Solaris Trusted Extensions Installation and Configuration

Sun microsystems

Contents

Tables

Figures

Preface

This book is for knowledgeable system administrators and security administrators who are installing Solaris™ Trusted Extensions software. The level of trust that is required by your site security policy, and your level of expertise, determines who can perform the tasks that configure the software.

Note – This Solaris release supports systems that use the SPARC® and x86 families of processor architectures: UltraSPARC®, SPARC64, AMD64, Pentium, and Xeon EM64T. The supported systems appear in the *Solaris 10 Hardware Compatibility List* at `http://www.sun.com/bigadmin/hcl`. This document cites any implementation differences between the platform types.

In this document these x86 related terms mean the following:

- "x86" refers to the larger family of 64-bit and 32-bit x86 compatible products.
- "x64" points out specific 64-bit information about AMD64 or EM64T systems.
- "32-bit x86" points out specific 32-bit information about x86 based systems.

For supported systems, see the *Solaris 10 Hardware Compatibility List*.

Implementing Site Security

Successfully configuring Solaris Trusted Extensions (Trusted Extensions) on a system that is consistent with site security requires understanding the security features of Trusted Extensions and your site security policy. Before you install the Solaris Trusted Extensions packages, read Chapter 1 for information on how to ensure site security when configuring the software.

Trusted Extensions and the Solaris Operating System

Trusted Extensions installs on top of the Solaris Operating System (Solaris OS). Because Trusted Extensions software can modify the Solaris OS, Trusted Extensions can require specific settings for Solaris installation options. For details, see Chapter 3. Also, Solaris Trusted Extensions books supplement Solaris books. As administrators, you should have access to Solaris books and Solaris Trusted Extensions books.

How This Book is Organized

Chapter 1 describes the security issues when configuring Trusted Extensions software on one or more Solaris systems.

Chapter 2 contains task maps for adding Trusted Extensions software to Solaris systems.

Chapter 3 provides instructions for preparing a Solaris system for Solaris Trusted Extensions software, and then adding the packages.

Chapter 4 provides step-by-step instructions for configuring Trusted Extensions software on a system with a monitor.

Chapter 5 provides step-by-step instructions for configuring LDAP for Trusted Extensions.

Chapter 6 describes how to configure and administer Trusted Extensions software on a headless system.

Chapter 7 describes procedures and administration tools that are specific to Trusted Extensions software. These utilities are used when configuring the software.

Appendix A addresses site security policy and places Trusted Extensions in the context of wider organizational and site security.

Appendix B provides a checklist for the install team when configuring Trusted Extensions.

Glossary defines selected terms and phrases that are used in this book.

How the Solaris Trusted Extensions Books Are Organized

The Solaris Trusted Extensions 1.0 documentation set supplements the documentation for the Solaris 10 11/06 release. Obtain a copy of both sets for a complete understanding of Solaris Trusted Extensions. The Solaris Trusted Extensions documentation set consists of the following books.

Book Title	Topics	Audience
Solaris Trusted Extensions Transition Guide	Provides an overview of the differences between Trusted Solaris 8 software, Solaris 10 11/06 software, and Solaris Trusted Extensions 1.0 software.	All
Solaris Trusted Extensions Reference Manual	Provides Solaris Trusted Extensions man pages.	All
Solaris Trusted Extensions User's Guide	Describes the basic features of Solaris Trusted Extensions. This book contains a glossary.	End users, administrators, and developers

Book Title	Topics	Audience
Solaris Trusted Extensions Release Notes	Lists known problems and describes workarounds for Solaris Trusted Extensions 1.0 software.	Administrators, developers
Solaris Trusted Extensions Installation and Configuration	Describes how to plan for, install, and configure Solaris Trusted Extensions.	Administrators, developers
Solaris Trusted Extensions Administrator's Procedures	Provides detailed information for performing specific administration tasks.	Administrators, developers
Solaris Trusted Extensions Developer's Guide	Describes how to develop applications with Solaris Trusted Extensions.	Developers, administrators
Solaris Trusted Extensions Label Administration	Provides information on specifying label components in the label encodings file.	Administrators
Compartmented Mode Workstation Labeling: Encodings Format	Describes the syntax used in the label encodings file. The syntax enforces the various rules for well-formed labels for a system.	Administrators

Related Books from Sun Microsystems

The following books contain information that is useful when installing Solaris Trusted Extensions software.

Solaris Books

Solaris Express Installation Guide: Basic Installations: Provides guidance on installation options for the Solaris OS.

Solaris Express Installation Guide: Custom JumpStart and Advanced Installations: Provides guidance on disk space requirements, installation methods, and configuration options.

System Administration Guide: Basic Administration – Describes basic administrative tasks in the Solaris OS, such as creating and mounting file systems.

System Administration Guide: Advanced Administration – Describes more advanced administrative tasks in the Solaris OS, such as print management.

System Administration Guide: IP Services – Describes network configuration tasks in the Solaris OS.

System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP) – Describes the naming services in the Solaris OS.

System Administration Guide: Security Services – Describes the security features in the Solaris OS.

System Administration Guide: Solaris Containers-Resource Management and Solaris Zones – Describes the containment features in the Solaris OS.

Books From Elsewhere

Your site security policy document – Describes the security policy and security procedures at your site.

Solaris Common Desktop Environment: Advanced User's and System Administrator's Guide – Describes the Common Desktop Environment (CDE).

The administrator guide for your currently installed operating system – Describes how to back up system files.

Related Third-Party Web Site References

Third party URLs are referenced in this document and provide additional, related information.

Note – Sun is not responsible for the availability of third-party Web sites that are mentioned in this document. Sun does not endorse and is not responsible or liable for any content, advertising, products, or other materials that are available on or through such sites or resources. Sun will not be responsible or liable for any actual or alleged damage or loss caused by or in connection with the use of or reliance on any such content, goods, or services that are available on or through such sites or resources.

Documentation, Support, and Training

Sun Function	URL	Description
Documentation	http://www.sun.com/documentation/	Download PDF and HTML documents, and order printed documents
Support and Training	http://www.sun.com/supportraining/	Obtain technical support, download patches, and learn about Sun courses

Typographic Conventions

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

TABLE P–1 Typographic Conventions

Typeface or Symbol	Meaning	Example
`AaBbCc123`	The names of commands, files, and directories, and onscreen computer output	Edit your `.login` file. Use `ls -a` to list all files. `machine_name% you have mail.`
`AaBbCc123`	What you type, contrasted with onscreen computer output	`machine_name%` **`su`** `Password:`
aabbcc123	Placeholder: replace with a real name or value	The command to remove a file is `rm` *filename*.
AaBbCc123	Book titles, new terms, and terms to be emphasized	Read Chapter 6 in the *User's Guide*. Perform a *patch analysis*. Do *not* save the file. [Note that some emphasized items appear bold online.]

Shell Prompts in Command Examples

The following table shows the default system prompt, role prompt, and superuser prompt for the C shell, Bourne shell, and Korn shell.

TABLE P–2 Shell Prompts

Shell	Prompt
C shell prompt	`machine_name%`
C shell superuser prompt	`machine_name#`
Profile shell prompt	`$`
Bourne shell and Korn shell prompt	`$`
Bourne shell and Korn shell superuser prompt	`#`

1

Security Overview

Solaris Trusted Extensions implements a portion of your site's security policy in software. This chapter provides an overview of the security aspects and the administrative aspects of configuring the software.

- "Planning for Security" on page 17
- "Installation Results from an Administrator's Perspective" on page 27

Planning for Security

This section outlines the planning required before installing and configuring Trusted Extensions software.

- "Understanding Trusted Extensions" on page 18
- "Understanding Your Site's Security Policy" on page 18
- "Devising an Administration Strategy" on page 19
- "Devising a Label Strategy" on page 19
- "Planning System Hardware and Capacity" on page 20
- "Planning Your Network" on page 20
- "Planning for Auditing" on page 23
- "Planning User Security" on page 23
- "Devising an Installation and Configuration Strategy" on page 25
- "Collecting Information" on page 26
- "Backing Up the System" on page 26
- "Installing Solaris Trusted Extensions Software" on page 27

For a checklist of Trusted Extensions configuration tasks, see Appendix B. If you are interested in localizing your site, see "For International Customers" on page 20. If you are interested in running an evaluated configuration, see "Understanding Your Site's Security Policy" on page 18.

Understanding Trusted Extensions

Installation and configuration of Solaris Trusted Extensions involves more than loading executable files, entering your site's data, and setting configuration variables. It requires considerable background. Trusted Extensions software provides a labeled environment that is based on the following concepts:

- Capabilities that in most UNIX® environments are assigned to superuser are available to discrete administrative roles.

- In addition to UNIX permissions, access to data is controlled by special security tags. These tags are called sensitivity labels. Labels are assigned to users, processes, and objects, such as data files and directories.

- The ability to override security policy can be assigned to specific users and applications.

Understanding Your Site's Security Policy

Trusted Extensions effectively enables you to integrate your site's security policy with the Solaris OS. Thus, you need to have a good feel for the scope of your policy and the ability of Trusted Extensions software to accommodate it. A good configuration should provide a balance between consistency with your site security policy and convenience for those working on the system.

Trusted Extensions is configured by default to conform with the Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408) at Assurance Level EAL4 against the following protection profiles:

- Labeled Security Protection Profile
- Controlled Access Protection Profile
- Role-Based Access Control Protection Profile

To meet these evaluated levels, you must configure LDAP as the naming service. Note that your configuration might no longer conform with the evaluation if you do any of the following:

- Change the kernel switch settings in the `/etc/system` file.

- Turn off auditing or device allocation.

- Change the default entries in the following configurable files:
  - `/usr/openwin/server/etc/*`
  - `/usr/dt/app-defaults/C/Dt`
  - `/usr/dt/app-defaults/C/Dtwm`
  - `/usr/dt/app-defaults/C/SelectionManager`
  - `/usr/dt/bin/Xsession`
  - `/usr/dt/bin/Xtsolsession`
  - `/usr/dt/bin/Xtsolusersession`
  - `/usr/dt/config/sel_config`
  - `/usr/X11/lib/X11/xserver/TrustedExtensionsPolicy`

For more information on Common Criteria, see the Common Criteria
(http://commoncriteriaportal.org/) web site.

Devising an Administration Strategy

The root user or the System Administrator role is responsible for loading the packages from the
Solaris Trusted Extensions installation media.

- The security administrator is responsible for security-related tasks, such as setting up and
  assigning sensitivity labels, configuring auditing, and setting password policy.
- The system administrator is responsible for the non-security aspects of setup, maintenance, and
  general administration.
- The primary administrator is responsible for creating rights profile for the security administrator,
  and for fixing things when the security and system administrators do not have the power.
- More limited roles can be configured. For example, an "oper" for operator could be responsible
  for backing up files.

As part of your administration strategy, you need to make the following decisions:

- Which users are handling which administration responsibilities
- Which non-administrative users are allowed to run trusted applications, that is, are permitted to
  override security policy when necessary
- Which users have access to which groups of data

Devising a Label Strategy

Planning labels requires setting up a hierarchy of sensitivity levels and a categorization of
information in your system. The label encodings file contains this type of information for your
organization. You can use one of the label_encodings files that are supplied on the Solaris Trusted
Extensions installation media. You could also modify one of the supplied files, or create a new label
encodings file that is specific to your site. The file should include the Sun-specific local extensions, at
least the COLOR NAMES section, when used with Trusted Extensions.

Caution – You must have the final version of the label_encodings(4) file ready prior to adding the
Solaris Trusted Extensions packages. The file should be on removable media.

Planning labels also involves planning label configuration. After installation, you need to decide if
the system can run at a single label only, or if the system can run at multiple labels. If all of your
non-administrative users can operate at the same security label, select a single-label system.

If labels display and which label names are displayed can also be configured. For more information,
see *Solaris Trusted Extensions Label Administration*. You can also refer to *Compartmented Mode
Workstation Labeling: Encodings Format*.

For International Customers

When localizing a label_encodings file, international customers should localize the label names *only*. The administrative label names, ADMIN_HIGH and ADMIN_LOW, must not be localized. All labeled hosts that you contact, from any vendor, must have label names that match the label names in the your label_encodings file.

Trusted Extensions supports fewer locales than does the Solaris OS. When you are working in a locale that Trusted Extensions does not support, items that are specific to Trusted Extensions are not translated into your locale. Solaris software continues to be translated into your locale.

Planning System Hardware and Capacity

System hardware includes the system itself and its attached devices. Such devices include tape drives, microphones, CD-ROM drives, and disk packs. Hardware capacity includes system memory, network interfaces, and disk space.

- Follow the recommendations for installing a Solaris release, as described in "System Requirements and Recommendations" in *Solaris Express Installation Guide: Basic Installations*. Trusted Extensions features can add to those requirements: Memory over the minimum is required on the following systems:
  - Systems that run the Solaris Management Console, a required administrative GUI
  - Systems that run at more than one sensitivity label
  - Systems that are used by users who can assume an administrative role
- More disk space is required on the following systems:
  - Systems that store files at more than one label
  - Systems whose users can assume administrative roles

Planning Your Network

For help in planning network hardware, see Chapter 2, "Planning Your TCP/IP Network (Tasks)," in *System Administration Guide: IP Services*.

As in any client-server network, you need to identify hosts by their function, that is, server or client, and configure the software appropriately. For assistance in planning, see *Solaris Express Installation Guide: Custom JumpStart and Advanced Installations*.

Trusted Extensions software recognizes two host types, labeled and unlabeled. Each host type has a default security template, as shown in Table 1–1.

TABLE 1–1 Default Host Templates in Trusted Extensions

Host Type	Template Name	Purpose
unlabeled	admin_low	At initial boot, labels the global zone.
		After initial boot, for hosts that send unlabeled packets.
cipso	cipso	For hosts or networks that send CIPSO packets. CIPSO packets are labeled.

If your network is open to other networks, you need to specify accessible domains and hosts, and identify which Trusted Extensions hosts are going to be gateways. You need to identify the label accreditation range for these gateways, and the sensitivity label at which data from other hosts can be viewed.

The tnrhtp(4) man page gives a complete description of each host type with several examples.

Planning for Zones

Trusted Extensions software is added to the global zone, that is, to the Solaris OS. You then configure non-global zones that are labeled. You can create one labeled zone for every unique label, though you do not have to create a zone for every label.

Trusted Extensions Zones and Solaris 10 Zones

Labeled zones differ from typical Solaris 10 zones. Labeled zones are primarily used to segregate data. In Trusted Extensions, ordinary users cannot remotely log in to a labeled zone. The only interactive interface to a labeled zone is by using the zone console. Only root can gain access to the zone console.

Zone Creation

To create a labeled zone involves copying an entire operating system, and then starting the services for the Solaris OS in every zone. The process can be time-consuming. A faster process is to create one zone, then copy that zone or clone the contents of that zone. The following table describes your options when creating zones in Trusted Extensions.

Zone Creation Method	Effort Required	Characteristics of This Method
Create each labeled zone from scratch.	Configure, initialize, install, customize, and boot each labeled zone.	■ This method is supported, and is useful when creating one or two additional zones. The zones can be upgraded. ■ This method is time-consuming.

