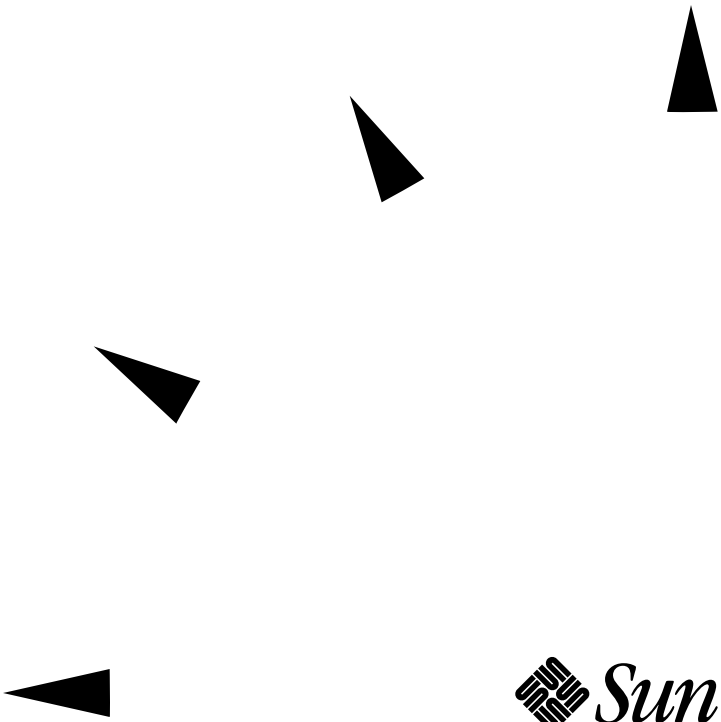
Trusted Solaris Label Administration



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

Part No: 805-8011-10
Revision A, July 1997

Sun microsystems

THE NETWORK IS THE COMPUTER™

Please
Recycle

Adobe PostScript

Contents

Figures

Tables

Preface

Labels, clearances, and handling caveats are used to protect information in the Trusted Solaris environment. The components of labels, clearances, and handling caveats are specified in a file called `label_encodings(4TSOL)`. This *Trusted Solaris Label Administration* manual provides needed background and describes how to go about editing, checking, and installing the `label_encodings` file.

See the *Trusted Solaris Administrator's Procedures* manual for how administrators assign the site's labels to files and directories and assign clearances and minimum labels to users.

Who Should Use This Book

This book is for security administrators whose task is to administer the site's labels.

Note – Even though a site may choose to configure the Trusted Solaris environment so that it looks like a Solaris environment from the user's point of view—with no visible labels and no apparent mandatory access control decisions being made—labels are always being used, and mandatory access control checks are always being made. Therefore, even with a "no-labels" configuration, the site's administrator needs to understand labels and to configure a single label in the `label_encodings` file, as described in this manual.

Before You Read This Book

- **Understand Solaris 2.x administration, CDE, Solstice, and NIS+**
  Administrators of Trusted Solaris must understand how to work within and administer the Solaris 2.x operating environment, which is the operating system upon which Trusted Solaris is based, and must also understand how to use and administer the Common Desktop Environment (CDE) window system, SolsticeAdminsuite system administration tools, and the NIS+ system for administering files. The necessary level of knowledge may be acquired through:

  - Training
    Sun Service provides training classes.
  - Documentation
    This manual, like all of the Trusted Solaris documentation, assumes you have access to and understanding of the principles described in the Solaris 2.x and CDE user's and administrator's document sets, the NIS+ administrator's documents, the documentation for Solstice AdminSuite, and the Solaris reference manual.
  - Experience

- **Read and understand the basic concepts and procedures described in the Trusted Solaris user document set**
  Administrators should understand how to work in the Trusted Solaris environment as a normal non-administrative user.

- **Read and understand the administrative concepts described in the Trusted Solaris administrator's overview manual**

- **Understand how administrative tasks are divided among roles at your site**
  This manual describes tasks assigned to the security administrator role in the default configuration. Some sites may assign the label encodings tasks to another site-specific role.

- **Understand the security requirements of your agency or organization.**

Note – This manual supplements the information in the DIA label encodings manual, *Compartmented Mode Workstation Labeling: Encodings Format*.

How This Book Is Organized

- **Chapter 1, “Introduction to Trusted Solaris Label Encodings”**

  Provides the needed labels-related concepts and planning steps for the security administrator who needs to get the site’s `label_encodings` file ready for installation.

- **Chapter 2, “Creating or Editing the Encodings File”**

  Describes how to create the site-specific version of the `label_encodings` file, which is installed after Trusted Solaris installation is complete.

- **Chapter 3, “Specifying Labels and Handling Guidelines for Printer Output”**

  Provides the needed information for understanding which labels are printed at the top and bottom of printer output, and which labels and text are printed on banner and trailer pages that accompany each print job. Also describes how to specify the fields printed on printer output.

- **Chapter 4, “Modifying Sun’s Extensions in the Local Definitions Section”**

  Describes how to define the flags, color names and other values in the LOCAL DEFINITIONS section of the Trusted Solaris label_encodings file.

- **Chapter 5, “Central Administration of Labels-related Files”**
  Describes how the security administrator can set up a boot server so the `label_encodings` and labels-related Trusted Solaris kernel switch settings that are created on the NIS+ master can be distributed to each machine as it is installed. Also describes how to change these files after the system is running and how to distribute the changes to all hosts in the distributed system.

- **Chapter 6, “Example: Planning an Organization’s Labels”**
  Gives a step by step example of how a site that needs labels to protect its intellectual property analyzes its requirements and creates a simple encodings file, with the resulting file in Appendix A, “Example: Simple Label Encodings File.”

- **Appendix A, “Example: Simple Label Encodings File”**
  An example of a `label_encodings` file at a site that plans to run without ILs.

Related Books

Prerequisite knowledge is contained in:

- *Trusted Solaris User's Guide*

This book is part of the Trusted Solaris 2.5 administrator's document set, which also includes:

- *Trusted Solaris Administration Overview*
  See especially, "Understanding Labels" on page 4 of Chapter 1, "Introduction to Administration."
- *Trusted Solaris Installation and Configuration*
- *Trusted Solaris Administrator's Procedures*
- *Trusted Solaris Audit Administration*
- *Trusted Solaris Developer's Guide*
- *Trusted Solaris 2.5 Transition Guide*
- *Compartmented Mode Workstation Labeling: Encodings Format*: *Encodings Format DIA document DDS-2600-6216-93 (shipped as part of the Trusted Solaris administrator's document set)*

What Typographic Changes and Symbols Mean

The following table describes the typographic changes used in this book.

Table P-1 Typographic Conventions

Type Style	Meaning	Example
`Filename, command,` or `code example`	The names of commands, files, and directories; on-screen computer output	Edit your `.login` file. Use `ls -a` to list all files. machine_name% You have mail.
`User Type`	What you type, contrasted with on-screen computer output	*`hostname`*`% su` `Password:`
Argument	Used in command line examples: replace with an appropriate name or value	To delete a file, type `rm` *filename.*
Title or *Emphasis*	Book titles, new words or terms, or words to be emphasized	Read Chapter 6 in *User's Guide.* These are called *class* options. You *must* be root to do this.

Which Trusted Solaris Prompts Go With Which Shells and User Types

Shell	Prompt
C shell prompt	*machine_name*%
Bourne shell and Korn shell prompt	$
Profile Shell prompt	$
root prompt	#
PROM mode prompt	>

Introduction to Trusted Solaris Label Encodings 1

Mandatory access control, a feature that is always enabled in the Trusted Solaris environment, relies on certain types of labels that must be defined by each site. The components of all types of labels are specified by each site's security administrator in a site-specific `label_encodings(4TSOL)` file. A placeholder version of the `label_encodings` file is initially installed on the NIS+ master based on answers given to related prompts during the Trusted Solaris installation process. (See "System-wide Label Configuration Choices During Installation" on page 29.) In almost all cases, the install team replaces the installed `label_encodings` file with its own local version when configuring the system after installation completes. This chapter prepares the security administrator to create the `label_encodings` file for hand off to the install team.

This chapter covers the topics that the security administrator needs to understand before encoding labels and gives steps for planning the encodings file. This chapter assumes you have read and comprehend "Understanding Labels" on page 4 of Chapter 1, "Introduction to Administration," in the *Trusted Solaris Administration Overview*, but reviews and expands the definitions for the needed terms in the context of the task at hand.

1

Note – An organization running the Trusted Solaris operating system may choose to configure the system so that labels are not displayed, making the look and feel of working in the Trusted Solaris environment similar to that of the Solaris environment. However, a minimum of three labels are always used and mandatory access control decisions are always being made behind the scenes, so even with this kind of a configuration, administrators must understand labels and modify the `label_encodings` file. If you plan to run without visible labels read all of this chapter and the next, and especially see "Running Without Labels" on page 51.

Topics in This Chapter

This chapter includes these topics:

When Using Either a Government-furnished or Already-Existing Labels File

Some organizations use a label encodings file either supplied by a government agency or obtained by some other means. The security administrator at these sites may modify the Sun extensions (in the LOCAL DEFINITIONS: section in the Trusted Solaris default file) and must append the extensions to the site‘s supplied label encodings file before having it installed. The Sun extensions allow you to set various label translation options, and to assign colors to labels, Chapter 4, “Modifying Sun’s Extensions in the Local Definitions Section,” describes how to append the Sun extensions to your file and modify the extensions for your site.

1

If Your Site Does Not Already Have a Labels File

At most organizations, the site's own version of the `label_encodings` file is created by the site's security administrator.

Appendix A, "Example: Simple Label Encodings File,"shows an example `label_encodings` file that is based on the analysis of one commercial site's labeling requirements described in Chapter 6, "Example: Planning an Organization's Labels."

After Installation

The `label_encodings.simple` file is on each installed system under `/etc/security/tsol`, and it can either be modified or used as is. The introduction to Appendix A describes the labels and compartments it contains.

Before Installation

To prepare a `label_encodings` file in advance, the security administrator can manually copy the example in Appendix A and make the site's modifications in the copy. Alternately, a label_encodings file can be created from scratch using the examples in this manual and in the DIA document referred to in the next section.

Creating Labels With Complex Relationships

This manual does not show how to encode the complex relationships between classifications, inverse, and hierarchical words that are needed in some installations. For that level of detail and for further reference, see the *Compartmented Mode Workstation Labeling: Encodings Format:* Defense Intelligence Agency document [DDS-2600-6216-93], Sun part number 805-8012-10, which is included in the Trusted Solaris administrator's document set.

Review of Label-Encodings Related Concepts

The *Trusted Solaris User Guide* and the *Trusted Solaris Administration Overview* describe the distinctions between types of labels and how labels are compared when access control decisions are being made. The chapters in Part 1 — *Procedures Common to All Tasks and Administrative Roles* in the *Trusted Solaris Administrator's Procedures* manual prepares the security administrator to assume the security administrator role, which is given the applications, actions, privileges, and authorizations it needs to set up labels along with the other tasks involved in security administration.

The following definitions review some of the basic label concepts in terms that are directly related to understanding how to encode the labels at a site. These facts are needed when making decisions about how sensitivity labels and information labels are going to be configured for a site. For more information about these and other related terms you may not recognize, see also the DEFINITIONS in the `Intro(1TSOL)` man page.

How Labels Are Used

Because in UNIX systems just about everything (including a spreadsheet, a printer, a letter, a chapter of a book, or a mail message) is handled as a file, and because files are stored in directories—the user must access files and directories to do just about anything. (Files are called documents and directories are called folders in the window system.) Labels are assigned to all users and administrators and to all files and directories, and the labels are compared when access decisions are being made by the mandatory access control mechanism.

Clearance and Minimum Label

A clearance label and a minimum label are assigned to user and role accounts when the security aspects of the account are configured by the security administrator. The clearance establishes the upper bound of the set of labels at which the account may work, while the minimum label establishes the lower bound. There are two types of clearance, the account clearance and the session clearance. When an employee logs into the system, he or she sets a session clearance for the duration of the login session, and that clearance must be within the account's clearance.

Account Label Range

The set of labels at which a user or role can work is referred to as the *account label range*. The upper bound of the account label range is the account's clearance and the lower bound is the account's minimum label

Session Clearance

The session clearance limits the range of labels at which processes can be run on the behalf of the normal user between any one login and logout. Roles have a session clearance set equal to their account clearance.

Label Ranges on Things Being Accessed

Label ranges are assigned to the following:

- All hosts and networks with which communications are allowed
- File systems
- Allocatable devices: tape drives, floppy drives, CDROM drives, and audio devices
- Other devices that are not allocatable: printers and workstations (controlled through a label range set on the framebuffer)

What Labels Ranges Do

Label ranges set limits on:

- 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 within file systems
- The labels at which users can use allocatable devices, which therefore determine the labels of the files and directories that may be written to storage media in these devices.
- The labels at which users can send jobs to printers
- The labels at which users can access workstations

Labels are also used in deciding the actual level of sensitivity of information and how information should be handled. In addition, labels are automatically assigned to email messages and printed on printer output.

Types of Labels

Besides the clearance labels mentioned already, there are two other types of labels, sensitivity labels and information labels. Information labels and sensitivity labels are both made up of two categories of components: *classifications* and optional *words*.

Classifications

The classification is the hierarchical portion of a sensitivity label, information label, or clearance, each of which has one classification. In a sensitivity label or information label of a file or directory, a classification indicates a relative level of protection based on the sensitivity of the information contained in the file or directory. In a clearance assigned to a user and to processes that execute applications and commands on behalf of the user, a classification indicates a level of trust.

The total number of possible classifications is 256. The value 0 is reserved for ADMIN_LOW.

Note – Because each site must have at least one sensitivity label, information label, and clearance defined, you must define at least one classification.

Compartments

A compartment is one of the optional types of *words* that may appear in a sensitivity label, information label, or clearance. (Compartments are called categories in some other trusted systems.) A compartment represents an area of interest or work group associated with the label that contains the compartment and with the files that are assigned the labels and the individuals that work with them.

Besides its classification field, each label has a 256 bit field available for compartments, as shown in Table 1-1 on page 8. To set up hierarchies between compartments requires that some compartments use more than one

compartment bit. Therefore, there may be up to 256 or fewer compartments at a site, depending on whether individual compartments make use of more than one bit.

Table 1-1 Bits Available for Classification and Compartment Components

Classification Field	Compartments Field
32767 bits	256 bits

As shown in Table 1-2, information labels have an additional 256 bits available for markings. To set up hierarchies between markings requires that some markings use more than one marking bit. Therefore, there may be up to 256 or fewer markings at a site, depending on whether individual markings make use of more than one bit.

Table 1-2 Bits Available for Information Label Components

Classification Field	Compartments Field	Markings Field
32767 bits	256 bits	256 bits

Sensitivity Labels Uses and Format

The sensitivity label of a file or directory is a *fixed* security label. A newly-created file or directory is assigned the sensitivity label of the process that creates it, which is usually determined by the sensitivity label of the workspace where the process is started, and the sensitivity label stays the same unless it is changed by an explicit action taken by its owner or an administrator or other user who has the needed authorization. (The authorizations are described in “Authorizations for Upgrading and Downgrading Sensitivity Labels” on page 9.)

Each sensitivity label is made up of a classification and zero or more compartments, as shown in Table 1-3.

Table 1-3 Components of a Sensitivity Label

Classification	Compartments
`name`	`word1[, word2, ..., word`*N*`]`

The example in Table 1-4 shows that the sensitivity label INTERNAL_USE_ONLY consists only of the classification INTERNAL_USE_ONLY with no compartments, while the sensitivity label NEED_TO_KNOW ENGINEERING SALES is made up of a NEED_TO_KNOW classification and the compartments ENGINEERING and SALES.

Table 1-4 Components of Example Sensitivity Labels

Classification	Compartments
`INTERNAL USE ONLY`	`none`
`NEED TO KNOW`	`ENGINEERING, SALES`

Authorizations for Upgrading and Downgrading Sensitivity Labels

A sensitivity label can only be changed by a user or an administrator who has the appropriate authorization in one of his or her profiles. The authorization to change a sensitivity label to one that dominates it is called the *upgrade file sensitivity label* authorization. The authorization to change a sensitivity label to one that it dominates is called the *downgrade file sensitivity label* authorization. See also `auth_desc(4TSOL)`.

How Computer Users May Be Restricted to a Single Sensitivity Label

If a system is configured to run with only a single sensitivity label, all non-administrative user accounts on that system are restricted to work at that single sensitivity label. In such systems, the clearance for every user's account would necessarily be set to be equal to the account's minimum sensitivity label.

In systems running with multiple sensitivity labels, any account may be restricted to work at a single sensitivity label if the security administrator sets the account's clearance equal to the minimum sensitivity label.

When the security administrator has configured an account with a account label range that includes multiple sensitivity labels, the user can voluntarily restrict a working session to a single sensitivity label, which is explained under "How Accounts With Multiple SLs Specify the SLs for Each Session."

How Accounts With Multiple SLs Specify the SLs for Each Session

Directly after a user logs in and starts a session on a Trusted Solaris host, if the account is set up to use multiple labels, the user can specify which sensitivity labels are available during the session by doing one of the following:

- Restrict the session to a single sensitivity label
- Set the session clearance to be the same as the user's own clearance
- Set a session clearance lower than the user's own clearance

The selected single-label or session clearance is in effect throughout the session, from login until logout. During a session, the user may work at any sensitivity label that is dominated by the session clearance and that dominates the user's minimum label (as long as the sensitivity label is a valid label defined in the `label_encodings` file).

Labeled Workspaces

The Trusted Solaris windowing system is a labels-aware version of the CDE window system. CDE *workspaces* play an important part in allowing users to potentially work at multiple sensitivity labels during a single session. When the employee logs in for the first time, the first workspace that comes up is assigned the employee's minimum sensitivity label. (Buttons for three additional workspaces are created at the same minimum sensitivity label in the workspace switch portion of the Front Panel.) The employee can bring up additional workspaces and change the sensitivity labels on any workspaces, but he or she cannot set the sensitivity label on a workspace to be higher than the session clearance—which means that the employee cannot do any work at any sensitivity label higher than the session clearance. The sensitivity label of the workspace is assigned to each new window tool that is created in that workspace to execute an application on the user's behalf.

Any user allowed a multilevel session may relabel any of the workspaces. Any user may specify which workspaces and applications are launched at future logins by means of the Startup dialog box in the Style Manager available on the Front Panel. Because the first workspace that comes up after second and subsequent logins may be specified by the user, the sensitivity label of the first workspace that comes up after any login after the initial login can be at any sensitivity label the user chooses (within the account's label range). The administrative role workspaces are an exception, because administrative role workspaces are destroyed at logout.

How Sensitivity Labels are Used in Access Control Decisions

Sensitivity labels are the only types of labels that are compared when access control decisions are made. The sensitivity label of a window tool is compared to the sensitivity label of anything that the application tries to access. For example the sensitivity label of a text editor is compared to the sensitivity label of a file that the text editor is trying to open for editing. The sensitivity labels are compared for *dominance*. For more about the mandatory access control rules that are enforced when sensitivity labels are compared, see the DEFINITIONS section in `Intro(1TSOL)`.

Within the window system, the sensitivity label of the process generally must be to equal the sensitivity label of the thing being accessed or access is not allowed. (A notable exception to the read equal / write equal rule include email readers, for which the write up / read down (wurd) rule applies).[1]

Example Mandatory Access Control Decision

If an employee brings up a text editor while in a workspace with a sensitivity label of PUBLIC, the text editor comes up with a sensitivity label of PUBLIC. The process executing the text editor is assigned the same sensitivity label as the workspace, in our example, the label of PUBLIC.

1. See the documents mentioned earlier for details.

Figure 1-1 shows a comparison between two sensitivity labels used in making an access control decision. The user is working in a workspace labeled with the sensitivity label INTERNAL_USE_ONLY. When he brings up a text editor, the sensitivity label of the process running the text editor is automatically set to be equal to the sensitivity label of his current workspace. When he uses the text editor to attempt to open a file for editing, the sensitivity label of the text editor is compared to the sensitivity label of the file. In the example, because the two sensitivity labels are equal, access is allowed.

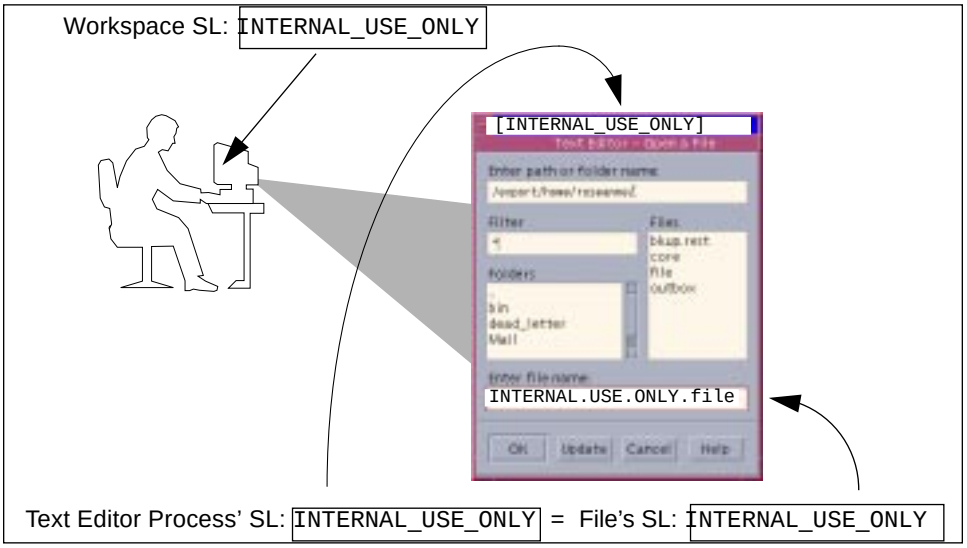


Figure 1-1 Comparing the SL of a Text Editor with the SL of the File to be Edited

Label Dominance

When any type of label (sensitivity label, information label, or clearance) has a security level equal to or greater than the security level of another label to which it is being compared, the first label is said to *dominate* the second. The classification of the dominant label must be *equal to* or *higher than* the classification of the second label, and the dominant label must *include all the words* (compartments and markings, if present) in the other label.

Two equal labels dominate each other. A second kind of dominance is called *strict dominance*. One label *strictly dominates* another label, when the first label has a security level *greater than* the security level of another label to which it is being compared. Strict dominance is dominance without equality. The

classification of the first label must be higher than that of the second label and the first label must contain all the compartments in the second label or, if the classifications of both labels are the same, the first label must contain all the compartments in the second label plus one or more additional compartments for the first label to strictly dominate the second.

Label Translation

Label translation occurs whenever programs manipulate label strings. For example, when a program such as `getlabel` gets the label of a file, before the label can display to the user, the binary representation of the label must be translated into human-readable ASCII form. The Trusted Solaris system permits label translations only if the calling process's sensitivity label dominates the label to be translated. If a process attempts to translate a label that the process's SL does not dominate, the translation is disallowed. The `sys_trans_label` privilege overrides this restriction. For example, when a program has the `sys_trans_label` privilege in its effective privilege set, the program can translate labels that dominate its process label.

Information Labels (ILs) Format and Uses

Some organizations make use of a type of label that advises about the actual sensitivity of the information contained in files and directories and which also may be used to determine how to distribute or store information. In the United Kingdom, these types of label are called advisory labels; in the United States, they are called *information labels*.

Like the sensitivity label, the information label is made up of one classification and zero or more compartments. In addition, the information label also may include one or more words called markings that indicate how the information should be handled. See Table 1-5 for the format of components.

Table 1-5 Components of an Information Label

Classification	Compartments	Markings
`name`	`word1[,word2,...,word`*`N`*`]`	`word1[,word2,...,word`*`N`*`]`

As shown in Table 1-6, the information label INTERNAL_USE_ONLY RELEASE SUN FEDERAL consists of the classification INTERNAL_USE_ONLY with no compartments and with the markings

RELEASE SUN FEDERAL, and the information label NEED TO KNOW ENGINEERING SALES RELEASE ALL USA consists of a NEED_TO_KNOW classification, the compartments ENGINEERING and SALES, and the marking RELEASE ALL USA. (The marking RELEASE SUN FEDERAL indicates that the information should only be released to the Sun Federal Division and the marking RELEASE ALL USA indicates that the information can be released to all divisions of the company that are within the USA.)

Table 1-6 Components of Example Information Labels

Classification	Compartments	Marking
INTERNAL USE ONLY	none	RELEASE SUN FEDERAL
NEED TO KNOW	ENGINEERING SALES	RELEASE ALL USA

CMW Labels

Each file, directory, and process in the Trusted Solaris system is labeled with a CMW label made up of an information label (IL) and a sensitivity label (SL).

Rules for the Display and Entering of CMW Labels

Note – If you need to enter labels on the command line, also see "Rules for the Display and Entering of Labels" in `Intro(1MTSOL)`.

The Trusted Solaris system always displays labels in uppercase. Users may enter labels in any combination of uppercase and lowercase. Whether the CMW label is being displayed by the system, in a window frame, for example, or it is being entered by users or roles, each CMW label has this format:

```
INFORMATION LABEL [ SL ]
```

- **In the CMW label, the full name of the information label is shown to the left of the short name of the sensitivity label, which appears in brackets.**
- **The label encodings require that each type of label has a classification and that both a full *name* (called *name*=) and a *short name* (called *sname*=) are defined for each classification.**

- **Each types of label may have other optional *words*, which are required only to have a full name defined, but may also have an optional short name defined.**
- **In the information label component, the full name of the classification and of any optional words is displayed. In the sensitivity label component, the short names of the classification and the short names of any optional words (if short names have been specified) are displayed within brackets.**

Examples of CMW Labels

For example, the following CMW label includes a simple information label and sensitivity label, each of which only contains a classification with no words. The information label of PUBLIC displays with its long name and the sensitivity label of INTERNAL_USE_ONLY displays with its short name of IUO:

```
PUBLIC [ IUO ]
```

For another example, the following CMW label includes an information label and a sensitivity label that both have the same classification NEED_TO_KNOW (with a sname defined as NTK) and the compartment word HUMAN_RESOURCES (that has a sname defined as HR). The information label also has another type of word called a release marking. The information label of displays with its long name and the sensitivity label displays with its short name:

```
NEED_TO_KNOW HUMAN_RESOURCES REL USA [ NTK HR]
```

Visibility of CMW Label Components

- **Every file, directory, and process always has a CMW label.**
- **Security administrators have the option to configure the system and the user's account so that either the information label or the sensitivity label portions of the CMW label are not visible or that neither portion is visible.**

Depending on how the system is configured and how the user is set up, a user may see information labels only, sensitivity labels only, the complete CMW label, or no labels at all in the top frame of each window and in the trusted stripe, among other places in the user's workspace. If information labels alone

are configured to display, they display alone. If sensitivity labels alone are configured to display, they display within brackets, in the long form (within the window system).

When both the information label and the sensitivity label are displayed, the full name of the classification portion of the information label is shown, while the short name of the classification portion of the sensitivity label is shown.

For example, with the `PUBLIC [ IUO ]` CMW label, things could be set up so that the employee would be able to see:

- The entire label `PUBLIC [ IUO ]`,
- The sensitivity label portion `[ IUO ]` alone,
- The information label portion `PUBLIC`, or
- Neither portion.

Avoiding Abbreviations and Acronyms in Labels

Some sites want easy-to-understand names for sensitivity labels and want to avoid abbreviations and acronyms. At sites that want to see the full names of labels, the security administrator may specify the short name of the classifications and words equal to their long names. Setting of the long name of classifications to equal the short names would be especially convenient at sites that either do not have information labels enabled or that hide information labels. The CMW label then would display with the full sensitivity label name within brackets. So, for example, because the sensitivity label INTERNAL_USE_ONLY consists only of a classification, to have the full name appear when the sensitivity label stands alone, the security administrator would define the short name identical to the long name and the sensitivity label would appear as [INTERNAL_USE_ONLY].

Initial Information Label

The information label of an empty file or directory is the lowest administrative label: ADMIN_LOW.

Note – The section “Administrative Labels” on page 20 gives more details about administrative labels. Because some sites want to hide the names of administrative labels from non-administrative employees, whether or not any

user sees the actual word ADMIN_LOW is determined by how the security administrator sets the *label view*. For how this is set, see “The Hierarchy of Label View Settings” on page 24.

Input Information Label Setting

Users can set an input information label (IIL) for any window tools through the Trusted Path menu, The IIL is the information label that is applied to all information entered from the keyboard to the window tool.

Information Label Floating

The information label floats in a window’s label and subsequently floats in the CMW label of a file or directory when the file is saved or the directory is written into, only in these two cases:

- If information with a higher information label is written into a file or directory from another labeled source or
- If a file being edited from the keyboard has the IIL set higher than current information label.

