Oracle® Solaris Trusted Extensions Label Administration

Part No: 819–0873–12
September 2010

ORACLE

100706@24378

Contents

Figures

Tables

Preface

Labels, clearances, and handling instructions are used to protect information on a system that is configured with the Oracle Solaris' Trusted Extensions feature. The components of labels, clearances, and handling instructions are specified in the `label_encodings` file. This guide provides background for creating or modifying the file. The guide provides examples, and helps you to create and install a `label_encodings` file that is appropriate for your site.

Who Should Use This Book

This book is for security administrators. Security administrators are responsible for defining the organization's labels. Some security administrators are also responsible for implementing the labels. This book is for definers and implementers.

Note – Labels are always being used. Labels provide mandatory access control (MAC), and MAC is always enforced. Therefore, the site's `label_encodings` file must be in place before any users or roles are created.

Trusted Extensions installs a default `label_encodings` file. The security administrator must provide a file that is appropriate for the site.

The security administrator who implements the labels should be familiar with Solaris administration. The necessary level of knowledge can be acquired through training and documentation. For details, see "Documentation, Support, and Training" on page 13.

How the Solaris Trusted Extensions Books Are Organized

The Solaris Trusted Extensions documentation set supplements the documentation for the Solaris release. Review both sets of documentation for a more complete understanding of Solaris Trusted Extensions. The following table lists the topics that are covered in the Solaris Trusted Extensions guides and the audience for each guide.

Book Title	Topics	Audience
Oracle Solaris Trusted Extensions User's Guide	Describes the basic features of Solaris Trusted Extensions. This book contains a glossary.	End users, administrators, developers
Oracle Solaris Trusted Extensions Administrator's Procedures	Shows how to perform specific administration tasks. Part I describes how to prepare for, enable, and initially configure Trusted Extensions. Part II describes how to administer a Trusted Extensions system. This book contains a glossary.	Administrators, developers
Oracle Solaris Trusted Extensions Developer's Guide	Describes how to develop applications with Solaris Trusted Extensions.	Developers, administrators
Oracle Solaris Trusted Extensions Label Administration	Provides information about how to specify label components in the label encodings file.	Administrators
Compartmented Mode Workstation Labeling: Encodings Format	Describes the syntax used in the label encodings file. The syntax enforces the various rules for well-formed labels for a system.	Administrators

How This Book Is Organized

- Chapter 1, "Labels in Trusted Extensions Software," discusses labels-related concepts for the security administrator who prepares the site's `label_encodings` file.
- Chapter 2, "Planning Labels (Tasks)," provides planning steps for the security administrator who prepares the site's `label_encodings` file. This chapter also describes the encodings files that Trusted Extensions provides.
- Chapter 3, "Making a Label Encodings File (Tasks)," describes how to create, customize, and check the `label_encodings` file.
- Chapter 4, "Labeling Printer Output (Tasks)," describes the labels and handling instructions on printer output and gives procedures for modifying them.
- Chapter 5, "Customizing `LOCAL DEFINITIONS`," describes the optional `LOCAL DEFINITIONS` section of the `label_encodings` file.
- Chapter 6, "Example: Planning an Organization's Labels," models how a site analyzes its label requirements and creates a `label_encodings` file.
- Appendix A, "Sample Label Encodings File," contains the example of the `label_encodings` file from Chapter 6, "Example: Planning an Organization's Labels."

Documentation, Support, and Training

See the following web sites for additional resources:

- Documentation (`http://docs.sun.com`)
- Support (`http://www.oracle.com/us/support/systems/index.html`)
- Training (`http://education.oracle.com`) – Click the Sun link in the left navigation bar.

Oracle Welcomes Your Comments

Oracle welcomes your comments and suggestions on the quality and usefulness of its documentation. If you find any errors or have any other suggestions for improvement, go to `http://docs.sun.com` and click Feedback. Indicate the title and part number of the documentation along with the chapter, section, and page number, if available. Please let us know if you want a reply.

Oracle Technology Network (`http://www.oracle.com/technetwork/index.html`) offers a range of resources related to Oracle software:

- Discuss technical problems and solutions on the Discussion Forums (`http://forums.oracle.com`).
- Get hands-on step-by-step tutorials with Oracle By Example (`http://www.oracle.com/technology/obe/start/index.html`).
- Download Sample Code (`http://www.oracle.com/technology/sample_code/index.html`).

Typographic Conventions

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

TABLE P–1 Typographic Conventions

Typeface	Meaning	Example
`AaBbCc123`	The names of commands, files, and directories, and onscreen computer output	Edit your `.login` file. Use `ls -a` to list all files. `machine_name% you have mail.`
`AaBbCc123`	What you type, contrasted with onscreen computer output	`machine_name%` **`su`** `Password:`
aabbcc123	Placeholder: replace with a real name or value	The command to remove a file is `rm` *filename*.

TABLE P–1 Typographic Conventions *(Continued)*

Typeface	Meaning	Example
AaBbCc123	Book titles, new terms, and terms to be emphasized	Read Chapter 6 in the *User's Guide*. A *cache* is a copy that is stored locally. Do *not* save the file. **Note:** Some emphasized items appear bold online.

Shell Prompts in Command Examples

The following table shows the default UNIX system prompt and superuser prompt for shells that are included in the Oracle Solaris OS. Note that the default system prompt that is displayed in command examples varies, depending on the Oracle Solaris release.

TABLE P–2 Shell Prompts

Shell	Prompt
Bash shell, Korn shell, and Bourne shell	`$`
Bash shell, Korn shell, and Bourne shell for superuser	`#`
C shell	`machine_name%`
C shell for superuser	`machine_name#`

◆ ◆ ◆ CHAPTER 1

Labels in Trusted Extensions Software

This chapter prepares the security administrator to create the file that encodes labels for Trusted Extensions. This chapter covers the following topics:

This chapter assumes that you have read the following sections:

- Chapter 3, "Getting Started as a Trusted Extensions Administrator (Tasks)," in *Oracle Solaris Trusted Extensions Administrator's Procedures* guide, which prepares the security administrator to assume the Security Administrator role
- "Labels in Trusted Extensions Software" in *Oracle Solaris Trusted Extensions Administrator's Procedures*

Labels and Security Policy

Site security policy is the security policy that an organization sets up to protect its proprietary information. With Trusted Extensions software, labels and mandatory access control (MAC) can be part of this policy. Labels implement a set of rules that is a part of *system security policy*. System security policy is the set of rules that is enforced by system software to protect information that is being processed on the system. The term security policy can refer to policy or to implementation of the policy.

All systems that are configured with Trusted Extensions have labels. Labels are specified in a `label_encodings` file. For a description of the file, see the `label_encodings(4)` man page. For descriptions of the encodings files that are delivered with Solaris Trusted Extensions packages, see "Sources for Encodings Files" on page 38.

Trusted Extensions installs a default version of the `label_encodings` file. The default version supplies several commercial labels. This version can sometimes be used in non-production environments for learning purposes. A site can also customize one of the label encodings files

that are delivered with the Solaris Trusted Extensions packages. For an example of a site-specific file, see Appendix A, "Sample Label Encodings File."

Every computer in the Trusted Extensions network needs its own copy of the site's `label_encodings` file. For interoperability, the `label_encodings` file on every computer in the network should be compatible. At the very least, each computer should recognize the labels on every other computer in the network.

Certain types of labels must be defined. The security administrator specifies the numeric values and the bits that make up the internal representation of labels. Users and roles see the textual representation of labels. The labeling software translates between the internal form and the textual form of labels. The `label_encodings` file provides the rules for translating the internal representation of labels to their textual strings. The textual strings can be visible on the desktop. The internal representation is recorded in the audit trail and is interpreted by the `praudit` command.

The *security administrator* is the person who defines and plans the implementation of an organization's security policy. The security administrator establishes information-protection procedures, makes sure computer users and administrators are properly trained, and monitors compliance.

The Security Administrator *role* is created in the software. The role is assigned to one or more administrators who fully understand Trusted Extensions administration. These administrators are cleared to view and to protect the highest level of information that is processed by Trusted Extensions. One of the responsibilities of the security administrator is to create the site's `label_encodings` file to replace the version that Trusted Extensions installs. The administrator can also decide whether labels are visible on the desktop. Even when labels are not visible, objects and processes on the system are labeled, and MAC is enforced.

Trusted Extensions provides the Security Administrator role with the tools and capabilities to put the organization's security policy into effect. To assume the role, you first log in as an ordinary user, then assume the role. At your site, the security administrator who defines the site's security policy might or might not be the same person who implements the policy.

Types of Labels, Their Components and Uses

Trusted Extensions defines two types of labels:

- Clearance labels, or *clearances*
- Sensitivity labels, often referred to as *labels*

Sensitivity labels, label ranges, and a label limit or *clearance* determine who can access what objects on the system. Clearance labels are assigned to users. Sensitivity labels are assigned to processes, including users' processes, and to files and directories.

Some objects have a label range. These objects can be accessed at a particular label within the defined label range. A label range from `ADMIN_LOW` to `ADMIN_HIGH` allows access at all labels. The security administrator can narrow that label range. Objects with label ranges include the following:

- All hosts and networks with which communications are allowed
- Zones
- Users and roles
- Allocatable devices, such as tape drives, floppy drives, CD-ROM and DVD devices, and audio devices
- Other devices that are not allocatable, for example, printers, workstations (controlled through the label range of the frame buffer), and serial lines when they are used as a login device

The various means for setting labels on these objects is described in *Oracle Solaris Trusted Extensions Administrator's Procedures*. "Device Allocation Manager GUI" in *Oracle Solaris Trusted Extensions Administrator's Procedures* describes how to set label ranges on devices.

Label Ranges Restrict Access

Label ranges set limits on the following:

- The labels at which hosts can send and receive information.
- The labels at which processes acting on behalf of users and roles can access files and directories in zones.
- The labels at which users can allocate devices, thereby restricting the labels at which files can be written to storage media in these devices.
- The labels at which users can send jobs to printers.
- The labels at which users can log in to workstations. In addition to the user's label range, a label range on the frame buffer can be used to restrict access to a system.

Labels are automatically assigned to email messages, and the labels then show on printed emails.

Labels Are Used in Access Control Decisions

Labels are used to implement and control access on a computer. Labels implement mandatory access control (MAC). With Trusted Extensions, both discretionary access control (DAC) checks and MAC checks must pass before access is allowed to an object. As in the Solaris OS, DAC is based on permission bits and access control lists (ACLs). For more information, see Chapter 6, "Controlling Access to Files (Tasks)," in *System Administration Guide: Security Services*.

MAC compares the label of a process that is running an application with the label or the label range of any object that the process tries to access. The labels implement the set of rules that enforce policy. One rule is read down-read equal. This rule applies when a process tries to access an object. The label of the process has to be greater than or equal to the label of the object, as in:

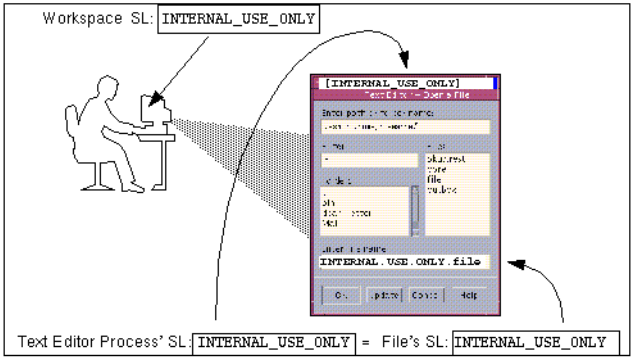
```
Label[Process] >= Label[Object]
```

On a system that is configured with Trusted Extensions, files and directories have slightly different access rules from each other and from process objects, network endpoint objects, device objects, and X window objects. In addition, an object can be accessed in three different ways. For each of the three ways that an object can be accessed, a slightly different set of rules applies:

- The name of the file, directory, or device can be viewed
- The contents or the attributes of the file, directory, or device can be viewed
- The contents or the attributes of the file, directory, or device can be modified

Figure 1–1 shows a system that uses labels to make an access control decision.

FIGURE 1–1 Comparing the Label of a Text Editor with the Label of a File



In the preceding figure, a user brings up a text editor in a workspace with the label `INTERNAL_USE_ONLY`. The system sets the label of the process that is running the text editor to be equal to the label of the current workspace. Therefore, the text editor displays a label of `INTERNAL_USE_ONLY`. When the text editor attempts to open a file for editing, the label of the process that is running the text editor is compared to the label of the file. When the two labels are equal, access for writing is allowed.

If the label of a file is less than the label of the text editor, the file can be opened for reading only. For example, the `INTERNAL_USE_ONLY` text editor can open and read a system file at `ADMIN_LOW`,

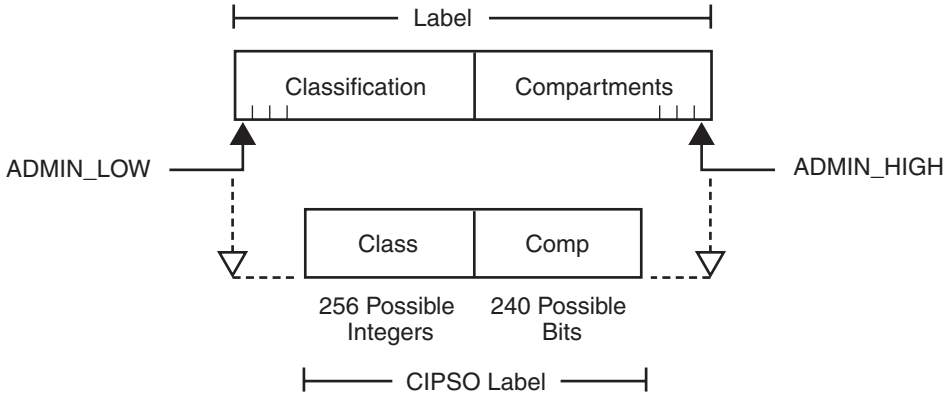
but the text file cannot be changed. Also, because of the read down requirement, a user cannot see a file whose label is higher than the current working label.

Label Components

Labels and clearances consist of a single *classification* and zero or more *compartment* words. The classification portion of a label indicates a *relative level of protection*. When a label is assigned to an object, the label's classification indicates the sensitivity of the information that is contained in the object. When a clearance is assigned to a user, the classification portion of the clearance label indicates the user's level of trust.

Trusted Extensions supports Common IP Security Option (CIPSO) labels. Each label and clearance label has a classification field that allows 256 values, and a 256-bit compartments field. You cannot use 0 (zero) for a classification, so you can define a total of 255 classifications. For CIPSO labels, 240 compartment bits are available, for a total of 2^{240} compartment combinations. The components are illustrated in the following figure.

FIGURE 1–2 CIPSO Label Definition



The `ADMIN_HIGH` label and the `ADMIN_LOW` label are administrative labels. These labels define the upper and lower bound of all labels on a system.

Each compartment word has one or more compartment bits assigned. The same compartment bit can be assigned to more than one word.

The textual format of a classification appears similar to the following:

```
CLASSIFICATIONS:

name= TOP SECRET; sname= TS; value= 6;initial compartments= 4-5;
```

The compartment portion of a label is optional. Compartment words in a label can be used to represent different kinds of groupings, such as work groups, departments, divisions, or geographical areas. Compartment words can also further identify how information should be handled.

When initial compartments are part of the classification definition, then compartments are part of that label.

```
WORDS:

name= A;          compartments= 0;
name= B;          compartments= 1;
name= CNTRY1;      sname= c1;      compartments= ~4;
name= CNTRY2;    sname= c2;      compartments= ~5;
```

Possible labels from the preceding classifications and compartments include TS, TS A, TS B, and TS AB. A file with TS A would be available only to individuals who have the TS classification and the A compartment in their clearances. For an illustration, see Figure 1–3.

Label Dominance

When any type of label has a security level that is equal to or greater than the security level of a second label, the first label is said to *dominate* the second label. This comparison of security levels is based on classifications and compartments in the labels. The classification of the dominant label must be equal to or higher than the classification of the second label. Additionally, the dominant label must include all the compartments in the second label. Two equal labels are said to dominate each other.

By these criteria, TS A dominates TS, and TS dominates TS. The classification and compartment bits of the TS label are shown in the following figure.

FIGURE 1–3 Representation of the TS, TS A, TS B, and TS AB Labels


```
TOP SECRET        A
value = 6         compartments = 0
                  B
                  compartments = 1
```

Another kind of dominance, *strict dominance*, is sometimes required for access. One label *strictly dominates* another label when the first label has a security level that is greater than the

security level of the other label. Strict dominance is dominance without equality. The classification of the first label is higher than the classification of the second label. The first label contains all the compartments in the second label. Or, if the classifications of both labels are the same, the first label contains all the compartments in the second label plus one or more additional compartments.

Labels that are not in a dominance relationship are said to be *disjoint*. Disjoint labels would be appropriate to separate departments at a company. For example, the label `TS HR` (Human Resources) would be disjoint from `TS Sales`.

Accreditation Ranges, Label Ranges, and Valid Labels

Certain combinations of label components can be disqualified by rules in the `label_encodings` file. Combination rules *implicitly* define the organization's usable labels. The security administrator is responsible for specifying combination rules.

A *valid* or *well-formed* label is a label that satisfies a combination rule. The security administrator defines combination rules by using one of the following means:

- *Initial compartments* (compartment bits) can be assigned to a classification.

  Initial compartment bits are always associated with the classification in a label. For more details, see "Classification Name Syntax" on page 45.
- A *minimum classification*, an *output minimum classification*, and a *maximum classification* can be associated with any word.
- *Hierarchies* among words can be defined by the *bit patterns* that are chosen for each word.
- *Required combinations* of words can be specified.
- *Combination constraints* can be specified for words.
- A *minimum clearance* and a *minimum sensitivity label* must be specified.

  These system-wide minimums establish the lowest clearance and the lowest label that any ordinary user can have.

Two *accreditation ranges* are implicitly specified in the `label_encodings` file:

- "System Accreditation Range" on page 22
- "User Accreditation Range" on page 23

The term *accreditation range* is also used for the label ranges that are assigned to user and role accounts, printers, hosts, networks, and other objects. Because rules can constrain the set of valid labels, label ranges and accreditation ranges might not include all the potential combinations of label components in a range.

System Accreditation Range

The system accreditation range includes the administrative labels `ADMIN_HIGH` and `ADMIN_LOW`. The system accreditation range also includes all the well-formed labels that are constructed from the label components in the `label_encodings` file.

Administrative role accounts are usually the only accounts that can work at every label within the system accreditation range. An organization can also set up ordinary user accounts to be able to perform a task that requires an administrative label.

The following figure presents an example of how rules can constrain the labels permitted in a system accreditation range.

FIGURE 1–4 How System Accreditation Range Is Constrained By Rules

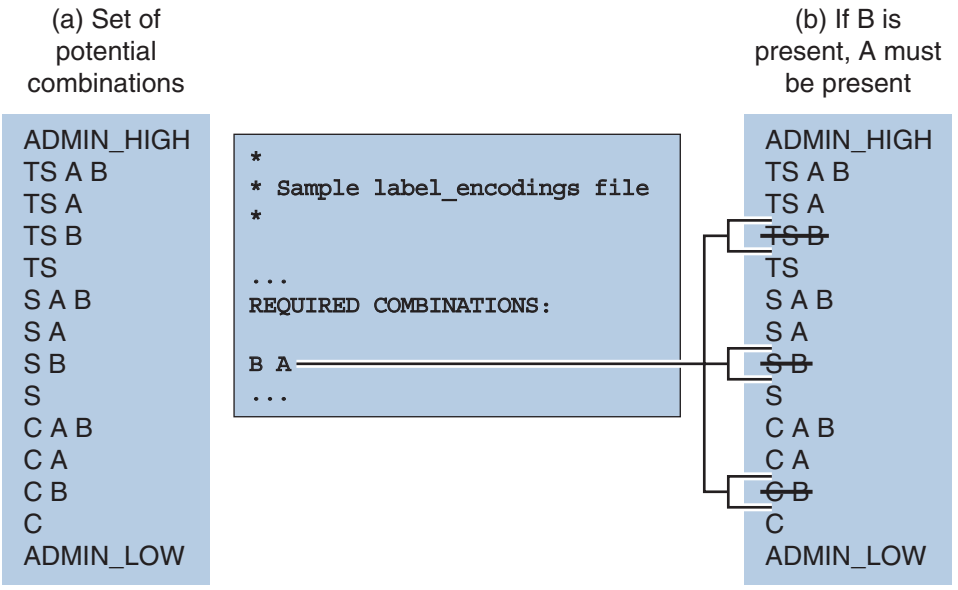


Figure 1–4 (a) shows all potential combinations given the classifications, `TS` (`TOP SECRET`), `S` (`SECRET`), and `C` (`CONFIDENTIAL`), and the compartments, `A` and `B`.

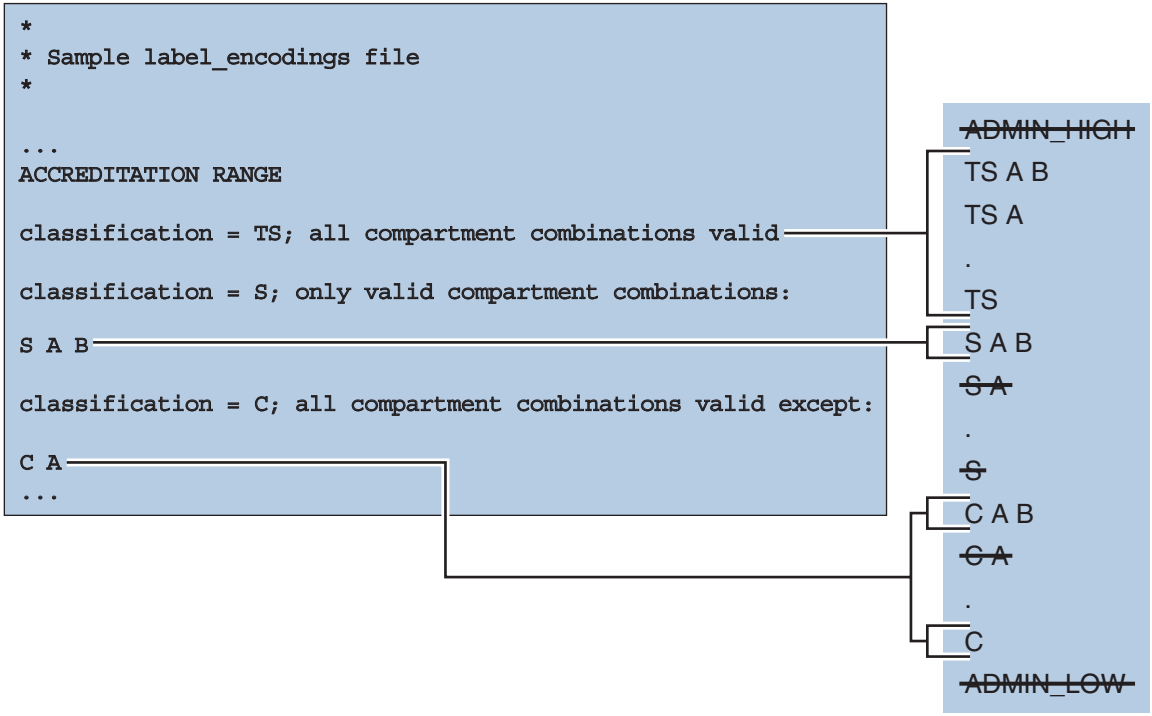
Figure 1–4 (b) shows a typical rule from the `REQUIRED COMBINATIONS` subsection of the `SENSITIVITY LABELS` section and its effects. The arrows point to the labels that are disqualified by the rule. Disqualified labels appear with lines through the labels. The `REQUIRED COMBINATIONS` syntax `B A` means that any label that has `B` as a compartment must also contain `A`. The converse is not true. Compartment A is not required to be combined with any other

compartments. Since compartment B is only permitted when A is also present, the labels TS B, S B, and C B are not well-formed. Labels that are not well-formed are not in the system accreditation range.

