accessible desktop.
label	Also referred to as a sensitivity label. A label indicates the security level of an entity. An entity is a file, directory, process, device, or network interface. The label of an entity is used to determine whether access should be permitted in a particular transaction. Labels have two components: a classification that indicates the hierarchical level of security, and zero or more compartments for defining who can access the entity at a given classification. See also label encodings file .
label builder	A trusted application of Trusted Extensions. This GUI enables users to choose a session clearance or a session label. The clearance or label must be within the account label range that the security administrator has assigned to the user.
label encodings file	A file that is managed by the security administrator . The encodings file contains the definitions for all valid clearances and labels . The file also defines the system accreditation range , user accreditation range , and defines the security information on printouts at the site.
label range	Any set of labels that are bounded on the upper end by a clearance or maximum label, on the lower end by a minimum label, and that consist of well-formed labels . Label ranges are used to enforce mandatory access control (MAC) . 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 security policy forbids exposing the labels <code>ADMIN_HIGH</code> and <code>ADMIN_LOW</code> , the labels <code>RESTRICTED</code> and <code>PUBLIC</code> can be substituted.

labeled workspace	The Trusted Extensions version of a CDE or Java DS workspace. A labeled workspace labels every activity that is launched from the workspace with the label of the workspace. When users move a window into a workspace of a different label, the moved window retains its original label.
least privilege	See principle of least privilege .
mandatory access control (MAC)	A system-enforced access control mechanism that uses clearances and labels to enforce security policy. A clearance or a label is a security level. MAC associates the programs that a user runs with the security level at which the user chooses to work in the session. MAC then 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 (DAC) .
minimum label	<p>A label that is assigned to a user as the lower bound of the set of labels at which that user can work. When a user first begins a Trusted Extensions session, the minimum label is the user's default label. At login, the user can choose a different label for the initial label.</p> <p>Also, the lowest label that is permitted to any non-administrative user. The minimum label is assigned by the security administrator and defines the bottom of the user accreditation range.</p>
network accreditation range	The set of labels within which Trusted Extensions hosts are permitted to communicate on a network. The set can be a list of four discrete labels.
object	A passive entity that contains or receives data, such as a data file, directory, printer, or other device. An object is acted upon by subjects . In some cases, a process can be an object, such as when you send a signal to a process.
operator	A role that can be assigned to the user or users who are responsible for backing up systems.
ordinary user	A user who holds no special authorizations that allow exceptions from the standard security policies of the system. Typically, an ordinary user cannot assume an administrative role .
permissions	A set of codes that indicate which users are allowed to read, write, or execute the file or directory (folder). Users are classified as owner, group (the owner's group), and other (everyone else). Read permission (indicated by <i>r</i>) lets the user read the contents of a file or, if a directory, list the files in the folder. Write permission (<i>w</i>) lets the user make changes to a file or, if a folder, add or delete files. Execute permission (<i>e</i>) lets the user run the file if the file is executable. If the file is a directory, execute permission lets the user read or search the files in the directory. Also referred to as UNIX permissions or permission bits.
principle of least privilege	The security principle that restricts users to only those functions that are necessary to perform their jobs. The principle is applied in Trusted Extensions by making privileges available to programs on an as-needed basis. Privileges are available on an as-needed basis for specific purposes only.