The information label never floats to be higher than the sensitivity label associated with the file or directory or window process that contains the information. The floating of information labels is configurable.

When Deciding Whether to Use Information Labels

The requirement for information labels was introduced by the Defense Intelligence Agency (DIA) for CMW systems. For sites that require them, information labels are used to identify the actual sensitivity of the information itself rather than the sensitivity that has been assigned to the container of the information. This means that information label applies to information while the sensitivity label applies to the files, directories, or other objects that hold the information.

Information labels can be useful for customers that want to control how information is distributed, because an information label can contain site-specific code words and warnings on how the information should be handled,

and it can provide guidance on the actual sensitivity of the information. This guidance can be used by authorized users when deciding whether to downgrade the sensitivity label. Following are some examples:

- Every email message sent from a Trusted Solaris host is automatically labeled with the information label that applies to the message.

Note – If information labels are not configured for the system, then the X-Sender-Information-Label does not get put into email messages.

Figure 1-2 shows an information label of NEED TO KNOW ENGINEERING RELEASE SUN FEDERAL that was automatically added to an email message.

```
From: roseanne@trusted(Roseanne Sullivan
To: shark_notes@odgers
Subject: IL floating on label translations
X-Sender-Information-Label: NEED TO KNOW ENGINEERING RELEASE SUN FEDERAL
```

Information Label

Figure 1-2 An X-Sender-Information-Label Added to a Mail Header

- Whenever an authorized user exports information to a tape or floppy, the device allocation system supplies an information label along with the sensitivity label. The user is prompted to write these labels on a physical label and affix it to the archive media.

  Figure 1-3 shows the user being prompted by the device allocation subsystem to write the information label of PUBLIC along with the sensitivity label of NEED_TO_KNOW_LEGAL on a label on an archive tape. The information label may be used by the appropriate person in deciding whether the sensitivity label of the archive should be downgraded.

```
trusted% deallocate st0
Please remove the tape

Please make sure tape is labeled PUBLIC {NEED_TO_KNOW LEGAL]
```

Information Label

Figure 1-3 The Information Label Supplied for Physically Labeling Exported Information

- The information label is printed on the top and bottom of every body page of every job sent to the printer and is displayed on banner and trailer pages for every print job.

  Figure 1-4 on page 19 shows an information label of `NEED_TO_KNOW EMG` on a printer banner page.

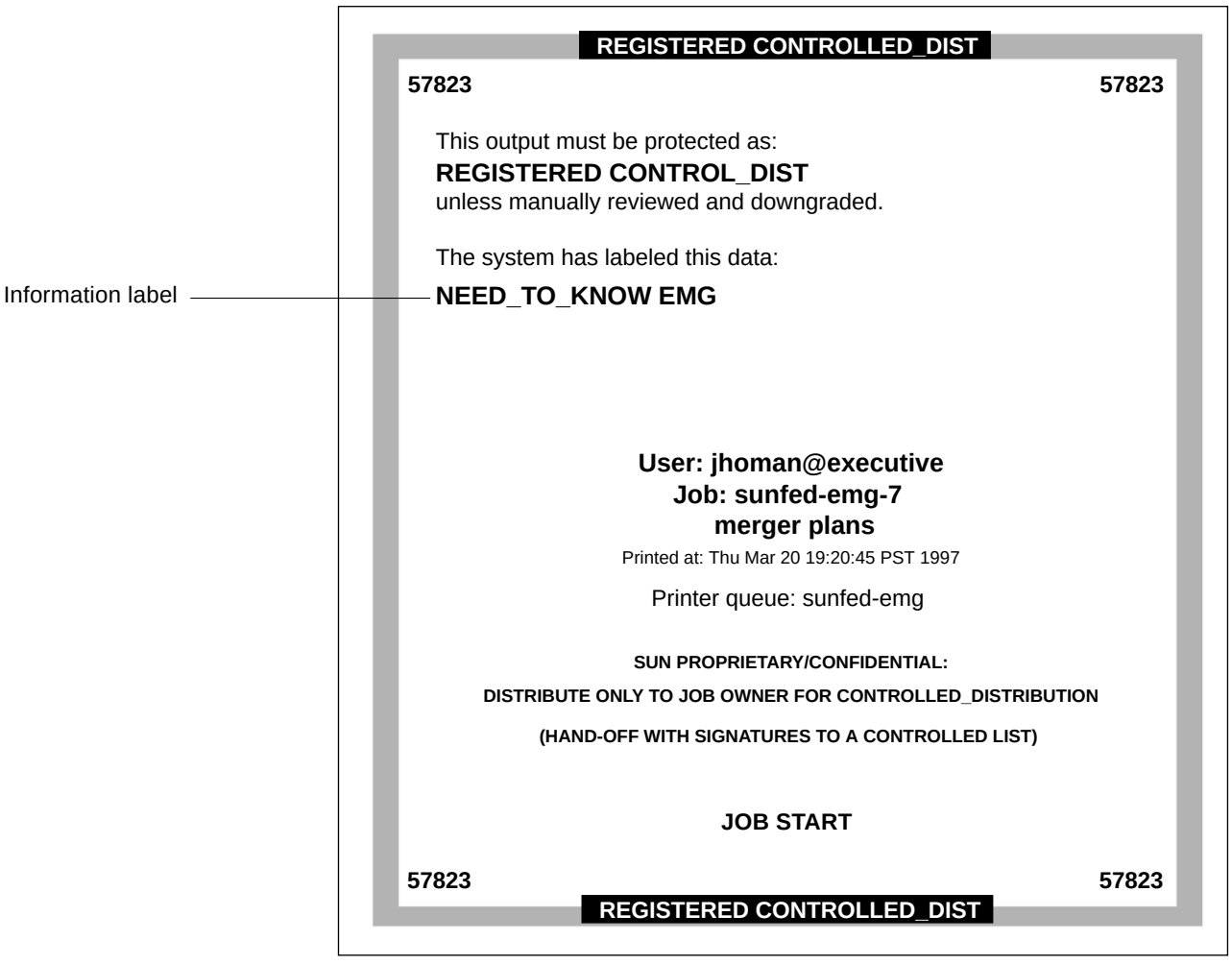


Figure 1-4 Information Label on the Printer Banner Page

ILs Used in Decide Whether to Downgrade a File's Labels

The information label provides a guide to the real sensitivity of the information on the tape or floppy, which may be used in deciding whether to manually downgrade the sensitivity label. (As mentioned earlier, users need authorizations to upgrade or downgrade a sensitivity label). A user might choose to downgrade the sensitivity label of a file if the information label (which reflects the actual security label of the information in the file) is below the file's sensitivity label of the file. Figure 1-5 shows a file called `project.status` whose information label of `PUBLIC` is lower than its sensitivity label of `NEED TO KNOW LEGAL`.

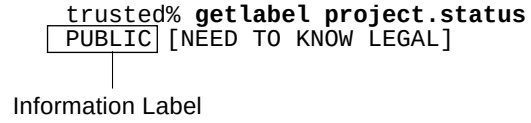


Figure 1-5 A File's Information Label Lower Than its Sensitivity Label

Issues About the Use of Information Labels

When considering whether to use information labels, it is important to realize that *user understanding and compliance are required to keep information labels accurate, while sensitivity labels are automatically maintained*. For an example of how user compliance is required, the information label will not float on a new file being created by entering text from the keyboard *unless* the user sets an IIL that is higher than the initial information label of ADMIN_LOW. In addition, the information label may be changed on a file by its owner after the file is created. In either case, the information label does not float in a meaningful way unless the user sets an IIL that accurately reflects the security level of the information being entered.

Administrative Labels

Two default administrative labels are always defined: ADMIN_LOW and ADMIN_HIGH. The two administrative labels are always automatically defined for all types of labels (sensitivity labels, information labels, and clearances).ADMIN_LOW is the lowest label in the system with a classification value of 0 and no compartments or markings, while ADMIN_HIGH is the highest label in the system with the classification value of 32767. As the highest

label in the system, the ADMIN_HIGH sensitivity label and the clearance have all 256 compartment bits set to 1. The ADMIN_HIGH information label has all 256 compartment bits and marking bits turned on. The ADMIN_LOW label is dominated by every other label and the ADMIN_HIGH label dominates all other labels.

As described under "How Labels Are Configured" on page 29, the Trusted Solaris system may be set up so that no one except administrators sees *any* labels. Or, as described under "Issues About the Names of Administrative Labels" on page 21, an organization may *change* the ASCII names of administrative labels (while leaving the binary values the same) or it may *hide* the names of administrative labels from all non-administrative employees (while substituting the names of other labels).

System files and commonly-available executables are assigned an ADMIN_LOW sensitivity label. Any files that contain data that should not be viewed by normal users, such as system log file are maintained at ADMIN_HIGH. Besides being used to protect system files, administrative labels are used in information labels and in the clearances and minimum labels of the default administrative roles.

Issues About the Names of Administrative Labels

The names of administrative labels do not *need* to be changed, but a site's security administrator may choose to do the following:

- Specify alternate names for administrative labels or
- Hide the names of administrative labels from non-administrative employees

Changing the Administrative Labels' Names

An option in the LOCAL DEFINITIONS section of the `label_encodings` file allows the security administrator to change the names of the administrative labels. The site's security administrator may activate and possibly edit the two commented-out lines shown in Figure 1-6 to substitute alternative ASCII names for the administrative labels.

```
LOCAL DEFINITIONS:

*
*       The names for the administrative high and low name are set to
*       site_high and site_low respectively by the example commands below.
*
*       NOTE:   Use of these options could lead to interoperability problems
*               with machines that do not have the same alternate names.
*
*Admin Low Name= site_low;
*Admin High Name= site_high;
```

Figure 1-6 Changing the Names of Administrative Labels in the `label_encodings` File

If desired see the procedure "To Change the Names of Administrative Labels" on page 108 in Chapter 4.

Specifying Whether Users See Administrative Labels' Names

Because some sites may choose not to train users about administrative labels while other sites may consider the names of administrative labels to be classified information, the option to set a label view allows the security administrator to determine whether the ASCII names for administrative labels are displayed to non-administrative users.

ADMIN_HIGH and ADMIN_LOW are the default ASCII names for the administrative labels. As described in "Changing the Administrative Labels' Names" on page 22, the security administrator role can specify alternate names for administrative labels in the `label_encodings(4TSOL)` file, so keep in mind that the administrative labels may have been renamed. The option for setting the default label view does not change the ASCII names for

administrative labels; *the default label view only affects whether the name of another label is substituted for the name of either administrative label whenever users would see either one of the administrative labels.*

Simply speaking, setting the label view mode to EXTERNAL hides the names, and setting the label view to INTERNAL allows the names to be seen.

In the default `label_encodings` files, the system-wide Default Label View is set to External:

```
Default Label View Is External
```

The site's security administrator either accepts the factory setting or changes it. In the `label_encodings` file the choices are:

- Internal, or
- External

Internal View

The INTERNAL view allows users to see the *names* of the administrative labels, which are either the strings "`ADMIN_HIGH`" and "`ADMIN_LOW`" or their administratively-set alternate names.

External View

The EXTERNAL view hides the ASCII names of administrative labels.

More specifically, if the label view is set to be EXTERNAL:

- The ADMIN_LOW label or its site-specified equivalent is not shown, and the minimum valid label of the same type is shown instead, and
- The ADMIN_HIGH label or its site-specific equivalent is not shown and the maximum valid label of the same type is shown instead.

Caution – It is important to keep in mind that the binary label remains the same whichever view is specified and that the view only affects whether the defined *ASCII name* of an administrative label *is replaced by an alternative ASCII name* when it is displayed.

Example of the Effects of the Label View

Here is an example of how the default label view affects what the user sees. Remember that the information label of a newly created file is always ADMIN_LOW because it is empty, while its sensitivity label is the label of the process that created it. So, if a user begins to edit a file in a Text Editor at REGISTERED, the CMW label of the new file is:

```
ADMIN_LOW [REGISTERED]
```

If the INTERNAL label view is set, the same CMW label shown above displays as usual as: ADMIN_LOW [REGISTERED]. When the EXTERNAL label view is set, the name of the lowest valid information label, PUBLIC, replaces the name of the administrative label, and CMW label displays as:

```
PUBLIC [REGISTERED]
```

The Hierarchy of Label View Settings

The label view is set to be either internal or external in three different ways that are described in this section in order of precedence, with the lowest first.

- In the `label_encodings(4TSOL)` file
- In the `tsoluser(4TSOL)` File (set in the User Manager)
- In programs

In the `label_encodings` *File*

The placeholder `label_encodings` file has the label view set to External in the LOCAL DEFINITIONS section, as shown in Figure 1-7. This is called the default because it is the system-wide setting that applies unless it is overridden by either of the other two settings.

```
Default Label View is External;
```

Figure 1-7 The Default Setting for the Label View

When creating the site's `label_encodings` file, the security administrator role may choose to accept or change the label view setting. Also, this value may be changed by the security administrator role after the system is up and running by later editing of the `label_encodings` file.

In the User Manager

The label view setting in a process may override the system-wide setting. A process' label view is set to be either *internal*, *external*, or *sys*. If sys, the label view is set to the default setting in the `label_encodings` file. A process' label view gets set indirectly:

- Each account has its own label view set to be either internal, external, or sys by the User Manager and those settings stored in the `tsoluser(4TSOL)` file.
- The initial process created at login sets the label view process attribute flag based on the setting for the account logging in.

Specifically, when each user and role account is being configured, the security administrator specifies a label view using the User Manager menu, either internal, external, or sys.

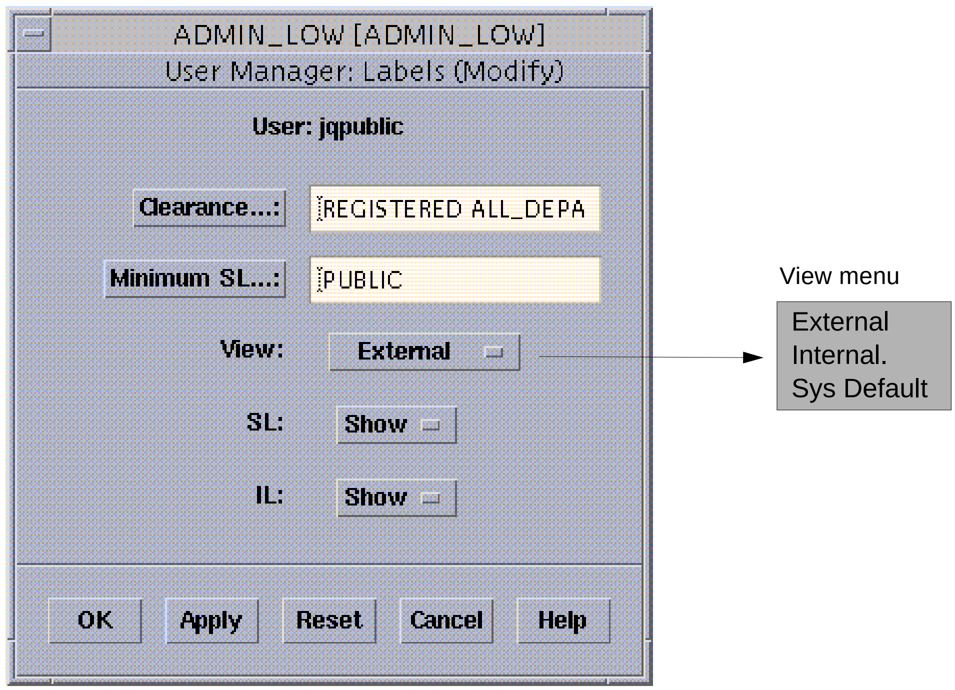


Figure 1-8 User Manager: Labels Dialog Box

The label view is the first value stored in the *labelview* field in the account's entry in the `/etc/security/tsol/tsoluser` file, followed by either *showil* or *hideil*, followed by either *showsl* or *hidesl*. In the example entry in Figure 1-9, because the first setting in the labelview field is internal, the label view is set to INTERNAL for the locally-created auditadmin administrative role account.

auditadmin:fixed:automatic:Audit Control,Audit Review,Media Restore,:none:5:lock:**`internal,showil,showsl`**:0x0
000:0x0000000000000000000000000000000000000000000000000000000000000000:0x7fffffffffffffffffffffffffffffffffffffffffffff
ffffffffffffffffffffff:utadm:res1:res2:res3

Figure 1-9 Example `tsoluser` Entry for an Audit Administration Role Account

Note – Do not edit the `tsoluser(4TSOL)` file directly. Change any account's label view through the Labels dialog box in the Trusted Solaris version of the Solstice User Manager.

How `setpattr(2TSOL)` *Sets the PAF_LABEL_VIEW flag for a Process*

When a user or role starts a process, the `tsoluser` file entry for the account is consulted and the process attribute flag `PAF_LABEL_VIEW` is set using `setpattr(2TSOL)`, according to the label view specified in the `tsoluser` file entry for the account. PAF_VIEW_EXT sets the external view and a PAF_VIEW_INT sets the internal view. If the sys label view is specified in `tsoluser`, the PAF_VIEW_DEF is set to the default setting in the `label_encodings` file.

In programs

Programs can use library routines [described on the `bltos(3TSOL)` man page and in Chapter 5, “Labels” from the *Trusted Solaris Developer’s Guide*] to set or get the label view of a process get the process’ label view.

Regardless of the value of the PAF_LABEL_VIEW flag, a library call used to translate labels from binary to ASCII can specify that labels be translated with either an INTERNAL or EXTERNAL label view. If the VIEW_EXTERNAL or VIEW_INTERNAL flags are not specified in the call to the library routine, translation of ADMIN_LOW and ADMIN_HIGH labels is controlled by the label view process attribute flags. If the label view process attribute flag is defined as VIEW_SYS, the translation is controlled by the label view configured in the `label_encodings` file.

Administrative Roles Overview

By default, Trusted Solaris administrative tasks are divided between two major administrative roles: the security administrator role, and the system administrator role. The account who is configured to assume an administrative role first logs in with her own user name, authenticates herself by providing a password, sets a session clearance, and begins work in a normal user workspace; all processes that she starts have her own UID. To do administrative tasks, the user must take another step and select an option from the Trusted Path menu to assume an administrative role. To assume the role, the user has to re-authenticate herself with the role password.

Once the role is assumed, an administrative workspace is then created with a number of unique attributes. While the normal user can only work at labels within the user clearance and cannot have a clearance or minimum sensitivity label outside of the user accreditation range unless that user has the *use all defined labels* authorization, the default roles can work at any valid label in the system including the two administrative labels, ADMIN_LOW and ADMIN_HIGH. In the default configuration, the ADMIN_LOW sensitivity label is assigned to an administrative role's initial workspace and to the three additional workspaces that are created and made available in the workspace switch area of the front panel. After the initial assumption of the role, the role can start new role workspaces and label them with any valid sensitivity label in that role's account accreditation range, including ADMIN_HIGH.

The administrative role workspace is the only place an application can be launched that requires the trusted path process attribute.

Trusted Solaris sites need both the security administrator and system administrator roles to install and configure hosts and set up users. The security administrator role oversees the installation to ensure that decisions related to the site's security policy are enforced correctly, specifies label ranges and views for each account, and provides the organization's `label_encodings` file that is used to replace the placeholder after installation.

How Labels Are Configured

The Trusted Solaris installation software asks the install team to make some system-wide choices about labels before the `label_encodings` file is even installed. The decisions about which options to choose are made by the security administrator in the light of the site's security policy. The choices are initially put into effect during installation and may be modified later. Whether or not users see administrative labels or any labels at all is determined in part by the choices made during installation as described in "System-wide Label Configuration Choices During Installation" below, and then further configured on a case by case basis for each individual user account as it is created using the Trusted Solaris User Manager. The aspects of label configuration that can be modified later are described in the relevant sections that follow.

System-wide Label Configuration Choices During Installation

During installation, the Customize Trusted Configuration dialog box comes up as shown in Figure 1-10 on page 29.

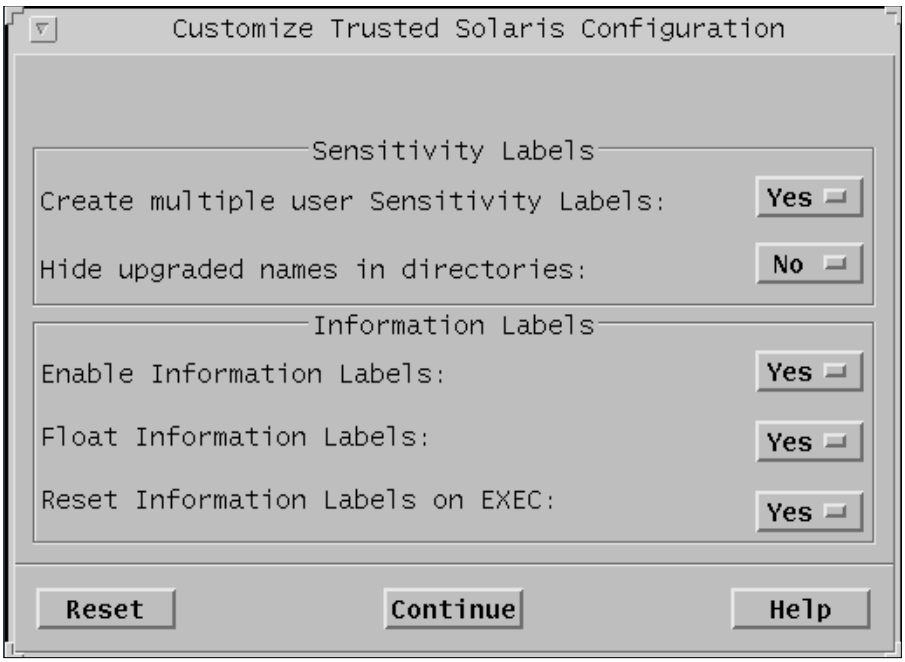


Figure 1-10 The Customize Trusted Solaris Configuration Dialog Box

Sensitivity Label Options on the Labels Configuration Dialog Box

As shown in Figure 1-11, three sensitivity label options appear on the Trusted Solaris Configuration dialog box.

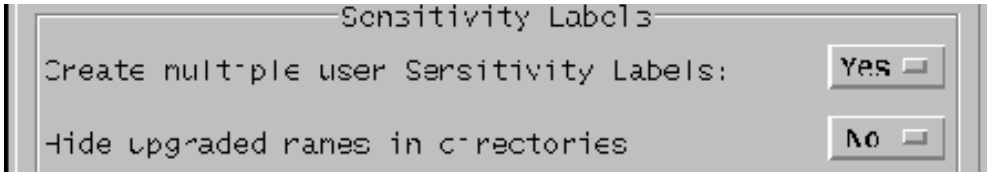


Figure 1-11 Sensitivity Labels Options in the Customize Trusted Solaris Configuration Dialog Box

- `Create multiple user Sensitivity Labels`

  The `Create multiple user Sensitivity Labels` menu option in the dialog box in Figure 1-11 allows the install team to choose between running with multiple sensitivity labels defined or with only one sensitivity label defined.

  If the answer to Create Multiple User Sensitivity Labels? is Yes, a sample `label_encodings` file is installed with multiple sensitivity labels defined. If the answer to Create Multiple User Sensitivity Labels? is No, then a `label_encodings` file is installed with a single sensitivity label.

  Whichever way the question was answered, each site must either review and edit or replace the `label_encodings` file, as described in “Default label_encodings Files” on page 48.

Note – There is no option to enable sensitivity labels because at least one sensitivity label must always be enabled in the user accreditation range, in addition to the two administrative labels that are automatically defined. As explained further, under “Running Without Labels” on page 51, a single sensitivity label must be defined even when an organization wants to run the Trusted Solaris system with no labels visible. The security administrator then hides the single sensitivity label when configuring individual user accounts so it appears to non-administrative users to be a “no labels” system.

- `Hide upgraded names in directories`

  Upgraded files (and directories) are those whose sensitivity label has been *changed to be at a higher level* than that at which they were created. (Upgrading of file sensitivity labels may be done only by a user or administrative role that has the upgrade sensitivity label authorization.) The `Hide upgraded names in directories` option lets each organization choose between having the names either hidden or viewable by normal users—because some organizations wish to ensure that normal users can see only those files and directories whose sensitivity labels are dominated by their process' sensitivity label.

Decision to Make for the Install Team to Follow

- **Decide whether your site's security policy requires a single sensitivity label or multiple labels**
- **Decide whether or not your site's security policy requires that the names of upgraded files and directories be hidden**

Information Label Options on the Labels Configuration Dialog Box

As shown in Figure 1-12, three information label options appear on the labels configure dialog box.

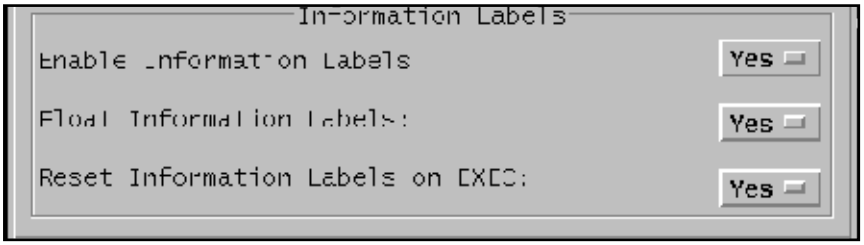


Figure 1-12 Information Label Options in the Customize Trusted Solaris Configuration Dialog Box

All of the information label-related settings in the Customize Trusted Solaris Configuration dialog box are saved as `tsolsys` switch settings in the `/etc/system` file. The `system`(4) file is a local file on each host that usually

should be the same on all hosts in the Trusted Solaris distributed system. The security administrator can later change the value of the `tsolsys` variables in the `/etc/system` file. Changes become effective only after a reboot.

Note – It is recommended that changing the `system` file values be done starting on the NIS+ master. In most cases, the master copy should then be distributed throughout the system so that the same settings are maintained on all NIS+ clients. One exception would be the `tsol_privs_debug` option, which the security administrator may wish to enable on his or her own host for privilege debugging of applications being ported to the system. “Distributing Changed Label Configuration Files to All Hosts in the Distributed System” on page 124 of Chapter 5, “Central Administration of Labels-related Files.”

- `Enable Information Labels`

  This option determines whether or not information labels are displayed anywhere on the system. If the answer is No, the other two options in this section of the dialog do not apply.

Note – Whether or not user accounts are configured to see information labels, if information labels are disabled in the system(4) file, users cannot see information labels. If information labels are disabled during installation, the security administrator may re-enable them later by changing the value of the `tsol_enable_il` setting in the `system` file from 0 to 1.

- ♦ `Float Information Labels`

  If information labels are enabled, this option determines whether information labels automatically float.

- ♦ `Reset Information Labels on EXEC`

  Unless this option is answered with a Yes, the information label from one program executed by a process affects the information label of any subsequent programs that may be executed by the same process. Answering Yes to this option causes the information label of a process to be reset to ADMIN_LOW at each `exec`(2).

Decisions to Make and to Ensure the Install Team Enforces

- ♦ **Decide whether or not your organization needs to use information labels**

- **Decide whether or not your organization needs to have information labels that float**
- **Decide whether or not your organization wants information labels to be reset to ADMIN_LOW when a process executes a new command**

Setting Users Labels Using the User Manager

The minimum sensitivity label and the clearance for an account is set using the Labels dialog box from the User Manager, as shown in Figure 1-13.

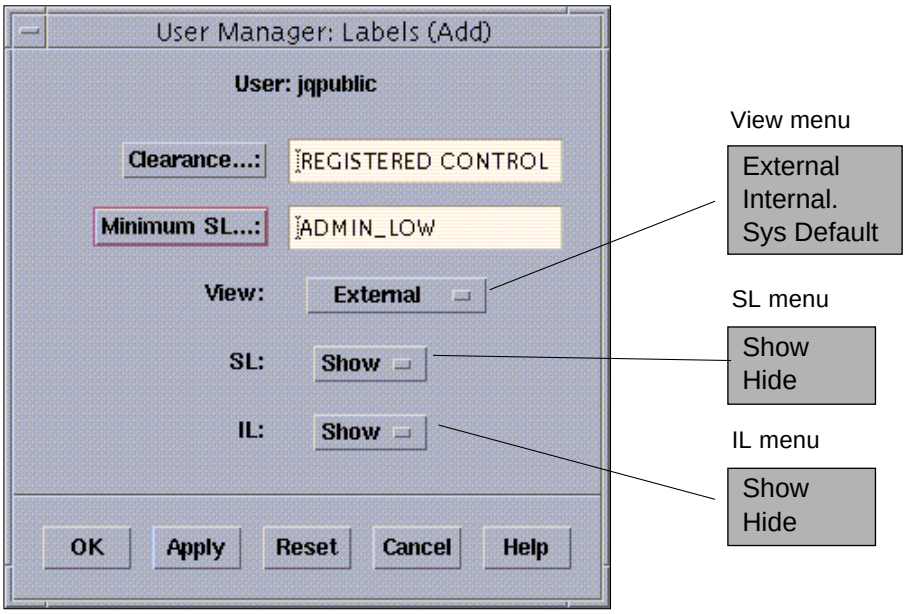


Figure 1-13 User Manager Labels Dialog Box

- The Clearance and Minimum SL buttons bring up label builders when selected.
- The View menu determines whether the user sees the names of administrative labels.

