Trusted Extensions Label Administration

Part No: E54843
November 2016

Trusted Extensions Label Administration

Part No: E54843

Copyright © 1997, 2016, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS. Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc`.

Access to Oracle Support

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

Référence: E54843

Copyright © 1997, 2016, Oracle et/ou ses affiliés. Tous droits réservés.

Ce logiciel et la documentation qui l'accompagne sont protégés par les lois sur la propriété intellectuelle. Ils sont concédés sous licence et soumis à des restrictions d'utilisation et de divulgation. Sauf stipulation expresse de votre contrat de licence ou de la loi, vous ne pouvez pas copier, reproduire, traduire, diffuser, modifier, accorder de licence, transmettre, distribuer, exposer, exécuter, publier ou afficher le logiciel, même partiellement, sous quelque forme et par quelque procédé que ce soit. Par ailleurs, il est interdit de procéder à toute ingénierie inverse du logiciel, de le désassembler ou de le décompiler, excepté à des fins d'interopérabilité avec des logiciels tiers ou tel que prescrit par la loi.

Les informations fournies dans ce document sont susceptibles de modification sans préavis. Par ailleurs, Oracle Corporation ne garantit pas qu'elles soient exemptes d'erreurs et vous invite, le cas échéant, à lui en faire part par écrit.

Si ce logiciel, ou la documentation qui l'accompagne, est livré sous licence au Gouvernement des Etats-Unis, ou à quiconque qui aurait souscrit la licence de ce logiciel pour le compte du Gouvernement des Etats-Unis, la notice suivante s'applique:

U.S. GOVERNMENT END USERS. Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

Ce logiciel ou matériel a été développé pour un usage général dans le cadre d'applications de gestion des informations. Ce logiciel ou matériel n'est pas conçu ni n'est destiné à être utilisé dans des applications à risque, notamment dans des applications pouvant causer des dommages corporels. Si vous utilisez ce logiciel ou matériel dans le cadre d' applications dangereuses, il est de votre responsabilité de prendre toutes les mesures de secours, de sauvegarde, de redondance et autres mesures nécessaires à son utilisation dans des conditions optimales de sécurité. Oracle Corporation et ses affiliés déclinent toute responsabilité quant aux dommages causés par l'utilisation de ce logiciel ou matériel pour ce type d'applications.

Oracle et Java sont des marques déposées d'Oracle Corporation et/ou de ses affiliés. Tout autre nom mentionné peut correspondre à des marques appartenant à d'autres propriétaires qu'Oracle.

Intel et Intel Xeon sont des marques ou des marques déposées d'Intel Corporation. Toutes les marques SPARC sont utilisées sous licence et sont des marques ou des marques déposées de SPARC International, Inc. AMD, Opteron, le logo AMD et le logo AMD Opteron sont des marques ou des marques déposées d'Advanced Micro Devices. UNIX est une marque déposée d'The Open Group.

Ce logiciel ou matériel et la documentation qui l'accompagne peuvent fournir des informations ou des liens donnant accès à des contenus, des produits et des services émanant de tiers. Oracle Corporation et ses affiliés déclinent toute responsabilité ou garantie expresse quant aux contenus, produits ou services émanant de tiers, sauf mention contraire stipulée dans un contrat entre vous et Oracle. En aucun cas, Oracle Corporation et ses affiliés ne sauraient être tenus pour responsables des pertes subies, des coûts occasionnés ou des dommages causés par l'accès à des contenus, produits ou services tiers, ou à leur utilisation, sauf mention contraire stipulée dans un contrat entre vous et Oracle.

Accessibilité de la documentation

Pour plus d'informations sur l'engagement d'Oracle pour l'accessibilité à la documentation, visitez le site Web Oracle Accessibility Program, à l'adresse `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc`.

Accès aux services de support Oracle

Les clients Oracle qui ont souscrit un contrat de support ont accès au support électronique via My Oracle Support. Pour plus d'informations, visitez le site `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` ou le site `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` si vous êtes malentendant.

Contents

Using This Documentation 13

1 About Labels in Trusted Extensions 15
- Labels and Security Policy 15
- Types of Labels, Their Components and Uses 16
  - Label Ranges Restrict Access 17
  - Labels Are Used in Access Control Decisions 17
  - Label Components 19
  - Label Dominance 20
  - Accreditation Ranges, Label Ranges, and Valid Labels 21
  - System Accreditation Range 22
  - User Accreditation Range 23
  - Account Label Range 24
  - Account Label Range Examples 25
  - Session Range 27
  - Label Availability in Trusted Extensions Sessions 29
  - Labeled Workspaces 30
- Label Administration 30
  - Label Visibility 30
  - Labels on Printed Output 31
  - Authorizations for Relabeling Information 31
  - Privileges for Translating Labels 31

2 Planning Labels in Trusted Extensions 33
- Planning Labels in Trusted Extensions 33
  - ▼ How to Plan for Labels 33
  - ▼ How to Plan the Encodings File 34
- Sources for Encodings Files 37
  - Encodings Files From Trusted Extensions 38
  - Oracle Solaris Extensions to `label_encodings` File 41

3 Creating a Label Encodings File 43
Encodings File Syntax 43
Word Order Requirements 44
Classification Name Syntax 45
Managing a Label Encodings File 50
▼ How to Create a `label_encodings` File 51
▼ How to Analyze and Verify the `label_encodings` File 51
▼ How to Distribute the `label_encodings` File 52
▼ How to Add or Rename a Classification 52
▼ How to Specify Default and Inverse Words 54
▼ How to Create a Single-Label Encodings File 55
▼ How to Debug a `label_encodings` File 58

4 Labeling Printer Output 59
Labels on Body Pages 59
Security Text on Banner and Trailer Pages 60
Specifying the "Protect As" Classification 62
Specifying Printer Banners 63
Specifying Channels 65
Configuring Security Text on Print Jobs 70
▼ How to Specify the Text in `PRINTER BANNERS` 70
▼ How to Specify Handling Instructions in `CHANNELS` 71
▼ How to Set a Minimum "Protect As" Classification 72

5 Customizing the `LOCAL DEFINITIONS` Section 73
`LOCAL DEFINITIONS` Section 73
Contents of `LOCAL DEFINITIONS` Section 74
Specifying Colors for Labels 74
Modifying Extensions From Oracle Solaris to the `label_encodings` File 77
▼ How to Add Extensions From Oracle Solaris to an Encodings File 77
▼ How to Specify Default User Labels 78
▼ How to Assign a Color to a Label or Word 79

6 Example of Planning an Organization's Encodings File 81
Identifying the Site's Label Requirements 81
Satisfying Information Protection Goals 82
Trusted Extensions Features That Address Labeling and Access 82
Climbing the Security Learning Curve 85

Analyzing the Requirements for Each Label 86
Requirements for `CONFIDENTIAL: INTERNAL_USE_ONLY` 86
Requirements for `CONFIDENTIAL: NEED_TO_KNOW` 86
Requirements for `CONFIDENTIAL: REGISTERED` 87
Names of Groups With `NEED_TO_KNOW` Label 87
Understanding the Set of Labels 88
Defining the Set of Labels 91
Planning the Classifications 91
Planning the Compartments 91
Planning the Use of Words in MAC 92
Planning the Use of Words in Labeling System Output 92
Planning Unlabeled Printer Output 93
Planning for Supporting Procedures 93
Planning the Classification Values in a Worksheet 94
Planning the Compartment Values and Combination Constraints in a Worksheet 95
Planning the Clearances in a Worksheet 96
Planning the Printer Banners in a Worksheet 97
Planning the Channels in a Worksheet 98
Planning the Minimum Labels in an Accreditation Range 99
Planning the Colors in a Worksheet 99
Editing and Installing the `label_encodings` File 100
Specifying the Version 100
Specifying the Classifications 101
Specifying the Sensitivity Labels 101
Specifying the Information Labels 102
Specifying the Clearances 102
Specifying the Channels 103
Specifying the Printer Banners 104
Specifying the Accreditation Range 105
Specifying the Local Definitions 105
Configuring Users and Printers for Labels 107

A Customized Encodings File for SecCompany 109
SecCompany's `label_encodings` File 109
SecCompany's Verification of the `label_encodings` File 113

Index 121

Figures

FIGURE 1 Comparing the Label of a Text Editor With the Label Property in the File Browser 18
FIGURE 2 CIPSO Label Definition 19
FIGURE 3 Representation of the `TS`, `TS A`, `TS B`, and `TS AB` Labels 20
FIGURE 4 How System Accreditation Range Is Constrained by Rules 22
FIGURE 5 `ACCREDITATION RANGE` Section of `label_encodings` File 24
FIGURE 6 Constraints on Account Label Ranges 26
FIGURE 7 Comparison of Session Ranges 28
FIGURE 8 Cumulative Effect of Constraints on a Session Range 29
FIGURE 9 Classifications in the Default `label_encodings` File 39
FIGURE 10 Compartments in the Default `label_encodings` File 40
FIGURE 11 Label Automatically Printed on Body Pages 60
FIGURE 12 Typical Banner Page of a Labeled Print Job 61
FIGURE 13 Differences on a Trailer Page 62
FIGURE 14 "Protect As" Statement 63
FIGURE 15 Commercial Use of `PRINTER BANNERS` Section on Banner Page 64
FIGURE 16 U.S. Government Use of `PRINTER BANNERS` Section on Banner Page 64
FIGURE 17 Commercial Use of `CHANNELS` Section on Banner Page 66
FIGURE 18 U.S. Government Use of `CHANNELS` Section on Banner Page 67
FIGURE 19 Window Labels With Colors From `COLOR NAMES` 75
FIGURE 20 Label Automatically Printed on Body Pages 83
FIGURE 21 How a Printer With a Restricted Label Range Handles Print Jobs 84
FIGURE 22 User Receiving Email Within the Account Label Range 85
FIGURE 23 Sample Planning Board for Label Relationships at SecCompany 90

Tables

TABLE 1 Accreditation Range and Account Label Range Examples 27
TABLE 2 `label_encodings` Keywords 43
TABLE 3 Effect of Minimum "Protect As" Classification on Printer Output 63
TABLE 4 Label Ranges on SecCompany Printers at Various Locations 94
TABLE 5 Classifications Planner for SecCompany 95
TABLE 6 Compartments and User Accreditation Range Combinations Planner for SecCompany 95
TABLE 7 Compartment Bits Planner for SecCompany 96
TABLE 8 Clearance Planner for SecCompany 96
TABLE 9 Printer Banners Planner for SecCompany 98
TABLE 10 Channels Planner for SecCompany 98
TABLE 11 Color Names Planner for SecCompany 99

Using This Documentation

- **Overview** – Describes how labels are used and are displayed in the Trusted Extensions feature of Oracle Solaris and how to plan labels in your organization. Also describes which parts of the *Compartmented Mode Workstation Labeling: Encodings Format* guide do not apply to the Trusted Extensions implementation.
- **Audience** – System administrators, security administrators, and developers of labeled applications.
- **Required knowledge** – Administratively assigned labels and site security requirements.

Product Documentation Library

Documentation and resources for this product and related products are available at `http://www.oracle.com/pls/topic/lookup?ctx=E53394`.

Feedback

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

♦ ♦ ♦ CHAPTER 1

About Labels in Trusted Extensions

This chapter prepares the security administrator to create the file that encodes labels for the Trusted Extensions feature of Oracle Solaris. This chapter assumes that you have read the following material:

- Chapter 9, "Common Tasks in Trusted Extensions" in *Trusted Extensions Configuration and Administration* guide, which prepares the security administrator to assume the Security Administrator role
- "Labels in Trusted Extensions Software" in *Trusted Extensions Configuration and Administration*

This chapter covers the following topics:

- "Labels and Security Policy" on page 15
- "Types of Labels, Their Components and Uses" on page 16

Labels and Security Policy

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

All systems that are configured with Trusted Extensions have labels. Labels are specified in a `label_encodings` file. For a description of the file, see the `label_encodings(4)` man page. For descriptions of the encodings files that Trusted Extensions provides, see "Sources for Encodings Files" on page 37.

Trusted Extensions installs a default version of the `label_encodings` file. The default version supplies several commercial labels. This version can sometimes be used in non-production environments for learning purposes. A site might also customize one of the `label_encodings` files that Trusted Extensions provides. For an example of a site-specific file, see Appendix A, "Customized Encodings File for SecCompany".

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

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

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

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

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

Types of Labels, Their Components and Uses

Trusted Extensions defines two types of labels:

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

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

Some objects have a label range. These objects can be accessed at a particular label within the defined label range. A label range from `ADMIN_LOW` to `ADMIN_HIGH` allows access at all labels.

The security administrator can narrow that label range. Objects with label ranges include the following:

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

The various procedures for setting labels on these objects is described in *Trusted Extensions Configuration and Administration*. "Device Manager GUI" in *Trusted Extensions Configuration and Administration* describes how to set label ranges on devices.

Label Ranges Restrict Access

Label ranges set limits on the following:

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

Labels are automatically assigned to email messages. Emails are only visible in an email reader at the label of the message. The label of an email is printed when the email is printed.

Labels Are Used in Access Control Decisions

Labels are used to implement and control access on a system. Labels implement mandatory access control (MAC). With Trusted Extensions, both discretionary access control (DAC) checks and MAC checks must pass before access is allowed to an object. As in Oracle Solaris, DAC is based on permission bits and access control lists (ACLs). For more information, see Chapter 1, "Controlling Access to Files" in *Securing Files and Verifying File Integrity in Oracle Solaris 11.3*.

MAC compares the label of a process that is running an application with the label or the label range of any object that the process tries to access. The labels implement the set of rules that

enforce policy. One rule is *read down-read equal*. This rule applies when a process tries to access an object. The label of the process has to be greater than or equal to the label of the object, as in:

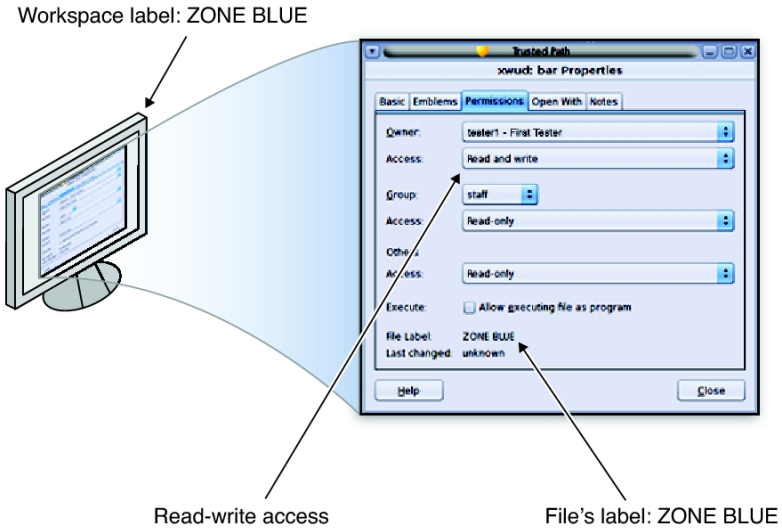
```
Label[Process] >= Label[Object]
```

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

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

The following figure shows a system that uses labels to make an access control decision.

FIGURE 1 Comparing the Label of a Text Editor With the Label Property in the File Browser



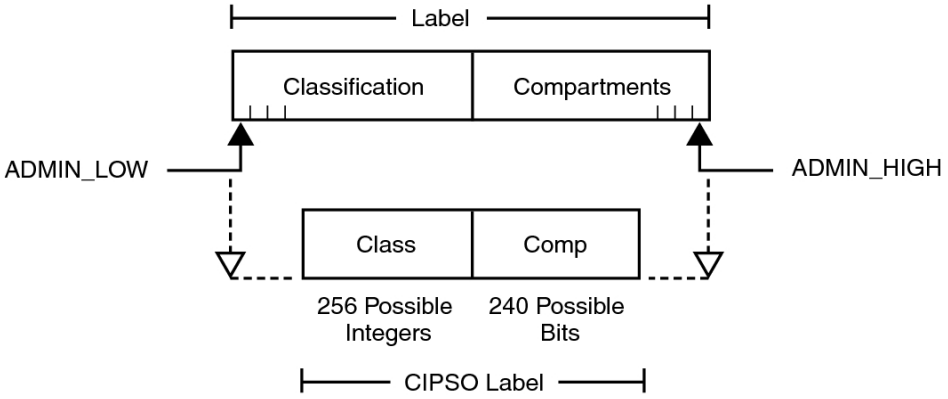
In the preceding figure, a user opens a text editor in a workspace with the label `ZONE BLUE`. The system sets the label of the process that is running the text editor to be equal to the label of the current workspace. Therefore, the text editor displays a label of `ZONE BLUE`. When the text editor attempts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

Label Components

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

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

FIGURE 2 CIPSO Label Definition



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

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

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

```
CLASSIFICATIONS:

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

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

When initial compartments are part of the classification definition, then compartments are part of that label. In the following excerpt, `name` indicates a compartment that can be used with the `TS` classification.