privilege	A security feature of the Solaris OS. A privilege is a permission that is granted to a program by the security administrator . A privilege can be required to override some aspect of security policy. See also authorization .
privileged process	A security feature of the Solaris OS. A privileged process runs with assigned has privileges .
process	A running program. Trusted Extensions processes have Solaris security attributes , such as user ID (UID) , group ID (GID) , the user's audit ID (AUID) , and privileges . Trusted Extensions adds a label to every process.
profile	See rights profile .
profile shell	A security feature of the Solaris OS. A version of the Bourne shell that enables a user to run programs with security attributes .
reading down	The ability of a subject to view an object whose label the subject dominates. Security policy generally allows reading down. For example, a text editor program that runs at Secret can read Unclassified data. See also mandatory access control (MAC) .
rights profile	A security feature of the Solaris OS. A rights profile enables a site's security administrator to bundle commands and CDE actions with security attributes . Attributes such as user authorizations and privileges enable the commands and actions to succeed. A rights profile generally contains related tasks. A profile can be assigned to users and to roles .
role	A security feature of the Solaris OS. A role is a special account that gives the user who assumes the role access to certain applications with the security attributes that are necessary for performing the specific tasks.
security administrator	On system that is configured with Trusted Extensions, the role that is assigned to the user or users who are responsible for defining and for enforcing security policy. The security administrator can work at any label in the system accreditation range , and potentially has access to all information at the site. The security administrator configures the security attributes for all users and equipment. See also label encodings file .
security attribute	A security feature of the Solaris OS. A property of an entity, such as a process, zone, user, or device, that is related to security. Security attributes include identification values such as user ID (UID) and group ID (GID) . Attributes that are specific to Trusted Extensions include labels and label ranges . Note that only certain security attributes apply to a particular type of entity.
security policy	The set of DAC, MAC, and label rules that define how information can be accessed and by whom. At a customer site, the set of rules that defines the sensitivity of the information that is processed at that site. Policy includes the measures that are used to protect the information from unauthorized access.
Selection Manager	A trusted application of Trusted Extensions. This GUI appears when authorized users attempt to upgrade information or downgrade information.

sensitivity label	See label .
session	The time between logging in to a Trusted Extensions host and logging out from the host. The trusted stripe appears in all Trusted Extensions sessions to confirm that users are not being spoofed by a counterfeit system.
session clearance	A clearance set at login that defines the upper boundary of labels for a Trusted Extensions session . If the user is permitted to set the session clearance, the user can specify any value within the user's account label range . If the user's account is configured for forced single-level sessions, the session clearance is set to the default value specified by the security administrator . See also clearance .
session range	The set of labels that are available to a user during a Trusted Extensions session. The session range is bounded at the upper boundary by the user's session clearance and at the lower end by the minimum label .
single-label configuration	A user account that has been configured for operation at a single label only. Also called a single-level configuration.
spoof	To counterfeit a software program in order to illegally get access to information on a system.
strict dominance	See dominating label .
subject	An active entity, usually a process that runs on behalf of a user or role . A subject causes information to flow among objects , or changes the system state.
system accreditation range	The set of all valid labels for a site. The set includes the administrative labels that are available to the site's security administrator and system administrator . The system accreditation range is defined in the label encodings file .
system administrator	A security feature of the Solaris OS. The System Administrator role can be assigned to the user or users who are responsible for performing standard system management tasks such as setting up the non-security-relevant portions of user accounts. See also security administrator .
trusted application	An application that has been granted one or more privileges.
trusted computing base (TCB)	The part of a system that is configured with Trusted Extensions that affects security. The TCB 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 system, plus all of the administrative activities that are necessary to maintain the security of a distributed system and the data that the system contains.

trusted path	Refers to the mechanism for accessing actions and commands that are permitted to interact with the trusted computing base (TCB) . See also Trusted Path menu , trusted symbol , and trusted stripe .
Trusted Path menu	A menu of Trusted Extensions operations that is displayed by holding down mouse button 3 over the switch area of the Front Panel. The menu selections fall into three categories: workspace-oriented selections, role assumption selections, and security-related tasks.
trusted stripe	A screen-wide rectangular graphic in a reserved area of the screen. The trusted stripe appears in all Trusted Extensions sessions to confirm valid Trusted Extensions sessions . Depending on a site's configuration, the trusted stripe has one or two components: (1) a mandatory trusted symbol to indicate interaction with the trusted computing base (TCB) , and (2) an optional label to indicate the label of the current window or workspace.
trusted symbol	The symbol that appears at the left of the trusted stripe area. The symbol is displayed whenever the user accesses any portion of the trusted computing base (TCB) .
upgraded label	A label of an object that has been changed to a value that dominates the previous value of the label.
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 that are available to administrators only. The user accreditation range is defined in the label encodings file .
user clearance	A clearance that is assigned by the security administrator . A user clearance defines the upper boundary of a user's account label range . The user's clearance determines the highest label at which the user is permitted to work. See also clearance and session clearance .
user ID (UID)	A security feature of the Solaris OS. A UID identifies a user for the purposes of discretionary access control (DAC) , mandatory access control (MAC) , and auditing . See also access permissions .
well-formed label	A label that can be included in a range, because the label is permitted by all applicable rules in the label encodings file .
workspace	See labeled workspace .