- The SL and IL menus allow the security administrator to configure the following options for individual users.

Table 1-7 How Showing and Hiding SLs and ILs Affects What the User Sees

Sensitivity Labels	Information Labels	Example of What User Sees
Show	Show	PUBLIC [REGISTERED]
Show	Hide	[REGISTERED]
Hide	Show	PUBLIC
Hide	Hide	

Note – Allowing an individual to see information labels is possible only if information labels have been enabled system-wide during installation. If information labels have been disabled system-wide, the IL toggle is grayed and not available for selection.

Note – If you hide sensitivity labels for a user's account, you probably also should restrict the user to work at a single sensitivity label by making the clearance equal to the initial label, because it would otherwise be confusing for a user to work with multiple sensitivity labels without being able to see them.

Setting the Label View

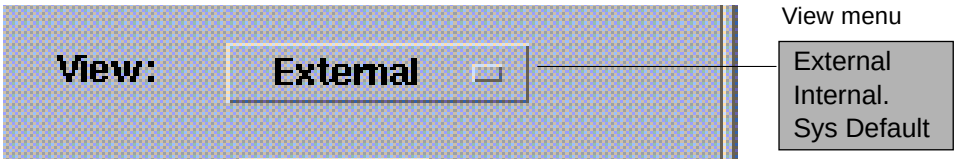


Figure 1-14 The View Menu on the User Manager Labels Dialog Box

Using the View menu in the User Manager Labels Dialog Box, which is shown in Figure 1-14, the security administrator can override the system default label view for each user or role account. (See "The Hierarchy of Label View Settings" on page 24 for background.) When each user or role's account is being set up, the security administrator sets the user's view to one of the following:

- Internal

- External
- Sys Default

Internal

The Internal view allows users to see the *names* of the administrative labels, which are either the strings "ADMIN_HIGH" and "ADMIN_LOW" or their administratively-set alternate names.

External

Users with the External option are not exposed to the ASCII names of the administrative labels. If the label view for an account is set to External, the *minimum* valid label of the same type in the `label_encodings` file is shown instead of the ADMIN_LOW label or its site-specified equivalent. Also, when the account's label view is External, the *maximum* valid label of the same type is shown instead of the ADMIN_HIGH label or its site-specific equivalent.

Sys Default

If the Sys Default option is selected for an account, whatever value is specified in the `label_encodings(4TSOL)` file for the "`DEFAULT LABEL VIEW`" keyword (EXTERNAL or INTERNAL) applies to the account.

How System Switches and Label View Settings Affect Each Other

As indicated in Table 1-8 on page 36, if information labels are disabled during installation (and as a result the system-wide configuration switch, tsol_enable_il, is set to 0), or if a user's account is configured so that information labels, or information labels, or both are not displayed, the setting of the default label view can have no effect on whatever type of label may be hidden. If information labels are enabled, the setting of either label view is then effective only insofar as an individual account is configured to allow the

showing of information labels and information labels. Table 1-8 shows how the system switches and each account's label visibility settings are affected by the label view setting

Table 1-8 How System Switches, Account's Label Visibility Settings, and Label View Settings Affect the Display of Labels for a User or Role Account

Setting	Results with EXTERNAL View	Results with INTERNAL View
`/etc/system`: information labels disabled system-wide (`tsol_enable_il=0`)	No information labels display	No information labels display
`/etc/system`: information labels enabled system-wide (`tsol_enable_il==1`)	Name of minimum well-formed information label replaces the name of the ADMIN_LOW information label. Name of maximum well-formed information label replaces the name of the ADMIN_HIGH information label. All other information labels display normally.	The ADMIN_LOW and ADMIN_HIGH names or secadmin-specified alternate administrative label names are displayed. All other information labels display normally.
User Manager account IL setting=Hide ILs	No information labels display	No information labels display
User Manager account IL setting=Show ILs	Name of minimum well-formed information label replaces the name of the ADMIN_LOW information label. Name of maximum well-formed information label replaces the name of the ADMIN_HIGH information label. All other information labels display normally.	The ADMIN_LOW and ADMIN_HIGH information label names or secadmin-specified alternate information label names are shown. All other information labels display normally.
User Manager account SL setting=Hide SLs	No sensitivity labels display	No sensitivity labels display
User Manager account SL setting=Show SLs	Name of minimum well-formed sensitivity label replaces the name of the ADMIN_LOW sensitivity label. Name of maximum well-formed sensitivity label replaces the name of the ADMIN_HIGH sensitivity label. All other sensitivity labels display normally.	The ADMIN_LOW and ADMIN_HIGH sensitivity label names or secadmin-specified alternate sensitivity label names are shown. All other sensitivity labels display normally.

Decision to Make Before Starting

- **Decide whether the user is allowed to see the names of administrative labels or if the user will see the minimum valid label in the `label_encodings` file instead of the name of the ADMIN_LOW label and see the maximum valid label in the `label_encodings` file instead of the ASCII name of the ADMIN_HIGH label.**

Types of Labels That Must Be Specified at Each Site

Required types of labels are:

- Sensitivity labels and clearances
- Information labels

Organizations also may specify certain fields that are printed on the banner and trailer pages that accompany each print job. These fields are called:

- *Printer banners* and
- *Handling caveats*

Configuring How Labels are Printed on Banner/Trailer and Body Pages

The security administrator can modify a number of things about how labels are printed on banner/trailer and body pages of print jobs and can modify the text that appears on the banner/trailer page. See Chapter 3, “Specifying Labels and Handling Guidelines for Printer Output.”

Overview of Planning

- **Allow time to complete the `label_encodings` file before installing the system.**
- **Be prepared to spend time on the planning process.**
  Building the encodings for a site and making it correct both syntactically and semantically is a manual, time-consuming process.
- **Know your site’s security policy.**
  Many Trusted Solaris installations already have a security policy developed according to government methods. Commercial businesses, even though they do not have as much experience in planning labeled security, can start

with examining their goals for information protection and use them as a basis for making 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 of how one commercial company developed a simple security policy based on its legal department's information labeling requirements, 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 *Trusted Solaris Installation and Configuration*.

- **Learn about the U. S. government label encodings file whose syntax and rules are used in the Trusted Solaris version.**
  See the *Compartmented Mode Workstation Labeling: Encodings Format:* Defense Intelligence Agency document [DDS-2600-6216-93].

- **Plan to finalize your encodings before installation.**
  Changing the label_encodings on a running system is risky. See "Changing the label_encodings File After System Start Up" on page 51 of Chapter 2.

Planning the Encodings File

The following steps help achieve the good organization required for a correct label encodings file that may be extended safely later.

- **Plan to leave room to add items.**
  Plan ahead for extending the file later, which may save you from needing to create a whole new file if additions are needed. For example, you could number classifications in increments of 10 to allow intermediate classifications to be added if the need arises. For the same reason, space compartment bit numbers for possible later additions.

- **If your site uses inverse compartments and markings, plan to reserve some initial compartment and marking bits for later definition.**
  If you need to learn more about inverse compartments and markings see the DIA document, *Compartmented Mode Workstation Labeling: Encodings Format*: *Encodings Format*, which is referred to in the "Preface." See also "Setting Default and Inverse Words" on page 55 of Chapter 2.

- **Determine classifications for the site.**

  As described under “Classifications” on page 7, the total number of classifications that may be defined at a site is 256. Do not use classification 0. The classification part of the label represents the relative sensitivity of one classification over another. Irrespective of what you call the human readable names associated with each classification, the system treats a classification whose value is 10 as more security sensitive than a classification whose value is 2.

Note – Note for that CLASSIFICATIONS, COMPARTMENTS, and MARKINGS, the security administrator can later change human readable names but cannot change the values without potentially serious complications.

  Different WORDS cannot be assigned the same classification value. Each classification WORD must be higher or lower than one or more others because all labels must dominate or be dominated by some other label. Assigning the same number to more than one name would create levels of security that are named differently but are treated as the same level by the system. No two labels can evaluate to the same level.

- **Decide on compartments.**
  Decide how data and programs are grouped and whether or not any data or programs can be intermixed. For example, a site’s security administrator may decide that weather data should not be seen by programs dealing with personnel files but that weather data should be accessible to programs that deal with targeting problems.

  At this point, keep people out of the picture. Think in terms of what, not who. Keep in mind that compartments are also considered to be handling channels.

- **Design the names.**
  CLASSIFICATIONS and WORDS in the `label_encodings` file have two forms: a mandatory long name and an optional short name. Long names for classifications and any words appear by default in the information label portion of the CMW label. Short names for classifications and any words appear by default within brackets in the sensitivity label portion. Labels on windows are truncated after the real estate on the top of the window is used up, and, even though you can view the full label, so labels on window system objects can be read more easily if you keep the long and short names as short as possible while still retaining meaning.

- **Arrange the relationships.**
  Compartments and markings are intrinsically non-hierarchial, even though they can be configured to have hierarchical relationships. They represent bits (or flags) attached to objects or subjects in the system. The combination of those bits determines the accessibility of a subject or object. Before setting up relationships, read very carefully the example section of *Compartmented Mode Workstation Labeling: Encodings Format* several times, walking through the examples.

  One way to make this step easier is to use a large board and pieces of paper marked with your classifications, compartments and markings, as shown in "Example Planning Board for Label Relationships" on page 41. With this method, you can visualize the relationships and rearrange the pieces until they all fit together.

Note – When the command, `chk_encodings(1MTSOL)`, is used to check label encodings files for errors, it checks syntax only. With the `-a` option `chk_encodings` can be used to analyze and report on relationships between labels.

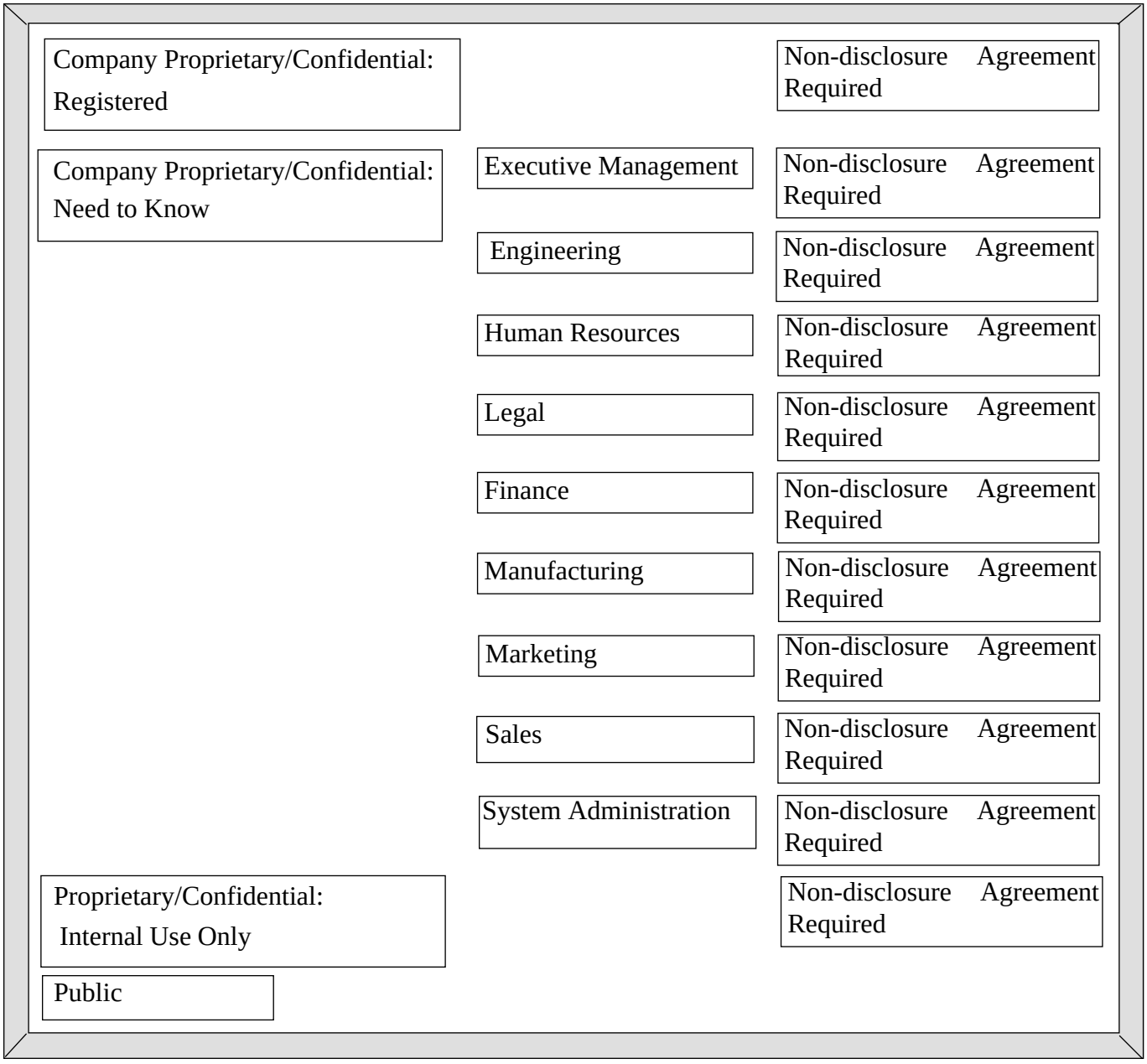


Figure 1-15 Example Planning Board for Label Relationships

- **Decide which clearances will be available to which users.** Arrange the labels that will be formed from the classifications, compartments, and markings in order of increasing sensitivity.
- **Associate the definitions for each word with an internal format of integers, bit patterns, and logical relationship statements.**
- **Decide what colors should be associated with labels.**

Creating or Editing the Encodings File

2

This chapter describes the steps for creating the `label_encodings(4TSOL)` file for your site. The guidelines should also be followed for any subsequent modifications of the `label_encodings` file.

This chapter includes these topics:

2

This chapter also describes these procedures:

Readying the Label Encodings File Before the NIS+ Master or Standalone System is Configured

Figure 2-1 on page 46 shows the overall process of administering the `label_encodings` file when the system is first being configured. Steps 1 through 4 in Figure 2-1 illustrate the first part of the overall process, which is described in this section.

Before the install team starts post-installation configuration on the NIS master or on a standalone system, the security administrator should have done the following:

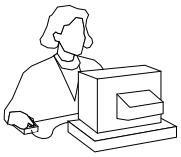
- The analysis and planning described in Chapter 1, “Introduction to Trusted Solaris Label Encodings” should be done
- The `label_encodings(4TSOL)` file should be ready as described in this chapter, if at all possible

As described in “How Labels Are Configured” on page 29 in Chapter 1, a placeholder single-label or multilabel file is installed in `/etc/security/tsol/label_encodings` by the installation software. The placeholder `label_encodings` file is almost always replaced with each site’s version during configuration.

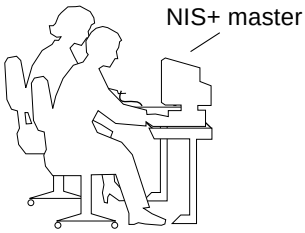
If no `label_encodings` file has been used previously at your site, the security administrator can create one by one of the following ways:

- Typing in and modifying a copy of either of the `label_encodings` files in this manual’s appendix
- Waiting until after installation to copy a placeholder file.

Note – Before the install team goes on to complete the software configuration, the security administrator can make the site’s modifications in the copied placeholder file. However, since creating the `label_encodings` file is usually a lengthy process, it is better to get it ready beforehand.



security administrator



install team

1.
Before installation begins, the security administrator prepares a site-specific security policy, decides what labels the site needs and which computer users can work at which labels, and prepares guidelines for the install team to use when answering labels-related questions during installation and when configuring users and hosts.

2.
If possible, before installation begins, the security administrator prepares a site-specific `label_encodings` file. (Sites where Trusted Solaris has never been installed before will not have an existing `label_encodings` file to modify but can copy one from Appendix A.)

3.
Whether setting up a distributed system beginning with the NIS+ master, or setting up a standalone host, the install team answers label-related questions on the Trusted Solaris Configuration dialog box. Based on the install team's answers, the installation software installs either a multilabel or a single-label `label_encodings` placeholder file and sets certain labels-related kernel switches in the `system` file.

4.
The security administrator supplies the site-specific `label_encodings` file (either prepared ahead of time or modified from the installed placeholder files), and the install team substitutes the site-specific `label_encodings` file for the placeholder file and finishes configuring users and hosts.

5.
At sites with a distributed system of multiple Trusted Solaris hosts, because the `label_encodings` and the label-related switches set in the `system` file are not administered through NIS+, the install team sets up procedure to distribute the `label_encodings` file and the label-related kernel switch settings from the NIS+ master to all NIS+ clients and any standalone hosts at the site.

6a.
If setting up a net install server or Custom JumpStart, the install team puts the master `label_encodings` and the answers to the labels-related configuration questions in a `/tsolconfig` directory and identifies the directory in the `bootparams`(4) file on the boot server.

6b.
For any hosts not being installed from a net install server or by means of Custom JumpStart, the install team uses `rdist`(1), tape, or some other method to copy the master `label_encodings` and (usually) the `system` file to all hosts in the distributed system.

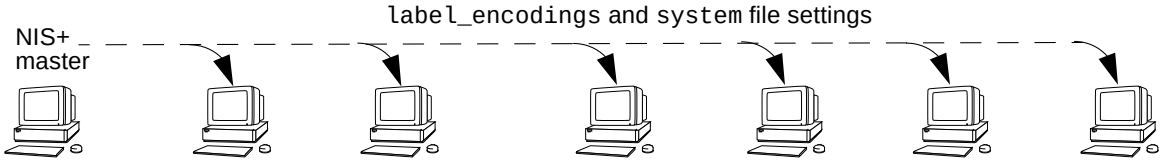


Figure 2-1 Centrally Administering Labels-related Non-NIS+ Files: The Big Picture

Labels-Related Files and Central Administration

After the NIS+ master for a distributed system is fully configured (with the master `label_encodings` file in place), the install team goes on to install the other hosts in the Trusted Solaris distributed system. Steps 5 and 6 in Figure 2-1 on page 46 show this part of the overall process of managing labels when a distributed system is first being configured. The security administrator should ensure that an identical copy of the `label_encodings` file is on every host. In most cases, the security administrator will also want to make sure that the labels-related kernel switch settings in the `system`(4) file are also the same on all hosts. The `label_encodings` file is not administered by NIS+, so another means of distribution must be used. See *Trusted Solaris Installation and Configuration* for more about configuration and distribution of configuration files and see also Chapter 5, "Central Administration of Labels-related Files," for details on how the labels are maintained the same across the distributed system.

Note – The maximum line length in the `label_encodings` file is 256 bytes.

Actions for Editing and Checking the `label_encodings` *File*

The `label_encodings` file is a flat, text file. The file must be checked using the `chk_encodings(1MTSOL)` command, which is not usually entered on the command line. Most often, the security administrator uses one of the two actions shown in Table 2-1, which are in the System_Admin folder within the Application Manager.

Table 2-1 Administrative Actions for Editing the `label_encodings` File

Action Name	Purpose
Edit Encodings	Edits and checks label_encodings
Check Encodings	Checks label_encodings

Note – Because it is a text file, the `label_encodings` file may be created or edited on any UNIX system. However, it must be checked and tested on a host running the Trusted Solaris operating system.

2

Hints

- **Make a backup copy (on a tape or floppy disk) of the original file installed with the system or, if this is a modification made on an operational system, back up the current file.**
  If your modifications create file labels that cannot be resolved, you may have to manually reset labels to `ADMIN_LOW` before re-assigning valid labels from the modified file. Alternately, you may wish to restore a known, usable `label_encodings` file from tape or floppy until the unresolvable changes are debugged.
- **Code the file using any text editor, and save a hard copy when done.**
  This procedure is detailed in "To Modify the label_encodings (4TSOL) File" on page 60. As soon as possible after you are satisfied with the file, print it out and keep a record.
- **Check the syntax of file entries with the `chk_encodings(1MTSOL)` command.**
- **Check the syntax and relationships of the labels with the `chk_encodings` command and the `-a` option.**
- **Test the encodings file on a standalone test machine if possible before moving it to a working system.**
- **Place an identical copy of the `label_encodings` file on every machine.**

Default `label_encodings` *Files*

The Create multiple user Sensitivity Labels menu on the Customize Trusted Solaris Configuration dialog box is shown in Figure 2-4. Either a multilevel or a single-label `label_encodings` file is put in place by the installation software, based on which option is selected by the install team.

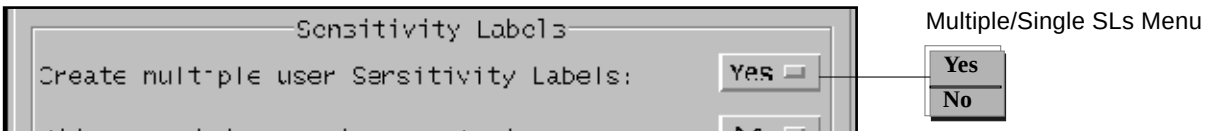


Figure 2-2 Create Multiple User Sensitivity Labels Menu on the Customize Trusted Solaris Configuration Dialog Box

Differences Between Default Single and Multiple User Sensitivity Labels Files

The `label_encodings` file that would be installed if No is selected from the "Create Multiple User Sensitivity Labels" menu during installation is almost identical to the multilabel version that would be installed if Yes is selected. The only differences are in the settings in the ACCREDITATION RANGE section, which defines which of the classifications and compartments are usable by ordinary users.

Multiple Sensitivity Labels Version

Figure 2-3 shows the ACCREDITATION RANGE Settings in the default multilabel encodings file. To allow the site to use all the classifications and compartment words defined elsewhere in the `label_encodings` file, the following are defined in the ACCREDITATION RANGE section:

- 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, and
- UNCLASSIFIED is defined as the minimum protect as classification (The minimum protect as classification is explained under"Specifying the Protect As Classification" on page 76 in Chapter 3.)

```
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;
```

Figure 2-3 ACCREDITATION RANGE Settings in the Default Multilabel Encodings File

Single Sensitivity Label Version

The only differences in the single-label version from the multilabel version are in the settings in the ACCREDITATION RANGE section shown in Figure 2-4. The settings shown restrict the user accreditation range to the following:

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

```
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;
```

Figure 2-4 ACCREDITATION RANGE Settings in the Default Single-label Encodings File

The easiest way to run with a single sensitivity label would be to change only the ACCREDITATION RANGE section in the installed single-label `label_encodings` file. You could also achieve the same result by creating an encodings file on your own with only one classification and either with no compartments or with only the compartments you decide you need. See “To Replace the Single Label in the Default Single-label Encodings File” on page 65 for guidelines for both approaches.

Changing the `label_encodings` *File After System Start Up*

After the Trusted Solaris system is fully configured and running, the security administrator may later wish to modify the `label_encodings` file. See Chapter 5, “Central Administration of Labels-related Files,” for what changes to avoid making, for how you can safely make other changes, and for how to distribute the changed file to all hosts on the system.

Running Without Labels

An organization may not want its computer users to see labels or be aware of mandatory access controls. By following the steps in “To Set Up No Labels Operation” on page 61, the Trusted Solaris security administrator can configure what appears to be a “no labels” operation, so that all non-administrative users see a working environment that is visually almost the same as working in a Solaris environment with the CDE window system.

In spite of appearances, it is important to remember that, even if you set things up so that non-administrative users do not see labels, certain labels are always present:

- ADMIN_LOW and ADMIN_HIGH clearances, sensitivity labels, and information labels (always included in the Trusted Solaris system, do not need to be defined)
- One sensitivity label in the user accreditation range
- One clearance in the user accreditation range
- One information label in the user accreditation range

Note – Even if your site does not use information labels, if no information labels are defined, the `label_encodings` file cannot pass `chk_encodings(1MTSOL)`. To work around this software requirement, copy the words defined in the SENSITIVITY LABELS WORDS to the INFORMATION LABELS WORDS section, and then disable information labels as described in “To Set Up No Labels Operation.”

Word Order Requirements

The order in which words are configured is not enforced but it is important when setting up relationships between words. See "How Channels Are Configured" on page 86 of Chapter 3 for an example of how the order affects how channels must be encoded. See also the DIA *Label Encodings Format* manual referenced in the Preface.

By convention, the WORDS in the INFORMATION LABELS section are arranged in decreasing order of importance and the WORDS in the SENSITIVITY LABELS section are arranged in increasing order of importance.

Template for a Trusted Solaris Label Encodings File

The `label_encodings` file has the following sections:

VERSION=

CLASSIFICATIONS:

INFORMATION LABELS:

SENSITIVITY LABELS:

CLEARANCES:

CHANNELS:

PRINTER BANNERS:

ACCREDITATION RANGE:

NAME INFORMATION LABELS:

LOCAL DEFINITIONS:

Adding or Renaming a Classification

The security administrator may replace all the default classifications and words defined in the default demo `label_encodings` file, or add classifications or words to the file, or create a new CLASSIFICATIONS: section in a site-created file.

Number of Classifications

The total number of classifications that can be defined at a site is 256.

Keywords Defined for Classifications

Table 2-2 shows the keywords that can be defined for classifications. Keywords that begin with an asterisk (*) are optional. See “Setting Default and Inverse Words” on page 55 for more about how to set up optional initial compartments and markings that may be associated with classifications.

Table 2-2 Values for Classifications *(1 of 2)*

Value	Requirements
`name=`	Cannot contain (/) or (,) or (;). All other alphanumeric characters and white space are allowed. The long name appears in information labels whenever CMW label with this classification is displayed. 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 (within brackets) whenever CMW labels are displayed.
`*aname=`	Name used only for input by users. The alternate name can be entered by users any time a classification is needed (in sensitivity labels, information labels, and clearances).

Table 2-2 Values for Classifications *(2 of 2)*

Value	Requirements
`value=`	The values you assign should represent the actual hierarchy among the classifications and leave room for later expansion. 0 is reserved for ADMIN_LOW, 62767 is reserved for ADMIN_HIGH. Values may start at 1 and go to 256.
`*initial compartments=`	Specify bit numbers for any default compartment words (words that should initially appear in any label that has the associated classification). ADVANCED: Also specify bit numbers for any inverse words. Recommended: set aside initial compartments for later additions of inverse words if your site uses inverse words for all but the minimum classification. It is not recommended to have initial compartments or markings for the minimum classification
`*initial markings=`	Specify bit numbers for any default words (words that initially are in any information label in which the associated classification appears). ADVANCED: also specify inverse words to be defined immediately or added later. RECOMMENDED: set aside initial markings for later additions, if your site uses inverse words.

Unless you are creating a set of encodings that must be compatible with another organization's label encodings, do not worry about which numbers to use for compartments and marking bits. Keep track of the ones you use and their relations to each other in Table 2-5.

Figure 2-5 shows the top of the placeholder Trusted Solaris `label_encodings` file, with the `CLASSIFICATIONS` sections.

```
CLASSIFICATIONS:

*
name= UNCLASSIFIED;  sname= U;  value= 1;
name= CONFIDENTIAL;  sname= C;  value= 4; initial compartments= 4-5 190-239;
                                          initial markings= 11 12 17 190-239;
name= SECRET;        sname= S;  value= 5; initial compartments= 4-5 190-239;
                                          initial markings= 11 12 17 190-239;
name= TOP SECRET;    sname= TS; value= 6; initial compartments= 4-5 190-239;
                                          initial markings= 11 12 17 190-239;
```

Figure 2-5 Trusted Solaris Placeholder `label_encodings` File (Top)

Each classification defined in Figure 2-5 has the mandatory *name*, *sname*, and *value* set. The CONFIDENTIAL, SECRET, and TOP SECRET classifications have *initial compartments* and *initial markings*, while UNCLASSIFIED has none.

Table 2-3 shows some initial compartments bit assignments and what they mean.

Table 2-3 Example Initial Compartments Bit Assignments and What They Mean

initial compartments= 4 5 100-227;	means compartment bits 1, 5, and 190 through 239 are initially on (set to 1) in a label with this classification.

Some of the initial compartments and marking shown in Figure 2-5 are used later in the encodings to define *default* and *inverse* words, and some are reserved for later definitions of inverse words.