```
WORDS:

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

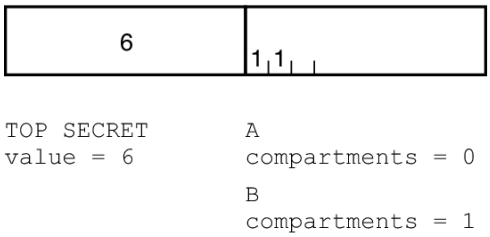
Possible labels from the preceding classifications and compartments include `TS`, `TS A`, `TS B`, and `TS AB`. A file with the `TS A` label would be available only to users who have the `TS` classification and the `A` compartment in their clearances. For an illustration, see Figure 3, "Representation of the TS, TS A, TS B, and TS AB Labels," on page 20.

Label Dominance

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

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

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



Another kind of dominance, *strict dominance*, is sometimes required for access. One label *strictly dominates* another label when the first label has a security level that is greater than the security level of the other label. Strict dominance is dominance without equality. The classification of the first label is higher than the classification of the second label. The first label contains all the compartments in the second label. Or, if the classifications of both labels are the same, the first label contains all the compartments in the second label, in addition to one or more additional compartments.

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

Accreditation Ranges, Label Ranges, and Valid Labels

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

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

- A *minimum clearance* and a *minimum sensitivity label* must be specified.

  These system-wide minimum labels establish the lowest clearance and the lowest label that any regular user can have.
- *Initial compartments* (compartment bits) can be assigned to a classification.

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

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

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

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

System Accreditation Range

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

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

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

FIGURE 4 How System Accreditation Range Is Constrained by Rules

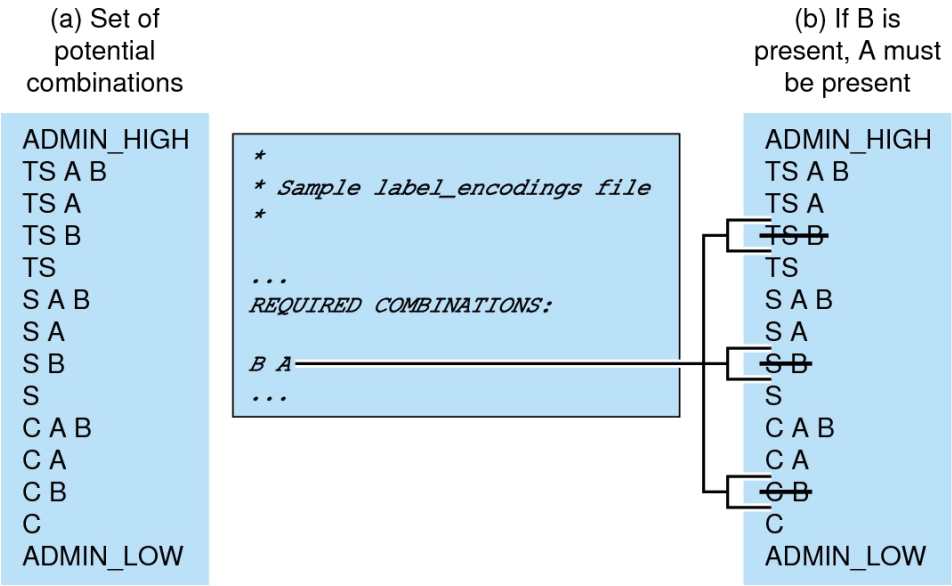


Figure 4, “How System Accreditation Range Is Constrained by Rules,” on page 22 (a) shows all potential combinations given the classifications, `TS` (`TOP SECRET`), `S` (`SECRET`), and `C` (`CONFIDENTIAL`), and the compartments, `A` and `B`.

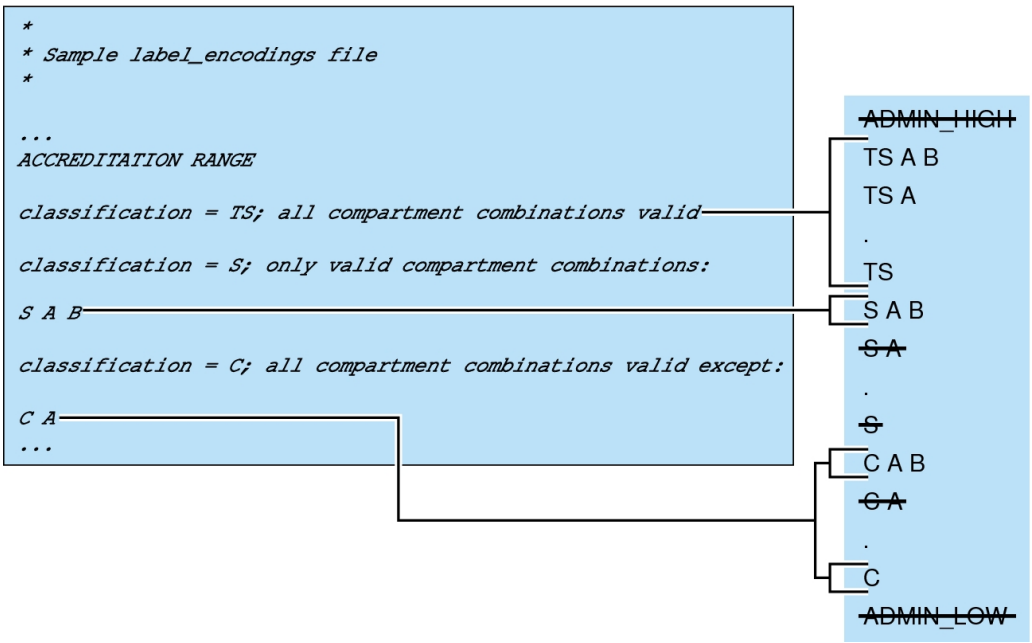
Figure 4, “How System Accreditation Range Is Constrained by Rules,” on page 22 (b) shows a typical rule from the `REQUIRED COMBINATIONS` subsection of the `SENSITIVITY LABELS`

section and its effects. The lines bracket the labels that are disqualified by the rule. Disqualified labels 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`. The converse is not true. Compartment A is not required to be combined with any other compartments. Because compartment `B` is only permitted when `A` is also present, the labels `TS B`, `S B`, and `C B` are not well-formed. Labels that are not well-formed are not in the system accreditation range.

User Accreditation Range

The *user accreditation range* is the largest set of labels that regular users can access when using Trusted Extensions. The user accreditation range always excludes `ADMIN_HIGH` and `ADMIN_LOW`. The user accreditation range is further constrained by any rules that constrain the "System Accreditation Range" on page 22. In addition, the user accreditation range can be constrained by a set of rules in the `ACCREDITATION RANGE` section of the `label_encodings` file. Figure 5, "`ACCREDITATION RANGE` Section of `label_encodings` File," on page 24 continues the Figure 4, "How System Accreditation Range Is Constrained by Rules," on page 22 example. Figure 5, "`ACCREDITATION RANGE` Section of `label_encodings` File," on page 24 shows three different types of rules in the `ACCREDITATION RANGE` section and their effects on the user accreditation range. The lines bracket to the well-formed labels that the particular rule permits.

FIGURE 5 `ACCREDITATION RANGE` Section of `label_encodings` File



As shown in the box to the right, the user accreditation range excludes `ADMIN_HIGH` and `ADMIN_LOW`. The rule for the `TS` classification (shown in Figure 4, "How System Accreditation Range Is Constrained by Rules," on page 22) includes all `TS` combinations except `TS B`. However, because `TS B`, and `S B` and `C B`, were previously overruled by the `REQUIRED COMBINATIONS` rule `B A` (as shown in Figure 4, "How System Accreditation Range Is Constrained by Rules," on page 22), `TS A B`, `TS A`, and `TS` are the only allowed `TS` combinations. As shown in Figure 5, "`ACCREDITATION RANGE` Section of `label_encodings` File," on page 24, because `S A B` is defined as the only valid combination for the `S` classification, `S B` is excluded again. All `C` combinations except `C A` are valid, according the rule for the `C` classification. However, because `C B` was overruled earlier, the only permitted combinations for the `C` classification are `C A B` and `C`.

Account Label Range

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

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

- The user clearance defines the upper bound of the account label range.

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

  The minimum sensitivity label in the `label_encodings` file defines an absolute minimum on labels at which any user can work.

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

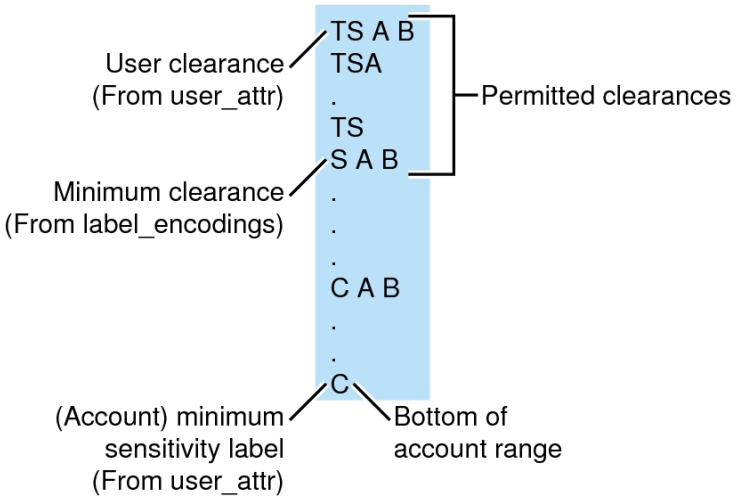
Consider a `label_encodings` file that prohibits the combination of compartments `A`, `B`, and `C` in a label. The valid clearance in this `label_encodings` file is not a valid label for a user.

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

Account Label Range Examples

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

FIGURE 6 Constraints on Account Label Ranges



In this example, `TS A B` is the highest label in the system accreditation range. This label contains the only two compartments, `A` and `B`, that are permitted to appear together in a label with any classification. `TS A B` is the clearance assigned to the account.

`C` is the user's minimum label. The definitions in the account label range constrain the user to work at labels `TS A B`, `TS A`, `TS`, `S A B`, `C A B`, or `C`.

The permitted clearances are `TS A B`, `TS A`, `TS` and `S A B`. A minimum clearance of `S A B` is set in the `label_encodings` file.

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

Table 1, “Accreditation Range and Account Label Range Examples,” on page 27 provides a more complex example. The example illustrates the differences between the possible label combinations, the system accreditation range, the user accreditation range, and some example account label ranges.

TABLE 1 Accreditation Range and Account Label Range Examples

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

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

Session Range

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

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

The session range of a single-label account is the label of the account. Choosing from a range of labels is possible only when a user account is configured to use multiple labels. User with accounts that are configured to use multiple labels can choose different labels during

the session. To specify a label, see "How to Change the Label of a Workspace" in *Trusted Extensions User's Guide*.

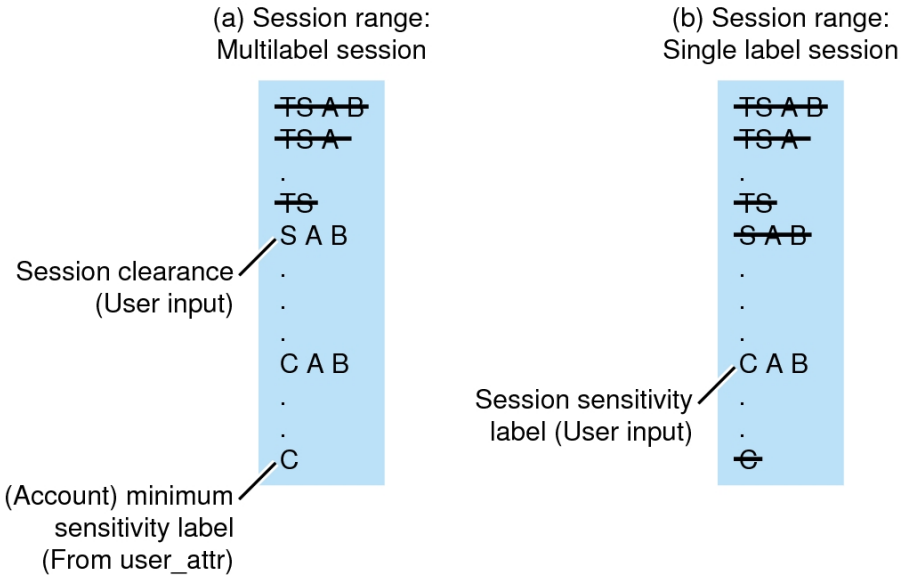
The single label or session clearance that is chosen at login is in effect throughout the session until logout. During a multilabel session, the user can work at any valid label that is dominated by the session clearance and that dominates the user's minimum label.

Figure 7, "Comparison of Session Ranges," on page 28 continues the Figure 6, "Constraints on Account Label Ranges," on page 26 example. As shown in Figure 6, "Constraints on Account Label Ranges," on page 26, the user can specify a session clearance that uses any well-formed label between `TS A B` and `S A B`.

Figure 7, "Comparison of Session Ranges," on page 28 (a) shows the labels that are available if the user selects a multilabel session with a session clearance of `S A B`. Because the other intermediate labels between `S A B` and `C` are not well-formed, the user can only work at `S A B`, `C A B`, or `C`.

Figure 7, "Comparison of Session Ranges," on page 28 (b) shows the labels that are available if the user selects a single-label session with a session label of `C A B`. Note that `C A B` is below the minimum clearance. However, `C A B` is accessible because the user is selecting a session label, not a clearance. Because the session is single-label, the user can work at only one label. In this example, the user specified `C A B`, although `S A B` or `C` could have been chosen instead.

FIGURE 7 Comparison of Session Ranges



Label Availability in Trusted Extensions Sessions

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

FIGURE 8 Cumulative Effect of Constraints on a Session Range

(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
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 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 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 B	.	.
C	C	C	C	C
ADMIN_LOW	ADMIN_LOW	~~ADMIN_LOW~~	.	.

The following set of examples show session label limitations and availability based on users' session choices. These examples continue the example from Figure 8, “Cumulative Effect of Constraints on a Session Range,” on page 29.

EXAMPLE 2 Effect of Using Default Label in Multilevel Session

At initial login, the user is assigned the lowest label in the user's account. If the lowest label is `CONFIDENTIAL`, the user user's first workspace is labeled `CONFIDENTIAL`. The user can then open workspaces at `CONFIDENTIAL A B` and `SECRET A B`, the session clearance.

EXAMPLE 3 Effect on Multilevel Session of User Choosing Higher Label at Initial Login

If the user chooses a higher label at initial login, such as `CONFIDENTIAL A B`, the user's first workspace is labeled `CONFIDENTIAL A B`. The user can open a higher-labeled workspace `SECRET A B`, but cannot open a `CONFIDENTIAL` workspace during that session.

EXAMPLE 4 Label Availability in Single-Level Session

At initial login, the user must choose a label. The available labels are within the user's label range up to the session clearance. If the clearance is `SECRET A B`, the labels that are available for the user to choose are `CONFIDENTIAL`, `CONFIDENTIAL A B`, `SECRET A B`. After choosing a label like `SECRET A B`, the user's first workspace is labeled `SECRET A B`. Because the session is single-level, the only available workspace label is `SECRET A B`.

Labeled Workspaces

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

If the user selects a range of labels for the session, the first workspace that appears is at the user's *minimum label*. By default, desktop panels exist for three other workspaces. By entering a workspace and selecting a label, all windows created in that workspace run processes at the selected label.

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

Label Administration

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

Label Visibility

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

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

Labels on Printed Output

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

Authorizations for Relabeling Information

The authorization to upgrade information to a label that dominates the label of the current information is called the `Upgrade File Label` authorization. The authorization that is used to downgrade information to a label that is lower than the label of the current information is called the `Downgrade File Label` authorization. For definitions of these authorizations, use the `getent auth_attr` command.

Privileges for Translating Labels

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

CHAPTER 2

Planning Labels in Trusted Extensions

This chapter covers the following topics:

- "Planning Labels in Trusted Extensions" on page 33
- "Sources for Encodings Files" on page 37

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

Planning Labels in Trusted Extensions

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

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

Task	Description	For Instructions
Study and outline your `label_encodings` file.	Make a `label_encodings` file that enforces your site security policy.	"How to Plan for Labels" on page 33
Build an extensible `label_encodings` file.	Create a file that can be modified without affecting existing label definitions.	"How to Plan the Encodings File" on page 34

▼ How to Plan for Labels

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

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

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

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

   - For more information about setting up site security policy, see Appendix A, "Site Security Policy," in *Trusted Extensions Configuration and Administration*.
   - For an example of planning a customized `label_encodings` file that is based on company requirements, see Chapter 6, "Example of Planning an Organization's Encodings File".

3. **Study the U. S. government's `label_encodings` file.**

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

4. **Determine your site's entries in the `LOCAL DEFINITIONS` section of the file.**

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

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

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

How to Plan the Encodings File

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

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

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

   For ideas, see "Sources for Encodings Files" on page 37. For the procedure, see "Managing a Label Encodings File" on page 50.

2. **Leave gaps in the `label_encodings` file to add items.**

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

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

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

Leave gaps in compartment bit numbers for possible later additions.