Zone Creation Method	Effort Required	Characteristics of This Method
Create additional labeled zones from a copy of the first labeled zone.	Configure, initialize, install, and customize one zone. Use this zone as a template for other labeled zones.	■ This method is supported, and is faster than creating zones from scratch. The zones can be upgraded. Use the Copy Zone method if you want Sun Support to help you with any zone difficulties. ■ This method uses UFS. UFS does not offer the additional isolation for the zones that ZFS offers.
Create additional labeled zones from a ZFS snapshot of the first labeled zone.	Set up a ZFS pool from a partition that you set aside during Solaris installation. Configure, initialize, install, and customize one zone. Use this zone as a ZFS snapshot for other labeled zones.	■ This method uses ZFS. This is the fastest method. This method makes every zone a file system, and thus provides more isolation than UFS. ZFS uses much less disk space. ■ If you are testing Trusted Extensions, and can reinstall the zones rather than upgrade, this method might be a good choice. It can be useful on systems whose contents are not volatile, because the system can quickly be reinstalled to a usable state. ■ This method is not supported. Zones that are created by using this method cannot be upgraded.

Solaris zones affect package installation and patching. For more information, see Chapter 24, "About Packages and Patches on a Solaris System With Zones Installed (Overview)," in *System Administration Guide: Solaris Containers-Resource Management and Solaris Zones*.

Planning for Multilevel Access

Typically, printing and NFS are configured as multilevel services. To access multilevel services, a properly configured system requires that every zone is able to access one or more network addresses. The following configurations provide multilevel services:

■ As in the Solaris OS, one IP address is assigned for every zone, including the global zone. A refinement of this configuration is to assign a separate network information card (NIC) to each zone. Such a configuration is used to physically separate the single-label networks that are associated with each NIC.

■ One all-zones address is assigned. One or more zones can have zone-specific addresses.

A system that satisfies the following two conditions cannot provide multilevel services:

- One IP address is assigned that the global zone and the labeled zones share.
- No zone-specific addresses are assigned.

If users in labeled zones are not supposed to have access to a local multilevel printer, and you do not need NFS exports of home directories, then you can assign one IP address to a system that you configure with Trusted Extensions. On such a system, multilevel printing is not supported, and home directories cannot be shared.

Planning for the LDAP Naming Service

If you are planning to install one or two labeled systems that are not networked to each other, then you can skip this section.

If you are installing a network of systems, LDAP is used by Trusted Extensions as a naming service. A populated Sun Java™ System Directory Server (LDAP server) is required when configuring several machines. If your site has an existing LDAP server, you can populate the server with Trusted Extensions databases. To access the information, you can set up an LDAP proxy on a Trusted Extensions system.

If your site does not have an existing LDAP server, you should plan to create an LDAP server on a system that is running Trusted Extensions software. The procedures are described in Chapter 5.

Planning for Auditing

Trusted Extensions turns on auditing. So, by default, `root` login and `root` logout are audited. To audit the users who are configuring the system, you can create roles early in the configuration process. For the procedure, see "Creating Roles and Users" on page 66.

Planning auditing is the same in Trusted Extensions as in the Solaris OS. For details, see Part VII, "Solaris Auditing," in *System Administration Guide: Security Services*. While Trusted Extensions adds classes, events, and audit tokens, the software does not change the way that auditing is administered. For Trusted Extensions additions to auditing, see Chapter 18, "Trusted Extensions Auditing," in *Solaris Trusted Extensions Administrator's Procedures*

Planning User Security

The software ships with reasonable security defaults for users. The security defaults are listed in the following table. Where two values are listed, the first value is the default. The security administrator can modify these defaults to reflect the site's security policy. After the security administrator has set the defaults, the system administrator can create all the users, who inherit the established defaults. For descriptions of the keywords and values for these two files, see the `label_encodings`(4) and `policy.conf`(4) man pages.

The system administrator can set up a standard user template that sets appropriate system defaults for every user. For example, by default each user's initial shell is a Bourne shell. The system administrator can set up a template that gives each user a C shell by default. For more information, see the Solaris Management Console online help for User Accounts.

TABLE 1–2 Solaris Trusted Extensions Security Defaults for User Accounts

File name	Keyword	Value
/etc/security/policy.conf	IDLECMD	lock | logout
	IDLETIME	30
	LABELVIEW	showsl | hidesl
	CRYPT_ALGORITHMS_ALLOW	1,2a,md5
	CRYPT_DEFAULT	_unix_
	LOCK_AFTER_RETRIES	no | yes
	PRIV_DEFAULT	basic
	PRIV_LIMIT	all
	AUTHS_GRANTED	solaris.device.cdrw
	PROFS_GRANTED	Basic Solaris User
LOCAL DEFINITIONS section of /etc/security/tsol/label_encodings	Default User Clearance	CNF NEED TO KNOW
	Default User Sensitivity Label	PUBLIC

Devising an Installation and Configuration Strategy

As in the Solaris OS, Solaris Trusted Extensions software is initially loaded by the root user. However, configuring the software by root is not a secure strategy. The following list describes the installation and configuration strategies from the most secure strategy to the least secure strategy.

- A two-person installation team installs and configures the software. The configuration process is audited.

  Two persons are at the computer when the software is loaded. Early in the configuration process, this team creates local users and roles. The team also sets up auditing to audit events that are executed by roles. Once roles have been assigned to users, and the computer is rebooted, the software enforces task division by role. The audit trail provides a record of the configuration process. For an illustration of a secure configuration process, see Figure 1–1.

- One person installs and configures the software by assuming the appropriate role. The configuration process is audited.

  Early in the configuration process, the root user creates a local user and roles. This user also sets up auditing to audit events that are executed by roles. Once roles have been assigned to the local user, and the computer is rebooted, the software enforces task division by role. The audit trail provides a record of the configuration process.

- One person installs and configures the software by assuming the appropriate role. The configuration process is not audited.

  By using this strategy, no record is kept of the configuration process.

- root installs and configures the software. The configuration process is audited.

  You set up auditing to audit every event that root performs during configuration. With this strategy, you must determine which events to audit. The audit trail does not include the name of the user who is acting as root.

- root installs and configures the software.

Task division by role is shown in the following figure. The security administrator sets up auditing, protects file systems, sets device policy, determines which programs require privilege to run, and protects users, among other tasks. The system administrator shares and mounts file systems, installs software packages, and creates users, among other tasks.
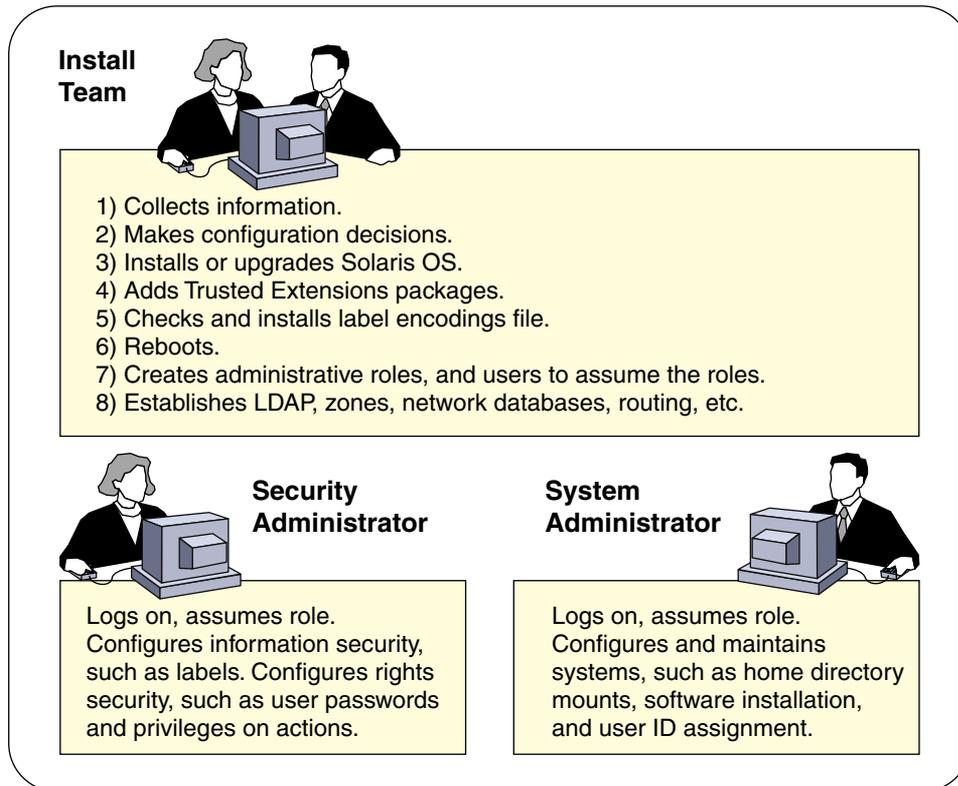
FIGURE 1–1 Two Roles Administering a System

Collecting Information

As when configuring Solaris, collect machine, user, network, and label before configuring Trusted Extensions. For details, see "Collect System Information Before Installing Trusted Extensions" on page 36.

Backing Up the System

If your system has files that should be saved, make sure to perform a backup. The safest way to back up files is to do a level 0 dump. If you do not have a backup procedure in place, see the administrator's guide to your current operating system for instructions.

> **Note** – If you are migrating from a Trusted Solaris 8 release, you can restore your data only if the Trusted Extensions labels are identical to the Trusted Solaris 8 labels. Because Trusted Extensions does not create multilevel directories, each file and directory on backup media is restored to a zone whose label is identical to the file label in the backup. Backup *must be completed* before installing the Solaris Trusted Extensions release.

Installing Solaris Trusted Extensions Software

Installing Trusted Extensions software means installing packages on a Solaris system. For security reasons, some of the options that are available for Solaris installation should not be chosen. For details, see "Installing or Upgrading the Solaris OS for Trusted Extensions (Tasks)" on page 33.

Installation Results from an Administrator's Perspective

After installing Trusted Extensions software, the following security features are in place. Many features are configurable by the security administrator.

- Auditing is enabled.
- A Sun label_encodings file is configured and installed.
- CDE creates four labeled workspaces in the global zone.
- As in the Solaris OS, rights profiles for roles are defined. As in the Solaris OS, roles are not defined.

  For roles to administer Trusted Extensions, you must create the roles. During configuration, you create the Security Administrator role.

- Three Trusted Extensions network databases, tnrhdb, tnrhtp, and tnzonecfg are installed. The databases are administered by using the Security Templates tool and the Trusted Network Zones tool in the Solaris Management Console.
- Trusted Extensions provides GUIs to administer the system. Some GUIs are extensions to a Solaris GUI.
  - In CDE, administrative actions are provided in the Trusted_Extensions folder. Some of these actions are used when initially configuring Trusted Extensions. The tools are introduced in Chapter 7. For a thorough description of the tools, see Chapter 2, "Trusted Extensions Administration Tools," in *Solaris Trusted Extensions Administrator's Procedures*.
  - A trusted editor enables administrators to modify local administrative files. In CDE, the Admin Editor action invokes a trusted editor.
  - The Device Allocation Manager manages attached devices.
  - The Solaris™ Management Console provides Java-based tools to manage local and network administrative databases. The use of these tools is required for managing the trusted network, zones, and users.

2

Installation and Configuration Roadmap

This chapter outlines the tasks for installing and configuring Solaris Trusted Extensions software.

Task Map: Preparing the Solaris OS for Trusted Extensions

Ensure that the Solaris OS on which you are installing Trusted Extensions supports the features of Trusted Extensions that you plan to use.

Do One of the Following Tasks	For Instructions
Prepare an existing or upgraded Solaris installation for Trusted Extensions.	"Prepare an Installed Solaris OS for Trusted Extensions" on page 35
Answer Solaris installation questions with Trusted Extensions features in mind.	"Answer Solaris Installation Questions for Trusted Extensions" on page 34

Task Map: Preparing For and Installing Trusted Extensions

Task	For Instructions
Complete the preparation of your Solaris system.	"Task Map: Preparing the Solaris OS for Trusted Extensions" on page 29
Back up a Trusted Solaris 8 system.	Back up your systems as described in the documentation for your release. A labeled backup can be restored to each identically labeled zone.
Back up a Solaris system.	*System Administration Guide: Basic Administration*
Gather information and make decisions about your system and your Trusted Extensions network.	"Collecting Information and Making Decisions Before Installing Trusted Extensions (Tasks)" on page 36

Task	For Instructions
Load the Trusted Extensions software packages.	"Add the Solaris Trusted Extensions Packages" on page 39

Task Map: Configuring Trusted Extensions

For secure installation, create roles early in the configuration process. The order of tasks when configuring as a role is shown in the following task map.

Task	Description	For Instructions
1. Protect the hardware.	Machine hardware can be protected by requiring a password to change hardware settings.	"Controlling Access to System Hardware" in *System Administration Guide: Security Services*
2. Configure labels.	Labels *must* be configured for your site. If you plan to use the default label_encodings file, you can skip this task.	"Check and Install Your Label Encodings File" on page 42
3. Enable IPv6 networking.	If you are running an IPv6 network, you modify a system file to enable IP to recognize labeled packets.	"Enable IPv6 Networking" on page 44
4. Reboot and log in.	After logging in, you are in the global zone. The system is using the label_encodings file to enforce mandatory access control (MAC).	"Reboot and Log In" on page 44
5. Create administrative roles and users for those roles locally.	Create the Security Administrator role, and other roles that you plan to use locally. You create these roles just as you would create them in the Solaris OS. You can delay this task until the end. For the effects of a delay, see "Devising an Installation and Configuration Strategy" on page 25.	"Creating Roles and Users" on page 66 "Verify That the Roles Work" on page 70
6a. Configure LDAP service for the trusted domain.	If you plan to use files to administer Trusted Extensions, you can skip the LDAP steps. If you have an existing Sun Java System Directory Server (LDAP server), you add Trusted Extensions databases to the server. Then you make your first Trusted Extensions system a proxy of the LDAP server. If you do not have an LDAP server, then you configure your first system as the server.	Chapter 5

Task	Description	For Instructions
6b. Configure the Solaris Management Console to work with the Sun Java System Directory Server.	You manually set up an LDAP toolbox for the Solaris Management Console. The toolbox can modify Trusted Extensions attributes on network objects.	"Configuring the Solaris Management Console for LDAP (Tasks)" on page 91
6c. Make the global zone an LDAP client.	For systems that are not the LDAP server or proxy server, make them an LDAP client.	"Make the Global Zone an LDAP Client" on page 45
6d. Create administrative roles and users for those roles on the network.	In the LDAP scope, create the Security Administrator role, and other roles that you plan to use. You can delay this task until the end. For pros and cons, see "Devising an Installation and Configuration Strategy" on page 25.	"Creating Roles and Users" on page 66 "Verify That the Roles Work" on page 70
7a. Identify zone interfaces, names, and labels.	Before creating the first labeled zone, identify the IP addresses, labels, and names of all the labeled zones that you plan to create.	"Preparing to Create Zones (Tasks)" on page 54
7b. Create labeled zones.	You have three options for creating multiple labeled zones. The options differ in speed of creation, disk space requirements, and robustness. If you decide to use the Clone Zone creation method, create a ZFS pool. Create your first labeled zone, then create the rest by the method that you have chosen.	"Creating the Labeled Zones (Tasks)" on page 59
8. Configure labeled networking.	Identify additional remote hosts that require a label, one or more multilevel ports, and a different control message policy.	"Specify Labels for Network Interfaces" on page 57
9. Configure home directories.	Create a multilevel home directory server, then automount the installed zones.	"Creating Home Directories" on page 71
10. Do other system and network configuration tasks.	Configure auditing, mount file systems, and do other tasks before enabling users to log in to the system.	"Finishing Up Trusted Extensions Configuration (Task Map)" on page 77
11. Add a user to an existing Trusted Extensions network.	Add users from a NIS environment to your LDAP server.	"Add a NIS User to the LDAP Server" on page 75
12. Add a host to an existing Trusted Extensions network.	Add a host and its labeled zones to the LDAP server.	"Add a Host to the LDAP Server" on page 77

Task Map: Configuring Trusted Extensions on a Headless System

Task	For Instructions
Enable a headless system to be administered remotely.	"Enable Remote Login" on page 98
Enable a headless system to be configured by using CDE actions from a desktop system.	"Use `dtappsession` to Log In to a Headless System" on page 100
Enable a headless system to be configured remotely from a desktop system that is running the Solaris Management Console.	"Set Up Remote Solaris Management Console Login to a Headless System" on page 101
Enable a headless system to be administered over a serial line.	"Set Up Administration by Serial Login" on page 102

Installing Solaris Trusted Extensions Software

This chapter describes how to prepare the Solaris Operating System (Solaris OS) for Trusted Extensions installation. This chapter also describes what information you should have before adding the Trusted Extensions packages, and then how to add the packages.