The example in Figure 2-6 shows a simple set of classifications that have no initial compartments or markings.

```
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;
initial compartments= 10;
```

Figure 2-6 Simplified Assignment of Initial Compartments

Setting Default and Inverse Words

When a bit is defined as either an initial compartment or initial marking, that means that the bit is 1 in every label that contains the classification. Each bit specified for an initial compartment or initial marking can be defined later in the label_encodings file so as to create either a *default word or an inverse word. Default words* always appear in the label that includes that classification. *Inverse words are not in a label unless the bit is on, but are in the label when the bit is turned off.* For an inverse word to be present in a label, the bit must be off.

A *default compartment word* is a word that you want to always appear in *any label that has the associated classification*. A *default marking word* is a word that you want to always appear in *any information label in which the associated classification appears*. An *inverse compartment word* is a word that you want to always appear in a label that has the associated classification *when another word you define with the inverse compartment's bit is not present.*

Table 2-4 summarizes the requirements for initial compartments and initial markings values associated with classifications.

Table 2-4 Initial Compartments and Initial Markings for Classifications

Value	Requirements
`*initial compartments=`	Specify bit numbers for any default compartment words (words that should always appear in any label that has the associated classification). ADVANCED: Also specify bit numbers for any inverse words. Recommended: set aside initial compartments for later additions of inverse words.
`*initial markings=`	Specify bit numbers for any default words (words that always appear in any information label in which the associated classification appears). ADVANCED: also specify inverse words to be defined immediately or added later. RECOMMENDED: set aside initial markings for later additions of inverse words.

Unless you are creating a set of encodings that must be compatible with another organization's label encodings, do not worry about which numbers to use for compartments and marking bits. Keep track of the ones you use and their relations to each other in Table 2-5, which provides a place to keep track of which bits have been used for compartments and which for markings.

Table 2-5 Compartment and Marking Bit Tracking Table

Compartment Bit Numbers	Marking Bit Numbers
1 2 3 4 5 6 7 8 9	1

Whatever bit you specify for each initial compartment and initial marking, you can create a *default word* later by assigning that bit to a corresponding compartment or marking word. *Default words that are assigned to initial compartments and markings for a classification always appear in the label that includes that classification.*

The example in Figure 2-7 shows the PUBLIC classification assigned no initial compartments or markings while the SUN FEDERAL classification is assigned initial compartments 4 and 5.

```
name= PUBLIC;  sname= P;  value= 1;
name= SUN FEDERAL;  sname= SUNFED;  value= 4; initial compartments= 4-5
```

Figure 2-7 Simplified Assignment of Initial Compartments

The result of the assignments in Figure 2-7 is that an information label that includes the PUBLIC classification has no default compartments assigned, while an information label that includes the SUN FEDERAL classification always has compartment bits 4 and 5 turned on. For an example of how these initial compartment bits can be assigned to words, see Figure 2-8 and the accompanying text.

```
INFORMATION LABELS:

WORDS:

name= DIVISION ONLY;     sname= DO;    minclass=  SUN FEDERAL; compartments= 4-5;
name= SMCC AMERICA_ALL;     sname= SMCCA;  minclass= SUN FEDERAL; compartments= ~4;
name= SMCC WORLD;     sname= SMCCW;    minclass= SUN FEDERAL; compartments= ~5;
```

Figure 2-8 Example of Defining Default and Inverse INFORMATION LABELS Words

Figure 2-8 shows WORDS defined in the INFORMATION LABELS section of the `label_encodings` file. Compartment bits 4 and 5 are assigned to the word, DIVISION ONLY. Both compartment bits 4 and 5 are each also associated with an inverse word: SMCC AMERICA is assigned to the inverse compartment bit ~4 and SMCC WORLD is assigned to the inverse compartment bit ~5. The result of this encodings is that an information label with the SUN FEDERAL classification initially includes the word DIVISION ONLY and its binary representation has the compartment bits 4 and 5 turned on, while an information label with the PUBLIC classification always has compartment bits 4 and 5 turned off, and as a result, the words SMCC AMERICA and SMCC WORLD are included in the label. Because a minclass of

IUO is specified for the inverse words, SMCC AMERICA and SMCC WORLD are not displayed in the PUBLIC information label; the presence of these two inverse words is understood.

In Classifications Planning Worksheet, for every initial compartment bit and marking bit specified, a word should be assigned to the bit in the WORDS in the INFORMATION LABELS and SENSITIVITY LABELS section, and for every initial compartment bit, a word should be assigned to the bit in the WORDS in the SENSITIVITY LABELS section. Do this unless you plan to reserve compartment or marking bits for later assignment after the system is up.

Table 2-6 Classifications Planning Worksheet

name=	**sname=/*aname=**	**value=**	***initial compartments= bit numbers/WORD**	***initial markings= bit numbers/ WORD**
PUBLIC	P	1	none	none
CLASSIFIED	C	4	4-5 190-239	11 12 17 190-239

Setting Up Single-label Operation

Figure 2-9 shows the accreditation range setting in the single-label `label_encodings` file that is installed if the install team answers No to "Create multiple user Sensitivity Labels during installation." As described in "Differences Between Default Single and Multiple User Sensitivity Labels Files" on page 49, the single-label file is the same as the multi-label file, except for the ACCREDITATION RANGE section settings shown here.

```
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;
```

Figure 2-9 ACCREDITATION RANGE Setting to Restrict Operations to a Single Label

"To Replace the Single Label in the Default Single-label Encodings File" on page 65 shows the easiest way to set up a single-label operation by replacing the label in the default single-label file with an alternate name. You do this by modifying only the name for the SECRET classification.

You could achieve the same result by creating an encodings file with only one classification and only the desired compartments. For example, you could set up a `label_encodings` file with the ANY_CLASS classification, and specify

compartments words A, B, REL CNTRY 1 for all types of labels, (information, sensitivity and classifications) then make the settings in the USER ACCREDITATION RANGE: section, that are shown in Figure 2-10.

```
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;
```

Figure 2-10 ACCREDITATION RANGE setting to restrict operations to a single-label

Any of these ways of creating single-label operation also require supporting procedures described in “To Configure Labels Not Visible to Users” on page 68.

Label_encodings-related Procedures

▼ To Modify the `label_encodings (4TSOL)` File

1. **As security administrator in an ADMIN_LOW workspace, make a copy of the installed `/etc/security/tsol/label_encodings` file.**
   EIther make the copy by using commands in a profile shell, as shown below, or by using the file manager.

Note – Keep the backed-up copy of the original file at least until you make sure the edited copy runs correctly.

```
$ cd /etc/security
$ cp label_encodings label_encodings.orig
$ cp label_encodings label_encodings.work
```

2. **Modify the working version of the file.**
   Use the `Edit Encodings` action to Save the file and close, using the Save and Close options in the Edit Encodings File menu. Edit Encodings action automatically runs `chk_encodings(1MTSOL)` on the edited file.

3. **Once the modified file passes `chk_encodings`, copy the edited working file to the `label_encodings` file.**

4. **Initialize the new encodings file.**
   Restart the Window Manager from the Workspace Menu.

5. **On a distributed system of Trusted Solaris hosts, distribute a copy of the `label_encodings` file from the NIS+ master to all hosts in the system.**
   See Chapter 5, "Central Administration of Labels-related Files," for how to distribute the modified file.

▼ To Use a Supplied Label Encodings File

♦ **Configure the Sun extensions in the default file to suit your site's security policy, copy the extensions to the end of your organization's file, check the file using the Check Encodings action, and then install it as described in the *Trusted Solaris Installation and Configuration* manual.**
See Chapter 4, "Modifying Sun's Extensions in the Local Definitions Section" for how to configure the extensions.

▼ To Set Up No Labels Operation

1. **During initial installation of the software in the Customize Trusted Solaris Configuration dialog box, the install team should do the following:**

   a. **Chose the No option on the "Create Multiple User Sensitivity Labels" menu.**

      A `label_encodings` file restricted to a single sensitivity label is installed when the answer to this question is No.

   b. **Chose the No option on the "Enable ILs" menu.**

2. **Change or accept the name of the single label in the installed single-label `label_encodings`.**
   See "To Replace the Single Label in the Default Single-label Encodings File" on page 65.

3. **When setting up user accounts in the User Manager, restrict the user to single-label operation.**
   The example shows the label PUBLIC.

   a. **Configure the user's clearance and initial (minimum) label to be equal to the only encoded label.**

```
Clearance: PUBLIC
Minimum Label: PUBLIC
```

   b. **Configure sensitivity labels to be hidden.**

```
SL: Hide
```

▼ To Add or Rename a Classification in the Default `label_encodings` File

1. **As security administrator in an `ADMIN_LOW` shell, create a working copy of the `label_encodings` file and use the Edit Encodings action to open the file.**
   See "To Modify the label_encodings (4TSOL) File" on page 60.

2. **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 - 5.8 97/05/28
```

   Sun uses SCCS keywords for the version number and the date.

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

3. **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. **Add the new classification(s) to the** ACCREDITATION RANGE **section.** Before a user can make use of a classification, it must be made available in the ACCREDITATION RANGE section. The example shows the three new classifications added to the ACCREDITATION RANGE section of the demo file. All three (i, n, and r) are 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 minimums specified in the** ACCREDITATION RANGE **section if necessary.**

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

▼ To Specify Default and Inverse Words

1. **Specify initial compartments and/or initial markings in the CLASSIFICATIONS section when defining the classification.**

```
CLASSIFICATIONS:

name= PUBLIC;  sname= P;  value= 1;
name= SUN FEDERAL;  sname= SUNFED;  value= 2; initial compartments= 4-5;
```

2. **Specify a default word by assigning an initial compartment or initial marking bit to the word.**

```
name= DIVISION ONLY;     sname= DO;    minclass=  IUO; compartments= 4-5;
name= SMCC AMERICA;   sname= SMCCA;  minclass= IUO; compartments= ~4;
name= SMCC WORLD;     sname= SMCCW;   minclass= IUO; compartments= ~5;
```

3. **Specify an inverse word by assigning an initial compartment or initial marking bit preceded by a tilde (~) to the word.**

```
name= DIVISION ONLY;     sname= DO;    minclass=  IUO;
compartments= 4-5;
name= SMCC AMERICA;   sname= SMCCA;  minclass= IUO; compartments=
~4;
name= SMCC WORLD;    sname= SMCCW;  minclass= IUO; compartments=
~5;
```

▼ To Replace the Single Label in the Default Single-label Encodings File

1. **Make sure that while entering information on the Configure Trusted Solaris options dialog box, the install team chooses No from the** Create multiple user Sensitivity Labels **menu**.
2. **Use the Edit Encodings action to open the** `/etc/security/tsol/label_encodings` **file for editing.**
3. **Replace the classification name with an alternate name.**
   a. **Under the CLASSIFICATIONS: section, change the name SECRET to an alternate name suitable for your site.**
   In the example, the name= is changed from SECRET to INTERNAL_USE_ONLY and the sname= is changed from s to INTERNAL. For simplicity's sake, neither the `value=` nor the `initial compartments=` definitions are changed.

```
CLASSIFICATIONS:

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

   b. **Under `ACCREDITATION RANGE`, replace the short name of the classification (`S`) with the new `sname`.**

```
ACCREDITATION RANGE:

classification= INTERNAL;      only valid compartment combinations:

INTERNAL a b rel cntry1
```

4. **If desired, remove the compartments from the user accreditation range, by deleting the compartments.**

```
ACCREDITATION RANGE:

classification= INTERNAL;    only valid compartment combinations:

INTERNAL
```

c. If appropriate, under `ACCREDITATION RANGE`, replace the definitions for minimum clearance, minimum sensitivity label, and minimum protect as classification 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;
```

▼ To Make Your Own Single-label Encodings File

1. **Create an encodings file with only one classification and only the desired compartments.**
   For example, you could set up a `label_encodings` file with the INTERNAL_USE_ONLY classification, and specify no words for information, sensitivity and clearance labels, channels or printer banners.

```
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:
```

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

Make the settings in the ACCREDITATION RANGE section shown in the example using your own classification, and your own compartment words, if any.

```
ACCREDITATION RANGE:

classification= INTERNAL_USE_ONLY;      only valid compartment
combinations:

INTERNAL_USE_ONLY

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

3. **Encode the LOCAL DEFINITIONS section as described in Chapter 4, "Modifying Sun's Extensions in the Local Definitions Section," making sure to set the system default label view to External.**
4. **Configure labels not visible to users.**
   See "To Configure Labels Not Visible to Users."

▼ To Configure Labels Not Visible to Users

Note – This procedure tells you to disable information labels because information labels are not of much use if they are not visible, and, unless ILs are disabled, the information label appears in printer output.

1. **Optional. If the Trusted Solaris software is not yet installed, make sure that the install team disables information labels during installation by choosing No from the Information Labels menu in the Configure Trusted Solaris dialog box.**
2. **After the system is running, disable ILs, if desired, by changing the enable ILs switch setting in the `/etc/system` file from 1 to 0.**
3. **When setting up user accounts using the User Manager, configure users to not see labels and to have only a single label in their label ranges.**
   a. **Set the default label view to External.**

b. Choose Yes from the Hide SLs menu.

c. If you have not disabled information labels system-wide, choose Yes from the Hide ILs menu.

d. Specify the account's Clearance equal to its Minimum SL.
With a single clearance and sensitivity label of INTERNAL_USE_ONLY, you would set the Clearance and the Minimum Label to INTERNAL_USE_ONLY.

2

Specifying Labels and Handling Guidelines for Printer Output 3

By default, labels are printed at the top and bottom of printer output, and labels and text are printed on banner and trailer pages that accompany each print job. This chapter gives the information needed to understand which labels and text are printed and to specify the fields on printer banner and trailer pages.

This chapter includes these topics:

This chapter also describes these procedures:

3

Labels on Body Pages

Figure 3-1 illustrates that, by default, any job sent to the printer is printed with the information label of the job (in this case, PUBLIC) at the top and bottom of every body page.

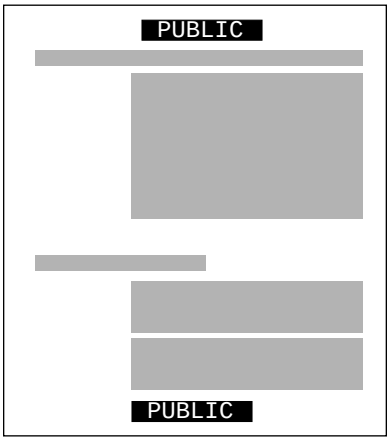


Figure 3-1 Information Label Automatically Printed on Body Pages

If information labels are disabled in the `system(4)` *file, then the job's sensitivity label is printed instead.*

The security administrator can change the defaults so that the sensitivity label or another label or no label is printed instead of the information label (see "Changing Default Labels on Print Jobs and Labels and Text on Printer Banner / Trailer Pages" on page 75).

Labels, Text, and Handling Caveats on Banner and Trailer Pages

Banner and trailer pages are automatically created for each print job. The banner/trailer pages are printed with company-specific handling guidelines that may be associated with certain words in the job's label. The fields and the text that are printed on the printer banner page are shown in Figure 3-2 on page 74. The callouts show the names of the labels and strings that appear on the banner/trailer page unless the security administrator role has changed the defaults. Changing the defaults and the terms "Protect as" classification, "access_related" words, CHANNELS and PRINTER BANNERS are explained in "Changing Default Labels on Print Jobs and Labels and Text on Printer Banner/Trailer Pages" on page 75.

The *text* that appears on the banner and trailer pages is affected by whether information labels are enabled for the system:

If information labels are disabled in the `system(4)` *file, then both the information label and the introductory text,* The system has labeled this data*:, are not printed and the space is left blank.*

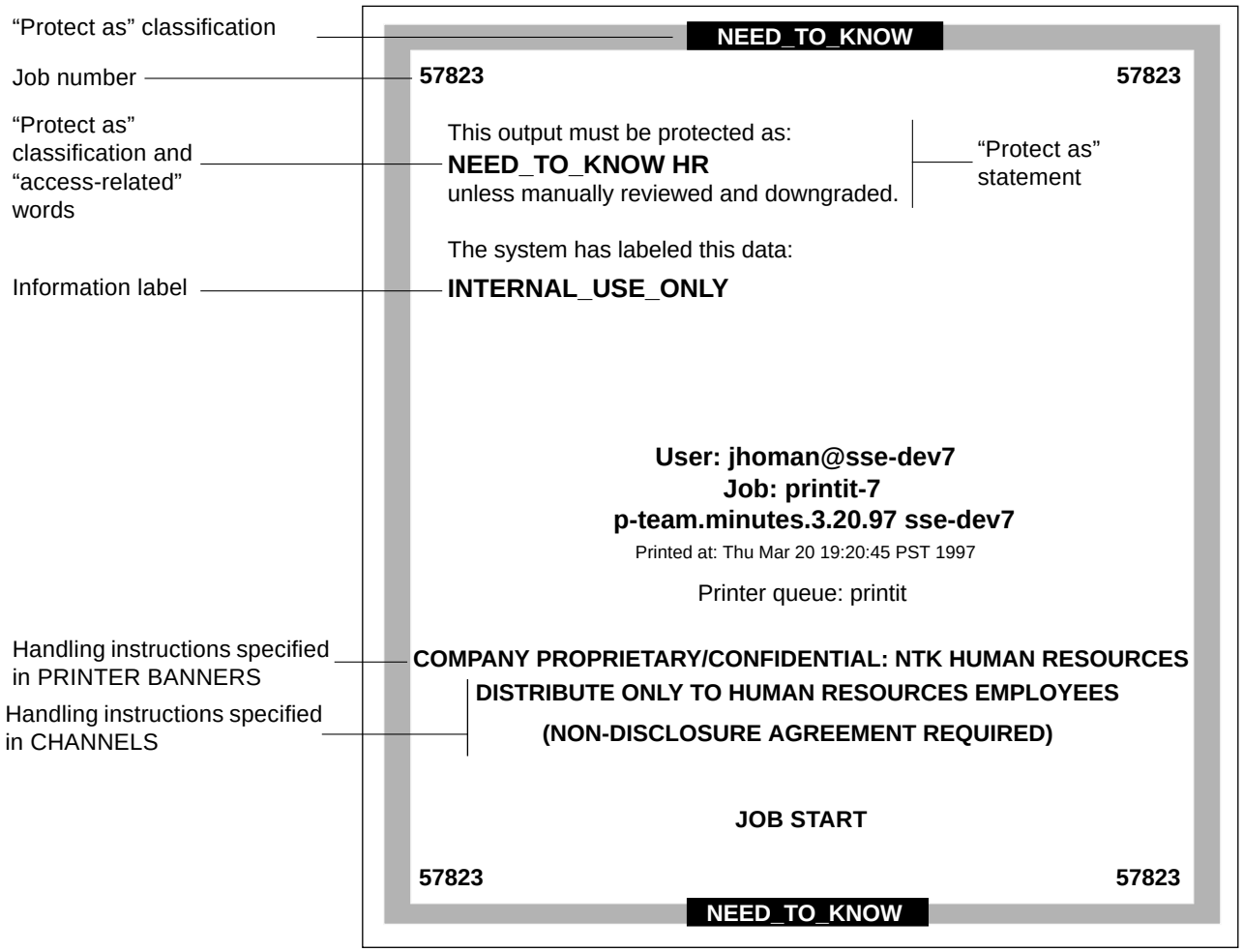


Figure 3-2 Typical Print Job Banner Page

Figure 3-3 shows the parts of the trailer pages that are different than they are on the banner pages. On the trailer page, a thick black line is used as a frame instead of the thicker gray frame that is printed on the banner page, and the page type identifier changes from JOB START to JOB END.

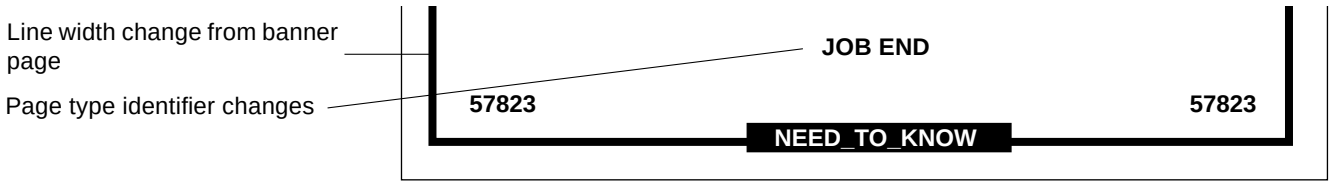


Figure 3-3 Differences on Trailer Pages

Changing Default Labels on Print Jobs and Labels and Text on Printer Banner/Trailer Pages

All the text and the labels and warnings that appear on print jobs are site-configurable; the security administrator may modify the `tsol_separator.ps` file in `/usr/lib/lp/postscript` directory to do the following:

- Internationalize the text on the banner and trailer pages
- Specify alternate labels to be printed in the various fields of the banner and trailer pages or at the top and bottom of body pages, or
- Change or omit any of the text or labels

The most-common substitution that sites choose to make is to specify that the sensitivity label prints instead of the information label at the top and bottom of banner pages. See "To Specify SLs to Print Instead of ILs on Body Pages," in Chapter 14 of the *Trusted Solaris Administrator's Procedures* manual. For how to do any other customizations or internationalization, see the comments in the `tsol_separator.ps` file in the `/usr/lib/lp/postscript` directory for how to make these changes. See also "Labels, Job Numbers, and Handling Information Printed on Banner and Trailer Pages" on page 358 of the *Trusted Solaris Administrator's Procedures* manual.

3

Specifying the Protect As Classification

The *protect as classification* shown on the banner page in Figure 3-2 on page 74 is NEED_TO_KNOW. The *protect as classification* is printed on the top and bottom of banner and trailer pages and is also included in the middle of the *protect as statement* along with *access-related words* from the job's sensitivity label and information label on the banner and trailer pages.

Figure 3-4 shows the minimum protect as classification defined in the ACCREDITATION RANGE section of the `label_encodings` file (which is the definition used in the "Example of How the Minimum Protect As Classification is Used" on page 76).

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

Figure 3-4 Example minimum protect as classification from a `label_encodings` File

In most cases the security administrator should simply specify the minimum protect as classification equal to the site's lowest defined classification. Your site needs to specify a minimum protect as classification whose value is higher than your lowest classification only in the following case:

- If your site's security policy requires that all printer output must be protected at least at the specified minimum classification (even if the sensitivity label of a print job has a lower classification)

Decision to Make Before Starting

- **Based on your site's security policy, decide whether to set a minimum protect as classification higher than the classification with the lowest value.**

Example of How the Minimum Protect As Classification is Used

In the example shown in Figure 3-5 on page 77, the protect as classification NEED_TO_KNOW is printed at the top of the banner page, and the Protect As field reads: This output must be protected as: followed by the protect as classification, NEED_TO_KNOW, followed by access-related words, followed by: unless manually reviewed and downgraded.

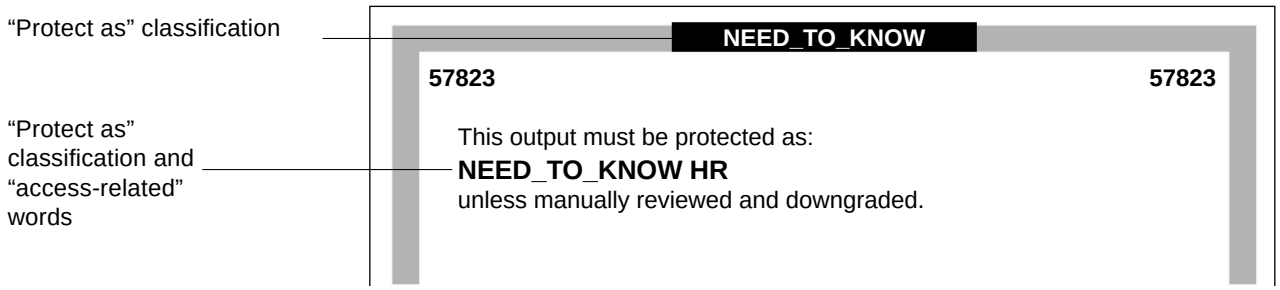


Figure 3-5 Classification Printed on Banner and Trailer Pages

The *protect as* classification is computed as shown in Figure 3-6. Figure 3-7 on page 78 illustrates how the rule is applied.

RULE FOR COMPUTING THE CLASSIFICATION
If the classification part of the print job's sensitivity label dominates the minimum protect as classification, print the classification from the job's sensitivity label. If not, print the minimum protect as classification.

Figure 3-6 Rule for computing the classification printed on banner / trailer pages

Figure 3-7 on page 78 shows an example in which the sensitivity label on the user's print tool is INTERNAL_USE_ONLY (shown in the window label with the short name for the classification, INTERNAL), and the minimum protect as classification defined in the `label_encodings` file is NEED_TO_KNOW. Because the minimum protect as classification dominates the classification portion of the print job's sensitivity label, the NEED_TO_KNOW classification is printed on the banner and trailer pages—even though INTERNAL_USE_ONLY is the actual classification of the print job's sensitivity label.

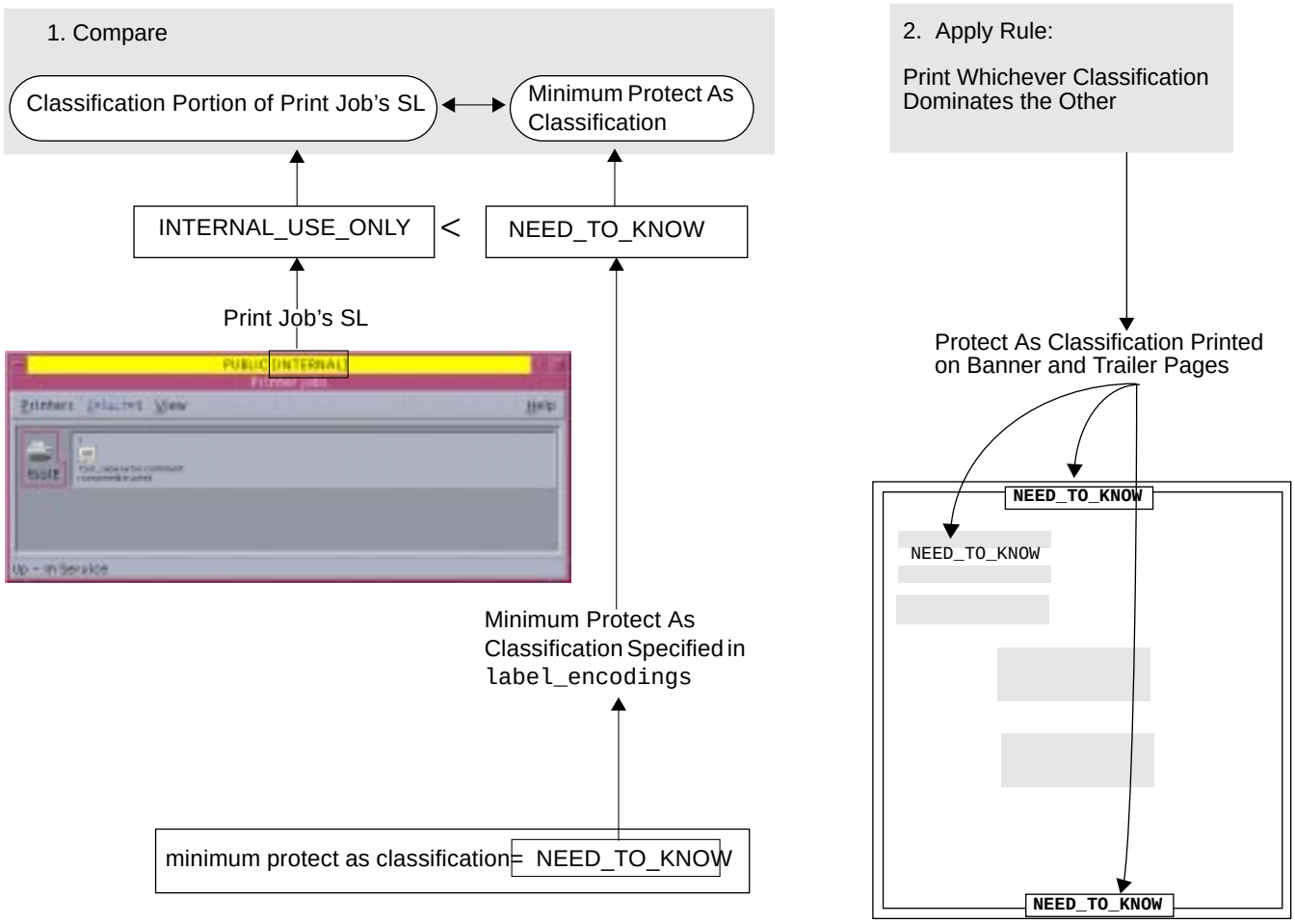


Figure 3-7 How the Classification Printed on Banner and Trailer Pages is Derived

For another example, a site with INTERNAL_USE_ONLY as the minimum protect as classification has the three classifications with the values shown in the first two columns Table 3-1. The third column shows the protect as classification printed on the banner/trailer pages for the print job when the classification on the left is in the job's sensitivity label.