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

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

3. **Determine classifications for the site.**

As described in Figure 2, "CIPSO Label Definition," on page 19, the total number of classification values that you can use is 254. Do not use classification 0.

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

The same classification value cannot be assigned to different names. Each classification must be higher or lower, or disjoint, from any other classification. Every classification must be distinct.

A table can be used to plan classifications. For a completed example, see Table 5, "Classifications Planner for SecCompany," on page 95.

4. **Determine the compartments for the site.**

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

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

5. **Name the classifications and compartments.**

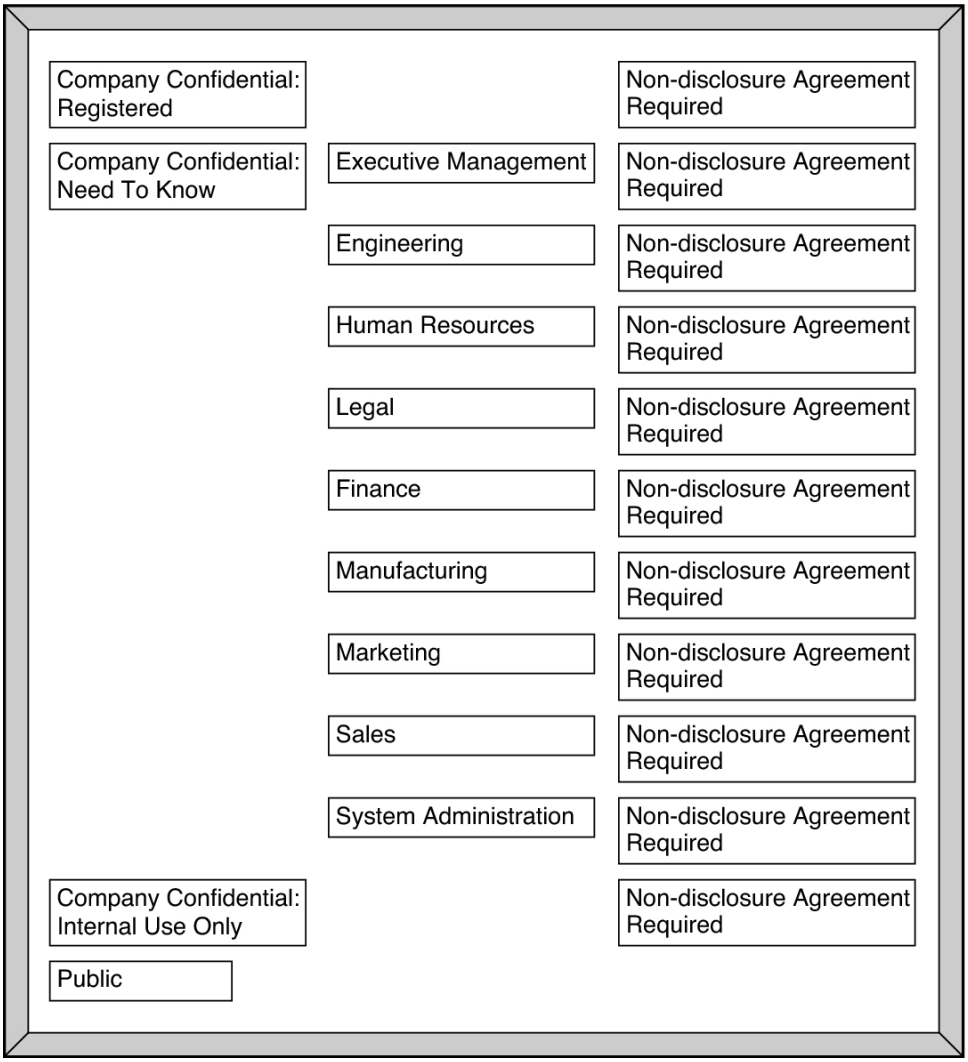
`CLASSIFICATIONS` and `WORDS` (for compartments) in the `label_encodings` file have two forms: a mandatory long name and an optional short name. Short names can be used interchangeably with long names when labels are being specified.

6. **Arrange the relationships among the classifications and among the compartments.**

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

To make this step easier, use a large board and pieces of paper that represent your classifications and compartments, as illustrated here. With this method, you can visualize the relationships and rearrange the pieces until they all fit together.

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



7. **Arrange the labels in order of increasing sensitivity.**

8. **Decide which clearances to assign to which users.**

You can use a table to plan clearances. For a completed example, see Table 8, "Clearance Planner for SecCompany," on page 96.

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

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

   A table can be used to track compartment bit assignments. For a completed example, see Table 7, "Compartment Bits Planner for SecCompany," on page 96.

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

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

11. **Decide which colors to associate with which labels.**

    For suggestions and examples, see "Specifying Colors for Labels" on page 74.

12. **Analyze the label relationships.**

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

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

Sources for Encodings Files

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

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

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

Encodings Files From Trusted Extensions

Oracle Solaris provides the following sample `label_encodings` files in the `/etc/security/tsol` directory. These samples can be modified to meet your site requirements.

`label_encodings`	Is installed by Trusted Extensions software as the default. This file uses commercial labels, such as Confidential: Need to Know.
`label_encodings.example`	Is similar to the example in Appendix A, "Customized Encodings File for SecCompany". The introduction to the appendix describes the label components in the file. Chapter 6, "Example of Planning an Organization's Encodings File" describes each step for creating this file.
`label_encodings.gfi.single`	Is the U.S. government single-level file.
`label_encodings.single`	Is Oracle Solaris's version of the U.S. government single-level file. The color assignments are different.
`label_encodings.gfi.multi`	Is the U.S. government multilevel file.
`label_encodings.multi` file	Is Oracle Solaris's version of the U.S. government multilevel file. The combinations are less restricted, the minimum clearance is higher, the default user label is lower, and the colors are different.

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

Default `label_encodings` File

By default, the `/etc/security/tsol/label_encodings` is installed with the following contents:

```
ACCREDITATION RANGE:
classification= PUB; all compartment combinations valid;

classification= SBX; all compartment combinations valid;

classification= CNF; all compartment combinations valid except:
CNF
```

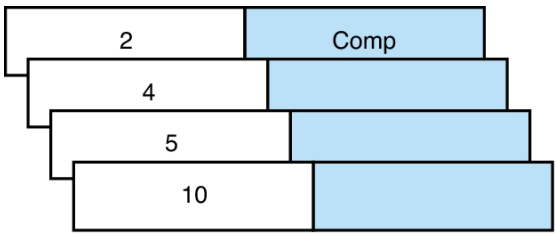
```
minimum clearance= PUB;
minimum sensitivity label= PUB;
minimum protect as classification= PUB;
```

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

- `PUBLIC` is defined as the lowest classification.
- `CONFIDENTIAL` is defined as a higher classification.
- `SANDBOX` is defined as the highest classification.
- `PUBLIC` is defined as the minimum clearance.
- `PUBLIC` is defined as the minimum sensitivity label.
- `PUBLIC` is defined as the minimum "Protect As" classification.

The Classifications section of the default file is illustrated in the following figure.

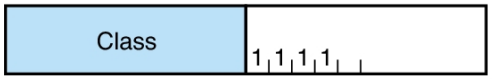
FIGURE 9 Classifications in the Default `label_encodings` File




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

The Compartments section of the file is illustrated in the following figure.

FIGURE 10 Compartments in the Default `label_encodings` File




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

Differences Between Simplified GFI Label Encodings Files

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

Oracle Solaris also provides two simplified versions of these files, `label_encodings.single` and `label_encodings.multi`. The differences are described in the following sections.

Simplified GFI Multilevel Label Encodings File

The `ACCREDITATION RANGE` settings in the `label_encodings.multi` follow:

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

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

The `ACCREDITATION RANGE` definition enables the site to use all the classifications and compartments that are defined in the `label_encodings.multi` file, as follows:

- `UNCLASSIFIED`, `CLASSIFIED`, `SECRET`, and `TOP SECRET` are defined with all compartment combinations valid.

- CLASSIFIED is defined as the minimum clearance.
- UNCLASSIFIED is defined as the minimum sensitivity label.
- UNCLASSIFIED is defined as the minimum protect as classification.

Simplified GFI Single-Level Label Encodings File

The ACCREDITATION RANGE settings in the label_encodings.single file follow:

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

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

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

Oracle Solaris Extensions to label_encodings File

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

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

♦ ♦ ♦ CHAPTER 3

Creating a Label Encodings File

This chapter describes how to create, modify, analyze, and verify a `label_encodings` file. This chapter covers the following topics:

- "Encodings File Syntax" on page 43
- "Managing a Label Encodings File" on page 50

Encodings File Syntax

The `label_encodings` file contains a `VERSION` specification and seven mandatory sections:

- `CLASSIFICATIONS`
- `INFORMATION LABELS`
- `SENSITIVITY LABELS`
- `CLEARANCES`
- `CHANNELS`
- `PRINTER BANNERS`
- `ACCREDITATION RANGE`

The sections must appear in that order. An optional `LOCAL DEFINITIONS` section can follow.

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

TABLE 2 `label_encodings` Keywords

Section	Notes
`VERSION=`	Mandatory keyword. The version specification is the single keyword `VERSION=`, followed by a character string that identifies this particular version of encodings.
`CLASSIFICATIONS:`	Mandatory keyword. At least one classification must be defined.
`INFORMATION LABELS:`	Mandatory keywords. Even though information labels are not used in Trusted Extensions software, you must assign one bit to an information

Section	Notes

`WORDS:`
 	
`REQUIRED COMBINATIONS:`
 	
`COMBINATION CONSTRAINTS:`
	label word for each bit that you assign to a sensitivity label word. The sensitivity label words are defined in the following section.

`SENSITIVITY LABELS:`
 	
`WORDS:`
 	
`REQUIRED COMBINATIONS:`
 	
`COMBINATION CONSTRAINTS`
	Mandatory keywords, although the `WORDS` definitions are optional. If you define sensitivity label words, the same bits must be assigned to `WORDS` in both the `INFORMATION LABELS` and `CLEARANCES` sections. The words that are assigned to the bits do not need to be the same.

`CLEARANCES:`
 	
`WORDS:`
 	
`REQUIRED COMBINATIONS:`
 	
`COMBINATION CONSTRAINTS`
	Mandatory keywords. One bit must be assigned to a clearance word for any sensitivity label word that you have defined. Clearance labels can allow combinations of words that have been disallowed in the definitions for sensitivity label words.

`CHANNELS:`	Mandatory keyword.
`PRINTER BANNERS:`	Mandatory keyword.
`ACCREDITATION RANGE:`	Mandatory keyword. A rule must be defined for each classification name. The minimum clearance, minimum sensitivity label, and minimum "Protect As" classification must be defined.
`LOCAL DEFINITIONS:`	Optional keyword.

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

Word Order Requirements

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

For the effect of word order, see "Specifying Channels" on page 65. Detailed information is provided in *Compartmented Mode Workstation Labeling: Encodings Format*: Defense Intelligence Agency document [DDS-2600-6216-93].

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

Clearance labels can allow combinations of words that have been disallowed in the definitions for sensitivity label words.

Classification Name Syntax

The classification is the hierarchical portion of a label. Each label has one and only one classification. A site can define up to 255 classifications. An integer value from 1 to 255 can be assigned to a classification in the `label_encodings` file. The value `0` is reserved for the `ADMIN_LOW` administrative label. The value `32,767` is reserved for the `ADMIN_HIGH` administrative label. For an illustration of a CIPSO label, see Figure 2, "CIPSO Label Definition," on page 19.

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

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

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

Keywords for Classifications

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

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

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

`aname=`	Optional. The alternative name that can be specified by users when a classification is needed.
`value=`	Mandatory. The values that you assign to represent the hierarchy among the classifications. Leave gaps for later expansion. `0` is reserved for `ADMIN_LOW`. Values can start at `1` and go to `255`.
`initial compartments=`	Optional. Specify bit numbers for any default compartment words. Default compartment words initially appear in any label that has the associated classification. Advanced: Specify bit numbers for any inverse words. The minimum classification must not have initial compartments. For a description of inverse words, see "Default and Inverse Words" on page 47.
`initial markings=`	Obsolete. Do not define.

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

EXAMPLE 5 Classifications With Initial Compartments in `label_encodings.multi` File

```
VERSION= Trusted Extensions Multi-Label GFI Distributed Demo Version

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

CLASSIFICATIONS:

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

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

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

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

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

EXAMPLE 6 Classifications With No Initial Compartments in `label_encodings.example` File

```
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;
```

Default and Inverse Words

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

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

EXAMPLE 7 Assigning Initial Compartments

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

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

The following shows how these initial compartment bits can be assigned to words by defining default and inverse words under `SENSITIVITY LABELS`.

```
SENSITIVITY LABELS:

WORDS:

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

In the preceding `WORDS` example, compartment bits `4` and `5` are assigned to the word `DIVISION ONLY`. Each compartment bit is also associated with an inverse word. The sensitivity label name `WEBC AMERICA` is assigned to the inverse compartment bit `~4`. The sensitivity label name `WEBC`

WORLD is assigned to the inverse compartment bit ~5. These assignments have the following results:

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

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

Compartment Words

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

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

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

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

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

```
WORDS:

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

Along with its classification field, each label has a 256–bit compartment field, of which 239 are available for CIPSO labels. Each bit is assignable in zero or more compartment words. Each word can have one or more compartment bits assigned. Out of the 239 available bits, many compartment words can be created. For an example, see the compartments planner in Table 6, “Compartments and User Accreditation Range Combinations Planner for SecCompany,” on page 95.

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

- only valid compartment combinations;

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

Hierarchical Compartment Words

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

EXAMPLE 8 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 more general compartment word must be defined below the word that is more specific. For example, by defining a word that uses bit number `1` and another word that uses bits number `1` and `2`, you give the two words a hierarchical relationship.

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

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

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

The assignments and effects are as follows:

- The security administrator assigns the `WebCo Direct_Sales` clearance to employees in the direct sales department. The `WebCo Indirect_Sales` clearance is assigned to employees in the indirect sales department.
- Documents that are created by an employee who is working at the `WebCo Direct_Sales` label are labeled with the label that is only accessible to employees in the direct sales department.
- Anyone in the indirect or direct sales departments can work at the `WebCo Sales` label because the compartment word `Sales` is below both the `Direct_Sales` and `Indirect_Sales` words. Creating documents at the `WebCo Sales` label makes the documents available to everyone in the sales department.

EXAMPLE 9 Using `REQUIRED COMBINATIONS` to Establish Hierarchies

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

In this example, the definitions of the `Direct_Sales`, `Indirect_Sales`, and `Sales` compartments serve essentially the same purpose as in Example 8, "Using Bit Combinations to Establish Hierarchies," on page 49. The difference is that the `Direct_Sales` word will always have the `Sales` word with it.

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

REQUIRED COMBINATIONS:

Direct_Sales            Sales
Indirect_Sales          Sales
```

Managing a Label Encodings File

Caution - The safest time to modify a `label_encodings` file is before a regular user logs in. Proceed with caution when modifying a file that is in use. For details, see the `label_encodings(4)` man page.

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

Task	For Instructions
Create or modify the `label_encodings` file.	"How to Create a `label_encodings` File" on page 51
Test the `label_encodings` file.	"How to Analyze and Verify the `label_encodings` File" on page 51
Distribute the `label_encodings` file.	"How to Distribute the `label_encodings` File" on page 52
Debug a `label_encodings` file.	"How to Debug a `label_encodings` File" on page 58
Change a classification definition.	"How to Add or Rename a Classification" on page 52
Create default or inverse words.	"How to Specify Default and Inverse Words" on page 54
Customize a single-label file.	"How to Create a Single-Label Encodings File" on page 55
Specify a label name.	Example 11, "Changing the Single Label Name," on page 57
Add a `LOCAL DEFINITIONS` section.	"Modifying Extensions From Oracle Solaris to the `label_encodings` File" on page 77

How to Create a label_encodings File

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

You can create a label_encodings file before you install Trusted Extensions on your first system. On that first system, you check the file. You can also create this file on the first system that you install with Trusted Extensions. The label_encodings file must be accurate and tested before a second system is configured with Trusted Extensions.

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

1. **Create a backup copy of the original label encodings file.**

   # cp *encodings-filename encodings-filename.orig*

2. **In an editor, open the label encodings file.**

3. **Modify the label encodings file.**

   For details, see "How to Plan the Encodings File" on page 34.

4. **Save your changes.**

Next Steps Continue with "How to Analyze and Verify the label_encodings File" on page 51.

How to Analyze and Verify the label_encodings File

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

1. **Check the label definitions and the relationships of the labels.**

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

   $ /usr/sbin/chk_encodings -a *encodings-file*

   If the file does not pass, see "How to Debug a label_encodings File" on page 58 for assistance. Do not continue to the next step until the file represents your label relationships correctly.

2. **Verify the syntax of the file.**

a. **Run the `chk_encodings` command.**

```
# /usr/sbin/chk_encodings encodings-file
```

b. **Resolve errors.**

If the command reports errors, the errors *must* be resolved before continuing.

