Trusted Extensions User's Guide

Part No: E36841
July 2014

ORACLE

Contents

Figures

Tables

Using This Documentation

- **Overview** – Describes how to use the Trusted Extensions feature of Oracle Solaris on a desktop system.
- **Audience** – Desktop users of Trusted Extensions.
- **Required knowledge** – GNOME desktop.

Product Documentation Library

Late-breaking information and known issues for this product are included in the documentation library at http://www.oracle.com/pls/topic/lookup?ctx=E36784.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Feedback

Provide feedback about this documentation at http://www.oracle.com/goto/docfeedback.

♦ ♦ ♦ CHAPTER 1

About Trusted Extensions

This chapter introduces you to the labels and other security features that the Trusted Extensions feature adds to the Oracle Solaris operating system (Oracle Solaris OS).

What Is Trusted Extensions?

Trusted Extensions provides special security features for your Oracle Solaris system. These features enable an organization to define and implement a labeled security policy on an Oracle 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 issues 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 which security features are configurable.

Trusted Extensions Protects Against Intruders

Trusted Extensions adds features to the Oracle Solaris OS that protect against intruders. Trusted Extensions also relies on some Oracle Solaris features, such as password protection. Trusted Extensions adds a password change GUI for roles. By default, users must be authorized to use a peripheral device, such as a microphone or camera.

Access to the Trusted Computing Base Is Limited

The term *trusted computing base* (*TCB*) refers to the part of Trusted Extensions that handles events that are relevant to security. The TCB includes software, hardware, firmware, documentation, and administrative procedures. Utilities and application programs that can access security-related files are all part of the TCB. Your administrator sets limits on all potential interactions that you can have with the TCB. Such interactions include programs that you need to perform your job, files that you are allowed to access, and utilities that can affect security.

Mandatory Access Control Protects Information

If an intruder manages to successfully log in to the system, further obstacles prevent access to information. Files and other resources are protected by access control. As in the Oracle 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 Discretionary and Mandatory Access Control" on page 15.

Peripheral Devices Are Protected

In Trusted Extensions, administrators control access to local peripheral devices such as tape drives, CD-ROM drives, USB devices, 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 following *trusted symbol*, a clearly recognizable, tamper-proof icon at the top of the screen.

FIGURE 1-1 Trusted Symbol

This 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. Figure 1-1 shows the trusted symbol.

Trusted Extensions Provides Discretionary and 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 user access to files and directories. DAC leaves setting protections for files and 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, the ability to override DAC is permitted for administrators and authorized users only. ACLs provide a finer granularity of access control. ACLs enable owners to specify separate permissions for specific users and specific groups. For more information, see Chapter 7, “Using ACLs and Attributes to Protect Oracle Solaris ZFS Files,” in “Managing ZFS File Systems in Oracle Solaris 11.2 ”.

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 or 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. Regular 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 the following two components:

- Classification, also referred to as a *level*

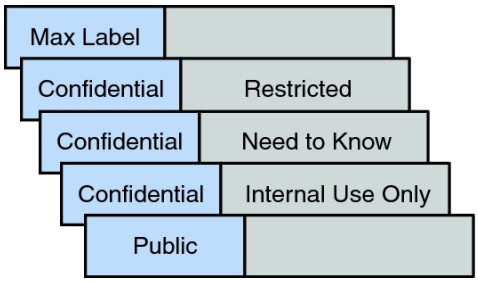
  This component indicates a hierarchical level of security. When applied to people, the classification represents a measure of trust. When applied to data, a classification is the degree of protection that is required.

  In the U.S. Government, the 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 1-2. The terms on the left are classifications. The terms 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 1-2, 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*. A user can be cleared to work at one or more sensitivity labels. A special label, known as the *user clearance*, determines the highest label at which a user is permitted to work. In addition, each user has a minimum sensitivity label. This label is used by default during login to a multilevel desktop session. After login, the user can 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`.

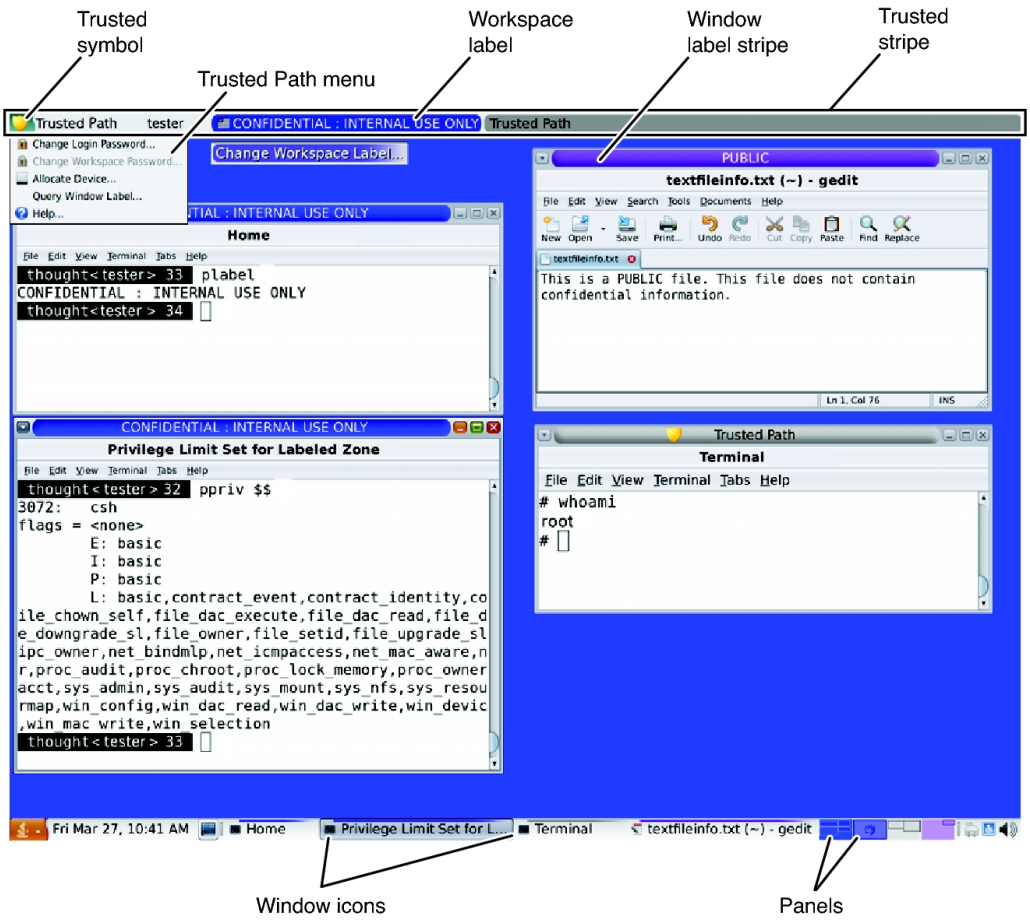
FIGURE 1-2 Typical Industry Sensitivity Labels



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 the `kill` command on a process.