Index

A

- access control
 - access control lists (ACLs), 17
 - discretionary access control (DAC), 17
 - mandatory access control (MAC), 17-22
 - permission bits, 17
- access control lists (ACLs), 17
- accessibility, provided by Java DS, 27
- accessing
 - for read only, 21
 - for reading and writing, 21
 - for writing, 21
 - initialization files at every label, 42-43
 - lower-level home directories, 19
- adding
 - labeled workspace, 51-52
 - workspaces, 51-52
- admin role
 - See* system administrator
 - See* System Administrator role
- Allocate Device menu item, 46-49
- allocating a device, 46-49
 - troubleshooting, 49
- Application Manager security in Trusted Extensions, 70
- Assume *rolename* role menu item, 49-50
- assuming a role, 49-50
- authorizations
 - changing labels, 22
 - for allocating devices, 16
 - required to change label of data, 53-55

C

- calendar security in Trusted Extensions, 67
- CDE
 - choosing as desktop, 29
 - customizing the desktop, 45
 - customizing the Workspace Menu, 41-42
 - finding online help for Trusted Extensions, 41
 - trusted applications on Front Panel, 66
 - Trusted Extensions desktop, 27
 - using the Style Manager, 45
- Change Password menu item, 45-46
- Change Workspace Label menu item, 50-51
- changing
 - labels by authorized users, 55-58
 - security level of data, 53-55, 55-58
 - workspace label, 50-51
 - your password, 45-46
- changing labels, troubleshooting, 58
- choosing
 - a desktop, 28, 29
 - label or clearance during login, 31
- classification component of label, defined, 18
- clearances
 - See also* labels
 - label type, 18
 - setting at login, 22-23, 32
 - setting session, 32
- clock security in Trusted Extensions, 67
- compartment component of label, defined, 18
- containers, *See* zones
- copy-and-paste, effect on labels, 22
- .copy_files file
 - creating, 42-43
 - described, 64

.copy_files file (*Continued*)

troubleshooting, 43

creating

\$HOME/.copy_files file, 42-43

\$HOME/.link_files file, 42-43

customizing

desktop, 45

Workspace Menu, 41-42

D

data

changing label of, 53-55

determining label of, 53

protecting with MAC, 17-22

desktops

common tasks, 44-45

in Trusted Extensions, 27

determining

label of a file, 53

label of a window, 43-44

devices

allocating, 46-49

clearing prior to reuse, 24

protecting, 16

troubleshooting, 49

using, 46-49

directories

changing labels, 55-58

visibility of home directories, 19

discretionary access control (DAC)