3. **Make the file the active `label_encodings` file.**

```
# cp /full-pathname-of-label-encodings-file \
/etc/security/tsol/label.encodings.site
# cd /etc/security/tsol
# cp label_encodings label_encodings.tx.orig
# cp label.encodings.site label_encodings
```

4. **Test the encodings file.**

Where possible, test the file on a few systems before approving the file for all systems at your site. For example, install one labeled system as a file server and another labeled system as a user's system. Communicate between the two at all labels. Transfer files at all labels, and so on.

Next Steps When the file is ready to be installed on the network, see "How to Distribute the `label_encodings` File" on page 52.

How to Distribute the `label_encodings` File

1. **Create a master copy of the `label_encodings` file.**

For copying instructions, see "How to Copy Files to Portable Media in Trusted Extensions" in *Trusted Extensions Configuration and Administration*.

Note - Store the master copy on labeled media in a protected location.

---

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

For copying instructions, see "How to Copy Files From Portable Media in Trusted Extensions" in *Trusted Extensions Configuration and Administration*.

How to Add or Rename a Classification

Before You Begin You must be in the Security Administrator role in the global zone. To be able to add classifications, you left gaps in the classification numbers in the `label_encodings` file.

1. **Back up the `label_encodings` file.**

```
# cp label_encodings label_encodings.orig
```

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

```
# pfedit encodings-file
```

3. **Update the version number.**

In the `VERSION=` section update the version number and the date.

```
VERSION= Trusted Extensions Example Version - 5.11 09/05/28
```

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

```
VERSION= MyCo Example Version - %I% %E%
```

4. **Add or rename the classification by performing one of the following:**

- **In the `CLASSIFICATIONS` section, add the new classification.**

  Specify a long name, short name, and numeric value.

```
name= REGISTERED; sname= R; value= 15;
```

- **In the `CLASSIFICATIONS` section, rename an existing classification.**

```
* name= INTERNAL_USE_ONLY; sname= IUO; value= 12;
name= INTERNAL; sname= I; value= 12;
```

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

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

Note - If you rename a classification, update the name in the `ACCREDITATION RANGE` section.

```
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;
```

6. **Adjust the `ACCREDITATION RANGE` section, if necessary.**

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

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

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

Next Steps Verify the file by performing "How to Analyze and Verify the `label_encodings` File" on page 51.

Distribute the file by following "How to Distribute the `label_encodings` File" on page 52.

▼ How to Specify Default and Inverse Words

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

1. **Back up the `label_encodings` file.**

```
# cp label_encodings label_encodings.orig
```

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

```
# pfedit encodings-file
```

3. **Specify initial compartments.**

   In the `CLASSIFICATIONS` section, specify the initial compartments as part of the classification definition. For example, in the following `CLASSIFICATIONS` section, `WEB COMPANY` has two initial compartments, `4` and `5`:

```
CLASSIFICATIONS:
name= PUBLIC;  sname= P;  value= 1;
```

```
name= WEB COMPANY;  sname= WEBCO;  value= 2; initial compartments= 4-5 ;
```

4. **Specify a default word by assigning an initial compartment bit to the word.**

   In the following example, the initial compartment bits, 4 and 5, are assigned to three words:

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

5. **Specify an inverse word.**

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

   In the following example, the initial compartment bits, 4 and 5, are preceded by a tilde in the WEBC words:

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

6. **Save your changes.**

Next Steps Verify the file by performing "How to Analyze and Verify the label_encodings File" on page 51.

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

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

How to Create a Single-Label Encodings File

Certain labels must always be present in a label_encodings file:

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

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

1. **Open an existing encodings file or create a new one.**

   Provide a name that is different from the installed label_encodings file.

```
# pfedit label_encodings.myco.single
```

2. **Specify one classification and only the desired compartments.**

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

```
VERSION= MyCompany Single-Label Encodings - 1.01 10/10/11
. . .
CLASSIFICATIONS:

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

INFORMATION LABELS:

WORDS:

SENSITIVITY LABELS:

WORDS:

CLEARANCES:

WORDS:

CHANNELS:

WORDS:

PRINTER BANNERS:

WORDS:
```

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

   In the following example, the `INTERNAL` classification is encoded.

```
ACCREDITATION RANGE:

classification= INTERNAL;
only valid compartment combinations:

INTERNAL

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

4. **Add and modify the `LOCAL DEFINITIONS` section.**

For details, see "Modifying Extensions From Oracle Solaris to the `label_encodings` File" on page 77.

Example 10 Defining the Accreditation Range in a Single-Label Encodings File

The following example shows the settings in the `ACCREDITATION RANGE` section for a single-level label encodings file. A single `ANY_CLASS` classification is defined. Compartment words `A`, `B`, and `REL CNTRY 1` are specified for all types of labels.

```
ACCREDITATION RANGE:

classification= ANY_CLASS;      only valid compartment combinations:

ANY_CLASS A B REL CNTRY1

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

Example 11 Changing the Single Label Name

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

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

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

```
ACCREDITATION RANGE:

classification= INTERNAL;      only valid compartment combinations:

INTERNAL

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

Next Steps Verify the file by performing "How to Analyze and Verify the `label_encodings` File" on page 51.

Distribute the file by following "How to Distribute the `label_encodings` File" on page 52.

How to Debug a `label_encodings` File

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

1. **In an editor, check the entries in the `INFORMATION LABELS: WORDS:` section.**

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

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

   ---

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

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

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

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

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

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

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

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

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

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

CHAPTER 4

Labeling Printer Output

This chapter describes how Trusted Extensions labels and handling instructions are printed on printer output. This chapter also describes how the Security Administrator role can make changes to the default printer output. This chapter covers the following topics:

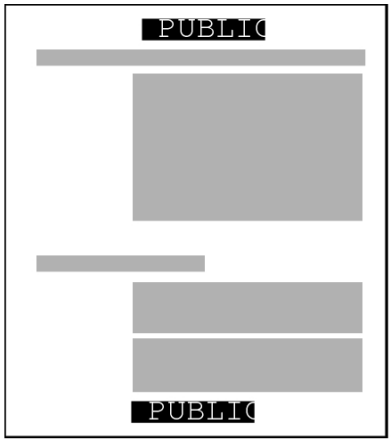
- "Labels on Body Pages" on page 59
- "Security Text on Banner and Trailer Pages" on page 60
- "Specifying the "Protect As" Classification" on page 62
- "Specifying Printer Banners" on page 63
- "Specifying Channels" on page 65
- "Configuring Security Text on Print Jobs" on page 70

Labels on Body Pages

When the printer is correctly configured with the `job-sheets=labeled` option, each print job's label is printed at the top and bottom of every body page. For the procedure, see "How to Configure a Multilevel Print Server and Its Printers" in *Trusted Extensions Configuration and Administration*.

Figure 11, "Label Automatically Printed on Body Pages," on page 60 shows the label `PUBLIC` printed at the top and bottom of a print job's body page.

FIGURE 11 Label Automatically Printed on Body Pages



The Security Administrator role can change the defaults so that a higher label is printed instead of the label of the print job. To print a higher label, see "Specifying Channels" on page 65. To remove labels from printed output, see "Reducing Printing Restrictions in Trusted Extensions" in *Trusted Extensions Configuration and Administration*.

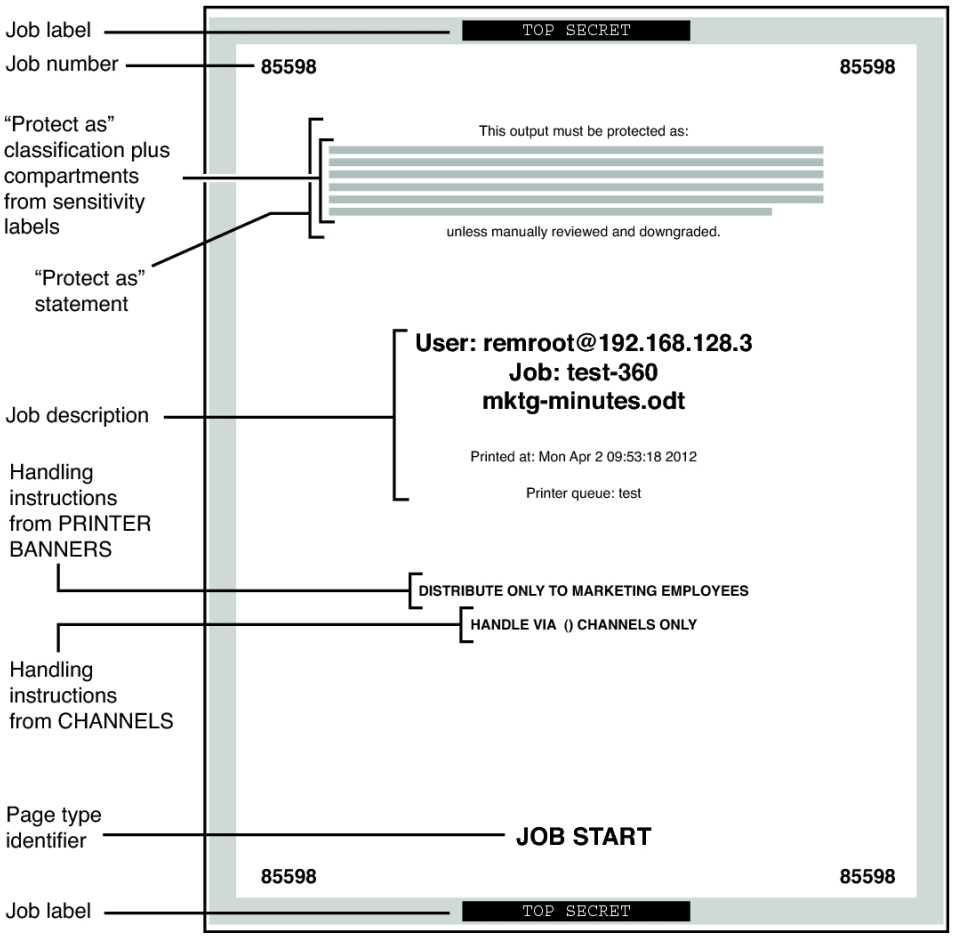
Security Text on Banner and Trailer Pages

When the printer is correctly configured with the `job-sheets=labeled` option, a *banner page* and a *trailer page* surround each print job. The banner and trailer pages contain label-related text and handling instructions for protecting printer output. For the printer configuration procedure, see "How to Configure a Multilevel Print Server and Its Printers" in *Trusted Extensions Configuration and Administration*.

The fields and the text that are printed on the banner page are shown in Figure 12, "Typical Banner Page of a Labeled Print Job," on page 61. The callouts show the names of the labels and the strings that appear by default.

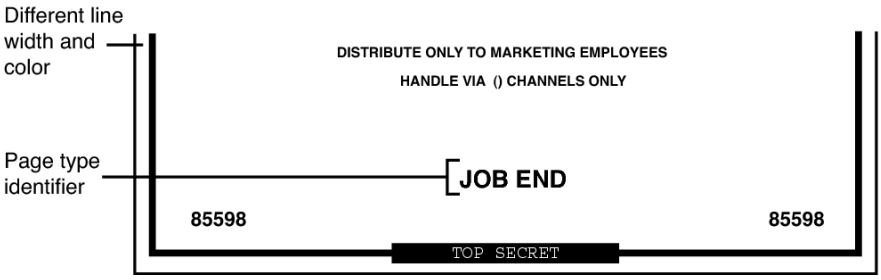
The text, labels, and warnings that appear on print jobs are configurable. The text can also be replaced with text in another language for localization.

FIGURE 12 Typical Banner Page of a Labeled Print Job



The differences on the trailer page are shown in the following figure. A thin black line is used as a frame on the trailer page, instead of the thick gray frame on the banner page. The page type identifier on a trailer page is JOB END.

FIGURE 13 Differences on a Trailer Page



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

- “Specifying the "Protect As" Classification” on page 62
- “Specifying Printer Banners” on page 63
- “Specifying Channels” on page 65

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

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

To customize the configuration file, see the comments in the `tsol_separator.ps` file in the `/usr/lib/cups/filter` directory. For further details, see Chapter 19, “Managing Labeled Printing” in *Trusted Extensions Configuration and Administration*.

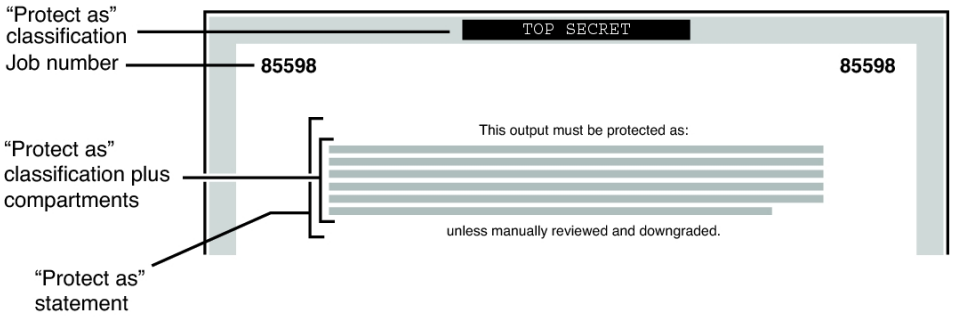
Specifying the "Protect As" Classification

The "Protect As" classification is printed in two places:

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

The following figure shows the "Protect as" statement on labeled print output.

FIGURE 14 "Protect As" Statement



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

TABLE 3 Effect of Minimum "Protect As" Classification on Printer Output

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

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

Specifying Printer Banners

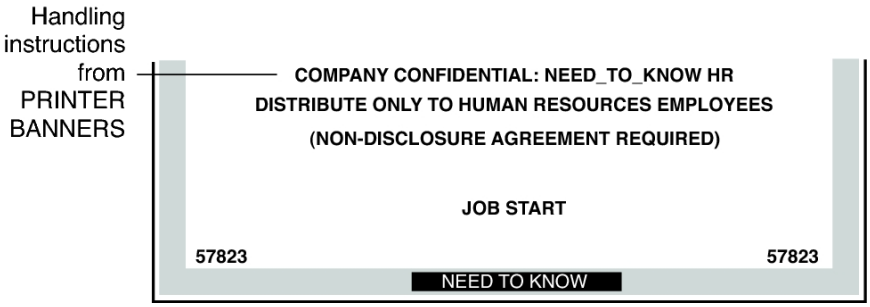
The `PRINTER BANNERS` section in the `label_encodings` file contains the first line or lines that can appear in the handling instructions in the lower third of the banner and trailer pages.

At commercial sites, the Security Administrator role can associate any text in the `PRINTER BANNERS` section with any compartment bit. The compartment bit must also be assigned to

a word in the `SENSITIVITY LABELS` section of the `label_encodings` file. In the following example, the printer banner is the line that reads `COMPANY CONFIDENTIAL: NEED_TO_KNOW HR`.

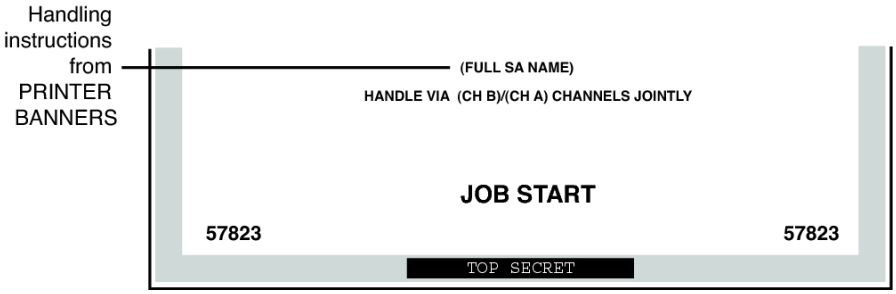
Compartments from the print job's label are printed in the "Protect As" field along with the print job's "Protect As" classification. In the following example, the compartment `HR` from the label is printed as an access-related word along with the "Protect As" classification because all compartments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

FIGURE 15 Commercial Use of `PRINTER BANNERS` Section on Banner Page



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

FIGURE 16 U.S. Government Use of `PRINTER BANNERS` Section on Banner Page



Following are the encodings for the printer banner line `(FULL SA NAME)` in Figure 16, “U.S. Government Use of `PRINTER BANNERS` Section on Banner Page,” on page 64.