Figure 1-3 shows a typical multilevel Trusted Extensions session. The trusted stripe is at the top. The Trusted Path menu is invoked from the trusted stripe. To assume a role, click the user name to invoke the roles menu. The workspace switches in the bottom panel display the color of the workspace label. The window list in the bottom panel displays the color of the window's label.

FIGURE 1-3 Typical Multilevel Session



Containers and Labels

Trusted Extensions uses containers for labeling. Containers are also called *zones*. The *global zone* is an administrative zone and is not available to users. Non-global zones are called *labeled zones*. Labeled zones are available to 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`. Users can read, but cannot change, the contents of an `ADMIN_LOW` file.

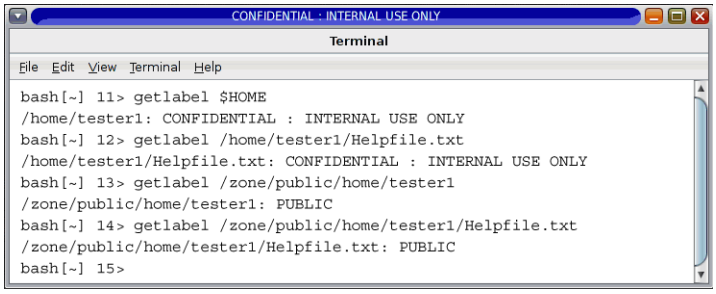
Network communication is restricted by label. By default, zones cannot communicate with each other because their labels are different. Therefore, one zone cannot write into another zone.

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 on a remote system. For example, a user's home directory in a lower-level zone can be mounted by using the automount service. The pathname convention for such lower-level home mounts includes the zone name, as follows:

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

The following terminal window illustrates lower-level home directory visibility. A user whose login label is `Confidential: Internal Use Only` can view the contents of the `Public` zone when the automount service is configured to make lower-level zones readable. The `textfileInfo.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.

FIGURE 1-4 Viewing Public Information From a Higher-Label 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 entity'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 is higher than 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.

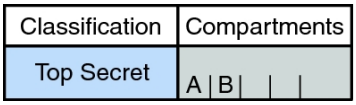
If one of the following conditions is met, then the first label is said to *strictly dominate* the second label.

- The first label has a higher classification than a second label
- The first label's classification is equal to a second label's classification, the first label includes the second label's compartments, and the first label has additional compartments

A label that strictly dominates a second label is permitted access to the second label.

Two labels are said to be *disjoint* if neither label dominates the other label. Access is not permitted between disjoint labels.

For example, consider the following figure.



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 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 compartments 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. Write transactions 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`.

The following table illustrates dominance relationships among U.S. Government labels and among a set of industry labels.

TABLE 1-1 Examples of Label Relationships in Trusted Extensions

	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 Use Only`
	`Confidential: Restricted`	dominates	`Public`
	`Confidential: Need to Know`	dominates	`Confidential: Internal Use Only`
	`Confidential: Need to Know`	dominates	`Public`
	`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 to do so, Trusted Extensions disallows the transaction. The security administrator can authorize you to upgrade or downgrade information. For more information, see “Performing Trusted Actions” on page 44.

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 use a mechanism 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 Browser, as described in Chapter 3, “Working in Trusted Extensions”.

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

Another aspect of protecting data involves email. 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:

- MAC is enforced for all transactions, including email.
- Files are stored in separate zones according to label.
- The desktop provides workspaces that are labeled.
- Users can select a single-level or a multilevel session.
- Data on objects is erased prior to object reuse.

Single-Level or Multilevel Sessions

When you first log in to a 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-level 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 labels that are equal to or lower than your session clearance. You can specify different labels for different workspaces. You can also have multiple workspaces at the same label.

Session Selection Example

Table 1-2 provides an example that shows 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 each 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. To view a sample label builder for a multilevel session, see Figure 3-4.

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 accesses the system. The Available Labels column lists the labels that the user is permitted to switch to during the session.

TABLE 1-2 Effect of Initial Label Selection on Available Session Labels

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 Use Only
				CNF: NTK

As the first row of the table shows, 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.

As the second row of the table shows, 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

On a Trusted Extensions desktop, the workspaces are accessed through workspace panels at the right of the bottom panel.

FIGURE 1-5 Labeled Workspaces on the Panel

Each workspace has a label. You can assign the same label to several workspaces, and you can assign different labels to different workspaces. Windows that are launched in a workspace have the label of that workspace. When the window is moved to a workspace of a different label, the window retains its original label. Thus, in a multilevel session, you can arrange windows of different labels in one workspace.

Enforcing MAC for Email Transactions

Trusted Extensions enforces MAC for email. You can send and read email at your current label. You can receive email at a label within your account range. In a multilevel session, you can switch to a workspace at a different label to read email at that label. You use the same mail reader and the same login. The system permits you to read mail at your current label only.

Erasing Data on Objects Prior to Object 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 USB devices, before allowing another user access to the drive.

Trusted Extensions Enables Secure Administration

In contrast to traditional UNIX systems, superuser (the `root` user) is not used to administer Trusted Extensions. Rather, administrative roles with discrete capabilities administer the system. In this way, 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 labels, authorizations, privileges, and effective UIDs/GIDs.

The following security practices are enforced 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.

Accessing Applications in Trusted Extensions

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

The Oracle Solaris OS provides security attributes such as *privileges* and *authorizations*. Trusted Extensions provides labels. Any of these attributes, if missing, can prevent use of the program or parts of the program. For example, a rights profile might include an authorization that enables you to read a database. A rights profile with different security attributes might be required for you to modify the database or 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, the administrator might assign you a profile shell as your login shell. A *profile shell* is a special version of a common shell that provides access to a particular set of applications and capabilities. Profile shells are a feature of the Oracle Solaris OS. For details, see the `pfexec`(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 program. Check with your security administrator.

