



Trusted Solaris Label Administration

Sun Microsystems, Inc.
901 San Antonio Road
Palo Alto, CA 94303-4900
U.S.A.

Part Number 805-8122-10
December 2000

Copyright 2000 Sun Microsystems, Inc. 901 San Antonio Road, Palo Alto, California 94303-4900 U.S.A. All rights reserved.

This product or document is protected by copyright and distributed under licenses restricting its use, copying, distribution, and decompilation. No part of this product or document may be reproduced in any form by any means without prior written authorization of Sun and its licensors, if any. Third-party software, including font technology, is copyrighted and licensed from Sun suppliers.

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

Sun, Sun Microsystems, the Sun logo, docs.sun.com, AnswerBook, AnswerBook2, Trusted Solaris, and Solaris are trademarks, registered trademarks, or service marks of Sun Microsystems, Inc. in the U.S. and other countries. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc. PostScript(TM) is a trademark or registered trademark of Adobe Systems, Incorporated, which may be registered in certain jurisdictions.

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

Federal Acquisitions: Commercial Software – Government Users Subject to Standard License Terms and Conditions

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

Copyright 2000 Sun Microsystems, Inc. 901 San Antonio Road, Palo Alto, Californie 94303-4900 Etats-Unis. Tous droits réservés.

Ce produit ou document est protégé par un copyright et distribué avec des licences qui en restreignent l'utilisation, la copie, la distribution, et la décompilation. Aucune partie de ce produit ou document ne peut être reproduite sous aucune forme, par quelque moyen que ce soit, sans l'autorisation préalable et écrite de Sun et de ses bailleurs de licence, s'il y en a. Le logiciel détenu par des tiers, et qui comprend la technologie relative aux polices de caractères, est protégé par un copyright et licencié par des fournisseurs de Sun.

Des parties de ce produit pourront être dérivées du système Berkeley BSD licenciés par l'Université de Californie. UNIX est une marque déposée aux Etats-Unis et dans d'autres pays et licenciée exclusivement par X/Open Company, Ltd.

Sun, Sun Microsystems, le logo Sun, docs.sun.com, AnswerBook, AnswerBook2, Trusted Solaris, et Solaris sont des marques de fabrique ou des marques déposées, ou marques de service, de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays. Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux Etats-Unis et dans d'autres pays. Les produits portant les marques SPARC sont basés sur une architecture développée par Sun Microsystems, Inc. PostScript est une marque de fabrique d'Adobe Systems, Incorporated, laquelle pourrait être déposée dans certaines juridictions.

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

CETTE PUBLICATION EST FOURNIE "EN L'ETAT" ET AUCUNE GARANTIE, EXPRESSE OU IMPLICITE, N'EST ACCORDEE, Y COMPRIS DES GARANTIES CONCERNANT LA VALEUR MARCHANDE, L'APTITUDE DE LA PUBLICATION A REpondre A UNE UTILISATION PARTICULIERE, OU LE FAIT QU'ELLE NE SOIT PAS CONTREFAISANTE DE PRODUIT DE TIERS. CE DENI DE GARANTIE NE S'APPLIQUERAIT PAS, DANS LA MESURE OU IL SERAIT TENU JURIDIQUEMENT NUL ET NON AVENU.



Contents

Preface 13

1. Introduction to Trusted Solaris Label Encodings 19

Labels-Related Tasks: Who Does What 20

Types of Labels, Their Components and Uses 21

What Labels Ranges Do 22

How Labels Are Used in Access Control Decisions 22

Labels' Components 24

Label Dominance 25

Accreditation Ranges, Label Ranges, and Valid Labels 26

System Accreditation Range 27

User Accreditation Range 28

Account Label Range 29

Account Label Range Examples 30

Session Range 33

Labeled Workspaces 35

Label Availability in Trusted Solaris Sessions 36

More About Labels 37

Authorizations for Upgrading and Downgrading Labels 37

Label Translation 38

Administering Administrative Labels	38
Issues About the Names of Administrative Labels	39
Specifying Whether Users See Administrative Labels' Names	39
Specifying Whether Users See Any Labels	41
Configuring How Labels are Printed on Banner/Trailer and Body Pages	41
Overview of Planning	42
Planning the Encodings File	43
Creating Large Numbers of Labels	47
2. Creating or Modifying the Encodings File	49
Preparing the Label Encodings File	50
For a Site Using a Government-furnished Labels File	50
For a Site Without a Previously-existing Labels File	51
Before Installation	51
After Installation	51
Central Administration	52
Tools for Editing and Checking the label_encodings File	52
Suggested Working Policies	53
Changing the label_encodings File After System Start Up	54
Running Without Labels	54
Setting Up Single-label Operation	55
Sections for Defining Labels	55
Word Order Requirements	57
Adding or Renaming a Classification	57
Number of Classifications	58
Keywords Defined for Classifications	58
Setting Default and Inverse Words	60
Defining Compartment Words	62
Hierarchical Words	64

	Cautions About Mapping Labels to CIPSO Labels	66
	Label_encodings-related Procedures	66
	▼ To Modify the label_encodings (4) File	66
	▼ To Copy the label_encodings File to a Floppy Disk	68
	▼ To Copy the label_encodings File from a Floppy Disk	68
	▼ To Add Sun Extensions to a Pre-Existing Label Encodings File	69
	▼ To Set Up No Labels Operation	70
	▼ To Add or Rename a Classification in the Default label_encodings File	70
	▼ To Specify Default and Inverse Words	72
	▼ To Replace the Single Label in the Default Single-label Encodings File	73
	▼ To Make Your Own Single-label Encodings File	74
	▼ To Configure Labels Not Visible to Users	76
	To Ensure Labels Map to CIPSO Labels	76
3.	Specifying Labels and Handling Guidelines for Printer Output	79
	Labels on Body Pages	79
	Labels, Text, and Handling Caveats on Banner and Trailer Pages	80
	Specifying the Protect As Classification	82
	Specifying Printer Banners	85
	Specifying CHANNELS	88
	Procedures	93
	▼ To Configure PRINTER BANNERS	93
	▼ To Configure CHANNELS	94
4.	Modifying Sun's Extensions in the Local Definitions Section	97
	LOCAL DEFINITIONS Section	97
	Values Specified in the LOCAL DEFINITIONS Section	98
	Specifying Whether Other Labels are Substituted for Administrative Labels	99
	Changing Label Component Names on Label Builders	100
	Specifying Colors for Labels	101

Order of Color Specification	103
Procedures for Modifying Sun Extensions	105
▼ To Specify the System Default for Administrative Label Names (Optional)	105
▼ To Change Label Component Names Used in Label Builders (Optional)	106
▼ To Specify a Default User Clearance and Minimum Label (Optional)	107
▼ To Assign a Color to a Label or Word	108
5. Example: Planning an Organization's Labels	111
Identifying the Site's Label Requirements	111
Problems Encountered in Trying to Meet Information Protection Goals	112
How Trusted Solaris Features Address Information Labeling and Access Control Requirements	112
Climbing the Security Learning Curve	116
Analyzing the Requirements for Each Label	117
PROPRIETARY/CONFIDENTIAL: INTERNAL_USE_ONLY	117
PROPRIETARY/CONFIDENTIAL: NEED_TO_KNOW	118
PROPRIETARY/CONFIDENTIAL: REGISTERED	118
Names of Group Associated with the Need to Know	119
Understanding the Set of Labels	119
Defining the Set of Labels	121
Planning the Classifications	122
Planning the Compartments	122
Planning the Use of Words in MAC	122
Planning the Use of Words in Labeling System Output	123
Planning How to Label Printer Output Pages as Desired	123
Planning for Supporting Procedures	124
Planning Classification Values in a Worksheet	125
Planning Compartment Values and Classification/Compartment Constraints in a Worksheet	126

Planning Clearances in a Worksheet	127
Planning the PRINTER BANNERS Wording in a Worksheet	129
Planning CHANNELS in a Worksheet	130
Planning the Minimums in an ACCREDITATION RANGE Worksheet	131
Planning the Colors in the COLOR NAMES Worksheet	132
Specifying the Labels During Post-Install Configuration	134
Encoding the VERSION	134
Encoding the CLASSIFICATIONS	134
Encoding the SENSITIVITY LABELS	135
Encoding the INFORMATION LABELS	135
Encoding the CLEARANCES	136
Encoding the CHANNELS	137
Encoding the PRINTER BANNERS	138
Encoding the ACCREDITATION RANGE	139
Encoding the Wording for Label Builders, Colors, and Other LOCAL DEFINITIONS Values	140
Encoding the Heading Names for Label Builders	140
Encoding the COLOR NAMES	141
Configuring Users to Enforce Labeling Decisions	142
Configuring Printing To Enforce Labeling Decisions	143
A. Example: Label Encodings File	145
B. Differences Between Default Label Encodings Files	153
Differences Between Single-label and Installed Label Encodings Files	153
Multiple Sensitivity Labels Version	153
Single Sensitivity Label Version	154

Tables

TABLE P-1	Typographic Conventions	16
TABLE 1-1	Components of a Label	24
TABLE 1-2	Bits and Values for Classification and Compartment Components	25
TABLE 1-3	System and User Accreditation Range and Account Label Range Examples	32
TABLE 1-4	Labels in Trusted Solaris Sessions	36
TABLE 1-5	Classifications Planner	43
TABLE 1-6	Clearance Planner	46
TABLE 1-7	Compartment Bit Tracking Table	46
TABLE 1-8	Potential Numbers of Labels for Each Classification	47
TABLE 1-9	Example: Defining Elements of Unique Labels	47
TABLE 2-1	Administrative Actions for Editing the label_encodings File	52
TABLE 2-2	Table Caption	55
TABLE 2-3	Values for Classifications	58
TABLE 2-4	Example Initial Compartments Bit Assignments and What They Mean	59
TABLE 2-5	Initial Compartments for Classifications	60
TABLE 2-6	Bits Available for Classification and Compartment Components	62
TABLE 2-7	Compartments and User Accreditation Range Combinations Planner	63
TABLE 3-1	Example: Minimum Protect As Classification's Effects on the Protect As Classification	84

TABLE 3-2	PRINTER BANNERS Planner	87
TABLE 3-3	CHANNELS Planner (for Prefixes, Channel Words, and Suffixes)	92
TABLE 4-1	Color Names Planner	105
TABLE 5-1	Printer Label Range Example Settings in Various Locations	124
TABLE 5-2	Classifications Planner	125
TABLE 5-3 Table	Compartments and User Accreditation Range Combinations Planning	126
TABLE 5-4	Compartment Tracking Table	127
TABLE 5-5	Clearance Planner	128
TABLE 5-6	Printer Banners Planner	129
TABLE 5-7	Channels Planner (for Prefixes, Channels, and Suffixes)	131
TABLE 5-8	ACCREDITATION RANGE Minimum Values	132
TABLE 5-9	Color Names Planner	132

Figures

Figure 1–1	Comparing the Label of a Text Editor with the Label of a File to be Edited	24
Figure 1–2	How System Accreditation Range Is Constrained By Rules	28
Figure 1–3	ACCREDITATION RANGE Portion of label_encodings File	29
Figure 1–4	Constraints on Account Label Ranges	31
Figure 1–5	Comparison of Session Ranges	34
Figure 1–6	Cumulative Effect of Constraints on a Session Range	35
Figure 1–7	Workspace Switch Area	36
Figure 1–8	Example Planning Board for Label Relationships	45
Figure 2–1	Bit Combinations Defining Hierarchical Relationships	64
Figure 2–2	REQUIRED COMBINATIONS Used to Establish Hierarchies	65
Figure 3–1	Label Automatically Printed on Body Pages	80
Figure 3–2	Typical Print Job Banner Page	81
Figure 3–3	Differences on Trailer Pages	82
Figure 3–4	Protect As Statement	83
Figure 3–5	How the Classification Printed on Banner and Trailer Pages is Derived	84
Figure 3–6	Commercial Use of the PRINTER BANNERS Specification on the Print Job's Banner Page	86
Figure 3–7	Government Use of the PRINTER BANNERS Section of the Banner Page	86

Figure 3-8	Commercial Use of the CHANNELS Specification on the Print Job's Banner	
Page	88	
Figure 3-9	Government Use of the CHANNELS Specification on the Banner Page	89
Figure 4-1	Label Component Names on Example Label Builder	101
Figure 4-2	Window Label with a Background Color from the COLOR NAMES	
Section	102	
Figure 5-1	Automatic Labeling of Print Jobs	113
Figure 5-2	Label Automatically Printed on Body Pages	114
Figure 5-3	Handling Guidelines on Banner and Trailer Pages	114
Figure 5-4	How a Printer With a Restricted Label Range Handles Jobs at Various	
Labels	115	
Figure 5-5	Automatic Labeling of Email	115
Figure 5-6	A User Receiving Email within His Account Label Range	116
Figure 5-7	Example Planning Board for Label Relationships	121
Figure 5-8	Label Builder With Changed Headings	141

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 the `label_encodings(4)` file. This manual provides needed background and describes how to edit, check, and install the `label_encodings` file.

Who Should Use This Book

This book is for security administrators, who are responsible for defining the organization's labels, and for those who assume the security administrator role to implement the labels in the site's `label_encodings` file on the Trusted Solaris system.

Note - Even though the Trusted Solaris environment can be configured with no visible labels, labels are always being used, and mandatory access control checks are always being made. Therefore, the security administrator role must always configure a `label_encodings` file as described in this manual.

Related Books

Prerequisite knowledge is contained in the following books in the Trusted Solaris documentation set:

- *Trusted Solaris User's Guide*

- *Trusted Solaris Administration Overview*
- *Trusted Solaris Installation and Configuration*
- *Trusted Solaris Administrator's Procedures*
- *Trusted Solaris Audit Administration*
- *Trusted Solaris 8 Transition Guide*
- *Compartmented Mode Workstation Labeling: Encodings Format*

Before You Read This Book

The person who works in the security administrator role to configure labels should:

- Understand how to administer the Solaris or compatible operating environment, the Common Desktop Environment (CDE) window system, Solstice AdminSuite system administration tools, and the NIS+ (or NIS) system for central administration of configuration files
- Know how to work in the Trusted Solaris environment as a normal (non-administrative) user (as described in the *Trusted Solaris User's Guide*)
- Understand the administrative concepts and know how to use the administrator's tools described in the *Trusted Solaris Administration Overview* and *Trusted Solaris Administrator's Procedures* manuals

Administrative tasks are divided among several administrative roles. The administrator's procedures manual describes how a user assumes the security administrator role and uses administrative actions to perform the work described in this manual.

- Understand how administrative tasks are divided among roles at your site
- Some sites may assign the label encodings tasks to a locally-created administrative role.
- Understand the security requirements of your agency or organization.

The necessary level of knowledge may be acquired through:

- Training

For information about the Trusted Solaris training class, see the course description or visit the Sun Education catalog.

- Documentation

The Trusted Solaris manuals are available in the following formats:

- At Sun's documentation website at `docs.sun.com`

- On the AnswerBook CD shipped with the product

AnswerBooks are document collections you can install on your local computer or on a document server and view onscreen. AnswerBooks for the Trusted Solaris operating environment, for the bundled CDE window system,; and for the base Solaris operating environment are on the Trusted Solaris AnswerBook CD.

- Printed versions

If not obtained when the product was purchased, the documentation set can be ordered through SunStore.

Ordering Sun Documents

Fatbrain.com stocks documentation from Sun Microsystems, Inc.

For a list of available documents and how to order them, visit <http://www1.fatbrain.com/documentation/sun>.

How This Book Is Organized

- Chapter 1

Provides labels-related concepts and planning steps for the security administrator who prepares the site's `label_encodings` file.

- Chapter 2

Describes how to create and check the `label_encodings` file.

- Chapter 3

Describes the labels and handling caveats on printer output and gives procedures for modifying them.

- Chapter 4

Describes the optional `LOCAL DEFINITIONS` section. Describes how to use the keywords in this section to set a system-wide minimum label and clearance for users; change the names of administrative labels, specify whether administrative labels display, change the names of labels' components on label builders, and specify colors for labels.

- Chapter 5

Models how a site analyzes its label requirements and creates a simple `label_encodings` file, which is shown in Appendix A.

- Appendix A

Contains an example of a simple `label_encodings` file that goes along with the chapter on planning.

Type Styles Usage in Text and Examples

The following table shows and explains the type styles used in this manual.

TABLE P-1 Typographic Conventions

Type Face	Meaning	Example
Literal	The names of commands, files, and directories, on-screen computer output	Edit your <code>.login</code> file. Use <code>ls -a</code> to list all files. <code>hostname%</code> You have mail.
UserType	What you type, contrasted with on-screen computer output	<code>hostname% su</code> Password:
Variable	Argument name in a command-line. You replace the argument with a real name or value.	To delete a file, enter <code>rm filename</code> . <code>hostname% rm myfile</code>
Title or Emphasis	Book titles, new words or terms, or words to be emphasized	Read Chapter 6 in <i>User's Guide</i> . These are called <i>class</i> options. You <i>must</i> be root to do this.

Trusted Solaris Prompts

The following table shows the Trusted Solaris prompts.

Shell	Prompt
C shell prompt	<i>hostname%</i>
Bourne shell and Korn shell prompt	\$
Profile Shell prompt	\$
root prompt (with any shell)	#
PROM mode prompt (SPARC only)	>

Introduction to Trusted Solaris Label Encodings

This chapter prepares the administrator who is responsible for creating the `label_encodings(4)` file. This chapter covers the following topics:

- “Labels-Related Tasks: Who Does What” on page 20
- “Types of Labels, Their Components and Uses” on page 21
- “Overview of Planning ” on page 42
- “Planning the Encodings File” on page 43
- “Creating Large Numbers of Labels” on page 47

This chapter assumes you have read the following:

- “Assuming a Role and Working in a Role Workspace” in the *Trusted Solaris Administrator’s Procedures* manual, which prepares the security administrator to assume the security administrator role
- “Understanding Labels” in *Trusted Solaris Administration Overview*

Even if you plan to run without visible labels, read all of this chapter and the next, and especially see “Running Without Labels ” on page 54 of this manual.

Note - This chapter does not give details about encoding complex relationships between classifications, inverse, and hierarchical words that are needed by some organizations. 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], which is included in the Trusted Solaris document set. Keep in mind that information labels and their components are not used at Sun when using the DIA manual (see also “Sections for Defining Labels” on page 55).

Labels-Related Tasks: Who Does What

The following defines what needs to be done and can help to identify who should do this task:

- The *security administrator* is the person who defines and plans the implementation of an organization's security policy, establishes information-protection procedures, makes sure computer users and administrators are properly trained, and monitors compliance.
- The task of implementing security policy is performed by an administrator who logs in and then assumes an administrative role called the security administrator role.
- The security administrator who defines the site's security policy may or may not be the same person who implements the policy while working in the security administrator role.
- The security administrator role is assigned to one or more administrators who fully understand Trusted Solaris administration and who are cleared to view and to protect the highest level of information processed on the Trusted Solaris system.
- The security administrator role has the tools and capabilities to put the organization's security policy into effect while configuring the system.
- The components that make up labels are specified in each organization's `label_encodings(4)` file.
- The security administrator specifies the numeric values and bits that make up the internal representation of label components.
- Certain types of labels must be defined.
- The labeling software translates between the internal and human-readable forms of labels, from their binary representation to the character strings assigned to them, based on the rules in the `label_encodings` file.
- A default version of the `label_encodings` file is initially installed on every Trusted Solaris host.
- The install team usually replaces the initially-installed `label_encodings` file with a version with the site's own labels. (The default version may sometimes be used in non-production environments while administrators or programmers are learning the system.)
- One of the responsibilities of the security administrator role is to create the `label_encodings(4)` file to replace the default version.
- Every computer in the system needs its own copy of the master `label_encodings` file. For interoperability, the label encodings file on every computer in the system should be the same, or at least should recognize each other's labels.