Table 3-1 Example: Minimum Protect As Classification's Effects on the Protect As Classification

Classification	Value	Protect As Classification Printed on Banner/Trailer Pages for Print Job
PUBLIC	1	INTERNAL_USE_ONLY
INTERNAL_USE_ONLY	2	INTERNAL_USE_ONLY
NEED_TO_KNOW	3	NEED_TO_KNOW

As shown in Table 3-1, any print job whose sensitivity label includes either the PUBLIC or the INTERNAL_USE_ONLY classification would have INTERNAL_USE_ONLY printed in the "Protect as statement" and at the top and bottom of banner/trailer pages, and any print jobs whose label includes the NEED_TO_KNOW classification would have NEED_TO_KNOW printed in the same locations.

How Access Related Words are Determined

Access related words are printed in the protect as field on the banner/trailer pages along with the print job's protect as classification. In *sensitivity labels*, access-related words are understood to be any *compartments* in the label. For example, in Figure 3-8, because all compartments are treated as access-related, the compartment HR that from the print job's sensitivity label is printed along with the protect as classification.

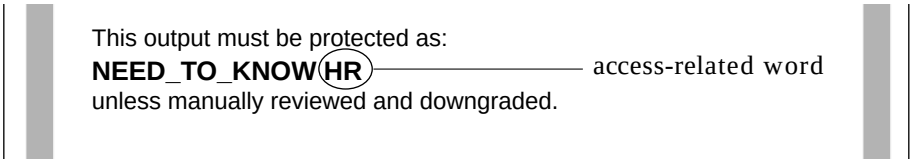


Figure 3-8 Classification Printed on Banner and Trailer Pages

In *information labels*, *compartment* or *marking* words may be access-related, but only if they are defined with the *access related;* keyword in the INFORMATION LABELS WORDS section of the `label_encodings` file. Figure 3-9 shows how some information labels words are assigned the access related; keyword in the default `label_encodings` files.

```
name= project x;  sname= px;    minclass=  C;                    markings= 14;
        suffix= LIMDIS; access related; flags= 3;
name= project y;  sname= py;    minclass=  C;                    markings= 6;
        suffix= LIMDIS; access related;
name= org x;      sname= ox;    minclass=  C;                    markings= 9;
        prefix= ORCON;  access related;
name= org y;      sname= oy;    minclass=  C;                    markings= 15;
        prefix= ORCON;  access related;
name= D/E;                      minclass=  C;                    markings= 16;
                        access related;
name= all eyes;         access related;                          markings= 8 10;
name= p1;                                                        markings= 8;
        suffix= eyes only; access related;
name= p2;                                                        markings= 10;
        suffix= eyes only; access related;
name= WNINTEL;    sname= WN;    minclass=  C;                    markings= 7;
        iname= WINTEL;  access related;
name= WARNING;                  minclass=  C;                    markings= 7;
name= NOFORN;     sname= NF;    minclass=  C; compartments= 4-5; markings= 11 13;
                        access related;
```

Figure 3-9 Information Labels Words Defined as Access-Related

How the Information Label is Used on Banner/Trailer Pages

On banner/trailer pages, the text, The system has labeled this data:. is followed by the information label of the print job. Some sites use this field when deciding whether to downgrade the sensitivity label of a document to match its information label. If information labels are disabled in the `system(4)` file at a site, then the text and the information label are not printed and the information label field is left blank.

Note – This information label field is not affected by the setting of hide ILs for the user or role account that sent the print job to the printer.

How Printer Banners are Configured

The printer banners field is the first line (or lines) that may appear in the handling caveats in the lower third of the banner and trailer pages.

At commercial sites, you can associate any text you choose in the PRINTER BANNERS section with any compartment bit you choose, as long as the compartment bit is also assigned to a word in the INFORMATION LABELS and SENSITIVITY LABELS section of the `label_encodings` file. The printer banner is the line that reads COMPANY PROPRIETARY / CONFIDENTIAL: NTK HUMAN RESOURCES in the example in Figure 3-10.

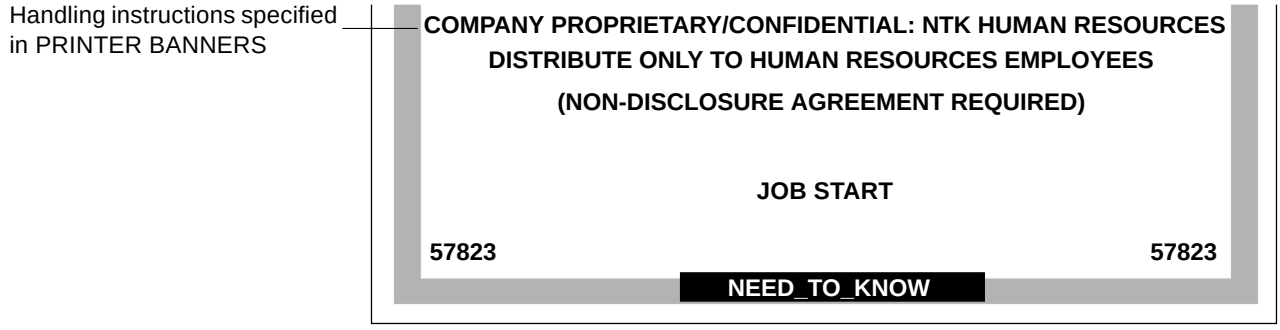


Figure 3-10 Commercial Use of the PRINTER BANNERS Specification on the Print Job's Banner Page

By convention, in government installations, the printer banner line of the banner page is specified to display any caveats that are associated with the *subcompartments* of the job's sensitivity label and with the *markings* of the job's information label. Figure 3-11 on page 82 shows a typical PRINTER BANNER at a government installation. The string (FULL SA NAME) could be any string of letters that meets the site's requirements.

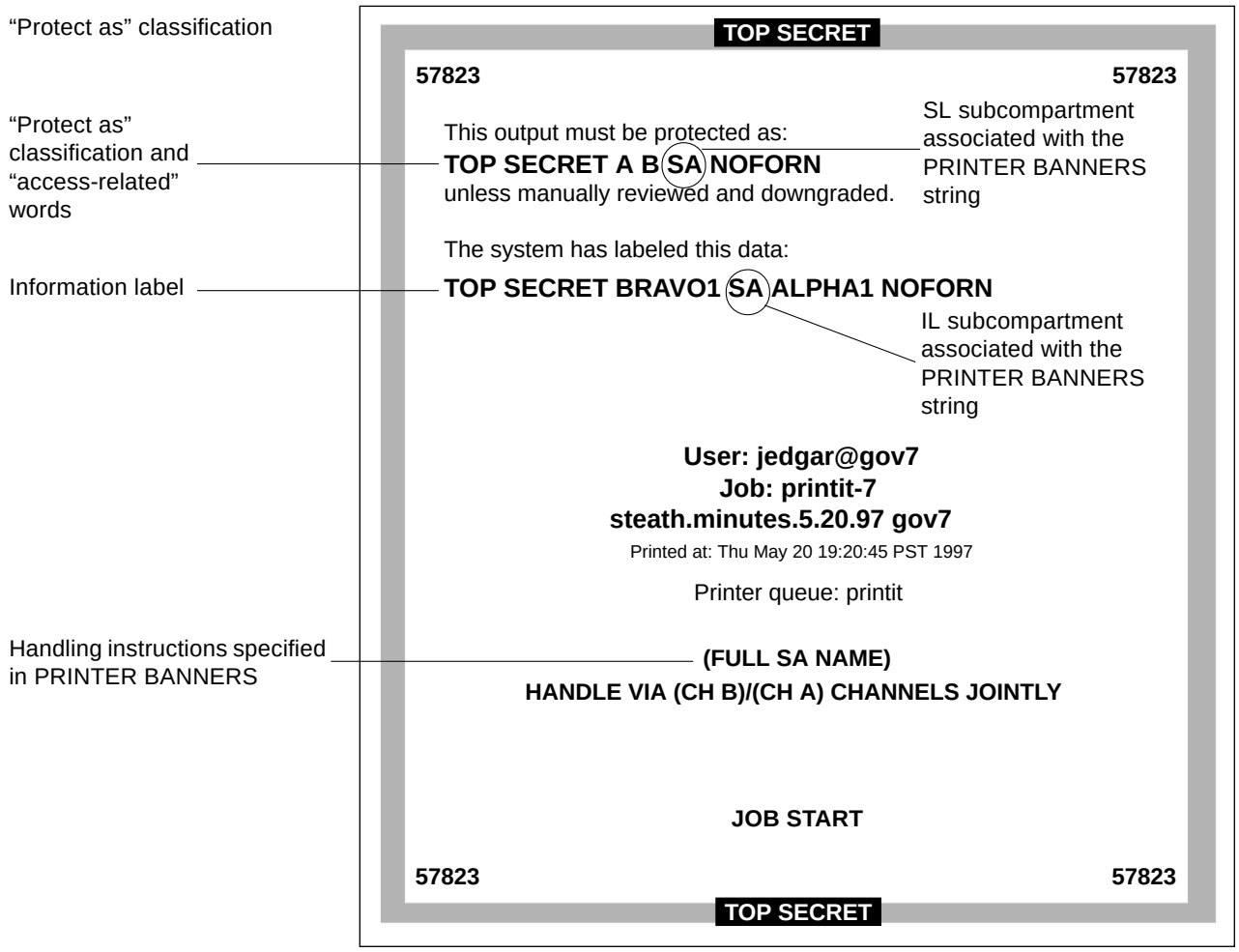


Figure 3-11 Government Use of the PRINTER BANNERS Section of the Banner Page

This discussion shows how the encodings are done that cause the printer banner line (FULL SA NAME) to be printed on the banner page shown in Figure 3-11 on page 82.

First, as shown in Figure 3-12, the word (FULL SA NAME) is associated in the PRINTER BANNERS section of the `label_encodings` with compartment bit 2.

```
PRINTER BANNERS:

WORDS:

name= ORCON;                    prefix;

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

Figure 3-12 Example: PRINTER BANNERS Specification in the `label_encodings` File

Figure 3-13 on page 84 shows the INFORMATION LABELS and SENSITIVITY LABELS definitions for the same compartments and markings used in the PRINTER BANNER definitions in Figure 3-12. Figure 3-13 shows that compartment bit 2 is associated with the subcompartment word SA for both sensitivity and information labels.

Therefore, the printer banner line is (FULL SA NAME) because:

- The sensitivity label and information label of the print job both contain the subcompartment word SA
- Compartment bit 2 is associated with the subcompartment word SA for both sensitivity and information labels
- Compartment bit 2 is associated with the string (FULL SA NAME) in the PRINTER BANNER encodings

```
INFORMATION LABELS:

WORDS:
  .
  .
  .
name= ORCON;      sname= OC;    prefix;

name= SA;           minclass= TS; compartments= 0 2; markings= 7;
name= SB;           minclass= TS; compartments= 1 3; markings= 7;
name= org x;      sname= ox;    minclass=  C;  markings= 9;
        prefix= ORCON;  access related;
name= org y;      sname= oy;    minclass=  C; markings= 15;
        prefix= ORCON;  access related;
  .
  .
  .
SENSITIVITY LABELS:

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

Figure 3-13 Information Labels and Sensitivity Labels WORDS associated with PRINTER BANNERS definitions in Figure 3-10 on page 81

Table 3-2 on page 85 provides a planning table for PRINTER BANNERS.

Table 3-2 PRINTER BANNERS Planning Table

When this/these subcompartment/compartment bit(s) and marking bit(s) are in the print job's CMW label	Print this Prefix	Print this Word	Print this Suffix
IL: name= SA; compartments= 0 2; markings= 7;SL: name= SA; compartments= 2;	—	(FULL SA NAME)	—

How Channels Are Configured

The main compartments in sensitivity labels are also called *channels*. The channels are the line (or lines) that may appear below the printer banner line(s) in the handling caveats in the lower third of the banner and trailer pages. The `CHANNELS` section in the `label_encodings` file can be specified to print any string in the channels part of the printer banner page whenever the sensitivity label of a print job contains a certain compartment.

The channels are the lines that read DISTRIBUTE ONLY TO HUMAN RESOURCES EMPLOYEES (NON-DISCLOSURE AGREEMENT REQUIRED) in the example in Figure 3-14. At commercial sites, it is possible to specify any text you want to appear in the CHANNELS section with any compartment bit you choose.

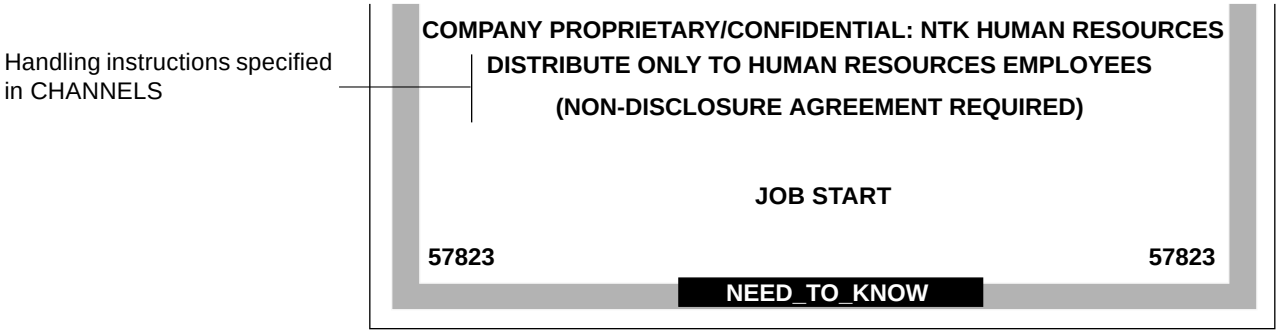


Figure 3-14 Commercial Use of the CHANNELS Specification on the Print Job's Banner Page

In government installations, the channels line(s) of the banner page conventionally are specified to display any caveats that are associated with the *compartments* of the job's sensitivity label. Figure 3-15 on page 88 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 discussion in this section explains and illustrates how the CHANNELS string HANDLE VIA (CH B)/(CH A) CHANNELS JOINTLY is specified to be printed on the banner page for a job with the compartment words A and B in the sensitivity label and the compartment words BRAVO1 and ALPHA1 in the information label. For the purpose of the example, only (CH A) and (CH B) apply, but since the compartment bit for a third channel (CH C) is included in their definitions, (CH C) is also mentioned in this discussion.

The explanation gets fairly complicated because:

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

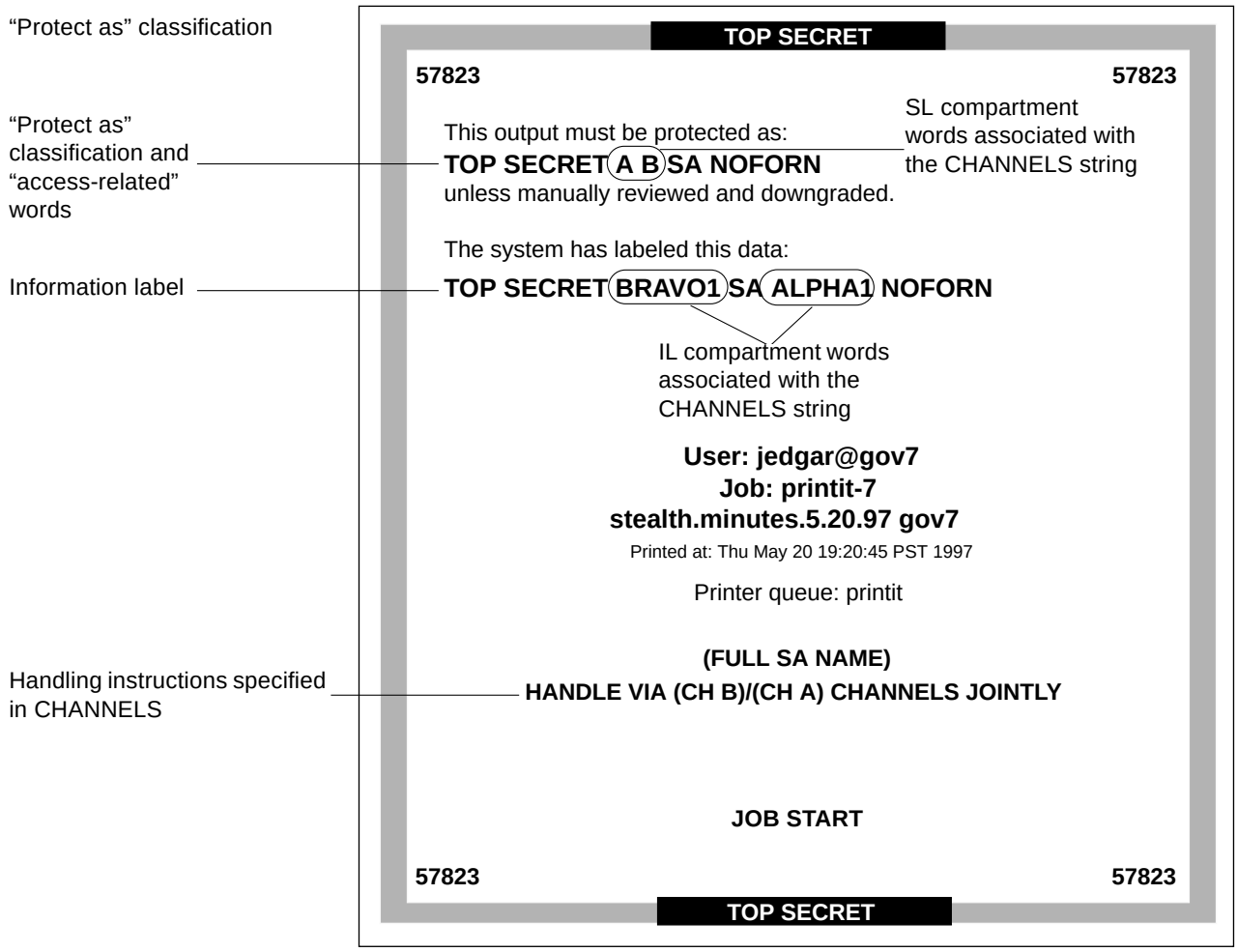


Figure 3-15 Government Use of the CHANNELS Specification on the Print Job's Banner Page

As shown in Figure 3-16, two suffixes CHANNELS JOINTLY and CHANNELS ONLY and a prefix HANDLE VIA are defined to be used in the encodings for the CHANNELS words.

```
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;
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;
```

Figure 3-16 Suffixes and Prefixes Defined in the CHANNELS Section in a Government `label_encodings` File

Following the prefixes and suffixes definitions in Figure 3-16, the channel names (CH A) and (CH B) and (CH C) are specified in two different ways to achieve these following results:

- Whenever any one of the three compartment bits that associated with channels is in the job's label, the HANDLE VIA: suffix is printed
- When only one of the three compartment bits (0, 1, or 6) that are associated with channels is in the job's label, the CHANNELS ONLY suffix is printed followed by the specified channel name (CH A), (CH B), or (CH C).
- When more than one compartment bit (0, 1, or 6) associated with channels is in the job's label, the specified channel names are printed after the suffix, separated by a slash (/) followed by the CHANNELS JOINTLY suffix.

The first three lines that define CHANNELS words in Figure 3-16 are repeated in Figure 3-17 to focus on how (CH A), (CH B), and (CH C) are encoded to appear with the CHANNELS ONLY suffix:

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

```
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;
```

Figure 3-17 CHANNELS ONLY Suffix Defined to Appear Alone with Individual Channels

The result of the first three lines of channel name definitions in the CHANNELS section shown in Figure 3-17 is that the HANDLE VIA prefix and the CHANNELS ONLY suffix are printed when *one* of the words associated with bits 0, 1, and 6 elsewhere in the `label_encodings` is in the job's label. The HANDLE VIA suffix and CHANNELS ONLY suffix are printed:

- With the (CH A) channel word when compartment bit 0 is turned on in the label and when compartment bits 1 and 6 are off
- With the (CH B) channel word when compartment bit 1 is turned on in the label and when compartment bits 0 and 6 are off
- With the (CH C) channel word when compartment bit 6 is turned on in the label and when compartment bits 0 and 1 are off

The last three lines that define CHANNELS WORDS in Figure 3-16 are repeated in Figure 3-18 to show 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 automatically put between the channels names when more than one of the bits defined in the channels section is in the job's sensitivity label.

```
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;
```

Figure 3-18 Encodings for More Than One Channel in the CHANNELS Section in a Government `label_encodings` File

The CHANNELS specification is one example of the importance of order when compartments are being encoded. The first three lines shown in Figure 3-17 on page 90 have already taken care of the cases when only one of the channels compartment bits is turned on, so the last three lines can take care of 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. Because any cases where any of the channels words appears in the job's label by itself have already been taken care of, 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 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 either of bit 0 or 6 or both are also turned on and
- (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

Figure 3-19 shows the information labels and sensitivity labels words associated with compartment bit 6. Figure 3-19 shows that compartment bit 6 is associated with the information labels words CC and SYSHI and with the sensitivity label word CC.

```
INFORMATION LABELS:

WORDS:
  .
  .
  .
name= CC;                    minclass= TS; compartments= 6;   markings= 7;
  .
name= SYSHI;                 minclass= TS; compartments= 0-6; markings= 0-16;
  .
SENSITIVITY LABELS:

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

Figure 3-19 Information Labels and Sensitivity Labels WORDS associated with Compartment Bit 6

Figure 3-20 shows that compartment bit 1 is associated with the information labels words SB, bravo1, bravo2, bravo3, bravo4, B, and SYSHI and with the sensitivity labels word B.

```
INFORMATION LABELS:

WORDS:
  .
  .
  .
name= SB;                       minclass= TS; compartments= 1 3; markings= 7;
name= bravo1;     sname= b1;    minclass= TS; compartments= 1;   markings= 3-4 7 12;
name= bravo2;     sname= b2;    minclass=  S; compartments= 1;   markings= 3 7 12;
name= bravo3;     sname= b3;    minclass=  S; compartments= 1;   markings= 5 7;
name= bravo4;     sname= b4;    minclass=  S;
                                maxclass=  S; compartments= 1;   markings= 3 7  ~12;
name= B;                        minclass=  C; compartments= 1;   markings= 7;
  .
  .
name= SYSHI;                    minclass= TS; compartments= 0-6; markings= 0-16;
  .
  .
  .
SENSITIVITY LABELS:

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

Figure 3-20 Information Labels and Sensitivity Labels WORDS associated with Compartment Bit 1

Figure 3-21 shows that compartment bit 0 is associated with information labels words SA, alpha1, alpha2, alpha3, A and SYSHI and with sensitivity labels word A.

```
WORDS:
   .
   .
   .
name= SA;                        minclass= TS; compartments= 0 2; markings= 7;
name= alpha1;     sname= a1;     minclass= TS; compartments= 0;   markings= 0-2 7;
name= alpha2;     sname= a2;     minclass=  S; compartments= 0;   markings= 0-1 7;
name= alpha3;     sname= a3;     minclass=  S; compartments= 0;   markings= 0 7;
name= A;                         minclass=  C; compartments= 0;   markings= 7;
   .
   .
   .
name= SYSHI;                     minclass= TS; compartments= 0-6; markings= 0-16;
   .
   .
   .
SENSITIVITY LABELS:

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

Figure 3-21 Information Labels and Sensitivity Labels WORDS Associated with Compartment Bit 0

To sum up the encodings, the channels line in the example is HANDLE VIA (CH B)/(CH A) CHANNELS JOINTLY because:

- HANDLE VIA is defined to always appear with any of the defined CHANNELS words
- The sensitivity label has two access-related words, A and B. that are associated with two compartment bits 0 and 1.
- The information label has two words BRAVO1 and ALPHA1 associated with two compartment bits 0 and 1.
- Because two of the bits defined for CHANNELS words appear in the job's label, the CHANNELS WORDS (CH A) and (CH B) are followed by CHANNELS JOINTLY

Any words to come before the channel name should be specified as *prefixes* and any words to come after the channel name should be specified as *suffixes*.

Table 3-3 CHANNELS Planner (for Prefixes, Channels, and Suffixes)

When This/These Compartment Bit(s) are 0n	Print This Prefix	Print This Channel	Print This Suffix
18	DISTRIBUTE ONLY TO	ENGINEERING	(NON-DISCLOSURE AGREEMENT REQUIRED)
0	HANDLE VIA	(CH A)	CHANNELS ONLY
0 1	HANDLE VIA	(CH A)/(CH B)	CHANNELS JOINTLY

Procedures

▼ To Configure PRINTER BANNERS

Note – See "How Printer Banners are Configured" on page 81, if necessary, before you start. Plan what printer banners line you want to associate with any of the words defined in the INFORMATION LABELS and SENSITIVITY LABELS sections of the `label_encodings` file, using Table 3-2.

1. **If necessary, use the Edit Encodings action to open the `label_encodings` file for editing as described in "To Modify the label_encodings (4TSOL) File" on page 60 of Chapter 2.**
2. **Find the PRINTER BANNERS section of the file.**

```
PRINTER BANNERS:

WORDS:
```

3. **Enter any prefixes or suffixes to associate with the WORDS in the printer banner line(s) of banner/trailer pages.**

```
PRINTER BANNERS:

WORDS:

name= ORCON;                    prefix;
```

4. **Enter the names of words to associate with any already-defined compartments in sensitivity labels or information labels, or with any already-defined markings in information labels, and specify any defined prefixes or suffixes as desired.**

```
name= (FULL SB NAME);                              compartments= 3
name= (FULL SA NAME);                              compartments= 2
name= org x;                 prefix= ORCON;           markings= 9;
name= org y;                prefix= ORCON;           markings= 15;
```

▼ To Configure CHANNELS

Note – See "How Channels Are Configured" on page 86, if necessary, before you start. Plan what channels line you want to associate with any of the words defined in the INFORMATION LABELS and SENSITIVITY LABELS sections of the `label_encodings` file, using Table 3-3.

1. **If necessary, use the Edit Encodings action to open the `label_encodings` file for editing as described in "To Modify the label_encodings (4TSOL) File" on page 60 of Chapter 2.**

2. **Find the CHANNELS section of the file.**

```
CHANNELS:

WORDS:
```

3. **Enter any prefixes or suffixes to associate with the WORDS in the CHANNELS line(s) of banner/trailer pages.**

```
CHANNELS:

WORDS:

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

4. **Enter the names of words to associate with any already-defined compartments in sensitivity labels or information labels, and specify any defined prefixes or suffixes as desired.**

```
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;
```

3

Modifying Sun's Extensions in the Local Definitions Section

4

This chapter describes what the security administrator needs to know to define the values in the LOCAL DEFINITIONS section of the Trusted Solaris `label_encodings` file. This chapter includes these topics:

This chapter includes these procedures:

4

Default LOCAL DEFINITIONS Section

Trusted Solaris operations require additional keywords beyond those defined in the government-furnished *Compartmented Mode Workstation Labeling: Encodings Format*. Figure 4-1 shows the LOCAL DEFINITIONS section of the default `label_encodings` file.

```
LOCAL DEFINITIONS:
*
*   The names for the administrative high and low name are set to
*   site_high and site_low respectively by the example commands below.
*
*   NOTE:  Use of these options could lead to interoperability problems
*   with machines that do not have the same alternate names.
*
*Admin Low Name=  site_low;
*Admin High Name= site_high;

default flags= 0x0;
forced flags= 0x0;

Default Label View is External;
Float Process Information Label;

Classification Name= Class;
Compartments Name= Comps;
Markings Name= Marks;

COLOR NAMES:

    label= Admin_Low;color= #bdbdbd;

    label= u;color= green;
    label= c;color= blue;

    label= s;color= yellow;
    label= ts;color= red;

    word= sb;color= cyan;
    word= cc;color= magenta;

    label= Admin_High;color= #636363;
* End of local site definitions
```

Figure 4-1 `LOCAL DEFINITIONS` section of `label_encodings` file

Values Specified in the LOCAL DEFINITIONS Section

The security administrator specifies the following options using keywords in the LOCAL DEFINITIONS section:

- Alternate names for administrative labels.

  See “To Change the Names of Administrative Labels” on page 108

- A default Label View that sets the system-wide default that determines whether users see the names of administrative labels

  See “To Specify the System-wide Viewing of Administrative Label Names” on page 109 or “To Specify the System-wide Viewing of Substitute Names for Administrative Labels” on page 109.

- Optional flags that will be made available to software that may want to use them, of either of these two types:
  - Default flags that will apply to the translation if none are specified with the command that is manipulating the labels

    See “To Specify Default Flags” on page 110.
  - Forced flags that will apply to all translations

    See “To Specify Forced Flags” on page 110.