```
PRINTER BANNERS:

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

Next are the SENSITIVITY LABELS definitions for the same compartments that are used in the PRINTER BANNERS definitions in Figure 16, "U.S. Government Use of PRINTER BANNERS Section on Banner Page," on page 64. Note that compartment bit 2 is associated with the subcompartment word SA:

```
SENSITIVITY LABELS:

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

The printer banner displays as (FULL SA NAME) for the following reasons:

- 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.

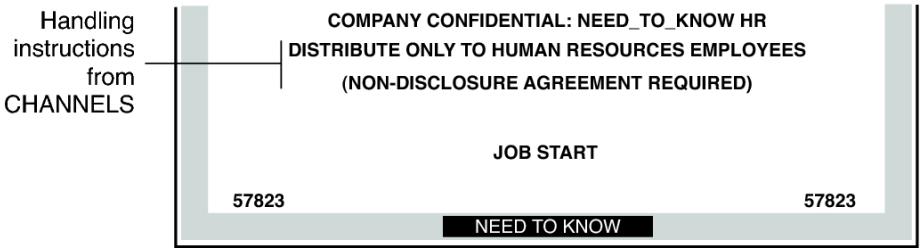
For a sample PRINTER BANNERS planner, see "Planning the Printer Banners in a Worksheet" on page 97.

Specifying Channels

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

Commercial sites can customize the text in the CHANNELS section with any compartment bit. The following figure shows a CHANNELS warning on a print job's banner page at a commercial site.

FIGURE 17 Commercial Use of `CHANNELS` Section on Banner Page



By convention in U.S. government installations, the channels lines of the banner page show the warnings that are associated with the *compartments* of the print job's label. Figure 18, "U.S. Government Use of `CHANNELS` Section on Banner Page," on page 67 shows a typical `CHANNELS` warning on a print job's banner page at a government installation: `HANDLE VIA (CH B)/(CH A) CHANNELS JOINTLY`.

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

The example illustrates these features:

- Two compartment bits are associated individually with one set of words and together with another set of words.
- A third compartment bit is included with the encodings for the first two bits.
- One suffix is defined for when *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 18 U.S. Government Use of `CHANNELS` Section on Banner Page

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

EXAMPLE 12 Suffixes and Prefixes in the `CHANNELS` Section in a U.S. Government `label_encodings` File

```
CHANNELS:

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

Next, the channel names `(CH A)`, `(CH B)`, and `(CH C)` are specified in two different ways to achieve the following results:

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

In the following example, the first three lines that define `CHANNELS` words in the preceding example are repeated.

This example focuses on how `(CH A)`, `(CH B)`, and `(CH C)` are encoded to appear with the `CHANNELS ONLY` suffix.

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

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

```
CHANNELS:

WORDS:

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

The first three lines of name definitions in the CHANNELS section have the following results:

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

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

EXAMPLE 13 Encodings for More Than One Channel in CHANNELS Section in a U.S. Government Encodings File

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

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

These CHANNELS definitions illustrate the importance of order when compartments are being encoded. The first three lines handle the cases when only one of the channels' compartment bits is turned on, so the last three lines can handle cases when more than one bit is turned on.

Therefore, none of the last three lines need to have any compartment bits explicitly set to `0`. The result of these last three lines is that the suffix `CHANNELS JOINTLY` is always printed when any of two or more of the three compartment words that are associated with the channels is in the label.

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

The following excerpt from the `label_encodings` file shows that compartment bit `6` is associated with the label word `CC`.

```
SENSITIVITY LABELS:


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

The next excerpt shows that compartment bit `1` is associated with the sensitivity label word `B`.

```
SENSITIVITY LABELS:

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

The next excerpt shows that compartment bit `0` is associated with sensitivity label word `A`.

```
SENSITIVITY LABELS:

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

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

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

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

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

Configuring Security Text on Print Jobs

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

Task	For Instructions
Print text on the banner page of a printout.	"How to Specify the Text in `PRINTER BANNERS`" on page 70
Print handling instructions.	"How to Specify Handling Instructions in `CHANNELS`" on page 71
Protect printouts at a higher label than the print job.	"How to Set a Minimum "Protect As" Classification" on page 72
Configure printers to label output.	"Configuring Labeled Printing" in *Trusted Extensions Configuration and Administration*

▼ How to Specify the Text in `PRINTER BANNERS`

In this procedure, you create the strings that appear at the top of the banner page and at the start of the handling instructions on the bottom of the page.

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

- For background information, see "Specifying Printer Banners" on page 63.
- For assistance, use "Planning the Printer Banners in a Worksheet" on page 97.

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

   `# pfedit` *encodings-file*

2. **Modify the `PRINTER BANNERS` section of the file.**

   a. **Create prefixes and suffixes.**

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

```
PRINTER BANNERS:

WORDS:

name= ORCON;                    prefix;
```

b. Specify the names of words to associate with any existing compartments in sensitivity labels.

You can associate compartments with particular prefixes and suffixes. Prefixes precede the compartment text and suffixes follow the compartment text on the printed output

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

Next Steps Continue with "How to Analyze and Verify the label_encodings File" on page 51.

How to Specify Handling Instructions in CHANNELS

In this procedure, you create the strings that state handling instructions on printer banner pages.

Before You Begin You must be in the Security Administrator role in the global zone. You have planned the prefixes and suffixes.

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

1. Edit the label_encodings file.

```
# pfedit encodings-file
```

2. Modify the CHANNELS section of the file.

a. Specify the prefixes and suffixes.

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

```
CHANNELS:

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

b. Specify the names of words to associate with existing compartments in sensitivity labels.

Use your defined prefixes and suffixes.

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

Next Steps Continue with "How to Analyze and Verify the `label_encodings` File" on page 51.

How to Set a Minimum "Protect As" Classification

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

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

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

   `# pfedit` *encodings-file*

2. **Specify a classification as the value for the `minimum protect as classification` entry.**

   This entry is defined in the `ACCREDITATION RANGE` section of the `label_encodings` file.

Example 14 Minimum "Protect As" Classification From a `label_encodings` File

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

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

Next Steps Continue with "How to Analyze and Verify the `label_encodings` File" on page 51.

CHAPTER 5

Customizing the LOCAL DEFINITIONS Section

This chapter describes how to customize the LOCAL DEFINITIONS section of the label_encodings file for Trusted Extensions. This chapter covers the following topics:

- "LOCAL DEFINITIONS Section" on page 73
- "Modifying Extensions From Oracle Solaris to the label_encodings File" on page 77

LOCAL DEFINITIONS Section

Oracle Solaris provides additional keywords that are not defined in the government-furnished *Compartmented Mode Workstation Labeling: Encodings Format* document. These Oracle Solaris keyword extensions are defined in the LOCAL DEFINITIONS section. The following is the LOCAL DEFINITIONS section from Trusted Extensions's default label_encodings file:

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

LOCAL DEFINITIONS:

Classification Name= Classification;
Compartments Name= Sensitivity;

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

COLOR NAMES:

label= Admin_Low;           color= #bdbdbd;

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

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

*

* End of local site definitions
*
```

Contents of LOCAL DEFINITIONS Section

The security administrator can do the following in the LOCAL DEFINITIONS section of the label_encodings file:

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

  For the procedure, see "How to Specify Default User Labels" on page 78.
- Specify which colors are assigned to labels.

Note - The ADMIN_LOW and ADMIN_HIGH labels must have color definitions. Color definitions for other labels are optional, but are highly recommended.

For more information, see "How to Assign a Color to a Label or Word" on page 79 and the label_encodings(4) man page.

Specifying Colors for Labels

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

```
COLOR NAMES:

label= Admin_Low;           color= #bdbdbd;

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

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

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

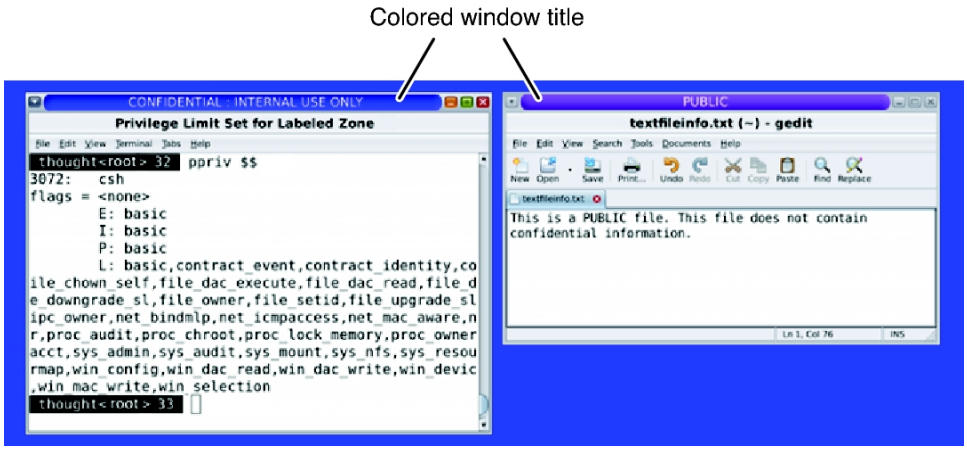
```
label= label-name;      color= color-name;
word= label-name;       color= color-name;
```

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

For an introduction to color values, see "Color Values" on page 76. A full discussion of how to specify color is outside the scope of this guide. For more information, see the `X11`(5) man page in the `/usr/X11/share/man/man5` or `/usr/share/man/man5` directory. Also, color specifications are covered in the *XWindows Systems User's Guide* (Vol. III), ISBN number 0-937175-29-3.

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

FIGURE 19 Window Labels With Colors From `COLOR NAMES`



Order of Color Specification

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

1. If a label contains a compartment word that has one or more colors specified, then the color value associated with the first `word=` value is used.

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

EXAMPLE 15 Colors Assigned According to Ordering Rules

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

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

The ordering rules result in the following color display:

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

EXAMPLE 16 Color Assigned to a Label With No Assigned Color

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

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

Color Values

The `/usr/share/X11/rgb.txt` database translates color names into red, green, and blue values. You can refer to the `rgb.txt` file for color names to use for your site's labels. You can also use hexadecimal color values.

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

- Color values specify the amount of red, green, and blue (RGB) that compose the color.
- RGB values can be specified with three hexadecimal numbers from 0 to FF. Each hexadecimal number indicates the amount of red, green, or blue in the color. For example:
  - Pure white is #FFFFFF
  - Pure red is #FF0000
  - Pure black is #000000

  For more information, see the X11(5) man page.
- The number of colors that are available on the screen depends on several factors:
  - Amount of memory available for specifying colors
  - Number of color planes
  - How many other clients are using color cells
  - Whether private color maps are being used by other applications

For a sample color name planner, see Table 11, "Color Names Planner for SecCompany," on page 99. To assign colors, see "How to Assign a Color to a Label or Word" on page 79.

Modifying Extensions From Oracle Solaris to the label_encodings File

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

Purpose	Instructions
Add a LOCAL DEFINITIONS section to your encodings file.	"How to Add Extensions From Oracle Solaris to an Encodings File" on page 77
Change label and clearance defaults for users.	"How to Specify Default User Labels" on page 78
Specify colors for labels.	"How to Assign a Color to a Label or Word" on page 79

▼ How to Add Extensions From Oracle Solaris to an Encodings File

The LOCAL DEFINITIONS section of the label_encodings file enables you to specify default user labels and colors for labels.

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

- **Add the `LOCAL DEFINITIONS` section to your `label_encodings` file.**

  Append the section from an Oracle Solaris-supplied `label_encodings` file. Oracle Solaris-supplied files are in the `/etc/security/tsol` directory.

How to Specify Default User Labels

Before You Begin You must be in the Security Administrator role in the global zone. You must have an encodings file with a `LOCAL DEFINITIONS` section.

1. **Back up the `label_encodings` file.**

   ```
   # cp label_encodings label_encodings.orig
   ```

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

   ```
   # pfedit label_encodings
   ```

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

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

4. **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;
   ```

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

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

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

6. **Save your changes.**

Next Steps Continue with "How to Analyze and Verify the `label_encodings` File" on page 51.

How to Assign a Color to a Label or Word

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

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

1. **Back up the `label_encodings` file.**

```
# cp label_encodings label_encodings.orig
```

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

```
# pfedit label_encodings
```

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

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

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

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

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

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

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

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

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

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

   b. **Assign the color names.**

For example, assign the color OrangeRed to the `EMGT` compartment:

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

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

   In this example, assign the color MediumPurple4 to the `NEED TO KNOW` label.

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

7. **Save your changes.**

Next Steps Continue with "How to Analyze and Verify the `label_encodings` File" on page 51.

CHAPTER 6

Example of Planning an Organization's Encodings File

This chapter discusses the creation of a set of Trusted Extensions labels that meet a company's goals for information protection. This chapter covers the following topics:

- "Identifying the Site's Label Requirements" on page 81
- "Climbing the Security Learning Curve" on page 85
- "Analyzing the Requirements for Each Label" on page 86
- "Defining the Set of Labels" on page 91
- "Editing and Installing the `label_encodings` File" on page 100
- "Configuring Users and Printers for Labels" on page 107

The `label_encodings` file that results from this planning is provided in Appendix A, "Customized Encodings File for SecCompany". A version of this file is installed as the `label_encodings.example` file.

Identifying the Site's Label Requirements

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

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

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

Satisfying Information Protection Goals

At SecCompany, the manager in charge of information protection makes use of all possible channels to communicate labeling requirements. However, some employees do not understand the requirements. Other employees forget about the requirements or ignore them. Even when labels are properly applied, the information is not always properly handled, stored, and distributed. For example, reports indicate that registered information is sometimes found unattended. Copies of registered information have been left next to copy machines and printers, in break rooms, and in lobbies.

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

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

Trusted Extensions Features That Address Labeling and Access

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

Even though security was not yet fully understood at the company, the manager in charge of information protection knew that Trusted Extensions could implement the following features immediately:

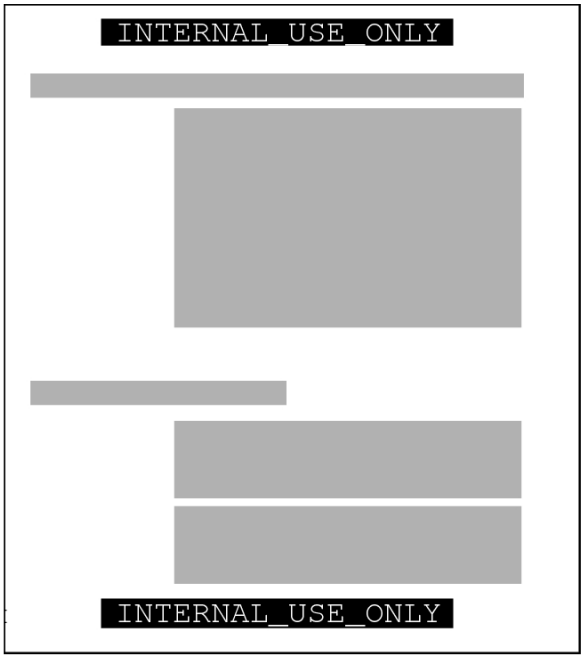
- Automatic labeling of print jobs
- Printers with restricted access by label
- Email with restricted access by label

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

For example, when an employee works at the level of `INTERNAL_USE_ONLY`, the work should be accessible only by people who have signed nondisclosure agreements with SecCompany. When this employee sends email to the printer, the print job is automatically assigned the label `INTERNAL_USE_ONLY`.

The following figure shows the user's working label, `INTERNAL_USE_ONLY`, printed at the top and bottom of a body page of the email.

FIGURE 20 Label Automatically Printed on Body Pages



Banner and trailer pages can include *handling instructions*. Printed below the sensitivity label, handling instructions provides distribution instructions for the printed material. The following example shows the text on the banner page of a print job. The sensitivity level of the print job is `NEED_TO_KNOW` in the department of `HUMAN_RESOURCES`.

```
                    NEED_TO_KNOW HR

DISTRIBUTE_ONLY_TO HUMAN RESOURCES (NON-DISCLOSURE AGREEMENT REQUIRED)
```

The instructions state that the information is only for human resources personnel who need to know the information. Also, the human resources personnel must have signed a nondisclosure agreement.

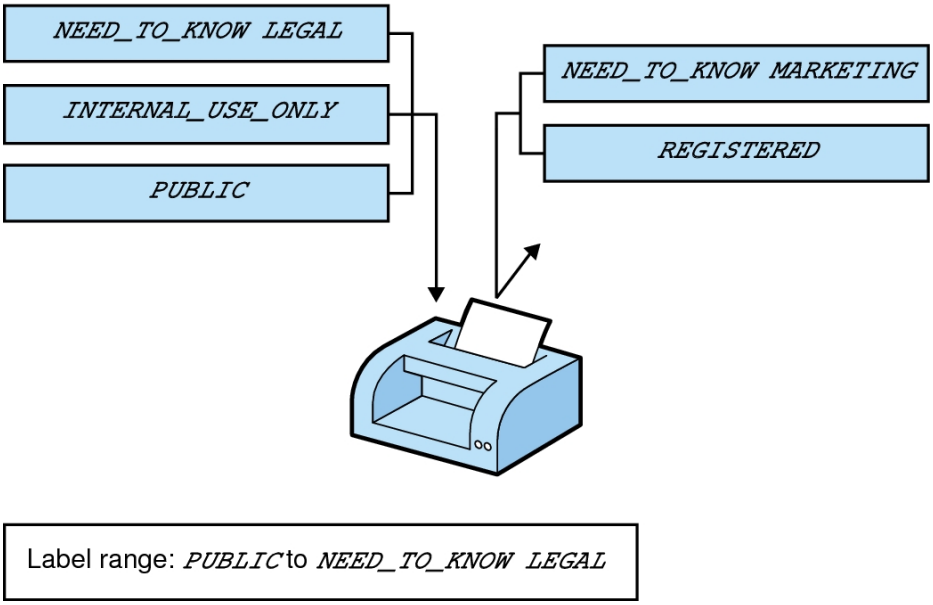
To retrieve a labeled printout, users must have access to a printer that prints at the label of the print job. A printer can be configured to print jobs at every label. For security, printers are configured to print only jobs within a restricted label range.