Administration by Role in Trusted Extensions

Trusted Extensions recommends the use of roles for administration. Make sure that you know who is performing which set of duties at your site. The following are common roles:

- root role – Is used primarily to prevent direct login by superuser.
- Security Administrator role – Performs security-relevant tasks, such as authorizing device allocation, assigning rights profiles, and evaluating software programs.
- System Administrator role – Performs standard system management tasks, such as creating users, setting up home directories, and installing software programs.
- Operator role – Performs system backups, manages printers, and mounts removable media.

♦ ♦ ♦ CHAPTER 2

Logging In to Trusted Extensions

This chapter describes the trusted desktop and the login process on a Trusted Extensions system. This chapter covers the following topics:

Desktop 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 desktop is a trusted version of the Oracle Solaris desktop.

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.

Trusted Extensions Login Process

The login process on a system that is configured with Trusted Extensions is similar to the login process for Oracle Solaris. However, in Trusted Extensions, you examine several screens for security-relevant information before the desktop session can be started. The process is described in more detail in the sections that follow. Here is a brief overview.

1. Identification – Type your username in the Username field.
2. Authentication – Type your password in the Password field.

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

3. Message checking and session type selection – You examine the information in the Message Of The Day dialog box. This dialog box displays the time you last logged in, any 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-label* or single-level configuration. For an example, see "Session Selection Example" on page 23.

---

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

Note - By default, remote login is not supported for regular users in Trusted Extensions. If your administrator has configured the Oracle Solaris Xvnc software, you can use a VNC client to remotely display a multilevel desktop. For the procedure, see "Logging In Remotely to Trusted Extensions" on page 32.

Identification and Authentication During Login

Identification and authentication during login are handled by the Oracle Solaris OS. The login screen initially contains the Username prompt. This part of the login process is referred to as *identification*.

After you have entered the username, the password prompt is displayed. 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 down your password 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 Attributes During Login

The review of security attributes is handled by Trusted Extensions, not by the Oracle Solaris OS. Before login is complete, Trusted Extensions displays the Message Of The Day (MOTD) dialog box. This dialog box provides status information for you to review. The status includes

past information, such as when the system was last used by you. You can also review the security attributes 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 a multilevel session.

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

Logging In to Trusted Extensions

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

▼ Identify and Authenticate Yourself to the System

1. **In the Username field of the login screen, type your username.**

   Be sure to type your username exactly as your administrator assigned it to you. Pay attention to spelling and capitalization.

   If you make an error, type a fake password. The Username field appears.

2. **Confirm your entry.**

   Press the Return key to confirm your username.

Caution - You should *never* see the trusted stripe when the login screen appears. If you see the trusted stripe while attempting to log in or unlock the screen, do not type your password. There is a possibility 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.

3. **Type your password in the password entry field, and press Return.**

   For security purposes, the characters do not display in the field. The system compares the login name and password against a list of authorized users.

Troubleshooting If the password that you provided is incorrect, the screen displays a message:

```
Authentication failed
```

Click OK to dismiss the error dialog box. Retype your user name, then 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.

1. **Examine the MOTD dialog box.**

   a. **Check that the time of your last session is accurate.**

      Always check that nothing is 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.

   b. **Check for any messages from the administrator.**

      The Message Of The Day field can contain warnings about scheduled maintenance or security problems. Always review the information in this field.

   c. **Examine the security attributes of your session.**

      The MOTD dialog box indicates any roles that you can assume, your minimum label, and other security characteristics.

   d. **(Optional) If you are permitted to log in to a multilevel session, decide if you want a single-level session.**

      Click the Restrict Session to a Single Label button to log in to a single-level session.

e. **Click OK.**

2. **Confirm your label choice.**

   You are presented with a label builder. If you are logging in at a single label, the label builder describes your session label. In a multilevel system, the label builder enables you to choose your session clearance. To view a sample label builder for a multilevel session, see Figure 3-4.

   - **Accept the default, unless you have a reason not to.**
   - **For a multilevel session, select a clearance.**

     To change the clearance, click the `Trusted Path` clearance, then click a clearance that you want.

   - **For a single-level session, select a label.**

     To change the label, click the `Trusted Path` label, then click the label that you want.

3. **Click OK.**

   The trusted desktop appears.

▼ Troubleshoot Login Problems

1. **If your username or password is not recognized, check with the administrator.**
2. **If your label range is not permitted on your workstation, check with the 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 specify is not accepted, check with an administrator to determine if the workstation is restricted.

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

   - **Contact your system administrator to correct the situation.**
   - **If you can become `root`, 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, a failsafe login is protected. Only the `root` account can access a failsafe login.

a. **Type your username in the login screen.**

b. **At the bottom of the screen, choose Solaris Trusted Extensions Failsafe Session from the desktop menu.**

c. **When prompted, provide your password.**

d. **When prompted for an additional password, provide the password for `root`.**

Logging In Remotely to Trusted Extensions

Virtual network computing (VNC) provides a way for you to access a central Trusted Extensions system from your laptop or home computer. The administrator at your site must configure the Oracle Solaris Xvnc software to run on a Trusted Extensions server and a VNC viewer to run on the client systems. You can work at any label in your label range that is installed on the server.

▼ How to Log In to a Remote Trusted Extensions Desktop

Before You Begin Your administrator has set up an Xvnc server. For pointers, see "How to Configure a Trusted Extensions System With Xvnc for Remote Access" in "Trusted Extensions Configuration and Administration ".

1. **In a terminal window, connect to the Xvnc server.**

   Type the name of the server that your administrator has configured with Xvnc.

   ```
   % /usr/bin/vncviewer Xvnc-server
   ```

2. **Log in.**

   Follow the procedures in "Logging In to Trusted Extensions" on page 29.

You can now work on the Trusted Extensions desktop in the VNC viewer.

♦ ♦ ♦ CHAPTER 3

Working in Trusted Extensions

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

Visible Desktop Security in Trusted Extensions

Trusted Extensions provides a multilevel desktop.

A system that is configured with Trusted Extensions displays the trusted stripe except during login and screen lock. At all other times, the trusted stripe is visible.

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 (TCB). When you change your password, for example, you interact with the TCB.

When the monitors of a multiheaded Trusted Extensions system are configured horizontally, one trusted stripe appears across the monitors. However, if the multiheaded system is configured to display vertically, or has separate desktops, one desktop per monitor, then the trusted stripe appears on one monitor only.

Caution - If a second trusted stripe appears on a multiheaded system, the stripe is not generated by the operating system. You might have an unauthorized program on your system.

Contact your security administrator immediately. To determine the correct trusted stripe, see "How to Find the Mouse Pointer" on page 42.

For details about the applications, menus, labels, and features of the desktop, see Chapter 4, "Elements of Trusted Extensions".