- Alternate names for classifications, compartments, and markings to be used on graphical user interface (GUI) dialog boxes

  See “To Change Label Component Names Used in Window Tools” on page 111.

- Colors that display on windows depending on the sensitivity label on the window

  See “To Assign a Color to a Label or Word” on page 111.

For more details on Trusted Solaris extensions to the label encodings keywords, see `label_encodings(4TSOL)`.

Note – The `Default Label View`, and `Flags` keywords can be specified in any order but must be specified before the `Color Names` section.

4

Changing the Names of Administrative Labels

The LOCAL DEFINITIONS: section of the default `label_encodings` file provides two commented-out lines that the site's security administrator may activate and possibly edit to substitute alternative ASCII names for the administrative labels. See "Issues About the Names of Administrative Labels" on page 21 and "Changing the Administrative Labels' Names" on page 22 in Chapter 1, "Introduction to Trusted Solaris Label Encodings" for needed background. For the procedure, see "To Change the Names of Administrative Labels" on page 108.

```
*Admin Low Name= site_low;
*Admin High Name= site_high;
```

Specifying Whether Administrative Labels Display

Besides the option described in "To Change the Names of Administrative Labels" on page 108, which allows the security administrator to specify alternate names for administrative labels, another related option, the label view, lets the security administrator specify whether the names display at all.

As discussed in "Specifying Whether Users See Administrative Labels' Names" on page 22 of Chapter 1, "Introduction to Trusted Solaris Label Encodings," some companies or agencies do not want their employees to see the names of the administrative labels ADMIN_LOW or ADMIN_HIGH. Therefore, the Trusted Solaris system offers the option of setting a variable called the default label view for all non-administrative users and of toggling the view setting for individual users.

The default label view set in the `label_encodings` file is a system-wide value. The system-wide label view may be overridden by the label view assigned to individual user and role accounts; each account may have its own label view, or each account's label view may be set to be the same as the system-wide default. Programs are also able to set their own label views. How these various settings relate to each other is described in "The Hierarchy of Label View Settings" on page 24 of Chapter 1."

See "To Specify the System-wide Viewing of Administrative Label Names" on page 109 and "To Specify the System-wide Viewing of Administrative Label Names" on page 109.

Configuring Optional Flags

Flags may be assigned to words in the `label_encodings` file, so that the flags may be used by applications that you may write at your site to explicitly use them. If a flag is assigned to a particular word, and if that flag is given when a translation of a label that includes that word is requested, then the word will display even if the word would normally not display. For details on the `Flags=` keyword, see *Compartmented Mode Workstation Labeling: Encodings Format*.

If the default setting are not changed, no flags are set.

See "To Specify Default Flags" on page 110 and "To Specify Forced Flags" on page 110.

Changing the Names of Labels Components on Label Builders

The default names used in label builder dialog boxes in the window system for classifications and compartments and markings are shown in Figure 4-2.

```
Classification Name= Class;
Compartments Name= Comps;
Markings Name= Marks;
```

Figure 4-2 Default Names for Classifications, Compartments and Markings

Figure 4-3 on page 104 shows the names CLASS and COMPS used on the Session SL dialog box. A label builder for an information label uses the MARKS name on the Markings column.

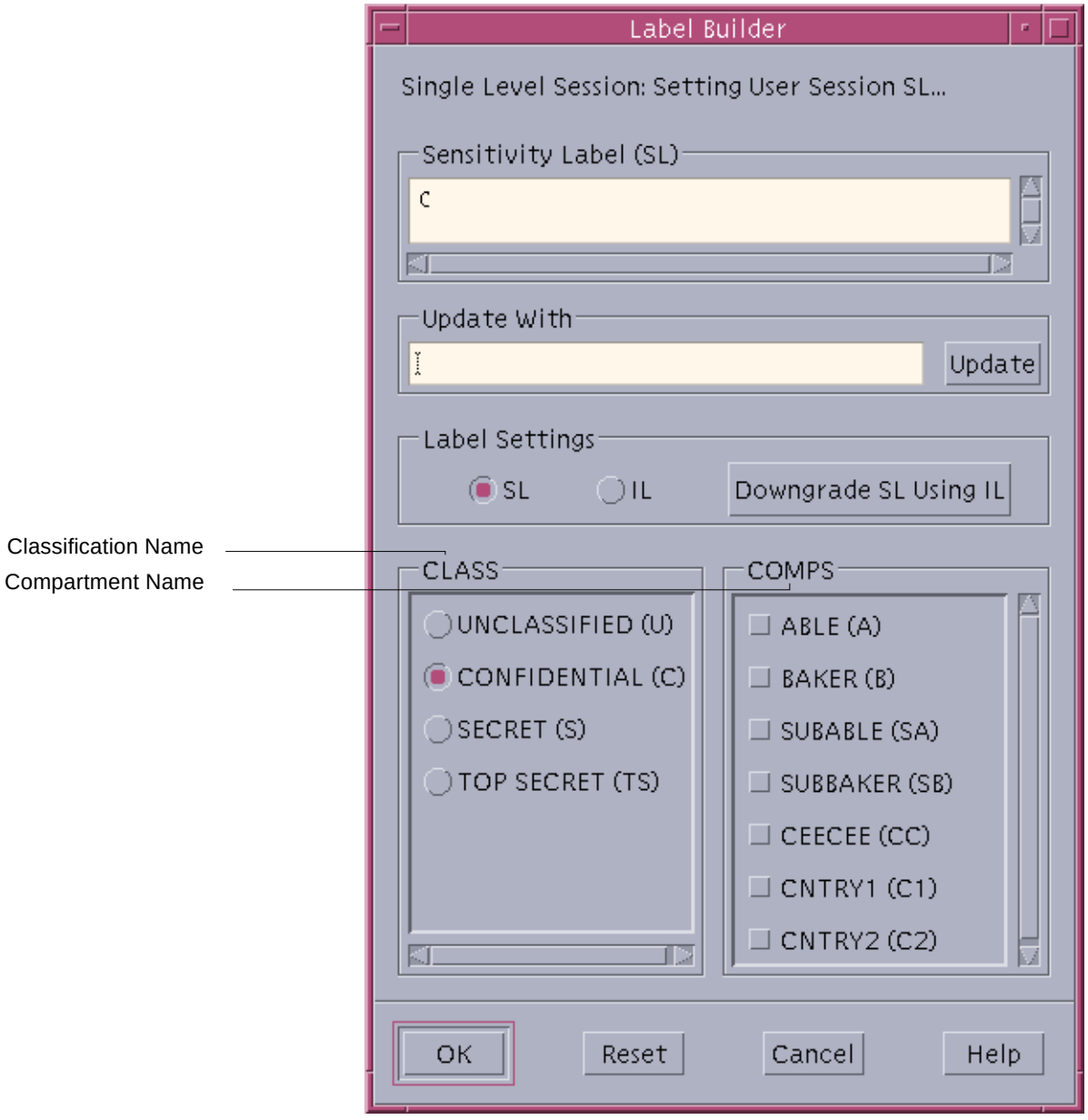


Figure 4-3 Session SL Dialog Box

See “To Change Label Component Names Used in Window Tools” on page 111.

Specifying Colors for Labels

In the COLOR NAMES part of the LOCAL DEFINITIONS: section, the COLOR NAMES: keyword is followed by zero or more color assignments. The default color values defined in Trusted Solaris `label_encodings` COLOR NAMES are shown in Figure 4-8 on page 108.

```
COLOR NAMES:

    label= Admin_Low;color= #bdbdbd;


    label= u;color= green;
    label= c;color= blue;

    label= s;color= yellow;
    label= ts;color= red;

    word= sb;color= cyan;
    word= cc;color= magenta;

    label= Admin_High;color= #636363;
*
* End of local site definitions
```

Figure 4-4 COLOR NAMES section in the LOCAL DEFINITIONS Section of `label_encodings` File

In this section the security administrator assigns colors to words and to labels, The *color name* can be either an ASCII color name or a hexadecimal color value to be associated with a *word or a label.* How to specify color values is discussed in “Color Values” on page 107. A full discussion of how to specify color is outside the scope of this manual. See also the discussion under “Color Specification” in the O‘Reilly and Associates, Inc. *XWindows Systems User’s Guide* (Vol. III), ISBN number 0-937175-29-3 for more information.

The color assigned to a label’s component displays as a background color whenever a sensitivity label includes the specified label components, according to the ordering rules described below. See Figure 4-5 on page 106 for an example of how the color is used. In the figure, the PUBLIC, INTERNAL, and NTK_SALES workspace buttons are colored differently from the standard workspace buttons.

Note – The windows software computes a complementary color for the lettering.

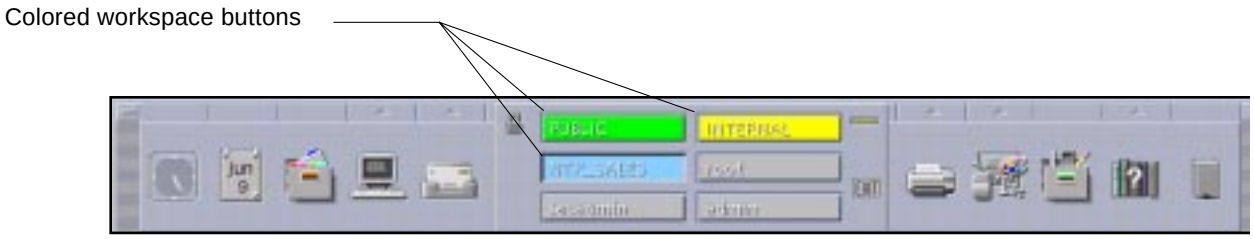


Figure 4-5 Window Label with a Background Color from the COLOR NAMES Section

Order of Color Specification

Colors are assigned to labels and to words within labels using the two following syntaxes:

```
word= label name;     color= color name;
or
label= label name;    color= color name;
```

The color used for any label is determined by the order of any defined entries that are part of the label.

1. If a label contains a compartment *word* that has one or more colors specified, 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, if any exact match exists for the label name, then the specified color is used.
3. If there is no exact match for the label, the color associated with the first specified `label=` value for the *classification* of the label is used.
4. If the classification has no color assigned, the color assigned to the first label that contains the same classification is used.

Following rule 3. in a system with the color definitions shown in Figure 4-6, the label TS A displays with a yellow background because yellow is the color assigned to the TS, classification.With the same definitions, any label with the

C classification displays with the color blue, unless the label also contains the word B, in which case it displays with the color orange. However, any label with the U classification always displays with the color green (because B is defined elsewhere in the encodings as having a minclass of C, so it never appears in the same label with the classification U).

```
        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;
```

Figure 4-6 Example 1 of Color to Word and Label Assignments

Following rule 4. in a system with the color definitions shown in Figure 4-7, TS A displays with the khaki background color because the TS classification did not have a color assigned, and TS SA is the only label that includes the TS classification and that has a color (khaki) assigned.

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

Figure 4-7 Example 2 of Colors Assigned to Words and Labels

Color Values

The `/usr/openwin/lib/rgb.txt` database translates ASCII color names into red, green, blue values. You can either refer to the `rgb.txt` file for color names to use for your site's labels or use hexadecimal 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 FFF; each of which indicates the amount of red, green, and blue present in the color. For example, pure red is #FF0000, pure green is #00FF00, pure blue is #0000FF, pure white is #FCFCFC, and pure black is #000000. The number of colors available on the screen depends on the amount of memory available for

specifying colors and number of color planes, on how many other window clients are using color cells, and whether private color maps are being used by other applications. To minimize conflicts you should use color *names*, or use hexadecimal color *values that you know have been specified for other applications that display without color flashing in the window environment*.

The default color values defined in Trusted Solaris `label_encodings` COLOR NAMES section have been chosen with these caveats in mind (see Figure 4-8).

```
label= Admin_Low;color= #bdbdbd;
label= u;color= green;
label= c;color= blue;
label= s;color= yellow;
label= ts;color= red;
word= sb;color= cyan;
word= cc;color= magenta;
label= Admin_High;color= #636363;
```

Figure 4-8 Default COLOR NAMES Assigned to Label Components

See “To Assign a Color to a Label or Word” on page 111

Procedures for Modifying Sun Extensions

▼ To Change the Names of Administrative Labels

1. **As security administrator in an ADMIN_LOW workspace, use the Edit Encodings action to open the `label_encodings` file.**
   See “To Modify the label_encodings (4TSOL) File” on page 60, if needed.

2. **Find the lines in the LOCAL DEFINITIONS section that define the administrative label names.**

```
*Admin Low Name= site_low;
*Admin High Name= site_high;
```

3. **Remove the asterisk (*) comment sign from the beginning of the lines that define the administrative names**

4. **Replace `site_low` and `site_high` with names that are consistent with your site's security policy, if desired.**

```
Admin Low Name= your_choice;
Admin High Name= your_choice;
```

5. **If you are done, save and close the file.**

▼ To Specify the System-wide Viewing of Administrative Label Names

1. **As security administrator in an ADMIN_LOW workspace, use the Edit Encodings action to open the `label_encodings` file.**
See "To Modify the label_encodings (4TSOL) File" on page 60, if needed.

2. **Find the lines in the LOCAL DEFINITIONS section that define the Default Label View.**

```
Default Label View Is Internal
```

3. **Ensure that the line that begins Default Label View is set to Internal as shown.**

4. **If you are done, save and close the file.**

▼ To Specify the System-wide Viewing of Substitute Names for Administrative Labels

1. **As security administrator in an ADMIN_LOW workspace, use the Edit Encodings action to open the `label_encodings` file.**
See "To Modify the label_encodings (4TSOL) File" on page 60, if needed.

2. **Find the lines in the LOCAL DEFINITIONS section that define the Default Label View.**

```
Default Label View Is Internal
```

3. **Ensure that the default label view is set to External, as shown below:**

```
Default Label View Is External
```

4. **If you are done, save and close the file.**

▼ To Specify Default Flags

1. **As security administrator in an ADMIN_LOW workspace, use the Edit Encodings action to open the `label_encodings` file.**
See "To Modify the label_encodings (4TSOL) File" on page 60, if needed.

1. **Find the line in the LOCAL DEFINITIONS section that defines the default flags.**

```
default flags= 0x0;
```

2. Specify a flag in hexadecimal format to be used by the label translation software if no other flag is specified as a parameter to a label translation:

`default flags=`*hexadecimal flagname*`;`

3. **If you are done, save and close the file.**

▼ To Specify Forced Flags

1. **As security administrator in an ADMIN_LOW workspace, use the Edit Encodings action to open the `label_encodings` file.**
See "To Modify the label_encodings (4TSOL) File" on page 60, if needed.

1. **Find the line in the LOCAL DEFINITIONS section that defines the forced flags.**

```
forced flags= 0x0;
```

2. Specify in hexadecimal form a flag to be used by the label translation:

```
forced flags=hexadecimal flagname
```

▼ To Change Label Component Names Used in Window Tools

1. **As security administrator in an ADMIN_LOW workspace, use the Edit Encodings action to open the** `label_encodings` **file.**
   See "To Modify the label_encodings (4TSOL) File" on page 60, if needed.

1. **Find the line in the LOCAL DEFINITIONS section that defines the labels components names used in label builder dialog boxes.**

```
Classification Name= Class;
Compartments Name= Comps;
Markings Name= Marks;
```

2. **If desired, change the defaults "Class," "Comps," and "Marks."**
   The example shows the alternate names used in `label_encodings`.simple

```
Classification Name= Classification;
Compartments Name= Departments;
Markings Name= Disclosure;
```

3. **If you are done, save and close the file.**

▼ To Assign a Color to a Label or Word

Note – It is important to define a color for each classification in the `COLOR NAMES` section of the `label_encodings` file. In a system with color monitors, if no color is defined for a classification, the default color used is black.

1. **As security administrator in an ADMIN_LOW workspace, use the Edit Encodings action to open the** `label_encodings` **file.**
   See "To Modify the label_encodings (4TSOL) File" on page 60, if needed.

1. **Find the section at the end of the LOCAL DEFINITIONS section that defines the names of colors used when labels display in the window system .**

```
COLOR NAMES:

        label= Admin_Low;       color= #bdbdbd;


        label= u;       color= green;
        label= c;       color= blue;

        label= s;       color= yellow;
        label= ts;      color= red;

        word= sb;       color= cyan;
        word= cc;       color= magenta;

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

2. **Optionally, define colors for individual compartment words.**
   If particular compartment words are important for your site to distinguish irrespective of the classification with which they may be associated, assign to those words a separate color.

```
word= EMG; color= RedOrange;
```

3. **Optionally, define colors for sensitivity labels.**
   In the example, the color assigned to `NEED TO KNOW SYSADM` is bluePurple.

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

4. **Make sure a color is defined for each classification.**
   When a label with a classification that is not included in any of the color definitions displays on a color monitor, the background color used is black. For this reason, make sure to always define every classification either as part

of a label definition or on its own as shown below. In the screen below, the classification REGISTERED is assigned the color red, and the NEED TO KNOW classification is assigned the color blue.

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

The three definitions combined mean that any label with the word EMG (for executive management group) always displays with the color RedOrange. The label NEED TO KNOW SYSADM always displays with the color orange. Any other label containing the NEED TO KNOW classification displays with the color blue (unless the label contains the word EMG). Any label with the REGISTERED classification displays with the color red, and any label with any classifications not defined displays with the color black.

```
word= EMG; color= RedOrange;
label= NEED TO KNOW SYSADM; color= bluePurple;
label=REGISTERED;  color= red;
label= NEED TO KNOW; color= blue;
```

5. If you are done, save and close the file.

4

Central Administration of Labels-related Files 5

This chapter reviews how the security administrator oversees the installation of the site's `label_encodings` file and the setting of the appropriate label-related kernel switches on the NIS+ master. This chapter reviews and expands the following topic, which is also covered in the *Trusted Solaris Installation and Configuration* manual, with specific attention to the labels-related aspects:

- How to set up network installations or Custom JumpStart so that identical copies of the `label_encodings` file are installed on all machines in the distributed system at the time of initial installation and configuration

This chapter also reviews how `label_encodings` and kernel switch settings may be changed and distributed to all hosts in the system.

- How to update the `system(4)` file, if the need arises
- How to use the remote distribution command to distribute copies of `label_encodings` and `system` files to all hosts.

This chapter includes the following major topics and procedures:

5

Label Configuration Review

The security administrator, as part of the install team, oversees the creation of the `label_encodings(4TSOL)` file on the NIS+ master machine. The security administrator also ensures that the desired system-wide label settings are made during installation on the NIS+ master server by ensuring that the install team selects the correct options on the Customize Trusted Solaris Configuration dialog box.

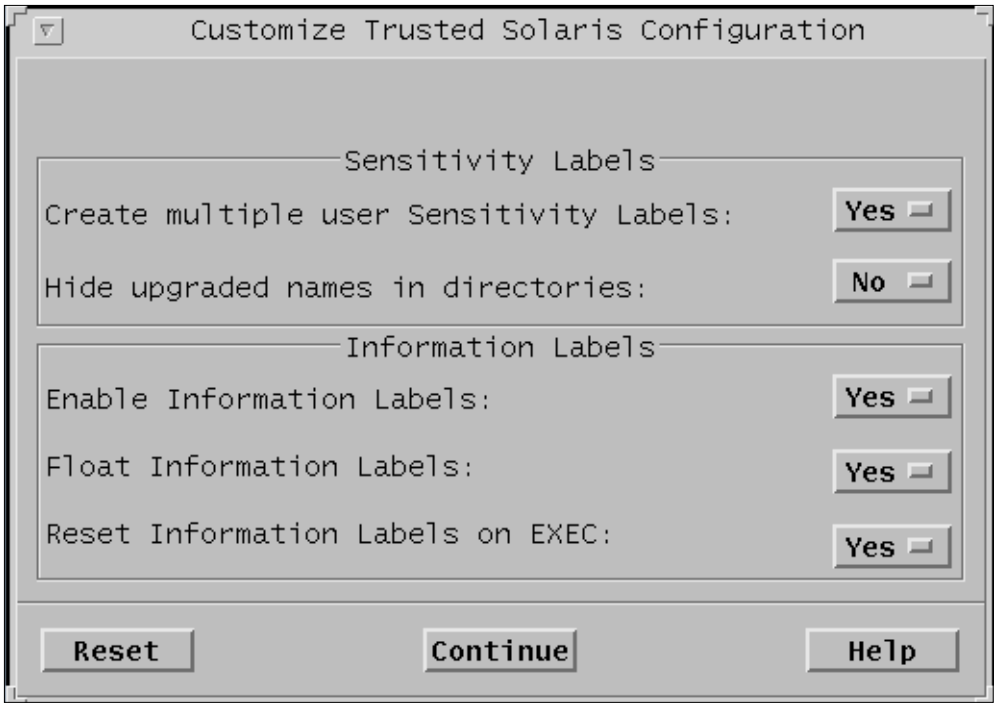


Figure 5-1 The Customize Trusted Solaris Configuration Dialog Box

- The answer to the first question in the Customize Trusted Solaris Configuration Dialog Box shown in Figure 5-1 affects which placeholder label_encodings file is installed.
  - When the answer to `Create multiple user Sensitivity Labels` is No, a `label_encodings` file with a single sensitivity label defined in the user accreditation range is installed.

- When the answer is `Create multiple user Sensitivity Labels` is Yes, a `label_encodings` file with multiple sensitivity labels is installed.

Note – Whether the single or multiple label file is installed, it serves as a placeholder that is almost always modified by the security administrator to specify the site's own set of labels.

The answers to the remaining four questions in the Customize Trusted Solaris Configuration Dialog Box determine the setting of Trusted Solaris-specific flags in the `/etc/system` file, as shown in Table 5-1.

Table 5-1 Configuration Options and Trusted Solaris Kernel Switch Settings

Option	Answer	tsol_ Switch Setting in the `/etc/system` File
`Hide upgraded names in directories`	Yes	tsol_hide_upgraded_names=1
	No	tsol_hide_upgraded_names=0
`Enable Information Labels`	Yes	tsol_enable_il=1
	No	tsol_enable_il=0
`Float Information Labels`	Yes	tsol_enable_il_floating=1
	No	tsol_enable_il_floating=0
`Reset Information Labels on EXEC`	Yes	tsol_reset_il_on_exec=1
	No	ttsol_reset_il_on_exec=0

Considerations When Deciding How to Ensure Label Encodings and Label-related Kernel Switch Settings are the Same on all Hosts

During initial setup of the Trusted Solaris distributed system, master copies of the `label_encodings` file and of the `system` file are installed on the NIS+ master. The security administrator is responsible for ensuring that the identical copies of the site's `label_encodings` and system files are also installed on all other hosts.

How these files are distributed to all NIS+ clients is determined by whether the NIS+ client host is installed by:

- Interactively installing from the Trusted Solaris CD with a tape copy of the master copy of the `label_encodings` at hand,

- Using Custom JumpStart™, or
- Using a network install

The method of installation you choose depends in turn on the number of machines you have to configure and on the number of types of configurations your site supports. For a site with a large number of machines that are configured the same, setting up Custom JumpStart installations may be worth the effort. For sites with fewer machines or with many varied configurations, JumpStart administration and setup is a less desirable alternative. In sites with fewer machines or many configurations, net installs may be set up so that the `label_encodings` and kernel switches (from the NIS+ master) are distributed automatically from a boot server using the new keyword in the `bootparams` file and the proper setup. In some cases the last option (sneakernet—carrying the configuration files to each host via tape or floppy) may be the only way to go.

Note – If you plan to use Custom JumpStart or net install for setting up NIS+ clients, you should consider using the new `tsolconfig` option in the `bootparams`(4) file, as described under "To Set Up a Boot Server to Distribute Label Information to All NIS+ Clients Doing Net Installations." Using the new `tsolconfig` option, you can make sure that your desired `label_encodings` and label configuration settings in the `system` file are distributed to every host during installation. If the `tsolconfig` option is not used, the Customize Trusted Solaris Configuration Dialog Box comes up during each installation and the questions have to be reanswered just as they were on the NIS+ master, after which the switch settings in the `system` file are set properly, and a placeholder `label_encodings` file is installed. You will then need to replace the placeholder `label_encodings` on every host.

▼ To Set Up a Boot Server to Distribute Label Information to All NIS+ Clients Doing Net Installations

1. **On a boot server, in the root role in an ADMIN_LOW workspace, create a directory for the Trusted Solaris configuration files.**

For example, the following command would create the directory called `tsolfiles` in the root file system:

```
$ mkdir /tsolfiles
```

2. **Create a `config_data` file that contains the answers the install team made during installation of the NIS+ master.**
   Figure 5-2 shows switches from the `/tsolfiles/config_data` file. The switches shown here correspond to the choices that the install team makes during installation on the Configure Trusted Solaris Options dialog box, as described in "Label Configuration Review" on page 117. During net install or Custom JumpStart, the settings in `config_data` will be used to set the labels-related kernel switches in the local `system` file

```
multiple_user_sl=yes
hide_upgraded_names=no
enable_il=yes
enable_il_floating=yes
rest_il_on_exec=yes
```

Figure 5-2 Sample `config_data` File

3. **Use the Share Filesystems administrative action from the System_Admin folder in the Application Manager to edit the `/etc/dfs/dfstab` file. Add the following entry:**

```
share -F nfs -o ro,anon=0 dir_path
```

   For example, the following entry would be correct for the example shown in Step 1:

```
share -F nfs -o ro,anon=0 /tsolfiles
```

4. **Enter `unshareall`.**

```
$ unshareall
```

5. **Enter** `shareall`.

```
$ shareall
```

6. **After the system administrator creates an install server, go to Step 7.** See the instructions for creating an install server or JumpStart server in *Trusted Solaris Installation and Configuration*.

7. **On the install server, use the Trusted Solaris version of the Solstice Database Manager to modify the** `bootparams` **file to add the following entry:**

```
* tsol_config=server:dir_path
```

Note – This new keyword entry is required in addition to the one that specifies the Custom JumpStart directory, if there is one.

In this entry:

*	Is a wildcard character specifying all workstations
server	Is the host name of the server where the Trusted Solaris configuration files are located
dir_path	Is the absolute path of the Trusted Solaris configuration directory on the server

For example, the following entry would enable all workstations to access the `/tsolfiles` directory on the boot server named `jasmine`:

```
* tsol_config=jasmine:/tsolfiles
```

8. **Update the NIS+ tables (if necessary) with the changes you made to the** `/etc/bootparams` **file:**

```
$  /usr/lib/nis/nispopulate -F -p /etc bootparams
```

5

Making Changes to Label Related Files After System Startup

Configuring the `label_encodings` file and specifying the Trusted Solaris-specific kernel switch settings that affect labels is also generally done only during initial installation and configuration of the system. However, both the `label_encodings` and the `/etc/system` switch settings may be changed after the system is running if the proper precautions are taken.

Changing the Label Encodings

On a running system, you run the risk of invalidating existing labels when you create new ones or modify old ones. To minimize the risk, limit yourself to these changes:

- Adding new classifications or words
- Changing the names of existing words
- Modifying the local extensions

Changing the Settings for the Trusted Solaris Labels-Related Switches in the `system` File

Figure 5-3 on page 123 shows the labels-related Trusted Solaris switches (with the comments removed) in the `system`(4) file that is in the `/etc` directory on each host. The label-related settings specified during installation of the NIS+ master are automatically used to update the `system` file that is installed. In most cases, the `system` file settings should be identical on every NIS+ client and standalone host in the Trusted Solaris distributed system.