Types of Labels, Their Components and Uses

Two types of labels are used in the Trusted Solaris system:

- Clearance labels
- Sensitivity labels

Labels, label ranges, and clearances are all used to determine who gets access to what in the Trusted Solaris system. Clearance labels (which are also called clearances) are assigned to users and to processes that act on their behalf. Sensitivity labels are assigned to processes and to files and directories. Sensitivity labels are often referred to simply as *labels* in the Trusted Solaris documentation set.

Some objects have a default label range that allow access at all labels, and the security administrator can restrict that label range. These objects can be accessed at a single-label within the defined label range. Objects with label ranges include the following:

- All hosts and networks with which communications are allowed
- Network interfaces
- File systems
- Allocatable devices: such as tape drives, floppy drives, CD-ROM devices, and audio devices
- Other devices that are not allocatable, for example, printers, workstations (controlled through a label range set on the framebuffer, `fb0`), and serial lines when they are configured for use at login.

See the various means for setting labels described in *Trusted Solaris Administrator's Procedures*. "Managing Device Allocation and Setting Device Label Ranges" in *Trusted Solaris Administrator's Procedures* describes how to set label ranges on devices.

The following sections detail these concepts and give examples:

- "How Labels Are Used in Access Control Decisions" on page 22
- "Labels' Components" on page 24
- "Label Dominance" on page 25
- "Accreditation Ranges, Label Ranges, and Valid Labels" on page 26
- "System Accreditation Range" on page 27
- "User Accreditation Range" on page 28
- "Account Label Range" on page 29
- "Account Label Range Examples" on page 30

- “Session Range” on page 33
- “Labeled Workspaces” on page 35
- “Label Availability in Trusted Solaris Sessions” on page 36

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 allocate devices, thereby restricting the labels at which files can be written to storage media in these devices
- The labels at which users can send jobs to printers
- The labels at which users can log into workstations—in addition to the user’s label range, a label range on the frame buffer may be used to restrict access

Labels are automatically assigned to email messages and printed on printer output.

How Labels Are Used in Access Control Decisions

In the Trusted Solaris system, both discretionary access control checks and mandatory access control checks must be passed before access is allowed to an object. Discretionary access control is based on `Permission Bits` and `Access Control Lists` (see the `DEFINITIONS` section of the *Intro(1)* man page, if needed).

Most of the Trusted Solaris documentation does not use the term sensitivity label. In releases beginning with Trusted Solaris 7, information labels are not supported, so it is no longer necessary to differentiate between sensitivity labels and information labels. However, because the label encodings file still has sections for both sensitivity labels and information labels, this document uses these terms where it is needed to clarify the differences.

Mandatory access control compares the label and clearance label of a process running an application with the label or the label range of anything that the process tries to access, according to a set of rules that is sometimes called the system security policy.

- Site security policy is the security policy set up by an organization to protect its information.

Using Trusted Solaris may be part of the site’s security policy.

- System security policy is the set of rules that is enforced by the operating system software to protect information being processed on the Trusted Solaris system.

If the term security policy appears by itself, consider the context.

The write up/read down (*wurd*) rule applies when a process tries to access an object.

Write Up to Session Clearance and Write Equal	$SL[Process] \leq SL[Object]$
Read Down and Read Equal	$SL[Process] \geq SL[Object]$

As shown in the previous table, writes up are always limited by the session clearance. A process cannot read or write an object whose label is higher than the process's clearance.

Strictly speaking everything, whether it is a file, directory, device, or other object, is treated as a file in a UNIX system. However, files and directories have slightly different access rules from each other and from process objects, System V IPC objects, STREAMS objects, network endpoint objects, device objects, and X window objects. In addition, an object can be accessed three different ways shown in the following list, and for each of the three ways an object can be accessed, a slightly-different set of rules applies:

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

For more details about the rules that are enforced when various types of access are attempted, see the `DEFINITIONS` sections in `Intro(1)` and `Intro(2)` man pages.

Simple Mandatory Access Control Example

If a user brings up a text editor in a workspace with a label of `PUBLIC`, the process executing the text editor gets the same label as the workspace.

Figure 1–1 shows a comparison between two labels used in making an access control decision. When a user in a workspace with the label `INTERNAL_USE_ONLY` brings up a text editor, the label of the process running the text editor is automatically set to be equal to the label of the current workspace, and the text editor displays a label of `INTERNAL_USE_ONLY`. When the text editor attempts to open a file for editing, the label of the process running the text editor is compared to the label of the file. In the example, because the two labels are equal, access for writing is allowed.

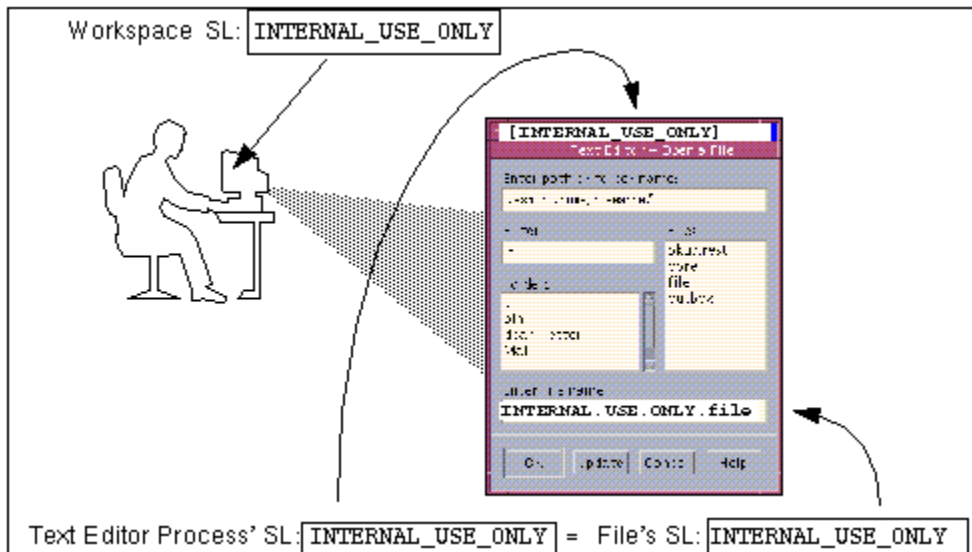


Figure 1-1 Comparing the Label of a Text Editor with the Label of a File to be Edited

If the label of a file is less than that of the text editor, the file can be opened only for reading. (For example, a normal user can use a text editor to open and read a system file at ADMIN_LOW while working at INTERNAL_USE_ONLY, but the text editor cannot save a change to the file. Another consequence of the WURD rule, because of the read down requirement a user cannot see a file whose label is higher than the current working label. However, if a normal user knows the name of a file that has a higher label, the text editor could be used to make a change to the higher-labeled file, even though the user cannot see the file's name.

Labels' Components

Both labels and clearance labels are made up of a single *classification* and zero or more compartment words. The human-readable format of labels is shown in the following table.

TABLE 1-1 Components of a Label

Classification	Compartments
name	[word1, word2, ..., wordN]

The security administrator creates all the label components by assigning names and numeric values to classifications and assigning compartment words to bits in the `label_encodings(4)` file. Along with a classification field of 15 bits, each label and clearance label has a 256 bit field available for compartments, as shown in Table 1–2. Each compartment word has one or more compartment bits assigned. The same compartment bit may be assigned to more than one word.

TABLE 1–2 Bits and Values for Classification and Compartment Components

Classification	Compartments
15 bits	256 bits
32,767 possible values	possible compartment and bit combinations: 10 to the 70 power
256 values limit enforced	

The classification portion of a label indicates a *relative level of protection*. When a label is assigned to an object, the label’s classification indicates *the sensitivity of the information contained in the object*. When a clearance label is assigned to a user, the classification portion of the clearance label indicates *the user’s level of trust*.

The use of one or more optional compartment words in a label can help to group individuals with a common area of interest and to further identify how information should be handled. A compartment word can be used to represent what ever kind of grouping you desire, such as a work group, a department, a division, or a geographical area.

For example, a classification of NEED TO KNOW in a label can be restricted by the presence of one or more compartment words defined with department names, such as ENGINEERING or HUMAN RELATIONS or LEGAL. A file with NEED TO KNOW LEGAL would be available only to individuals who have the NEED TO KNOW classification and the LEGAL compartment in their clearances.

Label Dominance

When any type of label 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. This comparison of security levels is based on classifications and compartments in the labels. The classification of the dominant label must be equal to or higher than the classification of the second label, and the dominant label must include all the compartments in the other label. Two equal labels are said to dominate each other. By these criteria, TS A dominates TS and TS dominates TS.

Another kind of dominance called *strict dominance* is sometimes required for access. One label *strictly dominates* another label when the first label has a security level greater than the security level of the other label. 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. By these criteria, TS A B strictly dominates TS A and S A but does not strictly dominate TS A B or S C. Because S C contains a word (C) that is not in the TS A B label, and it does not contain all the words in TS A B, the two labels are said to be *disjoint*.

The security administrator must make sure that the clearance labels assigned to user or role accounts dominate all the labels the account is allowed to access. An account's clearance must contain the highest classification and all the compartment words that are in any label that the account needs to work at. Suppose, for example, that a `label_encodings` file prohibits the combination of compartments A, B, and C in a label and that the minimum label allowed is TS with no compartments. TS A B C would be a valid clearance label although it would not be a valid label. As a clearance, it would let a user work at TS A, TS B, TS C, and TS.

Accreditation Ranges, Label Ranges, and Valid Labels

Certain combinations of label components may be disqualified by rule specified by the security administrator in the `label_encodings` file. By defining combination rules, the security administrator *implicitly defines* all the organization's usable labels.

A *valid* or *well-formed* label is one that satisfies any combination rules that may have been defined by the security administrator. The combination rules are defined using one of the means listed below:

- *Initial compartments* (compartment bits) can be assigned to a classification.
Initial compartment bits are always associated with the classification when it appears in a label. For more details, see also “Adding or Renaming a Classification” on page 57 for more about default words and inverse words that are assigned to initial compartment bits.
- A *minimum classification*, *output minimum classification*, and *maximum classification* can be associated with any word.
- *Hierarchies* among words can be defined by the *bit patterns* chosen for each word.
- *Required combinations* of words can be specified.
- *Combination constraints* can be specified for words.
- A *minimum clearance* and a *minimum sensitivity label* must be specified.

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

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

- System accreditation range
- User accreditation range

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

See the following sections: System Accreditation Range and User Accreditation Range for illustrations of how labels can be disallowed by some of the means listed in the previous list. Chapter 2 gives more details on how the rules are specified.

System Accreditation Range

The system accreditation range always includes administrative labels `ADMIN_HIGH` and `ADMIN_LOW`. The system accreditation range also includes all the well-formed labels that can be made up out of all label components defined in the `label_encodings` file.

Administrative role accounts are usually the only accounts configured to be able to work at all of the labels within the system accreditation range. An organization may also set up normal user (non-role accounts) to be able to perform a task that can only be done at one of the administrative labels `ADMIN_HIGH` or `ADMIN_LOW`. A good example in the default Trusted Solaris system is the `install` user account that is used for configuring the system after installation. The `install` account needs to log in at `ADMIN_LOW` because the site's `label_encodings` file is not yet installed, and therefore the site's non-administrative labels are not yet defined.

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

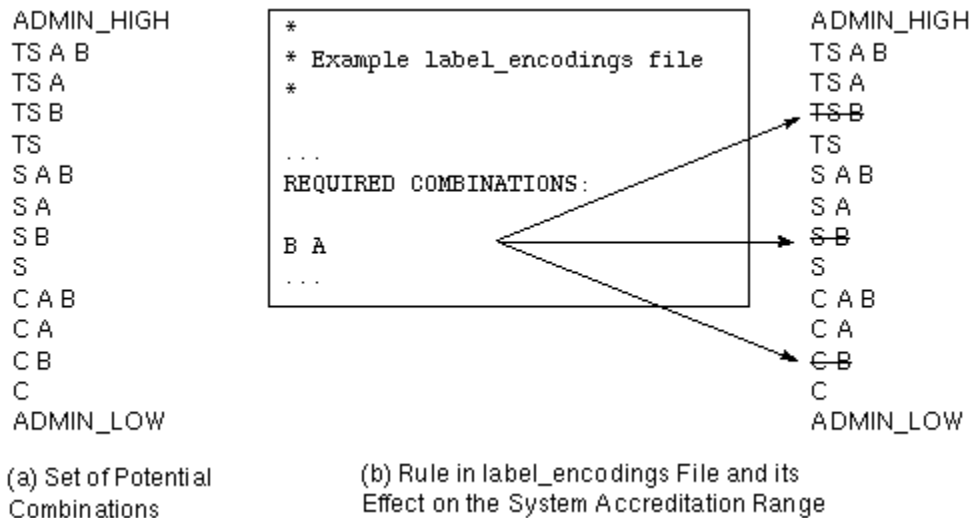


Figure 1-2 How System Accreditation Range Is Constrained By Rules

Figure 1-2 (a) shows all potential combinations given the classifications, TS (TOP SECRET), S (SECRET), and C (CONFIDENTIAL), and the compartments, A and B.

Figure 1-2 (b) shows a typical rule from the REQUIRED COMBINATIONS subsection of the SENSITIVITY LABELS section and its effects. The arrows point to the labels disqualified by the rule, which appear with lines through them. The REQUIRED COMBINATIONS syntax B A means that any label that has B as a compartment must also contain A. (Note that the converse is not true; compartment A is not required to be combined with any other compartments.) Since compartment B is only permitted when A is also present, the labels TS B, S B, and C B are not well-formed and hence are not in the system accreditation range.

User Accreditation Range

The *user accreditation range* is the largest set of labels that normal users can access on a Trusted Solaris system. The user accreditation range always excludes ADMIN_HIGH and ADMIN_LOW. The user accreditation range is further constrained by any rules that constrain the system accreditation range. In addition, the user accreditation range can also be constrained by a set of rules in the ACCREDITATION RANGE section. The following figure continues the System Accreditation range example, showing three different types of rules in the ACCREDITATION RANGE section and their effects on the user accreditation range. The arrows point to the well-formed labels permitted by the particular rule.

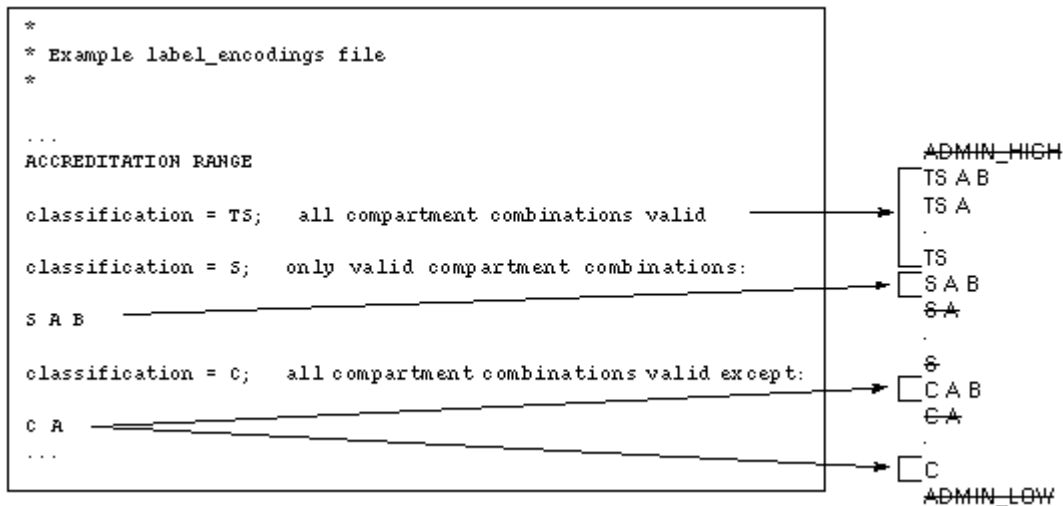


Figure 1-3 ACCREDITATION RANGE Portion of label_encodings File

As shown in the right column, the user accreditation range excludes ADMIN_HIGH and ADMIN_LOW. The rule for the TS classification includes all TS combinations except TS B. However, because TS B, along with S B and C B, were previously overruled by the REQUIRED COMBINATIONS rule B A illustrated in Figure 1-2, TS A B, TS A, and TS are the only allowed TS combinations. With S A B defined here as the only valid combination for the S classification, S B is excluded again. All C combinations except C A are valid according to the rule shown for the C classification, but since C B was overruled earlier, the only permitted combinations for the C classification are C A B and C alone without compartments.

Note - Make sure that the minimum clearance you plan to set in the label_encodings file is dominated by all the clearances you plan to assign to users. Also make sure that the minimum sensitivity label is similarly dominated by all the minimum labels you plan to assign to users.

Account Label Range

The *account label range* is the range of labels available to an individual user or role account. It governs which labels are available for the user to work at when logging into the system. (See “Setting the Session Level” in Chapter 2, “Accessing and Leaving the Trusted Solaris Environment,” in the *Trusted Solaris User’s Guide* and “Session Range” on page 33 of this chapter.)

The labels available in the account label range are constrained by:

- The user accreditation range—an unauthorized user cannot use any labels that have been disqualified for the user accreditation range in the `label-encodings` file.
- The top and bottom of the range can be set by security administrator role who defines security attributes for the account using the SMC User Accounts tool. If no values are set for the account, a `DEFAULT USER SENSITIVITY LABEL` and the `DEFAULT USER CLEARANCE` values in the optional `LOCAL DEFINITIONS` section of the `label_encodings` file are used, if they are defined. Otherwise, the minimum sensitivity label and minimum clearance set in the `ACCREDITATION RANGE` section of the `label_encodings` file are used. The values for each account are stored in the `user_attr(4)` database:
 - The user clearance defines the top of the account label range.
A clearance does not have to be a valid label. Because it must dominate all labels at which the account is to work, the clearance must contain all the components of all the labels at which the account is to work.
 - The minimum label sets the bottom of the account label range.
The minimum sensitivity label set in the `label_encodings` file defines an absolute minimum on labels at which any unauthorized users can work.
The SMC User Accounts Properties dialog allows the setting of an account's minimum label to below the `label_encodings`-defined minimum, if the account has also been assigned a profile with the `Set Label Outside User Accred Range` authorization. For example, the install user can log in at `ADMIN_LOW` because that user account has the `Outside Accred` profile, with the `e Set Label OUTside User Accred Range` authorization.