Trusted Extensions Logout Process

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

Working on a Labeled System

Caution - If the trusted stripe is missing from your workspace, contact the security administrator. The problem with your system could be serious.

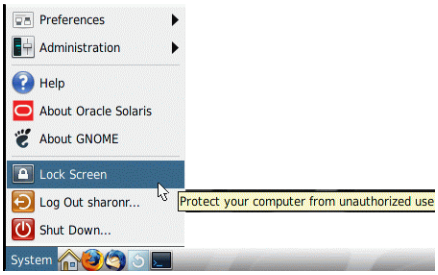
The trusted stripe must not appear during login, or when you lock your screen. If the trusted stripe shows, contact the administrator immediately.

▼ How to Lock and Unlock Your Screen

If you leave your workstation briefly, lock the screen.

1. **Choose Lock Screen from the Main menu.**

FIGURE 3-1 Lock Screen Selection



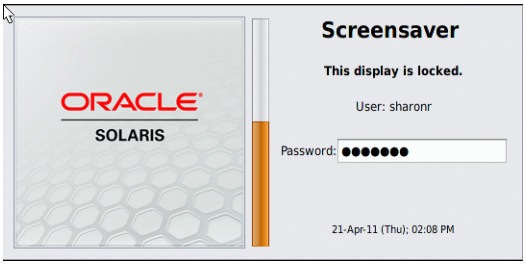
The screen turns black. At this point, only you can log in again.

Note - The trusted stripe must not appear when the screen is locked. If the stripe does appear, notify the security administrator immediately.

---

2. **To unlock your screen, do the following:**

   a. **Move your mouse until the Screensaver dialog box is visible.**



   If the Screensaver dialog box does not appear, press the Return key.

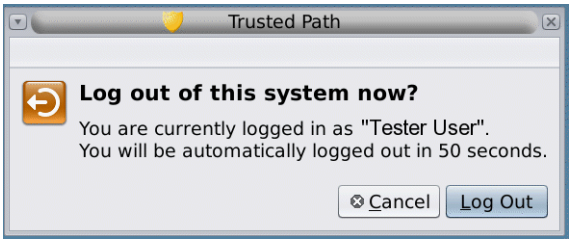
   b. **Type your password.**

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

How to Log Out of Trusted Extensions

At most sites, the screen automatically locks after a specified period of idleness. 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 of Trusted Extensions, choose Log Out** *your-name* **from the Main menu.**



2. **Confirm that you want to log out, or click Cancel.**

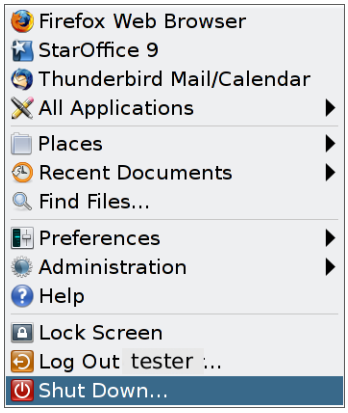
How to Shut Down Your System

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

Note - If you are not on the console, you cannot shut down the system. For example, VNC clients cannot shut down the system.

Before You Begin You must be assigned the Maintenance and Repair rights profile.

- **Choose Shut Down from the Main menu.**



Confirm the shutdown.

Note - By default, 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 Labeled Workspace

To view your files, you use the same applications that you would use on your desktop on an Oracle Solaris system. If you are working at multiple labels, only the files that are at the label of the workspace are visible.

- **Open a terminal window or the File Browser.**

  - **Open a terminal window and list the contents of your home directory.**

    Click mouse button 3 over the background. From the menu, choose Open Terminal.

  - **Click the Home folder on your desktop or desktop panel.**

    The folder opens in a File Browser. The File Browser application opens 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 18. To view files at different labels in one workspace, see "How to Move a Window to a Different Workspace" on page 52.

How to Access the Trusted Extensions Man Pages

- **In the Oracle Solaris release, review the `trusted_extensions(5)` man page in a terminal window.**

  ```
  % man trusted_extensions
  ```

  For a list of user commands that are specific to Trusted Extensions, see Appendix D, "List of Trusted Extensions Man Pages," in "Trusted Extensions Configuration and Administration ". The man pages are also available from Oracle's documentation web site (http://www.oracle.com/technetwork/indexes/documentation/index.html).

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. For more information, see ".copy_files and .link_files Files" in "Trusted Extensions Configuration and Administration ".

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

Work with your administrator when modifying these files.