For example, Figure 21, “How a Printer With a Restricted Label Range Handles Print Jobs,” on page 84 illustrates that the legal department's printer has been set up to print only jobs that have been assigned one of three labels:

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

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

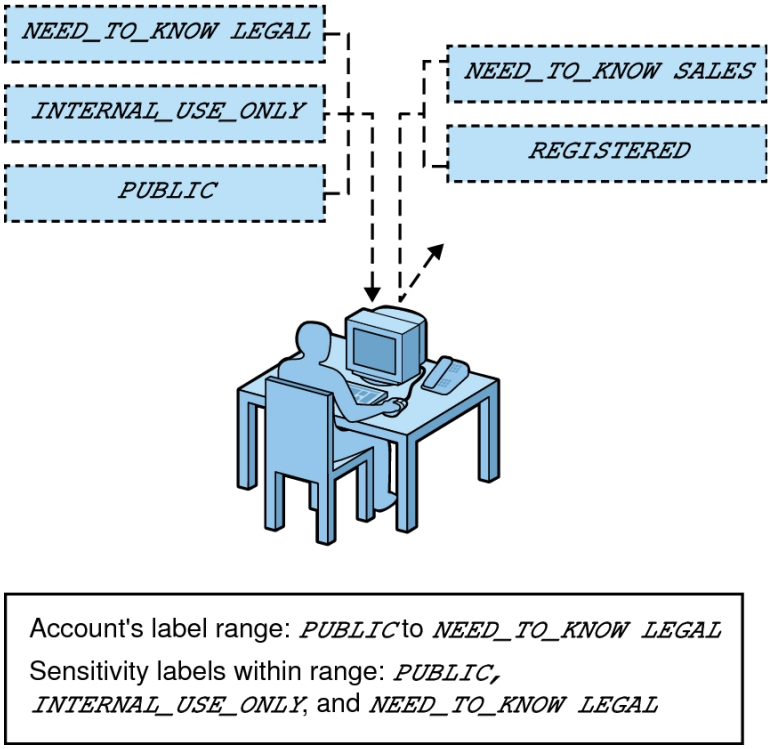
FIGURE 21 How a Printer With a Restricted Label Range Handles Print Jobs



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

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

FIGURE 22 User Receiving Email Within the Account Label Range



At SecCompany, gateways to the Internet are configured to screen email so that emails at inappropriate labels cannot be sent outside of the company. Inappropriate labels are any labels except `PUBLIC`.

Climbing the Security Learning Curve

The manager in charge of information protection identifies an experienced administrator with the following qualifications:

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

That person is assigned the job of security administrator.

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

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

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

Analyzing the Requirements for Each Label

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

Requirements for `CONFIDENTIAL: INTERNAL_USE_ONLY`

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

Suitable use of the `CONFIDENTIAL: INTERNAL_USE_ONLY` label includes the following:

- Spending guidelines
- Internal job postings

Requirements for `CONFIDENTIAL: NEED_TO_KNOW`

The `CONFIDENTIAL: NEED_TO_KNOW` label is for information that is proprietary to the company, has a higher level of sensitivity than `INTERNAL_USE_ONLY`, and has a more limited audience.

Distribution is limited to employees who need to know the information. Other people who need to know the information and who have signed nondisclosure agreements might also be in the audience.

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

Including the name of a group in the `CONFIDENTIAL: NEED_TO_KNOW` label makes it clear that the information must not be given to anyone outside of the group. Information with this label cannot be sent over the Internet, but it can be sent over email within the company.

Suitable use of the `NEED_TO_KNOW` label includes the following:

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

Requirements for `CONFIDENTIAL: REGISTERED`

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

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

Suitable use of the `CONFIDENTIAL: REGISTERED` label includes the following:

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

Names of Groups With `NEED_TO_KNOW` Label

The security administrator decides that the `NEED_TO_KNOW` label will contain the names of groups or departments. The security Administrator asks for suggestions about what words to

use to define groups or areas of interest within the organization. The following group names are in the initial list:

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

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

Understanding the Set of Labels

The next step for the security administrator is to resolve how to use the classifications and compartments to encode the labels and clearances.

The next step for the security administrator is to resolve the following issues:

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

The security administrator uses a large board. Pieces of paper are marked with the words that will be in the labels, as shown in Figure 23, “Sample Planning Board for Label Relationships at SecCompany,” on page 90. This setup illustrates the relationships among labels. The pieces are rearranged until they all fit together.

The administrator drafts the following label relationships:

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

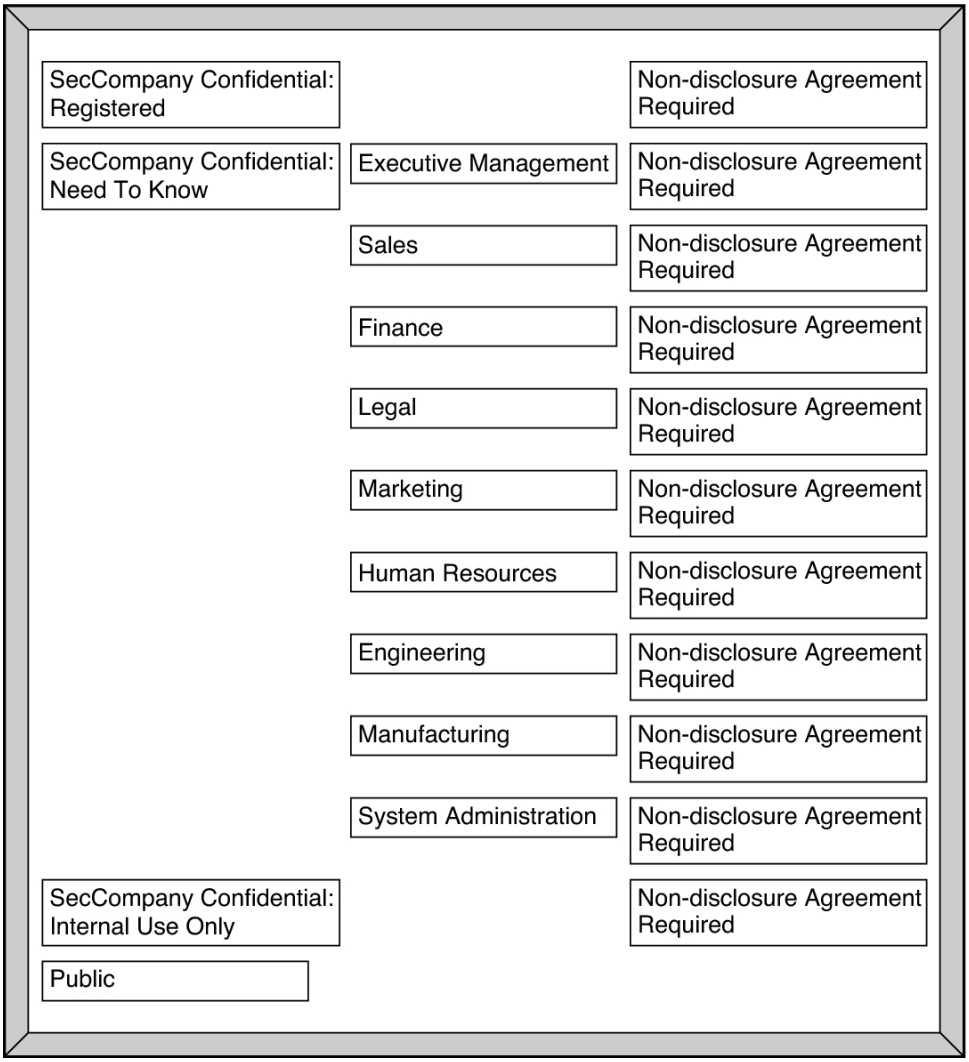
  The list of people who are cleared to receive registered information is limited on a case-by-case basis. Therefore, `REGISTERED` does not need any associated group names. `INTERNAL_USE_ONLY` applies to all employees and people who have signed nondisclosure agreements. `PUBLIC` labels are for everybody.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

- Each label except the `PUBLIC` label requires the person who is accessing the information to have signed a nondisclosure agreement.

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

  Along with information about the sensitivity of the printer output, handling instructions must explain that a nondisclosure agreement is required when the label requires such an agreement.

FIGURE 23 Sample Planning Board for Label Relationships at SecCompany



Defining the Set of Labels

In this section, SecCompany's set of labels is defined in lists that include the following required aspects of labels:

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

Planning the Classifications

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

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

The security administrator defines the following labels:

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

Planning the Compartments

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

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

Planning the Use of Words in MAC

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

SecCompany defines two sensitivity labels:

- `PUBLIC`, which is assigned the lowest value in the user accreditation range
- `INTERNAL_USE_ONLY`, which is assigned the next highest value above `PUBLIC`

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

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

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

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

Planning the Use of Words in Labeling System Output

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

`DISTRIBUTE_ONLY_TO` *Group Name* `(Non-Disclosure Agreement Required)`

Planning Unlabeled Printer Output

Users who are directed to an unlabeled printer can print output with no labels. Users in a labeled zone with its own print server can print output with no labels if they are assigned the `solaris.print.nolabel` authorization. Roles can be configured to print output with no labels to a local printer that is controlled by a Trusted Extensions print server.

Planning for Supporting Procedures

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

Rules for Protecting a `REGISTERED` File or Directory

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

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

EXAMPLE 17 Using DAC to Protect Registered Information

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

Rules for Configuring Printers

The following table shows how printers that are available to various SecCompany departments need to be configured.

TABLE 4 Label Ranges on SecCompany Printers at Various Locations

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

For more information, see Chapter 19, "Managing Labeled Printing" in *Trusted Extensions Configuration and Administration*.

Rules for Handling Printer Output

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

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

Planning the Classification Values in a Worksheet

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

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

TABLE 5 Classifications Planner for SecCompany

name=	sname=/aname=	value=	initial compartments= bit numbers/ WORD
PUBLIC	PUB	1	None
INTERNAL_USE_ONLY	IUO	4	None
NEED_TO_KNOW	NTK	5	None
REGISTERED	REG	6	None

Planning the Compartment Values and Combination Constraints in a Worksheet

The following table defines the relationships between words and classifications. The relationships were determined by using the planning board in Figure 23, "Sample Planning Board for Label Relationships at SecCompany," on page 90. PUBLIC and INTERNAL_USE_ONLY can never appear in a label with any compartment. NEED_TO_KNOW can appear in a label with any of the compartments or all of the compartments. The classification and compartment values are listed in ascending bit order.

TABLE 6 Compartments and User Accreditation Range Combinations Planner for SecCompany

Classification	Compartment Name/ sname/ Bit	Combination Constraints
PUBLIC		PUBLIC Only valid combinations
INTERNAL_USE_ONLY		INTERNAL_USE_ONLY Only valid combinations
NEED_TO_KNOW	EXECUTIVE_MANAGEMENT_GROUP/ EMGT/ 11	NEED_TO_KNOW All combinations valid
	SALES/ SALES/ 12	
	FINANCE/ FIN/ 13	
	LEGAL/ LEGAL/ 14	
	MARKETING/ MKTG/ 15 20	
	HUMAN_RESOURCES/ HR/ 16	
	ENGINEERING/ ENG/ 17 20	
	MANUFACTURING/ MFG/ 18	
	SYSTEM_ADMINISTRATION/ SYSADM/ 19	
	PROJECT_TEAM/ SYSADM/ 20	
	ALL_DEPARTMENTS/ ALL/ 11-20	
REGISTERED		REGISTERED Only valid combinations

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

TABLE 7 Compartment Bits Planner for SecCompany

11	12	13	14	15	16	17	18	19	20	

Planning the Clearances in a Worksheet

The components of these labels are also assigned to users in clearances. The worksheet's Clearance Planner in Table 8, “Clearance Planner for SecCompany,” on page 96 defines the label components to be used in clearances at SecCompany.

The following key to Table 8, “Clearance Planner for SecCompany,” on page 96 lists the components in descending classification bit order and ascending compartment bit order:

Abbreviation	Name	Component
REG	REGISTERED	CLASS
NTK	NEED_TO_KNOW	CLASS
IUO	INTERNAL_USE_ONLY	CLASS
PUB	PUBLIC	CLASS
EMGT	EXECUTIVE_MANAGEMENT_GROUP	COMP
SALES	SALES	COMP
FIN	FINANCE	COMP
LEGAL	LEGAL	COMP
MKTG	MARKETING	COMP
HR	HUMAN_RESOURCES	COMP
ENG	ENGINEERING	COMP
MFG	MANUFACTURING	COMP
SYSADM	SYSTEM_ADMINISTRATION	COMP
P_TEAM	PROJECT_TEAM	COMP
ALL	ALL_DEPARTMENTS	COMP

TABLE 8 Clearance Planner for SecCompany

CLASS	COMP	COMP	COMP	COMP	COMP	COMP	COMP	COMP	COMP	COMP	COMP	Notes
REG	EMGT	ENG	FIN	HR	LEGAL	MFG	MKTG	SALES	SYSADM	P_TEAM	ALL	Highest possible label, not used *
REG												Assigned to personnel as needed §

CLAS	SCOMP	COMP	COMP	COMP	COMP	COMP	COMP	COMP	COMP	COMP	COMP	Notes
NTK	EMGT											Assigned to EMGT group
NTK		ENG										Assigned to ENG group
NTK			FIN									Assigned to FIN group
NTK				HR								Assigned to HR group
NTK					LEGAL							Assigned to LEGAL group
NTK						MFG						Assigned to MFG group
NTK							MKTG					Assigned to MKTG group
NTK								SALES				Assigned to SALES group
NTK									SYSADM			Assigned to SYSADM group
NTK										P_TEAM		Assigned to P_TEAM group
NTK											ALL	Assigned to all groups
IUO												Assigned to people with NDAs
PUB												Assigned to anyone

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

§ When working at the REGISTERED sensitivity label, the user must set permissions to restrict access to everyone except the owner. UNIX file permissions of 600 and directory permissions of 700 restrict access.

Planning the Printer Banners in a Worksheet

The SecCompany legal department wants the following to appear on banner and trailer pages of printed output:

```
SecCompany Confidential:
```

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

SecCompany Confidential: *group-name*

In the following planner, the words in the second column are listed in order of ascending bit order.

TABLE 9 Printer Banners Planner for SecCompany

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

Planning the Channels in a Worksheet

The SecCompany legal department wants the following handling instructions to appear on banner and trailer pages on printed output:

`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 in Table 6, “Compartments and User Accreditation Range Combinations Planner for SecCompany,” on page 95. SecCompany plans to use the same group names in both the compartments and the channels.

The words that precede the channel name are specified as *prefixes*. The words that follow the channel name are specified as *suffixes*. The security administrator specifies prefixes and suffixes in the following planner. The planner lists the channels in ascending compartment bit order.

TABLE 10 Channels Planner for SecCompany

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)

Prefix	Channel	Suffix
DISTRIBUTE_ONLY_TO	SYSTEM_ADMINISTRATION	EMPLOYEES (NON-DISCLOSURE_AGREEMENT_REQUIRED)
DISTRIBUTE_ONLY_TO	PROJECT_TEAM	EMPLOYEES (NON-DISCLOSURE_AGREEMENT_REQUIRED)
DISTRIBUTE_ONLY_TO	ALL_DEPARTMENTS	EMPLOYEES (NON-DISCLOSURE_AGREEMENT_REQUIRED)

Planning the Minimum Labels in an Accreditation Range

The following minimum values must be set:

- Minimum sensitivity label
- Minimum clearance
- Minimum "Protect As" classification

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

The minimum "Protect As" classification is printed on 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, SecCompany requirements allow the minimum "Protect As" classification to always be equal to the real classification of the print job's sensitivity label. The security administrator specifies the value `PUBLIC` for the minimum sensitivity label, minimum clearance, and minimum "Protect As" classification.

Planning the Colors in a Worksheet

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

TABLE 11 Color Names Planner for SecCompany

Label or Name (`label=` or `name=`)	Color
ADMIN_LOW	#BDBDBD

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

Editing and Installing the label_encodings File

The SecCompany setup team for Trusted Extensions makes a printed copy and an online copy of the installed label_encodings file. The copy is used in case of problems with the new version of the file that the security administrator supplies.

The security administrator uses a text editor to create the label_encodings file and then uses the chk_encodings -a command to check the file. After the file passes all semantic and syntactic checks, the security administrator backs up the current version of the label_encodings file, and installs the new label_encodings file.

Specifying the Version

The following example shows the SecCompany VERSION string in the label_encodings file.

EXAMPLE 18 SecCompany VERSION String

```
VERSION= SecCompany, Inc. Example Version - 2.2 10/10/20
```

Specifying the Classifications

The following example shows the SecCompany classifications and values from Table 5, "Classifications Planner for SecCompany," on page 95 in the CLASSIFICATIONS section.