Account Label Range Examples

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

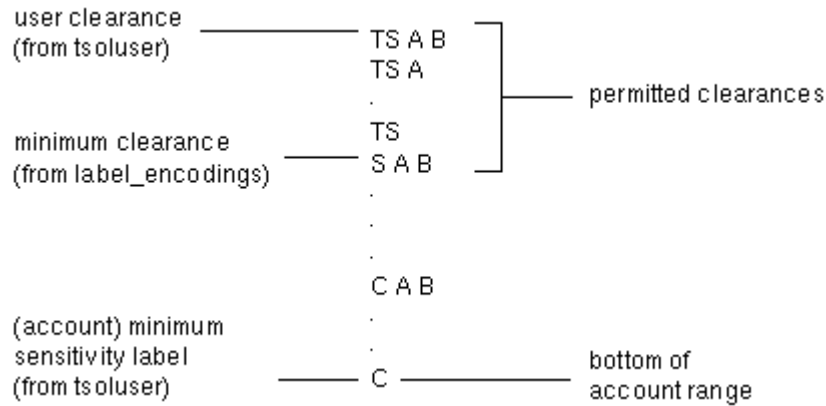


Figure 1-4 Constraints on Account Label Ranges

TS A B is the highest label in the user accreditation range from the ongoing example and contains the only two compartments permitted to appear in a label with any classification: A and B. The example user account range illustrated on the left of the previous figure is bounded at the top by TS A B, which the clearance assigned to the account, and at the bottom by C, the (account) minimum label. As a result of these definitions, the account is constrained to work at labels TS A B, TS A, TS, S A B, C A B, or C. The permitted clearances shown are TS A B, TS A, TS and S A B, with the minimum clearance of S A B set in the `label_encodings` file. Even if TS A B was not a valid label, the security administrator could assign it as a clearance to allow the account to use any valid labels that are dominated by TS and that contain the words A and B. In contrast, if TS was assigned as the account clearance, the only two labels at which the user could work would be TS and C, because TS without any compartments does not dominate S A B or C A B.

Note - If you specify the account's clearance to be the same as the account's minimum label, the user can only work at the specified single label. To do this you would also need to make sure that the minimum clearance you set in the `label_encodings` file is dominated by all the account clearances you plan to assign.

The following table summarizes the differences between the potential label combinations, the system accreditation range, the user accreditation range, and some example account label ranges. Normal users without any authorizations can work only with the labels in the User Accreditation Range column. The fourth column in Table 1-3 shows the Account Label Range for a user with a clearance of TS A B and a minimum label of S A B, which allows the user to work with the following set of labels: TS A B, TS A, TS, and S A B. As shown in the fifth column of Table 1-3, an account with a clearance of TS and a minimum label of C would be allowed to work only with TS, S, and C labels, because all the other valid labels dominated by TS include the words A and B, which are not in the clearance. A sixth column shows a

user authorized to work outside the user accreditation range, assigned a single label of ADMIN_LOW.

TABLE 1-3 System and User Accreditation Range and Account Label Range Examples

Possible Labels	System Accreditation Range	User Accred.Range	Account Label Range (with TS A B Clearance, S A B Min Label)	Account Label Range (with TS Clearance, C Min Label)	Account Label Range (with ADMIN_LOW Clearance and Min Label and the use all defined labels authorization)
ADMIN_HIGH	ADMIN_HIGH				
TS A B	TS A B		TS A B		
TS A	TS A	TS A	TS A		
TS	TS	TS	TS	TS	
S A B	S A B	S A B	S A B		
S A					
S				S	
C A B	C A B				
C A	C A				
C	C	C		C	
ADMIN_LOW	ADMIN_LOW				ADMIN_LOW

Session Range

Setting the range of labels available during a session is possible only when a user account is configured to use multiple labels. The user configured to work at a single label uses that single label throughout every login session. If a user account is set up to use multiple labels, that user can specify which labels are available during the session by doing one of the following:

- Restrict the session to a single 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

When a user logs in and starts a session on a Trusted Solaris host, the Workstation Information dialog box displays. The following indicator displays below the console message area when a user is configured to work only at a single label:

```
Single Label Session Label: name_of_label
```

The following indicator displays below the console message area with a check box to the left when the user is configured to work at multiple labels:

```
Restrict Session To a Single Label
```

If the user clicks the OK button after checking the box, then a Single-label Login: Setting Session Label dialog box displays, or if the user leaves the box unchecked, a Multilabel Login: Setting Session Clearance dialog box displays. The user then chooses the label or clearance for the session from the dialog box .

The choice of session clearances available in the clearance dialog box range from the account clearance down to the higher of the (accreditation) minimum clearance and the (account) minimum label, subject to any additional required combinations or constraints from the clearance rule definitions in the `label_encodings` file. The single label dialog allows the account to select among all the valid labels that are dominated by the account's clearance and that dominate the account's minimum label, subject to any required combinations or constraints from the label rule definitions in the `label_encodings` file.

The single label or session clearance chosen at login is in effect throughout the session until logout. During a multilabel session, the user may work at any valid label that is dominated by the session clearance and that dominates the user's minimum label. Processes started on behalf of a user get a process clearance equal to the session clearance.

The *session range* is the set of labels available to a user during a Trusted Solaris session. It is a function of:

- The account label range
- The account's choice of session mode (single-label or multilabel)
- The value the account enters in the Single-label Login: Setting Session Label dialog box (if single-label session) or the Multilabel Login: Setting Session LabelClearance dialog box (if multilabel session)
- The label range for the user's workstation
- The security administrator can restrict the default ADMIN_LOW to ADMIN_HIGH label range on a workstation by using the Device Allocation Manager to set the restricted label range on the framebuffer device, for example on fb0) For more information, see "Session Range" on page 33.

In the ongoing example from Figure 1-4 that is continued in the following figure, the user can specify a session clearance using any well-formed label between TS A B and S A B.

In the next figure, (a) continues the example showing the range of labels available if the user selects a multilabel session with a session clearance of S A B. Since the other potential labels between S A B and C have been disallowed, the user can only work at S A B, C A B, or C.

(b) shows the range of labels if the user chooses a single-label session with a session label of C A B. Note that C A B is below the minimum clearance but is accessible because the user is selecting a session label, not a clearance. Since this is a single-label session, the user can work at only one label; in this example, the user specified C A B, although S A B or C could have been chosen instead.

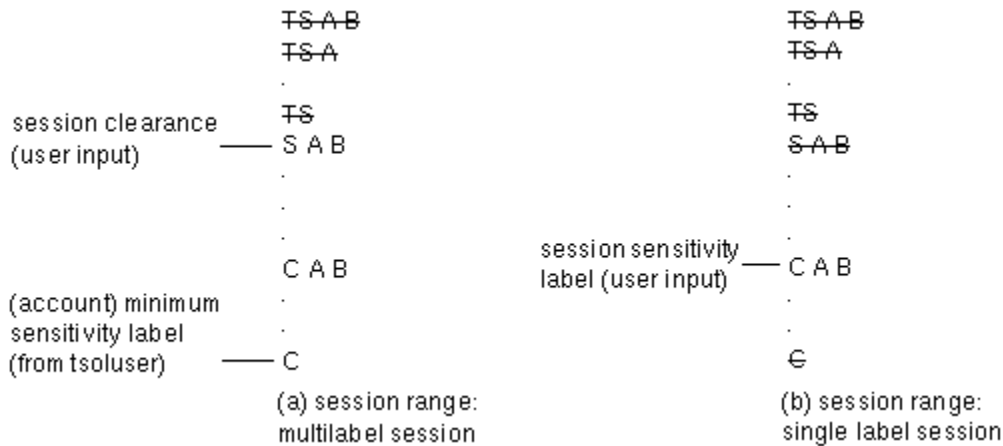


Figure 1-5 Comparison of Session Ranges

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

ADMIN_HIGH	ADMIN_HIGH	ADMIN_HIGH	.	.
TS A B	TS A B	TS A B	TS A B	TS A B
TS A	TS A	TS A	TS A	TS A
TS B	TS B	.	.	.
TS	TS	TS	TS	TS
S A B	S A B	S A B	S A B	S A B
S A	S A	S A	.	.
S B	S B	.	.	.
S	S	S	.	.
C A B	C A B	C A B	C A B	C A B
C A	C A	C A	.	.
C B	C B	.	.	.
C	C	C	C	C
ADMIN_LOW	ADMIN_LOW	ADMIN_LOW	.	.
(a) Set of Potential Combinations	(b) System Accreditation Range	(c) User Accreditation Range	(d) Account Label Range	(e) Multilabel Session Range Using S A B

Figure 1-6 Cumulative Effect of Constraints on a Session Range

Labeled Workspaces

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

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

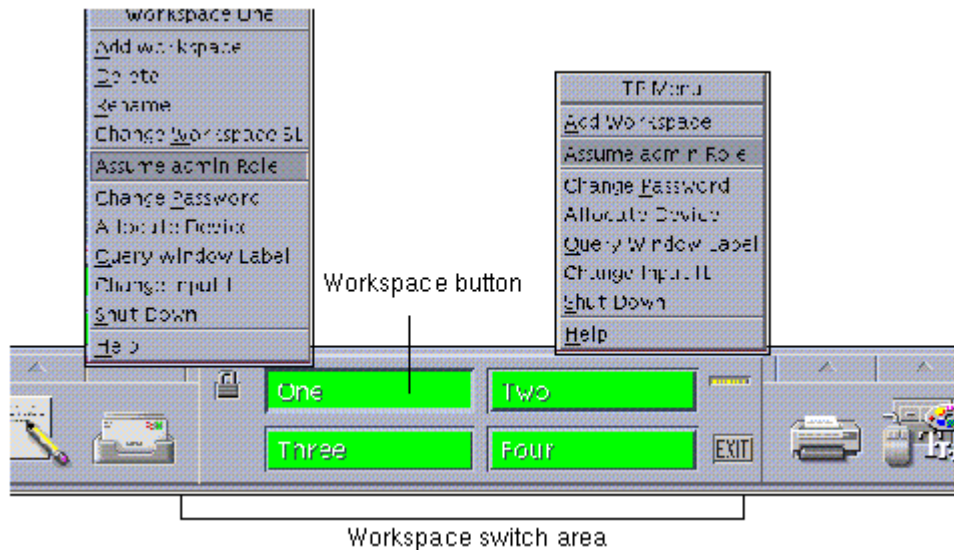


Figure 1-7 Workspace Switch Area

The user can bring up additional workspaces using the Add Workspace option from the Trusted Path menu. The label of the active or selected workspace is assigned to each new window or normal user workspace that is created in that workspace. A newly-created file or directory is assigned the label of the process that creates it, which is usually the label of the workspace where the process is started.

Any user allowed a multilevel session can relabel any of the workspaces to any label that is dominated by the current session clearance. Users relabel workspaces by using the Change Workspace Label option on the Trusted Path menu. Users switch labels by changing the label of a workspace and then clicking its button.

The label of the first workspace that comes up in subsequent login sessions after the first login can be at any label of the user's choosing within the account's label range. Any user can use the Startup dialog box in the Tools subpanel on the Front Panel to configure startup sessions' characteristics.

Label Availability in Trusted Solaris Sessions

The following table shows session label limitations and availability based on users' session choices; it continues the example from Figure 1-6. The left column identifies the types of label settings used in sessions. The middle two columns apply to a Multilevel Session and the right two columns apply to a Single-level Session. The columns labeled General Case show how the label types are determined. The columns marked Example show a typical user's session selections at login.

TABLE 1-4 Labels in Trusted Solaris Sessions

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

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

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

More About Labels

A label can only be changed by a user or an administrator who has the appropriate authorization.

Authorizations for Upgrading and Downgrading Labels

The authorization to change a label to one that dominates it is called the `Upgrade File Label` authorization. The authorization to change a label to one that it dominates is called the `Downgrade File Label` authorization. For definitions for these authorizations, see `/etc/security/auth_attr`.

Options for Restricting Users to a Single Label

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

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

When the security administrator role has configured an account with a account label range that includes multiple labels, the user can voluntarily restrict a working session to a single label, which is explained in the next section.

Label Translation

Label translation occurs whenever programs manipulate labels. Labels are translated to and from the character-coded strings to the binary representation. For example, when a program such as `getlabel(1)` 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 form. And when the `setlabel(1)` program sets a label specified on the command line, the character-coded string that makes up the label's name must be translated to the label's internal representation. The Trusted Solaris system permits label translations only if the calling process's label dominates the label to be translated. If a process attempts to translate a label that the process' SL does not dominate, the translation is disallowed. The `sys_trans_label` privilege overrides this restriction.

So, 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.

Administering Administrative Labels

Two default administrative labels are always defined.

- `ADMIN_LOW` is the lowest label in the system with a classification value of 0 and no compartments or markings.

The `ADMIN_LOW` label is dominated by every other label.

- `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` label and the `ADMIN_HIGH` clearance have all 256 compartment bits set to 1. The `ADMIN_HIGH` label dominates all other labels.

System files and commonly-available executables are assigned an `ADMIN_LOW` label. According to the WURD (write up read down) MAC rule, anyone working at any label can read files at `ADMIN_LOW`, unless the files' DAC permissions deny read access to the account attempting the reading. Files that contain data that should not be viewed by normal users, such as system log files, the `label_encodings` and `vfstab_adjunct` files are maintained at `ADMIN_HIGH`. To allow administrators access to protected system files, the `ADMIN_LOW` and `ADMIN_HIGH` administrative labels are assigned as the minimum label and clearance for the default roles. The following sections of this manual describe issues about administrative labels that the security administrator needs to consider.

- “Issues About the Names of Administrative Labels” on page 39
- “Specifying Whether Users See Administrative Labels’ Names” on page 39
- “Specifying Whether Users See Any Labels” on page 41

Issues About the Names of Administrative Labels

The site's security administrator role can choose to do the following:

- Specify alternate names for administrative labels (not recommended)
Because this is not recommended, this manual does not describe how to do it.
- Prevent normal users from seeing the names of administrative labels by substituting names of the lowest and highest labels in the user accreditation range.
See “Specifying Whether Users See Administrative Labels’ Names”.
- Prevent normal users from seeing any labels.
See “Specifying Whether Users See Any Labels” on page 41

Specifying Whether Users See Administrative Labels’ Names

The option to set a *label view* allows the security administrator role to determine whether the *names* for administrative labels are displayed to non-administrative users. If the label view is set to external, another label is substituted: `ADMIN_HIGH` is demoted to the maximum label and `ADMIN_LOW` is promoted to the minimum label within the user accreditation range.

Some reasons a site might hide the names of administrative labels are:

- The site assigns each user a single label to work at and chooses not to train users about administrative labels.
- The site's security policy treats the names of administrative labels as classified information.

The label view is set to be either `INTERNAL` or `EXTERNAL` in several different ways that are listed in order of precedence, with the lowest first.

- If not otherwise overridden, the system-wide label view is `EXTERNAL`.
- An optional system-wide setting can be made in the `label_encodings(4)` file
The default `label_encodings(4)` file has the label view set to `External` in the `LOCAL DEFINITIONS` section. If the optional definition is not found in the file, the default system-wide setting of `EXTERNAL` is used.
- The User Accounts and Administrative Roles Tools can set an individual value for any user or role account
The Security Administrator role can make an individual setting in the `Trusted Solaris Attributes` tab that is found in both the `User Accounts` and `Administrative Roles Properties` dialogs. The values are stored in the `user_attr(4)` file entry for the user or role account.

Note - Do not edit the `user_attr` file directly. Change any account's labels views using the SMC tools.

The View: choices are `External` | `Internal` | `System Default`

If the `System Default` is chosen, the Default Label View is *value* in the optional `LOCAL DEFINITIONS` section of the `label_encodings` file applies.

- Programs can use library routines to manipulate the label view of the process running the program.

The label view setting in a process can override the system-wide setting. A process's label view is set to be either *internal*, *external*, or *sys*. If *sys*, the process's label view is whatever is set in the `label_encodings` file, and if no value is set in the file, then the default of `External` is used.

A process's label view gets set indirectly through the following:

- From the `user_attr` entry for the owner of the process
When a user or role starts a process, the `user_attr` file entry for the account is consulted and the process attribute flag `PAF_LABEL_VIEW` is set using `setpattr(2)`, according to the label view specified in the 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, the `PAF_VIEW_DEF` is set equal to the optional setting in the `label_encodings(4)` file, or the default of `EXTERNAL` that applies if the option is not set.
- From within a program using library routines

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

Regardless of the value of the `PAF_LABEL_VIEW` flag, a library call used to translate labels from binary form to text 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 option configured in the `label_encodings(4)` file or by the default system-wide value of `EXTERNAL` if the option is not specified.

Specifying Whether Users See Any Labels

The system-wide default is to show labels. The default setting for all accounts in the `policy.conf(4)` file is show labels. The Security Administrator can change the `policy.conf` entry to hide labels. The Security Administrator can also override the `policy.conf` setting for individuals accounts by choosing Hide from the Labels: menu on the Trusted Solaris Attributes tab of the User Accounts and Administrative Roles tools.

See “User Attributes and Defaults in `policy.conf`” and “Precedence Relationships for Attributes” in *Trusted Solaris Administrator’s Procedures* for more details.

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

The security administrator role can change which labels are printed on banner/trailer and body pages of print jobs and can modify the text that appears on the banner/trailer page. Two fields that are specified in the `label_encodings(4)` file are:

- *Printer banners and*
- *Channels (handling caveats)*

See Chapter 3.

Overview of Planning

- ◆ **Allow time to complete the `label_encodings(4)` 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 may not have much experience in planning labeled security, can start by examining their goals for information protection and use those goals to make some common-sense decisions about how to use labels. If the company has developed legal requirements for labeling printed information and email, those guidelines are a good place to start. For an example of how one commercial company developed a simple security policy based on its legal department's information labeling requirements, see Chapter 5. 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 default Trusted Solaris installed 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(4)` on a running system is risky. See "Changing the `label_encodings` File After System Start Up" on page 54 of Chapter 2.

Planning the Encodings File

The following practices help achieve the good organization required for a correct `label_encodings(4)` file that may be extended safely later.

Note - For CLASSIFICATIONS and, COMPARTMENTS, the security administrator role can later change human readable names but cannot change the values without potentially serious complications.

◆ **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, consider spacing 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*. See also “Setting Default and Inverse Words” on page 60.

◆ **Determine classifications for the site.**

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

Whatever names you give 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.

Different names can not be specified with the same classification value. Each classification 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.

The following table can be used for planning classifications. An asterisk (*) is used where the item is optional.

TABLE 1-5 Classifications Planner

name=	sname=/*aname=	value=	*initial compartments= bit numbers/WORD

♦ **Decide on compartments.**

Decide how data and programs are grouped and whether or not any data or programs can be intermixed. For example, perhaps weather data should not be seen by programs dealing with personnel files, but 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*.

♦ **Design the names.**

CLASSIFICATIONS and WORDS in the `label_encodings(4)` file have two forms: a mandatory long name and an optional short name. Short names can be entered interchangeably with long names when labels are being specified. Long names and short names display in the label dialog boxes.

♦ **Arrange the relationships.**

Compartments and markings are intrinsically non-hierarchical, 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 Figure 1-8. With this method, you can visualize the relationships and rearrange the pieces until they all fit together.

Note - When the command, `chk_encodings(1M)`, 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.