User Accreditation Range

The *user accreditation range* is the largest set of labels that ordinary users can access when using Trusted Extensions. The user accreditation range always excludes ADMIN_HIGH and ADMIN_LOW. The user accreditation range is further constrained by any rules that constrain the "System Accreditation Range" on page 22. In addition, the user accreditation range can be constrained by a set of rules in the ACCREDITATION RANGE section. Figure 1–5 continues the Figure 1–4 example. Figure 1–5 shows three different types of rules in the ACCREDITATION RANGE section and their effects on the user accreditation range. The arrows point to the well-formed labels that the particular rule permits.

FIGURE 1–5 ACCREDITATION RANGE Portion of label_encodings File



As shown in the box to the right, the user accreditation range excludes ADMIN_HIGH and ADMIN_LOW. The rule for the TS classification includes all TS combinations except TS B.

However, because TS B, and S B and C B, were previously overruled by the REQUIRED COMBINATIONS rule B A, as shown in Figure 1–4, TS A B, TS A, and TS are the only allowed TS combinations. Because S A B is defined as the only valid combination for the S classification, S B is excluded again. All C combinations except C A are valid according the rule for the C classification. However, because C B was overruled earlier, the only permitted combinations for the C classification are C A B and C.

Account Label Range

The *account label range* is the range of labels that is available to an individual user or to a role account. This range governs the labels at which the user can work when logging in to the system.

The labels that are available in the account label range have the following constraints:

- The user clearance defines the top of the account label range.

  A clearance does not have to be a valid label. Because it must dominate all labels at which the account is to work, the clearance must contain all the components of all the labels at which the account is to work.
- The minimum label sets the bottom of the account label range.

  The minimum sensitivity label in the label_encodings file defines an absolute minimum on labels at which any user can work.
- The user accreditation range defines the set of valid labels from the user's clearance to the user's minimum label.

EXAMPLE 1–1 Defining a Valid Clearance That Is Not a Valid Label

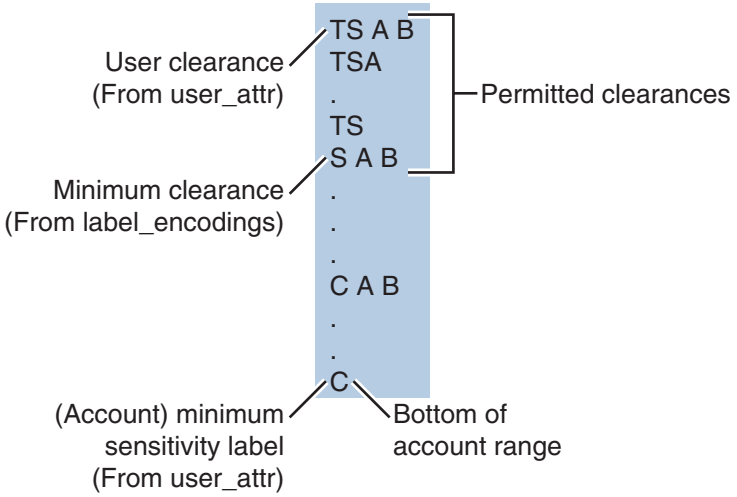
For example, a label_encodings file could prohibit the combination of compartments A, B, and C in a label.

- The minimum label would be TS with no compartments.
- TS A B C would be a valid clearance. TS A B C would not be a valid label.
- Valid labels for a user would be TS, TS A, TS B, and TS C.

Account Label Range Examples

The possible clearances and minimum labels that can be assigned to an account are shown in the following figure. These labels are based on the accreditation examples from the previous sections.

FIGURE 1–6 Constraints on Account Label Ranges



In this example, TS A B is the highest label in the user accreditation range. This label contains the only two compartments, A and B, that are permitted to appear together in a label with any classification. The account range that is illustrated on the left is bounded at the top by TS A B. TS A B is the clearance assigned to the account. C is the account's minimum label. These definitions constrain the account to work at labels TS A B, TS A, TS, S A B, C A B, or C. The permitted clearances are TS A B, TS A, TS and S A B. A minimum clearance of S A B is set in the `label_encodings` file.

Even if TS A B was not a valid label, the security administrator could assign the label as a clearance. The assignment would allow the account to use any valid labels that are dominated by TS and that contain the words A and B. In contrast, if TS was assigned as the account clearance, the user could work at the labels TS and C only. TS without any compartments does not dominate S A B or C A B.

TABLE 1–1 Accreditation Range and Account Label Range Examples

	Accreditation Range		**Account Label Range**		
Possible Labels	**System**	**User**	TS A B **Clearance,** S A B **Min Label**	TS **Clearance,** C **Min Label**	ADMIN_LOW **Clearance and Min Label,** `solaris.label.range` **Authorization**
ADMIN_HIGH	ADMIN_HIGH				
TS A B	TS A B		TS A B		
TS A	TS A	TS A	TS A		
TS	TS	TS	TS	TS	
S A B	S A B	S A B	S A B		

TABLE 1–1 Accreditation Range and Account Label Range Examples *(Continued)*

	Accreditation Range		Account Label Range		
Possible Labels	**System**	**User**	`TS A B` **Clearance,** `S A B` **Min Label**	`TS` **Clearance,** `C` **Min Label**	`ADMIN_LOW` **Clearance and Min Label,** `solaris.label.range` **Authorization**
`S A`					
`S`				`S`	
`C A B`	`C A B`				
`C A`	`C A`				
`C`	`C`	`C`		`C`	
`ADMIN_LOW`	`ADMIN_LOW`				`ADMIN_LOW`

Table 1–1 illustrates the differences between the potential label combinations, the system accreditation range, the user accreditation range, and some sample account label ranges.

- Ordinary users without any authorizations can work only with the labels in the User Accreditation Range column.
- The fourth column shows the Account Label Range for a user with a clearance of `TS A B` and a minimum label of `S A B`. This range allows the user to work with the labels `TS A B`, `TS A`, `TS`, and `S A B`.
- The fifth column of Table 1–1 shows an account with a clearance of `TS` and a minimum label of `C`. This account would be allowed to work only with `TS`, `S`, and `C` labels, because all the other valid labels that are dominated by `TS` include the words `A` and `B`. `A` and `B` are not in the clearance.
- A sixth column shows a user who is authorized to work outside the user accreditation range. This user is assigned a single label of `ADMIN_LOW`.

Session Range

The *session range* is the set of labels that is available to a user account during a Trusted Extensions session. The session range is a function of the following constraints:

- The label range of the user
- The label that the user chose
- The label range of the local system

The session range of a single-label account is the label of the account. A range of labels to choose from is possible only when a user account is configured to use multiple labels. User accounts that are configured to use multiple labels can choose different labels during the session. To specify a label, see "How to Change the Label of a Workspace" in *Oracle Solaris Trusted Extensions User's Guide*.

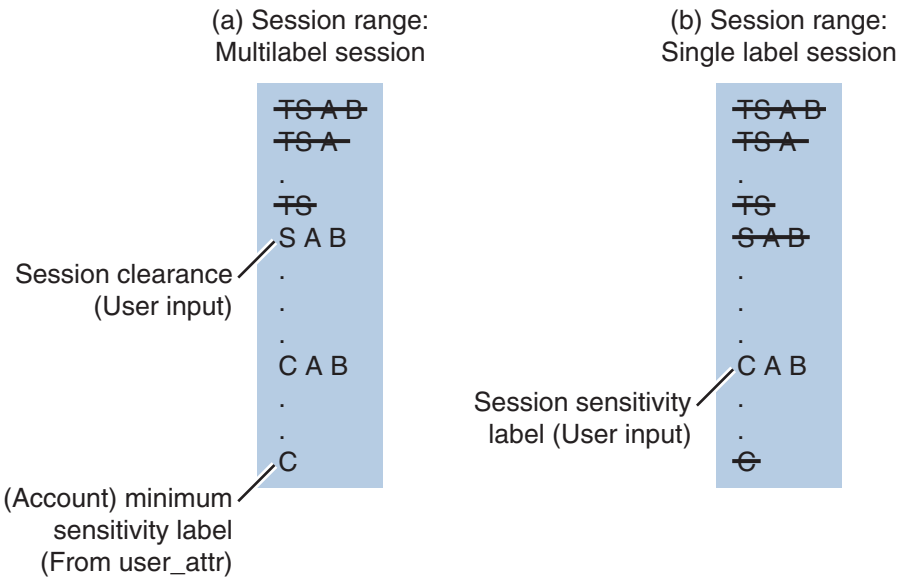
The single label or session clearance that is chosen at login is in effect throughout the session until logout. During a multilabel session, the user can work at any valid label that is dominated by the session clearance and that dominates the user's minimum label.

Example Figure 1–6 is continued in Figure 1–7. In this example, the user can specify a session clearance that uses any well-formed label between TS A B and S A B.

The (a) portion of Figure 1–7 shows the labels that are available if the user selects a multilabel session with a session clearance of S A B. Because the other intermediate labels between S A B and C are not well-formed, the user can only work at S A B, C A B, or C.

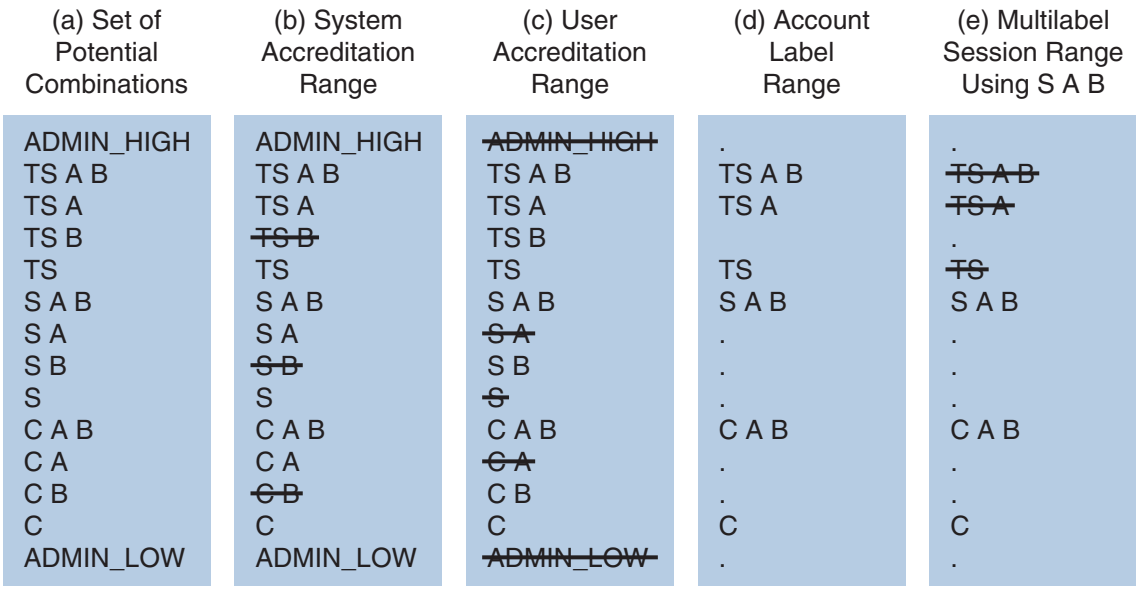
The (b) portion of Figure 1–7 shows the labels that are available if the user selects a single-label session with a session label of C A B. Note that C A B is below the minimum clearance. However, C A B is accessible because the user is selecting a session label, not a clearance. Because the session is single-label, the user can work at only one label. In this example, the user specified C A B, although S A B or C could have been chosen instead.

FIGURE 1–7 Comparison of Session Ranges



The following figure summarizes the progressive eliminations of available labels in this example. The eliminated labels are shown with a line through them in the range where they are filtered out. The filtered out labels are not shown in subsequent ranges.

FIGURE 1–8 Cumulative Effect of Constraints on a Session Range



Label Availability in Trusted Extensions Sessions

The following table shows session label limitations and availability based on users' session choices. The table continues the example from Figure 1–8.

TABLE 1–2 Labels in Trusted Extensions Sessions

	Multilevel Session		Single-level Session	
	General Case	**Example #1**	**General Case**	**Example #2**
		Multilevel with clearance of SECRET A B		**Single-level with session label of** SECRET A B
Initial Workspace Label (at first login)	Lowest label in account label range.	CONFIDENTIAL	Session label is specified by user	SECRET A B
Available Workspace Labels	Any label in account label range up to the session clearance	CONFIDENTIAL CONFIDENTIAL A B SECRET A B	Session label is specified by user	SECRET A B

- The left column identifies the types of label settings that are used in sessions.
- The middle two columns apply to a `Multilevel Session`.
- The right two columns apply to a `Single-level Session`.

- The columns that are labeled `General Case` describe how the label types are determined.
- The columns marked `Example` show a typical user's session selections at login.

In Example #1, the initial workspace label is set to `CONFIDENTIAL`, which is the label at the bottom of the user's account label range. The user can work at a label of `CONFIDENTIAL`, `CONFIDENTIAL A B`, or `SECRET A B`.

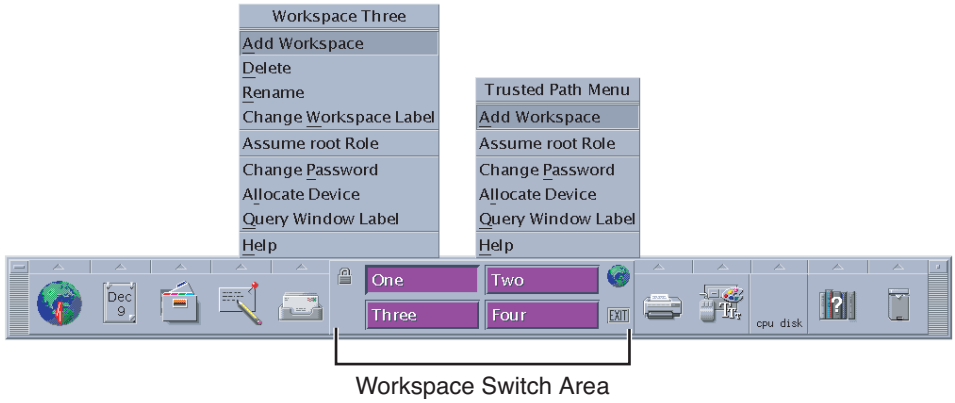
In Example #2, the user's initial workspace label is `SECRET A B`. Since the session is single-level, the only available workspace label is `SECRET A B`.

Labeled Workspaces

Labeled *workspaces* enable users to work at multiple labels during a single session.

If the user selects a range of labels for the session, the first workspace that comes up is at the user's *minimum label*. In CDE, buttons for three additional workspaces are created at the same minimum label in the workspace switch portion of the Front Panel.

FIGURE 1–9 Workspace Switch Area



For details on working in a labeled system, see *Oracle Solaris Trusted Extensions User's Guide*.

Administering Labels

Several aspects about how labels appear to users can be configured. Label visibility, label color, and labels on printed output can be configured. Some actions on labels require authorization or privilege. Upgrading or downgrading an object's label requires an authorization. Manipulating a label between its internal and its textual representation can require a privilege.

Label Visibility

As described in "Labeled Workspaces" on page 29, labels appear on windows on the desktop. On a single-label system, you might not want labels to be visible. Label visibility is configurable in the `policy.conf` file for a system for individual users. For a pointer to the configuration procedures, see "Managing Label Encodings (Task Map)" on page 50.

Typically, the content of files at a lower label can be read by a user at a higher label. For example, system files and commonly-available executables are assigned an `ADMIN_LOW` label. According to the read down-read equal rule, accounts who work at any label can read `ADMIN_LOW` files. As in the Solaris OS, DAC permissions can prevent read access. Zones also protect files from being read. If a lower-level zone is not mounted, a user in a higher-level zone cannot access the files for reading.

Files that contain data that should not be viewed by ordinary users, such as system log files and the `label_encodings` files, are maintained at `ADMIN_HIGH`. To allow administrators access to protected system files, the `ADMIN_LOW` and `ADMIN_HIGH` administrative labels are assigned as the minimum label and clearance for roles.

Labels on Printed Output

The labels that are printed on banner, trailer and body pages of print jobs can be customized. Also, accompanying text that appears on the banner and trailer pages can be customized. For more information, see Chapter 4, "Labeling Printer Output (Tasks)."

Authorizations for Relabeling Information

The authorization to upgrade information to a label that dominates the label of the current information is called the `Upgrade File Label` authorization. The authorization to downgrade information to a label that is lower than the the label of the current information is called the `Downgrade File Label` authorization. For definitions for these authorizations, see `/etc/security/auth_attr`.

Privileges for Translating Labels

Label translation occurs whenever programs manipulate labels. Labels are translated to and from the textual strings to the internal representation. For example, when a program such as `getlabel` gets the label of a file, before the label can display to the user, the internal representation of the label is translated into readable output. When the `setlabel` program sets a label specified on the command line, the textual string, that is, the label's name, is translated into the label's internal representation. Trusted Extensions permits label translations only if the calling process's label dominates the label that is to be translated. If a process attempts to translate a label that the process's label does not dominate, the translation is disallowed. The `sys_trans_label` privilege is required to override this restriction.

◆ ◆ ◆ CHAPTER 2

Planning Labels (Tasks)

This chapter covers the following topics:

For a greater level of detail and for further reference, see the *Compartmented Mode Workstation Labeling: Encodings Format*: Defense Intelligence Agency document [DDS-2600-6216-93]. This DIA reference is included in the Trusted Extensions document set. When using the DIA reference, keep in mind that information labels and their components are not used in Trusted Extensions.

Planning Labels (Task Map)

Planning labels requires a general knowledge of site security, and specific knowledge of the syntax of the `label_encodings` file. The security administrator is responsible for planning labels.

The following task map describes the planning tasks and points to more information.

Task	Description	For Instructions
Study and outline your label encodings file	Make a label encodings file that enforces your site security policy.	"How to Strategize for Labels" on page 34
Build an extensible `label_encodings` file	Create a file that can be modified without affecting existing label definitions.	"How to Plan the Encodings File" on page 34

How to Strategize for Labels

1 **Allow time to build a correct `label_encodings` file.**

Building the encodings for a site and making the encodings correct can be a time-consuming process. A system cannot be configured until the correct `label_encodings` file is installed.

2 **Know your site's security policy.**

Many sites already have a security policy that was developed according to government methods. Commercial businesses, even businesses that do not have much experience in planning labeled security, can start by examining their goals for information protection. These goals can be used to make some common-sense decisions about how to use labels. If the company has developed legal requirements for labeling printed information and email, those guidelines are a good place to start.

- For an example, see Chapter 6, "Example: Planning an Organization's Labels."
- For more about setting up your site's security policy, see Appendix A, "Site Security Policy," in *Oracle Solaris Trusted Extensions Configuration Guide*.

3 **Study the U. S. government label encodings file.**

The government's description of the file is in the *Compartmented Mode Workstation Labeling: Encodings Format:* Defense Intelligence Agency document [DDS-2600-6216-93].

4 **Customize the `LOCAL DEFINITIONS` section for your site.**

For suggestions and examples, see Chapter 5, "Customizing `LOCAL DEFINITIONS`."

5 **Finalize your encodings before installing Trusted Extensions.**

Changing the `label_encodings` file on a running system is risky. For more information, see the `label_encodings(4)` man page.

How to Plan the Encodings File

The following practices help create a correct `label_encodings` file that can be safely extended later.

Note – For `CLASSIFICATIONS` and `COMPARTMENTS`, the security administrator role can later change the textual representation. However, the integer and bit values cannot be changed without potentially serious complications.

---

1 **Create a `label_encodings` file.**

For ideas, see "Sources for Encodings Files" on page 38. For the procedure, see "Managing Label Encodings (Task Map)" on page 50.

2 **Leave room to add items.**

a. **Leave gaps when you number classifications.**

For example, you could number classifications in increments of 10. The increments allow intermediate classifications to be added later.

b. **Leave gaps in compartment bits.**

Space compartment bit numbers for possible later additions.

c. **Reserve some initial compartment bits for later definition.**

If your site uses inverse compartments, see "Default and Inverse Words" on page 47. To learn more about inverse compartments, see the DIA reference, *Compartmented Mode Workstation Labeling: Encodings Format*.

3 **Determine classifications for the site.**

As described in Figure 1–2, the total number of classification values that you can use is 254. Do not use classification 0.

The system treats a classification value of 10 as more security-sensitive than a classification value of 2. The textual representations are not used to determine security levels.

The same classification value cannot be assigned to different names. Each classification must be higher or lower, or disjoint, from any other classification. No two labels can evaluate to the same level.

A table can be used to plan classifications. For a completed example, see Table 6–2.

4 **Decide on compartments.**

Decide how data and programs are grouped. Decide whether any data or programs can be intermixed. For example, perhaps purchase order data should not be seen by programs that manage personnel files. Perhaps purchase order data should be accessible to programs that deal with shipment tracking problems.

At this point, do not consider users. Think in terms of *what*, not *who*.

5 **Design the names.**

`CLASSIFICATIONS` and `WORDS` in the `label_encodings` file have two forms: a mandatory long name and an optional short name. Short names can be entered interchangeably with long names when labels are being specified.