EXAMPLE 19 SecCompany CLASSIFICATIONS Section

```
CLASSIFICATIONS:

name= PUBLIC; sname= PUB; value= 1;
name= INTERNAL_USE_ONLY; sname= IUO; aname= IUO; value= 4;
name= NEED_TO_KNOW; sname= NTK; aname= NTK; value= 5;
name= REGISTERED; sname= REG; aname= REG; value= 6;
```

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

Specifying the Sensitivity Labels

The compartments from Table 6, "Compartments and User Accreditation Range Combinations Planner for SecCompany," on page 95 are specified in the following example. The labels do not have any required combinations or combination constraints.

EXAMPLE 20 SecCompany WORDS in the SENSITIVITY LABELS Section

```
SENSITIVITY LABELS:

WORDS:

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

Specifying the Information Labels

Even though information labels are not used, values must be supplied under the INFORMATION LABELS: WORDS: section of the label_encodings file for the file to pass the encodings check. The security administrator copies the words from the SENSITIVITY LABELS: WORDS: section. The result is shown in the following example.

EXAMPLE 21 SecCompany WORDS in the INFORMATION LABELS Section

```
INFORMATION LABELS:

WORDS:

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

Specifying the Clearances

Because the clearance words are the same as the sensitivity labels words, the words in the following example are the same as the words in "Specifying the Sensitivity Labels" on page 101.

EXAMPLE 22 SecCompany WORDS in the CLEARANCES Section

```
CLEARANCES:

WORDS:

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

```
name= FINANCE; sname= FIN; compartments= 13; minclass= NEED_TO_KNOW;
name= LEGAL; sname= LEGAL; compartments= 14; minclass= NEED_TO_KNOW;
name= MARKETING; sname= MKTG; compartments= 15 20; minclass= NEED_TO_KNOW;
name= HUMAN_RESOURCES; sname= HR; compartments= 16; minclass= NEED_TO_KNOW;
name= ENGINEERING; sname= ENG; compartments= 17 20; minclass= NEED_TO_KNOW;
name= MANUFACTURING; sname= MFG; 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:
```

Specifying the Channels

The security administrator specifies one channel for each group name compartment. Each channel uses the same compartment bits that are assigned to the compartment words in the `SENSITIVITY LABELS: WORDS:` section. The prefix is defined as `DISTRIBUTE_ONLY_TO`. The suffix is defined as `(NON-DISCLOSURE AGREEMENT REQUIRED)`. The following is the proposed wording for handling instructions:

`DISTRIBUTE_ONLY_TO` *group-name* `(NON-DISCLOSURE AGREEMENT REQUIRED)`

The channel specifications in the following example create this wording.

Note - No compartments are assigned to the prefixes and suffixes. The prefixes and suffixes are used to define the channels.

EXAMPLE 23 SecCompany `WORDS` in the `CHANNELS` Section

```
CHANNELS:

WORDS:

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

name= ALL_DEPARTMENTS; prefix= DISTRIBUTE_ONLY_TO; compartments= 11-20;
suffix= EMPLOYEES (NON-DISCLOSURE AGREEMENT REQUIRED);
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);
```

Specifying the Printer Banners

The term *printer banner* has a specialized meaning in the `label_encodings` file. A printer banner appears as a string on the banner page of printed output when the compartment that is associated with the printer banner string is part of a job's label.

The SecCompany `PRINTER BANNERS` section is shown in the following example. For a sample banner page, see Figure 12, “Typical Banner Page of a Labeled Print Job,” on page 61.

Note - No compartments are assigned to the prefixes and suffixes.

EXAMPLE 24 SecCompany `WORDS` in the `PRINTER BANNERS` Section

```
PRINTER BANNERS:

WORDS:

name= SECCOMPANY CONFIDENTIAL:;       prefix;
name= (NON-DISCLOSURE AGREEMENT REQUIRED);  suffix;

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

```
name= HUMAN_RESOURCES; prefix= SECCOMPANY CONFIDENTIAL:;
compartments= 16; suffix=(NON-DISCLOSURE AGREEMENT REQUIRED);
name= ENGINEERING; prefix= SECCOMPANY CONFIDENTIAL:;
compartments= 17 20; suffix=(NON-DISCLOSURE AGREEMENT REQUIRED);
name= MANUFACTURING; prefix= SECCOMPANY CONFIDENTIAL:;
compartments= 18; suffix=(NON-DISCLOSURE AGREEMENT REQUIRED);
name= SYSTEM_ADMINISTRATION; prefix= SECCOMPANY CONFIDENTIAL:;
compartments= 19; suffix=(NON-DISCLOSURE AGREEMENT REQUIRED);
name= PROJECT_TEAM; prefix= SECCOMPANY CONFIDENTIAL:;
compartments= 20; suffix=(NON-DISCLOSURE AGREEMENT REQUIRED);
```

Specifying the Accreditation Range

The `ACCREDITATION RANGE:` section in the following example shows the combination constraints from Table 6, “Compartments and User Accreditation Range Combinations Planner for SecCompany,” on page 95, and the minimum clearance, minimum sensitivity label, and minimum "Protect As" classification from “Planning the Minimum Labels in an Accreditation Range” on page 99. `PUBLIC`, `INTERNAL_USE_ONLY`, and `REGISTERED` are defined to never appear in a label with any compartment. `NEED_TO_KNOW` is defined to appear in a label with any combination of compartments.

EXAMPLE 25 SecCompany `ACCREDITATION RANGE` Section

```
ACCREDITATION RANGE:

classification= PUBLIC; only valid compartment combinations:
PUB

classification= INTERNAL_USE_ONLY; only valid compartment combinations:
IUO

classification= NEED_TO_KNOW; all compartment combinations valid;

classification= REGISTERED; only valid compartment combinations:
REG

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

Specifying the Local Definitions

SecCompany sets the default user labels, and customizes column headings and colors in the `LOCAL DEFINITIONS` section.

Specifying the Default User Labels

SecCompany enables all users to access the PUBLIC label.

EXAMPLE 26 SecCompany Default User Labels

```
Default User Sensitivity Label= PUB;
Default User Clearance= PUB;
```

Specifying the Color Names

The security administrator used the worksheet in Table 11, "Color Names Planner for SecCompany," on page 99 to complete the Color Names section.

EXAMPLE 27 SecCompany COLOR NAMES Section

```
COLOR NAMES:

label= Admin_Low;       color= #BDBDBD;

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

label= Admin_High;      color= #636363;

*
* End of local site definitions
```

Configuring Users and Printers for Labels

The security administrator has completed the `label_encodings` file. However, apart from the `label_encodings` file, labeling decisions at SecCompany need to be enforced on users and on printers.

For every user, the security administrator needs to specify the following:

- The appropriate clearance

  The default, `PUBLIC`, is too low for employees, but is required to prevent non-employees from accessing company files. For assistance, see "Planning the Clearances in a Worksheet" on page 96.
- The appropriate minimum label

  The default, `PUBLIC`, is not a company label. Company files start at the `INTERNAL_USE_ONLY` label. For assistance, see "Planning the Minimum Labels in an Accreditation Range" on page 99.

The security administrator can enable users to bypass certain Trusted Extensions print security features by assigning authorizations to the users.

For more information, see "Managing Users and Rights" in *Trusted Extensions Configuration and Administration*.

For every printer, the security administrator can specify a label range. For printer configuration procedures, see "Configuring Labeled Printing" in *Trusted Extensions Configuration and Administration*.

♦ ♦ ♦ APPENDIX A

Customized Encodings File for SecCompany

This appendix contains the `label_encodings` file that was customized for SecCompany, Inc. in Chapter 6, "Example of Planning an Organization's Encodings File". This appendix also contains a sample of the debugging steps that the security administrator performed to create a syntactically correct file. Sample output from the `chk_encodings -a` command is provided.

- "SecCompany's `label_encodings` File" on page 109
- "SecCompany's Verification of the `label_encodings` File" on page 113

SecCompany's `label_encodings` File

Note - This file is similar to the `label_encodings.example` file that is delivered by Trusted Extensions.

At SecCompany, `PUBLIC` is the sensitivity label for communications across the Internet. `INTERNAL_USE_ONLY` is the sensitivity label for communications within the company.

The `ALL_DEPARTMENTS` compartment word gets turned on when all defined compartment bits are on. This compartment word works as a toggle in a label builder.

```
* ident "@(#)label_encodings.seccompany     %I% %E%"
*
* Copyright 2010 SecCompany, Inc.  All rights reserved.
* Use is subject to license terms.
*
*
* These confidential labels are required by SecCompany's
* legal and information protection departments.
* Department names can be used for controlling
* access to information across department boundaries.

* These labels are used for mandatory access control
* checks based on user clearance labels and labels and
* sensitivity labels on files and directories.
```

```
VERSION= SecCompany, Inc. Example Version - 2.2 10/10/20



CLASSIFICATIONS:

name= PUBLIC; sname= PUB; value= 1;
name= INTERNAL_USE_ONLY; sname= IUO; aname= IUO; value= 4;
name= NEED_TO_KNOW; sname= NTK; aname= NTK; value= 5;
name= REGISTERED; sname= REG; aname= REG; value= 6;


INFORMATION LABELS:

WORDS:

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

SENSITIVITY LABELS:

WORDS:

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

REQUIRED COMBINATIONS:

COMBINATION CONSTRAINTS:

CHANNELS:

WORDS:

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

name= ALL_DEPARTMENTS; prefix= DISTRIBUTE_ONLY_TO; compartments= 11-20;
suffix= EMPLOYEES (NON-DISCLOSURE AGREEMENT REQUIRED);
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= SECCOMPANY CONFIDENTIAL:;       prefix;
name= (NON-DISCLOSURE AGREEMENT REQUIRED);  suffix;

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

ACCREDITATION RANGE:

classification= PUBLIC; only valid compartment combinations:
PUB

classification= INTERNAL_USE_ONLY; only valid compartment combinations:
IUO

classification= NEED_TO_KNOW; all compartment combinations valid;

classification= REGISTERED; only valid compartment combinations:
REG

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

*
* Local site definitions and locally configurable options.
*
LOCAL DEFINITIONS:
```

```
*

Classification Name= Classification;
Compartments Name= Departments;

Default User Sensitivity Label= PUB;
Default User Clearance= PUB;

COLOR NAMES:

label= Admin_Low;      color= #bdbdbd;

label= PUBLIC;    color= green;
label= INTERNAL_USE_ONLY;   color= yellow;
label= NEED_TO_KNOW;   color= blue;
label= NEED_TO_KNOW EMGT;    color= #7FA9EB;
label= NEED_TO_KNOW SALES;   color= #87CEFF;
label= NEED_TO_KNOW FIN;   color= #00BFFF;
label= NEED_TO_KNOW LEGAL;    color= #7885D0;
label= NEED_TO_KNOW MKTG;    color= #7A67CD;
label= NEED_TO_KNOW HR;    color= #7F7FFF;
label= NEED_TO_KNOW ENG;    color= #007FFF;
label= NEED_TO_KNOW MFG;    color= #0000BF;
label= NEED_TO_KNOW P_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
*
```

SecCompany's Verification of the `label_encodings` File

After the `chk_encodings -a` command several times, the security administrator corrected the syntax of the `label_encodings` file. The following corrections provide a sample:

```
Label encodings conversion error:

In PRINTER BANNERS WORDS, word "ALL_DEPARTMENTS": SUFFIX "(NON-DISCLOSURE AGREEMENT
REQUIRED)" not found.
```

Description: The final parenthesis after `REQUIRED` in the `ALL_DEPARTMENTS` entry was missing. The security administrator typed the parenthesis.

```
Label encodings conversion error at line 168:
In ACCREDITATION RANGE, classification "INTERNAL_USE_ONLY": SENSITIVITY LABEL
"INTERNAL_USE_ONLY" not in canonical form. Is IUO what was intended?
```

Description: The security administrator replaced INTERNAL_USE_ONLY with IUO at line 168.

```
Label encodings conversion error at line 172:
In ACCREDITATION RANGE, classification "NEED_TO_KNOW": No sensitivity labels allowed
after ALL COMPARTMENT COMBINATIONS VALID.
```

Description: The security administrator removed NEED_TO_KNOW at line 172.

```
"DEFAULT USER SENSITIVITY LABEL= PUBLIC" is not in canonical form. Is PUB what is
intended?
```

Description: The security administrator replaced PUBLIC with PUB.

```
Label encodings conversion error at line 206: Invalid color label "NEED_TO_KNOW EMG".
```

Description: The security administrator replaced EMG with EMGT.

The following is an excerpt from the successful execution of the chk_encodings -a command.

```
No errors found in label_encodings.seccompany.


---> VERSION = SECCOMPANY, INC. EXAMPLE VERSION - 2.2 10/10/20 <---

---> CLASSIFICATIONS <---

Classification 1: PUBLIC (PUB)
Initial Compartment bits: NONE
Initial Markings bits: NONE
Classification 4: INTERNAL_USE_ONLY (IUO) / IUO
Initial Compartment bits: NONE
Initial Markings bits: NONE
Classification 5: NEED_TO_KNOW (NTK) / NTK
Initial Compartment bits: NONE
Initial Markings bits: NONE
Classification 6: REGISTERED (REG) / REG
Initial Compartment bits: NONE
Initial Markings bits: NONE

---> COMPARTMENTS AND MARKINGS USAGE ANALYSIS <---

Normal compartment bits defined: 11-20
Regular inverse compartment bits defined: NONE
Compartment bits reserved as 1 but not defined: NONE

Normal marking bits defined: NONE
```

```
Regular inverse marking bits defined: NONE
Marking bits reserved as 1 but not defined: NONE

---> INFORMATION LABEL WORDS <---
...

---> SENSITIVITY LABEL WORDS <---

Word: ALL_DEPARTMENTS (ALL)
Valid classification range: NTK -> REG
Type: Normal
Words hierarchically above: NONE
Words hierarchically below:
EXECUTIVE_MANAGEMENT_GROUP (EMGT)
SALES (SALES)
FINANCE (FIN)
LEGAL (LEGAL)
MARKETING (MKTG)
HUMAN_RESOURCES (HR)
ENGINEERING (ENG)
MANUFACTURING (MFG)
SYSTEM_ADMINISTRATION (SYSADM)
PROJECT_TEAM (P_TEAM)

Word: EXECUTIVE_MANAGEMENT_GROUP (EMGT)
Valid classification range: NTK -> REG
Type: Normal
Words hierarchically above:
ALL_DEPARTMENTS (ALL)
Words hierarchically below: NONE

Word: SALES (SALES)
Valid classification range: NTK -> REG
Type: Normal
Words hierarchically above:
ALL_DEPARTMENTS (ALL)
Words hierarchically below: NONE

...
Word: MARKETING (MKTG)
Valid classification range: NTK -> REG
Type: Normal
Words hierarchically above:
ALL_DEPARTMENTS (ALL)
Words hierarchically below:
PROJECT_TEAM (P_TEAM)

...
Word: PROJECT_TEAM (P_TEAM)
Valid classification range: NTK -> REG
Type: Normal
```

```
Words hierarchically above:
ALL_DEPARTMENTS (ALL)
MARKETING (MKTG)
ENGINEERING (ENG)
Words hierarchically below: NONE

---> CLEARANCE WORDS <---

Word: ALL_DEPARTMENTS (ALL)
Valid classification range: NTK -> REG
Type: Normal
Words hierarchically above: NONE
Words hierarchically below:
EXECUTIVE_MANAGEMENT_GROUP (EMGT)
SALES (SALES)
FINANCE (FIN)
LEGAL (LEGAL)
MARKETING (MKTG)
HUMAN_RESOURCES (HR)
ENGINEERING (ENG)
MANUFACTURING (MFG)
SYSTEM_ADMINISTRATION (SYSADM)
PROJECT_TEAM (P_TEAM)

Word: EXECUTIVE_MANAGEMENT_GROUP (EMGT)
Valid classification range: NTK -> REG
Type: Normal
Words hierarchically above:
ALL_DEPARTMENTS (ALL)
Words hierarchically below: NONE

...
Word: MARKETING (MKTG)
Valid classification range: NTK -> REG
Type: Normal
Words hierarchically above:
ALL_DEPARTMENTS (ALL)
Words hierarchically below:
PROJECT_TEAM (P_TEAM)
...