- "Install Team Responsibilities" on page 33
- "Collecting Information and Making Decisions Before Installing Trusted Extensions (Tasks)" on page 36
- "Installing or Upgrading the Solaris OS for Trusted Extensions (Tasks)" on page 33
- "Installing the Solaris Trusted Extensions Packages (Tasks)" on page 39

Install Team Responsibilities

Solaris Trusted Extensions software is designed to be installed and configured by two people with distinct responsibilities. However, the installation program does not enforce two-role task division. Task division is enforced by roles. Because roles and users are not created until after installation, it is good practice to have an install team of at least two persons present when installing Trusted Extensions software.

Installing or Upgrading the Solaris OS for Trusted Extensions (Tasks)

The choice of Solaris installation options can affect the use and security of Trusted Extensions.

- To properly install Trusted Extensions, you should install the underlying Solaris OS securely. For Solaris installation choices that affect Trusted Extensions, see "Answer Solaris Installation Questions for Trusted Extensions" on page 34.
- If you have been using the Solaris OS, check your current configuration against the requirements for Trusted Extensions. For configuration choices that affect Trusted Extensions, see "Prepare an Installed Solaris OS for Trusted Extensions" on page 35.

▼ Answer Solaris Installation Questions for Trusted Extensions

This task applies to fresh installations of the Solaris OS. If you are upgrading, see "Prepare an Installed Solaris OS for Trusted Extensions" on page 35

◗ **Take the recommended action on the following installation choices.**

The choices are presented in the order of Solaris installation questions. Installation questions that are not mentioned in this table do not affect Trusted Extensions.

Solaris Option	Trusted Extensions Behavior	Recommended Action
NIS naming service NIS+ naming service	Trusted Extensions supports files and LDAP for a naming service. For host name resolution, DNS can be used.	Do not choose NIS or NIS+. You can choose None, which is equivalent to files. Later, you can configure LDAP to work with Trusted Extensions.
Upgrade	Trusted Extensions installs labeled zones with particular security characteristics.	If you are upgrading, go to "Prepare an Installed Solaris OS for Trusted Extensions" on page 35.
root password	Administration tools in Trusted Extensions require passwords. If root does not have a password, root cannot configure the system.	Provide a root password. Leave the default crypt_unix password encryption method. For details, see "Managing Password Information" in *System Administration Guide: Security Services*.
Developer Group	Trusted Extensions uses the Solaris Management Console to administer the network. The End User group and smaller groups do not install the packages for the Solaris Management Console.	On any system that you plan to use to administer remotely or to administer from, do not install the End User, Core, or Reduced Networking Group.
Select Products	You can install Java ES Software from this screen.	Do not select Solaris 10 Extra Value Software. You add Trusted Extensions software later, in "Installing the Solaris Trusted Extensions Packages (Tasks)" on page 39.
Custom Install	Because Trusted Extensions installs zones, you might need more space in partitions than the default install supplies.	Choose Custom Install, and lay out the partitions. Consider adding extra swap for roles. If you are going to clone zones, create a 1000MByte partition for the ZFS pool. For auditing files, best practice is to create a dedicated partition.

▼ Prepare an Installed Solaris OS for Trusted Extensions

This task applies to Solaris systems that have been in use, and on which you plan to add Trusted Extensions packages. Also, if you are upgrading a Solaris 10 system, follow this procedure. Other tasks that might modify an installed Solaris system can be done after the Trusted Extensions packages have been added.

1   If your system is part of a cluster, Trusted Extensions cannot be installed.

2   The installation of Trusted Extensions into an alternate boot environment (BE) is not supported.

Trusted Extensions can only be installed into the current boot environment.

If live_upgrade tools have been used to install the Solaris OS on an alternate BE, the alternate BE must first be activated, and the system booted from the new BE before Trusted Extensions packages are added. Live upgrade and BE are explained in the live_upgrade(5) man page.

3   If non-global zones are installed on your system, remove them.

Or, you can re-install the Solaris OS. If you are going to re-install, follow the instructions in "Answer Solaris Installation Questions for Trusted Extensions" on page 34.

4   If you are not using the LDAP naming service, plan to configure LDAP for your site.

The NIS and NIS+ naming services cannot be used with Trusted Extensions. If you are installing one or two systems, use local files. For larger sites, after adding the Trusted Extensions packages, follow the instructions in Chapter 5 to configure LDAP.

5   If your system does not have a root password, create one.

Administration tools in Trusted Extensions require passwords. If root does not have a password, root cannot configure the system.

Use the default crypt_unix password encryption method. For details, see "Managing Password Information" in *System Administration Guide: Security Services*.

Note – Users must not disclose their passwords to another person, as that person might then have access to the data of the user and will not be uniquely identified or accountable. Note that disclosure can be direct, through the user deliberately disclosing her/his password to another person, or indirect, for example, through writing it down, or choosing an insecure password. The Solaris OS provides protection against insecure passwords, but cannot prevent a user disclosing her or his password, or from writing it down.

---

6   Add the Solaris packages for the Solaris Management Console.

Trusted Extensions uses the Solaris Management Console to administer the network. If your system was installed with the End User group or a smaller group, the system does not have the packages for the Solaris Management Console. These packages are required only if you plan to administer the site from this system.

7   If you have created an `xorg.conf` **file, you need to modify it.**

Add the following line to the end of the `xorg.conf` file.

```
load "xtsol"
```

Note – By default, the `xorg.conf` file does not exist. Do nothing if this file does not exist.

8   If you want to clone zones, create a partition for the ZFS pool.

To decide on your zone creation method, see "Planning for Zones" on page 21.

9   (Optional) Check that your partitions have sufficient space for zones.

Most systems that are configured with Trusted Extensions install labeled zones. Labeled zones can require more disk space than the installed system has set aside.

However, some Trusted Extensions systems do not require that labeled zones be installed. For example, a multilevel printing server, a multilevel LDAP server, or a multilevel LDAP proxy server do not require labeled zones to be installed. These systems might not need the extra disk space.

10   (Optional) Add extra swap space for roles.

Roles administer Trusted Extensions. Consider adding extra swap for role processes.

11   (Optional) Dedicate a partition for audit files.

Trusted Extensions enables auditing by default. For audit files, best practice is to create a dedicated partition.

Collecting Information and Making Decisions Before Installing Trusted Extensions (Tasks)

For each system on which Solaris Trusted Extensions is going to be configured, you need to know some information, and make some decisions about configuration. For example, because you are going to create labeled zones, you might want to set aside disk space where the zones can be cloned as ZFS. ZFS provides additional isolation for the zones.

▼ Collect System Information Before Installing Trusted Extensions

1   Determine the machine's main hostname and IP address.

This is the name of the host on the network, and is the global zone. On a Solaris system, the `getent` command returns the hostname, as in:

```
# getent hosts machine1
192.168.0.11    machine1
```

2 Make the IP address assignments for labeled zones.

A system with two IP addresses can function as a multilevel server. A system with one IP address must have access to a multilevel server in order to print, or do multilevel tasks. For a discussion of IP address options, see "Planning for Multilevel Access" on page 22.

Most systems require a second IP address for the labeled zones. For example, on a host with a second IP address for labeled zones:

```
# getent hosts machine1-zones
192.168.0.12    machine1-zones
```

3 Determine the machine's ethernet hardware address.

If the machine is already installed, the address can be found in the last line of the output by using the ifconfig *device* command.

```
# ifconfig hme0
hme0: flags=1000843<UP,
...
     ether 8:0:20:cf:8c:4b
```

The ethernet address is needed if you are installing from the network.

4 Collect LDAP configuration information.

For the LDAP server that is running Trusted Extensions software, you need the following information:

- Name of the Trusted Extensions domain that the LDAP server serves
- IP address of the LDAP server
- LDAP profile name that should be loaded

For an LDAP proxy server, you also need the password for the LDAP proxy.

▼ Make System and Security Decisions Before Installing Trusted Extensions

For each system on which Solaris Trusted Extensions is going to be configured, make these configuration decisions before installing the packages.

1 Decide how securely the machine hardware should be protected.

At a secure site, this step has been done for every installed Solaris system.

- For SPARC systems, specify a PROM security level and provide a password.
- For x86 systems, protect the BIOS.
- On all systems, root is protected with a password.

2 Determine the source of your label_encodings file.

Decide which label_encodings file to use.

If you have a site-specific `label_encodings` file, the file must be checked and installed before other configuration tasks can be started. If your site does not have a `label_encodings` file, you can use the default file that Sun supplies. Sun also supplies other `label_encodings` files, which you can find in the `/etc/security/tsol` directory. The Sun files are demonstration files. They might not be suitable for production systems.

To customize a file for your site, see *Solaris Trusted Extensions Label Administration*.

3   From the list of labels in your `label_encodings` **file, make a list of the labeled zones to create.**

For the default `label_encodings` file, the labels are the following, and the zone names can be similar to the following:

Label	Zone Name
PUBLIC	public
CONFIDENTIAL : INTERNAL	internal
CONFIDENTIAL : NEED TO KNOW	needtoknow
CONFIDENTIAL : RESTRICTED	restricted

For ease of NFS mounting, the zone name of a particular label should be identical on every system. Some systems, such as multilevel print servers, do not need to have labeled zones installed. However, if you do install labeled zones on a print server, the zone names should be identical to the zone names of other systems on your network.

4   Decide when to create roles.

Your site's security policy can require you to administer Trusted Extensions by assuming a role. If your site requires this, or if you are configuring the system to satisfy criteria for an evaluated configuration, you should create roles early in the configuration process.

If you are not required to configure the system by using roles, you can choose to configure the system as superuser. This method of configuration is less secure. Audit records do not indicate which user was superuser during configuration. Superuser can do all tasks on the system, while a role has a more limited set of tasks. Therefore, configuration is more controlled when being done by roles.

5   Choose a zone creation method.

You can create zones from scratch, copy zones, or clone zones. These methods differ in speed of creation, disk space requirements, and robustness. For the trade-offs, see "Planning for Zones" on page 21.

6   Plan your LDAP configuration.

Using local files for administration is practical for non-networked systems. LDAP is the name service for a networked environment. A populated LDAP server is required when configuring several machines.

- If you have an existing Sun Java System Directory Server (LDAP server), you can create an LDAP proxy server on a system that is running Trusted Extensions. The multilevel proxy server handles communications with the unlabeled LDAP server.

- If you do not have an LDAP server, you can configure a system that runs Trusted Extensions software as a multilevel LDAP server.

7 Decide other security issues for each system and for the network.

For example, you might want to consider the following security issues:

- Specify what devices can be attached to the system and allocated for use

- Identify which printers at what labels are accessible from the system

- Identify any systems that have a limited label range, such as a gateway system or a public kiosk

- Identify which labeled systems can communicate with particular unlabeled systems

Installing the Solaris Trusted Extensions Packages (Tasks)

Before you install the packages, you should have completed the tasks in "Installing or Upgrading the Solaris OS for Trusted Extensions (Tasks)" on page 33 and "Collecting Information and Making Decisions Before Installing Trusted Extensions (Tasks)" on page 36.

▼ Add the Solaris Trusted Extensions Packages

Packages can be added by using the Java wizard or the pkgadd command. For options to the pkgadd command, see the pkgadd(1M) man page.

Before You Begin   You have completed the appropriate procedure in "Installing or Upgrading the Solaris OS for Trusted Extensions (Tasks)" on page 33.

1 Insert the Solaris installation media.

2 Navigate to the Trusted_Extensions **directory.**

cd Solaris_*release-number***/ExtraValue/CoBundled/Trusted_Extensions**

3 Load all packages.

Choose one of the following two options.

- **Use the Java wizard.**

    # **java wizard**

- **From the** Packages **directory, use the** pkgadd **command.**

  ```
  # cd Packages
  # pkgadd -d .
  ```

  a. **Press Return to load all the packages.**

     Press Return

  b. **Answer** yes **to all the prompts.**

     ```
     y
     y
     ...
     ```

4   Check for proper installation of the packages.

- **In the wizard, click the Details button.**

- **From the command line, scroll back through the log.**

  You can also go to the install log directory and read the log.

  Tip – You can also use the pkginfo command to see that the packages installed.

  ```
  # pkginfo | grep Trust
  system      SUNWdttshelp          Trusted Extensions, CDE Desktop Help
  system      SUNWdttsr             Trusted Extensions, CDE Desktop, (Root)
  system      SUNWdttsu             Trusted Extensions, CDE Desktop, (Usr)
  system      SUNWmgts              Trusted Extensions, SMC
  system      SUNWtsg               Trusted Extensions global
  system      SUNWtsman             Trusted Extensions Man Pages
  application SUNWtsmc              Trusted Extensions SMC Server
  system      SUNWtsr               Trusted Extensions, (Root)
  system      SUNWtsu               Trusted Extensions, (Usr)
  system      SUNWxwts              Trusted Extensions, X Window System
  ```

Troubleshooting   **Java wizard** – If the message Exception in thread "main" java.lang.NoClassDefFoundError: wizard, then you invoked the wizard from the wrong directory.

◆ ◆ ◆   **C H A P T E R   4**

4
Configuring Trusted Extensions

This chapter covers how to configure Trusted Extensions on a system with a monitor. To work properly, Trusted Extensions software requires label, zones, network, role, and tools configuration.

Getting Started

You should already have made decisions about your configuration. For the decisions, see "Collecting Information and Making Decisions Before Installing Trusted Extensions (Tasks)" on page 36.

Protecting Hardware, Loading Labels, and Using a Naming Service (Tasks)

Task	Description	For Instructions
Protect the hardware.	Machine hardware can be protected by requiring a password to change hardware settings.	"Controlling Access to System Hardware" in *System Administration Guide: Security Services*
Configure labels.	Labels *must* be configured for your site. If you plan to use the default label_encodings file, you can skip this step.	"Check and Install Your Label Encodings File" on page 42

Task	Description	For Instructions
For IPv6, modify /etc/system file.	If your network uses IPv6, this task is required. If your network uses IPv4, skip this step.	"Enable IPv6 Networking" on page 44
Reboot and log in.	Upon login, you are in the global zone, in an environment that recognizes and enforces mandatory access control (MAC).	"Reboot and Log In" on page 44
Configure LDAP service for the trusted domain.	If you have an existing LDAP server, you add Trusted Extensions databases to the server. Then you make a Trusted Extensions host a proxy of the LDAP server. If you do not have an LDAP server, then you configure a Trusted Extensions host as the server.	Chapter 5
Make the global zone an LDAP client.	For systems that are not the LDAP server or proxy server, make them an LDAP client.	"Make the Global Zone an LDAP Client" on page 45
Identify zone interfaces, names, and labels.	Before creating the first labeled zone, identify the IP addresses, labels, and names of all the labeled zones that you plan to create.	"Preparing to Create Zones (Tasks)" on page 54

▼ Check and Install Your Label Encodings File

Your encodings file must be compatible with any Trusted Extensions host with which you are communicating.