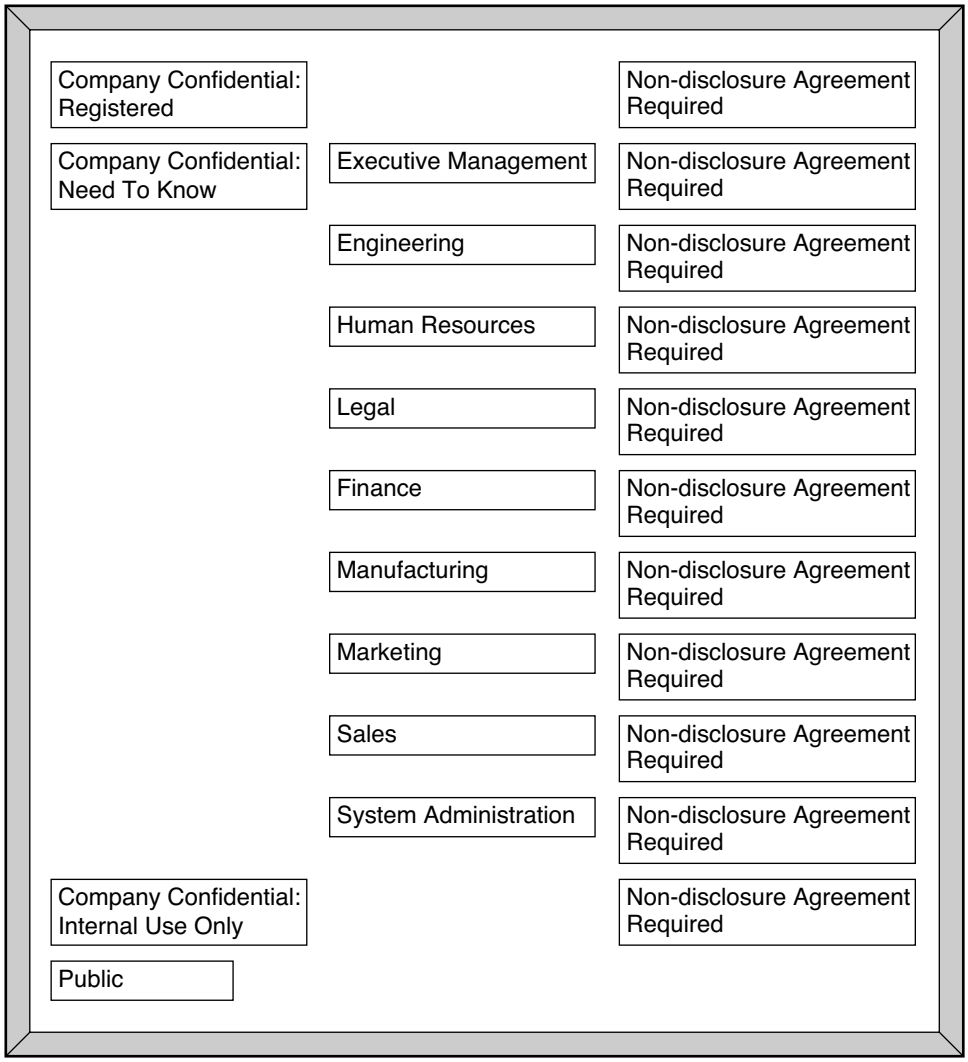
6 **Arrange the relationships.**

Compartments are not intrinsically hierarchical. However, compartments can be configured to have hierarchical relationships. Before setting up relationships, study the example section of *Compartmented Mode Workstation Labeling: Encodings Format*.

One way to make this step easier is to use a large board and pieces of paper that are marked with your classifications and compartments. For an example, see Figure 2–1. With this method, you can visualize the relationships and rearrange the pieces until they all fit together.

Note – Unless you are creating a set of encodings that must be compatible with another organization's labels, you can assign any valid number as a compartment bit. Keep track of the numbers that you use and their relations to each other.

FIGURE 2–1 Sample Planning Board for Label Relationships



7 Decide which clearances to assign to which users.

You can use a table to plan clearances. For a completed example, see Table 6–5.

When you assign a clearance to a user, the classification must dominate all classifications at which the user can work. The clearance can be equal to the user's highest work classification. The compartments in the clearance must include all compartments that the user might need.

8 Arrange the labels in order of increasing sensitivity.

9 **Associate the definitions for each word with an internal format of integers, bit patterns, and logical relationship statements.**

A table can be used to keep track of compartment bit assignments. For a completed example, see Table 6–4.

10 **Copy the `WORDS` section under `SENSITIVITY LABELS` to the `INFORMATION LABELS` section.**

Although Trusted Extensions does not support information labels, the `INFORMATION LABELS: WORDS:` section must be identical to the `SENSITIVITY LABELS: WORDS:` section to be a valid encodings file.

11 **Decide which colors should be associated with which labels.**

For suggestions and examples, see "Specifying Colors for Labels" on page 75.

12 **Analyze the label relationships.**

On a system that is configured with Trusted Extensions, use the `chk_encodings -a` command to write a detailed report on the label relationships in your file.

```
# chk_encodings -a encodings-file
```

Sources for Encodings Files

The `label_encodings` file is a flat text file. On a system that is configured with Trusted Extensions, the label of the file is `ADMIN_HIGH` to prevent ordinary users from reading it. The maximum line length in the `label_encodings` file is 256 bytes. The file can be edited with any text editor. The security administrator is responsible for the creation and distribution of the `label_encodings` file.

Note – The `label_encodings` file can be created or edited on any system. However, the file must be checked and tested on a host that is configured with Trusted Extensions.

Some organizations have a government-furnished `label_encodings` file that is based on Defense Intelligence Agency (DIA) specifications. Other organizations might want to base their encodings file on one of the files that are provided with the Trusted Extensions packages.

Labels Files in Solaris Trusted Extensions Packages

Trusted Extensions installs sample files in the `/etc/security/tsol` directory. These samples can be modified to your site requirements.

`label_encodings.simple` file	Is installed by Solaris Trusted Extensions software.

`label_encodings.example` file	Is similar to the example in Appendix A, "Sample Label Encodings File." The introduction to the appendix describes the label components in the file. Chapter 6, "Example: Planning an Organization's Labels," describes each step in creating this file.
`label_encodings.gfi.single` file	Is the U.S. Government single-level file.
`label_encodings.single` file	Is Sun's version of the U.S. Government single-level file. The color assignments are different.
`label_encodings.gfi.multi` file	Is the U.S. Government multilevel file.
`label_encodings.multi` file	Is Sun's version of the U.S. Government multilevel file. The combinations are less restricted, the minimum clearance is higher, the default user label is lower, and the colors are different.

Alternatively, you can build a `label_encodings` file from scratch. The syntax and structure of the `label_encodings` file is provided in "Encodings File Syntax" on page 43.

Default Label Encodings File

By default, the `label_encodings.simple` file is installed as `/etc/security/tsol/label_encodings`:

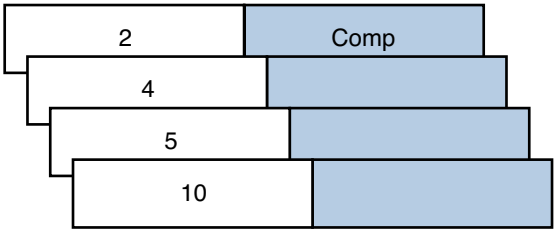
```
ACCREDITATION RANGE:  classification= public;
only valid compartment combinations:  public
minimum clearance= needtoknow;
minimum sensitivity label= public;
minimum protect as classification= public;
```

The `ACCREDITATION RANGE` definition restricts the user to the following label:

- `PUBLIC` is defined as the only classification
- `PUBLIC` is defined as the only valid compartment combination
- `NEEDTOKNOW` is defined as the minimum clearance
- `PUBLIC` is defined as the minimum sensitivity label
- `PUBLIC` is defined as the minimum protect as classification

The Classifications section is illustrated in the following figure.

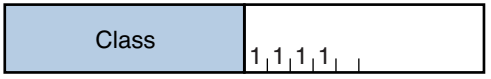
FIGURE 2–2 Classifications in Default `label_encodings` File




```
CLASSIFICATIONS:
PUBLIC         value = 2
CONFIDENTIAL   value = 4
SANDBOX        value = 5
MAX LABEL      value = 10
```

The compartments in the file are illustrated in the following figure.

FIGURE 2–3 Compartments in Default `label_encodings` File




```
SENSITIVITY LABELS:
WORDS:
INTERNAL USE ONLY   compartments = 1 ~2
NEED TO KNOW        compartments = 1-2 ~3
RESTRICTED          compartments = 1-3
PLAYGROUND          compartments = 0 ~1 ~2 ~3
```

Differences Between GFI Label Encodings Files

There are two government-furnished files, `label_encodings.single` and `label_encodings.multi`. The `label_encodings.single` file is single-level, and the `label_encodings.multi` is a multilevel version of the single-level file. The files also differ in the settings in the `ACCREDITATION RANGE` section. The `ACCREDITATION RANGE` section describes which classifications and compartments are available to ordinary users.

GFI Multilevel Label Encodings File

The `ACCREDITATION RANGE` settings in the `label_encodings.multi` file are shown in the following excerpt:

```
ACCREDITATION RANGE:
classification= u;   all compartment combinations valid;
classification= c;   all compartment combinations valid;
classification= s;   all compartment combinations valid;
classification= ts;   all compartment combinations valid;

minimum clearance= c;
minimum sensitivity label= u;
minimum protect as classification= u;
```

The ACCREDITATION RANGE definitions enable the site to use all the classifications and compartment words that are defined in the `label_encodings.multi` file:

- UNCLASSIFIED, CLASSIFIED, SECRET, and TOP SECRET are defined with all compartment combinations valid
- CLASSIFIED is defined as the `minimum clearance`
- UNCLASSIFIED is defined as the `minimum sensitivity label`
- UNCLASSIFIED is defined as the `minimum protect as classification`

GFI Single Level Label Encodings File

The ACCREDITATION RANGE settings in the `label_encodings.single` file are shown in the following excerpt:

```
ACCREDITATION RANGE:  classification= s;
only valid compartment combinations:  s a b rel cntry1
minimum clearance= s Able Baker NATIONALITY: CNTRY1;
minimum sensitivity label= s A B REL CNTRY1;
minimum protect as classification= s;
```

The ACCREDITATION RANGE definition restricts the user to the following label:

- SECRET is defined as the only classification
- SECRET A B REL CNTRY1 is defined as the only valid compartment combination
- SECRET ABLE BAKER NATIONALITY: CNTRY1 is defined as the minimum clearance
- SECRET A B REL CNTRY1 is defined as the minimum sensitivity label
- SECRET is defined as the minimum protect as classification

Sun Extensions to `label_encodings` File

Sun's implementation of the `label_encodings` file supports a LOCAL DEFINITIONS section. This section is optional. The section can be appended to an already-existing `label_encodings` file. The word LOCAL in the keyword that starts the section means *local to Sun's implementation*.

Options in the LOCAL DEFINITIONS section set label translation options and associate colors with labels. The title bars of application windows display each label against a background of the color that is specified for that label. If an invalid color or no color is specified in the COLOR NAMES option, a default color is supplied. Chapter 5, "Customizing LOCAL DEFINITIONS," describes how to modify the Sun extensions for your site.

◆ ◆ ◆ CHAPTER 3

Making a Label Encodings File (Tasks)

This chapter describes creating and modifying a `label_encodings` file.

Encodings File Syntax

The `label_encodings` file contains a `VERSION` specification and seven mandatory sections: `CLASSIFICATIONS`, `INFORMATION LABELS`, `SENSITIVITY LABELS`, `CLEARANCES`, `CHANNELS`, `PRINTER BANNERS`, and `ACCREDITATION RANGE`. The sections must appear in the order given. An optional `LOCAL DEFINITIONS` section can follow.

In the following table, *Mandatory keyword* means only that the keyword must be present. Not all keywords must have definitions. The notes for each section indicate what must be defined and what is optional.

TABLE 3–1 Label Encodings Keywords

Section	Notes
`VERSION=`	Mandatory keyword. The version specification is the single keyword `VERSION=`, followed by a character string that identifies this particular version of encodings.
`CLASSIFICATIONS:`	Mandatory keyword. At least one classification must be defined

`INFORMATION LABELS:`
`WORDS:`
`REQUIRED COMBINATIONS:`
`COMBINATION CONSTRAINTS:`
	Mandatory keywords. Even though information labels are not used in Trusted Extensions software, you must assign one bit to an information label word for each bit that you assign to a sensitivity label word. The sensitivity label words are defined in the following section.

TABLE 3–1 Label Encodings Keywords *(Continued)*

Section	Notes
SENSITIVITY LABELS: WORDS: REQUIRED COMBINATIONS: COMBINATION CONSTRAINTS	Mandatory keywords. WORDS definitions are optional. If you define sensitivity label words, the same bits must be assigned to WORDS in both the INFORMATION LABELS and CLEARANCES sections. The words that are assigned to the bits do not need to be the same.
CLEARANCES: WORDS: REQUIRED COMBINATIONS: COMBINATION CONSTRAINTS	Mandatory keywords. One bit must be assigned to a clearance word for any sensitivity label word that you have defined. Clearance labels can allow combinations of words that have been disallowed in the definitions for sensitivity label words.
CHANNELS:	Mandatory keyword.
PRINTER BANNERS:	Mandatory keyword.
ACCREDITATION RANGE:	Mandatory keyword. A rule must be defined for each classification name. The minimum clearance, minimum sensitivity label, and minimum protect as classification must be defined.
LOCAL DEFINITIONS:	Optional keyword.

For all the required sections, the keywords in the preceding table must be present, but not all of the sections must have definitions. For example, a `label_encodings` file with only `CLASSIFICATIONS` and `ACCREDITATION RANGE` definitions is valid.

Word Order Requirements

The order in which words are configured for sensitivity labels and clearances is not enforced. However, the order is important when setting up relationships between words. By convention, the `WORDS` in the `SENSITIVITY LABELS` section are arranged in increasing order of importance.

For the effect of word order, see "Specifying Channels" on page 65 of Chapter 4, "Labeling Printer Output (Tasks)." Detailed information is provided in *Compartmented Mode Workstation Labeling: Encodings Format*.

If a compartment word is defined for one type of label (by assigning the compartment word to one or more bits) in the `label_encodings` file, then the same bits must be assigned to a word in the definition of the other types of labels. While all types of labels use the same classification names, the words that are used for each type of label can be different. The words can be different even when they are encoded with the same bits and literally refer to the same thing. Clearance labels can allow combinations of words that have been disallowed in the definitions for sensitivity labels words.

Classification Name Syntax

The classification is the hierarchical portion of a label. Each label has one and only one classification. A site can define up to 255 classifications. An integer value from 1 to 255 can be assigned to a classification in the `label_encodings` file. The value 0 is reserved for the `ADMIN_LOW` administrative label. The value 32,767 is reserved for the `ADMIN_HIGH` administrative label. For an illustration, see Figure 1–2.

Classifications are defined once for clearances and for sensitivity labels in the `CLASSIFICATIONS` section of the `label_encodings` file.

A classification with a higher value dominates a classification with a lower value. The following table shows two sets of label names that are assigned the same values in different encodings files. The left column shows sample sensitivity labels from the `label_encodings.example` file. The middle column shows labels from the `label_encodings.gfi.multi` file. A label with the `Registered` or `Top Secret` classification, with a value of 6, dominates the labels that are listed in its column.

Commercial Example	U.S. Government Example	Value
`Registered`	`Top Secret`	6
`Need to Know`	`Secret`	5
`Internal Use Only`	`Confidential`	4
`Public`	`Unclassified`	1

Keywords for Classifications

The following list describes the keywords that can be defined for classifications. For examples of initial compartment definitions, see "Default and Inverse Words" on page 47.

`name=` Cannot contain (/) or (,) or (;). All other alphanumeric characters and white space are allowed. Users can enter either the `name` or the `sname` or the `aname` when specifying labels.

`sname=` Required in classifications only. The short name appears in sensitivity labels in brackets.

`aname=` Optional. Name that can be entered by users when a classification is needed.

`value=` The values that you assign should represent the actual hierarchy among the classifications. The values should leave room for later expansion. `0` is reserved for `ADMIN_LOW`. Values can start at `1` and go to 255.

`initial compartments=`	Optional. Specify bit numbers for any default compartment words. Default compartment words are words that should initially appear in any label that has the associated classification. Advanced: Specify bit numbers for any inverse words. The minimum classification should not have initial compartments.
`initial markings=`	Obsolete. Do not define.

The following example shows the top of the `label_encodings.multi` file.

EXAMPLE 3–1 Classifications With Initial Compartments in `label_encodings.multi`

```
VERSION= Trusted Solaris Multi-Label Sample Version - 5.6 05/07/27

*
*    WARNING:  If CIPSO Tag Type 1 network labels are to be used:
*
*        a) All CLASSIFICATIONS values must be less than or equal to 255.
*        b) All COMPARTMENTS bits must be less than or equal to 239.
*

CLASSIFICATIONS:

*
name= UNCLASSIFIED;  sname= U;  value= 1;
name= CONFIDENTIAL;  sname= C;  value= 4; initial compartments= 4-5 190-239;
name= SECRET;        sname= S;  value= 5; initial compartments= 4-5 190-239;
name= TOP SECRET;    sname= TS; value= 6; initial compartments= 4-5 190-239;
```

Each classification has the mandatory `name`, `sname`, and `value` fields. The `CONFIDENTIAL`, `SECRET`, and `TOP SECRET` classifications have `initial compartments`. The lowest classification, `UNCLASSIFIED`, has no initial compartments.

The initial compartment bit assignments of `4-5` and `190-239` signify that bits 4, 5, and 190 through 239 are turned on. These bits are set to `1` in a label with this classification.

Some of the initial compartments are later used to define *default* and *inverse* words. Some initial compartments are reserved for possible later definitions of inverse words.

The following example shows a set of classifications that have no initial compartments.

EXAMPLE 3–2 Classifications With No Initial Compartments in `label_encodings.example`

```
CLASSIFICATIONS:

name= PUBLIC; sname= PUBLIC; value= 1;
```

EXAMPLE 3–2 Classifications With No Initial Compartments in `label_encodings.example` *(Continued)*

```
name= INTERNAL_USE_ONLY; sname= INTERNAL; aname= INTERNAL; value= 4;
name= NEED_TO_KNOW; sname= NEED_TO_KNOW; aname= NEED_TO_KNOW; value= 5;
name= REGISTERED; sname= REGISTERED; aname= REGISTERED; value= 6;
```

Default and Inverse Words

When a bit is defined as an initial compartment, the bit is set to `1` in every label that contains the classification. Any bit that is specified for an initial compartment can be defined later in the `label_encodings` file as a *default word* or an *inverse word*.

- A *default compartment word* is a word that appears in any label that contains the classification.
- An *inverse compartment word* is a word that appears in a label that has the associated classification when another word that you define with the inverse compartment's bit is not present.

EXAMPLE 3–3 Assigning Initial Compartments

In this example, the `PUBLIC` classification is assigned no initial compartments, while the `WEB COMPANY` classification is assigned initial compartments 4 and 5. A label that includes the `PUBLIC` classification has no default compartments. A label that includes the `WEB COMPANY` classification always has compartment bits 4 and 5 turned on.

```
name= PUBLIC;  sname= P;  value= 1;
name= WEB COMPANY;  sname= WEBCO;  value= 4; initial compartments= 4-5
```

The following section shows how these initial compartment bits can be assigned to words.

EXAMPLE 3–4 Defining Default and Inverse `SENSITIVITY LABELS` Words

In this example, compartment bits 4 and 5 are assigned to the word `DIVISION ONLY`. Each compartment bit is also associated with an inverse word. `WEBC AMERICA` is assigned to the inverse compartment bit ~4. `WEBC WORLD` is assigned to the inverse compartment bit ~5. These assignments have the following results:

- A sensitivity label with the `WEB COMPANY` classification initially includes the word `DIVISION ONLY`. The label's binary representation has the compartment bits 4 and 5 turned on.
- A sensitivity label with the `PUBLIC` classification always has compartment bits 4 and 5 turned off. The words `WEBC AMERICA` and `WEBC WORLD` are included in the label.

  Because a `minclass` of `IUO` is specified for the inverse words, `WEBC AMERICA` and `WEBC WORLD` are not displayed in the `PUBLIC` sensitivity label. The presence of these two inverse words is understood.

EXAMPLE 3–4 Defining Default and Inverse SENSITIVITY LABELS Words *(Continued)*

```
SENSITIVITY LABELS:

WORDS:

name= DIVISION ONLY;  sname= DO;       minclass= WEB COMPANY; compartments= 4-5;
name= WEBC AMERICA;   sname= WEBCA;    minclass= WEB COMPANY; compartments= ~4;
name= WEBC WORLD;     sname= WEBCW;    minclass= WEB COMPANY; compartments= ~5;
```

Compartment Words

Compartments are optional words that can be defined to appear in labels. Compartments are called categories in some other trusted systems. Compartments are used to indicate the special handling procedures to be used for the information whose label contains the compartment and the general class of people who might have access to the information.

Compartment words are assigned to non-hierarchical bits. However, hierarchies can be established between compartment words. These hierarchies are based on rules for including bits from one compartment word in the bits that are defined for another compartment word.

Compartment words are optionally defined in the WORDS subsection for each label type. Each compartment word is assigned to one or more bits.

While all types of labels use the same classifications, the words that are used for each type of label can be different. The words can be different even when they are encoded with the same bits and literally refer to the same thing.

The following example shows the WEB COMPANY compartment word. The word is specified with a short name (sname) of WEBCO and compartment bits 40-50.

EXAMPLE 3–5 Sample Compartment Definition for a Sensitivity Label

```
WORDS:

name= WEB COMPANY; sname= WEBCO; compartments= 40-50;
```

Along with its classification field, each label has a 256-bit compartment field, of which 239 are available for CIPSO labels. Each bit is assignable in zero or more compartment words. Each word can have one or more compartment bits assigned. Out of the 239 available bits, many compartment words can be created. For an example, see the compartments planner in Table 6–3.

The classification, compartments, and combination requirements affect the accreditation range. The `ACCREDITATION RANGE` for each classification setting should be one of the following strings:

- `only valid compartment combinations;`
- `all compartment combinations valid;`
- `all compartment combinations valid except;`

Hierarchical Compartment Words

Hierarchical compartments can be used to differentiate between documents that are available to everyone in a larger group, and documents that are available to subgroups only.

EXAMPLE 3–6 Using Bit Combinations to Establish Hierarchies

By defining a word that uses one bit and a second word that uses that same bit along with a second bit, you define a hierarchical relationship between the two words. The compartment word that is more general must be defined below the word that is more specific. For example, by defining a word that uses bit number 1 and another word that uses bits number 1 and 2, you give the two words a hierarchical relationship.

In this example, a Sales compartment is defined with two subcompartments, Direct Sales, and Indirect Sales. A single classification that is named WebCo is previously defined.

```
name= Direct_Sales;   compartments= 1, 2
name= Indirect_Sales;   compartments= 1, 3
name= Sales;   compartments= 1
```

This definition allows the WebCo company to differentiate between documents that can be accessed by anyone in the entire sales force, documents that can be accessed only by members of the indirect sales force, and documents that can be accessed only by members of the direct sales force.

- The security administrator gives the WebCo Direct_Sales clearance to employees in the direct sales organization. The WebCo Indirect_Sales clearance is given to employees in the indirect sales organization.
- Documents created by anyone working at the WebCo Direct_Sales label get the same label, so the documents are only accessible to employees in the direct sales department.
- Anyone in the indirect or direct sales forces can work at the WebCo Sales label because the compartment word Sales is below both the Direct_Sales and Indirect_Sales words. Creating documents at the WebCo Sales label makes the documents available to everyone in the Sales department.