See DAC

defined, 17

dominance between labels, 20-22

downgrading information, 22

drag-and-drop, effect on labels, 22

E

email, label enforcement, 24

email instructions, user responsibilities, 22

F

failsafe login, 32-33

File Browser

changing labels, 56

displaying label of file, 53

viewing contents, 40

File Manager

changing file labels, 58-59

changing labels, 55-58

security in Trusted Extensions, 67

viewing contents, 39

files

\$HOME/.copy_files, 42-43, 64

\$HOME/.link_files, 42-43, 65

accessing initialization files at every label, 42-43

changing labels, 55-58

linking between File Managers at different labels, 58-59

moving between File Managers, 55-58

viewing in a workspace, 39-40

finding

calendar events at every label, 45

man pages in Trusted Extensions, 40

online help for Trusted Extensions, 41

Trusted Path menu, 49, 62

Front Panel

description of trusted applications on, 66

restoring when minimized, 66

H

help in Trusted Extensions

man pages, 40

online help, 41

home directories, visible from higher-level zone, 19

IIDs, *See* UIDsinformation, *See* data

initialization files

accessing at every label, 42-43

troubleshooting when customized, 33

J

- Java Desktop System (Java DS)
 - choosing as desktop, 29
 - customizing the desktop, 45
 - online help, 41
 - Trusted Extensions desktop, 27

L

- label ranges
 - described, 18
 - troubleshooting a workstation with a restricted range, 32
- labels
 - See also* clearances
 - changing label of data, 53-55
 - changing label of files, 55-58
 - changing label on information, 22
 - components, 18-19
 - determining by window query, 43-44
 - displayed in Trusted Extensions, 62-63
 - displayed on desktop, 18
 - dominance, 20-22
 - labeled zones, 19-20
 - means of protecting data, 22-24
 - ranges, 18
 - relationships, 20-22
 - sample government labels, 20
 - sample industry labels, 18
 - sample label relationships, 21
 - setting at login, 32
 - setting clearance at login, 22-23
 - setting session labels, 32
 - types, 18
 - visible on desktop, 36
- Launch menu, using, 41
- .link_files file
 - creating, 42-43
 - described, 65
 - troubleshooting, 43
- linking files at different labels, 58-59
 - by using .link_files, 42-43
- logging in
 - at a different label, 46
 - choosing a desktop, 28, 29

- logging in (*Continued*)
 - choosing a label or clearance, 31
 - failsafe, 32-33
 - five steps of, 28
 - reviewing security settings, 30-32
 - troubleshooting, 30, 32-33
- logging out
 - procedure, 38
 - user responsibilities, 36
- login process, *See* logging in

M

- mail security in Trusted Extensions, 68
- man pages in Trusted Extensions, 40
- mandatory access control (MAC)
 - See* MAC
 - defined, 17-22
 - enforced for email, 24
- moving
 - a window to a workspace at a different label, 52-53
 - data to different label, 53-55
 - file to different label, 55-58
- multilevel login, CDE or Java DS, 29
- multilevel sessions, defined, 22-23

N

- no trusted stripe, troubleshooting, 37
- no trusted symbol, troubleshooting, 64
- Not Found error message, 25
- Not in Profile error message, 25

O

- object
 - defined, 18
 - reuse, 24
- oper role
 - See* Operator role
 - See* system operator
- Operator role, responsibilities, 26

P

- passwords, user responsibilities, 65
- peripheral devices, *See* devices
- permissions
 - at discretion of file owner, 17
 - user responsibilities, 22
- pfsh command
 - See* profile shell
- policy
 - See* security policy
- Printer tool security in Trusted Extensions, 68-69
- printing, typical labeled banner page, 68
- privileges
 - See also* authorizations
- procedures, *See* users
- profile shell, defined, 25
- profiles
 - See* rights profiles
- protecting files
 - by label, 22-24
 - DAC, 17
 - MAC, 17-22
 - user responsibilities, 22

Q

- Query Window Label menu item, 43-44

R

- read access, in labeled environment, 21
- responsibilities
 - of administrators, 26
 - users for password security, 65
 - users to clear media, 24
 - users to protect data, 22
 - users when logging out, 38
- reviewing security settings
 - Last Login dialog box, 29
 - procedure during login, 30-32
- rights profiles, defined, 25-26
- roles
 - adding a labeled workspace, 51-52
 - changing workspace label, 50-51

roles (*Continued*)

- common roles, 26
- responsibilities of, 26
- special user account, 25-26
- root role, responsibilities, 26