Note – Trusted Extensions installs a default label_encodings file. This default file is useful for demos. However, this file might not be a good choice for your use. If you plan to use the default file, you can skip this step.

- If you are familiar with encodings files, you can use the following procedure.
- If you are not familiar with encodings files, consult *Solaris Trusted Extensions Label Administration* for requirements, procedures, and examples.

⚠ **Caution –** You *must* successfully install labels before continuing or the configuration will fail.

Before You Begin You have just added the Trusted Extensions packages, so you are already logged in. "You" refers to the security administrator.

The security administrator is responsible for editing, checking, and maintaining the label_encodings file. If you plan to edit the label_encodings file, make sure that the file itself is writable.

For more information, see the label_encodings(4) man page.

1   Allocate the appropriate device.

To allocate a device, see "How to Allocate a Device" on page 109

2   Load the label_encodings **file from the allocated device.**

3   Check the syntax of the new label encodings file.

   a.   Open the Trusted_Extensions folder.

   Click mouse button 3 on the background.

   b.   In the Workspace menu, choose Applications → Application Manager.

   c.   Double-click the Trusted_Extensions folder icon.

4   Double-click the Check Encodings action.

In the dialog box, enter the full path name to the file:

/full-pathname-of-label-encodings-file

5   Read the contents of the Check Encodings dialog box that is displayed.

The chk_encodings command checks the syntax of the file.

6   Do one of the following:

CONTINUE	Only if Check Encodings reports no errors can you continue configuring. Go to Step 7.
RESOLVE ERRORS	If Check Encodings reports errors, the errors *must* be resolved before continuing. For assistance, see Chapter 3, "Making a Label Encodings File (Tasks)," in *Solaris Trusted Extensions Label Administration*.

7   If the file passes the check, click Yes.

The Check Encodings action creates a backup copy of the original file, then installs the checked version. The action then restarts the label daemon.

> ⚠ **Caution –** Your label encodings file *must* pass the Check Encodings test before you continue.

8   Deallocate the device.

To deallocate the device, see "How to Deallocate a Device" on page 110.

▼ Enable IPv6 Networking

When IPv6 is disabled, Trusted Extensions cannot forward IPv6 packets with CIPSO options. To enable an IPv6 network in Trusted Extensions requires an entry in /etc/system.

▶ **Type the following entry into the** /etc/system **file.**

```
set ip:ip6opt_ls = 0x0a
```

Troubleshooting   Error messages when booting indicate that your IPv6 configuration is incorrect. To correct the entry, do the following:

- Check that the entry is spelled correctly.
- Check that the system has been rebooted after adding the correct entry to the /etc/system file.

If you install Trusted Extensions on a Solaris system that currently has IPv6 enabled, but fail to add the IP entry in /etc/system, you see the following error message: t_optmgmt: System error: Cannot assign requested address *time-stamp*

If you install Trusted Extensions on a Solaris system that has not enabled IPv6, and fail to add the IP entry in /etc/system, you see the following types of error messages:

- WARNING: IPv6 not enabled via /etc/system
- Failed to configure IPv6 interface(s): hme0
- rpcbind: Unable to join IPv6 multicast group for rpc broadcast *broadcast-number*

▼ Reboot and Log In

At most sites, two or more administrators, an install team, are present when configuring the system. "You", in the following procedures, refers to the install team.

1   Reboot.

```
# /usr/sbin/reboot
```

2   Log in.

You are logging in to the Solaris Trusted Extensions (CDE) desktop.

3   Log in as superuser.

Type root and the root password.

Users must not disclose their passwords to another person, as that person might then have access to the data of the user and will not be uniquely identified or accountable. Note that disclosure can be direct, through the user deliberately disclosing his/her password to another person, or indirect, such

as through writing it down, or choosing an insecure password. Solaris Trusted Extensions software provides protection against insecure passwords, but cannot prevent a user disclosing his/her password or writing it down.

4   Read the Last Login dialog box.

```
                     Last Login: Thu Oct 09 17:05:25 2006 on console
    ┌─Message Of The Day──────────────────────────────────────────────────┐
    │ Sun Microsystems Inc.   SunOS 5.11    Oct. 10, 2006              ▲   │
    │ Solaris Trusted Extensions                                          │
    │                                                                 ▼   │
    └─────────────────────────────────────────────────────────────────────┘

    ┌─Session Attributes for Lokanath Das─────────────────────────────────┐
    │ Rights:  All                                                    ▲   │
    │ Roles:  root,admin                                                  │
    │ Minimum Label: PUBLIC                                               │
    │ Clearance: CONFIDENTIAL INTERNAL USE ONLY                          │
    │ Current Desktop: Solaris Trusted Extensions (CDE)                  │
    │ Idle Time before session lock: 30 minutes                      ▼   │
    └─────────────────────────────────────────────────────────────────────┘

                       ⊔ Restrict Session To A Single Label

                              ┌────────┐
                              │   OK   │
                              └────────┘
```

Then click OK to dismiss the box.

5   Read the Label Builder.

Click OK to accept the default label.

Once the login process is complete, the Trusted Extensions screen appears briefly, and you are in a CDE session with four workspaces. The Trusted Path symbol is displayed in the trusted stripe.

Note – You must log off or activate the lockscreen functionality before leaving a system unattended. Otherwise, a person can access the system without having to pass identification and authentication, and that person would not be uniquely identified or accountable.

▼ Make the Global Zone an LDAP Client

This completes the naming service configuration for the global zone.

Before You Begin   The Sun Java System Directory Server, that is, the LDAP server, must exist. The server must be populated with Trusted Extensions databases, and this system must be able to contact the server. So, this system must be an entry in the tnrhdb database on the LDAP server, or must be included in a wildcard entry.

If an LDAP server that is configured with Trusted Extensions does not exist, you must complete Chapter 5 before you attempt this procedure.

1 Save a copy of the original nsswitch.ldap **file.**

The standard naming service switch file for LDAP is too restrictive.

```
# cd /etc
# cp nsswitch.ldap nsswitch.ldap.orig
```

2 If you are using DNS, change the entries for the following services in the nsswitch.ldap **file.**

The correct entries are similar to the following:

```
hosts:      files dns ldap

ipnodes:    files dns ldap

networks:   ldap files
protocols:  ldap files
rpc:        ldap files
ethers:     ldap files
netmasks:   ldap files
bootparams: ldap files
publickey:  ldap files

services:   files
```

Note that Trusted Extensions adds two entries:

```
tnrhtp:     files ldap
tnrhdb:     files ldap
```

3 Copy the modified nsswitch.ldap **file to** nsswitch.conf**.**

```
# cp nsswitch.ldap nsswitch.conf
```

4 Navigate to the Trusted_Extensions folder.

a. Click mouse button 3 on the background.

b. From the Workspace menu, choose Applications → Application Manager.

c. Double-click the Trusted_Extensions folder icon.

This folder contains actions that set up interfaces, LDAP clients, and labeled zones.

5 Double-click the Create LDAP Client action.

Answer the prompts.

```
Domain Name:                Type the domain name
Hostname of LDAP Server:    Type the name of the server
IP Address of LDAP Server:  Type the IP address
LDAP Proxy Password:        Type the password to the server
Profile Name:               Type the profile name
```

6 When a completion message appears, close the action window.

```
global zone will be LDAP client of LDAP-server
System successfully configured.

*** Select Close or Exit from the window menu to close this window ***
```

7 Verify that the information is correct on the server.

a. Open a terminal, and query the LDAP server.

```
# ldapclient list
```

The output looks similar to the following:

```
NS_LDAP_FILE_VERSION= 2.0
NS_LDAP_BINDDN= cn=proxyagent,ou=profile,dc=domain-name
...
NS_LDAP_BIND_TIME= number
```

b. Correct any errors.

If you get an error, run the Create LDAP Client action with the correct values. For example, the following error can indicate that the system does not have an entry on the LDAP server:

```
LDAP ERROR (91): Can't connect to the LDAP server.
Failed to find defaultSearchBase for domain domain-name
```

Check the LDAP server.

Associating IP Addresses With Zones (Tasks)

Do only one of the following tasks. For the trade-offs, see "Planning for Multilevel Access" on page 22.

Task	Description	For Instructions
Share a logical interface	Map the global zone to one IP address, and all labeled zones to a different IP address.	"Specify Two IP Addresses for the System" on page 48

Task	Description	For Instructions
Do not share any IP addresses	Assign one IP address to every zone.	
Do not share any interfaces	Assign one network interface card (NIC) to every zone.	
Share a physical interface	Map all zones to one IP address.	

▼ Specify Two IP Addresses for the System

In this configuration, the host's address applies only to the global zone. Labeled zones share a second IP address with the global zone. In CDE, an action is provided to simplify this procedure.

Before You Begin You are superuser in the global zone.

1 Open the Trusted_Extensions folder.

For details, see .

2 Run the Share Logical Interface action.

Double-click Share Logical Interface and answer the prompts.

Note – The system must already have been assigned two IP addresses. For this action, provide the second address and a host name for that address. The second address is the shared address.

```
Hostname:        Type the name for your labeled zones interface
IP Address:      Type the IP address for the interface
```

This action configures a host with more than one IP address. The IP address for the global zone is the name of the host. The IP address for a labeled zone has a different host name. In addition, the IP address for the labeled zones is shared with the global zone. When this configuration is used, labeled zones are able to reach a network printer.

Tip – Use a standard naming convention for labeled zones. For example, add -zones to the host name.

---

3 (Optional) Verify the results of the action.

Use the ifconfig -a command. For example, the following output shows a shared logical interface, hme0:3 on network interface 192.168.0.12 for the labeled zones. The hme0 interface is the unique IP address of the global zone.

```
# ifconfig -a
 lo0: flags=2001000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4,VIRTUAL> mtu 8232 index 1
         inet 127.0.0.1 netmask ff000000
```

```
       hme0: flags=1000843<BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
               inet 192.168.0.11 netmask ffffff00 broadcast 192.168.0.255
       hme0:3 flags=1000843<BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
               inet 192.168.0.12 netmask ffffff00 broadcast 192.168.0.255
```

Example 4–1   Assigning Two Interfaces – One for the Global Zone and One for the Labeled Zones

On a system where the global zone has a unique interface, and labeled zones share a second interface with the global zone, the /etc/hosts file would appear similar to the following:

```
# cat /etc/hosts
...
127.0.0.1  localhost
192.168.0.11 machine1 loghost
192.168.0.12 machine1-zones
```

In the default configuration, the tnrhdb file would appear similar to the following:

```
# cat /etc/security/tsol/tnrhdb
...
127.0.0.1:cipso
192.168.0.11:cipso
192.168.0.12:cipso
0.0.0.0:admin_low
```

▼ Specify One IP Address Per Zone on the System

If you have an IP address for every labeled zone, follow this procedure. You configure the interfaces as you would configure them on a Solaris system.

Before You Begin   You are superuser in the global zone. You must have decided on the names of every labeled zone, as described in "Make System and Security Decisions Before Installing Trusted Extensions" on page 37.

Tip – Use a standard naming convention for labeled zones. For example, add -*label* to the host name.

---

1   **In a terminal, configure each computer interface.**

Use the zonecfg -z *zone-name* command. For details, see the zonecfg(1M) man page. The following are examples only. The command is interactive. The interactive display is shown in the first example.

```
# zonecfg -z public
zonecfg:public> add net
zonecfg:public:net> set address=10.8.57.131/24
zonecfg:public:net> set physical=ce0
zonecfg:public:net> end
```

```
zonecfg:public> add net
zonecfg:public:net> set address=fe80::130:1/10
zonecfg:public:net> set physical=ce0
zonecfg:public:net> end
zonecfg:public> add net
zonecfg:public:net> set address=2001:a08:3903:1::130:1/64
zonecfg:public:net> set physical=ce0
zonecfg:public:net> end
zonecfg:public> commit
zonecfg:public> exit

# zonecfg -z internal
add net
        set address=10.8.57.133/24
        set physical=ce0
end
add net
        set address=fe80::130:2/10
        set physical=ce0
end
add net
        set address=2001:a08:3903:1::130:2/64
        set physical=ce0
end
commit
exit

# zonecfg -z needtoknow
add net
        set address=10.8.57.134/24
        set physical=ce0
end
add net
        set address=fe80::130:3/10
        set physical=ce0
end
add net
        set address=2001:a08:3903:1::130:3/64
        set physical=ce0
end
commit
exit

# zonecfg -z restricted
add net
        set address=10.8.57.135/24
        set physical=ce0
end
```

```
add net
        set address=fe80::130:4/10
        set physical=ce0
end
add net
        set address=2001:a08:3903:1::130:4/64
        set physical=ce0
end
commit
exit
```

2   (Optional) Verify the results of the action.

Use the ifconfig -a command. For example, the following excerpts show the INTERNAL interfaces.

```
# ifconfig -a
lo0: flags=2001000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4,VIRTUAL> mtu 8232 index 1
        inet 127.0.0.1 netmask ff000000
...
lo0:2: flags=2001000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4,VIRTUAL> mtu 8232 index 1
        zone internal
        inet 127.0.0.1 netmask ff000000
...
ce0: flags=1004843<UP,BROADCAST,RUNNING,MULTICAST,DHCP,IPv4> mtu 1500 index 2
        inet 10.8.57.130 netmask ffffff00 broadcast 10.8.57.255
        ether 0:e:c:8:0:fc
...
ce0:2: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
        zone internal
        inet 10.8.57.133 netmask ffffff00 broadcast 10.8.57.255
...
lo0: flags=2001000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv6,VIRTUAL> mtu 8252 index 1
        inet6 ::1/128
...
lo0:2: flags=2001000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv6,VIRTUAL> mtu 8252 index 1
        zone internal
        inet6 ::1/128
...
ce0: flags=2000841<UP,RUNNING,MULTICAST,IPv6> mtu 1500 index 2
        inet6 fe80::20e:cff:fe08:fc/10
        ether 0:e:c:8:0:fc
...
ce0:3: flags=2000841<UP,RUNNING,MULTICAST,IPv6> mtu 1500 index 2
        zone internal
        inet6 fe80::130:2/10
ce0:4: flags=2000841<UP,RUNNING,MULTICAST,IPv6> mtu 1500 index 2
        zone internal
        inet6 2001:a08:3903:1::130:2/64
...
```

▼ Specify One NIC Per Zone on the System

If you have a separate physical interface for every labeled zone, follow this procedure. In this configuration, you isolate networks by dedicating a network interface card (NIC) to each network. Each network is single-label. Therefore, each NIC is dedicated to a zone.

Note – Before you can boot a labeled zone, the zone must be plumbed in the global zone.

Before You Begin   You are superuser in the global zone. You must have decided on the names of every labeled zone, as described in "Make System and Security Decisions Before Installing Trusted Extensions" on page 37.

1   **In the global zone, add each network interface to the** hosts **and** tnrhdb **databases.**

Follow the procedure in "Specify Labels for Network Interfaces" on page 57.

2   **Create persistent hostname files for the labeled zones interfaces.**

The file names must exist so that the labeled zones are plumbed during boot. The files can be empty.

```
# touch /etc/hostname.interface:n
```

3   **Create a hostname file for an all-zones interface for the global zone.**

The all-zones interface for the global zone requires a separate IP address. The file contains the separate IP address and the word all-zones. This file ensures that the labeled zones can talk to the X server.

You have two options when creating this file.