EXAMPLE 3–7 Using `REQUIRED COMBINATIONS` to Establish Hierarchies

If two words are specified together in the `REQUIRED COMBINATIONS` section, the second label is added to the label whenever the first word is used.

In this example, the definition of the Direct Sales, Indirect_Sales, and Sales serves essentially the same effect as the example in Example 3–6. The difference is that the Direct_Sales word will always have the Sales word with it

```
name= Direct_Sales;   compartments= 2
name= Indirect_Sales;   compartments= 3
name= Sales;   compartments= 1

REQUIRED COMBINATIONS:

Direct_Sales            Sales
Indirect_Sales          Sales
```

Managing Label Encodings (Task Map)

Caution – The safest time to modify a `label_encodings` file is when the first host is installed. Proceed with caution when modifying a file that is in use. For details, see the `label_encodings(4)` man page.

The following task map describes the tasks for modifying and installing a `label_encodings` file.

Task	For Instructions
Create or change the `label_encodings` file	"How to Create a `label_encodings` File" on page 51
Test the `label_encodings` file	"How to Analyze and Verify the `label_encodings` File" on page 52
Distribute the `label_encodings` file	"How to Distribute the `label_encodings` File" on page 52
Debug a `label_encodings` file	"How to Debug a `label_encodings` File" on page 58
Change a classification definition	"How to Add or Rename a Classification" on page 53
Create default or inverse words	"How to Specify Default and Inverse Words" on page 54
Customize a single-label file	"How to Create a Single-Label Encodings File" on page 55
Specify a label name	Example 3–9

Task	For Instructions
Add a `LOCAL DEFINITIONS` section	"How to Add Sun Extensions to an Encodings File" on page 57
Prevent all users of a particular system from seeing labels	"How to Modify policy.conf Defaults" in *Oracle Solaris Trusted Extensions Administrator's Procedures*

▼ How to Create a `label_encodings` File

For sample files, see the `/etc/security/tsol` directory on an installed system. The files are described in "Labels Files in Solaris Trusted Extensions Packages" on page 38.

Before You Begin You can create this file before you install Trusted Extensions on your first system. On that first system, you check the file. You can also create this file on the first system that you install with Trusted Extensions. This procedure must be completed before a second computer is configured with Trusted Extensions.

On a system that is configured with Trusted Extensions, you must be in the global zone in the Security Administrator role. On other systems, you can create and edit the file in any editor.

1. **Create a backup copy of the original file.**
2. **Open a new or existing version of the file.**
   - **On a system that is not configured with Trusted Extensions, use any editor to create the file.**
   - **On a system that is configured with Trusted Extensions, use the Edit Encodings action to create the file.**

     In CDE, the Trusted_Extensions folder in the Application Manager contains two actions for the encodings file.

     Edit Encodings — Edits and checks the syntax of the specified `label_encodings` file.

     Check Encodings — Checks the syntax of a specified `label_encodings` file.
3. **Modify the file.**

   For details, see "How to Plan the Encodings File" on page 34.
4. **Continue with "How to Analyze and Verify the `label_encodings` File" on page 52.**

▼ How to Analyze and Verify the `label_encodings` File

Before You Begin You must be in the global zone in the Security Administrator role.

1. **Check the syntax and relationships of the labels.**

   In a terminal, use the `chk_encodings -a` command to analyze and report on label relationships.

   ```
   $ chk_encodings -a encodings-file
   ```

2. **Verify the file.**

   The Check Encodings action runs the `chk_encodings` command on the specified file.

   - **If the file passes, install it.**

     ```
     Do you want to install this label_encodings file? yes
     ```

   - **If the file does not pass, see "How to Debug a `label_encodings` File" on page 58 for assistance.**

3. **Test the encodings file.**

   Where possible, test the file on a few systems before approving the file for all systems at your site.

4. **Create a master copy.**

   For copying instructions, see "How to Copy Files to Portable Media in Trusted Extensions" in *Oracle Solaris Trusted Extensions Configuration Guide*.

5. **Save a labeled copy of the file in a protected location.**

▼ How to Distribute the `label_encodings` File

1. **Create a master copy.**

   For copying instructions, see "How to Copy Files to Portable Media in Trusted Extensions" in *Oracle Solaris Trusted Extensions Configuration Guide*.

2. **Immediately after installing a system with Trusted Extensions, copy the master file onto the system.**

   For copying instructions, see "How to Copy Files From Portable Media in Trusted Extensions" in *Oracle Solaris Trusted Extensions Configuration Guide*.

▼ How to Add or Rename a Classification

Before You Begin You must be in the Security Administrator role in the global zone.

1 **Edit the `label_encodings` file.**

Use the Edit Encodings action. For details, see "How to Create a `label_encodings` File" on page 51.

2 **Specify a version number.**

In the `VERSION=` section put your site's name, a title for the file, a version number and the date.

```
VERSION= Sun Microsystems, Inc. Example Version - 5.10 04/05/28
```

Trusted Extensions uses SCCS keywords for the version number and the date. For details, see the `sccs(1)` man page.

```
VERSION= Sun Microsystems, Inc. Example Version - %I% %E%
```

3 **Specify the classification.**

In the `CLASSIFICATIONS` section, supply the long name, short name, and numeric value for the new classification.

```
name= NEW_CLASS; sname= N; value= 2;
```

4 **Include the new classification in the accreditation range.**

Add the new classification to the `ACCREDITATION RANGE` section.

The following example shows three new classifications added to the `ACCREDITATION RANGE` section. Each classification is specified with `all compartment combinations valid`.

```
ACCREDITATION RANGE:

classification= UNCLASSIFIED;        all compartment combinations valid;

* i is new in this file
classification= INTERNAL_USE_ONLY;   all compartment combinations valid;

* n is new in this file
classification= NEED_TO_KNOW;        all compartment combinations valid;

classification= CONFIDENTIAL;        all compartment combinations valid except:
c
c a
c b

classification= SECRET;               only valid compartment combinations:
. . .
```

```
* r is new in this file
classification= REGISTERED;          all compartment combinations valid;
```

5 **Adjust the `ACCREDITATION RANGE` section if necessary.**

You might need to make the new classification a minimum classification.

```
minimum clearance= u;
minimum sensitivity label= u;
minimum protect as classification= u;
```

Note – Make sure that you set a minimum clearance that is dominated by all the clearances that you plan to assign to users. Similarly, make sure that the minimum sensitivity label is dominated by all the minimum labels that you plan to assign to users.

6 **Save your changes.**

▼ How to Specify Default and Inverse Words

Before You Begin You must be in the Security Administrator role in the global zone.

1 **Edit the `label_encodings` file.**

Use the Edit Encodings action. For details, see "How to Create a `label_encodings` File" on page 51.

2 **Specify initial compartments.**

In the `CLASSIFICATIONS` section, specify compartments as part of the classification definition.

```
CLASSIFICATIONS:
name= PUBLIC;  sname= P;  value= 1;
name= WEB COMPANY;  sname= WEBCO;  value= 2; initial compartments= 4-5 ;
```

3 **Specify a default word.**

Assign an initial compartment bit to the word.

```
name= DIVISION ONLY;  sname= DO;  minclass=  IUO; compartments= 4-5;
name= WEBC AMERICA;  sname= WEBCA; minclass= IUO; compartments= 4;
name= WEBC WORLD;  sname= WEBCW; minclass= IUO; compartments= 5;
```

4 **Specify an inverse word.**

Inverse words are created by preceding an initial compartment with a tilde (~).

```
name= DIVISION ONLY;  sname= DO;  minclass=  IUO; compartments= 4-5;
name= WEBC AMERICA;  sname= WEBCA; minclass= IUO; compartments= ~4;
name= WEBC WORLD;  sname= WEBCW; minclass= IUO; compartments= ~5;
```

5 **Save your changes.**

Troubleshooting For any compartment bits that are not reserved for later assignment, you need to assign a word to the bit in the following sections:

- `SENSITIVITY LABELS: WORDS:`
- `INFORMATION LABELS: WORDS:`
- `COMPARTMENTS: WORDS:`

▼ How to Create a Single-Label Encodings File

Certain labels must always be present in a `label_encodings` file:

- One sensitivity label in the user accreditation range must be defined
- One clearance in the user accreditation range must be defined
- One information label in the user accreditation range must be defined

Before You Begin You must be in the Security Administrator role in the global zone.

1 **Edit an encodings file.**

Use the Edit Encodings action. For details, see "How to Create a `label_encodings` File" on page 51. Provide a name that is different from the installed `label_encodings` file.

2 **Create an encodings file with only one classification and only the desired compartments.**

For example, you could set up an encodings file with the `INTERNAL_USE_ONLY` classification, and specify no words.

```
VERSION= Single-Label Encodings

. . .
CLASSIFICATIONS:

name= INTERNAL_USE_ONLY;       sname= INTERNAL;  value= 5;

INFORMATION LABELS:

WORDS:

SENSITIVITY LABELS:

WORDS:

CLEARANCES:
```

```
WORDS:

CHANNELS:

WORDS:

PRINTER BANNERS:

WORDS:
```

3 **In the** ACCREDITATION RANGE **section, include only one classification and one valid compartment combination.**

The following example encodes the INTERNAL classification.

```
ACCREDITATION RANGE:

classification= INTERNAL;
only valid compartment combinations:

INTERNAL

minimum clearance= INTERNAL;
minimum sensitivity label= INTERNAL;
minimum protect as classification= INTERNAL;
```

4 **Encode the** LOCAL DEFINITIONS **section.**

For details, see Chapter 5, "Customizing LOCAL DEFINITIONS."

5 **Ensure that the file is syntactically correct.**

- **If the file does not pass** chk_encodings**, see "How to Debug a** label_encodings **File" on page 58**
- **Otherwise, continue with "How to Analyze and Verify the** label_encodings **File" on page 52.**

Example 3–8 Defining the Accreditation Range in a Single-Label Encodings File

The following example shows the settings in the ACCREDITATION RANGE: section. A single ANY_CLASS classification is defined. Compartments words A, B, and REL CNTRY 1 are specified for all types of labels.

```
ACCREDITATION RANGE:

classification= ANY_CLASS;      only valid compartment combinations:

ANY_CLASS A B REL CNTRY1
```

```
minimum clearance= ANY_CLASS A B REL CNTRY1;
minimum sensitivity label= ANY_CLASS A B REL CNTRY1;
minimum protect as classification= ANY_CLASS;
```

Example 3–9 Changing the Single Label Name

In this example, the `label_encodings.example` file is changed to handle a single-label company. The `name=` value is changed from `SECRET` to `INTERNAL_USE_ONLY`. The `sname=` value is changed from `s` to `INTERNAL`. Neither the `value=` nor the `initial compartments=` definition is changed.

```
CLASSIFICATIONS:
name= INTERNAL_USE_ONLY;  sname= INTERNAL;  value= 5; initial compartments= 4-5
190-239;
```

In the `ACCREDITATION RANGE` section, the short name of the classification is replaced. Also, the minimums are replaced with the new `sname`.

```
ACCREDITATION RANGE:

classification= INTERNAL;      only valid compartment combinations:

INTERNAL

minimum clearance= INTERNAL;
minimum sensitivity label= INTERNAL;
minimum protect as classification= INTERNAL;
```

▼ How to Add Sun Extensions to an Encodings File

Before You Begin You must be in the Security Administrator role in the global zone. You must have an encodings file that does not have a `LOCAL DEFINITIONS` section.

1. **Add the `LOCAL DEFINITIONS` section to your file.**

   Append the section from a Trusted Extensions-supplied `label_encodings` file. Trusted Extensions-supplied files are in the `/etc/security/tsol` directory.

2. **Customize the extensions for your site.**

   For details, see "Modifying Sun Extensions (Task Map)" on page 78.

▼ How to Debug a `label_encodings` File

Before You Begin You must be in the Security Administrator role in the global zone.

1. **Edit the `label_encodings` file.**

   Use the Edit Encodings action. For details, see "How to Create a `label_encodings` File" on page 51.

2. **Check the entries in the `INFORMATION LABELS: WORDS:` section.**

   The entries must exactly match the entries in the `SENSITIVITY LABELS: WORDS:` section.

   Tip – Encode the sensitivity label words, then copy the words to the `INFORMATION LABELS` section.

3. **Check that no label in the user accreditation range has a value of 0 with no compartment bits.**

   This step ensures that no label is indistinguishable from the label `ADMIN_HIGH`.

4. **Check that no label in the user accreditation range has a value of 255 with all compartment bits from 0 to 239.**

   This step ensures that no label is indistinguishable from the label `ADMIN_HIGH`.

5. **Check that no compartment has a value higher than 239.**

   This step ensures that all labels can be mapped to CIPSO labels.

6. **For labels that cannot be resolved, do the following:**

   a. **Reset any objects with the new labels to a low system label, `ADMIN_LOW`.**

   b. **Restore a known, usable `label_encodings` file from the backup.**

   c. **Use the `chk_encodings -a` command to analyze the label problems in the faulty file.**

◆ ◆ ◆ CHAPTER 4

Labeling Printer Output (Tasks)

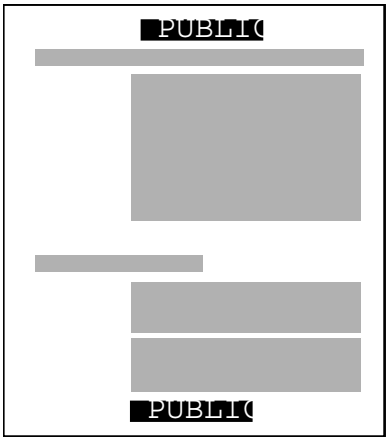
This chapter describes how labels and handling guidelines are printed on printer output. This chapter also describes how the Security Administrator role can make changes to the default. This chapter includes these topics:

Labels on Body Pages

By default, each print job's label is printed at the top and bottom of every body page.

Figure 4–1 shows the label `PUBLIC` printed at the top and bottom of a print job's body page.

FIGURE 4–1 Label Automatically Printed on Body Pages



The Security Administrator role can change the defaults so that a higher label is printed instead of the label of the print job. To print a higher label, see "Specifying Channels" on page 65. To hide labels completely, see "Reducing Printing Restrictions in Trusted Extensions (Task Map)" in *Oracle Solaris Trusted Extensions Administrator's Procedures*.

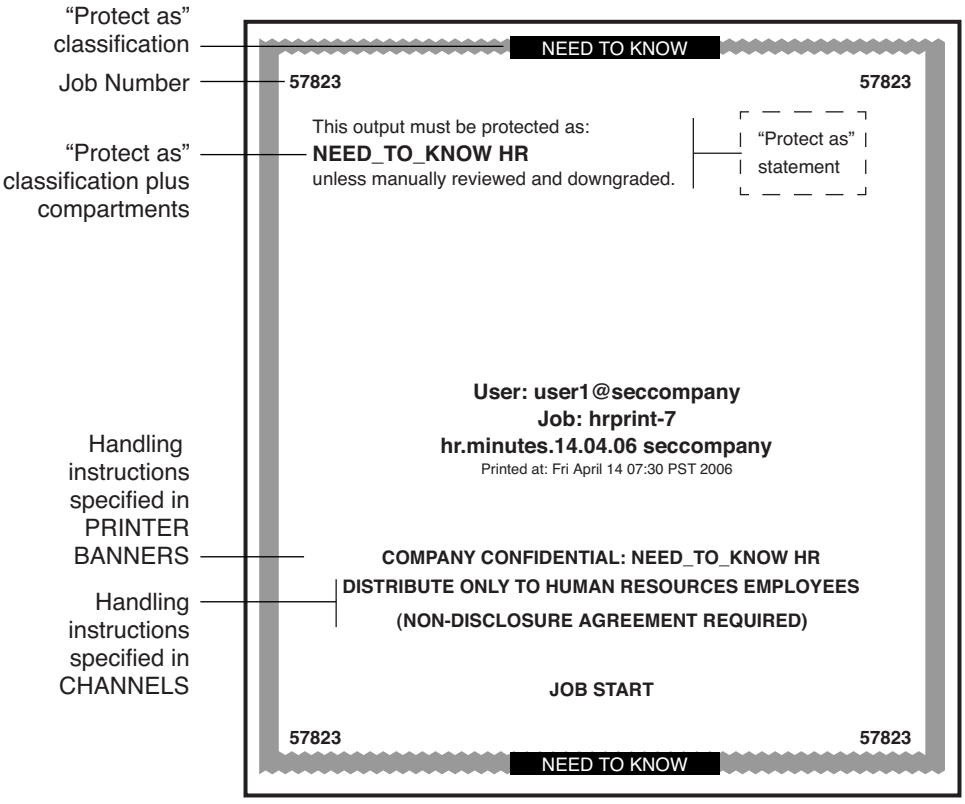
Security Text on Banner and Trailer Pages

By default, both a *banner* and a *trailer* page are automatically created for each print job. The banner and trailer pages contain label-related text and other guidelines for protecting printer output.

The fields and the text that are printed on the banner page are shown in Figure 4–2. The callouts show the names of the labels and the strings that appear by default.

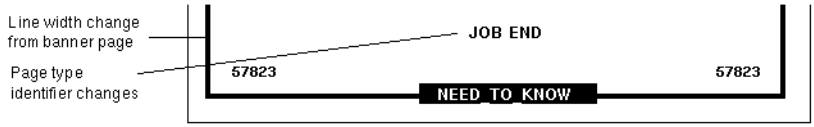
All the text and the labels and text on banner and trailer pages are configurable.

FIGURE 4–2 Typical Print Job Banner Page



The differences on the trailer page are shown in Figure 4–3. A thick black line is used as a frame on the trailer page, instead of the thicker gray frame on the banner page. The page type identifier on a trailer page is JOB END.

FIGURE 4–3 Differences on Trailer Pages



The parts of banner and trailer pages that the Security Administrator role can configure are described in the following sections:

- "Specifying the Protect As Classification" on page 62
- "Specifying Printer Banners" on page 63

- "Specifying Channels" on page 65

In addition, the Security Administrator role can make the following changes in a print configuration file that is called `tsol_separator.ps` in the `/usr/lib/lp/postscript` library:

- Localize (translate) the text on the banner and trailer pages
- Specify alternates to default labels printed at the top and bottom of body pages
- Change or omit any of the text or labels

To customize the configuration file, see the comments in the `tsol_separator.ps` file in the `/usr/lib/lp/postscript` directory. For further detail, see Chapter 15, "Managing Labeled Printing (Tasks)," in *Oracle Solaris Trusted Extensions Administrator's Procedures*.

Specifying the Protect As Classification

The `protect as` classification is printed in two places:

- On the top and bottom of banner and trailer pages
- In the middle of the *protect as statement*, together with compartments from the job's label

In the following figure, the `NEED_TO_KNOW` `protect as` classification is printed at the top of the banner page.

The `protect as statement` reads:

```
This output must be protected as:
```

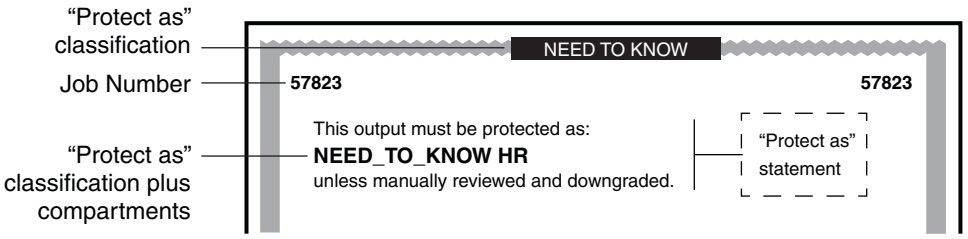
This statement is followed by the `protect as classification` along with compartments from the label:

```
NEED_TO_KNOW HR
```

This statement is followed by:

```
unless manually reviewed and downgraded.
```

FIGURE 4–4 Protect As Statement



For example, a site uses `INTERNAL_USE_ONLY` as the `minimum protect as` classification. The site has three classifications with the values that are shown in the first two columns of the following table. The third column shows the `protect as` classification. This classification is printed on the banner and trailer pages for the print job when the classification in the left column is in the job's label.

TABLE 4–1 Effect of Minimum Protect As Classification on Printer Output

Classification of Print Job	Value	Protect As Classification Printed on Banner and Trailer Pages
`NEED_TO_KNOW`	3	`NEED_TO_KNOW`
`INTERNAL_USE_ONLY`	2	`INTERNAL_USE_ONLY`
`PUBLIC`	1	`INTERNAL_USE_ONLY`

As the preceding table illustrates, any print job whose label includes either the `PUBLIC` or the `INTERNAL_USE_ONLY` classification would print `INTERNAL_USE_ONLY` in the `Protect as statement` and at the top and bottom of banner and trailer pages. Any print jobs whose label includes the `NEED_TO_KNOW` classification would print `NEED_TO_KNOW` in the same locations.

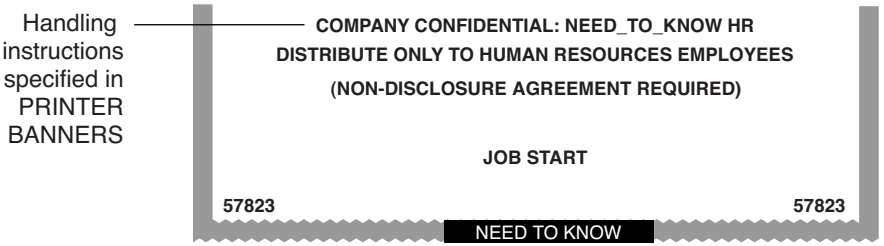
Specifying Printer Banners

The `PRINTER BANNERS` field occupies the first line or lines that can appear in the handling instructions in the lower third of the banner and trailer pages.

At commercial sites, the Security Administrator role can associate any text in the `PRINTER BANNERS` section with any compartment bit. The compartment bit must also be assigned to a word in the `SENSITIVITY LABELS` section of the `label_encodings` file. In the following example, the printer banner is the line that reads `COMPANY CONFIDENTIAL: NEED_TO_KNOW HR`.

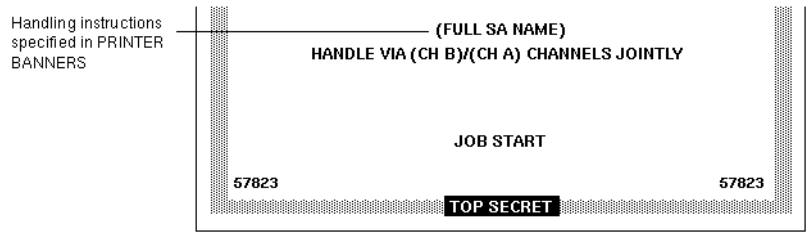
Compartments from the print job's label are printed in the `protect as` field along with the print job's `protect as` classification. In the following example, the compartment `HR` from the label is printed as an access-related word along with the `protect as` classification because all compartments are treated as access-related.

FIGURE 4–5 Commercial Use of PRINTER BANNERS on Banner Page



By convention in U.S. government installations, the printer banner line displays any warnings that are associated with the *subcompartments* of the job's sensitivity label. The following example shows a typical PRINTER BANNER at a government installation. Any string could be specified instead of the string that is shown here: (FULL SA NAME).