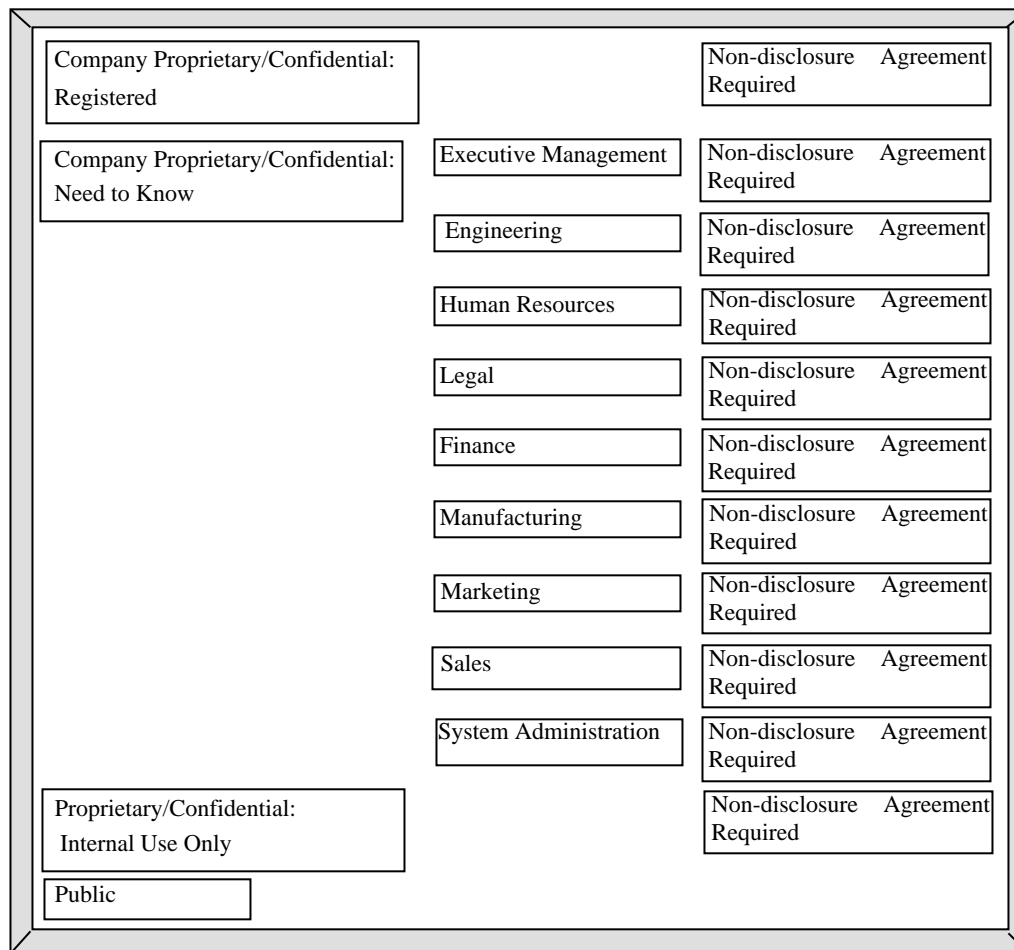


Figure 1-8 Example Planning Board for Label Relationships

♦ **Decide which clearances will be available to which users.**

Use the following table, if desired, for planning clearances.

TABLE 1-6 Clearance Planner

CLASS	COMP	COMP	COMP	COMP	COMP	OOMP	Notes

- ♦ Arrange the labels that will be formed from the classifications and compartments 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.

The following table can be used to keep track of compartment bit assignments.

TABLE 1-7 Compartment Bit Tracking Table

Creating Large Numbers of Labels

Using the 256 compartment bits available for assignment to compartment words, the maximum total number of possible labels that can be constructed using these words is 32767 for each classification. See the following table for the totals of the possible different labels (labels that may dominate each other) and unique labels (labels that do not dominate each other)

TABLE 1–8 Potential Numbers of Labels for Each Classification

# of Unique Labels	Total # of Different Labels
10 to the 40th power	10 to the 70th power

The unique labels can use either words or numbers, such as social security numbers. Creation of large numbers of unique labels is made possible by:

- Defining sets (or groups) of compartments to use in constructing labels, and
- Making sure that each label contains one and only one compartment from each compartment group.

As shown by the examples in the following table, the larger the number of compartment groups you define, the smaller the number of compartment words you can have in each set, and the greater the number of possible unique labels.

TABLE 1–9 Example: Defining Elements of Unique Labels

Number of Groups of Compartments	Number of Compartments in each Groups	Number of Possible Disjoint Labels
85	3	10 to the 40th power
4	20 (company set) 50 (division set) 50 (group set)	6 million
9	10	more than all the U.S. social security numbers

Note - The `User Accounts` label dialog box is not suited to constructing large numbers of labels with large numbers of components. The label builder is not designed to enforce the rules, such as ensuring that each label has one compartment from each compartment group. When an organization needs large numbers of labels, a script should be written to automate the assignment of labels to users in the `user_attr(4)` file while enforcing the rules.

Creating or Modifying the Encodings File

This chapter describes the steps for preparing the `label_encodings(4)` file.

This chapter includes these topics:

- “Preparing the Label Encodings File” on page 50
- “Central Administration” on page 52
- “Tools for Editing and Checking the `label_encodings` File” on page 52
- “Changing the `label_encodings` File After System Start Up” on page 54
- “For a Site Using a Government-furnished Labels File” on page 50
- “For a Site Without a Previously-existing Labels File ” on page 51
- “Running Without Labels ” on page 54
- “Word Order Requirements” on page 57
- “Adding or Renaming a Classification” on page 57
- “Setting Default and Inverse Words” on page 60

This chapter also describes these procedures:

- “To Modify the `label_encodings (4)` File” on page 66
- “To Copy the `label_encodings` File to a Floppy Disk” on page 68
- “To Copy the `label_encodings` File from a Floppy Disk” on page 68
- “To Add Sun Extensions to a Pre-Existing Label Encodings File” on page 69
- “To Set Up No Labels Operation” on page 70
- “To Add or Rename a Classification in the Default `label_encodings` File” on page 70
- “To Specify Default and Inverse Words” on page 72

- “To Replace the Single Label in the Default Single-label Encodings File” on page 73
- “To Make Your Own Single-label Encodings File” on page 74
- “To Configure Labels Not Visible to Users” on page 76
- “To Ensure Labels Map to CIPSO Labels” on page 76

Preparing the Label Encodings File

The overall process of configuring the `label_encodings` file is described below:

- Before the install team starts post-installation configuration, the security administrator finishes the analysis and planning described in Chapter 1.

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 follow when configuring users and hosts.

- The Security Administrator role prepares the `label_encodings(4)` file, as described in this chapter.

If a `label_encodings` file has not been used previously at the site, the Security Administrator role can create one by doing one of the following:

- Typing in and modifying a copy of the `label_encodings` files shown in Appendix A
- Waiting until after installation to copy and modify a demonstration file.

Note - Since creating the `label_encodings` file is usually a lengthy process, it is recommended that the encodings file be prepared beforehand.

- The install team installs the site-specific `label_encodings` file before finishing the configuration.

For a Site Using a Government-furnished Labels File

Some organizations use a government-furnished `label_encodings(4)` file that is based on Defense Intelligence Agency (DIA) specifications. Sun’s implementation of the `label_encodings` file supports an optional LOCAL DEFINITIONS section that

can be appended to an already-existing `label_encodings` file. (The word *LOCAL* in the keyword that starts the section means *local to Sun's implementation*). Options in the LOCAL DEFINITIONS section can be defined to set various label translation options and to associate colors with labels. Windows applications display each label against a background of the color specified for that label. If an invalid color or no color is specified in the COLOR NAMES option, a default color is supplied.

The Security Administrator role at a site with its own government-furnished `label_encodings` file can append a LOCAL DEFINITIONS: section to the organization's `label_encodings` file and then specify any desired options before the file's installation. Chapter 4 describes how to modify the Sun extensions for your site.

For a Site Without a Previously-existing Labels File

In most organizations, a version of the `label_encodings(4)` file is created by the Security Administrator role either before or after installation.

The Security Administrator can use the example `label_encodings` file in Appendix A, which is based on a planning example in Chapter 5. The introduction to Appendix A describes the labels components defined in the example file.

Before Installation

To prepare a `label_encodings(4)` file in advance, the Security Administrator role can manually make a copy of the example in Appendix A and make modifications in the copy. Alternatively, a `label_encodings` file can be created from the examples in this manual and in the *Compartmented Mode Workstation Labeling: Encodings Format*.

After Installation

The example `label_encodings.simple` file shown in Appendix A can be found in the `/etc/security/tsol` directory, and this label encodings file can either be modified or used as is. Alternately, the default version of the `label_encodings` file or one of the other `label_encodings` files in `/etc/security/tsol` can be modified to suit a site's requirements. See Appendix B for the differences between the default single-label and multilabel files.

Central Administration

If a naming server is used, the master `label_encodings` file is installed during the naming server's configuration. After the naming server 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. The Security Administrator role should ensure that an identical copy of the `label_encodings` file is installed on every host. The `label_encodings` file is a local file on each host.

Tools for Editing and Checking the `label_encodings` File

The `label_encodings` file is a flat, text file. Its label is `ADMIN_HIGH` to prevent normal users from reading it. The maximum line length in the `label_encodings` file is 256 bytes. The file can be edited with any text editor. During development of the file, the labels and their relationships can be checked by using the `chk_encodings(1M)` command with the `-a` option on the command line in a terminal. The file must pass `chk_encodings(1M)` before it is installed on the working system.

The Security Administrator role uses one of the two actions shown in Table 2-1. The actions 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 the specified <code>label_encodings</code> file.
Check Encodings	Checks the specified <code>label_encodings</code> . If the file specified for editing is not the installed version, after the file passes the check, Check Encodings offers the option of installing the checked file. Before overwriting an existing file, Check Encodings creates a backup of the installed <code>label_encodings</code> file, while preserving the required DAC attributes.

Note - Starting with release 7, Trusted Solaris does not support information labels. However, a `label_encodings` file still needs information labels defined. The `chk_encodings(1M)` utility fails unless the `label_encodings(4)` contains an `INFORMATION LABELS WORDS` section that defines the same bits defined `SENSITIVITY LABELS WORDS` section.

Note - The `label_encodings` file may be created or edited on any system. However, it must be checked and tested on a host running the Trusted Solaris operating environment.

Suggested Working Policies

- ♦ **Make a backup copy (on a tape or floppy disk) of the original file installed with the system. If modifying the file on an operational system, back up the current file.**

If your modifications create labels that cannot be resolved, you would need to manually reset labels to `ADMIN_LOW` before assigning the new labels from the modified file. Restore a known, usable `label_encodings` file from tape or floppy until problems with the new version are debugged. Backup copies are made using File Manager options.

Note - The File Manager allows the Security Administrator role to restore ownership, group, and permissions on files. By default, the needed changes to maintain the correct file attributes cannot be made by using utilities on the command line.

- ♦ **Code the file using any text editor, and save a hard copy when done.**
This procedure is detailed in “To Modify the `label_encodings` (4) File” on page 66. As soon as possible after you are satisfied with the file, print it out, and keep a record.
- ♦ **Check the syntax and relationships of the labels with the `chk_encodings` command and the `-a` option.**
- ♦ **Check the syntax with the `chk_encodings(1M)` command.**

- ◆ **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.**

Changing the `label_encodings` File After System Start Up

After the Trusted Solaris system is fully configured and running, the Security Administrator role can later modify the `label_encodings(4)` file. See the man page for what to avoid and for how to safely make other changes.

Running Without Labels

An organization may not want non-administrative users to see labels or be aware of mandatory access controls. By following the steps in “To Set Up No Labels Operation” on page 70, the Security Administrator role can configure what appears to be a *no labels* operation, so that all normal users work in an environment that is visually almost the same as working in the Solaris environment with the CDE window system.

Even if non-administrative users do not see labels, certain labels must always be present:

- `ADMIN_LOW` and `ADMIN_HIGH` clearances and labels are always included and do not need to be defined
- One sensitivity label in the user accreditation range must be defined
- One clearance in the user accreditation range must be defined
- One information label in the user accreditation range must be defined (even though information labels are not used in Trusted Solaris 7 and later releases)

Note - Even though Trusted Solaris 7 does not use information labels, the `label_encodings` file cannot pass `chk_encodings(1M)` unless it has information labels defined. To fulfill this software requirement, copy the words defined in the `SENSITIVITY LABELS WORDS` to the `INFORMATION LABELS WORDS` section.

Setting Up Single-label Operation

You can use or modify the default example single-label file (/etc/security/tsol/label_encodings.single), copy the /etc/security/tsol/label_encodings.simple file manually from Appendix A, or create an encodings file with one classification and any number of compartments. The following example shows the settings in the ACCREDITATION RANGE: section with a single ANY_CLASS classification defined and compartments words A, B, and REL CNTRY 1 specified for all types of labels.

```
ACCREDITATION RANGE:
```

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

```
ANY_CLASS A B REL CNTRY1
```

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

Any of these ways of creating single-label operation also require supporting procedures described in “To Configure Labels Not Visible to Users” on page 76.

Sections for Defining Labels

Label components are defined by the Security Administrator role in the /etc/security/tsol/label_encodings file in the sections described here. The encodings are comprised of a VERSION specification and seven mandatory sections: CLASSIFICATIONS, INFORMATION LABELS, SENSITIVITY LABELS, CLEARANCES, CHANNELS, PRINTER BANNERS, AND ACCREDITATION RANGE, which must appear in the order given. An optional LOCAL DEFINITIONS section may follow. Mandatory means only that all the keywords must be present. Not all keywords must be defined. See the notes for each section for what must be defined and what is optional.

TABLE 2-2 Table Caption

Section	Notes
VERSION=	Mandatory keyword must be present. The version specification is the single keyword VERSION=, followed by a character string that identifies this particular version of encodings. An example is: VERSION= DISTRIBUTED DEMO VERSION
CLASSIFICATIONS:	Mandatory keyword must be present. At least one classification must be defined
INFORMATION LABELS: WORDS: REQUIRED COMBINATIONS: COMBINATION CONSTRAINTS	Mandatory keywords must be present. Even though information labels are not used in Trusted Solaris, you must assign one bit to an INFORMATION LABEL WORD for each bit you assign to a SENSITIVITY LABEL WORD that you may define in the following section. Hint: Encode the SENSITIVITY LABELS WORDS first and then copy them to the INFORMATION LABELS section.
SENSITIVITY LABELS:WORDS: REQUIRED COMBINATIONS: COMBINATION CONSTRAINTS	Mandatory keywords must be present. WORDS definitions are optional. If you define SENSITIVITY LABELS WORDS, the same bits must be assigned to WORDS in both the INFORMATION LABELS and CLEARANCES section, even though the words assigned to the bits do not need to be the same.
CLEARANCES:WORDS: REQUIRED COMBINATIONS: COMBINATION CONSTRAINTS	Mandatory keywords must be present. One bit must be assigned to a CLEARANCE WORD for any SENSITIVITY LABEL WORD you define. Clearance labels may allow combinations of words that have been disallowed in the definitions for sensitivity labels words.
CHANNELS:	Mandatory keyword must be present
PRINTER BANNERS:	Mandatory keyword must be present
ACCREDITATION RANGE:	Mandatory keyword must be present. A rule must be defined for each CLASSIFICATION name; the minimum clearance, minimum sensitivity label, and minimum protect as classification must be defined.
LOCAL DEFINITIONS:	Optional.

For all the required sections, the keywords shown must be present, but not all of the sections must have elements defined. This means that you could have a valid label

encodings file with only CLASSIFICATIONS and ACCREDITATION RANGE definitions.

Word Order Requirements

The order in which words are configured for sensitivity labels and clearances is not enforced, but it is important when setting up relationships between words. See “Specifying CHANNELS” on page 88 of Chapter 3 for examples of how the order affects how words must be encoded. See also the *Compartmented Mode Workstation Labeling: Encodings Format*: Defense Intelligence Agency document [DDS-2600-6216-93]DIA] manual.

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

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

Adding or Renaming a Classification

The Security Administrator role can replace classification names defined in the default `label_encodings` file, define new classification names, or create a new file with unique classifications.

The classification is the hierarchical portion of a label. Each label has one and only one classification. The internal representation of each label has 15 bits available for storing classification values.

Classification Field
15 bits/32,767 possible values/256 values limit enforced

The labels translation software enforces a limit of 256 classification values. A numeric value (integer) from 1 to 255 can be assigned to each classification in the `label_encodings` file. The values 0 is reserved for the ADMIN_LOW administrative label.

Classifications are defined once for all types of labels in the `CLASSIFICATIONS` section of the `label_encodings(4)`.

A classification with a higher value is said to dominate a classification with a lower value. The following table shows two sets of label names that are assigned to the same values in two example `label_encodings` file in the `/etc/security/tsol` directory. The left column shows example information protection labels from the `label_encodings.simple` file and the middle column shows example labels from the `label_encodings.gfi.multi` file. A label with the Registered or Top Secret classification would dominate all labels with any other classification shown.

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

Number of Classifications

The total number of classifications that can be defined at a site is 255.

Keywords Defined for Classifications

The following table 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 60 for more about how to set up optional initial compartments and markings that may be associated with classifications.

TABLE 2-3 Values for Classifications

Value	Requirements
<code>name=</code>	Cannot contain (/) or (,) or (;). All other alphanumeric characters and white space are allowed. Users can enter either the <i>name</i> or the <i>sname</i> or the <i>aname</i> when specifying labels.
<code>sname=</code>	Required in classifications only. The short name appears in sensitivity labels (within brackets).
<code>*aname=</code>	Name used only for input by users. The alternate name can be entered by users any time a classification is needed.

TABLE 2-3 Values for Classifications *(continued)*

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. Values can start at 1 and go to 255.
*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=	Used for information labels, which are not used in Trusted Solaris 7 and later releases. Do not define.

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 compartment bits. Keep track of the ones you use and their relations to each other.

The following example shows the top of the demonstration Trusted Solaris label_encodings file, with the CLASSIFICATIONS section.

CODE EXAMPLE 2-1 Trusted Solaris Demonstration label_encodings File (Top)

CLASSIFICATIONS:

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

Each classification defined in Code Example 2-1 has the mandatory *name*, *sname*, and *value*. The CONFIDENTIAL, SECRET, and TOP SECRET classifications have *initial compartments*, while UNCLASSIFIED has none.

The following table shows some initial compartments bit assignments and what they mean.

TABLE 2-4 Example Initial Compartments Bit Assignments and What They Mean

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

Some of the initial compartments shown in Code Example 2-1 are used later to define *default* and *inverse* words, and some are reserved for possible later definitions of inverse words.