1. **Decide which initialization files you want to link 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 you want to copy 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.

```
% vi .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 C shell defaults to be identical at all labels.

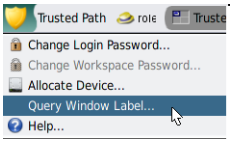
```
% vi .link_files
# Link these files to my home directory in every zone
.cshrc
.mailrc
```

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.

How to Interactively Display a Window Label

This operation can be useful to identify the label of a partially hidden window.

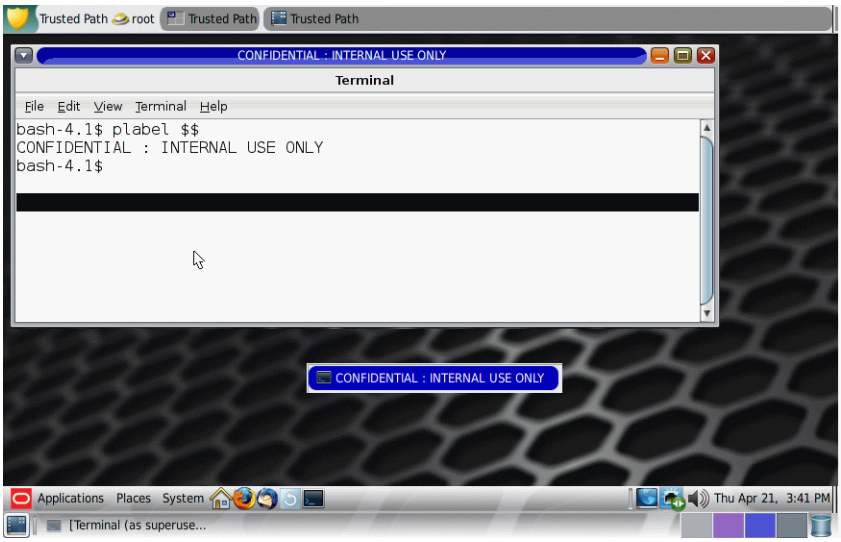
1. **Choose Query Window Label from the Trusted Path menu.**



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 3-2 Query Window Label Operation



3. **Click the mouse button to end the operation.**

How to Find the Mouse Pointer

An untrusted application can gain control of the keyboard or mouse pointer. By finding the pointer, you can regain control of the desktop focus.

1. **To regain control of a Sun keyboard, press Meta-Stop.**

   Press the keys simultaneously to regain control of the current desktop focus. On the Sun keyboard, the diamond key on either side of the spacebar is the Meta key.

   If the grab of the keyboard or mouse pointer is not trusted, the pointer moves to the trusted stripe. A trusted pointer does not move to the trusted stripe.

2. **If you are not using a Sun keyboard, press Alt-Break.**

Example 3-3 Forcing the Mouse Pointer to the Trusted Stripe

In this example, a user is not running any trusted processes but cannot see the mouse pointer. To bring the pointer to the center of the trusted stripe, the user presses the Meta-Stop keys simultaneously.

Example 3-4 Finding the Real Trusted Stripe

On a multiheaded Trusted Extensions system whose monitors are configured to display a separate desktop on each monitor, a user sees one trusted stripe per monitor. Therefore, a program other than Trusted Extensions is generating a trusted stripe. Only one trusted stripe displays when a multiheaded system is configured to display a separate desktop per monitor.

The user halts work and immediately contacts the security administrator. Then, the user finds the real trusted stripe by placing the mouse pointer in an untrusted location, such as over the workspace background. When the user presses the Alt-Break keys simultaneously, the pointer moves to the trusted stripe that is generated by Trusted Extensions.

▼ How to Perform Some Common Desktop Tasks in Trusted Extensions

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

- Emptying the trash
- Finding calendar events

1. Empty the trash.

Click mouse button 3 over the Trash Can icon on the desktop. Choose Empty Trash, then confirm.

Note - 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.

---

2. Find calendar events at every label.

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

- **In a multilevel session, open your calendar from each workspace that has a different label.**

- **In a single-level session, log out. Then, log in at a different label to view the calendar events at that label.**

3. **Save a customized desktop at every label.**

   You can customize the workspace configuration for every label at which you log in.

   a. **Configure the desktop.**

   Note - Users can save desktop configurations. Roles cannot save desktop configurations.

      i. **From the Main menu, click System > Preferences > Appearance.**

      ii. **Arrange windows, establish the font size, and perform other customizations.**

   b. **To save the current desktop, click the Main menu.**

      i. **Click System > Preferences > Startup Applications.**

      ii. **Click the Options tab.**

      iii. **Click Remember Currently Running Applications, then close the dialog box.**

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

Performing Trusted Actions

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.

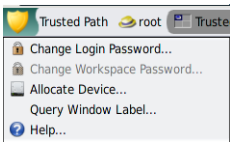
How to Change Your Password in Trusted Extensions

Unlike the Oracle Solaris OS, Trusted Extensions provides a GUI for changing your password. The GUI grabs the pointer until the password operation is completed. To stop a process that has grabbed the pointer, see Example 3-5.

1. **Choose `Change Login Password` or `Change Workspace Password` from the Trusted Path menu.**

   To select the password menu item, click `Trusted Path` in the trusted stripe.

   FIGURE 3-3 Trusted Path Menu



Note - The Trusted Path menu item `Change Workspace Password` is active when your site is running a separate naming service per zone.

2. **Type your current password.**

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

Caution - When you type 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 trusted 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 by retyping it.**

Note - If you chose `Change Password` and your site is using local accounts, your new password does not go into effect until the zone or the system is rebooted. To reboot the zone, you must be assigned the Zone Security rights profile. To reboot the system, you must be assigned the Maintenance and Repair rights profile. If you are not assigned one of these profiles, contact your system administrator to schedule a reboot.

Example 3-5 Testing If the Password Prompt Can Be Trusted

On an x86 system that has a Sun keyboard, the user has been prompted for a password. The mouse pointer has been grabbed and is positioned in the password dialog box. To check that the prompt is trusted, the user presses the Meta-Stop keys simultaneously. If the pointer remains in the dialog box, the user knows that the password prompt is trusted.

If the pointer does not remain in the dialog box, the user knows that the password prompt cannot be trusted. The user then must contact the administrator.