FIGURE 4–6 Government Use of PRINTER BANNERS on Banner Page



Following are the encodings for the printer banner line (FULL SA NAME) in Figure 4–6.

First, the word (FULL SA NAME) is associated in the PRINTER BANNERS section of the label_encodings with compartment bit 2.

EXAMPLE 4–1 Defining Words in the PRINTER BANNERS Section

```
PRINTER BANNERS:

WORDS:
. . .
name= (FULL SA NAME);                    compartments= 2;
```

Example 4–2 shows the SENSITIVITY LABELS definitions for the same compartments that are used in the PRINTER BANNER definitions in Figure 4–6. In the example, compartment bit 2 is associated with the subcompartment word SA.

The printer banner displays as (FULL SA NAME) because:

- The label contains the subcompartment word SA.
- Compartment bit 2 is associated with the subcompartment word SA.
- Compartment bit 2 is associated with the string (FULL SA NAME) in the PRINTER BANNERS encodings.

EXAMPLE 4–2 Sensitivity Labels WORDS Associated With PRINTER BANNERS Definitions

```
SENSITIVITY LABELS:

WORDS:
  .
  .
  .
name= SB;                       minclass= TS; compartments= 3-5;
name= SA;                       minclass= TS; compartments= 2;
```

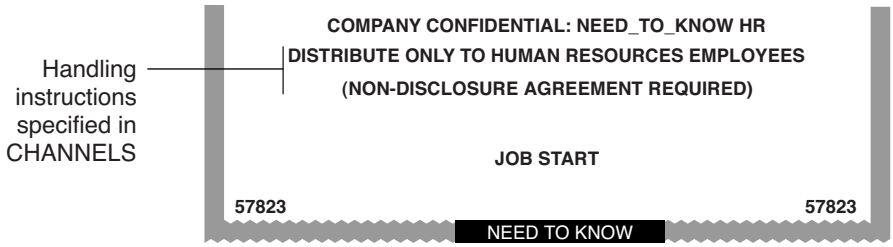
For a sample PRINTER BANNERS planner, see "Planning the Printer Banners in a Worksheet" on page 97.

Specifying Channels

The CHANNELS section in the label_encodings file defines the lines that can appear below the PRINTER BANNER lines on the lower third of the banner and trailer pages. The CHANNELS section can be specified to print a string whenever the label of a print job contains a certain compartment.

Commercial sites can customize the text in the CHANNELS section with any compartment bit. Figure 4–7 shows a CHANNELS warning on a print job's banner page at a commercial site.

FIGURE 4–7 Commercial Use of CHANNELS on Banner Page



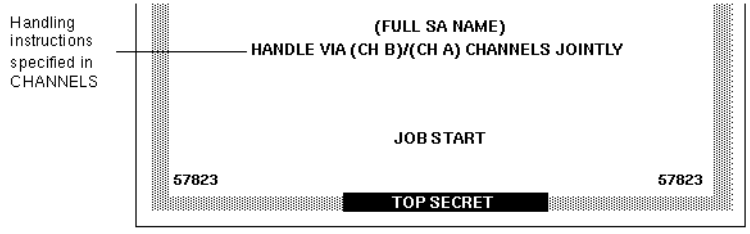
In U.S. government installations, the channels lines of the banner page conventionally show the warnings that are associated with the *compartments* of the job's label. Figure 4–8 shows a typical `CHANNELS` warning on a print job's banner page at a government installation: `HANDLE VIA (CH B)/(CH A) CHANNELS JOINTLY`.

The following discussion shows how the `CHANNELS` string `HANDLE VIA (CH B)/(CH A) CHANNELS JOINTLY` is specified for a job whose label includes the compartment words `A` and `B`. For the purpose of the example, only `(CH A)` and `(CH B)` apply. However, since the compartment bit for a third channel `(CH C)` is included in their definitions, `(CH C)` is also mentioned in this discussion.

The example illustrates these features:

- Two compartment bits are associated individually with one set of words and together with another set of words
- A third compartment bit is included with the encodings for the first two bits
- One suffix is defined for whenever *any combination of one or more* channel words is in the label
- Another suffix is defined for when a *single* channel word is in the label
- A third suffix is defined for when more than one channel word is in the print job's label

FIGURE 4–8 U.S. Government Use of `CHANNELS` Specification on Banner Page



As shown in the following example, two suffixes `CHANNELS JOINTLY` and `CHANNELS ONLY` and a prefix `HANDLE VIA` are defined.

EXAMPLE 4–3 Suffixes and Prefixes in the `CHANNELS` Section in a Government `label_encodings` File

```
CHANNELS:

WORDS:
name= CHANNELS JOINTLY;         suffix;
name= CHANNELS ONLY;            suffix;
name= HANDLE VIA;               prefix;
```

After the prefixes and suffixes are defined as in Example 4–3, the channel names `(CH A)`, `(CH B)`, and `(CH C)` are specified in two different ways to achieve the following results:

- Whenever any one of the three compartment bits associated with channels is in the label, the `HANDLE VIA:` prefix is printed.
- When only one of the three compartment bits associated with channels is in the label, the `CHANNELS ONLY` suffix is printed after the channel name `(CH A)`, `(CH B)`, or `(CH C)`.
- When more than one compartment bit that is associated with channels is in the label, the prefix is followed by the channel names separated by a slash (/). This channel name is then followed by the `CHANNELS JOINTLY` suffix.

  The first three lines that define `CHANNELS` words in Example 4–3 are repeated in Example 4–4. The second examples focuses on how `(CH A)`, `(CH B)`, and `(CH C)` are encoded to appear with the `CHANNELS ONLY` suffix:

- `(CH A)` is encoded with bit 0 on and bits 1 and 6 explicitly set to off using the tilde (~): 0 ~1 ~6
- `(CH B)` is encoded with bit 1 on and bits 0 and 6 explicitly set to off using the tilde (~): ~0 1 ~6
- `(CH C)` is encoded with bit 6 on and bits 0 and 1 explicitly set to off using the tilde (~): ~0 ~1 6

EXAMPLE 4–4 `CHANNELS ONLY` Suffix That Appears Alone with Individual Channels

```
CHANNELS:

WORDS:

name= CHANNELS JOINTLY;         suffix;
name= CHANNELS ONLY;            suffix;
name= HANDLE VIA;               prefix;
name= (CH A);   prefix= HANDLE VIA; suffix= CHANNELS ONLY;
compartments= 0 ~1 ~6;
name= (CH B);   prefix= HANDLE VIA; suffix= CHANNELS ONLY;
compartments= ~0 1 ~6;
name= (CH C);   prefix= HANDLE VIA; suffix= CHANNELS ONLY;
compartments= ~0 ~1 6;
```

The first three lines of channel name definitions in the CHANNELS section that is shown in Example 4–4 have the following results:

- The HANDLE VIA prefix and the CHANNELS ONLY suffix are printed when *one* of the words that is associated with bits 0, 1, and 6 elsewhere in the label_encodings is in the job's label
- The HANDLE VIA prefix and CHANNELS ONLY suffix are printed:
  - With (CH A) when compartment bit 0 is turned on in the label and compartment bits 1 and 6 are off
  - With (CH B) when compartment bit 1 is turned on in the label and compartment bits 0 and 6 are off
  - With (CH C) when compartment bit 6 is turned on in the label and compartment bits 0 and 1 are off

    The last three lines that define CHANNELS WORDS in Example 4–4 are repeated in Example 4–5. The repetition shows how (CH A), (CH B), and (CH C) are encoded to appear with the CHANNELS JOINTLY suffix when more than one of the words associated with bits 0, 1, and 6 is in the job's label. A slash is inserted between the channels names when more than one of the bits defined in the channels section is in the job's label.

EXAMPLE 4–5 Encodings for More Than One Channel in CHANNELS Section in Government Encodings File

```
name= (CH A);   prefix= HANDLE VIA; suffix= CHANNELS ONLY; compartments= 0 ~1 ~6;
name= (CH B);   prefix= HANDLE VIA; suffix= CHANNELS ONLY; compartments= ~0 1 ~6;
name= (CH C);   prefix= HANDLE VIA; suffix= CHANNELS ONLY; compartments= ~0 ~1 6;

name= (CH C);   prefix= HANDLE VIA; suffix= CHANNELS JOINTLY; compartments= 6;
name= (CH B);   prefix= HANDLE VIA; suffix= CHANNELS JOINTLY; compartments= 1;
name= (CH A);   prefix= HANDLE VIA; suffix= CHANNELS JOINTLY; compartments= 0;
```

The CHANNELS specification in Example 4–5 illustrates the importance of order when compartments are being encoded. The first three lines handle the cases when only one of the channels compartment bits is turned on, so the last three lines can handle cases when more than one bit is turned. Therefore, none of the last three lines need to have any compartment bits explicitly set to 0. The result of these last three lines is that the suffix CHANNELS JOINTLY is always printed when any of two or more of the three compartment words that are associated with the channels is in the label.

- (CH C) is printed with CHANNELS JOINTLY when bit 6 is turned on, and either of bit 0 or 1 or both are also turned on.
- (CH B) is printed with CHANNELS JOINTLY when bit 1 is turned on, and either of bit 0 or 6 or both are also turned on.
- (CH A) is printed with CHANNELS JOINTLY when compartment 0 is turned on, and either of bit 6 or 1 or both are also turned on.

The following example shows that compartment bit 6 is associated with the label word CC.

EXAMPLE 4–6 Label WORDS Associated With Compartment Bit 6

```
SENSITIVITY LABELS:


WORDS:
  .
  .
  .
name= CC;                       minclass= TS; compartments= 6;
```

Example 4–7 shows that compartment bit 1 is associated with the sensitivity label word B.

EXAMPLE 4–7 Label WORDS Associated With Compartment Bit 1

```
SENSITIVITY LABELS:

WORDS:
  .  .  .
name= B;                        minclass=  C; compartments= 1;
```

Example 4–8 shows that compartment bit 0 is associated with sensitivity label word A.

EXAMPLE 4–8 Label WORDS Associated With Compartment Bit 0

```
SENSITIVITY LABELS:

WORDS:
   .   .   .
name= A;                        minclass=  C; compartments= 0;
```

To sum up, the channels line prints as HANDLE VIA (CH B)/(CH A) CHANNELS JOINTLY because of the following specifications:

- HANDLE VIA is defined to always appear with any CHANNELS word
- The sensitivity label has two access-related words, A and B, that are associated with two compartment bits, 0 and 1.
- Because two of the bits that are defined for CHANNELS words appear in the job's label, the CHANNELS WORDS (CH A) and (CH B) are followed by CHANNELS JOINTLY.

  Any string that should print before the channel name is specified as a *prefix*. Any string that should print after the channel name is specified as a *suffix*.

For a sample CHANNELS planner, see "Planning the Channels in a Worksheet" on page 98.

Configuring Security Text on Print Jobs (Task Map)

The following task map describes how to format body pages and banner pages with labels.

Task	For Instructions
Print wording on the front page of a printout	"How to Specify the Words in PRINTER BANNERS" on page 70
Print handling instructions	"How to Specify Handling Instructions in CHANNELS" on page 71
Protect printouts at a higher label than the print job	"How to Set a Minimum Protect As Classification" on page 72
Configure printers to label output	"Configuring Labeled Printing (Task Map)" in *Oracle Solaris Trusted Extensions Administrator's Procedures*

▼ How to Specify the Words in PRINTER BANNERS

Create the strings that appear at the top of the banner page, and at the start of the handling instructions on the bottom of the page.

Before You Begin You must be in the Security Administrator role in the global zone.

1. **Plan the printer banners.**

   For background information, see "Specifying Printer Banners" on page 63.

   For assistance, use "Planning the Printer Banners in a Worksheet" on page 97.

2. **Edit the `label_encodings` file.**

   Use the Edit Encodings action.

3. **Modify the PRINTER BANNERS section of the file.**

   a. **Create prefixes and suffixes.**

      These strings are associated with the WORDS in the printer banner lines of banner and trailer pages.

```
PRINTER BANNERS:

WORDS:

name= ORCON;                    prefix;
```

b. Enter the names of words to associate with any already-defined compartments in sensitivity labels.

You can associate compartments with particular prefixes and suffixes.

```
name= (FULL SB NAME);            compartments= 3;
name= (FULL SA NAME);            compartments= 2;
```

4 Continue with "How to Analyze and Verify the `label_encodings` File" on page 52.

▼ How to Specify Handling Instructions in CHANNELS

Create the strings that state handling instructions on printer banner pages.

Before You Begin You must be in the Security Administrator role in the global zone.

1 Plan the prefixes and suffixes.

For assistance, use "Planning the Channels in a Worksheet" on page 98.

2 Edit the `label_encodings` file.

Use the Edit Encodings action.

3 Modify the `CHANNELS` section of the file.

```
CHANNELS:

WORDS:
```

a. Enter the prefixes or suffixes.

The `WORDS` in the `CHANNELS` lines of banner and trailer pages become prefixes or suffixes.

```
CHANNELS:

WORDS:
name= CHANNELS JOINTLY;          suffix;
name= CHANNELS ONLY;             suffix;
name= HANDLE VIA;                prefix;
```

b. Enter the names of words to associate with already-defined compartments in sensitivity labels.

You can use the defined prefixes and suffixes.

```
name= (CH C);   prefix= HANDLE VIA; suffix= CHANNELS JOINTLY;
compartments= 6;
name= (CH B);   prefix= HANDLE VIA; suffix= CHANNELS JOINTLY;
compartments= 1;
```

```
name= (CH A);   prefix= HANDLE VIA; suffix= CHANNELS JOINTLY;
compartments= 0;
```

4 **Continue with "How to Analyze and Verify the `label_encodings` File" on page 52.**

How to Set a Minimum Protect As Classification

The `minimum protect as` classification protects all printer output at the specified minimum classification or above. Site security policy might require this setting if lower-level information must be protected at a higher label.

Before You Begin You must be in the Security Administrator role in the global zone.

1 **Set a minimum protect as classification.**

This classification is defined in the `ACCREDITATION RANGE` section of an encodings file.

2 **Continue with "How to Analyze and Verify the `label_encodings` File" on page 52.**

Example 4–9 Minimum Protect As Classification From a `label_encodings` File

This example shows a minimum protect as classification. This classification is defined in the `ACCREDITATION RANGE` section of the `label_encodings.simple` file. With this setting, files that are labeled `INTERNAL` print with `NEED_TO_KNOW` on the banner and trailer pages.

```
minimum protect as classification= NEED_TO_KNOW;
```

◆ ◆ ◆ CHAPTER 5

Customizing LOCAL DEFINITIONS

This chapter describes how to customize the LOCAL DEFINITIONS section of the label_encodings file. This chapter includes the following topics:

LOCAL DEFINITIONS Section

Trusted Extensions provides additional keywords that are not defined in the government-furnished *Compartmented Mode Workstation Labeling: Encodings Format*. The keyword extensions are in a LOCAL DEFINITIONS section.

```
*
* Local site definitions and locally configurable options.
*

LOCAL DEFINITIONS:

Classification Name= Classification;
Compartments Name= Sensitivity;

Default User Sensitivity Label= PUB;
Default User Clearance= CNF NEED TO KNOW;

COLOR NAMES:

     label= Admin_Low;           color= #bdbdbd;

     label= PUB;                 color= blue violet;
     label= SBX PLAYGROUND;      color= yellow;
     label= CNF;                 color= navy blue;
     label= CNF : INTERNAL USE ONLY;  color= blue;
```

```
        label= CNF : NEED TO KNOW;  color= #00bfff;
        label= CNF : RESTRICTED;    color= #87ceff;

        label= Admin_High;          color= #636363;

*

* End of local site definitions
*
```

Contents of LOCAL DEFINITIONS Section

The Security Administrator role can do the following in the LOCAL DEFINITIONS section:

- Specify a user clearance and user minimum label that is different from the definitions in the ACCREDITATION RANGE: section.

  For the procedure, see "How to Specify Default User Labels" on page 78.
- Specify the names for column headers in label builder dialog boxes. The column headers indicate classifications and compartments.

  For the procedure, see "How to Name Column Headers in Label Builders" on page 80.
- Specify which colors are assigned to labels.

  Color definitions are optional. However, assigning colors to labels is highly recommended.

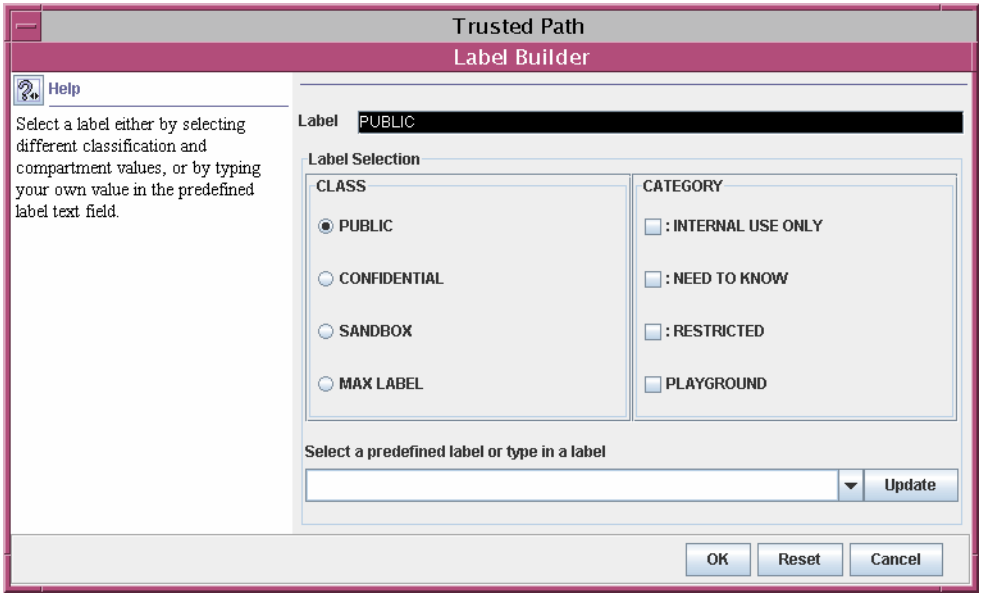
  For the procedure, see "How to Assign a Color to a Label or Word" on page 79.

For more details on the extensions to the label encodings keywords that Trusted Extensions provides, see the label_encodings(4) man page.

Changing Column Headers on Label Builders

The following figure shows the column headers Classification and Category in the label builder that is displayed by the Solaris Management Console.

FIGURE 5–1 Column Headers on Label Builder



To change the column headers, see "How to Name Column Headers in Label Builders" on page 80.

Specifying Colors for Labels

In the `LOCAL DEFINITIONS` section, the `COLOR NAMES` keyword is followed by zero or more color assignments. If no color is defined for a classification in the `COLOR NAMES` section of the `label_encodings` file, the color black is used. The default color values are shown in the following excerpt.

```
COLOR NAMES:

     label= Admin_Low;           color= #bdbdbd;

     label= PUB;                 color= blue violet;
     label= SBX PLAYGROUND;      color= yellow;
     label= CNF;                 color= navy blue;
     label= CNF : INTERNAL USE ONLY;  color= blue;
     label= CNF : NEED TO KNOW;  color= #00bfff;
     label= CNF : RESTRICTED;    color= #87ceff;

     label= Admin_High;          color= #636363;
```

Colors are assigned to labels and to words within labels with the following syntax:

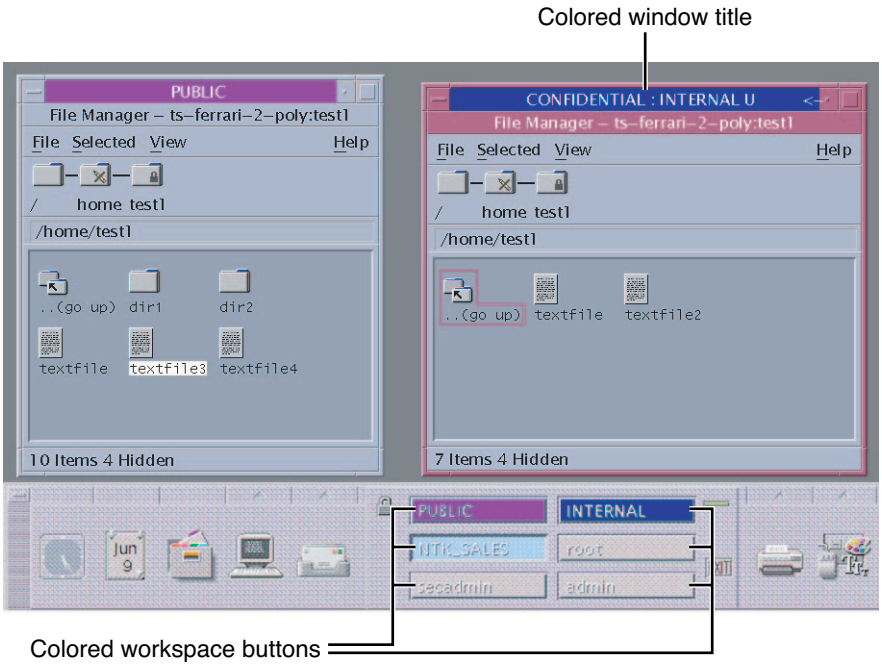
```
label= label-name;      color= color-name;
word= label-name;      color= color-name;
```

The value of *color-name* can be either a text color name or a hexadecimal color value. The color is associated with a word or a label. The color that is assigned to a label's component displays as a background color whenever a label includes the specified label components. The windows software computes a complementary color for the lettering.

For an introduction to color values, see "Color Values" on page 78. A full discussion of how to specify color is outside the scope of this guide. For more information, see the `X11`(5) man page in the `/usr/openwin/share/man` directory. For a fuller description, see "Color Specification" in the O'Reilly and Associates, Inc. *XWindows Systems User's Guide* (Vol. III), ISBN number 0-937175-29-3.

Color is assigned to a label's components according to the ordering rules that are described in the following section. For a desktop example of color use, see Figure 5–2. The `PUBLIC`, `INTERNAL`, and `NTK_SALES` workspace buttons are colored differently from each other and from standard workspace buttons.

FIGURE 5–2 Window Labels With Colors from `COLOR NAMES`



Order of Color Specification

The color that is used for any label is determined according to the following rules.

1. If a label contains a compartment word that has one or more colors specified, then the color value associated with the first `word=` value is used.
2. If a label contains none of the compartment words that are associated with colors, and an exact match exists for the label name, then the specified label color is used.
3. If there is no exact match for the label name, then the color that is associated with the first specified `label=` value for the *classification* of the label is used.
4. If the classification has no assigned color, then the color that is assigned to the first label that contains the same classification is used.