- **Create an interface name that is based on the physical interface.**

  ```
  # cat /etc/hostname.interface:n
  IP-address all-zones
  ```

- **Create a software-only device that can be reached only by the zones on this system.**

  For more information, see the vni(7d) man page.

  ```
  # cat /etc/hostname.vin0
  IP-address all-zones
  ```

4   **In the global zone, plumb the interfaces that you have created.**

Choose one of the following options to plumb the interfaces.

- **Reboot.**

- **Use the** ifconfig **command.**

  ```
  # ifconfig labeled-zone-interface plumb
  # ifconfig global-zone-all-zones-interface plumb
  ```

5 Continue with .

Example 4–2 Configuring Three NICs for Three Separate Networks

In the following example, the administrator is configuring a system that physically separates its labeled zones by using NICs.

- `e1000g1` is the interface (NIC) for the global zone
- `vin0` is the all-zones interface for the global zone
- `e1000g2` is the interface for the CONFIDENTIAL: INTERNAL USE ONLY zone
- `e1000g3` is for the interface for the CONFIDENTIAL: RESTRICTED zone

In the global zone, the administrator creates the empty hostname files for the labeled zones interfaces.

```
# touch /etc/hostname.e1000g2:1
# touch /etc/hostname.e1000g3:1
```

In the global zone, the administrator creates an all-zones interface for the global zone by using a `vin0` pseudo device. The following shows the contents of the file.

```
# cat /etc/hostname.vin0
192.168.0.7 all-zones
```

After defining the IP addresses in the Solaris Management Console, the `tnrhdb` database is similar to the following. The annotation is provided for assistance.

```
192.168.0.1:cipso      #### e1000g1 Global Zone
192.168.0.7:cipso      #### e1000g1:1 or vin0 Global Zone all-zones
192.168.1.1:cipso      #### e1000g2:1  CNF: IUO zone
192.168.2.1:cipso      #### e1000g3:1  CNF: R zone
192.168.0.11/24:admin_low  #### e1000g1 Global Zone network
192.168.1.11/24:iuo        #### e1000g2 single-label IUO network
192.168.2.11/24:restrict   #### e1000g3 single-label restricted network
```

The administrator runs the `ifconfig` command to plumb the interfaces.

```
# ifconfig e1000g2:1 plumb
# ifconfig e1000g3:1 plumb
# ifconfig vin0 plumb
```

The first two `ifconfig` commands enable the labeled zones to boot after the zones are configured and are installed. The third `ifconfig` command enables the labeled zones to communicate with the X server. The administrator chose the `vin0` interface for its security advantage over an `e1000g1:1` interface. Because the `vin0` interface has no physical presence, it cannot be seen outside of the zones on the system.

▼ Specify One IP Address for the System

In this configuration, the host's address applies to all the zones, including the labeled zones. In CDE, an action is provided to simplify this procedure.

Before You Begin   You are superuser in the global zone.

1   Open the Trusted_Extensions folder.

For details, see .

2   Run the Share Physical Interface action.

Double-click Share Physical Interface.

This action configures a host with one IP address. The global zone does not have a unique address. This system cannot be used as a multilevel print server or an NFS server.

3   (Optional) Verify the results of the action.

The Share Physical Interface action configures all zones to have logical NICs that share a single physical NIC in the global zone.

Use the ifconfig -a command. For example, the following output shows the shared physical interface, hme0 on network interface 192.168.0.11 for all the zones.

```
# ifconfig -a
 lo0: flags=2001000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4,VIRTUAL> mtu 8232 index 1
         inet 127.0.0.1 netmask ff000000
 hme0: flags=1000843<BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
         inet 192.168.0.11 netmask ffffff00 broadcast 192.168.0.255
```

Preparing to Create Zones (Tasks)

The following task map prepares the system for zone creation. For a discussion of zone creation methods, see .

Task	Description	For Instructions
Name each zone, and link the zone name and the zone label.	Name each labeled zone with a version of its label, then associate the name with the label in the Solaris Management Console.	"Specify Zone Names and Zone Labels" on page 55
Configure the network before creating the zones.	Assign a label to the network interface on every host, and do further configuration.	"Specify Labels for Network Interfaces" on page 57
Create space for a ZFS snapshot.	Perform this task if you are going to use the Clone Zone action to create zones.	"Create ZFS Pool for Cloning Zones" on page 58

Task	Description	For Instructions
Create labeled zones.	Create your first labeled zone. Then, create the rest by the method that you have chosen.	"Creating the Labeled Zones (Tasks)" on page 59

▼ Specify Zone Names and Zone Labels

You do not have to create a zone for every label in your label_encodings file, but you can. The tnzonecfg database enumerates the labels that can have zones created for them on this computer.

1 In the Trusted_Extensions folder, find and run the Configure Zone action.

The action prompts you for a name.

Tip – Give the zone the same name as the zone's label. So, the name of a zone whose label is public would be public.

---

2 Repeat the Configure Zone action for every zone.

For example, the default label_encodings file contains the following labels:

```
PUBLIC
CONFIDENTIAL: INTERNAL USE ONLY
CONFIDENTIAL: NEED TO KNOW
CONFIDENTIAL: RESTRICTED
SANDBOX: PLAYGROUND
MAX LABEL
```

You could run the Configure Zone action six times to create one zone per label. However, because MAX LABEL is defined to be a clearance, you probably would not create a zone for MAX LABEL. SANDBOX is defined as a disjoint label for developers. Therefore, many machines would not create a zone for this label. On a system for an ordinary user, you might create one zone for the PUBLIC label, and three zones for the CONFIDENTIAL labels.

3 Use the Trusted Network Zone Configuration tool.

The tools in the Solaris Management Console are designed to prevent user error. These tools check for syntax errors and automatically run commands in the correct order to update databases.

a. Launch the Solaris Management Console.

```
# /usr/sbin/smc &
```

Wait for the Welcome screen.

b. Open the Trusted Extensions toolbox for the local system.

i. Use the Console → Open Toolbox menu item.

ii. Select the toolbox that is named This Computer (*this-host*: Scope=Files, Policy=TSOL).

          iii. Click Open.

   c. (Optional) Make this toolbox the Home toolbox.

          i. Use the Console → Preferences menu item.

          ii. To make the Trusted Extensions toolbox the Home Toolbox, click Use Current Toolbox.

          iii. Click OK.

   d. Click System Configuration.

   e. Double-click the Computers and Networks tool.

   Provide a password when prompted.

   f. Double-click the Trusted Network Zone Configuration tool.

4 For each zone, associate the appropriate label with a zone name.

   a. Use the Action → Add Zone Configuration menu item.

   The dialog box displays the name of a zone that does not have an assigned label.

   b. Look at the zone name before clicking Edit.

   c. In the Label Builder, click the appropriate label for the zone name.

   If you click the wrong label, click the label again to deselect it, then click the correct label.

   d. Save the assignment.

   Click OK in the Label Builder, then OK in the Trusted Network Zone Properties dialog box.

You are finished when every zone that you want is listed in the panel, or the Add Zone Configuration menu item opens a dialog box that does not have a value for Zone Name.

Troubleshooting   If the Trusted Network Zone Properties dialog box does not prompt for a zone that you want to create, either the zone network configuration file does not exist, or you have already created the file.

- Check that the zone network configuration file does not already exist. Look in the panel for the name.

- If the file does not exist, run the Configure Zone action to supply the zone name. Then repeat Step 4 to create the file.

▼ Specify Labels for Network Interfaces

You turn your host, and other already-defined hosts into labeled hosts. These hosts are defined as sending and receiving labeled CIPSO packets. You need only add systems that are not known by your LDAP server.

1 Display the computers that are known by the system.

In the Solaris Management Console, navigate to Computers.

This tool is in the Computers and Networks tool set.

2 In the panel, double-click your host.

3 Copy the IP address.

4 Open Security Templates, then cipso.

5 Explicitly assign the host to the cipso template

    a. Click the Hosts Assigned to Template tab.

    If you completed "Make the Global Zone an LDAP Client" on page 45, the LDAP server is assigned to the cipso security template.

    b. Paste the host's IP address into the IP Address field.

    c. Type the host name into the Hostname field.

    d. Click the Add button.

    e. Click OK.

6 Repeat Step 1 to Step 5 for every host.

In the default configuration, every host that is not explicitly labeled is defined as an unlabeled host. Every unlabeled host can be contacted at boot at the label ADMIN_LOW. This is not a secure configuration. To modify the default configuration, see "How to Limit the Hosts That Can Be Contacted on the Trusted Network" in *Solaris Trusted Extensions Administrator's Procedures*.

Next Steps You can also modify the default configuration by doing some or all of the following:

- Create remote host templates for labeled hosts.
- Create remote host templates for unlabeled hosts.
- Remove the 0.0.0.0 wildcard address from the admin_low Unlabeled template, and explicitly assign the unlabeled computers that can be contacted at ADMIN_LOW.

See Also   For procedures, see "Configuring Trusted Network Databases (Tasks)" in *Solaris Trusted Extensions Administrator's Procedures*. For overview information, see Chapter 12, "Trusted Networking," in *Solaris Trusted Extensions Administrator's Procedures*.

▼ Create ZFS Pool for Cloning Zones

If you plan to use a ZFS snapshot as your zone template, you need to create a ZFS pool from a ZFS file or a ZFS device. This pool holds the snapshot for cloning each zone.

Before You Begin   You set aside space during Solaris installation for a Zetabyte file system (ZFS). For details, see "Planning for Zones" on page 21.

1   Use a file or a ZFS device as the source of your pool.

- **Use the** /zone **device for your ZFS pool.**

   During installation, you created a /zone partition with sufficient space, about 1000 MBytes.

   a.   Comment out the /zone **entry in the** vfstab **file.**

       i.   Open the Admin Editor from the Trusted_Extensions folder.

       ii.   Type /etc/vfstab **in the Pathname field.**

       iii.   Prevent the /zone **entry from being read.**

       Prefix the entry with a comment sign.

   ```
   #/dev/dsk/cntndnsn  /dev/dsk/cntndnsn  /zone  ufs  2  yes  -
   ```

       iv.   Copy the disk slice, cntndnsn, **to the clipboard.**

       v.   Save the file and close the editor.

   b.   Unmount the /zone **partition.**

   ```
   # umount /zone
   ```

   c.   Remove the /zone **mount point.**

   ```
   # cd /
   # rmdir /zone
   ```

   d.   Use the disk slice to recreate /zone **as a ZFS pool.**

   ```
   # zpool create -f zone cntndnsn
   ```

For example, if your /zone entry used disk slice c0t0d0s5, then the command would be similar to the following:

```
# zpool create -f zone c0t0d0s5
```

   e. **Continue with Step 2.**

■ **From the** /export **directory, create a ZFS pool.**

During installation, you created an /export partition with sufficient space, about 1000 MBytes. The template for all of your zones is created in this file.

```
# mkfile 1000m /export/zone
# zpool create zone /export/zone
```

To verify the health of the zone, see Step 3. Otherwise, continue with Step 2.

2 **Create a new file system as the root for one of your configured zones.**

```
# zfs create zone/zonename
# chmod 0700 /zone/zonename
```

For a configured zone that is named public, the commands would be similar to the following:

```
# zfs create zone/public
# chmod 0700 /zone/public
```

3 **(Optional) Verify that the ZFS pool is healthy.**

Use one of the following commands.

```
# zpool status -x zone
pool 'zone' is healthy
```

```
# zpool list
NAME   SIZE   USED   AVAIL   CAP   HEALTH   ALTROOT
/zone  992M   67.4M  92.5M   7%    ONLINE   -
```

For more information, see the zpool(1M) man page.

4 **Continue with "Creating the Labeled Zones (Tasks)" on page 59.**

Creating the Labeled Zones (Tasks)

For every entry that you made in the Trusted Network Zone Configuration database, one zone can be created. You completed this task in "Specify Zone Names and Zone Labels" on page 55, by running the Configure Zone action.

The Trusted_Extensions folder in the Application Manager contains actions that create labeled zones for Trusted Extensions.

- Configure Zone – Creates a zone configuration file for every zone name.
- Install Zone – Adds the correct packages and file systems to the zone.
- Zone Terminal Console – Provides a window for watching events in a zone.
- Initialize Zone for LDAP – Makes the zone an LDAP client and prepares the zone for booting.
- Start Zone – Boots the zone, then starts all the service management framework (SMF) services.
- Shut Down Zone – Changes the state of the zone from Started to Halted.

Task	Description	For Instructions
Install and boot one zone.	Create the first labeled zone. Install the packages, make the zone an LDAP client, and start all services in the zone.	"Install, Initialize, and Boot a Labeled Zone" on page 60
Customize the zone.	Remove unwanted services. If you plan to copy or clone the zone, remove zone-specific information.	"Customize a Booted Zone" on page 62
Create the other zones.	Use one of the following methods to create the other zones. You chose the method in "Make System and Security Decisions Before Installing Trusted Extensions" on page 37.	
	Create each zone from scratch.	"Install, Initialize, and Boot a Labeled Zone" on page 60 "Customize a Booted Zone" on page 62
	Copy the first labeled zone to another label. Repeat for all zones.	"Use the Copy Zone Method" on page 64
	Use a ZFS snapshot to clone the other zones from the first labeled zone.	"Use the Clone Zone Method" on page 65

▼ Install, Initialize, and Boot a Labeled Zone

Because zone creation involves copying an entire operating system, the process is time-consuming. A faster process is to create one zone, make the zone a template for other zones, then copy or clone that zone template.

Before You Begin You have completed "Make the Global Zone an LDAP Client" on page 45.

You have completed "Specify Zone Names and Zone Labels" on page 55.

If you are going to clone zones, you have completed "Create ZFS Pool for Cloning Zones" on page 58. Install the zone that you prepared.

1   **Double-click the Install Zone action.**

    a.   **Type the name of the zone that you are installing.**

       This action creates a labeled virtual operating system. This step takes some time to finish. Do not do other tasks on the system while Install Zone is running.

```
# Zonename: Install Zone
Preparing to install zone <zonename>
Creating list of files to copy from the global zone
Copying <total> files to the zone
Initializing zone product registry
Determining zone package initialization order.
Preparing to initialize <subtotal> packages on the zone.
Initializing package <number> of <subtotal>: percent complete: percent

Initialized <subtotal> packages on zone.
Zone <zonename> is initialized.
The file /zone/internal/root/var/sadm/system/logs/install_log
contains a log of the zone installation.

*** Select Close or Exit from the window menu to close this window ***
```

    b.   **Open a console to monitor events in the installed zone.**

       i.   **When the Install Zone action finishes, click the Zone Terminal Console action.**

       ii.   **Type the name of the zone that was just installed.**

2   **Double-click the Initialize Zone for LDAP action.**

```
Zone name:                   Type the name of the installed zone
Host name for the zone:      Type the host name for this zone
```

For example, on a system with a shared logical interface, the values would be similar to the following:

```
Zone name:              public
Host name for the zone: machine1-zones
```

This action makes the labeled zone an LDAP client of the same LDAP server that serves the global zone. The action is complete when the following information appears:

```
zonename zone will be  LDAP client of IP-address
zonename is ready for booting
Zone label is LABEL

*** Select Close or Exit from the window menu to close this window ***
```

3   Double-click the Start Zone action.

Answer the prompt.

`Zone name:`   *Type the name of the zone that you are configuring*

This action boots the zone, and starts all the services that run in the zone. For details on the services, see the `smf(5)` man page.