Word: PROJECT_TEAM (P_TEAM)
Valid classification range: NTK -> REG
Type: Normal
Words hierarchically above:
ALL_DEPARTMENTS (ALL)
MARKETING (MKTG)
ENGINEERING (ENG)
Words hierarchically below: NONE

---> CHANNEL WORDS <---
```

```
Prefix Word: DISTRIBUTE_ONLY_TO

Suffix Word: EMPLOYEES (NON-DISCLOSURE AGREEMENT REQUIRED)

Word: DISTRIBUTE_ONLY_TO ALL_DEPARTMENTS EMPLOYEES (NON-DISCLOSURE AGREEMENT REQUIRED)
Valid classification range: PUB -> REG
Type: Normal
Words hierarchically above: NONE
Words hierarchically below:
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)

Word: DISTRIBUTE_ONLY_TO EXECUTIVE_MANAGEMENT_GROUP EMPLOYEES (NON-DISCLOSURE AGREEMENT
 REQUIRED)
Valid classification range: PUB -> REG
Type: Normal
Words hierarchically above:
DISTRIBUTE_ONLY_TO ALL_DEPARTMENTS EMPLOYEES (NON-DISCLOSURE AGREEMENT REQUIRED)
Words hierarchically below: NONE

...
Word: DISTRIBUTE_ONLY_TO PROJECT_TEAM EMPLOYEES (NON-DISCLOSURE AGREEMENT REQUIRED)
Valid classification range: PUB -> REG
Type: Normal
Words hierarchically above:
DISTRIBUTE_ONLY_TO ALL_DEPARTMENTS EMPLOYEES (NON-DISCLOSURE AGREEMENT REQUIRED)
DISTRIBUTE_ONLY_TO MARKETING EMPLOYEES (NON-DISCLOSURE AGREEMENT REQUIRED)
DISTRIBUTE_ONLY_TO ENGINEERING EMPLOYEES (NON-DISCLOSURE AGREEMENT REQUIRED)
Words hierarchically below: NONE

---> PRINTER BANNER WORDS <---

Prefix Word: SECCOMPANY CONFIDENTIAL:

Suffix Word: (NON-DISCLOSURE AGREEMENT REQUIRED)

Word: SECCOMPANY CONFIDENTIAL: ALL_DEPARTMENTS (NON-DISCLOSURE AGREEMENT REQUIRED)
Valid classification range: PUB -> REG
Type: Normal
Words hierarchically above: NONE
Words hierarchically below:
```

```
SECCOMPANY CONFIDENTIAL: EXECUTIVE_MANAGEMENT_GROUP (NON-DISCLOSURE AGREEMENT REQUIRED)
SECCOMPANY CONFIDENTIAL: SALES (NON-DISCLOSURE AGREEMENT REQUIRED)
SECCOMPANY CONFIDENTIAL: FINANCE (NON-DISCLOSURE AGREEMENT REQUIRED)
SECCOMPANY CONFIDENTIAL: LEGAL (NON-DISCLOSURE AGREEMENT REQUIRED)
SECCOMPANY CONFIDENTIAL: MARKETING (NON-DISCLOSURE AGREEMENT REQUIRED)
SECCOMPANY CONFIDENTIAL: HUMAN_RESOURCES (NON-DISCLOSURE AGREEMENT REQUIRED)
SECCOMPANY CONFIDENTIAL: ENGINEERING (NON-DISCLOSURE AGREEMENT REQUIRED)
SECCOMPANY CONFIDENTIAL: MANUFACTURING (NON-DISCLOSURE AGREEMENT REQUIRED)
SECCOMPANY CONFIDENTIAL: SYSTEM_ADMINISTRATION (NON-DISCLOSURE AGREEMENT REQUIRED)
SECCOMPANY CONFIDENTIAL: PROJECT_TEAM (NON-DISCLOSURE AGREEMENT REQUIRED)

Word: SECCOMPANY CONFIDENTIAL: EXECUTIVE_MANAGEMENT_GROUP (NON-DISCLOSURE AGREEMENT
 REQUIRED)
Valid classification range: PUB -> REG
Type: Normal
Words hierarchically above:
SECCOMPANY CONFIDENTIAL: ALL_DEPARTMENTS (NON-DISCLOSURE AGREEMENT REQUIRED)
Words hierarchically below: NONE
...
Word: SECCOMPANY CONFIDENTIAL: PROJECT_TEAM (NON-DISCLOSURE AGREEMENT REQUIRED)
Valid classification range: PUB -> REG
Type: Normal
Words hierarchically above:
SECCOMPANY CONFIDENTIAL: ALL_DEPARTMENTS (NON-DISCLOSURE AGREEMENT REQUIRED)
SECCOMPANY CONFIDENTIAL: LEGAL (NON-DISCLOSURE AGREEMENT REQUIRED)
SECCOMPANY CONFIDENTIAL: ENGINEERING (NON-DISCLOSURE AGREEMENT REQUIRED)
Words hierarchically below: NONE

---> LOCAL DEFINITIONS <---

Classification Field Name is "CLASSIFICATION"
Compartments Field Name is "DEPARTMENTS"

Default User Clearance = "PUB"

Default User Sensitivity Label = "PUB"

---> SENSITIVITY LABEL to COLOR MAPPING <---

ADMIN_LOW = "#BDBDBD"
PUB = "GREEN"
IUO = "YELLOW"
NTK = "BLUE"
NTK EMGT = "#7FA9EB"
NTK SALES = "#87CEFF"
NTK FIN = "#00BFFF"
NTK LEGAL = "#7885D0"
NTK MKTG = "#7A67CD"
NTK HR = "#7F7FFF"
NTK ENG = "#007FFF"
NTK MFG = "#0000BF"
```

```
NTK P_TEAM = "#9E7FFF"
NTK SYSADM = "#5B85D0"
NTK ALL = "#4D658D"
REG = "RED"
ADMIN_HIGH = "#636363"
```

Index

A

access control
  example, 18
  label range, by, 17
access decisions
  using labels, 17
access-related words
  definitions, 62
accounts
  label range, 24, 25
  session range, 27
`ACCREDITATION RANGE` keyword, 44
`ACCREDITATION RANGE` section
  description, 44
  example, 105
accreditation ranges
  example, 105
  overview, 21
  system, 22
  user, 23
`ADMIN_HIGH` label
  classification value, 45
  illustrating numerical value, 19
`ADMIN_LOW` label
  classification value, 45
  illustrating numerical value, 19
administrative labels
  configuring appearance, 30
  specifying name visibility, 30
  system accreditation range, in, 22
`aname=` classification keyword, 46
authorizations
  `Downgrade File Label`, 31
  `Print Without Labels`, 93
  `Upgrade File Label`, 31

B

banner pages
  appearance, 60
  computing the classification for, 63
  customizing, 62
  internationalizing, 62
  labeling, 60
body pages
  appearance, 59
  labeling, 59

C

caveats *See* handling instructions
channels
  example, 103
  prefixes and suffixes, 66
  specifying handling instructions, 71
  strings on banner and trailer pages, 65, 70
  worksheet example, 98
`CHANNELS` keyword, 44
`CHANNELS` section
  description, 44
  example, 103
`chk_encodings -a` command, 51
CIPSO labels
  illustration of, 19
  numerical values, 19
  troubleshooting, 58
  warning in `label_encodings` file, 46
classifications
  adding to existing `label_encodings` file, 52
  analyzing, example of, 86
  dominance, 45
  keywords, 45
  maximum number, 19, 45

numerical values, 45
planning, example of, 91
renaming, 52
rules for printing, 63
specifying colors, 79
syntax, 45
`CLASSIFICATIONS` section
assigning initial compartments, 47
description, 43
example, 101
keywords, 45
words, 47
clearances
account label range, 24
example, 102
type of label, 16
worksheet example, 96
`CLEARANCES` keyword, 44
`CLEARANCES` section
description, 44
example, 102
`COLOR NAMES` section
color planner, 99
description, 41, 74
example, 106
colors
assigning, 79
finding color values, 79
rules of use for labels, 75
specifying for labels, 74
values, 76
worksheet example, 99
combination constraints
definition, 21
example, 22, 24, 26, 105
`COMBINATION CONSTRAINTS` keyword, 44
combination rules *See* combination constraints
Common IP Security Option (CIPSO) *See* CIPSO
labels
comparing
GFI files, 40
`label_encodings` files, 38
labels, 18
compartments
default and inverse words, 47
hierarchical, 49
numerical values, 48
planning, example of, 91
representing areas of interest, 48
words, 48
words, example of, 48
worksheet example, 95
`CONFIDENTIAL: INTERNAL_USE_ONLY` label
requirements, 86
`CONFIDENTIAL: NEED_TO_KNOW` label
groups that use, 87
requirements, 86
`CONFIDENTIAL: REGISTERED` label
adding DAC protections, 93
requirements, 87
Configuring Security Text on Print Jobs (Task Map), 70
creating
`label_encodings` file, 51
customizing
banner pages, 62
color assignments to labels, 79, 99
handling instructions by using channels, 71
handling instructions in printed output, 70
label appearance, 30
security text on printer output, 60

D

debugging
`label_encodings` file, 51, 58
`label_encodings` file example, 113
default words
definition, 47
specifying, 54
defaults
user labels, 106
Defense Intelligence Agency (DIA)
`label_encodings` reference, 37
demonstration files
`label_encodings` file for SecCompany, 109
`label_encodings` samples, 38
`label_encodings` verification log, 113
`label_encodings.example` file, 47
`label_encodings.multi` file, 46
dominance, 20

`Downgrade File Label` authorization, 31

E

`/etc/security/tsol` directory, 38
encodings file *See* `label_encodings` file
examples
  account label range, 25
  `ACCREDITATION RANGE` section, 105
  `CHANNELS` section, 103
  `chk_encodings -a` log, 113
  `CLASSIFICATIONS` section, 101
  `CLEARANCES` section, 102
  `COLOR NAMES` section, 106
  commercial `label_encodings` file, 81
  debugging `label_encodings` file, 113
  default user clearance, 106
  default user sensitivity label, 106
  `label_encodings` file for SecCompany, 109
  `label_encodings` verification log, 113
  labels planning, 81
  `LOCAL DEFINITIONS` section, 105
  MAC decision, 18
  `PRINTER BANNERS` section, 104
  `SENSITIVITY LABELS` section, 101

F

files
  `label_encodings`, 38
  `label_encodings` SecCompany example, 109
  `label_encodings` verification log, 113
  `label_encodings` versions, 38
  `/usr/lib/cups/filter/tsol_separator.ps`, 62
  `/usr/share/man/man5/X11.5`, 75
  `/usr/share/X11/rgb.txt`, 76
  `/usr/X11/share/man/man5/X11.5`, 75

G

GFI files
  comparing, 40
  in `/etc/security/tsol` directory, 38

H

handling instructions
  printer banners, 31
  specifying by using channels, 71
  specifying in `PRINTER BANNERS`, 70

I

`INFORMATION LABELS` keyword, 43
`INFORMATION LABELS` section
  description, 43
  example, 102
initial compartments
  assigning bits to words, 47
  definition, 47
`initial compartments=` classification keyword, 46
internationalizing
  banner and trailer pages for printed output, 60, 62
inverse words
  definition, 47
  specifying, 54

J

`job-sheets=labeled` option
  banner and trailer pages, 60
  body pages, 59

K

keywords for classifications, 45

L

`label_encodings` file
  access-related words, 62
  `ACCREDITATION RANGE` section, 105
  changing classification names, 52
  `CHANNELS` section, 65, 70, 103
  classification keywords, 45
  classifications
    example, 46
    name syntax, 45
  `CLASSIFICATIONS` section, 45, 101
  `CLEARANCES` section, 102

color encoding example, 99
commercial example, 81
compartment words, 48
creating
example of, 91
initial, 51
single-label, 55
debugging, 58, 113
default versions, 38
description, 37
`INFORMATION LABELS` section, 102
installed with Trusted Extensions, 38
list of, 38
`LOCAL DEFINITIONS` section, 73, 105
Oracle Solaris extensions to GFI encodings, 41
Oracle Solaris version of GFI multilabel file, 40
Oracle Solaris version of GFI single-label file, 41
planning, 33
`PRINTER BANNERS` section, 104
Protect As classification, 62
`REQUIRED COMBINATIONS` section, 50
SecCompany example, 109
`SENSITIVITY LABELS` section, 101
specifying default and inverse words, 54
specifying label colors, 74, 79
syntax, 43
U.S. government versions, 40
`VERSION` section, 100
word order requirements, 44
`label_encodings` file, 38
`label_encodings.example` file, 38
`label_encodings.gfi.multi` file, 38
`label_encodings.gfi.single` file, 38
`label_encodings` file, 38
`label_encodings.multi` file, 38
`label_encodings.single` file, 38
labels
access decisions, 17
account label range, 24
accreditation ranges, 21
analyzing, example of, 86
arranging relationships, 35
authorizations for changing, 31
available during sessions, 29
banner and trailer pages, 60
CIPSO, 19, 48
clearance, 16
color planning example, 99
commercial example, 81
comparing, 18
components, 19
configuring on printer output, 31
defaults
user clearance, 106
user sensitivity label, 106
dominance, 20
example, 101
files supplied by Oracle Solaris, 38
installation example, 100
internal representation, 31
`job-sheets=labeled` option, 59, 60
length of components, 48
limit, 21
lower bound, 21
mandatory access and printing considerations, 82
minimum "Protect As" classification, 72
planning, 33, 34
printed body pages, 59
ranges, 16, 21
requirements for `CONFIDENTIAL: INTERNAL_USE_ONLY`, 86
requirements for `CONFIDENTIAL: NEED_TO_KNOW`, 86
requirements for `CONFIDENTIAL: REGISTERED`, 87
restricting access by, 17, 17
session range, 27
sources for `label_encodings` files, 37
specifying colors, 79
system accreditation range, 22
textual strings, 31
translating between representations, 31
translating into another language on banner and trailer pages, 62
types, 16
upper bound, 21
user accreditation range, 23
users
default clearance, 106
default sensitivity label, 106
valid, 21
visible in workspaces, 30

well-formed, 21
worksheet example, 94
`LOCAL DEFINITIONS` keyword, 44
`LOCAL DEFINITIONS` section
adding to GFI encodings file, 41
description, 44, 73
example, 105
localizing *See* internationalizing
logs
`label_encodings` verification log, 113

M

Managing Label Encodings (Task Map), 50
mandatory access control (MAC)
definition, 15
used in access decisions, 18
minimum "Protect As" classification
example, 62, 63
printed output, 72
minimum clearance
example, 105
minimum labels
account label range, 24
commercial example, 99
minimum sensitivity label
definition, 24
example, 54, 57, 105
Modifying Oracle Solaris Extensions (Task Map), 77

N

`name=` classification keyword, 45

O

Oracle extensions *See* `LOCAL DEFINITIONS` section

P

planners *See* worksheets
planning labels
colors, 99
commercial example, 81
initial, 33
`label_encodings` file, 34
overview, 33
steps for, 34
supporting procedures, 93
unlabeled printer output, 93
Planning Labels (Task Map), 33
prefixes
in channels, 67
`Print Without Labels` authorization, 93
printer banners
appearance, 60
example, 104
specifying handling instructions, 70
worksheet example, 97
`PRINTER BANNERS` keyword, 44
`PRINTER BANNERS` section
description, 44
example, 104
printer output
banner text, 63
changing printed labels, 31
channels, 67
configuring labels and text, 60
further label configuration, 107
planning, example of, 92
prefixes and suffixes, 67
rules for handling, 94
setting minimum "Protect As" classification, 72
printing *See* printer output
privileges
changing labels, 31
Protect As classification
example, 63, 105
overview, 62
setting minimum for printed output, 72

R

required combinations *See* combination constraints
`REQUIRED COMBINATIONS` keyword, 44, 50
`rgb.txt` file, 76

S

security policy

definition, 15
identifying site requirements, 81
protecting information, 82
setting minimum "Protect As", 72
site-specific, 34
sensitivity
type of label, 16
sensitivity labels *See* labels
`SENSITIVITY LABELS` keyword, 44
`SENSITIVITY LABELS` section
description, 44
example, 101
sessions
duration of label restrictions chosen at login, 28
session range definition, 27
single-label
`label_encodings` file, 55
`sname=` classification keyword, 45
strict dominance, 21
suffixes
in channels, 67
syntax of `label_encodings` file, 43
`sys_trans_label` privilege, 31
system accreditation range, 22
system security policy, 15

T

task maps
Configuring Security Text on Print Jobs (Task Map), 70
Managing Label Encodings (Task Map), 50
Modifying Oracle Solaris Extensions (Task Map), 77
Planning Labels (Task Map), 33
trailer pages
computing the classification for, 63
example, 61
internationalizing, 62
labeling, 60, 62
translating, 15
See also internationalizing
between label representations, 31
troubleshooting
`label_encodings` file, 58
`tsol_separator.ps` file, 62
types of labels, 16

U

`Upgrade File Label` authorization, 31
user accreditation range, 23
users
authorizations for changing labels, 31
further label configuration, 107
printing authorizations, 93
workspace access, 92
`/usr/lib/cups/filter/tsol_separator.ps` file, 62
`/usr/share/X11/rgb.txt` file, 76

V

`value=` classification keyword, 46
values
of administrative classifications, 45
of classifications, 45
of compartments, 48
verifying
`label_encodings` file, 51
`label_encodings` file example, 113
`VERSION` section
description, 43
example, 100
`VERSION=` keyword, 43

W

word order requirements
`label_encodings` file, 44
words
planning, example of, 92
`WORDS` keyword, 44
workgroups
represented by label compartments, 48
worksheets
channels planner, 98
classifications planner, 94
clearances planner, 96
color planner, 99

compartments planner, 95
printer banners planner, 97
workspaces
access by users, 29, 92
labeled, 30