EXAMPLE 5–1 Colors Assigned According to Ordering Rules

In this example, a system has the following color definitions:

```
label= u;       color= green
label= c;       color= blue
label= S;       color= red;
word= B;        color= orange;
label= TS;      color= yellow;
label= TS SA;   color= khaki;
```

The rules result in the following color display:

- The label `TS A` displays with a yellow background, because yellow is the color assigned to the `TS` classification. Rule 3.
- Any label with the `C` classification displays with the color blue, unless the label also contains the word `B`. Rule 2.
- A label with the `C B` classification displays with the color orange, because word `B` is orange. Rule 1.
- Any label with the `U` classification always displays with the color green. In the encodings file, word `B` cannot appear with the classification `U`. Rule 2.

EXAMPLE 5–2 Color Assigned to a Label With No Assigned Color

This example illustrates rule 4. The label `TS` displays the color khaki, because `TS SA` is the only label that includes the `TS` classification. `TS SA` is defined to display the color khaki.

```
label= u;       color= green
label= c;       color= blue
label= S;       color= red;
word= B;        color= orange;
label= TS SA;   color= khaki;
```

Color Values

The `/usr/openwin/lib/rgb.txt` database translates color names into red, green, blue values. You can refer to the `rgb.txt` file for color names to use for your site's labels. You can also use hexadecimal color values.

Briefly, here are a few high-level points about color values:

- Color values specify the amount of red, green, and blue (RGB) that compose the color.
- RGB values can be specified with three hexadecimal numbers from 0 to FF. Each hexadecimal number indicates the amount of red, green, or blue in the color.

  For example, pure red is #FF0000, pure green is #00FF00, pure blue is #0000FF, pure white is #FFFFFF, and pure black is #000000. For more information, see the `X11`(5) man page in the `/usr/openwin/share/man` directory.
- The number of colors that are available on the screen depends on several factors:
  - Amount of memory available for specifying colors
  - Number of color planes
  - How many other clients are using color cells
  - Whether private color maps are being used by other applications

For a sample color name planner, see Table 6–8. To assign colors, see "How to Assign a Color to a Label or Word" on page 79.

Modifying Sun Extensions (Task Map)

The following task map describes how to modify the extensions in the `label_encodings` file.

Purpose	Instructions
Change label and clearance defaults for users	"How to Specify Default User Labels" on page 78
Specify colors for labels	"How to Assign a Color to a Label or Word" on page 79
Customize label builder headers	"How to Name Column Headers in Label Builders" on page 80

▼ How to Specify Default User Labels

Before You Begin You must be in the Security Administrator role in the global zone.

1 Edit the `label_encodings` file.

Use the Edit Encodings action. For details, see "How to Create a `label_encodings` File" on page 51.

2. **Find the line in the `LOCAL DEFINITIONS` section that begins with `Default User Sensitivity Label`.**

   ```
   Default User Sensitivity Label= u;
   Default User Clearance= c;
   ```

3. **Replace the sensitivity label with your desired minimum user label.**

   The following example shows a new minimum label of `c`.

   ```
   Default User Sensitivity Label= c;
   ```

4. **Replace the clearance with your desired user clearance.**

   The following example shows a new clearance of `s`.

   ```
   Default User Clearance= s;
   ```

How to Assign a Color to a Label or Word

To minimize color-flashing, use color names or hexadecimal color values that you know have been specified for other applications. The default color values have been chosen with memory limitations for color in mind.

Before You Begin You must be in the Security Administrator role in the global zone.

1. **Edit the `label_encodings` file.**

   Use the Edit Encodings action. For details, see "How to Create a `label_encodings` File" on page 51.

2. **Find the `COLOR NAMES` section.**

   ```
   COLOR NAMES:
            label= Admin_Low;       color= #bdbdbd;
            ...
            label= Admin_High;      color= #636363;
   ```

3. **Define a color for each classification.**

   In this example, the classification `REGISTERED` is assigned the color red. The `NEED_TO_KNOW SYSADM` classification is assigned the color blue.

   ```
   label= REGISTERED;  color= red;
   label= NEED TO KNOW; color= blue;
   ```

4 **(Optional) Define colors for individual compartment words.**

To distinguish certain compartment words irrespective of the classification with which they are associated, assign a separate color to those words.

a. **Determine the possible color names on your system.**

The names are defined in a local color database. For more information, see the `X11`(5) man page in the `/usr/openwin/share/man` directory.

```
% grep Red /usr/openwin/lib/X11/rgb.txt
...
255  69   0            OrangeRed
219 112 147            PaleVioletRed
...
139   0   0            DarkRed
```

b. **Assign the color names.**

```
word= EMGT; color= OrangeRed;
```

5 **(Optional) Define colors for labels.**

In this example, the color MediumPurple4 is assigned to a label.

```
label= NEED TO KNOW SYSADM; color= MediumPurple4;
```

▼ How to Name Column Headers in Label Builders

Before You Begin You must be in the Security Administrator role in the global zone.

1 **Edit the `label_encodings` file.**

Use the Edit Encodings action. For details, see "How to Create a `label_encodings` File" on page 51.

2 **Find the "Classification Name" line in the `LOCAL DEFINITIONS` section.**

This line and the following line define the column headers in the label builder.

```
Classification Name= Classification;
Compartments Name= Sensitivity;
```

3 **Assign different names to the column headers.**

The following example shows the column headers from `label_encodings.simple`.

```
Classification Name= Classification;
Compartments Name= Department;
```

◆ ◆ ◆ CHAPTER 6

Example: Planning an Organization's Labels

This chapter discusses the creation of a set of labels that meet a company's goals for information protection.

Identifying the Site's Label Requirements

SecCompany, Inc. is a fictional name for the company whose label requirements are modeled in this example. To protect the corporation's intellectual property, the company's legal department mandates that employees use three labels on all sensitive email and printed materials. The three labels, from most sensitive to least sensitive are the following:

- `SecCompany Confidential: Registered`
- `SecCompany Confidential: Need To Know`
- `SecCompany Confidential: Internal Use Only`

The legal department also approves the use of an optional fourth label, `Public`. The `Public` label is for information that can be distributed to anyone without restrictions.

Satisfying Information Protection Goals

At SecCompany, Inc, the manager in charge of Information Protection makes use of all possible channels to communicate labeling requirements. However, some employees do not understand the requirements. Other employees forget about requirements or ignore the requirements. Even when labels are properly applied, the information is not always properly handled, stored, and

distributed. For example, reports indicate that even Registered information is sometimes found unattended. Copies of Registered information have been left next to copy machines and printers, in break rooms, or in lobbies.

The legal department wants a better way to ensure that information is properly labeled without relying totally on employee compliance. The system administrators want a better way to control the following:

- Who can see or modify sensitive information
- Which information is printed on which printers
- How printer output is handled
- How email at various levels of security is distributed internally and externally

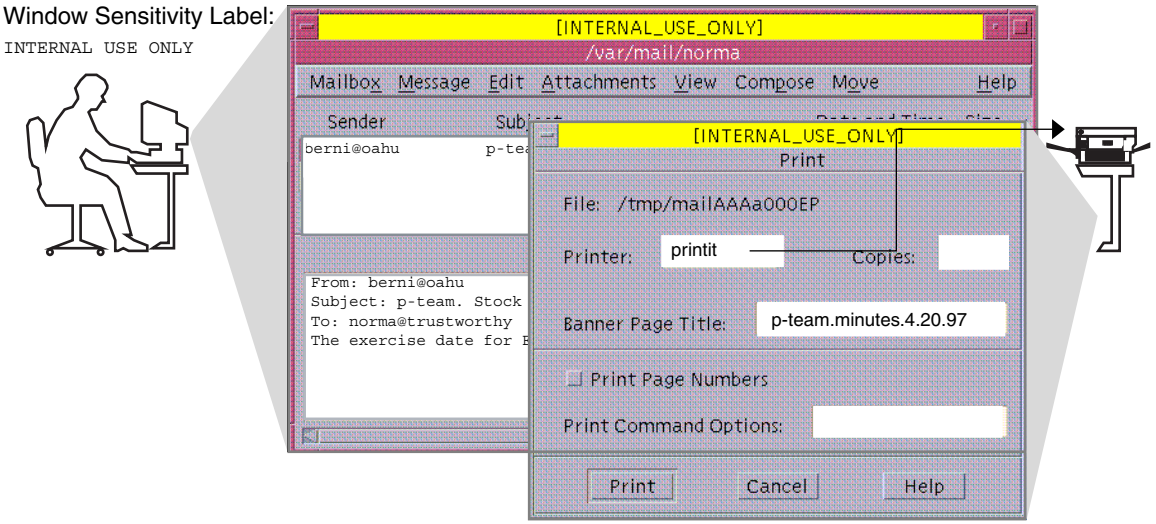
Trusted Extensions Features That Address Labeling and Access

Trusted Extensions software does not leave labeling up to the discretion of computer users. All printer output from print servers that are configured with Trusted Extensions is automatically labeled according to the site's requirements.

Even though security was not yet fully understood at the company, executives knew that Trusted Extensions could implement certain features immediately.

- Automatic labeling of print jobs
- Printers with restricted access by label
- Email with restricted access by label

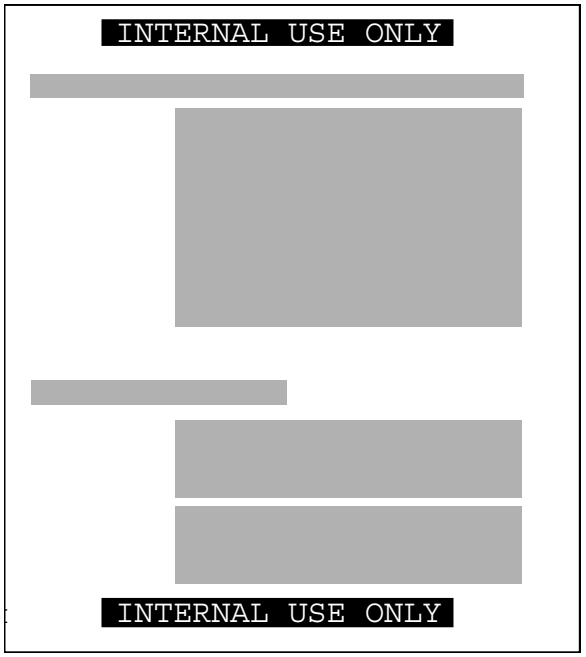
FIGURE 6–1 Automatic Labeling of Print Jobs



Each print job is automatically assigned a *label*. The label corresponds either to the *level* at which the user is working or to the user's level of responsibility.

Figure 6–1 shows an employee working at a level of `INTERNAL_USE_ONLY`. At this level, the work should only be accessible by SecCompany employees and others who have signed nondisclosure agreements. When the employee sends email to the printer, the print job is automatically assigned the label `INTERNAL_USE_ONLY`.

FIGURE 6–2 Label Automatically Printed on Body Pages



The printer automatically prints a company-specified label at the top and bottom of each page of printed output.

Figure 6–2 shows the letter that was sent to the printer in Figure 6–1 being printed with the user's working label. The label, `INTERNAL_USE_ONLY`, is printed at the top and bottom of every page.

EXAMPLE 6–1 Handling Guidelines on Banner and Trailer Pages

This example shows the wording for a print job whose sensitivity level has a classification of `NEED_TO_KNOW` and a department of `HUMAN_RESOURCES`. Banner and trailer pages are automatically created for each print job and are printed with company-specific handling guidelines.

```
NEED_TO_KNOW HR

DISTRIBUTE ONLY TO HUMAN RESOURCES (NON-DISCLOSURE AGREEMENT REQUIRED)
```

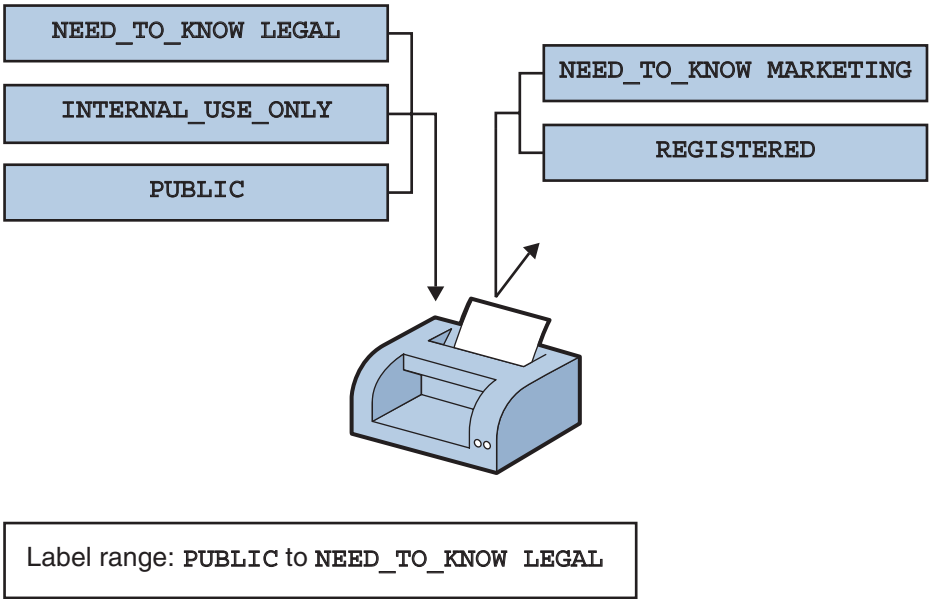
Printed below the sensitivity label, *handling instructions* provides distribution instructions for the printed material. The instructions state that the information should be distributed only to human resources personnel who need to know the information. Also, a reader must have signed a nondisclosure agreement.

Printers can be configured to print only jobs with labels within a restricted label range. For example, Figure 6–3 illustrates that the legal department's printer has been set up to print only jobs that have been assigned one of three labels:

- NEED_TO_KNOW LEGAL – Can be viewed only by employees with a need to know within the legal department
- INTERNAL_USE_ONLY – Can be viewed only by permanent employees of the SecCompany company and customers who have signed nondisclosure agreements
- PUBLIC – Can be viewed by anyone

This printer setup excludes jobs that are sent at any other label. For example, this printer would reject jobs at the labels NEED_TO_KNOW MARKETING and REGISTERED.

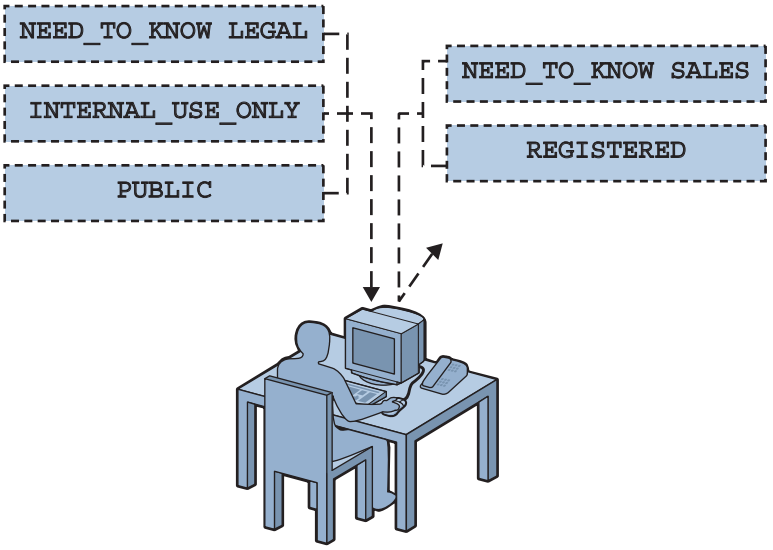
FIGURE 6–3 How a Printer With a Restricted Label Range Handles Jobs



Printers in locations that are accessible to all employees can be similarly restricted. For example, printers can be configured to print jobs only at the two labels that all employees can view, INTERNAL_USE_ONLY and PUBLIC.

Similar to how the printer label range controls which jobs can be printed on a particular printer, a user's *account sensitivity label range* limits which email the person can handle. Figure 6–4 shows email that is being labeled at the sensitivity label of the user's mail application. The email is sent to the mail application at that label.

FIGURE 6–4 A User Receiving Email Within the Account Label Range



Account's label range: `PUBLIC` to `NEED_TO_KNOW LEGAL`
Sensitivity labels within range: `PUBLIC`, `INTERNAL_USE_ONLY`, and `NEED_TO_KNOW LEGAL`

Gateways to the Internet were set up to screen email so that emails at inappropriate labels could not be sent outside of the company. Inappropriate labels are any labels except `PUBLIC`.

Climbing the Security Learning Curve

The management identifies an experienced administrator with the following qualifications:

- Is assessed to be trustworthy
- Knows how to administer Solaris systems
- Understands the organization's information-processing goals well enough to be responsible for overseeing or implementing the site's security

That person is assigned the job of security administrator.

Long before installing Trusted Extensions software, the security administrator starts to learn about security and to prepare a plan for the site's security policy. First, the security administrator reads the following documents:

- Chapter 1, "Security Planning for Trusted Extensions," in *Oracle Solaris Trusted Extensions Configuration Guide* – For guidance on creating a site's security policy
- *Oracle Solaris Trusted Extensions User's Guide* – To become familiar with label types and appearance
- *Oracle Solaris Trusted Extensions Administrator's Procedures* – To become familiar with security administrator responsibilities and tools
- Chapter 1, "Labels in Trusted Extensions Software" – To review label concepts

Then, the security administrator starts with a plan for the site's labels. The planning process is described in the following sections.

Analyzing the Requirements for Each Label

The security administrator agrees that the set of labels that are mandated by the legal department is a useful starting point. However, the further analysis is needed before the labels can be encoded.

Requirements for `CONFIDENTIAL: INTERNAL_USE_ONLY`

The `CONFIDENTIAL: INTERNAL_USE_ONLY` label is for information that is proprietary to the company but which, because of its low level of sensitivity, can be distributed to all employees. All employees have signed nondisclosure agreements before starting employment. Information with this label might also be distributed to others. For example, the employees of vendors and contractors who have signed a nondisclosure agreement can receive the information. Because the Internet can be snooped, information with this label cannot be sent over the Internet. The information can be sent over email within the company.

Candidates for the `CONFIDENTIAL: INTERNAL_USE_ONLY` label include the following:

- Spending guidelines
- Internal job postings

Requirements for `CONFIDENTIAL: NEED_TO_KNOW`

The `CONFIDENTIAL: NEED_TO_KNOW` label is intended for information that is proprietary to the company, has a higher level of sensitivity than `INTERNAL_USE_ONLY`, and has a more limited audience. Distribution is limited to employees who need to know the information. Other people who need to know the information and who have signed nondisclosure agreements might also be in the audience.

For example, if only the group of people working in a particular project should see certain information, then NEED_TO_KNOW should be used on that information. Whenever information should be restricted to a particular group, the name of the group should be specified on the paper version of the information.

Having the name of a group in this label makes it clear that the information should not be given to anyone outside of the group. Information with this label cannot be sent over the Internet but it can be sent over email within the company.

Candidates for the NEED_TO_KNOW label include the following:

- Product design documents
- Project details
- Employee Status Change form

Requirements for CONFIDENTIAL: REGISTERED

The CONFIDENTIAL: REGISTERED classification is intended for information that is proprietary to the company, has a very high level of sensitivity, and could significantly harm the company if released. Registered information must be numbered and be tracked by the owner. Each copy must be assigned to a specific person. The copy must be returned to the owner for destruction after being read. Copies can be made only by the owner of the information. Use of brownish-red paper is recommended because this color cannot be copied.

This label is to be used when only one specific group of people should be allowed to see the proprietary information. This information cannot be shown to anyone who is not authorized by the owner. The information cannot be shown to employees of other companies who have not signed a nondisclosure agreement, even if the owner authorizes the disclosure. Information with this label cannot be sent through email.

Candidates for the CONFIDENTIAL: REGISTERED label include the following:

- End of quarter financial information that has not yet been released
- Sales forecasts
- Marketing forecasts

Names of Groups With NEED_TO_KNOW Label

The security administrator decided that the NEED_TO_KNOW label should contain the names of groups or departments. The security Administrator asked for suggestions about what words to use to define groups or areas of interest within the organization. The following items were in the initial list:

- Engineering
- Executive Management

- Finance
- Human Resources
- Legal
- Manufacturing
- Marketing
- Sales
- System Administration

Later, the security administrator added the Project Team group, which enabled all members of the Engineering and Marketing groups to share project data.

Understanding the Set of Labels

The next step is to resolve the following issues:

- How to use the classifications and compartments to encode the labels and clearances
- Which handling instructions should appear on printed output

The security administrator used a large board. Pieces of paper were marked with the words that should be in the labels, as shown in Figure 6–5. This setup graphed the relationships. The pieces could be rearranged until all the pieces fit together.

The administrator drafted the following label relationships:

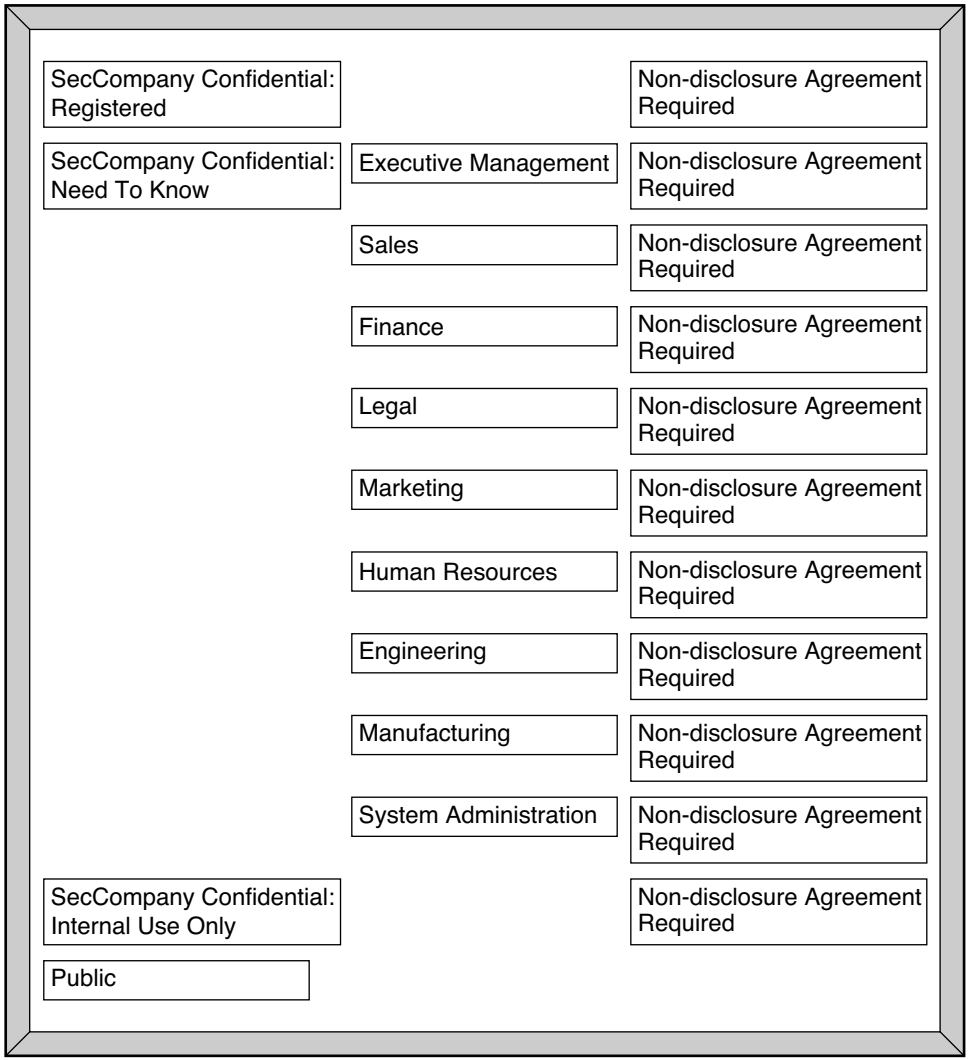
- The four labels are hierarchical with the label that contains `REGISTERED` the highest. The `PUBLIC` label is the lowest.
- Only one label needs to be associated with group names

  The list of people who are cleared to receive registered information is limited on a case by case basis. Therefore, `REGISTERED` does not need any group names. `INTERNAL_USE_ONLY` applies to all employees and people who have signed nondisclosure agreements and `PUBLIC` labels are for everybody. Therefore, `INTERNAL_USE_ONLY` and `PUBLIC` labels do not need further qualification. The `NEED_TO_KNOW` label does need to be associated with non-hierarchical words, such as `NEED_TO_KNOW MARKETING` or `NEED_TO_KNOW ENGINEERING`. The words that identify the group or department can also be included in a user's clearance, as part of establishing that user's need to know.
- Each of the labels except `PUBLIC` requires the person who is accessing the information to have signed a nondisclosure agreement.