The Zone Terminal Console tracks the progress of booting the zone. Messages that are similar to the following appear in the console:

```
[Connected to zone 'public' console]

[NOTICE: Zone booting up]
...
Hostname: zonename
Loading smf(5) service descriptions: number/total
Creating new rsa public/private host key pair
Creating new dsa public/private host key pair

rebooting system due to change(s) in /etc/default/init

[NOTICE: Zone rebooting]
```

4   Monitor the console output.

Before continuing with , make sure that the zone has rebooted. The following console login prompt indicates that the zone has rebooted.

hostname `console login:`

Troubleshooting   For Install Zone: If you get warnings that are similar to the following: `Installation of these packages generated errors: SUNW`*pkgname*, read the install log and finish installing the packages.

▼ Customize a Booted Zone

If you are going to clone zones, this procedure configures a zone to be a template for other zones. If you are not going to clone zones, this procedure configures the zone for use.

1   Ensure that the zone has been completely started.

a.   In the *zonename***: Zone Terminal Console, log in as root.**

hostname `console login:` **root**
`Password:`   *Type root password*

b. Check that the zone is running.

```
# zoneadm list -v
ID NAME        STATUS       PATH
 2 public      running      /
```

2 (Optional) Disable services that you do not want to run.

If you are copying or cloning this zone, the services that you disable are disabled in every zone that is cloned from this zone. The services that are online on your system depend on the service manifest that the install team chose during installation. The limited option leaves very few services to be turned off. The open option leaves many services that can be turned off.

For more information on the service management framework, see the smf(5) man page.

```
# svcadm disable service
```

For example, you might want to disable graphical login:

```
# svcs cde-login
STATE        STIME    FMRI
online       13:05:00  svc:/application/graphical-login/cde-login:default
# svcadm disable svc:/application/graphical-login/cde-login
# svcs cde-login
STATE        STIME    FMRI
disabled     13:06:22  svc:/application/graphical-login/cde-login:default
```

3 Shut down the zone.

You can shut down the zone in one of two ways.

- **Run the Shut Down Zone action.**

  Provide the name of the zone.

- **In a terminal in the global zone, use the** zlogin **command.**

  ```
  # zlogin zonename init 0
  ```

  For more information, see the zlogin(1) man page.

4 Verify that the zone is shut down.

In the *zonename*: Zone Terminal Console, the following notice indicates that the zone is shut down.

```
[ NOTICE: Zone halted]
```

If you are not copying or cloning this zone, create the remaining zones in the way that you created this first zone.

5 If you are using this zone as a template for other zones, do the following:

a. Remove the auto_home_*zonename* **file.**

In a terminal in the global zone, remove this file from the *zonename* zone.

```
cd /zone/zonename/root/etc
# ls auto_home*
auto_home   auto_home_zonename
# rm auto_home_zonename
```

For example, if the public zone were the basis for cloning other zones, remove its auto_home file:

```
# cd /zone/public/root/etc
# rm auto_home_public
```

b. If you are copying a zone, go to "Use the Copy Zone Method" on page 64.

c. If you are cloning a zone, go to "Use the Clone Zone Method" on page 65.

▼ Use the Copy Zone Method

Before You Begin
- You have completed "Specify Zone Names and Zone Labels" on page 55.
- You have customized a zone that is a source for cloning in "Creating the Labeled Zones (Tasks)" on page 59.
- You are not currently running the zone that is your source for cloning.

1 Create a new zone from the original zone.

Run the Copy Zone action and answer the prompts.

```
New Zone Name:          Type name of target zone
From Zone Name:         Type name of source zone
```

2 Wait for the Copy Zone action to finish.

3 Repeat Step 1 and Step 2 for every zone.

4 Check the status of every zone.

a. Run the Zone Terminal Console action.

b. Log in to each zone.

c. Check the status of the zone.

```
# zoneadm list -v
ID NAME          STATUS          PATH
 3 internal     running          /
```

```
4 needtoknow   running       /
5 restricted   running       /
```

▼ Use the Clone Zone Method

Before You Begin
- You have completed "Specify Zone Names and Zone Labels" on page 55.
- You have completed "Create ZFS Pool for Cloning Zones" on page 58.
- You have customized a zone that is a source for cloning in "Creating the Labeled Zones (Tasks)" on page 59.
- The zone that is your source for cloning is shut down.

1 Create a ZFS snapshot of the zone template.

You created the zone template in "Create ZFS Pool for Cloning Zones" on page 58.

```
# cd /
# zfs snapshot zone/zonename@snapshot
```

For a configured zone that is named public, the snapshot command would be similar to the following:

`# zfs snapshot zone/public@snapshot`

This is the snapshot that you use to clone the remaining zones.

2 Clone a zone.

Run the Clone Zone action and answer the prompts.

```
New Zone Name:        Type name of source zone
ZFS Snapshot:         Type name of snapshot
```

3 Read the information in the dialog box.

```
Zone label is <LABEL>
zonename is ready for booting

*** Select Close or Exit from the window menu to close this window ***
```

4 Repeat Step 2 for each remaining zone.

5 Check the status of every zone.

a. By using the Zone Terminal Console action, log in to each zone.

b. For each zone, run the Start Zone action.

Complete each startup before running the action for another zone.

c. **Check the status of the zone.**

```
# zoneadm list -v
```

▼ Enable Users to Log In to a Zone

When the host is rebooted, the association between the devices and the underlying storage must be re-established.

Before You Begin   You have created at least one labeled zone. That zone is not being used for cloning.

1   **Reboot the system.**

2   **Log in as the** root **user.**

3   **Restart the zones service.**

```
# svcs zones
STATE          STIME    FMRI
offline        -        svc:/system/zones:default

# svcadm restart svc:/system/zones:default
```

4   **Log out.**

Ordinary users can now log in. Their session is in a labeled zone.

Creating Roles and Users

If you are already using administrative roles, you might want to add a Security Administrator role. For sites that have not yet implemented roles, the procedure for creating them is similar to the procedure in the Solaris OS. Trusted Extensions adds the Security Administrator role, and requires the use of the Solaris Management Console to administer a Trusted Extensions domain.

▼ Create the Security Administrator Role

Role creation in Trusted Extensions is identical to role creation in the Solaris OS. However, in Trusted Extensions, a Security Administrator role is required. To create a local Security Administrator role, you can also use the command line interface, as in Example 4–3.

Before You Begin   You must be superuser, or in the root role, or in the Primary Administrator role.

To create the role on the network, you must have completed "Configuring the Solaris Management Console for LDAP (Tasks)" on page 91.

1 If the Solaris Management Console is not running, start it.

   # **/usr/sbin/smc &**

2 Select the appropriate toolbox.

   - **To create the role locally, use This Computer (***this-host***:** Scope=Files, Policy=TSOL**).**

   - **To create the role in the LDAP service, use This Computer (***this-host***:** Scope=LDAP, Policy=TSOL**).**

3 Click System Configuration, then click Users.

4 When prompted, enter the appropriate password.

5 Double-click Administrative... (Administrative Roles).

6 Choose Add Administrative Role from the Action menu.

7 Create the Security Administrator role.

   Use the following information as a guide.

   - Role name – secadmin
   - Full name – Security Administrator
   - Description – Site Security Officer *No proprietary information here.*
   - Role ID Number – ≥100
   - Role shell – Administrator's Bourne (profile shell)
   - Create a role mailing list – Leave checkmarked.
   - Password and confirm – Assign a password of at least 6 alphanumeric characters.

     The password for the Security Administrator role, and all passwords, should be one that is not easy to guess, thus reducing the chance of an adversary gaining unauthorized access by attempting to guess passwords.

     Note – For all administrative roles, make the account Always Available, and do not set password expiration dates.

   - Available and Granted Rights – Information Security, User Security
   - Home Directory Server – *home directory server*
   - Home Directory Path – /*mount-path*
   - Assign Users– This field is automatically filled in when you assign a role to a user.

8 After creating the role, check that the settings are correct.

   Select the role, then double-click it.

Use the following information as a guide to review the values for the fields.

- Available Groups – Add groups if required.
- Trusted Extensions Attributes – Defaults are correct.

  If this system is single-label, and labels should not be visible, choose Hide for Label: Show or Hide.

- Audit Excluded and Included – Set audit flags only if the role's audit flags are exceptions to the system settings in the audit_control file.

9 To create other roles, use the Security Administrator role as a guide.

For examples, see "How to Create and Assign a Role By Using the GUI" in *System Administration Guide: Security Services*. Give each role a unique ID, and assign to it the correct rights profile. Possible roles include the following:

- admin Role – System Administrator Granted Rights
- primaryadmin Role – Primary Administrator Granted Rights
- oper Role – Operator Granted Rights

Example 4–3 Using the roleadd Command to Create a Local Security Administrator Role

In this example, root adds the Security Administrator role to the local system. For details, see the roleadd(1M) man page. root consults Table 1–2 before creating the role.

```
# roleadd -c "Local Security Administrator" -d /export/home1 \
-u 110 -P "Information Security,User Security" -K lock_after_retries=no \
-K idletime=5 -K idlecmd=lock -K labelview=showsl \
-K min_label=ADMIN_LOW -K clearance=ADMIN_HIGH secadmin
```

root provides an initial password for the role.

```
# passwd -r files secadmin
New Password:            <Type password>
Re-enter new Password:   <Retype password>
passwd: password successfully changed for secadmin
#
```

To assign the role to a local user, see Example 4–4.

▼ Create Users Who Can Assume Roles

To create a local user, you can also use the command line interface, as in Example 4–4. Where site security policy permits, you can choose to create a user who can assume more than one administrative role.

Before You Begin You must be superuser, or in the root role, or in the Security Administrator role, or in the Primary Administrator role. The Security Administrator role has the least amount of privilege that is required for user creation.

For secure user creation, the System Administrator role creates the user, and the Security Administrator role assigns security-relevant attributes, such as password.

1 **Double-click User Accounts in the Solaris Management Console.**

2 **Choose Add User → Use Wizard from the Action menu.**

> **Caution –** Role and user IDs come from the same pool of IDs. Do not use existing names or IDs for the users that you add.

3 **Follow the online help.**

You can also follow the procedures in "How to Add a User With the Solaris Management Console's Users Tool" in *System Administration Guide: Basic Administration*.

4 **After creating the user, double-click the created user to modify the settings.**

For users who can assume roles, ensure that the user is always available. Make sure the following fields are correctly set:

- Description – No proprietary information here.
- Password and confirm – Assign a password of at least 6 alphanumeric characters.

> **Note –** When the install team chooses a password, the team must select one that is not easy to guess, thus reducing the chance of an attacker gaining unauthorized access by attempting to guess passwords.

- Account Availability – Always Available.
- Trusted Extensions Attributes – Defaults are correct.

  If this system is single-label, and labels should not be visible, choose Hide for Label: Show or Hide.

- Account Usage – Set Idle time and Idle action.

  Lock account … – Set to No for any user who can assume a role.

5 **Customize the user's environment.**

- **Assign Convenient Authorizations –**

  After checking your site security policy, you might want to grant your first users the Convenient Authorizations rights profile. With this right, users can allocate devices, print PostScript files, print without labels, remotely log in, and shut down the system.

- **Customize user initialization files –**

  Chapter 7, "Managing Users, Rights, and Roles in Trusted Extensions," in *Solaris Trusted Extensions Administrator's Procedures*

  "Managing Users and Rights With Solaris Management Console (Tasks)" in *Solaris Trusted Extensions Administrator's Procedures*

- **Create multilabel copy and link files –**

  On a multilabel system, users and roles can be set up with files that list user initialization files to be copied or linked to other labels. For further discussion, see ".copy_files and .link_files Files" in *Solaris Trusted Extensions Administrator's Procedures*.

Example 4–4 Using the `useradd` Command to Create a Local User

In this example, `root` creates a local user who can assume the Security Administrator role. For details, see the useradd(1M) and atohexlabel(1M) man pages.

First, `root` determines the hexadecimal format of the user's minimum label and clearance label.

```
# atohexlabel public
0x0002-08-08
# atohexlabel -c "confidential restricted"
0x0004-08-78
```

root consults Table 1–2 before creating the user.

```
# useradd -c "Local user for Security Admin" -d /export/home1 \
-K  idletime=10 -K idlecmd=logout -K lock_after_retries=no
-K min_label=0x0002-08-08 -K clearance=0x0004-08-78 -K labelview=showsl jandoe
```

Then, `root` provides an initial password.

```
# passwd -r files jandoe
New Password:           <Type password>
Re-enter new Password:      <Retype password>
passwd: password successfully changed for jandoe
#
```

Finally, `root` adds the Security Administrator role to the user's definition. The role was created in "Create the Security Administrator Role" on page 66.
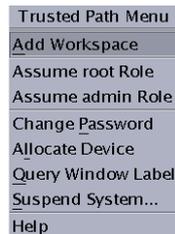
```
# usermod -R secadmin jandoe
```

▼ Verify That the Roles Work

For each role, assume the role. Then, perform tasks that only that role can perform.

Before You Begin   If you have set up DNS or static routing, you must reboot between creating the roles and verifying that the roles work.

1   **For each role, log in as a user who can assume the role.**

2   **In CDE, bring up the Trusted Path menu from the Workspace Switch Area.**

From the menu, assume the role.

```
Trusted Path Menu
Add Workspace
Assume root Role
Assume admin Role
Change Password
Allocate Device
Query Window Label
Suspend System...
Help
```

3   **In the role workspace, launch the Solaris Management Console.**

$ **/usr/sbin/smc &**

4   **Select the appropriate scope for the role that you are testing.**

5   **Click System Services and navigate to Users.**

    a.   **Provide the role password when prompted.**

    b.   **Double-click User Accounts.**

6   **Click a user.**

- The System Administrator role should be able to modify fields under the tabs General, Home Directory, and Group.
- The Security Administrator role should be able to modify fields under all tabs.
- The Primary Administrator role should be able to modify fields under all tabs.

Creating Home Directories

In Trusted Extensions, users can have home directories at every label at which the users work. To make every home directory available to the user requires that you create a multilevel home directory server, run the automounter on the server, and export the home directories. On the client side, you can run scripts to find the home directory for every zone for each user, or you can have the user log in to the home directory server.

▼ Create the Home Directory Server

Before You Begin   You must be superuser, or in the root role, or in the Primary Administrator role.

1   Install and configure the home directory server.

Follow the instructions for installing and configuring a system with Trusted Extensions software.

- If you are cloning zones, make sure that you use a snapshot that has empty home directories.
- Because users require a home directory at every label they they can log in to, create every zone that a user can log in to. For example, if you use the default label_encodings file, you would create a zone for the SANDBOX label.

2   If you are using UFS and not ZFS, enable the NFS server to serve itself.

a.   In the global zone, modify the automount **entry in the** nsswitch.conf **file.**

Use the Admin Editor to edit the /etc/nsswitch.conf file.

```
automount: files
```

b.   In the global zone, run the automount **command.**

3   For every labeled zone, create a new dfstab **file.**

Each zone shares the home directories at the label of the zone.

a.   Go to the zone's /etc/dfs **directory.**

```
# cd /zone/zone-name/root/etc/dfs
```

b.   Open the Admin Editor.

c.   Type the full pathname of the dfstab **file into the editor.**

```
# /zone/zone-name/etc/dfs/dfstab
```

d.   Add an entry to share home directories.

```
share -F nfs -o rw /export/home
```

4   In the global zone, run the shareall **command.**

The actual sharing occurs when each zone is brought into the ready or running state.

5   Display the status of the labeled zones.

```
# zoneadm list -cv
```

6   For each zone, share the directories.

As root in the global zone, run one of the following commands for each zone. Each zone can share its directories in any of these ways.