How to Log In at a Different Label

The label of the first workspace that appears 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 for every label at which they log in.

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

1. **Create workspaces at every label.**

   For details, see "How to Add a Workspace at Your Minimum Label" on page 51.

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

3. **Go to the labeled workspace that you want to see when you log in at its label.**

4. **Save this current workspace.**

   For details, see "How to Perform Some Common Desktop Tasks in Trusted Extensions" on page 43.

How to Allocate a Device in Trusted Extensions

The Allocate Device 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”.

Before You Begin You must be authorized to allocate a device.

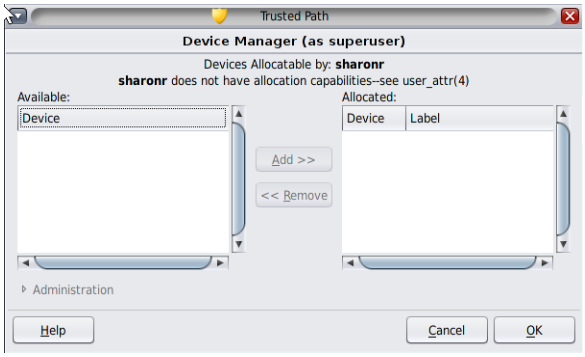
1. **Choose Allocate Device from the Trusted Path menu**

2. **Double-click the device that you want to use.**

   The devices that you are permitted to allocate at your current label appear under Available Devices:.

   - `audio`*n* – Indicates a microphone and speaker
   - `cdrom`*n* – Indicates a CD-ROM drive
   - `mag_tape`*n* – Indicates a tape drive (streaming)
   - `rmdisk`*n* – Indicates a removable disk, such as a JAZ or ZIP drive, or USB hot-pluggable media

   The following dialog box indicates that you are not authorized to allocate devices:



3. **Select the device.**

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

   - **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. For example, the following instructions appear for microphone use:

Then, the device is mounted. The device name now appears in the Allocated Devices list. This device is now allocated for your exclusive use.

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. When you move the Device Manager to a workspace at a different label, the Available and Allocated Devices lists change to reflect the correct context.

If a File Browser window does not appear, open the window manually, then navigate to the root directory, `/`. In this directory, navigate to the allocated device to view its contents.

▼ How to Deallocate a Device in Trusted Extensions

1. **Deallocate the device.**

   a. **Go to the workspace where the Device Manager is displayed.**

   b. **Move the device to be deallocated from the list of allocated devices.**

2. **Remove the media.**

3. **Click OK in the Deallocation dialog box.**

   The device is now available for use by another authorized user.

How to Assume a Role in Trusted Extensions

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

1. **Click your user name at the right of the trusted symbol.**

2. **Choose a role name from the menu.**

3. **Type the role password and press Return.**

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

Caution - When you type 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 trusted 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 current workspace becomes the 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 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 multilevel session.

Use this procedure to work in the same workspace at a different label. To create a workspace at a different label, see "How to Add a Workspace at Your Minimum Label" on page 51.

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

1. **Click the window label in the trusted stripe.**

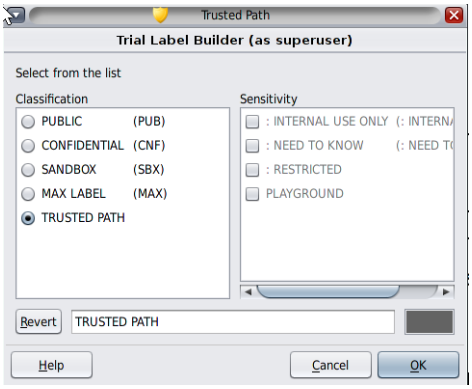
You can also click a workspace panel.

2. **Click Change Workspace Label.**

3. **Choose a label from the label builder.**

The following illustration shows the user clicking the Trusted Path button.

FIGURE 3-4 Label Builder



After clicking this button, the user can select from the user labels. The workspace label is changed to the new label. On a system where labels are color-coded, new windows are marked with the new color.

4. **If you are prompted for your password, provide it.**

If your site is running a separate naming service per zone, users are prompted for a password when entering a workspace at a new label.

How to Add a Workspace at Your Minimum Label

The ability to set workspace labels in Trusted Extensions provides a convenient means of working at different labels within the same multilevel session. You can add a workspace at your minimum label.

To change the label of the current workspace, see "How to Change the Label of a Workspace" on page 49.

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

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

   a. **Click mouse button 3 over a workspace panel.**

   b. **From the menu, choose Preferences.**

   c. **Increase the number in the Number of Workspaces field.**

      The new workspaces are created at your minimum label. You can also use this dialog box to name the workspaces. The name appears in the tooltip.

   d. **(Optional) Name the workspaces.**

      When the mouse hovers over the workspace panel, the name appears in the tooltip.

2. **To change the workspace label, select a workspace panel and change its label.**

   For details, see "How to Change the Label of a Workspace" on page 49.

How to Switch to a Workspace at a Different Label

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

1. **Click a workspace panel of a different color.**

2. **If you are prompted for your password, provide it.**

If your site is running a separate naming service per zone, users are prompted for a password when entering a workspace at a new label.

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.

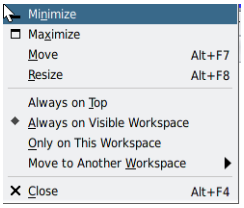
How to Move a Window to a Different Workspace

If you drag a window to a workspace at a different label, the window retains its original label. Any actions in that window is performed 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 the panel display, drag the window from one panel to a different panel.**