  A phrase such as `NON-DISCLOSURE AGREEMENT REQUIRED` would be a good reminder that this requirement exists.
- The handling instructions on banner and trailer pages should have clear wording on how to handle the information. How to handle the information is based on the classification and on any group name that can appear in the label.

Along with information on the sensitivity of the printer output, handling instructions should print that a nondisclosure agreement is required when the label requires such an agreement.

FIGURE 6–5 Sample Planning Board for Label Relationships



Defining the Set of Labels

In this section the set of labels is defined in lists that include all of the following required aspects of labels:

- Classifications
- Other words
- Relations between and among the words
- Classification restrictions that are associated with use of each word
- Intended use of the words in sensitivity labels and clearances
- Intended use of the words in labeling system output, such as print and email

Planning the Classifications

Because the four labels are hierarchical, the four labels are encoded as hierarchical classifications.

With the legal department's approval, the security administrator shortened the labels by omitting SecCompany Confidential: from the label names. Long classifications make labels hard to read in window frames. The name of a label is truncated from right to left in the window frames. Because the truncated names of all the label names above `PUBLIC` would begin with the words `SECCOMPANY`, the truncated names would be indistinguishable without manually extending the frame for each window.

The security administrator defined the following labels:

- `REGISTERED`
- `NEED_TO_KNOW`
- `INTERNAL_USE_ONLY`
- `PUBLIC`

Planning the Compartments

The group names will be encoded as non-hierarchical *compartments*. Compartments will be restricted to appear only in labels that have the `NEED_TO_KNOW` classification. Compartment restrictions are encoded in the `ACCREDITATION RANGE` section under `COMBINATION CONSTRAINTS`.

User *clearances* will control which users can create files and directories that have a group name in the label. User clearances will also control which users can create documents that have a label with more than one group name along with the `NEED_TO_KNOW` classification.

Planning the Use of Words in MAC

The classifications and compartments in sensitivity labels and user clearances are used in mandatory access control (MAC). Therefore, the legal department's hierarchical labels and the group names need to be encoded as classifications and compartments so that they can be used in the labels that control which individual employees can access files and do other work.

SecCompany, Inc. defines a sensitivity label with the `PUBLIC` classification, which is assigned the lowest value in the User Accreditation Range, and another sensitivity label with the `INTERNAL_USE_ONLY` classification with the next highest value above `PUBLIC`.

An employee with no authorizations whose clearance is `PUBLIC` and whose minimum label is `PUBLIC` is able to use the system as follows:

- Works only in a `PUBLIC` workspace.
- Creates files only at `PUBLIC`.
- Reads email only at `PUBLIC`.
- Uses printers that have `PUBLIC` in their label range.

  In contrast, an employee with no authorizations whose clearance is `INTERNAL_USE_ONLY` is able to use the system as follows:

- Works in either a `PUBLIC` or an `INTERNAL_USE_ONLY` workspace.
- Creates files at either `PUBLIC` or `INTERNAL_USE_ONLY`, depending on the employee's current workspace.
- Receives and sends email at either sensitivity label.
- Can print a file that is labeled `PUBLIC` on any printer with `PUBLIC` in its label range. Can send a file labeled `INTERNAL_USE_ONLY` to any printer with `INTERNAL_USE_ONLY` in its label range.

Planning the Use of Words in Labeling System Output

When the sensitivity label of a printer job contains a group name compartment, the mandatory printer banner and trailer pages print the following text:

`Distribute Only To` *Group Name* `(Non-Disclosure Agreement Required)`

Planning Unlabeled Printer Output

The `Print Without Labels` authorization allows a user or role to use the `lp -o nolabels` option to suppress the printing of top and bottom labels on body pages of a print job. The Security Administrator role can give the `Print Without Labels` authorization to everyone or to no one.

The Print PostScript File authorization allows a user to submit a PostScript file to the printer. PostScript printing is usually not allowed because of the risk that a knowledgeable user can change the labels in the PostScript file.

To permit technical writers to produce master copies of documents without labels printed on them, the Security Administrator role gives the Print Without Labels and Print PostScript File authorizations to all the writers.

Planning for Supporting Procedures

The security administrator creates security policies to enforce the labeling scheme.

Rules for Protecting a REGISTERED File or Directory

The security administrator realizes that anyone with a clearance that includes the word REGISTERED can access any registered information anywhere in the company. Further precautions are needed. For example, users who have REGISTERED in their clearance must be instructed to use UNIX permissions to protect their files. Permissions should be set so that only the creator can look at or modify the file. The following example shows a user who is applying discretionary access control to protect the contents of a REGISTERED directory.

EXAMPLE 6–2 Using DAC to Protect Registered Information

```
% plabel
REGISTERED
% mkdir registered.dir
% chmod 700 registered.dir
% cd registered.dir
% touch registered.file
% ls -l
-rwxrwxrwx registered.file
% chmod 600 registered.file
% ls -l
-rw------- registered.file
```

As shown in the example, the user who creates a file or directory while working at an sensitivity label of REGISTERED needs to set the file's permissions to be read and write for the owner only. Directory permissions are set to be readable, writable, and searchable only by the owner. These permissions ensure that another user who can work at REGISTERED cannot read the file.

Rules for Configuring Printers

The following table shows how printers that are available to various work groups need to be configured.

TABLE 6–1 Printer Label Range Example Settings in Various Locations

Printer Location	Type of Access	Label Range
Lobby or public meeting room	Anyone	PUBLIC to PUBLIC
Internal company printer room	Available to all employees and others who have signed nondisclosure agreements	PUBLIC to INTERNAL_USE_ONLY
Restricted area for one group	Members of group specified in the NEED_TO_KNOW *group-name* compartment	NEED_TO_KNOW *group-name* to NEED_TO_KNOW *group-name*
Strictly controlled area	Available only to people who have the REGISTERED classification in their clearance	REGISTERED to REGISTERED

See Chapter 15, "Managing Labeled Printing (Tasks)," in *Oracle Solaris Trusted Extensions Administrator's Procedures*.

Rules for Handling Printer Output

People who have access to restricted printers will be instructed to do the following:

- Protect information according to the instructions on the printer banner and trailer pages.
- Shred jobs that do not have both a banner and a trailer page. Also shred jobs that do not have matching job numbers on the banner and trailer pages.

Planning the Classification Values in a Worksheet

The worksheet in the following table shows names and hierarchical values defined for the four classifications. Because the value 0 is reserved for the administrative ADMIN_LOW label, the value of the PUBLIC classification is set to 1. The values of the other classifications are set higher in ascending sensitivity.

Note – The names of groups in the labels are specified later, as WORDS in the SENSITIVITY LABELS and CLEARANCES sections.

TABLE 6–2 Classifications Planner

name=	sname=/aname=	value=	initial compartments= bit numbers/WORD
PUBLIC	PUB	1	None
INTERNAL_USE_ONLY	IUO	4	None

TABLE 6–2 Classifications Planner *(Continued)*

name=	sname=/aname=	value=	initial compartments= bit numbers/WORD
NEED_TO_KNOW	NTK	5	None
REGISTERED	REG	6	None

Planning the Compartment Values and Combination Constraints in a Worksheet

The following table defines the relationships between words and classifications. The relationships were determined by moving things around on the planning board in Figure 6–5. PUBLIC and INTERNAL_USE_ONLY can never appear in a label with any compartment. NEED_TO_KNOW can appear in a label with any of the compartments or all of the compartments.

TABLE 6–3 Compartments and User Accreditation Range Combinations Planner

Classification	Compartment Name/ sname/ Bit	Combination Constraints
PUBLIC		PUBLIC only valid combinations
INTERNAL_USE_ONLY		INTERNAL_USE_ONLY only valid combinations
NEED_TO_KNOW	SYSTEM ADMINISTRATION/ SYSADM/ 19	NEED_TO_KNOW all combinations valid
	MANUFACTURING/ MANU/ 18	
	ENGINEERING/ ENG/ 17 20	
	HUMAN RESOURCES/ HR/ 16	
	MARKETING/ MKTG/ 15 20	
	LEGAL/ LEGAL/ 14	
	FINANCE/ FINANCE/ 13	
	SALES/ SALES/ 12	
	EXECUTIVE MANAGEMENT GROUP/ EMGT/ 11	
	ALL_DEPARTMENTS/ ALL/ 11-20	
REGISTERED		REGISTERED only valid combinations

The security administrator uses the following table to keep track of which bits have been used for compartments.

TABLE 6–4 Compartment Bit Tracking Table

11	12	13	14	15	16	17	18	19	20	

Planning the Clearances in a Worksheet

The components of these labels are also assigned to users in clearances. The worksheet's Clearance Planner, Table 6–5, defines the label components to be used in clearances.

Key to Table 6–5:

Abbreviation	Name
REG	REGISTERED
NTK	NEED_TO_KNOW
IUO	INTERNAL_USE_ONLY
EMGT	EXECUTIVE MANAGEMENT GROUP
SALES	SALES
FIN	FINANCE
LEGAL	LEGAL
MKTG	MARKETING
HR	HUMAN RESOURCES
ENG	ENGINEERING
MANU	MANUFACTURING
SYSADM	SYSTEM ADMINISTRATION
NDA	NON-DISCLOSURE AGREEMENT

TABLE 6–5 Clearance Planner

CLASS	COMP	COMP	COMP	COMP	COMP	COMP	COMP	COMP	COMP	Notes
REG	EMGT	ENG	FIN	HR	LEGAL	MANU	MKTG	SALES	SYSADM	Highest, not used *

TABLE 6–5 Clearance Planner *(Continued)*

CLASS	COMP	COMP	COMP	COMP	COMP	COMP	COMP	COMP	COMP	Notes
REG										Assigned to selected personnel as needed **
NTK		ENG								Assigned to ENG group
									SYSADM	Assigned to system administrator
IUO										Assigned to employees. and others with NDAs
PUB										Assigned to anyone

* The highest possible label in the system consists of the highest classification and all of the defined compartments. Because no one should be able to access all information in all departments, this label is not in the user accreditation range. No one should be assigned this clearance.

** When working at the REGISTERED sensitivity label, the user should set permissions to restrict access to everyone except the owner. File permissions of 600 and directory permissions of 700 restrict access.

Planning the Printer Banners in a Worksheet

The SecCompany legal department wants the following to appear on printer banner and trailer pages.

```
SecCompany Confidential:
```

The PRINTER BANNERS can be used to associate a string with any compartment that appears in the sensitivity label of the print job. In this encodings, only the NEED_TO_KNOW classification has compartments. The following table shows how the desired wording is specified as a prefix and assigned to each compartment. The abbreviation NTK is assigned to each channel so that the wording in the PRINTER BANNERS section includes the group name:

```
SecCompany Confidential: group-name
```

TABLE 6–6 SecCompany Printer Banners Planner

Prefix	Printer Banner (Word, No Suffix)
SECCOMPANY CONFIDENTIAL:	ALL_DEPARTMENTS
SECCOMPANY CONFIDENTIAL:	EXECUTIVE_MANAGEMENT_GROUP
SECCOMPANY CONFIDENTIAL:	SALES
SECCOMPANY CONFIDENTIAL:	FINANCE
SECCOMPANY CONFIDENTIAL:	LEGAL
SECCOMPANY CONFIDENTIAL:	MARKETING
SECCOMPANY CONFIDENTIAL:	HUMAN_RESOURCES
SECCOMPANY CONFIDENTIAL:	ENGINEERING
SECCOMPANY CONFIDENTIAL:	MANUFACTURING
SECCOMPANY CONFIDENTIAL:	SYSTEM_ADMINISTRATION
SECCOMPANY CONFIDENTIAL:	PROJECT_TEAM

Planning the Channels in a Worksheet

The SecCompany legal department wants the following handling instructions to appear on printer banner and trailer pages.

DISTRIBUTE ONLY TO *group-name* EMPLOYEES (NON-DISCLOSURE AGREEMENT REQUIRED)

This goal is met by assigning in the CHANNELS section the same compartment bits that were assigned to group names earlier in this example. The SecCompany company plans to use the same group names both in the compartments and in the channels.

The words that come before the channel name are specified as *prefixes* and the words that come after the channel name are specified as *suffixes*. The security administrator specifies prefixes and suffixes in the following worksheets.

TABLE 6–7 SecCompany Channels Planner

Prefix	Channel	Suffix
DISTRIBUTE_ONLY_TO	EXECUTIVE_MANAGEMENT_GROUP	EMPLOYEES (NON-DISCLOSURE_AGREEMENT_REQUIRED)
DISTRIBUTE_ONLY_TO	SALES	EMPLOYEES (NON-DISCLOSURE_AGREEMENT_REQUIRED)
DISTRIBUTE_ONLY_TO	FINANCE	EMPLOYEES (NON-DISCLOSURE_AGREEMENT_REQUIRED)
DISTRIBUTE_ONLY_TO	LEGAL	EMPLOYEES (NON-DISCLOSURE_AGREEMENT_REQUIRED)

TABLE 6–7 SecCompany Channels Planner *(Continued)*

Prefix	Channel	Suffix
DISTRIBUTE_ONLY_TO	MARKETING	EMPLOYEES (NON-DISCLOSURE_AGREEMENT_REQUIRED)
DISTRIBUTE_ONLY_TO	HUMAN_RESOURCES	EMPLOYEES (NON-DISCLOSURE_AGREEMENT_REQUIRED)
DISTRIBUTE_ONLY_TO	ENGINEERING	EMPLOYEES (NON-DISCLOSURE_AGREEMENT_REQUIRED)
DISTRIBUTE_ONLY_TO	MANUFACTURING	EMPLOYEES (NON-DISCLOSURE_AGREEMENT_REQUIRED)
DISTRIBUTE_ONLY_TO	SYSTEM_ADMINISTRATION	EMPLOYEES (NON-DISCLOSURE_AGREEMENT_REQUIRED)
DISTRIBUTE_ONLY_TO	PROJECT_TEAM	EMPLOYEES (NON-DISCLOSURE_AGREEMENT_REQUIRED)

Planning the Minimums in an Accreditation Range

The following minimums must be set:

- Minimum sensitivity label
- Minimum clearance
- Minimum protect as classification

The SecCompany company wants employees to be able to use all the defined sensitivity labels. Also, the company wants to be able to assign the `PUBLIC` clearance to some employees. Therefore, the `minimum sensitivity label` and `minimum clearance` need to be set to `PUBLIC`.

The `minimum protect as` classification is printed on printer banner and trailer pages instead of the actual classification from the job's sensitivity label. The `minimum protect as classification` can be set higher than the *actual* minimum classification. However, the SecCompany company requirements allow the `minimum protect as` classification to always be equal to the real classification of the print job's sensitivity label. The security administrator specifies the value `PUBLIC` for the `minimum sensitivity label`, `minimum clearance` and `minimum protect as` classification.

Planning the Colors in a Worksheet

The color that is assigned to a label displays in the background whenever the name of the label appears at the top of a window. The lettering is displayed in a color that is computed by the window system to complement the background. In our example, the security administrator chooses to keep the colors already assigned to the administrative labels in the default `label_encodings` file. The administrator assigns green to `PUBLIC`, yellow to `INTERNAL_USE_ONLY`, blue to labels that contain `NEED_TO_KNOW` (with different shades of blue assigned to each compartment), and red to `REGISTERED`, as shown in the following table.

TABLE 6–8 SecCompany Color Names Planner

Label or Name (label= **or** name=)	**Color**
ADMIN_LOW	#BDBDBD
PUBLIC	green
INTERNAL_USE_ONLY	yellow
NEED_TO_KNOW	blue
NEED_TO_KNOW EMGT	#7FA9EB
NEED_TO_KNOW SALES	#87CEFF
NEED_TO_KNOW FINANCE	#00BFFF
NEED_TO_KNOW LEGAL	#7885D0
NEED_TO_KNOW MKTG	#7A67CD
NEED_TO_KNOW HR	#7F7FFF
NEED_TO_KNOW ENG	#007FFF
NEED_TO_KNOW MANU	#0000BF
NEED_TO_KNOW PROJECT_TEAM	#9E7FFF
NEED_TO_KNOW SYSADM	#5B85D0
NEED_TO_KNOW ALL	#4D658D
NEED_TO_KNOW SYSADM	#5B85D0
REGISTERED	red
ADMIN_HIGH	#636363

Editing and Installing the label_encodings File

The install team makes a printed copy and an online copy of the installed label_encodings file. The copy is used in case of problems with the new version of the file that the Security Administrator role supplies.

The Security Administrator role uses a text editor to create the label_encodings file, and then uses the Check Encodings action to check the file. If the file passes Check Encodings, the action offers the option of installing the new version. When the Security Administrator role answers Yes, Check Encodings backs up the current version of the label_encodings file, and creates a new label_encodings file.

Encoding the Version

The following example shows the VERSION string that is modified with the name of company, a title, version number, and date.

EXAMPLE 6–3 SecCompany VERSION Entry

```
VERSION= SecCompany, Inc. Example Version - 2.2 00/04/18
```

Encoding the Classifications

The following example shows the SecCompany classifications and values from Table 6–2, Table 6–3 and Table 6–4 added to the CLASSIFICATIONS section.

EXAMPLE 6–4 SecCompany CLASSIFICATIONS Section

```
CLASSIFICATIONS:

name= PUBLIC; sname= PUBLIC; value= 1;
name= INTERNAL_USE_ONLY; sname= INTERNAL; aname= INTERNAL; value= 4;
name= NEED_TO_KNOW; sname= NEED_TO_KNOW; aname= NEED_TO_KNOW; value= 5;
name= REGISTERED; sname= REGISTERED; aname= REGISTERED; value= 6;
```

Note – A classification cannot contain the slash (/), or comma (,) character. The classifications are specified from the lowest value to the highest.

Encoding the Sensitivity Labels

The compartments in the Table 6–3 are encoded in the following example. The labels do not have any required combinations or combination constraints.

EXAMPLE 6–5 SecCompany WORDS in the SENSITIVITY LABELS Section

```
SENSITIVITY LABELS:

WORDS:

name= ALL_DEPARTMENTS; sname= ALL; compartments= 11-20;
minclass= NEED_TO_KNOW;
name= EXECUTIVE_MGT_GROUP; sname= EMGT; compartments= 11;
minclass= NEED_TO_KNOW;
name= SALES; sname= SALES; compartments= 12;
```

EXAMPLE 6–5 SecCompany WORDS in the SENSITIVITY LABELS Section *(Continued)*

```
minclass= NEED_TO_KNOW;
name= FINANCE; sname= FINANCE; compartments= 13;
minclass= NEED_TO_KNOW;
name= LEGAL; sname= LEGAL; compartments= 14;
minclass= NEED_TO_KNOW;
name= MARKETING; sname= MKTG; compartments= 15 20; minclass= NEED_TO_KNOW;
name= HUMAN_RESOURCES; sname= HR; compartments= 16; minclass= NEED_TO_KNOW;
name= ENGINEERING; sname= ENG; compartments= 17 20; minclass= NEED_TO_KNOW;
name= MANUFACTURING; sname= MANUFACTURING; compartments= 18;
minclass= NEED_TO_KNOW;
name= SYSTEM_ADMINISTRATION; sname= SYSADM; compartments= 19;
minclass= NEED_TO_KNOW;
name= PROJECT_TEAM; sname= P_TEAM; compartments= 20; minclass= NEED_TO_KNOW;

REQUIRED COMBINATIONS:

COMBINATION CONSTRAINTS:
```

Encoding the Information Labels

Even though information labels are not used, values must be supplied under the INFORMATION LABELS: WORDS: section for the file to pass the encodings check. The Security Administrator role copies the words from the SENSITIVITY LABELS: WORDS: section, as shown in the following example.

EXAMPLE 6–6 SecCompany WORDS in the INFORMATION LABELS Section

```
INFORMATION LABELS:

WORDS:

name= ALL_DEPARTMENTS; sname= ALL; compartments= 11-20;
minclass= NEED_TO_KNOW;
name= EXECUTIVE_MGT_GROUP; sname= EMGT; compartments= 11;
minclass= NEED_TO_KNOW;
name= SALES; sname= SALES; compartments= 12;
minclass= NEED_TO_KNOW;
name= FINANCE; sname= FINANCE; compartments= 13;
minclass= NEED_TO_KNOW;
name= LEGAL; sname= LEGAL; compartments= 14;
minclass= NEED_TO_KNOW;
name= MARKETING; sname= MKTG; compartments= 15 20; minclass= NEED_TO_KNOW;
name= HUMAN_RESOURCES; sname= HR; compartments= 16; minclass= NEED_TO_KNOW;
name= ENGINEERING; sname= ENG; compartments= 17 20; minclass= NEED_TO_KNOW;
```

EXAMPLE 6–6 SecCompany WORDS in the INFORMATION LABELS Section *(Continued)*

```
name= MANUFACTURING; sname= MANUFACTURING; compartments= 18;
minclass= NEED_TO_KNOW;
name= SYSTEM_ADMINISTRATION; sname= SYSADM; compartments= 19;
minclass= NEED_TO_KNOW;
name= PROJECT_TEAM; sname= P_TEAM; compartments= 20; minclass= NEED_TO_KNOW;

REQUIRED COMBINATIONS:

COMBINATION CONSTRAINTS:
```

Encoding the Clearances

Because the clearance words are the same as the sensitivity labels words, the words in the following example are the same as the words in Example 6–5.