- **If the zone is not in the running state and you do not want users to log in to the server at the label of the zone, set the zone state to** ready**.**

  ```
  # zoneadm -z zonename ready
  ```

- **If the zone is not in the running state and users are allowed to log in to the server at the label of the zone, boot the zone.**

  ```
  # zoneadm -z zonename boot
  ```

- **If the zone is already running, reboot the zone.**

  ```
  # zoneadm -z zonename reboot
  ```

7   Verify that the home directories are shared.

In the global zone, use the showmount command.

```
# showmount -e
export list for home-directory-server:
/zone/zone-1/root/export/home (everyone)
/zone/zone-2/root/export/home (everyone)


...
/zone/zone-n
```

8   Verify the home directories setup.

  a.   Log out.

  b.   As an ordinary user, log in to the home directory server.

  c.   In the login zone, open a terminal.

  d.   In the terminal, check that the user's home directory is created.

  If an "Action Failed" dialog box appears, click OK. A terminal then displays.

  e.   Create workspaces for every zone that the user can work in.

  f.   In each zone, open a terminal to check that the user's home directory is created.

9   Log out.

▼ Enable Users to Access Their Home Directories

Users can log in to the home directory server initially to create a home directory that can be exported. To create a home directory at every label, the user must log in to the home directory server at every label.

Alternatively, you as administrator can create a script to create a mount point for users' home directories on the user's home machine before the user first logs in. The script would create mount points at every label at which the user is permitted to work.

Before You Begin   If you have set up DNS or static routing, you must reboot between creating the roles and verifying that the roles work.

◗ **Choose whether to allow direct login to the server, or whether to run a script.**

■ **Enable users to log in directly to the home directory server.**

This is an administrative choice.

a. **Instruct each user to log in to the home directory server.**

After successful login, the user should log out.

b. **Instruct each user to log in again, and this time, to choose a different login label.**

The user uses the label builder to choose a different login label. After successful login, the user should log out.

c. **Each user repeats the login process for every label that the user is permitted to use.**

d. **The users then go to their home machine, and log in.**

Their home directory for their default label should be available. When a user changes the label of a session, or adds a workspace at a different label, the user's home directory for that label should be mounted.

■ **Write a script that creates a home directory mount point for every user.**

From the global zone, run this script on the NFS server. Then, run this script on every multilevel desktop that the user is going to log in to.

```
#!/bin/sh
#
for zoneroot in '/usr/sbin/zoneadm list -p | cut -d ":" -f4' ; do
    if [ $zoneroot != / ]; then
        prefix=$zoneroot/root/export

        for j in 'getent passwd|tr ' ' _' ; do
            uid='echo $j|cut -d ":" -f3'
            if [ $uid -ge 100 ]; then
```

```
                          gid='echo $j|cut -d ":" -f4'
                          homedir='echo $j|cut -d ":" -f6'
                          mkdir -m 711 -p $prefix$homedir
                          chown $uid:$gid $prefix$homedir
                    fi
              done
        fi
    done
```

Adding Users and Hosts to an Existing Trusted Network

If you have users who are defined in NIS maps, you can add them to your network. To add a host, you use the Computers and Networks tool set in the Solaris Management Console.

▼ Add a NIS User to the LDAP Server

Before You Begin   You must be superuser, or in the root role, or in the Primary Administrator role.

1   From the NIS database, gather the information that you need.

a.   Create a file from the user's entry in the aliases **database.**

```
% ypcat -k aliases | grep login-name > aliases.name
```

b.   Create a file from the user's entry in the passwd **database.**

```
% ypcat -k passwd | grep "Full Name" > passwd.name
```

c.   Create a file from the user's entry in the auto_home_ **database.**

```
% ypcat -k auto_home | grep login-name > auto_home_label
```

2   Reformat the information for LDAP and Trusted Extensions.

a.   Use the sed **command to reformat the** aliases **entry.**

```
% sed 's/ /:/g' aliases.login-name > aliases
```

b.   Use the nawk **command to reformat the** passwd **entry.**

```
% nawk -F: '{print $1":x:"$3":"$4":"$5":"$6":"$7}' passwd.name > passwd
```

c.   Use the nawk **command to create a** shadow **entry.**

```
% nawk -F: '{print $1":"$2":6445:::::"}' passwd.name > shadow
```

d.   Use the nawk **command to create a** user_attr **entry.**

```
% nawk -F: '{print $1":::::lock_after_retries=yes-or-no;profiles=user-profile,...;
labelview=int-or-ext,show-or-hide;min_label=min-label;
```

```
clearance=max-label;type=normal;roles=role-name,...;
auths=auth-name,..."}' passwd.name > user_attr
```

3   Copy the modified files to the /tmp **directory on the LDAP server.**

```
# cp aliases auto_home_internal passwd shadow user_attr /tmp/name
```

4   Add the entries in the files in Step 3 to the LDAP server.

```
# /usr/sbin/ldapaddent -D "cn=directory manager" -w DM-password \
-a simple -f /tmp/name/aliases aliases
# /usr/sbin/ldapaddent -D "cn=directory manager" -w DM-password \
-a simple -f /tmp/name/auto_home_internal auto_home_internal
# /usr/sbin/ldapaddent -D "cn=directory manager" -w DM-password \
-a simple -f /tmp/name/passwd passwd
# /usr/sbin/ldapaddent -D "cn=directory manager" -w DM-password \
-a simple -f /tmp/name/shadow shadow
# /usr/sbin/ldapaddent -D "cn=directory manager" -w DM-password \
-a simple -f /tmp/name/user_attr user_attr
```

Example 4–5   Adding a User From a NIS Database to the LDAP Server

In the following example, the administrator adds a new user to the trusted network. The user's information is stored originally in a NIS database. To protect the LDAP server password, the administrator runs the ldapaddent commands on the server.

In Trusted Extensions, the new user can allocate devices, and can assume the Operator role. Because the user can assume a role, the user account does not get locked out. The user's minimum label is PUBLIC. The label at which the user works is INTERNAL, so jan is added to the auto_home_internal file. The auto_home_internal file automounts jan's home directory read-write.

1.   On the LDAP server, extract user information from NIS databases.

```
# ypcat -k aliases | grep jan.doe > aliases.jan
# ypcat passwd | grep "Jan Doe" > passwd.jan
# ypcat -k auto_home | grep jan.doe > auto_home_internal
```

2.   Reformat the entries for LDAP.

```
# sed 's/ /:/g' aliases.jan > aliases
# nawk -F: '{print $1":x:"$3":"$4":"$5":"$6":"$7}' passwd.jan > passwd
# nawk -F: '{print $1":"$2":6445:::::::"}' passwd.jan > shadow
```

3.   Create a user_attr entry for Trusted Extensions.

```
# nawk -F: '{print $1"::::lock_after_retries=no;profiles=Media User;
labelview=internal,showsl;min_label=0x0002-08-08;
clearance=0x0004-08-78;type=normal;roles=oper;
auths=solaris.device.allocate"}' passwd.jan > user_attr
```

4.   Copy the files to the /tmp/jan directory.

```
# cp aliases auto_home_internal passwd shadow user_attr /tmp/jan
```

5. Populate the server with the files in the /tmp/jan directory.

```
# /usr/sbin/ldapaddent -D "cn=directory manager" -w a2b3c4d5e6 \
-a simple -f /tmp/jan/aliases aliases
# /usr/sbin/ldapaddent -D "cn=directory manager" -w a2b3c4d5e6 \
-a simple -f /tmp/jan/auto_home_internal auto_home_internal
# /usr/sbin/ldapaddent -D "cn=directory manager" -w a2b3c4d5e6 \
-a simple -f /tmp/jan/passwd passwd
# /usr/sbin/ldapaddent -D "cn=directory manager" -w a2b3c4d5e6 \
-a simple -f /tmp/jan/shadow shadow
# /usr/sbin/ldapaddent -D "cn=directory manager" -w a2b3c4d5e6 \
-a simple -f /tmp/jan/user_attr user_attr
```

▼ Add a Host to the LDAP Server

◗ **Follow the procedures in "Configuring Trusted Network Databases (Tasks)" in** *Solaris Trusted Extensions Administrator's Procedures***.**

Note – Remember to add all IP addresses that are associated with the host. All-zones addresses, including addresses for labeled zones, must be added to the LDAP server.

Finishing Up Trusted Extensions Configuration (Task Map)

For other configuration tasks, see *Solaris Trusted Extensions Administrator's Procedures*.

Task	Description	For Instructions
Configure auditing.	The security administrator is responsible for auditing decisions.	"Audit Management by Role in Trusted Extensions" in *Solaris Trusted Extensions Administrator's Procedures*
Copy configuration files for distribution.	You must be root.	"Copying To and From Portable Media" on page 110
Do some common tasks.		"Common Tasks in Trusted Extensions (Tasks)" in *Solaris Trusted Extensions Administrator's Procedures*
Configure machine security settings.		"How to Change Security Defaults in System Files" in *Solaris Trusted Extensions Administrator's Procedures*
Configure mounting.		"Managing Files and File Systems (Tasks)" in *Solaris Trusted Extensions Administrator's Procedures*

Task	Description	For Instructions
Administer remotely.		"Administering Remotely (Tasks)" in *Solaris Trusted Extensions Administrator's Procedures*
Administer zones.		"Managing Zones (Tasks)" in *Solaris Trusted Extensions Administrator's Procedures*
Administer networking.	Identify remote hosts. Determine their label, multilevel ports, and control message policy.	"Managing the Trusted Network (Task Map)" in *Solaris Trusted Extensions Administrator's Procedures*
Administer users.		"Customizing the User Environment for Security (Tasks)" in *Solaris Trusted Extensions Administrator's Procedures*
Troubleshoot a system that cannot be logged in to.		"How to Log In to a Failsafe Session in CDE" in *Solaris Trusted Extensions Administrator's Procedures*
Administer printing	.	"Managing Printing in Trusted Extensions (Task Map)" in *Solaris Trusted Extensions Administrator's Procedures*
Administer devices		"Handling Devices in Trusted Extensions (Task Map)" in *Solaris Trusted Extensions Administrator's Procedures*
Administer third-party software		"Managing Software (Tasks)" in *Solaris Trusted Extensions Administrator's Procedures*

5

Configuring LDAP for Trusted Extensions

This chapter covers how to configure the Sun Java System Directory Server and the Solaris Management Console for use with Trusted Extensions. The Sun Java System Directory Server (LDAP server) provides LDAP services. LDAP is the supported naming service for Trusted Extensions. The Solaris Management Console is the administrative GUI for local and LDAP databases.

You have two options. You can configure an LDAP server on a Trusted Extensions host, or you can use an existing server and connect to it by using a Trusted Extensions proxy server.

- "Configuring an LDAP Server on a Trusted Extensions Host (Task Map)" on page 79
- "Configuring an LDAP Proxy Server on a Trusted Extensions Host (Task Map)" on page 80

Configuring an LDAP Server on a Trusted Extensions Host (Task Map)

Task	Description	For Instructions
Set up a Trusted Extensions LDAP server.	If you do not have an existing Sun Java System Directory Server, make your first Trusted Extensions host the LDAP server. The other Trusted Extensions hosts are clients of this server.	"Collect Information for the LDAP Service" on page 81
		"Install the Sun Java System Directory Server" on page 81
		"Protect Access Logs for the Sun Java System Directory Server" on page 84
		"Protect Error Logs for the Sun Java System Directory Server" on page 86
		"Configure a Multilevel Port for the Sun Java System Directory Server" on page 88

Task	Description	For Instructions
Add Trusted Extensions databases to the server.	Populate the LDAP server with data from the Trusted Extensions system files.	"Populate the Sun Java System Directory Server" on page 88
Configure the Solaris Management Console to work with the Sun Java System Directory Server.	Manually set up an LDAP toolbox for the Solaris Management Console. The toolbox can modify Trusted Extensions attributes on network objects.	"Configuring the Solaris Management Console for LDAP (Tasks)" on page 91
Configure all other Trusted Extensions hosts as clients of this server.	When you configure another system with Trusted Extensions, make the system a client of this LDAP server.	"Make the Global Zone an LDAP Client" on page 45

Configuring an LDAP Proxy Server on a Trusted Extensions Host (Task Map)

Use this task map if you have an existing Sun Java System Directory Server that is running on a Solaris system.

Task	Description	For Instructions
Add Trusted Extensions databases to the server.	The Trusted Extensions network databases, tnrhdb and tnrhtp, need to be added to the LDAP server.	"Populate the Sun Java System Directory Server" on page 88
Set up an LDAP proxy server.	Make one Trusted Extensions host the proxy server for the other Trusted Extensions hosts. The other Trusted Extensions hosts use this proxy server to reach the LDAP server.	"Create an LDAP Proxy Server" on page 90
Configure the proxy server to have a multilevel port for LDAP.	Enable the Trusted Extensions proxy server to communicate with the LDAP server at specific labels.	"Configure a Multilevel Port for the Sun Java System Directory Server" on page 88
Configure the Solaris Management Console to work with the LDAP proxy server.	You manually set up an LDAP toolbox for the Solaris Management Console. The toolbox can modify Trusted Extensions attributes on network objects.	"Configuring the Solaris Management Console for LDAP (Tasks)" on page 91
Configure all other Trusted Extensions hosts as clients of the LDAP proxy server.	When you configure another system with Trusted Extensions, make the system a client of the LDAP proxy server.	"Make the Global Zone an LDAP Client" on page 45

Configuring the Sun Java System Directory Server (Tasks)

The LDAP directory service is the supported naming service for Trusted Extensions. If your site is not yet running the LDAP directory service, configure a Sun Java System Directory Server on a system that is configured with Trusted Extensions. If your site is running a Sun Java System Directory Server, then you need to add the Trusted Extensions databases to the server. To access the directory server, you then set up an LDAP proxy on a Trusted Extensions host.

Note – If you do not use this LDAP server as an NFS server or as a server for Sun Rays, then you do not need to install any labeled zones on this server.

▼ Collect Information for the LDAP Service

▶ **Determine the values for the following items.**

Sample values follow the colons.

```
Administration domain : example-domain.com
Administration Server port number : 5200
Directory Administrator ID : admin
Directory Administrator password : admin123
Directory Manager DN : cn=Directory Manager
Directory Manager password : dirmgr123
Directory Server port number : 389
Fully qualified host distinguished name : myhost.example-domain.com
Server ID : myhost
Server suffix : dc=example-domain,dc=com
ServerRoot : /var/Sun/mps
Server group ID : root
Server user ID : root
```

▼ Install the Sun Java System Directory Server

The Sun Java System Directory Server is delivered as packages with the Solaris release.

1 **Find the Sun Java System Directory Server packages.**

You can download the software from the web site.

a. **Click 'Get the Software'.**

b. **Click the checkbox in front of 'Sun Java Identity Management Suite'.**

c. **Submit the request for the software.**

Scroll down the page to the Submit button, and click it.

d. **If you are registered, log in to download the software.**

e. **If you are not registered, register, then log in to download the software.**

f. **Select the 'Download Center' at the upper left of the screen.**

g. **Under 'Identity Management', download the most recent software that is appropriate for your platforms.**

2 **In the** /etc/hosts **file, add the fully qualified domain name (FQDN) to your system's hostname entry.**

192.168.5.5 myhost myhost.example.com

3 **Install the Sun Java System Directory Server packages.**

Answer the questions by using the following table as a guide.