   The dragged window now appears in the second workspace.

2. **To display the window in all workspaces, choose Always Visible from the right-button menu in the title bar.**



The selected window now appears in every workspace.

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 label 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 Browser.

- **Use the File Browser.**

Tip - You can also use the Query Label menu item from the Trusted Path menu.

How to Move Data Between Windows of Different Labels

As on an Oracle 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, the containing zone must permit relabeling, and you must be authorized to move data between labels.

Therefore, your administrator must have completed the following tasks:

- "How to Enable Files to Be Relabeled From a Labeled Zone" in "Trusted Extensions Configuration and Administration "
- "How to Enable a User to Change the Security Level of Data" in "Trusted Extensions Configuration and Administration "

You must be logged in to a multilevel session.

1. **Create workspaces at both labels.**

   For details, see "How to Add a Workspace at Your Minimum 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 52.

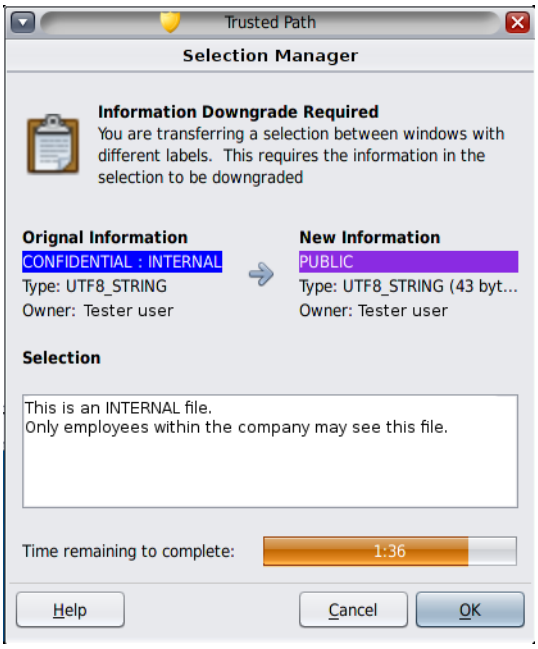
3. **Move the window with the source information to a workspace at the target label.**

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

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

   The Selection Manager Confirmation dialog box is displayed.

FIGURE 3-5 Selection Manager Confirmation Dialog Box



5. **Review the Selection Manager Confirmation dialog box, then confirm or cancel the transaction.**

   This dialog box:

   - Describes why confirmation of the transaction is needed.
   - Identifies the label and the owner of the source file.
   - Identifies the label and the 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 default, the selected data is visible in text format.
   - 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.

How to Upgrade Data in a Multilevel Dataset

Multilevel datasets in Trusted Extensions ease the task of relabeling files. For more information about multilevel datasets, see “Multilevel Datasets for Relabeling Files” in “Trusted Extensions Configuration and Administration ”.

Before You Begin You must be authorized to relabel files. You can operate at two or more labels, one of which dominates the other.

A multilevel dataset is mounted in at least one of the labeled zones, and the mount name is identical, such as `/multi`, in every zone that mounts the dataset.

To permit relabeling, your administrator must have completed the following tasks:

- “How to Create and Share a Multilevel Dataset” in “Trusted Extensions Configuration and Administration ”
- “How to Enable Files to Be Relabeled From a Labeled Zone” in “Trusted Extensions Configuration and Administration ”
- “How to Enable a User to Change the Security Level of Data” in “Trusted Extensions Configuration and Administration ”

You must be logged in to a multilevel session.

1. **Create a workspace at the higher label.**

   For example, to upgrade a file from `PUBLIC` to `INTERNAL`, create a workspace at the `INTERNAL` label.

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

2. **Open a terminal window and list the directory that contains the file to be upgraded.**

   In this example, the filename is `temppub1`.

   ```
   $ ls /multi/public
   temppub1
   ```

3. **Relabel the file.**

   ```
   $ setlabel "cnf : internal" /multi/public/temppub1
   ```

4. **Verify the label change.**

   ```
   $ getlabel  /multi/public/temppub1
   /multi/public/temppub1: "CONFIDENTIAL : INTERNAL USE ONLY"
   ```

5. **(Optional) Move the file to a directory at the target label.**

   ```
   $ mv /multi/public/temppub1 /multi/internal/temppub1
   ```

How to Downgrade Data in a Multilevel Dataset

To downgrade date, you first move the file to its target directory, then relabel it. For an explanation, see "Multilevel Datasets for Relabeling Files" in "Trusted Extensions Configuration and Administration ".

Before You Begin You must be authorized to downgrade files. The administrator has mounted a multilevel dataset in at least one of the labeled zones, and has used a standard name, such as `/multi`, for all mounts of the dataset that you can access, and has permitted relabeling in that zone.

Therefore, your administrator must have completed the following tasks:

- "How to Create and Share a Multilevel Dataset" in "Trusted Extensions Configuration and Administration "
- "How to Enable Files to Be Relabeled From a Labeled Zone" in "Trusted Extensions Configuration and Administration "
- "How to Enable a User to Change the Security Level of Data" in "Trusted Extensions Configuration and Administration "

You must be logged in to a multilevel session.

1. **Create a workspace at the label of the source file.**

   For example, create an `internal` workspace.

   For details, see "How to Add a Workspace at Your Minimum Label" on page 51.

2. **Open a terminal window and open a profile shell.**

   ```
   % pfbash
   $
   ```

3. **(Optional) Confirm the label of the source file and its containing directory.**

   For details, see "How to Determine the Label of a File" on page 52.

   Note - If the source file is at the same label as its parent directory, it cannot be downgraded in place. You must move the file. Moving the file is a privileged operation.

4. **Move the source file to a directory at the target label.**

   ```
   $ mv /multi/internal-directory/file /multi/public-directory
   ```

5. **Change the label to the label of the target directory.**

   ```
   $ cd /multi/public-directory
   $ setlabel public file
   ```

6. **(Optional) Verify that the file has been relabeled.**