```
tsol_enable_il=1

tsol_enable_il_floating=1

tsol_float_sysv_msg=0

tsol_float_sysv_sem=0

tsol_float_sysv_shm=0

tsol_hide_upgraded_names=0

tsol_reset_il_on_exec=1
```

Figure 5-3 Trusted Solaris Label-related Kernel Switches

The `tsol_float_sysv_*` variables are not set by the install team during installation. The default settings are off (0).

Note – See "To Find Out Which Privileges an Application Needs" on page 451 in Chapter 16 of the *Trusted Solaris Administrator's Procedures* for the complete set of steps to perform privilege debugging, which is enabled by the `tsol_privs_debug` switch, which is not shown in Figure 5-3.

▼ To Make Changes to Label-related Switches in the `system(4)` File

1. **As security administrator, use the Admin Editor action from the System_Admin folder in the Application Manager to open `/etc/system` for editing.**
2. **To turn on or off the variable for enabling information labels, find `tsol_enable_il=` and set the value to 1 (on) or 0 (off).**
   Because the switches for information label floating and for the reset of the information label when a new program is executed are looked at only when the switch shown in Step 2 is set to 1, do either of Step a or Step b only if you have enabled information labels.

a. **To turn on or off the variable for enabling information label floating, find** `tsol_enable_il_floating=` **and set the value to 1 (on) or 0 (off).**

   i. **To turn on or off the variable for enabling information label floating on System V message queues, find** `tsol_float_sysv_msg=` **and set the value to 1 (on) or 0 (off).**

   ii. **To turn on or off the variable for enabling information label floating on System V semaphores, find** `tsol_float_sysv_sem=` **and set the value to 1 (on) or 0 (off).**

   iii. **To turn on or off the variable for enabling information label floating on System V shared memory segments, find** `tsol_float_sysv_shm=` **and set the value to 1 (on) or 0 (off).**

b. **To turn on or off the variable for resetting information labels on** `exec`**, find** `tsol_reset_il_on_exec=` **and set the value to 1 (on) or 0 (off).**

3. **To turn on or off the variable for hiding the names of files whose sensitivity labels have been upgraded, find** `tsol_hide_upgraded_names=` **and set the value to 1 (on) or 0 (off).**

4. **Reboot.**

Distributing Changed Label Configuration Files to All Hosts in the Distributed System

Modifications seldom need to be made to the `label_encodings` or `system`(4) files after an site has been installed and configured. However, if modifications prove necessary, once any modifications are done, the `label_encodings` file should be updated on all hosts in the distributed system, and in most cases, the system file should also.You can use the `rdist(1)` command to automatically distribute identical copies of the file to all machines in the distributed system.

▼ To Remotely Distribute the `label_encodings` and `system` Files

Note – Make sure that every host has only a plus in the `hosts.equiv` file, and that there are no entries in either the `/.rlogin` or in any `$HOME/.rlogin` files.

1. **As security administrator in an ADMIN_LOW workspace, use the Admin Edit action to set up a `distfile` to copy the configuration files from a master directory.**
   The example shows a sample `distfile` that is set up to tell `rdist` to copy the `label_encodings` and `system` file to all the listed hosts in the distributed system.

```
# #
HOSTS = ( machiavelli muckraker mugwump diehard warhorse )
FILES = ( /etc/security/tsol/label_encodings /etc/system )

${FILES} -> ${HOSTS}
    install ;
```

2. **Run the `rdist` command.**
   You can either run `rdist` in the same directory as the `distfile` or use `rdist` with the `-f` option followed by the full pathname of a file with some other name.

```
$ rdist \* OR *\
$ rdist -f /home/machiavelli/jedgar/label_encodings.master/distfile.sample
```

   See also the `rdist(1)` and `hosts.equiv(4)`man pages.

3. **Reboot each machine.**

5

Example: Planning an Organization's Labels

6

This chapter provides guidance about how to get started for organizations that have not previously used labels. It shows how one organization went about analyzing its labeling requirements and setting up a fairly simple set of labels, in the following major sections.

This chapter models how to do the following:[1]

- Identify the set of labels to be represented and understand how the labels meet the company's information protection goals
- Define the components of labels and their relationships:
  - Classifications (the words that specify which labels are more sensitive than others)
  - Compartments (words that associate a label or clearance with a project or group)
  - Markings (words that provide guidance on how information should be handled)
  - Intended use of the words in mandatory access control
  - Intended use of the words in labeling printed output

1. These steps are similar to the preparatory steps outlined in the *Compartmented Mode Workstation Labeling: Encodings Format* manual from the Defense Intelligence Agency.

6

Identifying the Site's Label Requirements

Let's call the company whose label requirements are considered in this example, "Solar Systems, Inc." To protect the corporation's legal interests in its intellectual property, the legal department of the Solar Systems company mandates that employees use three labels on all sensitive email and printed materials. The three labels, from highest to lowest, are:

```
Solar Proprietary/Confidential: Registered

Solar Proprietary/Confidential: Need To Know

Solar Proprietary/Confidential: Internal Use Only
```

The legal department also approves the use of an optional fourth label for information that can be distributed to anyone with no restrictions:

```
Public
```

Problems Encountered in Trying to Meet Information Protection Goals

At Solar Systems, Inc., the manager in charge of Information Protection makes use of all possible channels to get the word out about labeling requirements. She set up a home page and regularly sends email to employees describing the requirements. Some employees either do not understand or forget about or ignore the requests. Even when labels are properly applied by employees, the information is not always properly handled, stored, and distributed. For example, reports trickle back to the IP manager that even highly sensitive Registered information (which only a limited list of people should see and nobody but the originator should copy) is sometimes found unattended next to copy machines and printers, in break rooms and lobbies.

- The legal department wants a better way *to ensure that information is properly labeled without relying totally on employee compliance*
- The system administrators wants a better way *to control*:
  - *who can see or modify sensitive information*,
  - *what information is printed on which printers*,
  - *how printer output is handled*, and
  - *how information at various levels of sensitivity is distributed internally and externally via email*

How Trusted Solaris Features Address Information Labeling and Access Control Requirements

The Trusted Solaris operating system does not leave the labeling up to employees. All email and printer output from hosts running Trusted Solaris software is *automatically labeled* according to the site's requirements. The Solar Systems' executives decided to use the Trusted Solaris operating system on its distributed system of Sun workstations and servers when they realized that the product could both meet the requirements of the legal department and support the goals of the system administrators.

Even though security administration was not yet fully understood at the company, they knew they could put the following features to use right away:

- Each print job is automatically assigned a *sensitivity label*, which is the label that corresponds to the *sensitivity level* at which the user is working or to the user's level of responsibility.

  Figure 6-1 shows an employee working at a sensitivity level of INTERNAL_USE_ONLY, which means that the work he is doing should only be accessible by Solar Systems employees and others who have signed non-disclosure agreements. When he sends email to the printer, the print job is automatically assigned the sensitivity label INTERNAL_USE_ONLY.

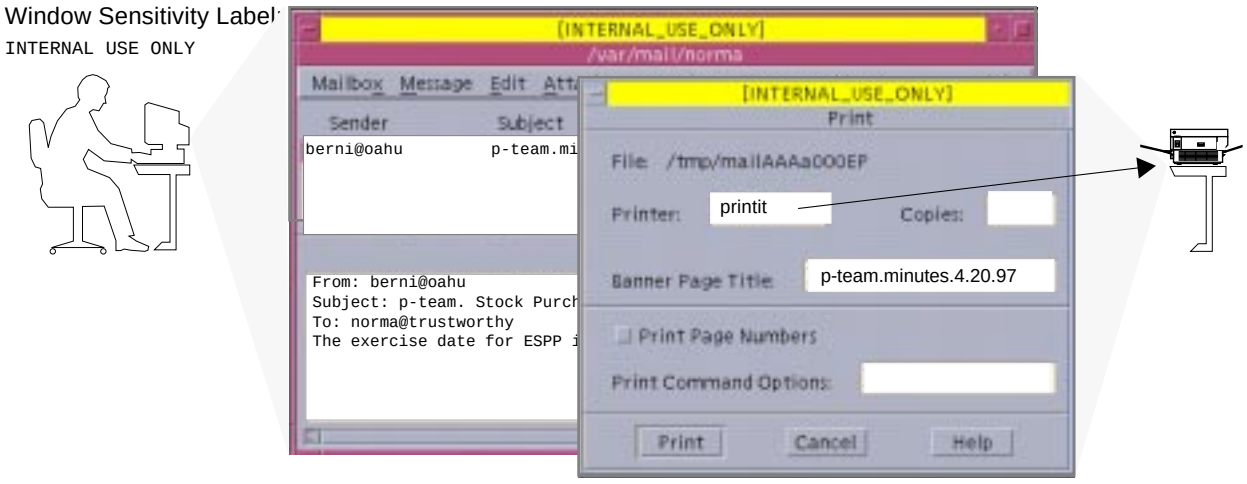


Figure 6-1 Automatic Labeling of Print Jobs

- The printer automatically prints a company-specified label that indicates the job's sensitivity level at the top and bottom of each page of printed output.

  In Figure 6-2, the letter that was sent to the printer in Figure 6-1 on page 129 is printed with the user's working label, INTERNAL_USE_ONLY, at the top and bottom of every page.

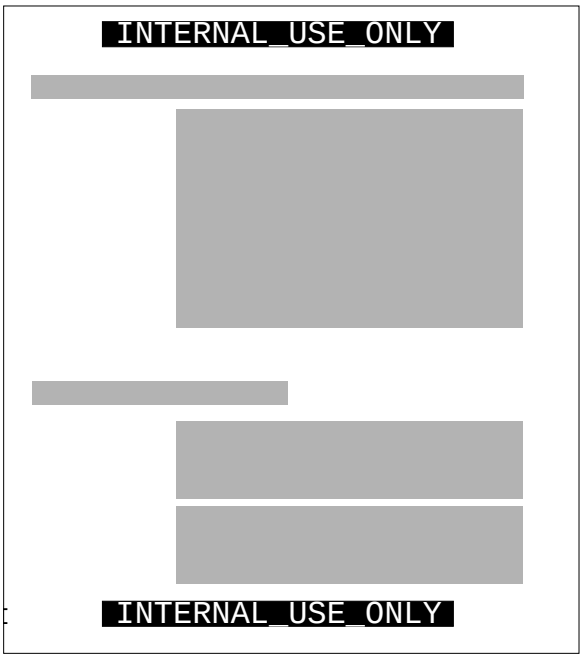


Figure 6-2 Label Automatically Printed on Body Pages

- Banner and trailer pages are automatically created for each print job and are printed with company-specific handling guidelines.

  Figure 6-3 shows the wording for a print job whose sensitivity level has a classification of Need to Know and a department of Human Resources.

```
Need to Know Human Resources

Distribute Only to Human Resources (Non-Disclosure Agreement Required)
```

Figure 6-3 Handling Guidelines on Banner and Trailer Pages

Below the sensitivity label in Figure 6-3 on page 130, a *handling caveat* provides instructions about how the printed material should be distributed. The handling caveat directs that the information should be distributed only to Human Resources personnel with a need to know about it and that the reader must have signed a non-disclosure agreement.

- Printers can be configured to print only jobs whose labels are within a restricted label range.

  For example, the legal department's printer can be set up (as illustrated in Figure 6-4) to print only jobs sent at the following three labels:

  - NEED_TO_KNOW LEGAL (to be viewed only by those with a need to know within the legal department)
  - INTERNAL_USE_ONLY (to be viewed only by permanent employees of the Solar Systems company who have signed non-disclosure agreements), and
  - PUBLIC (to be viewed by anybody)

  A printer set up as specified above would exclude jobs sent at any other label. For example, the legal department printer set up as described above would reject jobs at:

  - Need to Know Marketing, and
  - Registered

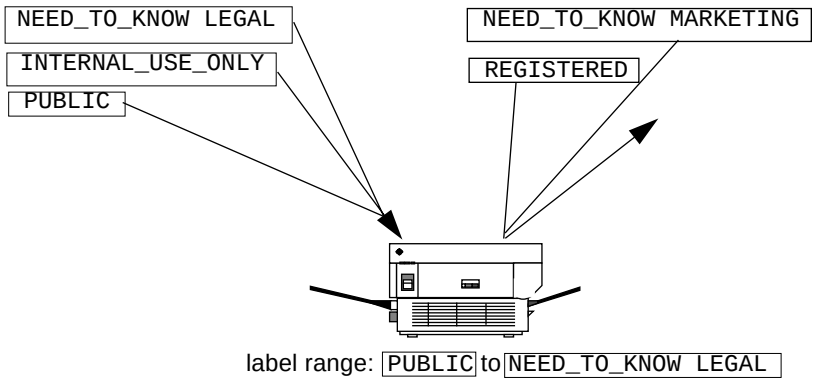


Figure 6-4 How a Printer With a Restricted Label Range Handles Jobs at Various Labels

Printers in other locations that are accessible to all employees can be configured to print jobs only at the two labels that allow the output to be viewed by all employees:

- INTERNAL_USE_ONLY
- PUBLIC

- A label is automatically assigned to each email message based on the sensitivity level at which the sender is working.

  Figure 6-5 shows email being labeled at the sensitivity label of the user's mail application and sent to the mail application at that label.

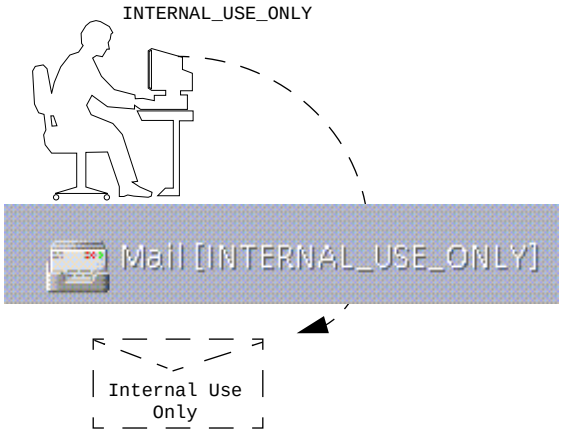


Figure 6-5 Automatic Labeling of Email

Similar to how the printer label range controls which jobs can be printed on a particular printer (as shown in Figure 6-4 on page 131), an employee's *personal sensitivity label range* limits which email the person can receive and send (see Figure 6-6 on page 133).

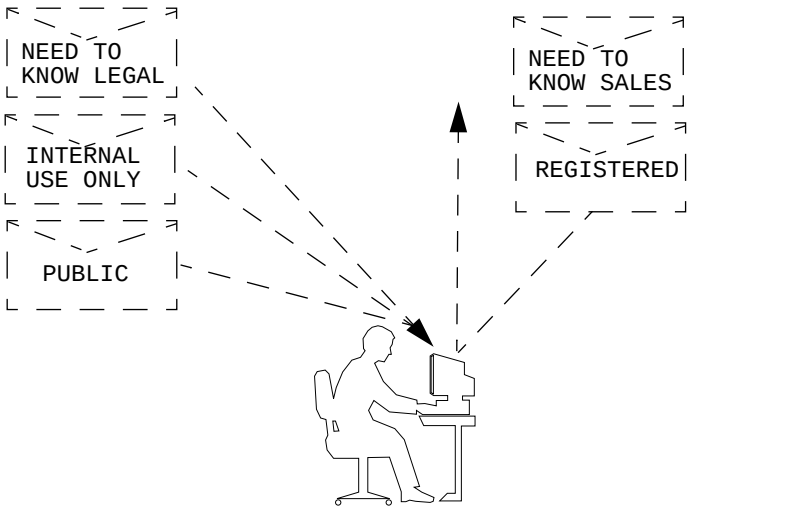


Figure 6-6 An Employee on a Trusted Solaris Host Receiving Email Within His Account Label Range

- Gateways to the Internet can be set up to screen email so that email at inappropriate labels (any label except PUBLIC) could not be sent outside of the company

Climbing the Security Learning Curve

The management identifies an experienced administrator who:

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

That person is assigned the job of security administrator.

Long before installing Trusted Solaris software, the security administrator starts to learn about security and to prepare a plan for the site's security policy—starting with a plan for the site's labels as described in the immediately-following sections.

6

By reading the *Trusted Solaris User's Guide* and the *Trusted Solaris Administration Overview*, the security administrator becomes familiar with the distinctions between types of labels and how labels are compared when access control decisions are being made. Reading the *Trusted Solaris Administrator's Procedures* manual prepares the security administrator to do the tasks to administer the system and to assign administrative responsibilities. Appendix A, "Site Security Policy" in the *Trusted Solaris Installation and Configuration* manual provides guidance on the site's security policy.

She also reads through "Review of Label-Encodings Related Concepts" on page 5 of this manual to reviews the concepts that are directly related to understanding how to set up security and encode the labels at the site.

Analyzing the Requirements for Each Label

The security administrator agrees that the set of labels mandated by the legal department was a good start, but she realizes that she has to analyze them further before deciding how to encode them.

PROPRIETARY/CONFIDENTIAL: INTERNAL_USE_ONLY

The PROPRIETARY / CONFIDENTIAL: INTERNAL_USE_ONLY label is for information that is proprietary to the company but which, because of its low level of sensitivity, may be distributed to all of the Solar Systems company's employees, all of whom have signed non-disclosure agreements upon starting employment. Information with this label may also be distributed to others such as the employees of vendors and contractors, as long as each person who receives the information has also signed a non-disclosure agreement. Because the Internet may be snooped, information with this label may not be sent over the Internet, but it may be sent via email within the company.

Memos containing spending guidelines
Internal job postings

PROPRIETARY/CONFIDENTIAL: NEED_TO_KNOW

The PROPRIETARY / CONFIDENTIAL: NEED_TO_KNOW label is intended for information that is proprietary to the Solar Systems company, has a higher level of sensitivity than INTERNAL_USE_ONLY, and has a more limited

audience. Distribution is limited to company employees who have a need to know the information and to others who have signed non-disclosure agreements who also have a need to know. 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. People who receive information with this label may copy it and pass it on to other people who have a need to know and who have signed a non-disclosure agreement. Whenever information should be restricted to a particular group, the name of the group should be specified on the printed or otherwise copied version of the information.

Having the name of the group in this label would help ensure that the information would not be given to anyone outside of the group. Information with this label may not be sent over the Internet but it may be sent via email within the company.

Product design documents
Project details
Employee Status Change Form

PROPRIETARY/CONFIDENTIAL: REGISTERED

The PROPRIETARY / CONFIDENTIAL: REGISTERED classification is intended for information that is proprietary to the Solaris Systems company, has a very high level of sensitivity, and could significantly harm the company if released to the wrong parties or if it was released at the wrong time. Registered information must be numbered and tracked by the owner. Each copy must be assigned to a specific person and returned to the owner for destruction after being read. Copies may 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 of the information, and it cannot be shown to employees of other companies who have not signed a non-disclosure agreement—even if the owner authorizes them to see it. Information with this label may not be sent over email.

End of quarter financial information not yet released
Sales forecasts
Marketing forecasts

Names of Group Associated With the Need to Know

The security administrator decided that the NEED_TO_KNOW label should be associated with groups or departments with a common interest in both labels on files and in user clearances. The security administrator consulted with the rest of the organization for suggestions about what words to use to define groups or areas of interest within the Solar Systems' organization, and came up with the following list.

Engineering
Executive Management
Finance
Human Resources
Legal
Manufacturing
Marketing
Sales
System Administration

Understanding the Set of Labels

The next step is to decide:

- How to encode the labels into the classifications and compartments that make up sensitivity labels and clearances,
- What kinds of handling instructions should appear on printed output.

The security administrator used a large board and pieces of paper marked with the words that should be in the labels, as shown in “Example Planning Board for Label Relationships” on page 138, to visualize the relationships and rearrange the pieces until they all fit together.

While thinking about how to encode the labels, the administrator came up with the following facts:

- The four labels are hierarchical with the label containing REGISTERED the highest and the PUBLIC label the lowest.
- Only one label needs to be associated with group names

  The list of those cleared to receive registered information is limited on a case by case basis, so REGISTERED does not need any group names. INTERNAL_USE_ONLY applies to all employees and those that have signed non-disclosure agreements, and PUBLIC labels are for everybody, so neither of these labels needs 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 require that the person accessing the information must have signed a non-disclosure 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 based on the classification and on any group name that may appear in the label.

  Along with information on the sensitivity of the printer output, handling instructions should remind the reader that a non-disclosure agreement is required for any output whose label requires it.

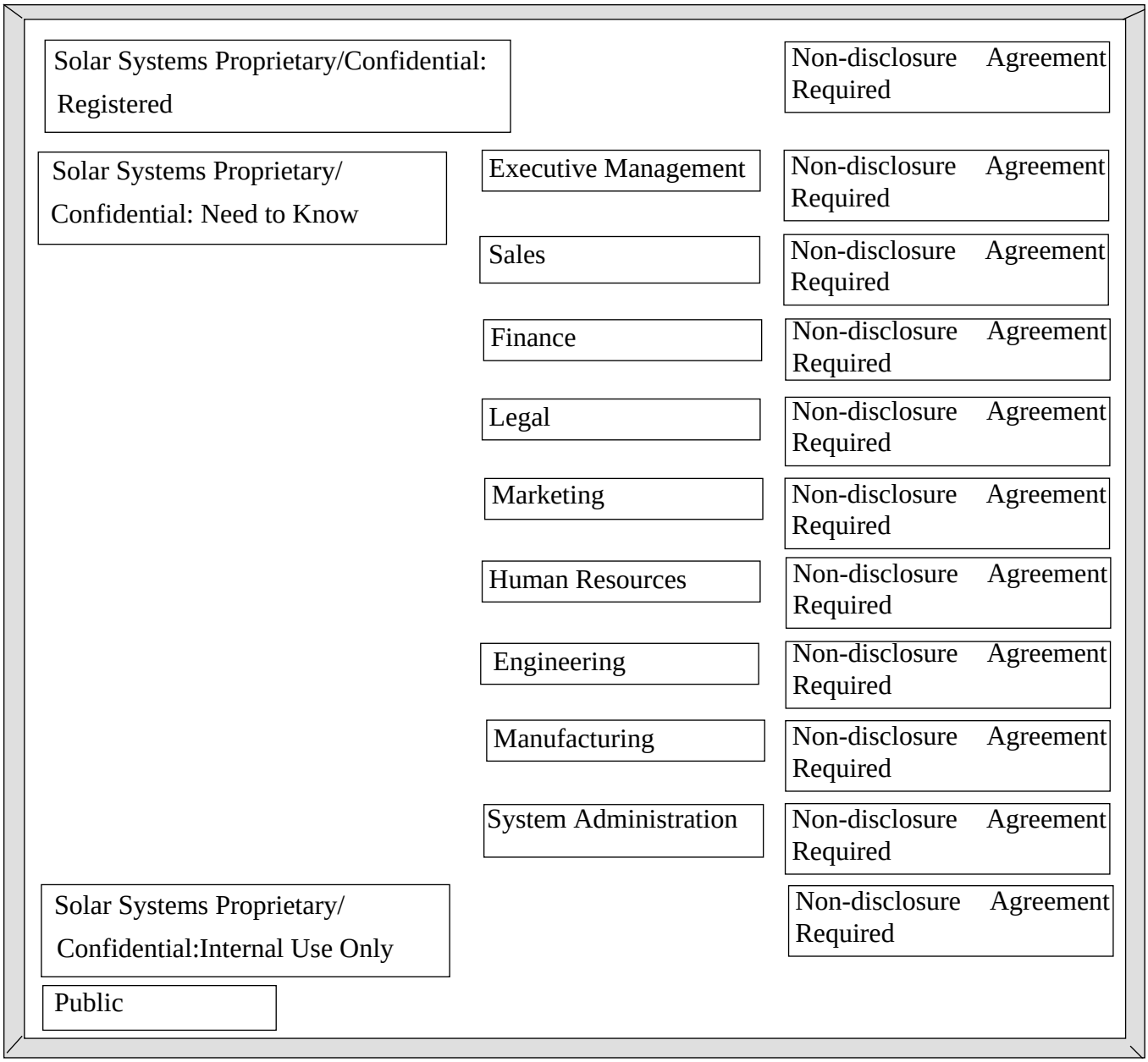


Figure 6-7 Example Planning Board for Label Relationships

Defining the Set of Labels

In this section we define the set of labels by creating lists. In these lists, we define all of the following required aspects of labels, although not in the order given:

- Classifications
- Other words
- Relations between and among the words
- Classification restrictions associated with use of each word
- Intended use of the words in mandatory access control (in sensitivity labels and clearances)
- Intended use of the words in labeling system output.

Planning the Classifications

Because the four labels are hierarchical, they will be encoded as hierarchical classifications.

With the legal department's approval, the security administrator shortened the labels by omitting Solar Systems Proprietary/Confidential: from the label names. Classifications do not allow the use of a slash in the label, and long classifications make it difficult for employees to read the labels in the window system. The name of a label is truncated from right to left in the window frames. The truncation causes a problem because all the suggested label names above PUBLIC begin with the words SOLAR SYSTEMS PROPRIETARY CONFIDENTIAL, which would probably fill the window frame. To read the words that distinguish the labels from each other, employees would have to manually extend 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 that need to be associated with NEED_TO_KNOW are to be encoded as non-hierarchical *compartments*. The compartments need to be restricted to appear only in labels that have the NEED_TO_KNOW classification; compartments are restricted to appear with certain classifications by making the appropriate settings in the ACCREDITATION RANGE section under COMBINATION CONSTRAINTS. User *clearances* will control which users can create files and directories with labels that include a group name, and user clearances will also control whether some users will be able to create documents labeled 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. 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 controlling the labels at which individual employees can access files and do other work.

In the following example, Solar Systems, 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, and
- Uses printers only if they 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 at INTERNAL_USE_ONLY (depending on what workspace the employee is currently in)
- Receives and sends email at either sensitivity label.
- Can print a file labeled PUBLIC on any printer with PUBLIC in its label range, and 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 will state:

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

Planning How to Label Printer Output Pages as Desired

The “print without labels” authorization allows a user or role to submit a print request to the Trusted printing system that specifies by means of the `lp -o nolabels` option) that the body pages of the print job should have the top and bottom labels suppressed. The security administrator may decide to 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, which is normally 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 created by a desktop publishing system in PostScript form without labels printed on them, the security administrator gives the print without labels and print a PostScript file to all the writers.

Planning for Supporting Procedures

Rules for Protecting a File or Directory Labeled With the REGISTERED Sensitivity Label

The security administrator realizes that any employee who has a clearance that includes the word REGISTERED would be able to access any registered information anywhere in the company, unless certain additional precautions

are taken. Therefore, those who have REGISTERED in their user clearances must be instructed to use UNIX permissions to further restrict access, so that only the creator can look at or modify the file.

```
trusted% getplabel
R
trusted% mkdir registered.dir

trusted% chmod 700 registered.dir

trusted% cd registered.dir
trusted% touch registered.file

trusted% ls -l

-rwxrwxrwx registered.file

trusted% chmod 600 registered.file

trusted% ls -l

-rw------- registered.file
```

Figure 6-8 Using DAC to Protect Registered Information

As shown in the example in Figure 6-8 on page 142, when working at an sensitivity label of REGISTERED, the user who creates a file or directory needs to set the file's permissions to be read and write for the owner only and set the directory's permissions to be readable, writable, and searchable only by the owner. This ensures that another user who can work at an sensitivity label with the word REGISTERED cannot read the file.

Rules for Configuring Printers

Table 6-1 shows how printers in various locations accessible to various types of people 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 non-disclosure 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 those who have the `REGISTERED` classification in their clearance	`REGISTERED` to `REGISTERED`

See “To Set Up a Printer and Configure Its Label Range Using the Device Manager” on page 374,” in Chapter 14, “Managing Printing,” in the *Trusted Solaris Administrator’s Procedures* manual.

Rules for Handling Printer Output

Those who have access to restricted printers will be instructed to:

- 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 and that do not have matching job numbers on the banner and trailer pages.

6

Planning Classification Values in a Worksheet

The worksheet in Table 6-2 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, and the values of the others are set higher in ascending sensitivity.

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

Table 6-2 Classifications Planning Table

name=	**sname=/*aname=**	**value=**	***initial compartments= bit numbers/WORD**	***initial markings= bit numbers/ WORD**
PUBLIC		1	none	none
INTERNAL_USE_ONLY		4	none	none
NEED_TO_KNOW		5	none	none
REGISTERED		6	none	none

Planning Compartment Values and Classification/Compartment Constraints in a Worksheet

Table 6-3 defines the relationships between words and classifications that were arrived at by moving things around on the planning board in Figure 6-7 on page 138. Because of the way PUBLIC and INTERNAL_USE_ONLY are defined in the third column, these two classifications can never appear in a label with any compartment while NEED_TO_KNOW can appear in a label with any or all of the compartments.

Table 6-3 Compartments and User Accreditation Range Combinations Planning Table

Classification	Compartment Name/sname/Bit	Combination Constraints
PUBLIC		PUBLIC only valid combination
INTERNAL_USE_ONLY		INTERNAL_USE_ONLY only valid combination
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 / EMG / 11	
	ALL_DEPARTMENTS / 11-20	
REGISTERED		REGISTERED only valid combination

The security administrator uses Table 6-4 to keep track of which bits have been used for compartments and which for markings.

Table 6-4 Compartment and Marking Bit Tracking Table

Compartment Bit Numbers										Marking Bit Numbers
11	12	13	14	15	16	17	18	19	20	

Planning Clearances in a Worksheet

Besides being used in the sensitivity labels on files and directories and processes, the components of these labels are also assigned to users in clearances. The worksheet's Clearance Planner (shown in Table 6-5 on page 147) defines the label components to be used in clearances.

Key to Table 6-5 on page 147:

Abbreviation	Name
REG	REGISTERED
NTK	NEED_TO_KNOW
IUO	INTERNAL_USE_ONLY
EMG	EXECUTIVE MANAGEMENT GROUP
SALES	SALES
FIN	FINANCE
LEG	LEGAL
MRKTG	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	EMG	ENG	FIN	HR	LEG	MANU	MKTG	SALES	SYSADM	**Highest, not used**[1]
REG										**Assigned to selected personnel on an as needed basis**[2]
NTK		ENG								**Assigned to ENG emps.**
.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.
									SYSADM	**Assigned to system admin.**
IUO										**Assigned to employees. and others w/NDAs**
PUB										**Assigned to anyone**

1. This is the highest possible label in the system, consisting of the highest classification and all of the defined compartments. Because nobody in an organization should be able to access all of its information in all departments, it is not in the user accreditation range, an d no one should be assigned this clearance.

2. When working at the sensitivity label that contains the word Registered, the employee should take care to make sure that any newly-created files or directories have permissions that keep out everyone except the owner (file permissions 600, directory permissions, 700).

Planning the PRINTER BANNERS Wording in a Worksheet

The Solar Systems' legal department wants the following to appear on printer banner and trailer pages.