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

CODE EXAMPLE 2-2 Simple Classifications Defined Without 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;
```

Setting Default and Inverse Words

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

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

The following table summarizes the requirements for initial compartments values associated with classifications.

TABLE 2-5 Initial Compartments 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.

The following example shows the `PUBLIC` classification assigned no initial compartments while the `SUN FEDERAL` classification is assigned initial compartments 4 and 5.

CODE EXAMPLE 2-3 Simplified Assignment of Initial Compartments

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

With the bits assigned in Code Example 2-3, a label that includes the `PUBLIC` classification has no default compartments assigned, while a label that includes the `SUN FEDERAL` classification always has compartment bits 4 and 5 turned on. See the example below and the following text for how these initial compartment bits can be assigned to words.

CODE EXAMPLE 2-4 Example of Defining Default and Inverse SENSITIVITY LABELS Words

SENSITIVITY LABELS:

WORDS:

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

The example above shows `WORDS` defined in the `SENSITIVITY LABELS` section of a `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`. As a result, a sensitivity 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 a sensitivity 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` sensitivity label; the presence of these two inverse words is understood.

For any compartment or marking bits not reserved for later assignment, remember that for every initial compartment bit specified, you need to assign a word to the bit in the `SENSITIVITY LABELS: WORDS:`, `INFORMATION LABELS: WORDS:`, and `COMPARTMENTS: WORDS:` sections.

Defining Compartment Words

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

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

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

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

The following example shows the `SUN FEDERAL` compartment word specified with a short name (`sname`) of `SUNFED` and compartment bits 40-50.

CODE EXAMPLE 2-5 Example Compartment Definition for a Sensitivity Label

```
WORDS:

name= SUN FEDERAL; sname= SUNFED; compartments= 40-50;
```

Along with its classification field, each label has a 256 bit compartment field. Each bit is assignable in zero or more compartment words, as shown in Table 2-6. Each word can have one or more compartment bits assigned. Out of the 255 available bits, the number of compartment words that can be created is practically limitless. See “Creating Large Numbers of Labels” on page 47 for examples.

TABLE 2-6 Bits Available for Classification and Compartment Components

Classification Field	Compartments Field
15 bits/32,767 possible values/256 values limit enforced	256 bits

The following table can be used for planning compartments and user accreditation range combinations. The ACCREDITATION RANGE for each classification settings should be one of the following.

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

TABLE 2-7 Compartments and User Accreditation Range Combinations Planner

[illegible]

TABLE 2-7 Compartments and User Accreditation Range Combinations Planner *(continued)*

Classification	Compartment Name/ sname/ Bit	REQUIRED COMBINATIONS/ COMBINATION CONSTRAINTS	ACCREDITATION RANGE Settings

Hierarchical Words

Hierarchical compartments can be used when you want some way to differentiate between documents that have to be accessible to everyone in a larger group and documents that can be accessed only by subgroups. Hierarchical compartments can be created by:

- Assigning shared bits to words
- Defining required combinations

Using Bit Combinations to Establish Hierarchies

By defining a word that uses one bit and a second word that uses that same bit along with a second bit, you define a hierarchical relationship between the two words. The compartment word that is more general must be defined below the word that is more specific.

For example, by defining a word that uses bit number 1 and another word that uses bits number 1 and 2, you give the two words a hierarchical relationship. The following screen example shows definitions for a Sales compartment with two subcompartments, Direct Sales, and Indirect Sales. It supposes that a single classification named WebCo is defined.

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

(continued)

Figure 2-1 Bit Combinations Defining Hierarchical Relationships

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

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

Using REQUIRED COMBINATIONS to Establish Hierarchies

If two words are specified together in the REQUIRED COMBINATIONS section, the second label is added to the label whenever the first word is used. The following example shows a definition of the Direct Sales, Indirect_Sales, and Sales that serves essentially the same effect as the example in Figure 2-2. The difference is that the Direct_Sales word will always have the Sales word with it

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

```
REQUIRED COMBINATIONS:
```

```
Direct_Sales Sales
Indirect_Sales Sales
```

Figure 2-2 REQUIRED COMBINATIONS Used to Establish Hierarchies

Cautions About Mapping Labels to CIPSO Labels

When a template assigned to a computer is specified with one of the CIPSO label indicators, the trusted networking software derives a CIPSO label from the message's label and inserts the CIPSO label into the IP options portion of packets sent to that computer. For a label to map to and from a CIPSO label, the classification value must be less than or equal to 255 and all compartment bit numbers must be less than or equal to 239.

By default, a message to a CIPSO-identified host is dropped if it is sent with a sensitivity label that cannot be mapped to a CIPSO label. The `ADMIN_HIGH` label is too big to map to a CIPSO label, so, by default, a message sent at the `ADMIN_HIGH` label to a CIPSO-identified host is always dropped. To avoid this, the Security Administrator role can add the `tsol_admin_high_to_cipso` switch set equal to 1 in the `/etc/system` file. Setting this switch causes the label on a packet to be mapped to a valid CIPSO label with the highest classification and all compartments turned on, instead of being dropped. See "Changing Configurable Trusted Solaris Kernel Switches" in *Trusted Solaris Administrator's Procedures*

If the switch is set so that the `ADMIN_HIGH` label is mapped, make sure that no label in the user accreditation range has the classification value of 255 with all compartment bits from 0 to 239. Otherwise, the user label would be indistinguishable from `ADMIN_HIGH` after mapping.

To ensure that all labels are mappable, be sure that no user label has compartments numbered above 239.

Label_encodings-related Procedures

▼ To Modify the label_encodings (4) File



Caution - Modifying the `label_encodings` file can safely be done at the time the host is installed. If a need arises where an operational file needs to be changed, proceed with caution. Review the caveats described in the `label_encodings(4)` file.

1. Assume the Security Administrator role in an `ADMIN_HIGH` workspace.
2. Open a new or existing version of the file.
 - a. If creating a new version of the `label_encodings` file, use any text editor or use the `Edit Encodings` action to create the file.

The `Edit Encodings` action both edits and runs `chk_encodings(1M)` on the file.

Note - If creating a new file from scratch, make sure to include all the sections shown in Table 2-2 or copy and modify the example in Appendix A.

Note - During development of the file, `chk_encodings(1M)` can be entered on the command line with the `-a` option to analyze and report on relationships between labels in the `label_encodings` file.

- b. When a new version is ready to install, use the Check Encodings action to open and check the file.**

The Check Encodings action runs `chk_encodings(1M)` on the specified file, and if the file passes the check, the action asks whether you want to overwrite the currently-installed `label_encodings` file. If the answer is yes, the action creates a backup copy (naming it `label_encodings.orig`), and overwrites the installed version.

Note - By default, both the Security Administrator and root roles have the Check Encodings action. The root role uses the action to install the `label_encodings` file when configuring the system after installation.

- c. If you are installing a new `label_encodings`, answer affirmatively when prompted.**

Do you want to install this `label_encodings` file?

- 3. If necessary, restart the Window Manager from the Workspace Menu to initialize the new encodings file.**

- 4. On a distributed system of Trusted Solaris hosts, distribute a copy of the `label_encodings` file from the naming service master to the `/etc/security/tsol` directory on all hosts in the system.**

See “To Copy the `label_encodings` File to a Floppy Disk” on page 68 for how to copy the file to a floppy disk for manual distribution of the modified file.

▼ To Copy the label_encodings File to a Floppy Disk

1. Assume the Security Administrator role in an ADMIN_HIGH workspace.
2. Allocate the floppy device at ADMIN_HIGH.
 - a. Highlight the name of the floppy device.
 - b. Move the device to the Allocated Devices list.
 - c. In the Update With field, type in ADMIN_HIGH.
 - d. Click OK.
3. Double-click the File Manager icon in the Front Panel.
4. Using the File Manager, navigate to the folder that contains the label_encodings file.

Note - Give another name to the version of the label_encodings file to be copied. For compatibility with the PC file systems on most floppy disks, use a name with fewer than eight characters and without a dot (.) in the name. (A string after a dot in a PC file's name is treated as the suffix that indicates the file's type, like .doc.)

5. Choose Open Floppy from the File menu.
6. Highlight the icon for the file.
7. Drag the file to the floppy disk folder.
8. On the floppy disk folder, chose Eject from the File menu.

▼ To Copy the label_encodings File from a Floppy Disk

1. Assume the Security Administrator role in an ADMIN_HIGH workspace.
2. Allocate the floppy device at ADMIN_HIGH.
 - a. Highlight the name of the floppy device.

- b. **Move the device to the** `Allocated Devices` **list.**
 - c. **In the** `Update With` **field, type in** `ADMIN_HIGH`.
 - d. **Click** `OK`.
3. **Double-click the** `File Manager` **icon in the** `Front Panel`.
4. **Using the** `File Manager`, **navigate to the desired destination directory.**
5. **Chose** `Open Floppy` **from the** `File` **menu.**
The floppy disk folder displays.
6. **Highlight the icon for the** `label_encodings` **file.**
7. **Drag the file from the floppy disk folder to the desired destination directory.**
If dragging the file to the `/etc/security/tsol` folder, make sure the file being dragged is not named `label_encodings`. Otherwise, by dropping the file, you will be attempting to overwrite the existing `label_encodings` file. Instead, copy the file onto the host, and then use the `Check Encodings` action to install the file, as described in “To Modify the `label_encodings` (4) File” on page 66.
8. **On the floppy disk folder, chose** `Eject` **from the** `File` **menu.**
9. **Initialize the new encodings file.**
Restart the `Window Manager` from the `Workspace Menu`.

▼ To Add Sun Extensions to a Pre-Existing Label Encodings File

1. **Copy the** `LOCAL DEFINITIONS` **sections from one of the default** `label_encodings` **files in** `/etc/security/tsol` **and append the section to your site’s existing file.**
See “To Modify the `label_encodings` (4) File” on page 66, if needed, for how to edit and check the file.
2. **Modify the definitions to suit your site’s security policy.**
See Chapter 4 for how to configure the extensions.
3. **Check the file using the** `Check Encodings` **action.**

4. When prompted by the `Check Encodings` action, install the modified version of the `label_encodings` file.

▼ To Set Up No Labels Operation

The install team should do the following:

1. **Change or accept the name of the single label in the `label_encodings.single`.**
The example uses the label `PUBLIC`. See “To Replace the Single Label in the Default Single-label Encodings File” on page 73.
2. **When setting up user accounts, restrict the user to single-label operation.**
 - a. **Configure the user’s clearance and initial (minimum) label to equal the only encoded label.**

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

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

```
Labels: Hide
```

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

1. **In the Security Administrator role in an `ADMIN_HIGH` workspace, open the `label_encodings` file for editing.**
See “To Modify the `label_encodings` (4) File” on page 66, if needed.
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. (See the `sccs(1)` man page, if needed, for more about SCCS.)

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.

The following example shows the three new classifications added to the ACCREDITATION RANGE section of the demonstration file. All three (INTERNAL_USE_ONLY, NEED_TO_KNOW, and REGISTERED) 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;
```

6. If you are done, save and quit the file.
7. If you want to install the file, use the `Check Encodings` action and answer yes when asked if you want to install the new version of the file.

▼ To Specify Default and Inverse Words

1. In the Security Administrator role in an `ADMIN_HIGH` shell, open the file for editing.
See “To Modify the `label_encodings` (4) File” on page 66 if needed.
2. 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 ;
```

3. 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;
```

4. Specify an inverse word by assigning an initial compartment 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. In the **Security Administrator** role in an **ADMIN_HIGH** workspace, open the `/etc/security/tsol/label_encodings.single` file for editing.

See “To Modify the `label_encodings (4)` File” on page 66 if needed.

2. 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=` value is changed from **SECRET** to **INTERNAL_USE_ONLY** and the `sname=` value 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 centryl

```

3. If desired, delete the compartments `a b rel centryl` from the accreditation range.

```
ACCREDITATION RANGE:
```

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

```
INTERNAL
```

- 4. 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. In the Security Administrator role in an ADMIN_HIGH workspace, open the label_encodings file for editing.**

See “To Modify the label_encodings (4) File” on page 66 if needed.

- 2. 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.

```
VERSION= Single-label Encodings
```

```
. . .  
CLASSIFICATIONS:
```

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

```
INFORMATION LABELS:
```

```
WORDS:
```

(continued)

```
SENSITIVITY LABELS:
```

```
WORDS:
```

```
CLEARANCES:
```

```
WORDS:
```

```
CHANNELS:
```

```
WORDS:
```

```
PRINTER BANNERS:
```

```
WORDS:
```

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

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;
only valid compartment combinations:
```

```
INTERNAL
```

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

- 4. Encode the LOCAL DEFINITIONS section as described in Chapter 4, making sure to specify Default Label View is External.**

- 5. Configure labels not visible to users.**

See “To Configure Labels Not Visible to Users” on page 76.

▼ To Configure Labels Not Visible to Users

1. **When setting up user accounts using the Trusted Solaris Attributes tab on the SMC User Accounts tool, configure users to not see labels and to have only a single label in their label ranges.**
 - a. **Make sure the label View is set to External.**
 - b. **Choose Show from the Labels menu.**
2. **Specify the account's Clearance equal to its Minimum Label.**

With a clearance and label of `INTERNAL_USE_ONLY`, you would (naturally) set the Clearance and the Minimum Label to `INTERNAL_USE_ONLY`.

To Ensure Labels Map to CIPSO Labels

See the discussion in “Cautions About Mapping Labels to CIPSO Labels” on page 66.

1. **Assume the Security Administrator role on the forwarding host and go to an `ADMIN_LOW` workspace.**

See “Assuming a Role and Working in a Role Workspace” in *Trusted Solaris Administrator's Procedures*, if needed.
2. **Use the Admin Editor action to open the `/etc/system` file for editing.**

See “Accessing the Administration Tools” in *Trusted Solaris Administrator's Procedures*, if needed.
3. **Add a line to set the `tsol_admin_high_to_cipso` flag equal to 1.**

```
set tsolsys:tsol_admin_high_to_cipso=1
```

The default in the kernel, which is not shown in the `system` file, is set to 0.

4. **Write and quit the file.**

```
:wq
```

5. **Make sure that no label in the user accreditation range has the classification value of 255 with all compartment bits from 0 to 239.**

This step ensures that no label is indistinguishable from ADMIN_HIGH after mapping.

6. **Make sure that no user label has compartments numbered above 239.**

This step ensures that all labels are mappable to CIPSO labels.

Specifying Labels and Handling Guidelines for Printer Output

This chapter gives the information needed to understand which labels are printed at the top and bottom of printer output and which labels and text are printed on banner and trailer pages. This chapter also describes how the Security Administrator role can make changes to the default.

This chapter includes these topics:

- “Labels on Body Pages” on page 79
- “Labels, Text, and Handling Caveats on Banner and Trailer Pages” on page 80
- “Specifying the Protect As Classification” on page 82
- “Specifying Printer Banners” on page 85
- “Specifying CHANNELS” on page 88

This chapter also describes these procedures:

- “To Configure PRINTER BANNERS” on page 93
- “To Configure CHANNELS” on page 94

Labels on Body Pages

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

Figure 3–1 shows a label (in this case, `PUBLIC`) printed at the top and bottom of a print job’s body page.

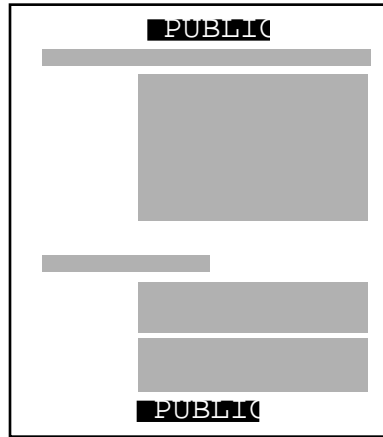


Figure 3-1 Label Automatically Printed on Body Pages

The Security Administrator role can change the defaults so that another label or no label is printed instead of the default label. (See “Labels, Text, and Handling Caveats on Banner and Trailer Pages” on page 80.)

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

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

The fields and the text that are printed on the banner page are shown in Figure 3-2. The callouts show the names of the labels and the strings that appear by default.

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

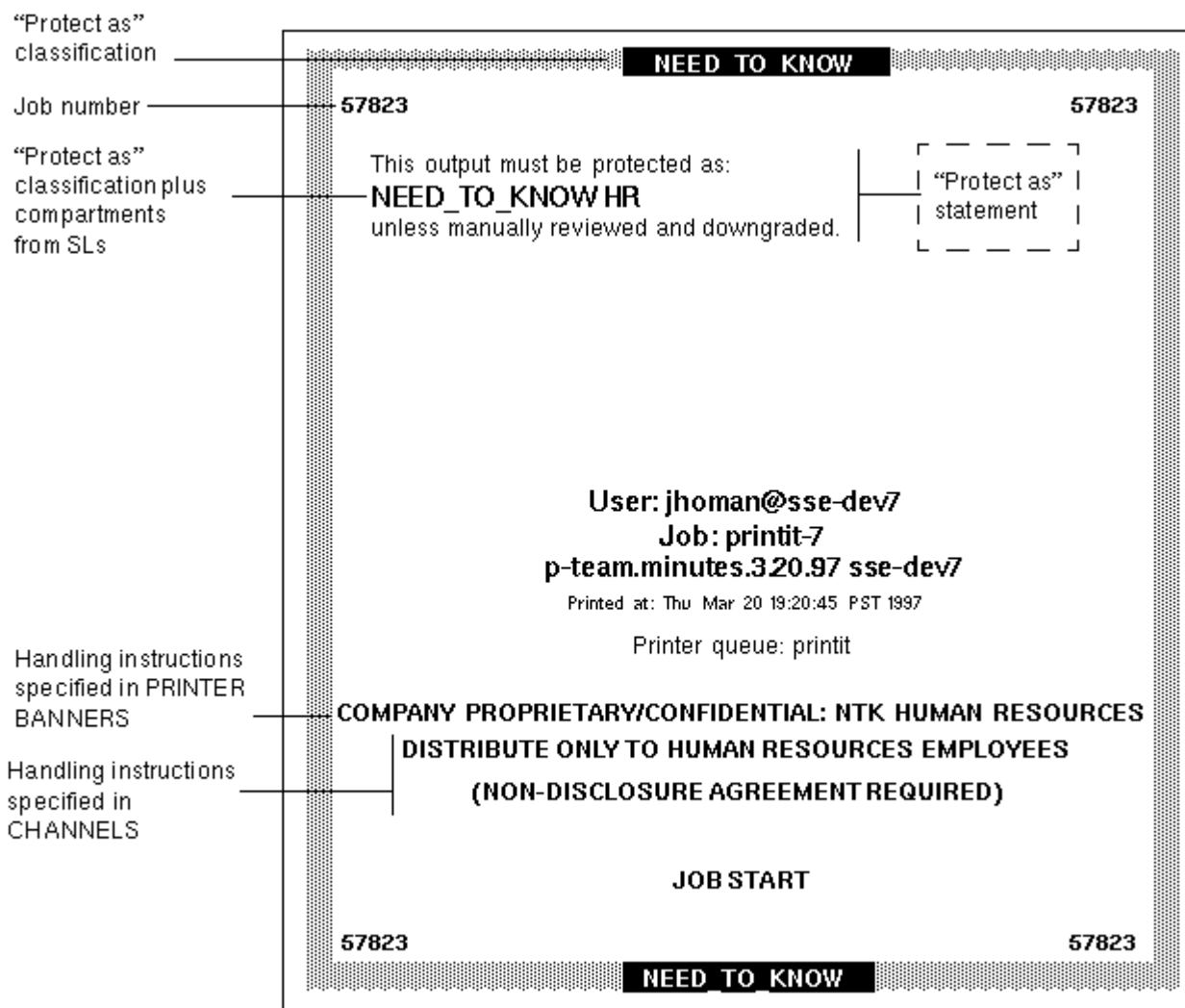


Figure 3-2 Typical Print Job Banner Page

The differences on the trailer page are shown in Figure 3-3. A thick black line is used as a frame on the trailer page, instead of the thicker gray frame on the banner page, and the page type identifier changes from JOB START to JOB END.