```
$ getlabel /multi/public-directory/file
/multi/public-directory/file: PUBLIC
```

You can edit the file at the `PUBLIC` label.

Example 3-6 Changing the Label of a Directory

In this example, an authorized user relabels a directory.

First, the user moves or removes all files from the directory.

```
$ getlabel /multi/conf
/multi/conf: CONFIDENTIAL : NEED TO KNOW
$ mv /multi/conf/* /multi/confNTK/temp
```

Then, the user sets the label of the directory and verifies the new label.

```
$ setlabel "Confidential : Internal Use Only" /multi/conf
getlabel /multi/conf
/multi/conf: "CONFIDENTIAL : INTERNAL USE ONLY"
```

♦ ♦ ♦ CHAPTER 4

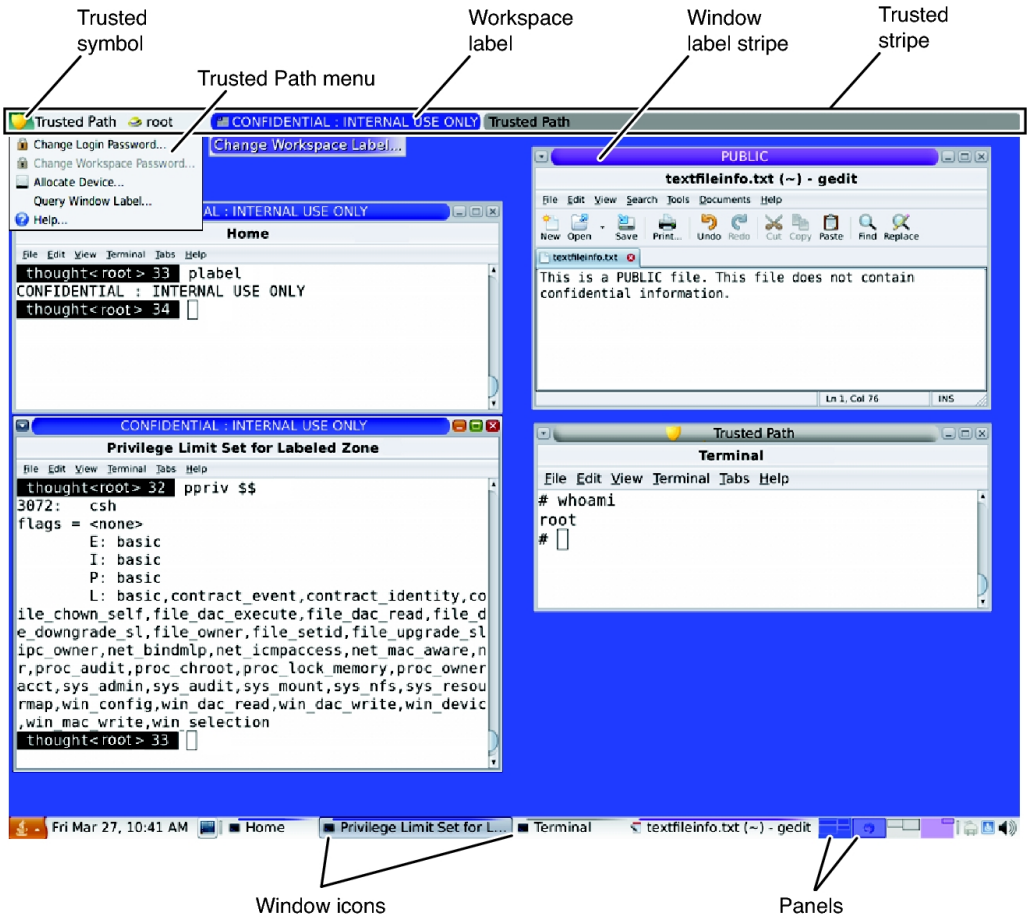
Elements of Trusted Extensions

This chapter explains the key elements of Trusted Extensions. This chapter covers the following topics:

Visible Features of Trusted Extensions

After you have successfully completed the login process, as explained in Chapter 2, "Logging In to Trusted Extensions", 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, several features distinguish a system that is configured with Trusted Extensions from an Oracle Solaris system.

FIGURE 4-1 Trusted Extensions Multilevel Desktop



- **Label displays –** All windows, workspaces, files, and applications have a label. The desktop provides label stripes and other indicators for viewing an entity's label.
- **Trusted stripe –** This stripe is a special graphical security mechanism. In every workspace, the stripe is displayed at the top of the screen.
- **Limited access to applications from the workspace –** The workspace provides access to only those applications that are permitted in your account.
- **Trusted Path menu –** The trusted symbol provides access to the menu.

Labels on Trusted Extensions Desktops

As discussed in “Mandatory Access Control” on page 15, all applications and files in Trusted Extensions have labels. Trusted Extensions displays labels in the following locations:

- Window label stripes above the window title bar
- Label color stripe above the window icon in the window list
- Window label indicator in the trusted stripe
- Query window label indicator from the Trusted Path menu that displays the label of the window or window icon that is specified by the pointer location

In addition, the color of the panels indicate the label of the workspace.

FIGURE 4-2 Panels Indicating Workspaces at Different Labels

Figure 4-1 shows how labels display on a Trusted Extensions desktop. Also, the Query Window Label menu item can be used to display the label of a window. For an illustration, see Figure 3-2.

Trusted Stripe

The trusted stripe appears at the top of the screen.

FIGURE 4-3 Trusted Stripe on the Desktop

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

The trusted stripe has the following elements:

- **The trusted symbol –** Displays when the screen focus is security-related

- **The window label –** Displays the label of the active window when the screen focus is not security-related
- **A role marker –** At the right of the trusted symbol, before the account name, displays a hat icon if the account is a role account
- **The current account name –** At the right of the trusted symbol, displays the name of the owner of new processes in the workspace
- **Labeled windows –** Displays the labels of all windows in the workspace

Trusted Symbol

Whenever you access any portion of the TCB, the trusted symbol appears at the left of the trusted stripe area.

The trusted symbol is not displayed when the mouse 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 TCB.

Caution - If the trusted stripe is missing from your workspace, contact the security administrator. The problem with your system could be serious.

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

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 TCB. For example, when you change your password, the Trusted Path indicator displays in the trusted stripe.

Device Security in Trusted Extensions

By default in Trusted Extensions, devices are protected by device allocation requirements. Users cannot use a device without being given explicit authorization to allocate devices, and an

allocated device cannot be used by another user. A device in use at one label cannot be used at another label until it is deallocated from the first label and allocated at the second label.

To use a device, see “How to Allocate a Device in Trusted Extensions” on page 47.

Files and Applications in Trusted Extensions

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

In Trusted Extensions, files are objects in data transactions. Files can be accessed only 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

The `.copy_files` file stores file names to be copied when you first change to a workspace with a higher label. This file 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. The `.copy_files` file enables you to specify that the application update the file at every label.

`.link_files` File

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

Password Security in the Oracle Solaris OS

Users who change passwords on a frequent basis shorten the window of opportunity for intruders to use illegally obtained passwords. Therefore, your site's security policy can require you to change your password regularly. The Oracle Solaris OS can set content requirements for passwords and enforce password 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 are sent an email message that warns you to change your password prior to the cutoff date.

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

- 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 must 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 by using the Change Password menu item from the Trusted Path menu. For the steps, see “How to Change Your Password in Trusted Extensions” on page 45.

Workspace Security in Trusted Extensions

In Trusted Extensions, the workspaces and desktop applications are label-aware. Applications run at the label of the current workspace and display information only at the label of the process that opened the application.

The behavior and location of security features for the trusted desktop are as follows:

- The Trusted Path menu is available from the trusted stripe.
- The label name of a window in the task list on the panel appears in a tooltip when the mouse hovers over the window. Similarly, the label name of a workspace in the switch area appears in the tooltip.
- To change a role, you click the account name in the trusted stripe and choose the role.
- To add a workspace at a particular label, you select an existing workspace and change its label.
- The desktop is configured so that each workspace reflects the color of the label at which you are working in that workspace. The panels on the bottom stripe also display the label color.

Glossary

access control list (ACL) A security feature of the Oracle 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.

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 Oracle 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, audio devices, and CD-ROM devices. See also device allocation.

audit ID (AUID) A security feature of the Oracle 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 Oracle 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 *audit trail*. Auditing produces system activity reports to fulfill site security policy.

authorization A security feature of the Oracle 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 classification 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.

compartment A nonhierarchical component of a label that is 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 *Security Requirements for System High and Compartmented Mode Workstations*, DIA document number DDS-2600-5502-87. Specifically, it defines a trusted, X Window System-based operating system for UNIX workstations.

covert channel 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 Oracle 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 Oracle 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 Manager.

Device 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 *equal*. If one label dominates the other and the labels are not equal, the first label is said to *strictly dominate* the other. Two labels are *disjoint* 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 Oracle 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 `setuid` 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 `tnrhtp` database. For IPv4 addresses, the fallback mechanism recognizes `0` 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 Oracle 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 `tnrhtp` 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 `tnrhtp` database. The host type determines whether

the CIPSO network protocol is used to communicate with other hosts on the network. *Network protocol* refers to the rules for packaging communication information.

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 `ADMIN_HIGH` and `ADMIN_LOW`, the labels `RESTRICTED` and `PUBLIC` can be substituted.

labeled workspace A workspace that is associated with a label. 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. Every workspace on a trusted desktop is labeled. Two workspaces can be associated with the same 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 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.

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.

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 *r*) lets the user read the contents of a file or, if a directory, list the files in the folder. Write permission (*w*) lets the user make changes to a file or, if a folder, add or delete files. Execute permission (*e*) lets the user run the file if 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 the Oracle Solaris OS 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 Oracle 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 Oracle Solaris OS.. A privileged process runs with assigned has privileges.

process A running program. Trusted Extensions processes have Oracle 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 Oracle 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 Oracle Solaris OS.. A rights profile enables a site's security administrator to bundle commands with security attributes. Attributes such as user

	authorizations and privileges enable the commands 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 Oracle 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 Oracle 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-level 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 Oracle 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 GNOME A labeled graphical desktop that includes a session manager, a window manager, and various desktop tools. The desktop is fully accessible.

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. The trusted stripe has two components: (1) a mandatory trusted symbol to indicate interaction with the trusted computing base (TCB), and (2) a 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 Oracle Solaris OS.. A UID identifies a user for the purposes of discretionary access control (DAC), mandatory access control (MAC), and auditing. See also access permission.

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

M

N

O

P

Q

R

S

T

U

V

W

Z