EXAMPLE 6–7 SecCompany WORDS in the CLEARANCES Section

```
CLEARANCES:

WORDS:

name= ALL_DEPARTMENTS; sname= ALL; compartments= 11-20; minclass= NEED_TO_KNOW;
name= EXECUTIVE_MANAGEMENT_GROUP; sname= EMGT; compartments= 11;
minclass= NEED_TO_KNOW;
name= SALES; sname= SALES; compartments= 12; minclass= NEED_TO_KNOW;
name= FINANCE; sname= FINANCE; compartments= 13; minclass= NEED_TO_KNOW;
name= LEGAL; sname= LEGAL; compartments= 14; minclass= NEED_TO_KNOW;
name= MARKETING; sname= MKTG; compartments= 15 20; minclass= NEED_TO_KNOW;
name= HUMAN_RESOURCES; sname= HR; compartments= 16; minclass= NEED_TO_KNOW;
name= ENGINEERING; sname= ENG; compartments= 17 20; minclass= NEED_TO_KNOW;
name= MANUFACTURING; sname= MANUFACTURING; compartments= 18; minclass= NEED_TO_KNOW;
name= SYSTEM_ADMINISTRATION; sname= SYSADM; compartments= 19; minclass= NEED_TO_KNOW;
name= PROJECT_TEAM; sname= P_TEAM; compartments= 20;
minclass= NEED_TO_KNOW;

REQUIRED COMBINATIONS:

COMBINATION CONSTRAINTS:
```

Encoding the Channels

This example is encoded with one channel for each group name compartment. Each channel uses the same compartment bits that are assigned to the compartment words in the

SENSITIVITY LABELS: WORDS: section. The prefix is defined as DISTRIBUTE ONLY TO. The suffix is defined as (NON-DISCLOSURE AGREEMENT REQUIRED).

```
DISTRIBUTE ONLY TO group-name (NON-DISCLOSURE AGREEMENT REQUIRED)
```

The channel specifications in the following example create the desired wording in the handling instructions section.

Note – The prefixes and suffixes are defined at the top of the section as shown in the following example. No compartments are assigned to them. The prefixes and suffixes are used to define the channels.

EXAMPLE 6–8 SecCompany WORDS in the CHANNELS Section

```
CHANNELS:

WORDS:

name= DISTRIBUTE_ONLY_TO;       prefix;
name= EMPLOYEES (NON-DISCLOSURE AGREEMENT REQUIRED);
suffix;

name= EXECUTIVE_MANAGEMENT_GROUP;
prefix= DISTRIBUTE_ONLY_TO; compartments= 11;
suffix= EMPLOYEES (NON-DISCLOSURE AGREEMENT REQUIRED);
name= SALES; prefix= DISTRIBUTE_ONLY_TO; compartments= 12;
suffix= EMPLOYEES (NON-DISCLOSURE AGREEMENT REQUIRED);
name= FINANCE; prefix= DISTRIBUTE_ONLY_TO; compartments= 13;
suffix= EMPLOYEES (NON-DISCLOSURE AGREEMENT REQUIRED);
name= LEGAL; prefix= DISTRIBUTE_ONLY_TO; compartments= 14;
suffix= EMPLOYEES (NON-DISCLOSURE AGREEMENT REQUIRED);
name= MARKETING; prefix= DISTRIBUTE_ONLY_TO;
compartments= 15 20;
suffix= EMPLOYEES (NON-DISCLOSURE AGREEMENT REQUIRED);
name= HUMAN_RESOURCES; prefix= DISTRIBUTE_ONLY_TO;
compartments= 16;
suffix= EMPLOYEES (NON-DISCLOSURE AGREEMENT REQUIRED);
name= ENGINEERING; prefix= DISTRIBUTE_ONLY_TO;
compartments= 17 20;
suffix= EMPLOYEES (NON-DISCLOSURE AGREEMENT REQUIRED);
name= MANUFACTURING; prefix= DISTRIBUTE_ONLY_TO;
compartments= 18;
suffix= EMPLOYEES (NON-DISCLOSURE AGREEMENT REQUIRED);
name= SYSTEM_ADMINISTRATION; prefix= DISTRIBUTE_ONLY_TO;
compartments= 19;
suffix= EMPLOYEES (NON-DISCLOSURE AGREEMENT REQUIRED);
```

EXAMPLE 6–8 SecCompany WORDS in the CHANNELS Section *(Continued)*

```
name= PROJECT_TEAM; prefix= DISTRIBUTE_ONLY_TO; compartments= 20;
suffix= EMPLOYEES (NON-DISCLOSURE AGREEMENT REQUIRED);
```

Encoding the Printer Banners

Note – The term *printer banners* has a specialized meaning in the label_encodings file. A printer banner appears as a string on the printer banner page when the compartment that is associated with it appears in a job's label.

The printer banner specifications that are shown in the following example create the desired wording in the PRINTER BANNERS section. For a sample banner page, see Figure 4–2.

Note – Prefixes are defined at the top of the section, as shown in the following example. The prefixes have no assigned compartments.

EXAMPLE 6–9 SecCompany WORDS in the PRINTER BANNERS Section

```
PRINTER BANNERS:

WORDS:

name= COMPANY CONFIDENTIAL:;       prefix;

name= ALL_DEPARTMENTS; prefix= COMPANY CONFIDENTIAL:;
suffix=(NON-DISCLOSURE AGREEMENT REQUIRED); compartments= 11-20;
name= EXECUTIVE_MANAGEMENT_GROUP; prefix= COMPANY CONFIDENTIAL:;
suffix=(NON-DISCLOSURE AGREEMENT REQUIRED); compartments= 11;
name= SALES; prefix= COMPANY CONFIDENTIAL:;
suffix=(NON-DISCLOSURE AGREEMENT REQUIRED); compartments= 12;
name= FINANCE; prefix= COMPANY CONFIDENTIAL:;
suffix=(NON-DISCLOSURE AGREEMENT REQUIRED); compartments= 13;
name= LEGAL; prefix= COMPANY CONFIDENTIAL:;
suffix=(NON-DISCLOSURE AGREEMENT REQUIRED); compartments= 14;
name= MARKETING; prefix= COMPANY CONFIDENTIAL:;
suffix=(NON-DISCLOSURE AGREEMENT REQUIRED); compartments= 15 20;
name= HUMAN_RESOURCES; prefix= COMPANY CONFIDENTIAL:;
suffix=(NON-DISCLOSURE AGREEMENT REQUIRED); compartments= 16;
name= ENGINEERING; prefix= COMPANY CONFIDENTIAL:;
suffix=(NON-DISCLOSURE AGREEMENT REQUIRED); compartments= 17 20;
name= MANUFACTURING; prefix= COMPANY CONFIDENTIAL:;
```

EXAMPLE 6–9 SecCompany WORDS in the PRINTER BANNERS Section *(Continued)*

```
suffix=(NON-DISCLOSURE AGREEMENT REQUIRED); compartments= 18;
name= SYSTEM_ADMINISTRATION; prefix= COMPANY CONFIDENTIAL:;
suffix=(NON-DISCLOSURE AGREEMENT REQUIRED); compartments= 19;
name= PROJECT_TEAM; prefix= COMPANY CONFIDENTIAL:;
suffix=(NON-DISCLOSURE AGREEMENT REQUIRED); compartments= 20;
```

Encoding the Accreditation Range

The combination constraints from Table 6–3, and the minimum clearance, minimum sensitivity label and minimum protect as classification from "Planning the Minimums in an Accreditation Range" on page 99 are encoded in the ACCREDITATION RANGE: section in the following example. PUBLIC and INTERNAL_USE_ONLY are defined to never appear in a label with any compartment. NEED_TO_KNOW is defined to appear in a label with any combination of compartments. REGISTERED is defined to appear with no compartments.

EXAMPLE 6–10 SecCompany ACCREDITATION RANGE Section

```
ACCREDITATION RANGE:

classification= PUBLIC; only valid compartment combinations:

PUBLIC

classification= INTERNAL_USE_ONLY; only valid compartment combinations:

INTERNAL

classification= NEED_TO_KNOW; all compartment combinations valid;

classification= REGISTERED; only valid compartment combinations:

REGISTERED


minimum clearance= PUBLIC;
minimum sensitivity label= PUBLIC;
minimum protect as classification= PUBLIC;
```

Encoding the Local Definitions

SecCompany, Inc. encodes site column headers and colors in the LOCAL DEFINITIONS section.

Encoding the Column Headers in Label Builders

Label builders are displayed whenever you need to set a label. The following example shows the modifications that changed the default values for the Classification Name and Compartments Name in the label builders.

EXAMPLE 6–11 SecCompany Headers in label_encodings File

The following excerpt shows the modifications that changed the column headers in the label builders. The SecCompany Security Administrator role modified the compartment name.

```
Classification Name= Classification;
Compartments Name= Department;
```

Encoding the Color Names

The color names that are used in Example 6–12 were taken from the worksheet in Table 6–8.

EXAMPLE 6–12 SecCompany COLOR NAMES Section

```
COLOR NAMES:

        label= Admin_Low;       color= #bdbdbd;

        label= PUBLIC;        color= green;
        label= INTERNAL_USE_ONLY;  color= yellow;
        label= NEED_TO_KNOW;  color= blue;
        label= NEED_TO_KNOW EMGT;  color= #7FA9EB;
        label= NEED_TO_KNOW SALES;  color= #87CEFF;
        label= NEED_TO_KNOW FINANCE;  color= #00BFFF;
        label= NEED_TO_KNOW LEGAL;  color= #7885D0;
        label= NEED_TO_KNOW MKTG;  color= #7A67CD;
        label= NEED_TO_KNOW HR;  color= #7F7FFF;
        label= NEED_TO_KNOW ENG;  color= #007FFF;
        label= NEED_TO_KNOW MANUFACTURING;  color= #0000BF;
        label= NEED_TO_KNOW PROJECT_TEAM;  color= #9E7FFF;
        label= NEED_TO_KNOW SYSADM; color= #5B85D0;
        label= NEED_TO_KNOW ALL; color= #4D658D;
        label= REGISTERED;  color= red;

        label= Admin_High;      color= #636363;

*
* End of local site definitions
```

Configuring Users and Printers for Labels

Labeling decisions need to be enforced on users, and on printers.

When setting up user accounts, the Security Administrator role needs to specify the following for every user:

- The appropriate clearance

  To plan user clearances, see "Planning the Clearances in a Worksheet" on page 96.
- The appropriate minimum label
- Label visibility

For details, see "Managing Users and Rights With the Solaris Management Console (Task Map)" in *Oracle Solaris Trusted Extensions Administrator's Procedures*.

The Security Administrator role can customize labeling or not labeling printed output. For the procedures, see "Managing Printing in Trusted Extensions (Task Map)" in *Oracle Solaris Trusted Extensions Administrator's Procedures*.

◆ ◆ ◆ APPENDIX A

Sample Label Encodings File

This appendix contains the `label_encodings` file that was customized in Chapter 6, "Example: Planning an Organization's Labels."

Classifications and Compartments

The sample file has the following four classifications:

- `PUBLIC`
- `INTERNAL_USE_ONLY`
- `NEED_TO_KNOW`
- `REGISTERED`

In this model, `PUBLIC` is the sensitivity label for communications across the Internet. `INTERNAL_USE_ONLY` is the sensitivity label for communications within the company.

The sample file defines compartments to appear only in labels that have the `NEED_TO_KNOW` classification. The sample file also specifies that the default word `Comps` is changed to the word `Departments` in label-builder GUIs.

`NEED_TO_KNOW` compartments are:

- `ALL_DEPARTMENTS`

  The `ALL_DEPARTMENTS` compartment word gets turned on when all defined compartment bits are on and works as a toggle in a label builder.
- `EXECUTIVE_MGT_GROUP`
- `SALES`
- `FINANCE`
- `LEGAL`
- `MARKETING`

- HUMAN_RESOURCES
- ENGINEERING
- MANUFACTURING
- SYSTEM_ADMINISTRATION
- PROJECT_TEAM

  PROJECT_TEAM is hierarchically below both ENGINEERING and MARKETING. The hierarchy enables a user who is working at NEED_TO_KNOW ENGINEERING or at NEED_TO_KNOW MARKETING to read files with the NEED_TO_KNOW PROJECT_TEAM label. The user cannot write to files that have that label.

label_encodings.example File

This printed version is slightly different from the delivered version.

- CIPSO label warning is added.
- The word "proprietary" is removed to match the examples in this guide.
- Indications of CMW labels are removed.

```
* ident "@(#)label_encodings.example    5.13    06/08/04 SMI"
*
* Copyright 2006 Sun Microsystems, Inc.  All rights reserved.
* Use is subject to license terms.
*
*
* This version of the label_encodings file encodes the Sun
* confidential labels that are required by Sun's
* legal and information protection departments. The prefix
* COMPANY is omitted from the labels for
* brevity. This encodings includes some example department
* names that can be used for controlling access to information
* across department boundaries. Commercial sites with different
* requirements can copy this file and change the definitions to suit.

* This example shows how to specify labels that meet an actual
* site's legal information  protection requirements for
* labeling email and printer output. These labels can also
* be used to enforce mandatory access control checks that are
* based on user clearance labels, and on labels on files
* and directories.


VERSION= Sun Microsystems, Inc. Example Version - 5.13 06/08/04
```

```
*    WARNING:  If CIPSO Tag Type 1 network labels are to be used:
*
*        a) All CLASSIFICATIONS values must be less than or equal to 255.
*        b) All COMPARTMENTS bits must be less than or equal to 239.
*

CLASSIFICATIONS:

name= PUBLIC; sname= PUBLIC; value= 1;
name= INTERNAL_USE_ONLY; sname= INTERNAL; aname= INTERNAL; value= 4;
name= NEED_TO_KNOW; sname= NEED_TO_KNOW; aname= NEED_TO_KNOW; value= 5;
name= REGISTERED; sname= REGISTERED; aname= REGISTERED; value= 6;


INFORMATION LABELS:

WORDS:

name= SYSTEM_ADMINISTRATION; sname= SYSADM; compartments= 19;
minclass= NEED_TO_KNOW;
name= MANUFACTURING; sname= MANUFACTURING; compartments= 18;
minclass= NEED_TO_KNOW;
name= ENGINEERING; sname= ENG; compartments= 17 20;
minclass= NEED_TO_KNOW;
name= HUMAN_RESOURCES; sname= HR; compartments= 16;
minclass= NEED_TO_KNOW;
name= MARKETING; sname= MRKTG; compartments= 15 20;
minclass= NEED_TO_KNOW;
name= LEGAL; sname= LEGAL; compartments= 14;
minclass= NEED_TO_KNOW;
name= FINANCE; sname= FINANCE; compartments= 13;
minclass= NEED_TO_KNOW;
name= SALES; sname= SALES; compartments= 12;
minclass= NEED_TO_KNOW;
name= EXECUTIVE_MGMNT_GROUP; sname= EMG; compartments= 11;
minclass= NEED_TO_KNOW;
name= ALL_DEPARTMENTS; sname= ALL; compartments= 11-20;
minclass= NEED_TO_KNOW;
name= PROJECT_TEAM; sname= P_TEAM; compartments= 20;
minclass= NEED_TO_KNOW;

REQUIRED COMBINATIONS:

COMBINATION CONSTRAINTS:

SENSITIVITY LABELS:

WORDS:
```

```
name= ALL_DEPARTMENTS; sname= ALL; compartments= 11-20;
minclass= NEED_TO_KNOW;
name= EXECUTIVE_MGMNT_GROUP; sname= EMG; compartments= 11;
minclass= NEED_TO_KNOW;
name= SALES; sname= SALES; compartments= 12;
minclass= NEED_TO_KNOW;
name= FINANCE; sname= FINANCE; compartments= 13;
minclass= NEED_TO_KNOW;
name= LEGAL; sname= LEGAL; compartments= 14;
minclass= NEED_TO_KNOW;
name= MARKETING; sname= MRKTG; compartments= 15 20;
minclass= NEED_TO_KNOW;
name= HUMAN_RESOURCES; sname= HR; compartments= 16;
minclass= NEED_TO_KNOW;
name= ENGINEERING; sname= ENG; compartments= 17 20;
minclass= NEED_TO_KNOW;
name= MANUFACTURING; sname= MANUFACTURING; compartments= 18;
minclass= NEED_TO_KNOW;
name= SYSTEM_ADMINISTRATION; sname= SYSADM; compartments= 19;
minclass= NEED_TO_KNOW;
name= PROJECT_TEAM; sname= P_TEAM; compartments= 20;
minclass= NEED_TO_KNOW;

REQUIRED COMBINATIONS:

COMBINATION CONSTRAINTS:

CLEARANCES:

WORDS:

name= ALL_DEPARTMENTS; sname= ALL; compartments= 11-20;
minclass= NEED_TO_KNOW;
name= EXECUTIVE_MANAGEMENT_GROUP; sname= EMG; compartments= 11;
minclass= NEED_TO_KNOW;
name= SALES; sname= SALES; compartments= 12;
minclass= NEED_TO_KNOW;
name= FINANCE; sname= FINANCE; compartments= 13;
minclass= NEED_TO_KNOW;
name= LEGAL; sname= LEGAL; compartments= 14;
minclass= NEED_TO_KNOW;
name= MARKETING; sname= MRKTG; compartments= 15 20;
minclass= NEED_TO_KNOW;
name= HUMAN_RESOURCES; sname= HR; compartments= 16;
minclass= NEED_TO_KNOW;
name= ENGINEERING; sname= ENG; compartments= 17 20;
minclass= NEED_TO_KNOW;
```

```
name= MANUFACTURING; sname= MANUFACTURING; compartments= 18;
minclass= NEED_TO_KNOW;
name= SYSTEM_ADMINISTRATION; sname= SYSADM; compartments= 19;
minclass= NEED_TO_KNOW;
name= PROJECT_TEAM; sname= P_TEAM; compartments= 20;
minclass= NEED_TO_KNOW;

REQUIRED COMBINATIONS:

COMBINATION CONSTRAINTS:

CHANNELS:

WORDS:

name= DISTRIBUTE_ONLY_TO;       prefix;
name= EMPLOYEES (NON-DISCLOSURE AGREEMENT REQUIRED);
suffix;

name= EXECUTIVE_MANAGEMENT_GROUP;
prefix= DISTRIBUTE_ONLY_TO; compartments= 11;
suffix= EMPLOYEES (NON-DISCLOSURE AGREEMENT REQUIRED);
name= SALES; prefix= DISTRIBUTE_ONLY_TO; compartments= 12;
suffix= EMPLOYEES (NON-DISCLOSURE AGREEMENT REQUIRED);
name= FINANCE; prefix= DISTRIBUTE_ONLY_TO; compartments= 13;
suffix= EMPLOYEES (NON-DISCLOSURE AGREEMENT REQUIRED);
name= LEGAL; prefix= DISTRIBUTE_ONLY_TO; compartments= 14;
suffix= EMPLOYEES (NON-DISCLOSURE AGREEMENT REQUIRED);
name= MARKETING; prefix= DISTRIBUTE_ONLY_TO;
compartments= 15 20;
suffix= EMPLOYEES (NON-DISCLOSURE AGREEMENT REQUIRED);
name= HUMAN_RESOURCES; prefix= DISTRIBUTE_ONLY_TO;
compartments= 16;
suffix= EMPLOYEES (NON-DISCLOSURE AGREEMENT REQUIRED);
name= ENGINEERING; prefix= DISTRIBUTE_ONLY_TO;
compartments= 17 20;
suffix= EMPLOYEES (NON-DISCLOSURE AGREEMENT REQUIRED);
name= MANUFACTURING; prefix= DISTRIBUTE_ONLY_TO;
compartments= 18;
suffix= EMPLOYEES (NON-DISCLOSURE AGREEMENT REQUIRED);
name= SYSTEM_ADMINISTRATION; prefix= DISTRIBUTE_ONLY_TO;
compartments= 19;
suffix= EMPLOYEES (NON-DISCLOSURE AGREEMENT REQUIRED);
name= PROJECT_TEAM; prefix= DISTRIBUTE_ONLY_TO; compartments= 20;
suffix= EMPLOYEES (NON-DISCLOSURE AGREEMENT REQUIRED);

PRINTER BANNERS:
```

```
WORDS:

name= CONFIDENTIAL:;       prefix;

name= ALL_DEPARTMENTS;
prefix= CONFIDENTIAL:;
compartments= 11-20;
name= EXECUTIVE_MANAGEMENT_GROUP;
prefix= CONFIDENTIAL:;
compartments= 11;
name= SALES; prefix= CONFIDENTIAL:;
compartments= 12;
name= FINANCE; prefix= CONFIDENTIAL:;
compartments= 13;
name= LEGAL; prefix= CONFIDENTIAL:;
compartments= 14;
name= MARKETING; prefix= CONFIDENTIAL:;
compartments= 15 20;
name= HUMAN_RESOURCES;
prefix= CONFIDENTIAL:;
compartments= 16;
name= ENGINEERING;
prefix= CONFIDENTIAL:;
compartments= 17 20;
name= MANUFACTURING;
prefix= CONFIDENTIAL:;
compartments= 18;
name= SYSTEM_ADMINISTRATION;
prefix= CONFIDENTIAL:;
compartments= 19;
name= PROJECT_TEAM;
prefix= CONFIDENTIAL:;
compartments= 20;

ACCREDITATION RANGE:

classification= PUBLIC; only valid compartment combinations:

PUBLIC

classification= INTERNAL_USE_ONLY; only valid compartment combinations:

INTERNAL

classification= NEED_TO_KNOW; all compartment combinations valid;

classification= REGISTERED; only valid compartment combinations:
```

```
REGISTERED


minimum clearance= PUBLIC;
minimum sensitivity label= PUBLIC;
minimum protect as classification= PUBLIC;

*
* Local site definitions and locally configurable options.
*

LOCAL DEFINITIONS:


Classification Name= Classification;
Compartments Name= Departments;

Default User Sensitivity Label= public;
Default User Clearance= public;

COLOR NAMES:

     label= Admin_Low;       color= #bdbdbd;

     label= PUBLIC;               color= green;
     label= INTERNAL_USE_ONLY;    color= yellow;
     label= NEED_TO_KNOW;         color= blue;
     label= NEED_TO_KNOW EMG;     color= #7FA9EB;
     label= NEED_TO_KNOW SALES;   color= #87CEFF;
     label= NEED_TO_KNOW FINANCE;  color= #00BFFF;
     label= NEED_TO_KNOW LEGAL;    color= #7885D0;
     label= NEED_TO_KNOW MRKTG;    color= #7A67CD;
     label= NEED_TO_KNOW HR;       color= #7F7FFF;
     label= NEED_TO_KNOW ENG;      color= #007FFF;
     label= NEED_TO_KNOW MANUFACTURING;  color= #0000BF;
     label= NEED_TO_KNOW PROJECT_TEAM;   color= #9E7FFF;
     label= NEED_TO_KNOW SYSADM;   color= #5B85D0;
     label= NEED_TO_KNOW ALL;      color= #4D658D;
     label= REGISTERED;            color= red;

     label= Admin_High;      color= #636363;

*
* End of local site definitions
*
```

Index

D

M

N

P

R

S

T

U

V

W