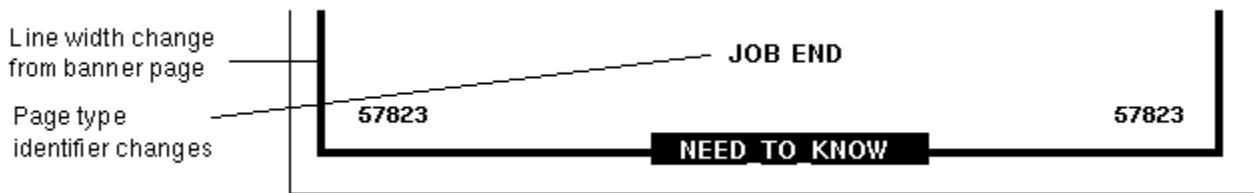


Figure 3-3 Differences on Trailer Pages

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

- “Specifying the Protect As Classification” on page 82
- “Specifying Printer Banners” on page 85
- “Specifying CHANNELS” on page 88

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

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

For how to do customizations, see the comments in the `tsol_separator.ps` file in the `/usr/lib/lp/postscript` directory. See also “Managing Printing” in *Trusted Solaris Administrator’s Procedures*.

Specifying the Protect As Classification

The *protect as classification* is printed:

- On the top and bottom of banner and trailer pages and
- In the middle of the *protect as statement* (along with compartments from the job’s label)

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

The `protect as statement` reads:

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

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

NEED_TO_KNOW HR

followed by:

unless manually reviewed and downgraded

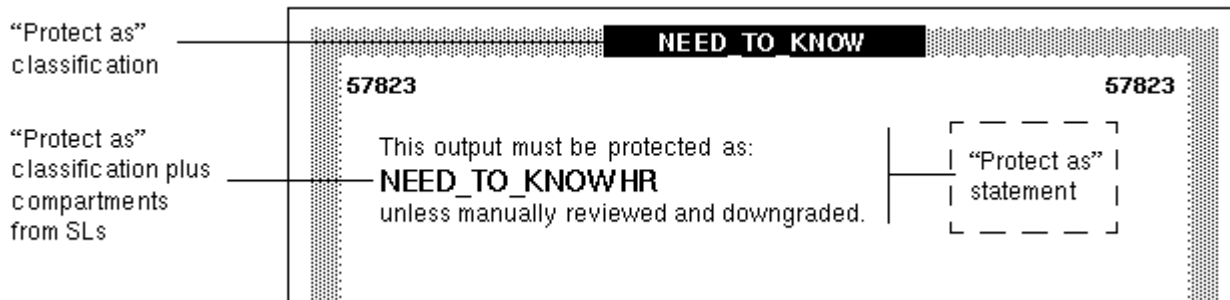


Figure 3-4 Protect As Statement

Code Example 3-1 shows the minimum protect as classification defined in the ACCREDITATION RANGE section of the `label_encodings.simple` file.

CODE EXAMPLE 3-1 Minimum protect as classification from a `label_encodings` File

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

In most cases the Security Administrator role specifies the minimum protect as classification equal to the site's lowest defined classification. Specify a minimum protect as classification higher than the lowest classification only if you need to protect all printer output at the specified minimum classification or above (whether or not the label has a lower classification).

Example

Figure 3-5 shows an example in which the label on the user's print tool is `INTERNAL_USE_ONLY`, and the minimum protect as classification is `NEED_TO_KNOW`. The `NEED_TO_KNOW` classification is printed in this case because the minimum protect as classification dominates the classification.

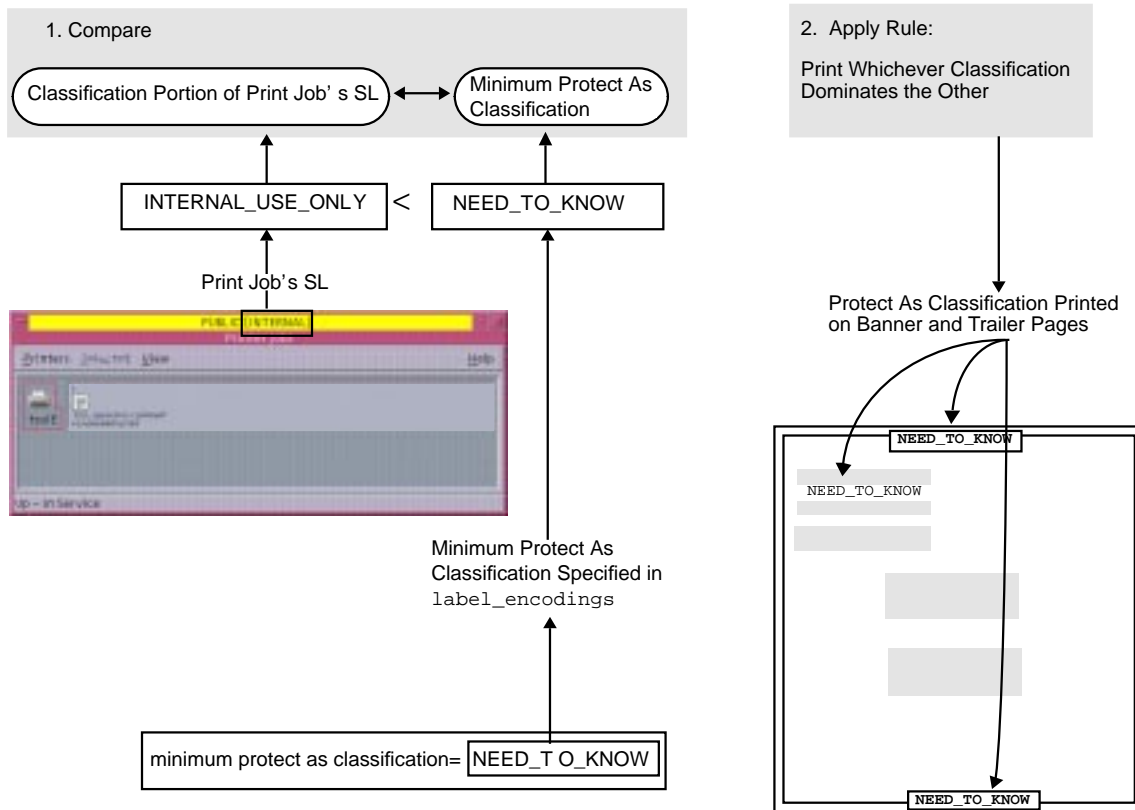


Figure 3-5 How the Classification Printed on Banner and Trailer Pages is Derived

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 of the following table. 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 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

TABLE 3–1 Example: Minimum Protect As Classification's Effects on the Protect As Classification *(continued)*

As shown in the table above, any print job whose 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.

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.**

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

Specifying Printer Banners

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

At commercial sites, the Security Administrator role can associate any text in the `PRINTER BANNERS` section with any compartment bit, as long as the compartment bit is also assigned to a word in the `SENSITIVITY LABELS` section of the `label_encodings` file. In the following example, the printer banner is the line that reads `COMPANY PROPRIETARY/CONFIDENTIAL: NTK HUMAN RESOURCES`.

Handling instructions
specified in PRINTER
BANNERS

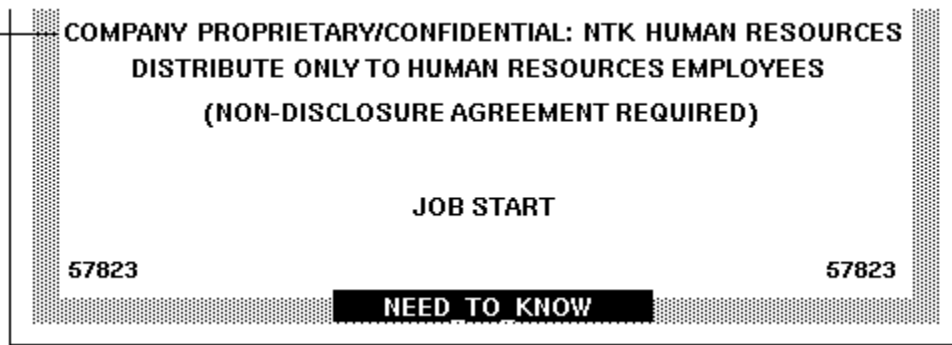


Figure 3-6 Commercial Use of the PRINTER BANNERS Specification on the Print Job's Banner Page

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

Handling instructions
specified in PRINTER
BANNERS



Figure 3-7 Government Use of the PRINTER BANNERS Section of the Banner Page

Following are the encodings for the printer banner line (FULL SA NAME) in Figure 3-7.

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

CODE EXAMPLE 3-2 Example: PRINTER BANNERS Specification

PRINTER BANNERS:

WORDS:

(continued)

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

Code Example 3-3 shows the SENSITIVITY LABELS definitions for the same compartments and markings used in the PRINTER BANNER definitions in Figure 3-7. In the example, compartment bit 2 is associated with the subcompartment word SA.

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

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

CODE EXAMPLE 3-3 Sensitivity Labels WORDS associated with PRINTER BANNERS Definitions
Figure 3-6

```
SENSITIVITY LABELS:

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

Following is a planning table for PRINTER BANNERS.

TABLE 3-2 PRINTER BANNERS Planner

When this/these subcompartment/ compartment bit(s) are in the print job's label	Print this Prefix	Print this Word	Print this Suffix

TABLE 3-2 PRINTER BANNERS Planner (continued)

When this/these subcompartment/ compartment bit(s) are in the print job's label	Print this Prefix	Print this Word	Print this Suffix

Specifying CHANNELS

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

In the example in Figure 3-8, the channels are the lines that read `DISTRIBUTE ONLY TO HUMAN RESOURCES EMPLOYEES (NON-DISCLOSURE AGREEMENT REQUIRED)`. 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 3-8 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 label. Figure 3-9 shows a typical CHANNELS warning on a print job's banner

page at a government installation: HANDLE VIA (CH B)/(CH A) CHANNELS JOINTLY.

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

The example illustrates the following:

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

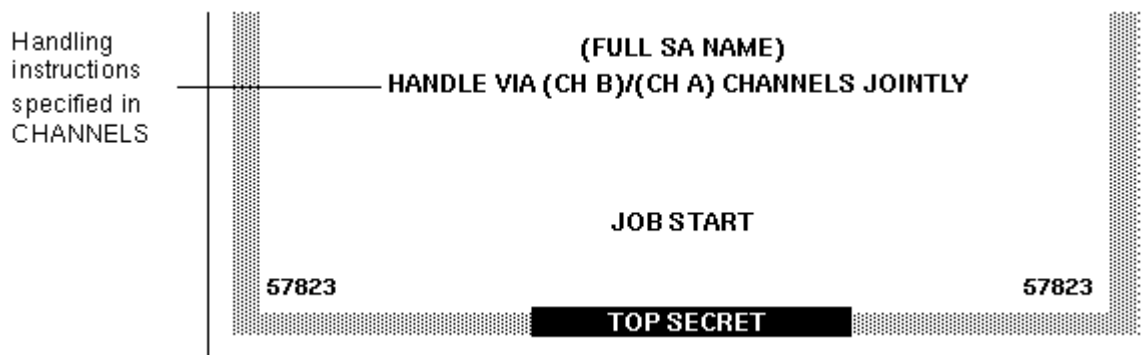


Figure 3-9 Government Use of the CHANNELS Specification on the Banner Page

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

CODE EXAMPLE 3-4 Suffixes and Prefixes Defined in the CHANNELS Section in a Government label_encodings File

```
CHANNELS:

WORDS:
name= CHANNELS JOINTLY;      suffix;
name= CHANNELS ONLY;        suffix;
```

(continued)

```
name= HANDLE VIA;           prefix;
```

Following the prefixes and suffixes definitions in Code Example 3-4, the channel names (CH A), (CH B), and (CH C) are specified in two different ways to achieve the following results:

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

The first three lines that define `CHANNELS` words in Code Example 3-4 are repeated in Code Example 3-5 to focus on how (CH A), (CH B), and (CH C) are encoded to appear with the `CHANNELS ONLY` suffix:

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

CODE EXAMPLE 3-5 CHANNELS ONLY Suffix Defined to Appear Alone with Individual Channels

```
CHANNELS:
```

```
WORDS:
```

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

The first three lines of channel name definitions in the `CHANNELS` section shown in Code Example 3-5 have the following results:

- 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` prefix and `CHANNELS ONLY` suffix are printed:
 - With `(CH A)` when compartment bit 0 is turned on in the label and compartment bits 1 and 6 are off
 - With `(CH B)` when compartment bit 1 is turned on in the label and compartment bits 0 and 6 are off
 - With `(CH C)` when compartment bit 6 is turned on in the label and compartment bits 0 and 1 are off

The last three lines that define `CHANNELS WORDS` in Code Example 3–5 are repeated in Code Example 3–6 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 inserted between the channels names when more than one of the bits defined in the channels section is in the job's label.

CODE EXAMPLE 3–6 Encodings for More Than One Channel in the `CHANNELS` Section in a Government `label_encodings` File

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

The `CHANNELS` specification illustrates the importance of order when compartments are being encoded. The first three lines shown in Code Example 3–6 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

Code Example 3–7 shows the labels with compartment bit 6. The figure shows that compartment bit 6 is associated words associated with the label word `CC`.

CODE EXAMPLE 3-7 labels WORDS associated with Compartment Bit 6

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

Code Example 3-8 shows that compartment bit 1 is associated with the sensitivity labels word B.

CODE EXAMPLE 3-8 Sensitivity Labels WORDS Associated with Compartment Bit 1

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

Code Example 3-9 shows that compartment bit 0 is associated with sensitivity labels word A.

CODE EXAMPLE 3-9 Sensitivity Labels WORDS Associated with Compartment Bit 0

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

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

- `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.
- 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 are specified as *prefixes* and any words to come after the channel name are specified as *suffixes*.

The following table may be used to plan `CHANNELS`.

TABLE 3-3 CHANNELS Planner (for Prefixes, Channel Words, and Suffixes)

For Compartment Bit(s)	Print This Prefix	Print This Channel	Print This Suffix

Procedures

▼ To Configure PRINTER BANNERS

Note - See “Specifying Printer Banners” on page 85, if necessary, before you start. Plan what printer banners you want to associate with any of the words defined in the SENSITIVITY LABELS section of the `label_encodings` file, using Table 3-2.

1. Open the `label_encodings` file for editing as described in “To Modify the `label_encodings` (4) File” on page 66 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:

(continued)

```
name= ORCON;                prefix;
```

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

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

▼ To Configure CHANNELS

Note - See “Specifying CHANNELS” on page 88, if necessary, before you start. Plan what channels line you want to associate with any of the words defined in the SENSITIVITY LABELS section of the `label_encodings` file, using Table 3-3.

1. Open the `label_encodings` file for editing as described in “To Modify the `label_encodings` (4) File” on page 66 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, 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;
```


Modifying Sun's Extensions in the Local Definitions Section

This chapter describes what the Security Administrator role needs to know to define the values in the `LOCAL DEFINITIONS` section of the `label_encodings(4)` file. This chapter includes these topics:

- “Values Specified in the `LOCAL DEFINITIONS` Section” on page 98
- “Specifying Whether Other Labels are Substituted for Administrative Labels” on page 99
- “Changing Label Component Names on Label Builders” on page 100
- “Specifying Colors for Labels” on page 101

This chapter includes these procedures:

- “To Specify the System Default for Administrative Label Names (Optional)” on page 105
- “To Specify a Default User Clearance and Minimum Label (Optional)” on page 107
- “To Change Label Component Names Used in Label Builders (Optional)” on page 106
- “To Assign a Color to a Label or Word” on page 108

LOCAL DEFINITIONS Section

Trusted Solaris uses additional keywords beyond those defined in the government-furnished *Compartmented Mode Workstation Labeling: Encodings Format*. The following example shows the optional `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;

Classification Name= Class;
Compartments Name= Comps;

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

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
```

Values Specified in the LOCAL DEFINITIONS Section

The Security Administrator role can do the following using keywords in the LOCAL DEFINITIONS section (shown in :

- Replace names for administrative labels with administrator-defined alternates.

The renaming of administrative label names can cause interoperability options and is highly discouraged.

- Substitute other valid low and high label names in the user accreditation range for the ADMIN_HIGH and ADMIN_LOW administrative labels.
See “Specifying Whether Other Labels are Substituted for Administrative Labels” on page 99.
- Specify a user clearance and user minimum label.
You only need to specify a user clearance or minimum label here if they should be different from the mandatory minimum clearance= and minimum sensitivity label= definitions in the ACCREDITATION RANGE: section.
See “To Specify a Default User Clearance and Minimum Label (Optional)” on page 107.
- Specify alternate names for classifications and compartments to be used on label builder dialog boxes.
See “To Change Label Component Names Used in Label Builders (Optional)” on page 106.
- Specify which colors are assigned to labels.
Even though the color definitions are optional, assigning colors to labels is highly recommended.
See “To Assign a Color to a Label or Word” on page 108.

Note - Trusted Solaris 7 and later releases do not support flags. Leave the default flags values as they are shown in Code Example 4-1.

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

Specifying Whether Other Labels are Substituted for Administrative Labels

The optional `Default Label View` defined in the installed `label_encodings`. Without a definition in the `label_encodings` file, the default system-wide setting is `External`.

- The `Default Label View` set in the `label_encodings` file is system-wide.
- The system-wide label view can be overridden by the label view assigned to individual user and role accounts.
- Programs are can set their own label views.

The relation between these various settings is described in “Specifying Whether Users See Administrative Labels’ Names” on page 39 in Chapter 1.

To change the system-wide specification, see “To Specify the System Default for Administrative Label Names (Optional)” on page 105 .

Note - The optional `Default Label View` must be specified before the `Color Names` section.

Changing Label Component Names on Label Builders

The following figure shows the names `CLASS` and `COMPS` used on the Multilabel Login: Setting Session Clearance dialog box.

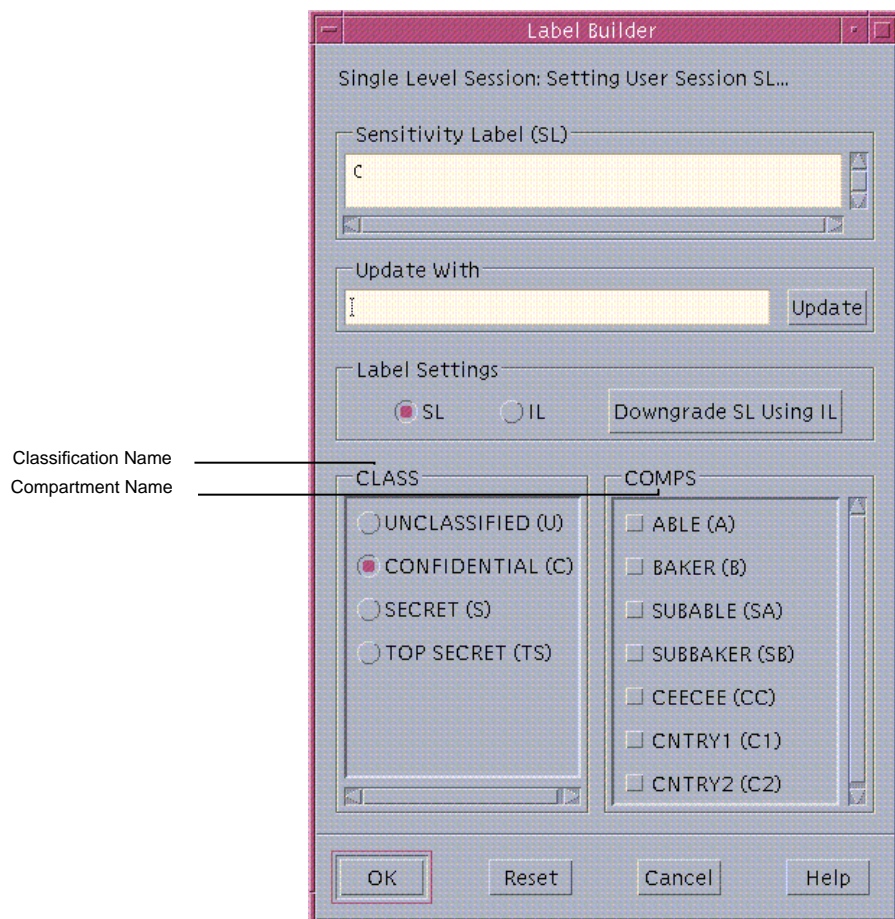


Figure 4–1 Label Component Names on Example Label Builder

To replace the classification and compartment names, see “To Change Label Component Names Used in Label Builders (Optional)” on page 106.

Specifying Colors for Labels

In the `LOCAL DEFINITIONS:` section, the `COLOR NAMES:` keyword is followed by zero or more color assignments. The default color values are shown in the following figure.

CODE EXAMPLE 4-2 COLOR NAMES Section in the LOCAL DEFINITIONS Section of label_encodings File

```
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
```

In the COLOR NAMES section, the Security Administrator role assigns colors to words and to labels. The *color name* can be either a text 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 104. A full discussion of how to specify color is outside the scope of this manual. See 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, if desired.

The color assigned to a label’s component displays as a background color whenever a label includes the specified label components, according to the ordering rules described below. See Figure 4-2 for an example of how the color is used. Although the example is not in color, the PUBLIC, INTERNAL, and NTK_SALES workspace buttons are colored differently than the standard workspace buttons.

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

Colored workspace buttons

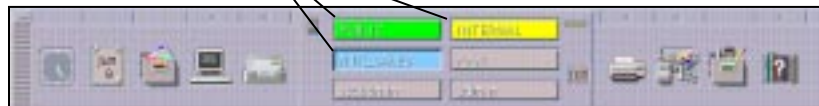


Figure 4-2 Window Label with a Background Color from the COLOR NAMES Section

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 name, 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 the following screen, 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`).

Example 1: Colors Assigned to Words and Labels

```
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;
```

Example 2: Colors Assigned to Words and Labels

Following rule 4 in a system with the color definitions shown in the following example, `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;

```

Color Values

The `/usr/openwin/lib/rgb.txt` database translates 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.