S

- secadmin role
 - See* security administrator
 - See* Security Administrator role
- Security Administrator role
 - contacting about missing trusted stripe, 37
 - contacting for missing trusted symbol, 64
 - responsibilities, 26
- security policy
 - defined, 15, 76
- security practices, defined, 15
- selection, changing label, 53-55
- Selection Manager, 54
- sensitivity labels
 - See* labels
 - label type, 18
- session clearances, defined, 22-23
- sessions
 - choosing clearance, 22-23
 - effect of selecting level, 23
 - setting level, 32
 - single-level or multilevel, 22-23
- shutting down a workstation, 39
- single-level login, CDE or Java DS, 29
- single-level sessions, defined, 22-23
- SLs, *See* labels
- Solaris Trusted Extensions (CDE), *See* CDE
- spoofing
 - defined, 16, 77
- Stop-A (L1-A) keyboard combination, 39
- Style Manager
 - changing session characteristics, 46
 - limitations in Solaris Trusted Extensions (CDE), 69-70
 - requires the trusted path, 45
- subject, defined, 18
- Suspend System menu item, 39
- switching to a workspace at a different label, 52
- system administration, on Trusted Extensions, 25-26

System Administrator role, responsibilities, 26

T

tasks, *See* users

Text Editor security in Trusted Extensions, 67

Trash Can security in Trusted Extensions, 70

troubleshooting

\$HOME/.copy_files file, 43

\$HOME/.link_files file, 43

command line error messages, 25

device allocation, 49

login, 32-33

minimized Front Panel, 66

missing trusted stripe, 37

password failure, 30

relabeling files, 58

trusted applications

by using rights profiles, 25-26

on Front Panel, 66

Trusted Computing Base, *See* TCB

trusted computing base (TCB)

defined, 16

procedures that interact with the TCB, 45-59

symbol of interacting with, 16, 63

Trusted Extensions

basic features, 61-64

overview, 15

Trusted Path menu

Allocate Device, 46-49

Assume *rolename* role, 49-50

Change Password, 45-46

Change Workspace Label, 50-51

described, 66-67

location, 62

Query Window Label, 43-44

trusted stripe

described, 63

location in CDE, 18, 62

location in Java DS, 62

not on lockscreen, 37

what to do if missing, 37

trusted symbol

described, 63

missing, 64

trusted symbol (*Continued*)

on labeled CDE workspace, 36

tamper-proof icon, 16

types of labels, 18

U

unlabeled screens

lockscreen, 37

login screen, 27

upgrading information, 22

user clearances, defined, 18

user IDs, *See* UIDs

user responsibilities

password security, 65

protecting data, 22

when leaving workstation, 36

users

accessing initialization files at every label, 42-43

adding a labeled workspace, 51-52

allocating a device, 46-49

assuming a role, 49-50

authorized to change label of file, 55-58

authorized to change security level of data, 53-55

changing workspace label, 50-51

changing your password, 45-46

customizing the Workspace Menu, 41-42

determining the label of a file, 53

finding online help for Trusted Extensions, 41

getting online help, 40

linking files at different labels, 58-59

locking your screen, 37-38

logging in at a different label, 46

logging out, 38

moving a window to a workspace at a different label, 52-53

moving data between labels, 53-55

moving files between labels, 55-58

responsibilities

clearing devices, 24

password security, 65

protecting data, 22

when leaving workstation, 38

shutting down a workstation, 39

switching to a workspace at a different label, 52

users (*Continued*)

- unlocking your screen, 37
- viewing files in a workspace, 39-40
- using a device, *See* allocating a device
- using trusted desktop, single-level or multilevel, 29

V

visibility

- desktop security, 35-36
- labels after login, 27
- reading lower-level home directories, 19
- trusted stripe, 18, 37, 62

W

Window Label indicator, 64

Workspace Menu

- customizing, 41-42
- Suspend System, 39

workspace switch area

- illustration, 24
- in Trusted Extensions CDE, 66

workspaces

- labeled, 24
- setting default label, 46

write access, in labeled environment, 21

Z

zones

- home directory visibility, 19
- labeled, 19-20