```
Solar Systems Proprietary/Confidential:
```

The PRINTER BANNERS section lets the system administrator associate a string with any compartment or marking that appears in the CMW label of the print job. In this encodings, only one classification has compartments (departments): NEED_TO_KNOW. Table 6-6 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 will read:

```
Solar Systems Proprietary/Confidential: <GROUP_NAME>
```

Table 6-6 Printer Banners Planner

Prefix	**PRINTER BANNER**
SOLAR SYSTEMS PROPRIETARY/CONFIDENTIAL:	ALL_DEPARTMENTS
SOLAR SYSTEMS PROPRIETARY/CONFIDENTIAL:	EXECUTIVE_MANAGEMENT_GROUP
SOLAR SYSTEMS PROPRIETARY/CONFIDENTIAL:	SALES
SOLAR SYSTEMS PROPRIETARY/CONFIDENTIAL:	FINANCE
SOLAR SYSTEMS PROPRIETARY/CONFIDENTIAL:	LEGAL
SOLAR SYSTEMS PROPRIETARY/CONFIDENTIAL:	MARKETING
SOLAR SYSTEMS PROPRIETARY/CONFIDENTIAL:	HUMAN_RESOURCES
SOLAR SYSTEMS PROPRIETARY/CONFIDENTIAL:	ENGINEERING
SOLAR SYSTEMS PROPRIETARY/CONFIDENTIAL:	MANUFACTURING
SOLAR SYSTEMS PROPRIETARY/CONFIDENTIAL:	SYSTEM_ADMINISTRATION
SOLAR SYSTEMS PROPRIETARY/CONFIDENTIAL:	PROJECT_TEAM

Planning CHANNELS in a Worksheet

The Solar Systems' 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)
```

Using the CHANNELS section this goal can partially be met. The group names have been defined as compartments earlier in this example. In the CHANNELS section, the compartments need to be defined as channels. In government installations where the encoding of classified information determined the original format of the `label_encodings` file, compartments are thought of as channels. The Solar Systems company in the example wants 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 worksheet so that the desired handling caveats are included on printed banner and trailer pages.

Table 6-7 Channels Planner (for Prefixes, Channels, and Suffixes)

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)
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 Worksheet

The following minimums must be set: a *minimum sensitivity label*, a *minimum clearance*, and a *minimum protect as classification*. Because the Solar Systems company wants employees to be able to use all the defined sensitivity labels and to be able to assign the PUBLIC clearance to some employees, 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. Setting the minimum protect as classification higher than the *actual* minimum classification means that all jobs must be handled at the specified classification. However, because the Solar Systems company wants the "minimum protect as classification" to always be equal to the real classification of the print job's sensitivity label, the security administrator defines all of values for the minimum sensitivity label, minimum clearance and minimum protect as classification as PUBLIC as shown in Table 6-8.

Table 6-8 ACCREDITATION RANGE Minimum Values

Minimum Sensitivity Label	PUBLIC
Minimum Clearance	PUBLIC
Minimum Protect as Classification	PUBLIC

Planning the Colors in the COLOR NAMES Worksheet

Whatever color is assigned to a sensitivity label displays in the background whenever the name of the label appears at the top of a window. The lettering of the sensitivity label is displayed in a color that complements the background. (The complementary color is computed by the window system.) In our example, the security administrator chooses to keep the colors already assigned to the administrative labels in the default `label_encodings` file and

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 Table 6-9.

Table 6-9 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 EMG	#7FA9EB
NEED_TO_KNOW SALES	#87CEFF
NEED_TO_KNOW FINANCE	#00BFFF
NEED_TO_KNOW LEGAL	#7885D0
NEED_TO_KNOW MRKTG	#7A67CD
NEED_TO_KNOW HR	#7F7FFF
NEED_TO_KNOW ENG	#007FFF
NEED_TO_KNOW MANUFACTURING	#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

Specifying the Labels

During Installation

During Trusted Solaris installation on the NIS+ Master, the install team (made up of the security administrator and the system administrator) should choose `Create multiple sensitivity labels` when answering the first

question under Customize Trusted Solaris Configuration, Labels (shown in Figure 6-9 on page 152). As a result, the installation software installs a `label_encodings` file with multiple sensitivity labels defined.

Because information labels are not being used, they chose No to on the options menu next to

- Enable Information Labels

Because the Solar Systems company does not consider the names of files to be sensitive information, the install team chose No to:

- Hide upgraded names in directories

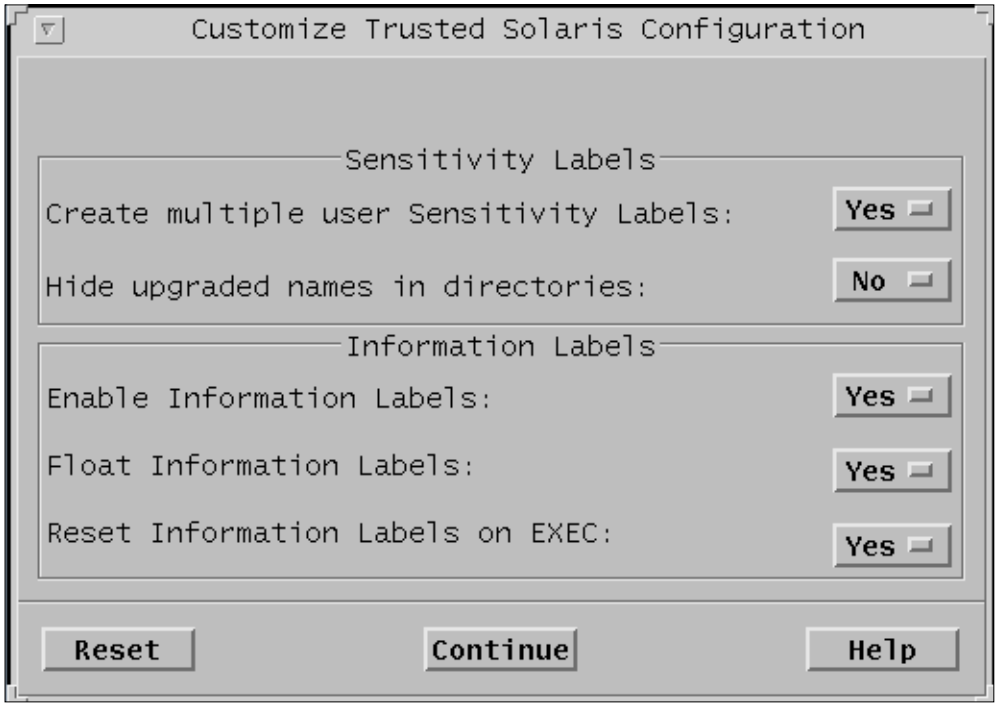


Figure 6-9 Specifying Initial Labels Set Up During Installation

During Post-Install Configuration

The install makes a printed copy and an online copy in case of problems with the new version of the file supplied by the security administrator.

The security administrator uses the Edit Encodings action from the Application Manager in the System_Admin folder to edit and then to check the `label_encodings` file. The Check Encodings action from the same folder may be used on its own to run `chk_encodings(1MTSOL)`on a `label_encodings` file.

Note – The encodings for Solar Systems, Inc. are shown in **`User Type font`** in the screen examples.

Encoding the VERSION

The example in Figure 6-10 shows the VERSION string is modified with the name of company, a title, version number, and date.

```
VERSION= Solar Systems, Inc. Example Version - 2.2 97/04/18
```

Figure 6-10 Modified VERSION Entry

Encoding the CLASSIFICATIONS

Figure 6-11 shows the Solar Systems' classifications and values from Table 6-2, "Classifications Planning Table," on page 144 added to the 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;
```

Figure 6-11 Modified CLASSIFICATIONS Section

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

Encoding the INFORMATION LABELS

Even though information labels are not going to be used, values must be supplied under the INFORMATION LABELS, WORDS section for the file to pass the encodings check. The security administrator copies the words from the SENSITIVITY LABELS: WORDS: section, as shown in Figure 6-12 on page 155.

```
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; compartme;fsnts= 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;
name= DO_NOT_FORWARD; sname= NO_FORWD; minclass= INTERNAL; markings= 0;
access related;
name= RELEASE_AFTER_BETA; sname= AFTER_BETA; minclass= NEED_TO_KNOW;
markings= ~0 1 ~2; access related;
name= RELEASE_AFTER_FCS; sname= AFTER_FCS; minclass= NEED_TO_KNOW;
markings= ~0 ~1 2; access related;

REQUIRED COMBINATIONS:

COMBINATION CONSTRAINTS:
```

Figure 6-12 Modified WORDS: in the INFORMATION LABELS Section

Encoding the SENSITIVITY LABELS

The compartments in the Table 6-3 on page 145 are encoded in the SENSITIVITY LABELS: WORDS: example shown in Figure 6-13 on page 156.

This example does not have any required combinations or 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:
```

Figure 6-13 Modified WORDS: in the SENSITIVITY LABELS Section

Encoding the CLEARANCES:

Because the words in this example in CLEARANCES: will be the same as the ones in the SENSITIVITY LABELS:, the words in Figure 6-14 are the same as those in Figure 6-13 on page 156.

```
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:
```

Figure 6-14 Modified WORDS: in the CLEARANCES Section

Encoding the CHANNELS:

Compartments are also called channels, so this example is encoded with one channel for each group name compartment, using the same compartment bits 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). The channel specifications shown in Figure 6-15 will create the desired wording in the handling caveats section:

```
DISTRIBUTE ONLY TO <GROUP_NAME> (NON-DISCLOSURE AGREEMENT REQUIRED)
```

Note – The prefixes and suffixes are defined at the top of the section and have no compartments assigned to them. They are used in defining the channels; each channel has a prefix and suffix assigned to it.

```
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);
```

Figure 6-15 Modified WORDS in the CHANNELS Section

6

Encoding the PRINTER BANNERS:

Note – The term *printer banners* has a specialized meaning in the `label_encodings` file, and it does not refer to the banner page that is printed before a job. Any printer banners defined in the label encodings appear as a string on the printer banner page when the compartment or marking associated with it appears in the job's sensitivity label.

As shown in Figure 6-16, the values from the default file are removed and not replaced, since the Printer Banners are not being defined by the Solar Systems company.

```
PRINTER BANNERS:

WORDS:

name= COMPANY PROPRIETARY/CONFIDENTIAL:;       prefix;

name= ALL_DEPARTMENTS; prefix= COMPANY PROPRIETARY/CONFIDENTIAL:;
suffix=(NON-DISCLOSURE AGREEMENT REQUIRED); compartments= 11-20;
name= EXECUTIVE_MANAGEMENT_GROUP; prefix= COMPANY PROPRIETARY/CONFIDENTIAL:;
suffix=(NON-DISCLOSURE AGREEMENT REQUIRED); compartments= 11;
name= SALES; prefix= COMPANY PROPRIETARY/CONFIDENTIAL:;
suffix=(NON-DISCLOSURE AGREEMENT REQUIRED); compartments= 12;
name= FINANCE; prefix= COMPANY PROPRIETARY/CONFIDENTIAL:;
suffix=(NON-DISCLOSURE AGREEMENT REQUIRED); compartments= 13;
name= LEGAL; prefix= COMPANY PROPRIETARY/CONFIDENTIAL:;
suffix=(NON-DISCLOSURE AGREEMENT REQUIRED); compartments= 14;
name= MARKETING; prefix= COMPANY PROPRIETARY/CONFIDENTIAL:;
suffix=(NON-DISCLOSURE AGREEMENT REQUIRED); compartments= 15 20;
name= HUMAN_RESOURCES; prefix= COMPANY PROPRIETARY/CONFIDENTIAL:;
suffix=(NON-DISCLOSURE AGREEMENT REQUIRED); compartments= 16;
name= ENGINEERING; prefix= COMPANY PROPRIETARY/CONFIDENTIAL:;
suffix=(NON-DISCLOSURE AGREEMENT REQUIRED); compartments= 17 20;
name= MANUFACTURING; prefix= COMPANY PROPRIETARY/CONFIDENTIAL:;
suffix=(NON-DISCLOSURE AGREEMENT REQUIRED); compartments= 18;
name= SYSTEM_ADMINISTRATION; prefix= COMPANY PROPRIETARY/CONFIDENTIAL:;
suffix=(NON-DISCLOSURE AGREEMENT REQUIRED); compartments= 19;
name= PROJECT_TEAM; prefix= COMPANY PROPRIETARY/CONFIDENTIAL:;
suffix=(NON-DISCLOSURE AGREEMENT REQUIRED); compartments= 20;
```

Figure 6-16 Modified PRINTER BANNERS Section

Encoding the ACCREDITATION RANGE

The combination constraints from the Table 6-3 on page 145 and the minimum clearance, minimum sensitivity label and minimum protect as classification from Table 6-8 on page 150 are encoded in the ACCREDITATION RANGE: example shown in Figure 6-17. PUBLIC and INTERNAL_USE_ONLY are defined so that these two classifications can never appear in a label with any compartment while NEED_TO_KNOW is defined so it can appear in a label with any combination of compartments, and REGISTERED with no compartments.

```
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;
```

Figure 6-17 Modified `ACCREDITATION RANGE` Section

Encoding the NAME INFORMATION LABELS WORDS

As shown in Figure 6-18, the default values are removed, since the NAME INFORMATION LABELS: WORDS: are not being used by the company.

```
NAME INFORMATION LABELS:


WORDS:
```

Figure 6-18 Modified NAME INFORMATION LABELS Section

Encoding the Wording for Label Builders and Colors and Accepting The Defaults for All Other LOCAL DEFINITIONS Values

Figure 6-19 shows that none of the default values are changed at Solar Systems, Inc. for the default and forced flags, Default Label View, and Float Process Information Label in the LOCAL DEFINITIONS: section.

```
LOCAL DEFINITIONS:


default flags= 0x0;
forced flags= 0x0;

Default Label View is External;
Float Process Information Label;
```

Figure 6-19 Accepting Defaults in the LOCAL DEFINITIONS Section

Encoding the Heading Names for Label Builders

The default settings for heading names used in label builders are shown in Figure 6-20.

```
Classification Name= Class;
Compartments Name= Comps;
Markings Name= Marks;
```

Figure 6-20 Default Heading Names for Label Builders

Label builders are displayed whenever you need to set a label. For example, Figure 6-21 shows the label builder that comes up when you change the sensitivity label of a workspace—with the names specified at the Solar Systems company: *Classification* instead of *Class*, *Departments* instead of *Comps*, and *Disclosure* instead of *Marks*.

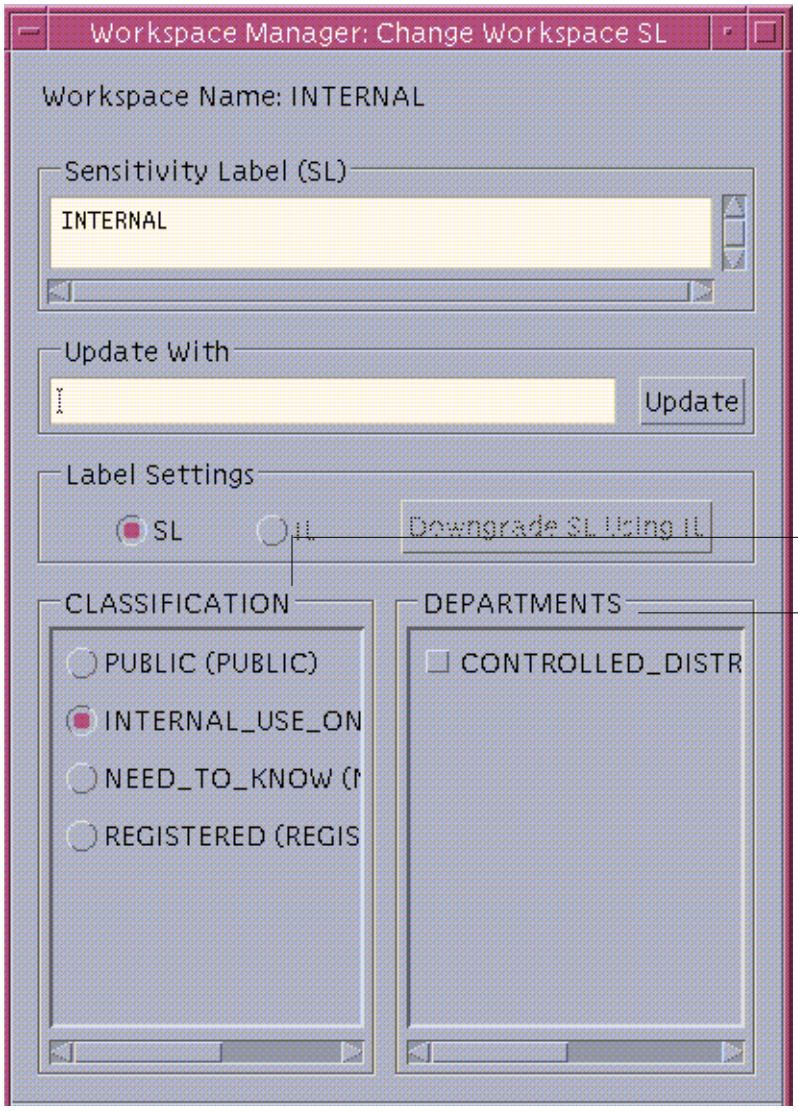


Figure 6-21 Change Workspace SL Label Builder With Changed Headings

Figure 6-22 shows the modifications the Solar System security administrator made to change the default values set for the Classification Name, Compartments Name, and Markings Name.

```
Classification Name= Classification;
Compartments Name= Departments;
Markings Name= Markings;
```

Figure 6-22 Modified Wording for Label Builders

Encoding the COLOR NAMES

The color names used in Figure 6-23 were taken from the worksheet in Table 6-9 on page 151.

```
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; colo= #4D658D;
        label= REGISTERED;  color= red;

        label= Admin_High;      color= #636363;

*
* End of local site definitions
```

Figure 6-23 Modified COLOR NAMES Section

6

Configuring Users to Enforce Labeling Decisions

While setting up user accounts during the post-installation configuration, the security administrator needs to specify the following for all users in the User Manager: Labels dialog (see Figure 6-24).

- The appropriate clearance (in the Clearance dialog)
  See “Planning Clearances in a Worksheet” on page 146
- The appropriate minimum label (in the Minimum SL Dialog Box)
- Show sensitivity labels

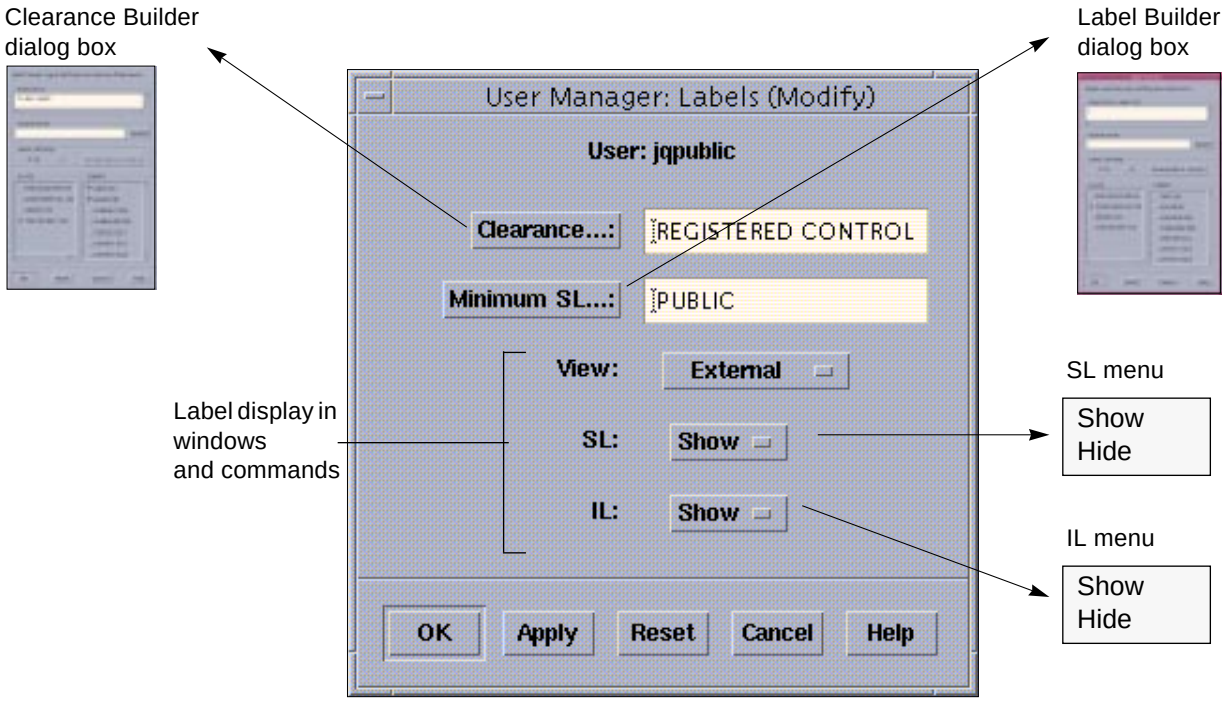


Figure 6-24 User Manager: Labels Dialog Box

Configuring Printing To Enforce Labeling Decisions

The security administrator needs to configure the following when setting up printers:

- **Configure the label range on printers based on their accessibility as described in "Rules for Configuring Printers" on page 143.**

The security administrator needs to do the following to allow the company's technical writers to print PostScript files and to print without labels on their output:

1. Give each of the users that need it the *print a PostScript file* and the *print without labels* authorizations.
2. For printing files from a desktop publishing system such as FrameMaker, inform each user to save (print) the file as a PostScript file.
3. Inform each user to use `lp` with the `-o nolabels` option when printing.
4. Set aside a specific printer that the writers can use to print jobs without labels.
   a. For a printer server running the unlabeled Solaris operating system, do the following.
      i. specify a sensitivity label for the print server that matches the sensitivity label at which users are working when they send jobs to the printer.

         For example, if documents are created at INTERNAL, the print server should be configured with the INTERNAL label, while if documents are created at PUBLIC, the print server should have the PUBLIC label. See Chapter 14, "Managing Printing" in the *Trusted Solaris Administrator's Procedures* for how to specify a default label for an unlabeled print server.

Note – No labels or banner/trailer pages will be printed on a printer connected to an unlabeled print server.

---

      ii. If desired, set up a separate `.login` file in the single-level directory (SLD) at the appropriate sensitivity label for each of the writers so that the $PRINTER variable is set to be the special-use printer.

b. If the print server for the writers printer is running Trusted Solaris 2.5, do one of the following:

   i. Make sure the printer is configured with the Always Print Banners check box NOT selected on the Print Manager dialog box.

   ii. To turn off page labels for *all* print jobs sent by *anyone*, on the Trusted Solaris print server make the change in the `/usr/lib/lp/postscript/tsol.separator.ps` file that eliminates page labels.

```
%% To eliminate page labels completely, change this line to
%% set the page label to an empty string: /PageLabel () def
          /PageLabel () def
```

Example: Simple Label Encodings File

This chapter contains a sample `label_encodings` file developed from the example in Chapter 6, “Example: Planning an Organization’s Labels.” Once the Trusted Solaris software is installed, the security administrator can copy the file from `/etc/security/tsol/label_encodings.simple`. and modify it to suit the site’s requirements. To prepare a label_encodings file in advance, the security administrator can manually copy the example in this chapter and make the site’s modifications in the copy.

Classifications

There are four classifications:

- PUBLIC
- INTERNAL_USE_ONLY
- NEED_TO_KNOW
- REGISTERED

Compartments (called Departments)

Compartments are defined to appear in labels only with the NEED_TO_KNOW classification. NEED_TO_KNOW Departments:

- ENG
- FINANCE
- ENG
- HR
- SYSADM

- MRKTNG
- LEGAL
- MANUFACTURING
- SALES
- PROJECT_TEAM
- ALL_DEPARTMENTS

The ALL_DEPARTMENTS word gets turned on when all compartments are turned on and also works as a toggle in the label builder.

PROJECT_TEAM is hierarchically below both ENG and MRKTNG. This allows employees working at NEED_TO_KNOW ENG and at NEED_TO_KNOW MRKTNG to read files created by someone working at NEED_TO_KNOW PROJECT_TEAM, but they cannot write to those files without changing to the NEED_TO_KNOW PROJECT_TEAM sensitivity label.

Internet and Intranet Labels

In this model, PUBLIC is the sensitivity label for communications with the Internet, and INTERNAL_USE_ONLY is the sensitivity label for communications within the company outside of the Trusted Solaris networks.

- PUBLIC = INTERNET
- INTERNAL_USE_ONLY = INTRANET (Company's WAN)

Markings (called Disclosure)

Markings are called `Disclosure`. The following markings are used:

- DO_NOT_FORWARD
  Can be included in any label with a classification of INTERNAL_USE_ONLY
- RELEASE_AFTER_BETA
  Cannot appear in the same label with RELEASE_AFTER_FCS or with DO_NOT_FORWARD. Minimum classification is NEED_TO_KNOW.
- RELEASE_AFTER_FCS
  Cannot appear in the same label with RELEASE_AFTER_BETA or with DO_NOT_FORWARD. Minimum classification is NEED_TO_KNOW.

Table 6-10 label_encodings.simple *(1 of 7)*

```
* @(#)label_encodings.simple 5.8 97/05/28 SMI; TSOL 2.x
*
*
* Copyright (c) 1997 by Sun Microsystems, Inc.
* All rights reserved.
*
*
* This version of the label_encodings file encodes the Sun
* proprietary/confidential labels that are required by Sun's
* legal and information protection departments. The prefix
* SUN PROPRIETARY/CONFIDENTIAL 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 (Sun's) legal information protection requirements for
* labeling email and printer output. These labels may also
* be used to enforce mandatory access control checks based on user
* clearance labels and labels and sensitivity labels on files
* and directories.


VERSION= Sun Microsystems, Inc. Example Version - 5.8 97/05/28



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;
```

Table 6-10 label_encodings.simple *(2 of 7)*

```
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;
name= DO_NOT_FORWARD; sname= NO_FORWD; minclass= INTERNAL;
markings= 0;
access related;
name= RELEASE_AFTER_BETA; sname= AFTER_BETA;
minclass= NEED_TO_KNOW; markings= ~0 1 ~2; access related;
name= RELEASE_AFTER_FCS; sname= AFTER_FCS;
minclass= NEED_TO_KNOW;
markings= ~0 ~1 2; access related;


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;
```

Table 6-10 label_encodings.simple *(3 of 7)*

```
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;
```

Table 6-10 label_encodings.simple *(4 of 7)*

```
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:
```

Table 6-10 label_encodings.simple *(5 of 7)*

```
WORDS:

name= COMPANY PROPRIETARY/CONFIDENTIAL:;       prefix;

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

ACCREDITATION RANGE:

classification= PUBLIC; only valid compartment combinations:

PUBLIC

classification= INTERNAL_USE_ONLY; only valid compartment combinations:

INTERNAL
```

Table 6-10 label_encodings.simple *(6 of 7)*

```
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;

NAME INFORMATION LABELS:

*
* Local site definitions and locally configurable options.
*

LOCAL DEFINITIONS:

*
*       The names for the administrative high and low name are set to
*       site_high and site_low respectively by the example commands below.
*
*       NOTE:   Use of these options could lead to interoperability problems
*               with machines that do not have the same alternate names.
*
*Admin Low Name= site_low;
*Admin High Name= site_high;

default flags= 0x0;
forced flags= 0x0;

Default Label View is External;
Float Process Information Label;

Classification Name= Classification;
Compartments Name= Departments;
Markings Name= Disclosure;

COLOR NAMES:

       label= Admin_Low;       color= #bdbdbd;
```

Table 6-10 label_encodings.simple *(7 of 7)*

```
        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
```

A

Index

F

G

H

I

K

L

M

N

P

R

S

T

U

V

W

X