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

- Color values specify the amount of red, green, and blue (RGB) that compose the color.
- RGB values can be specified with three hexadecimal numbers from 0 to 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 #FFFFFF, 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.

The default color values defined in Trusted Solaris `label_encodings COLOR NAMES` section have been chosen with these caveats in mind (see the following screen).

Default COLOR NAMES Assigned to Label Components

```

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;

```

See “To Assign a Color to a Label or Word” on page 108.

Planning Color Names

The following table may be used for planning color names.

TABLE 4-1 Color Names Planner

Label or Name (label= or name=)	Color

Procedures for Modifying Sun Extensions

▼ To Specify the System Default for Administrative Label Names (Optional)

1. In the **Security Administrator** role in an `ADMIN_HIGH` workspace, open the `label_encodings` file for editing.
See “To Modify the `label_encodings` (4) File” on page 66, if needed.
2. Find the lines in the `LOCAL DEFINITIONS` section that define the Default Label View.

```
Default Label View Is External
```

3. **To allow the label names to display, ensure that the line that begins `Default Label View` is set to `Internal`.**

```
Default Label View Is Internal
```

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

▼ To Change Label Component Names Used in Label Builders (Optional)

1. **In the Security Administrator role in an `ADMIN_HIGH` workspace, open the `label_encodings` file for editing.**
See “To Modify the `label_encodings` (4) File” on page 66, if needed.
2. **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;
```

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

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

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

To Specify a Default User Clearance and Minimum Label (Optional)

- 1. In the Security Administrator role in an ADMIN_HIGH workspace, open the label_encodings file for editing.**

See “To Modify the label_encodings (4) File” on page 66, if needed.

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

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

- 3. Replace the Sensitivity Label with your desired minimum user label:**

The following example shows a new minimum label of c.

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

- 4. Replace the Clearance with your desired user clearance:**

The following example shows a new clearance of s.

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

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

▼ To Assign a Color to a Label or Word

Note - If no color is defined for a classification in the `COLOR NAMES` section of the `label_encodings` file, the color black is used.

1. **In the Security Administrator role, open the `label_encodings` file for editing.**
See “To Modify the `label_encodings` (4) File” on page 66, if needed.

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

```
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;
```

3. **Optionally, define colors for individual compartment words.**

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

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

4. **Optionally, define colors for labels.**

In the example, the color assigned to `NEED_TO_KNOW SYSADM` is bluePurple.

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

5. **Make sure a color is defined for each classification.**

If a color is not defined for a classification, the background color used is black, so, make sure to define every classification.

In the screen below, the classification `REGISTERED` is assigned the color red, and the `NEED_TO_KNOW SYSADM` classification is assigned the color blue.

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

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

Example: Planning an Organization's Labels

This chapter models how to get started if you have not previously used labels. The following major sections show how one organization analyzed its labeling requirements and set up a fairly simple set of labels:

- “Identifying the Site's Label Requirements ” on page 111
- “ Analyzing the Requirements for Each Label” on page 117
- “Defining the Set of Labels” on page 121
- “Specifying the Labels During Post-Install Configuration” on page 134

This chapter models how to do the following:

- Identify a set of labels that meet your company's information-protection goals
- Define the components of labels and their relationships:
 - Classifications (words that specify which labels are more sensitive)
 - Compartments (words that associate a label or clearance with a project or group)

Identifying the Site's Label Requirements

Solar Systems, Inc. is a fictional name for the company whose label requirements are modeled in this example. To protect the corporation's intellectual property, the company's legal department mandates that employees use three labels on all

sensitive email and printed materials. The three labels, from most-sensitive to least-sensitive are:

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 without 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. Some employees either do not understand, forget about, or ignore the requirements. Even when labels are properly applied, the information is not always properly handled, stored, and distributed. For example, reports trickle back that even 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 want a better way *to control:*
 - *Who can see or modify sensitive information,*
 - *Which information is printed on which printers,*
 - *How printer output is handled, and*
 - *How information at various levels of 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 labeling up to computer users. All 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 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 was not yet fully understood at the company, executives knew they could put the following features to use right away:

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

Figure 5-1 shows an employee working at a 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 nondisclosure agreements. When he sends email to the printer, the print job is automatically assigned the label `INTERNAL_USE_ONLY`.

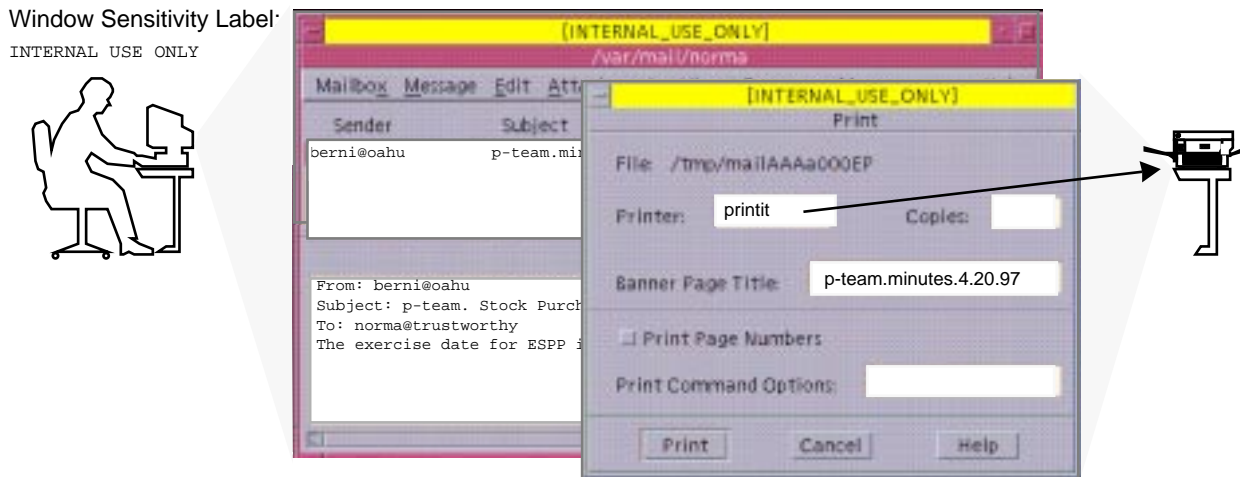


Figure 5-1 Automatic Labeling of Print Jobs

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

In Figure 5-2, the letter that was sent to the printer in Figure 5-1 is printed with the user's working label, `INTERNAL_USE_ONLY`, at the top and bottom of every page.

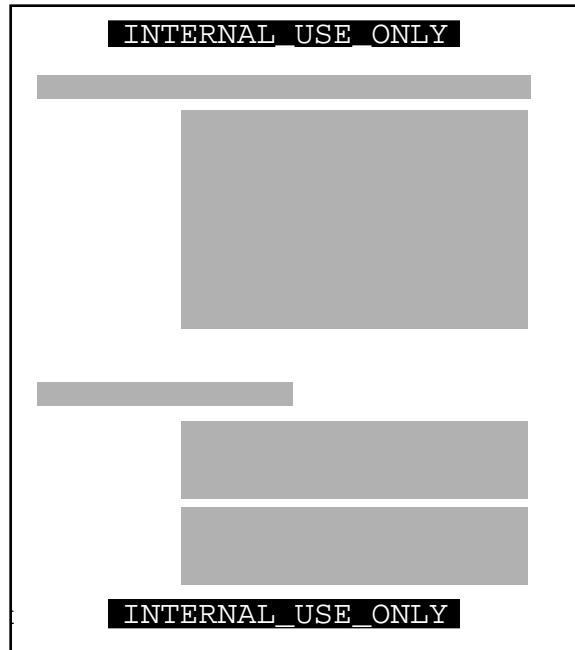


Figure 5-2 Label Automatically Printed on Body Pages

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

Figure 5-3 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 HR`

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

Figure 5-3 Handling Guidelines on Banner and Trailer Pages

Below the sensitivity label in the previous example, a *handling caveat* provides instructions about how the printed material should be distributed. The instructions are understood to mean 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 nondisclosure agreement.

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

For example, the legal department's printer can be set up (as illustrated in Figure 5-4) 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 and other who have signed nondisclosure 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

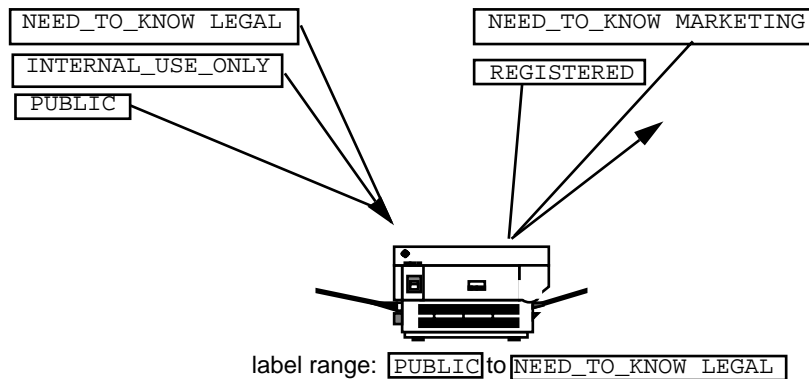


Figure 5-4 How a Printer With a Restricted Label Range Handles Jobs at Various Labels

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



Figure 5-5 Automatic Labeling of Email

Similar to how the printer label range controls which jobs can be printed on a particular printer, a user's *personal sensitivity label range* limits which email the person can receive and send (see Figure 5-6).

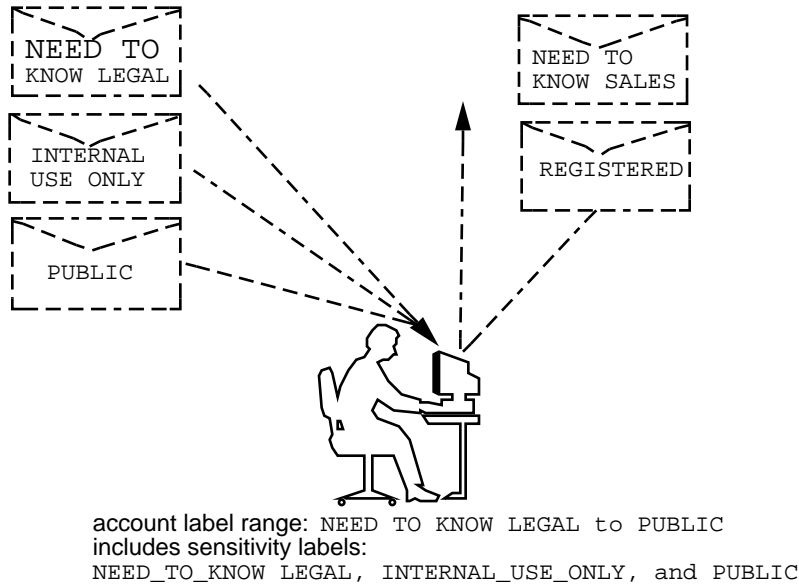


Figure 5-6 A User Receiving Email within His Account Label Range

- Gateways to the Internet can be set up to screen email so that email at inappropriate labels (any label except PUBLIC) cannot 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 organization's information-processing goals well enough to be responsible for overseeing or implementing the site's security

That person is assigned the job of Security Administrator.

Long before installing Trusted 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.

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 assume the Security Administrator role for administering system security and assigning administrative responsibilities. The section called "Implement Trusted Solaris in Accordance with Site Security" in *Trusted Solaris Installation and Configuration* provides guidance on creating a site's security policy.

The Security Administrator also reads "More About Labels" on page 37 in this manual to review concepts directly related to setting up security and encoding labels.

Analyzing the Requirements for Each Label

The Security Administrator agrees that the set of labels mandated by the legal department is a good start but realizes that the labels need to be analyzed further before they can be encoded.

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 employees, all of whom have signed nondisclosure agreements before 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 nondisclosure 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 company, has a higher level of sensitivity than INTERNAL_USE_ONLY, and has a more limited audience. Distribution is limited to employees who have a need to know the information and to others who have signed nondisclosure 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 can copy it and pass it on to other people who also have a need to know and have signed a nondisclosure 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 a group in this label makes it clear that the information should not be given to anyone outside of the group. Information with this label 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 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, and it cannot be shown to employees of other companies who have not signed a nondisclosure agreement—even if the owner authorizes them to see it. Information with this label may not be sent via 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 contain the names of groups or departments. The Security Administrator asked for suggestions about what words to use to define groups or areas of interest within the organization, 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 Figure 5-7, to visualize the relationships and rearrange the pieces until they all fit together.

The administrator came up with the following:

- 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 nondisclosure 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 nondisclosure agreement.

A phrase such as NON-DISCLOSURE AGREEMENT REQUIRED would be a good reminder that this requirement exists.

- The handling instructions on banner and trailer pages should have clear wording on how to handle the information 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 nondisclosure agreement is required for any output whose label requires it.

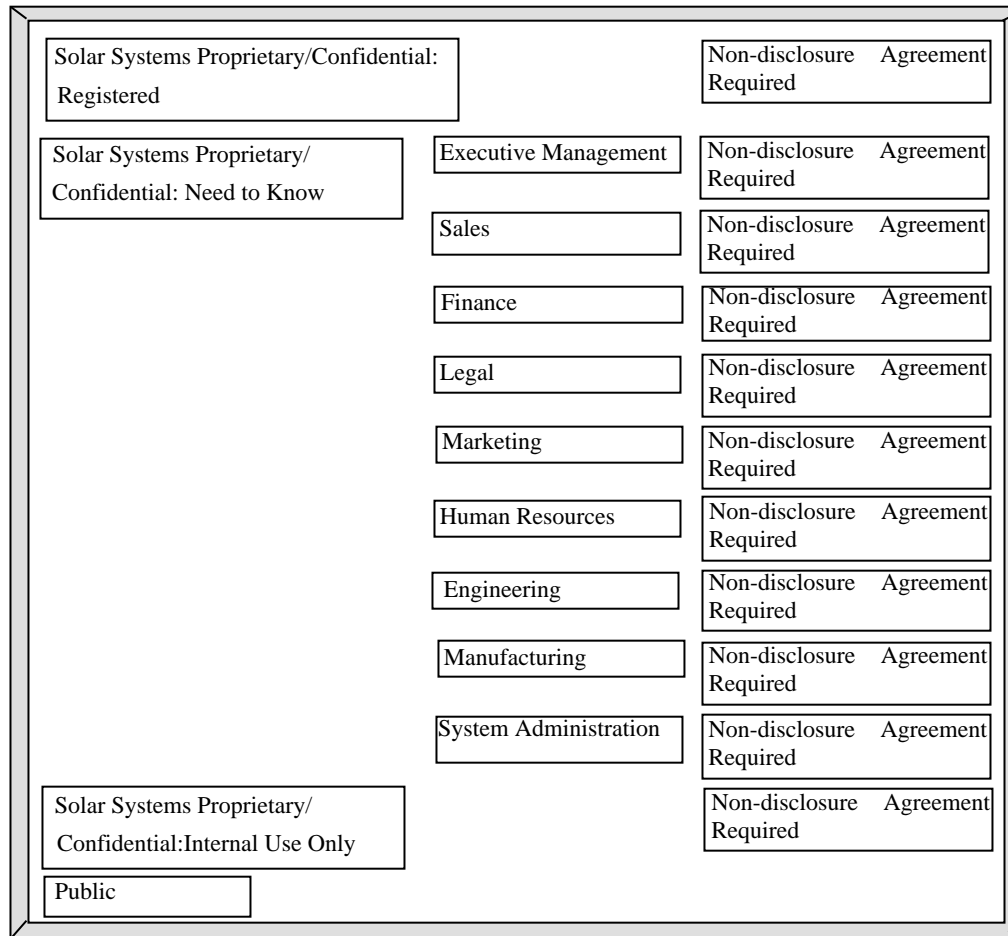


Figure 5-7 Example Planning Board for Label Relationships

Defining the Set of Labels

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

- Classifications
- Other words
- Relations between and among the words
- Classification restrictions 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. Because the truncated names of all the label names above PUBLIC would begin with the words SOLAR SYSTEMS PROPRIETARY CONFIDENTIAL, the truncated names would be indistinguishable without manually extending the frame for each window.

The Security Administrator defined the following labels:

- REGISTERED
- NEED_TO_KNOW
- INTERNAL_USE_ONLY
- PUBLIC

Planning the Compartments

The group names will be encoded as non-hierarchical *compartments*. Compartments will be restricted to appear only in labels that have the NEED_TO_KNOW classification. Compartments are restricted to appear with certain classifications by 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 whose labels have more than one group 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 the labels that control 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 use the `lp -o nolabels` option to suppress the printing of top and bottom labels on body pages of a print job. The Security Administrator role can give the `Print Without Labels` authorization to everyone or to no one.

The Print PostScript File authorization allows a user to submit a PostScript file to the printer, 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 without labels printed on them, the Security Administrator role gives the Print Without Labels and Print PostScript File authorizations to all the writers.

Planning for Supporting Procedures

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

The Security Administrator realizes that anyone with a clearance that includes the word REGISTERED can access any registered information anywhere in the company unless certain additional precautions are taken. Therefore, those who have REGISTERED in their clearance must be instructed to use UNIX permissions, so that only the creator can look at or modify the file. See the following example.

CODE EXAMPLE 5-1 Using DAC to Protect Registered Information

```
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
```

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

Rules for Configuring Printers

Table 5-1 shows how printers in various locations accessible to various types of people need to be configured.

TABLE 5–1 Printer Label Range Example Settings in Various Locations

Printer Location	Type of Access	Label Range
lobby or public meeting room	Anyone	PUBLIC to PUBLIC
internal company printer room	Available to all employees and others who have signed nondisclosure agreements	PUBLIC to INTERNAL_USE_ONLY
restricted area for one group	Members of group specified in the NEED_TO_KNOW GROUP_NAME compartment	NEED_TO_KNOW GROUP_NAME to NEED_TO_KNOW GROUP_NAME
strictly controlled area	Available only to those who have the REGISTERED classification in their clearance	REGISTERED to REGISTERED

See “Managing Printing” in *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.

Planning Classification Values in a Worksheet

The worksheet in Table 5–2 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 SENSITIVITY LABELS, and CLEARANCES sections.

TABLE 5-2 Classifications Planner

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

Planning Compartment Values and Classification/ Compartment Constraints in a Worksheet

Table 5-3 defines the relationships between words and classifications that were arrived at by moving things around on the planning board in Figure 5-7. Because of how 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 5-3 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	

TABLE 5-3 Compartments and User Accreditation Range Combinations Planning Table *(continued)*

Classification	Compartment Name/ sname/ Bit	Combination Constraints
	HUMAN RESOURCES/ HR/ 16	
	MARKETING/ MKTG/ 15 20	
	LEGAL/ LEGAL/ 14	
	FINANCE/ FINANCE/ 13	
	SALES/ SALES/ 12	
	EXECUTIVE MANAGEMENT GROUP/ EMG/ 11	
	ALL_DEPARTMENTS/ ALL/ 11-20	
REGISTERED		REGISTERED only valid combination

The Security Administrator uses Table 5-4 to keep track of which bits have been used for compartments and which for markings.

TABLE 5-4 Compartment Tracking Table

11	12	13	14	15	16	17	18	19	20	
----	----	----	----	----	----	----	----	----	----	--

Planning Clearances in a Worksheet

The components of these labels are also assigned to users in clearances. The worksheet's Clearance Planner (shown in Table 5-5) defines the label components to be used in clearances.

Key to Table 5-5:

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 5-5 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 as needed 2
NTK		ENG								Assigned to ENG group

TABLE 5-5 Clearance Planner (continued)

CLASS	COMP	COMP	COMP	COMP	COMP	COMP	COMP	COMP	COMP	Notes
									SYSADM	Assigned to system admin
IUO										Assigned to employees, and others w/NDAs
PUB										Assigned to anyone

1. The highest possible label in the system, consisting of the highest classification and all of the defined compartments. Because no one should be able to access all information in all departments, this label is not in the user accreditation range, and no one should be assigned this clearance.
2. When working at the REGISTERED sensitivity label, the user should set permissions to restrict access to 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 can be used to associate a string with any compartment that appears in the sensitivity label of the print job. In this encodings, only the NEED_TO_KNOWclassification has compartments. Table 5-6 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 5-6 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)

This goal is met by assigning in the CHANNELS section the same compartment bits that were assigned to group names earlier in this example. The Solar Systems

company plans to use the same group names both in the compartments and in the channels.

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

TABLE 5-7 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:

- *minimum sensitivity label*
- *minimum clearance,*
- *minimum protect as classification*

Because the Solar Systems company wants employees to be able to use all the defined sensitivity labels and wants 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. The minimum protect as classification can be set higher than the *actual* minimum classification. However, the Solar Systems company requirements allow the minimum protect as classification to always be equal to the real classification of the print job's sensitivity label. The Security Administrator defines all of values for the minimum sensitivity label, minimum clearance and minimum protect as classification as PUBLIC as shown in the following table.

TABLE 5-8 ACCREDITATION RANGE Minimum Values

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

Planning the Colors in the COLOR NAMES Worksheet

The color assigned to a label displays in the background whenever the name of the label appears at the top of a window. The lettering is displayed in a color that 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(4)` 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 the following table.

TABLE 5–9 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 MANU	#0000BF
NEED_TO_KNOW PROJECT_TEAM	#9E7FFF
NEED_TO_KNOW SYSADM	#5B85D0
NEED_TO_KNOW ALL	#4D658D
NEED_TO_KNOW SYSADM	#5B85D0
REGISTERED	red
ADMIN_HIGH	#636363

Specifying the Labels During Post-Install Configuration

The install team makes a printed copy and an on-line copy of the installed `label_encodings(4)` file in case of problems with the new version of the file supplied by the Security Administrator role.

The Security Administrator role uses any text editor to create the `label_encodings(4)` file, and then uses the `Check Encodings` action to check the file. If the file passes `Check Encodings`, the action offers the option of installing the new version. When the Security Administrator role answers Yes, `Check Encodings` overwrites the current version of the `label_encodings` file. The `Check Encodings` action creates a backup version of the existing file (naming it `label_encodings.orig`), before overwriting it.

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

Encoding the VERSION

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

CODE EXAMPLE 5-2 Modified `VERSION` Entry

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

Encoding the CLASSIFICATIONS

The following example shows the Solar Systems' classifications and values from Table 5-2, Table 5-3 and Table 5-4 added to the `CLASSIFICATIONS` section.

CODE EXAMPLE 5-3 Modified `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;
```

(continued)

```
name= REGISTERED; sname= REGISTERED; aname= REGISTERED; value= 6;
```

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

Encoding the SENSITIVITY LABELS

The compartments in the Table 5-3 are encoded in the SENSITIVITY LABELS: WORDS: example shown below.

This example does not have any required combinations or combination constraints.

CODE EXAMPLE 5-4 Modified WORDS in the SENSITIVITY LABELS Section

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:

Encoding the INFORMATION LABELS

Even though information labels are not used, values must be supplied under the INFORMATION LABELS: WORDS: section for the file to pass the encodings check.

The Security Administrator role copies the words from the SENSITIVITY LABELS: WORDS: section, as shown in the following example.

CODE EXAMPLE 5-5 WORDS in the INFORMATION LABELS Section

INFORMATION LABELS:

WORDS:

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

Encoding the CLEARANCES

Because the clearance words are the same as the sensitivity labels words, the words in the following example are the same as those in Code Example 5-4.

CODE EXAMPLE 5-6 Modified WORDS in the CLEARANCES Section

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;
```

(continued)


```

name= HUMAN_RESOURCES; sname= HR; compartments= 16; minclass= NEED_TO_KNOW;
name= ENGINEERING; sname= ENG; compartments= 17 20; minclass= NEED_TO_KNOW;
name= MANUFACTURING; sname= MANUFACTURING; compartments= 18; minclass= NEED_TO_KNOW;
name= SYSTEM_ADMINISTRATION; sname= SYSADM; compartments= 19;
minclass= NEED_TO_KNOW;
name= PROJECT_TEAM; sname= P_TEAM; compartments= 20;
minclass= NEED_TO_KNOW;

```

REQUIRED COMBINATIONS:

COMBINATION CONSTRAINTS:

Encoding the CHANNELS

This example is encoded with one channel for each group name compartment, 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).

DISTRIBUTE ONLY TO *GROUP_NAME* (NON-DISCLOSURE AGREEMENT REQUIRED)

The channel specifications shown in the following example will create the desired wording in the handling caveats section.

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

CODE EXAMPLE 5-7 Modified WORDS in the CHANNELS Section

CHANNELS:

WORDS:

```

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

name= EXECUTIVE_MANAGEMENT_GROUP;
prefix= DISTRIBUTE_ONLY_TO; compartments= 11;
suffix= EMPLOYEES (NON-DISCLOSURE AGREEMENT REQUIRED);
name= SALES; prefix= DISTRIBUTE_ONLY_TO; compartments= 12;
suffix= EMPLOYEES (NON-DISCLOSURE AGREEMENT REQUIRED);
name= FINANCE; prefix= DISTRIBUTE_ONLY_TO; compartments= 13;
suffix= EMPLOYEES (NON-DISCLOSURE AGREEMENT REQUIRED);

```

(continued)

```

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);

```

Encoding the PRINTER BANNERS

Note - The term *printer banners* has a specialized meaning in the `label_encodings(4)` file, and it does not refer to the banner page that is printed before a job. Printer banners appear as a string on the printer banner page when the compartment associated with it appears in a job's label.

The printer banner specifications shown in the following example will create the desired wording in the PRINTER BANNERS section.

Note - Any prefixes are defined at the top of the section as shown in the following example, and they have no compartments assigned to them. They are used in defining the PRINTER BANNERS; each printer banner has a prefix assigned to it.

CODE EXAMPLE 5-8 Modified WORDS in the PRINTER BANNERS Section

```
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;;

```

(continued)

```

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;

```

Encoding the ACCREDITATION RANGE

The combination constraints from the Table 5-3 and the minimum clearance, minimum sensitivity label and minimum protect as classification from Table 5-8 are encoded in the ACCREDITATION RANGE: example shown in the following example. 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.

CODE EXAMPLE 5-9 Modified ACCREDITATION RANGE Section

ACCREDITATION RANGE:

classification= PUBLIC; only valid compartment combinations:

PUBLIC

classification= INTERNAL_USE_ONLY; only valid compartment combinations:

INTERNAL

classification= NEED_TO_KNOW; all compartment combinations valid;

classification= REGISTERED; only valid compartment combinations:

REGISTERED

(continued)

```

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

```

Encoding the Wording for Label Builders, Colors, and Other LOCAL DEFINITIONS Values

The following example shows that none of the default values are changed at Solar Systems, Inc. for the default and forced flags, and Default Label View in the LOCAL DEFINITIONS section.

CODE EXAMPLE 5-10 Accepting Defaults in the LOCAL DEFINITIONS Section

LOCAL DEFINITIONS:

```

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

```

Default Label View is External;

Encoding the Heading Names for Label Builders

The default settings for heading names used in label builders are shown in the following example.

CODE EXAMPLE 5-11 Default Heading Names for Label Builders

```

Classification Name= Class;
Compartments Name= Comps;

```

Label builders are displayed whenever you need to set a label. For example, the following figure shows a label builder with the heading names specified at the Solar Systems company: *Classification* instead of *Class*, and *Departments* instead of *Comps*.

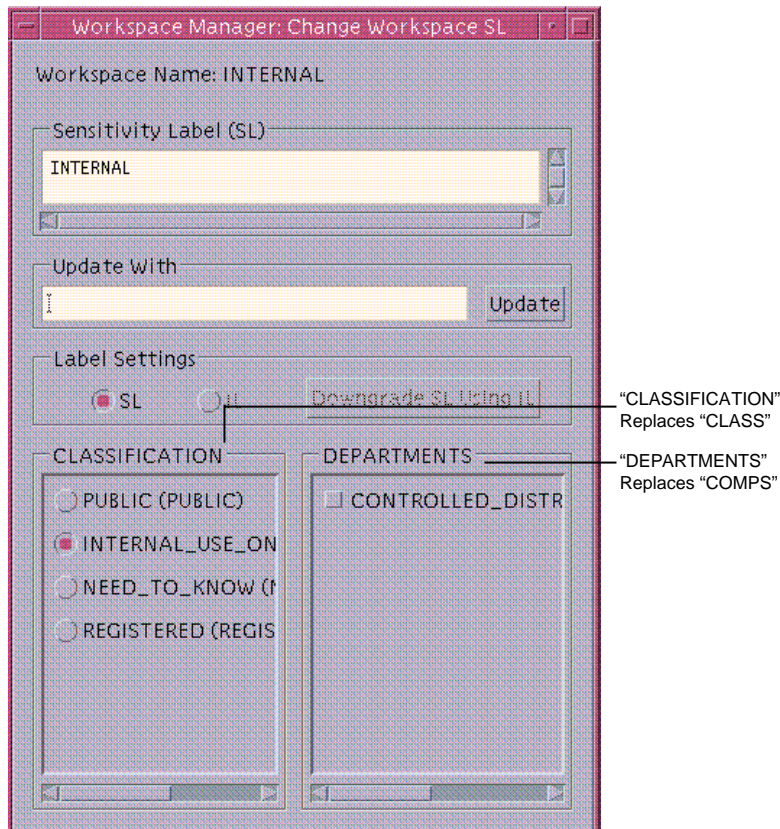


Figure 5–8 Label Builder With Changed Headings

The following example shows the modifications the Solar System Security Administrator role made to change the default values set for the Classification Name, Compartments Name, and Markings Name.

CODE EXAMPLE 5–12 Modified Wording for Label Builders

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

Encoding the COLOR NAMES

The color names used in Code Example 5–13 were taken from the worksheet in Table 5–9.

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= #F7FFF7;
label= NEED_TO_KNOW ENG;  color= #007FFF;
label= NEED_TO_KNOW MANUFACTURING; color= #0000BF;
label= NEED_TO_KNOW PROJECT_TEAM; color= #9E7FFF;
label= NEED_TO_KNOW SYSADM; color= #5B85D0;
label= NEED_TO_KNOW ALL;  color= #4D658D;
label= REGISTERED;       color= red;

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

*

* End of local site definitions

Configuring Users to Enforce Labeling Decisions

While setting up user accounts during the post-installation configuration, the Security Administrator role needs to specify the following for all users in the `User Manager: Labels` dialog (see the figure that follows the list).

- The appropriate clearance (in the Clearance dialog)
 - See “Planning Clearances in a Worksheet ” on page 127.
- The appropriate minimum label (in the Minimum SL Dialog Box)
- Show sensitivity labels

Configuring Printing To Enforce Labeling Decisions

The Security Administrator role 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 124.**

The Security Administrator role 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 the writers 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 and to use `lp` with the `-o nolabels` option when printing the PostScript file.
3. 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 label for the print server that matches the 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 “Managing Printing” in the *Trusted Solaris Administrator’s Procedures* for how to specify a default label for an unlabeled print server.

Note - When a printer is connected to an unlabeled print server, no labels or labeled banner/trailer pages are printed.

- ii. If desired, set up a separate `.login` file in the single-level directory (SLD) at the appropriate 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, do one of the following:
 - i. Make sure the printer is configured so that the `Always Print Banners` check box is 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 shown in the following example in the `/usr/lib/lp/postscript/tsol.separator.ps` file.

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


Example: Label Encodings File

This appendix contains a sample `label_encodings` file developed along with Chapter 5.

Classifications

The example file has the following four classifications:

- PUBLIC
- INTERNAL_USE_ONLY
- NEED_TO_KNOW
- REGISTERED

Compartments

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

`NEED_TO_KNOW` compartments are:

- ALL_DEPARTMENTS
- EXECUTIVE_MGMNT_GROUP
- SALES
- FINANCE
- LEGAL
- MARKETING
- HUMAN_RESOURCES

- ENGINEERING
- MANUFACTURING
- SYSTEM_ADMINISTRATION
- PROJECT_TEAM
- The ALL_DEPARTMENTS compartment word gets turned on when all defined compartment bits are on and works as a toggle in a label builder.

PROJECT_TEAM is hierarchically below both ENGINEERING and MARKETING. The hierarchy allows someone working at NEED_TO_KNOW ENGINEERING or at NEED_TO_KNOW MARKETING to read files with the NEED_TO_KNOW PROJECT_TEAM label but not to write to files that have that 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.

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

CODE EXAMPLE A-1 label_encodings.simple

```
* @(#)label_encodings.simple 5.9 99/11/01 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 - 5.9 99/11/01
```

(continued)

```

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

```

INFORMATION LABELS:

WORDS:

```

name= SYSTEM_ADMINISTRATION; sname= SYSADM; compartments= 19;

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

```

REQUIRED COMBINATIONS:

COMBINATION CONSTRAINTS:

SENSITIVITY LABELS:

WORDS:

```

name= ALL_DEPARTMENTS; sname= ALL; compartments= 11-20;
minclass= NEED_TO_KNOW;
name= EXECUTIVE_MGMNT_GROUP; sname= EMG; compartments= 11;
minclass= NEED_TO_KNOW;
name= SALES; sname= SALES; compartments= 12;
minclass= NEED_TO_KNOW;
name= FINANCE; sname= FINANCE; compartments= 13;
minclass= NEED_TO_KNOW;
name= LEGAL; sname= LEGAL; compartments= 14;

```

(continued)

```

minclass= NEED_TO_KNOW;
name= MARKETING; sname= MRKTG; compartments= 15 20;
minclass= NEED_TO_KNOW;
name= HUMAN_RESOURCES; sname= HR; compartments= 16;
minclass= NEED_TO_KNOW;
name= ENGINEERING; sname= ENG; compartments= 17 20;
minclass= NEED_TO_KNOW;
name= MANUFACTURING; sname= MANUFACTURING; compartments= 18;
minclass= NEED_TO_KNOW;
name= SYSTEM_ADMINISTRATION; sname= SYSADM; compartments= 19;
minclass= NEED_TO_KNOW;
name= PROJECT_TEAM; sname= P_TEAM; compartments= 20;
minclass= NEED_TO_KNOW;
REQUIRED COMBINATIONS:
COMBINATION CONSTRAINTS:

CLEARANCES:

WORDS:

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

REQUIRED COMBINATIONS:

COMBINATION CONSTRAINTS:

CHANNELS:

WORDS:

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

```

(continued)

```

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

```

PRINTER BANNERS:

WORDS:

```

name= 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;

```

(continued)

```

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

classification= NEED_TO_KNOW; all compartment combinations valid;

classification= REGISTERED; only valid compartment combinations:

REGISTERED

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

Classification Name= Classification;
Compartments Name= Departments;
COLOR NAMES:

        label= Admin_Low;          color= #bdbdbd;

```

(continued)

```
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
```


Differences Between Default Label Encodings Files

This appendix describes the differences between the single-label and multilabel versions of the `label_encodings` file, which are in the `/etc/security/tsol/` directory in the default system.

Differences Between Single-label and Installed Label Encodings Files

The `label_encodings.single` file that is installed by default is almost identical to the multilabel version `label_encodings.multi`. 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

The `ACCREDITATION RANGE` settings in the default `label_encodings` file are shown in the following example.

CODE EXAMPLE B-1 `ACCREDITATION RANGE` Settings in the Default Multilabel Encodings File

```
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;

```

To allow the site to use all the classifications and compartment words defined elsewhere in the `label_encodings.multi` 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 82 in Chapter 3.)

Single Sensitivity Label Version

This section describes the ACCREDITATION RANGE settings in the default `label_encodings.single` file, as shown in the following example.

CODE EXAMPLE B-2 ACCREDITATION RANGE Settings in the Default Single-label Encodings File

```

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

```

The `label_encodings.single` file restricts the user ACCREDITATION RANGE in the ACCREDITATION RANGE section:

- 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

An easy way to run with a single sensitivity label is to change only the ACCREDITATION RANGE section in the `label_encodings.single` file. Alternately, you can create an encodings file from scratch with only one classification and with either no compartments or with only the compartments you need. See “To Replace the Single Label in the Default Single-label Encodings File” on page 73 for guidelines for both approaches.