Dialog Box or Screen	Action or Information
Environment Check	Click Next.
Welcome	Click Next.
License Agreement	Accept.
Fully Qualified Computer Name	Provide the FQDN that is in your /etc/hosts file. This name should appear as the default.
Select Server or Console Installation	Choose Sun Java™ System Servers.
Type of Installation	Choose Typical.
Select installation directory	Type the path where the product should be installed. This path is also used later if the proxy software is also installed. The default value is /var/Sun/mps. You might need to respond to an extra prompt if the directory must be created.
Select Components	Click Next. By default, all components are selected.
Sun Java System Directory Server User and Group	Accept the default values of root.
Configuration Directory Server	Accept the default, The new instance will be the configuration Directory Server.
Data Storage Location	Accept the default, Store the data in the new Directory Server.

Dialog Box or Screen	Action or Information
Directory Server Settings	Accept the default, ?Server Identifier.?.
	For the Server Port: If you plan to use the Directory Server to provide standard LDAP naming services to client systems, use the default value, 389. If you plan to use the Directory Server as a Configuration Directory Server to support a subsequent installation of the Directory Proxy Server, enter a nonstandard port, such as 10389. For the Suffix, include a custom domain component at the beginning, as in dc=example-domain,dc=com.
Configuration Directory Server Administrator	Accept the default Administrator ID of "admin" and enter your desired password. Suggested password: "admin123"
Administration Domain	Change to correspond to the Suffix already entered, as in, example-domain.com.
Directory Manager Settings	Accept the default Directory Manager DN of cn=Directory Manager. Then type your desired password.
Administration Server Port Selection	If you want, change the port number. A suggested convention is software-version TIMES 1000. For software version 5.2, this convention would result in port 5200.

4   Click Install Now.

5   Click Next, then Close.

Ignore the three known errors relating to bad file number, assertion failure, and interrupted system call.

6   Ensure that the Sun Java System Directory Server starts at every boot.

a.   Add an init.d **script.**

In the following example, change the SERVER_ROOT and SERVER_INSTANCE variables to match your installation.

```
/etc/init.d/ldap.directory-myhost
---------------------------------------
#!/sbin/sh

SERVER_ROOT=/var/Sun/mps
SERVER_INSTANCE=myhost

case "$1" in
start)
${SERVER_ROOT}/slapd-${SERVER_INSTANCE}/start-slapd
;;
stop)
```

```
${SERVER_ROOT}/slapd-${SERVER_INSTANCE}/stop-slapd
;;
*)

echo "Usage: $0 { start | stop }"
exit 1
esac
exit 0
```

b. Link the `init.d` **script to the** `rc2.d` **directory.**

```
/usr/bin/ln \
/etc/init.d/ldap.directory-myhost \
/etc/rc2.d/S70ldap.directory-myhost
```

7 Verify your installation.

■ **Examine your installation directory.**

A subdirectory that is named `slapd-`*server hostname* should exist.

■ **You should be able to start the Sun Java System Directory Server.**

installation-directory/`slapd-`*server hostname*/`restart-slapd`

■ **The** `slapd` **process should exist.**

```
# ps -ef | grep slapd
```
`./ns-slapd -D ` *installation-directory*/`slapd-`*server instance* `-i`
installation-directory/`slapd-`*server instance*/

Troubleshooting For strategies to solve LDAP configuration problems, see Chapter 13, "LDAP Troubleshooting (Reference)," in *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)*.

▼ Protect Access Logs for the Sun Java System Directory Server

The LDIF script in this procedure sets up the following rules for access logs:

■ Log level 256 and buffered logs (default)
■ Rotate logs daily
■ Keep a maximum of 100 log files and each file is at most 500 MB
■ Expire log files that are older than 3 months
■ Delete oldest logs if less than 500 MB free disk space is available
■ All log files use a maximum of 20,000 MB of disk space

1   Create a script to manage access logs.

Create a file /var/tmp/logs-access.ldif with the following content.

```
dn: cn=config
changetype: modify
replace: nsslapd-accesslog-logging-enabled
nsslapd-accesslog-logging-enabled: on
-
replace: nsslapd-accesslog-level
nsslapd-accesslog-level: 256
-
replace: nsslapd-accesslog-logbuffering
nsslapd-accesslog-logbuffering: on
-
replace: nsslapd-accesslog-logrotationtime
nsslapd-accesslog-logrotationtime: 1
-
replace: nsslapd-accesslog-logrotationtimeunit
nsslapd-accesslog-logrotationtimeunit: day
-
replace: nsslapd-accesslog-maxlogsize
nsslapd-accesslog-maxlogsize: 500
-
replace: nsslapd-accesslog-maxlogsperdir
nsslapd-accesslog-maxlogsperdir: 100
-
replace: nsslapd-accesslog-logexpirationtime
nsslapd-accesslog-logexpirationtime: 3
-
replace: nsslapd-accesslog-logexpirationtimeunit
nsslapd-accesslog-logexpirationtimeunit: month
-
replace: nsslapd-accesslog-logmaxdiskspace
nsslapd-accesslog-logmaxdiskspace: 20000
-
replace: nsslapd-accesslog-logminfreediskspace
nsslapd-accesslog-logminfreediskspace: 500
```

2   Run the script.

```
# ldapmodify -h localhost -D 'cn=directory manager' \
-f /var/tmp/logs-access.ldif
```

3   Answer the prompts.

```
Enter bind password:
modifying entry cn=config
```

▼ Protect Error Logs for the Sun Java System Directory Server

The LDIF script in this procedure sets up the following rules for the error files:

- Rotate logs weekly
- Keep a maximum of 30 log files and each file is at most 500 MB
- Expire log files that are older than 3 months
- Delete oldest logs if less than 500 MB free disk space is available
- All log files use a maximum of 20,000 MB of disk space

1   Create a script to manage error logs.

Create a file /var/tmp/logs-error.ldif with the following content.

```
dn: cn=config
changetype: modify
replace: nsslapd-errorlog-logging-enabled
nsslapd-errorlog-logging-enabled: on
-
replace: nsslapd-errorlog-logexpirationtime
nsslapd-errorlog-logexpirationtime: 3
-
replace: nsslapd-errorlog-logexpirationtimeunit
nsslapd-errorlog-logexpirationtimeunit: month
-
replace: nsslapd-errorlog-logrotationtime
nsslapd-errorlog-logrotationtime: 1
-
replace: nsslapd-errorlog-logrotationtimeunit
nsslapd-errorlog-logrotationtimeunit: week
-
replace: nsslapd-errorlog-maxlogsize
nsslapd-errorlog-maxlogsize: 500
-
replace: nsslapd-errorlog-maxlogsperdir
nsslapd-errorlog-maxlogsperdir: 30
-
replace: nsslapd-errorlog-logmaxdiskspace
nsslapd-errorlog-logmaxdiskspace: 20000
-
replace: nsslapd-errorlog-logminfreediskspace
nsslapd-errorlog-logminfreediskspace: 500
```

2   Run the script.

```
# ldapmodify -h localhost -D 'cn=directory manager' -f
/var/tmp/logs-error.ldif
```

3   Answer the prompts.

```
Enter bind password:
modifying entry cn=config
```

▼ Configure the Sun Java System Directory Server for LDAP Naming Services

Before You Begin   You have completed "Collect Information for the LDAP Service" on page 81.

◗ **Configure the LDAP naming service.**

The following is the complete list of installation questions, and the default answers that appear during the typical installation process.

```
Enter the Directory Server's hostname to set up: myhost

            - Enter the port number for iDS (h=help): [389]
            - Enter the directory manager DN: [cn=Directory Manager]
            - Enter passwd for cn=Directory Manager :dirmgr123
            - Enter the domainname to be served (h=help): [example-domain.com]
            - Enter LDAP Base DN (h=help): [dc=example-domain,dc=com]
            - Enter the profile name (h=help): [default]
            - Default server list (h=help): [129.146.108.90]
            - Preferred server list (h=help):
            - Choose desired search scope (one, sub, h=help):  [one]
            - The following are the supported credential levels:
                  1   anonymous
                  2   proxy
                  3   proxy anonymous
              Choose Credential level [h=help]: [1] 2
            - The following are the supported Authentication Methods:
                  1   none
                  2   simple
                  3   sasl/DIGEST-MD5
                  4   tls:simple
                  5   tls:sasl/DIGEST-MD5
              Choose Authentication Method (h=help): [1] 2
            - Do you want to add another Authentication Method? n
            - Do you want the clients to follow referrals (y/n/h)? [n]
            - Do you want to modify the server timelimit value (y/n/h)? [n]
            - Do you want to modify the server sizelimit value (y/n/h)? [n]
            - Do you want to store passwords in "crypt" format (y/n/h)? [n] y
            - Do you want to set up a Service Authentication Method (y/n/h)? [n]
            - Client search time limit in seconds (h=help): [30]
            - Profile Time To Live in seconds (h=help): [43200]
            - Bind time limit in seconds (h=help): [10]
            - Do you wish to set up Service Search Descriptors (y/n/h)? [n]
```

```
     - Enter config value to change: (1-19 0=commit changes) [0]
     - Enter DN for proxy agent:
[cn=proxyagent,ou=profile,dc=example-domain,dc=com]
     Enter passwd for proxyagent: proxy
     Re-enter passwd: proxy
     - WARNING: About to start committing changes. (y=continue,
n=EXIT) y
```

Note – When the idsconfig command completes, you can ignore the message about building the vlv_indexes files. This command has built the files.

▼ Configure a Multilevel Port for the Sun Java System Directory Server

To work in Trusted Extensions, the global zone of the Sun Java System Directory Server must be configured as a multilevel port (MLP).

1 **Launch the Solaris Management Console, and navigate to the Trusted Network Zone tool.**

2 **Double-click the global zone.**

3 **For the TCP protocol, do the following:**

    a. **Click Add for the Multilevel Ports for Zone's IP Addresses.**

    b. **Type 389 for the port number, and click OK.**

4 **For the UDP protocol, do the following:**

    a. **Click Add for the Multilevel Ports for Zone's IP Addresses.**

    b. **After typing 389, choose the udp protocol, and click OK.**

5 **Click OK to save the settings.**

6 **Update the kernel.**
   # **tnctl -fz /etc/security/tsol/tnzonecfg**

▼ Populate the Sun Java System Directory Server

Several LDAP databases have been created or modified to hold Trusted Extensions data about label configuration, users, and remote hosts.

1   Create a staging area for files that you plan to use to populate the naming service databases.

```
# mkdir -p /setup/files
```

2   Copy the sample /etc **files into the staging area.**

```
# cd /etc
# cp aliases group networks netmasks protocols /setup/files
cp rpc services auto_master /setup/files

# cd /etc/security
# cp  auth_attr prof_attr exec_attr /setup/files/
#
# cd /etc/security/tsol
# cp tnrhdb tnrhtp /setup/files
#
# cd /etc/inet
# cp ipnodes /setup/files
```

3   Remove the +auto_master **entry from the** /setup/files/auto_master **file.**

4   Remove the ?:::::? **entry from the** /setup/files/auth_attr **file.**

5   Create the zone automaps in the staging area.

In the following list of automaps, the first of each pair of lines shows the name of the file. The second line of each pair shows the file contents. The zone names identify labels from the default label_encodings file that is shipped with the Trusted Extensions software.

- Substitute your zone names for the zone names in these lines.
- *myNFSserver* identifies the NFS server for the home directories
- FQDN means fully qualified domain name.

```
/setup/files/auto_home_public
 * myNFSserver_FQDN:/zone/public/root/export/home/&

/setup/files/auto_home_internal
 * myNFSserver_FQDN:/zone/internal/root/export/home/&

/setup/files/auto_home_needtoknow
 * myNFSserver_FQDN:/zone/needtoknow/root/export/home/&

/setup/files/auto_home_restricted
 * myNFSserver_FQDN:/zone/restricted/root/export/home/&
```

6   Add every host on the network to the /setup/files/tnrhdb **file.**

No wildcard mechanism can be used here. The IP address of every host to be contacted *must* be in this file. This includes the IP addresses of labeled zones.

a.   Open the Admin Editor and edit /setup/files/tnrhdb**.**

    b. Add every IP address on a labeled host in the Trusted Extensions domain.

    Labeled hosts are of type `cipso`. In the default configuration, a cipso entry is similar to the following:

```
192.168.25.2:cipso
```

Note – This list includes the IP addresses of global zones and of labeled zones.

---

    c. Add every unlabeled host with which the domain can communicate.

    Unlabeled hosts are of type `unlabeled`. In the default configuration, `admin_low` is the template name for an unlabeled host:

```
192.168.35.2:admin_low
```

    d. Save the file and exit the editor.

    e. Check the syntax of the file.

    # `tnchkdb -h /setup/files/tnrhdb`

    Fix any errors before continuing.

7 **Copy the** `/setup/files/tnrhdb` **file to** `/etc/security/tsol/tnrhdb`**.**

At this point, these two files should be identical.

8 **Use the** `ldapaddent` **command to populate every file in the staging area.**

 # `/usr/sbin/ldapaddent -D "cn=directory manager" \`
`-w dirmgr123 -a simple -f /setup/files/hosts hosts`

Using a Proxy for the Sun Java System Directory Server (Tasks)

First, you need to add the Trusted Extensions databases to the server. Second, to enable Trusted Extensions hosts to access the directory server, you then make one Trusted Extensions host an LDAP proxy server.

▼ Create an LDAP Proxy Server

If an LDAP server already exists at your site, create a proxy server on a Trusted Extensions host.

1 **On a system that is configured with Trusted Extensions, create a proxy server.**

2 **Add the Trusted Extensions databases to the LDAP server.**

For details, see "Populate the Sun Java System Directory Server" on page 88.

3 Verify that Trusted Extensions databases can be viewed by the proxy server.

ldaplist -l *database*

Troubleshooting For strategies to solve LDAP configuration problems, see Chapter 13, "LDAP Troubleshooting (Reference)," in *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)*.

Configuring the Solaris Management Console for LDAP (Tasks)

The Solaris Management Console is the GUI for administering the network of systems that are running Trusted Extensions.

Task	Description	For Instructions
Register credentials	Authenticate the Solaris Management Console with the LDAP server.	"Register LDAP Credentials With the Solaris Management Console" on page 91
Enable LDAP administration on a system	By default, LDAP administration is turned off at installation. You explicitly enable particular systems to be LDAP administration systems.	"Enable an LDAP Client to Administer LDAP" on page 92
Create the LDAP toolbox	Create the LDAP toolbox in the Solaris Management Console for Trusted Extensions.	"Edit the LDAP Toolbox in the Solaris Management Console" on page 92
Initialize the Solaris Management Console	Initialize the Solaris Management Console. This procedure is done once per system in the global zone.	"Initialize the Solaris Management Console Server" on page 94
Verify that the Solaris Management Console is communicating with the LDAP server		"Make the Global Zone an LDAP Client" on page 45

▼ Register LDAP Credentials With the Solaris Management Console

Before You Begin You must be the root user on an LDAP server that is running Trusted Extensions. The server can be a proxy server.

Your Sun Java System Directory Server must be configured. You have completed one of the following configurations:

- "Configuring an LDAP Server on a Trusted Extensions Host (Task Map)" on page 79
- "Configuring an LDAP Proxy Server on a Trusted Extensions Host (Task Map)" on page 80

1 **Register the LDAP administrative credentials.**

```
# /usr/sadm/bin/dtsetup storeCred
Administrator DN:      Type the value for cn on your system
Password:      Type the Directory Manager password
Password (confirm):      Retype the password
```

2 **Verify communication with the directory service.**

```
# /usr/sadm/bin/dtsetup scopes
Getting list of manageable scopes...
Scope 1 file:      Displays name of file scope
Scope 2 ldap:      Displays name of ldap scope
```

Example 5–1 Registering LDAP Credentials

In this case, the name of the LDAP server is LDAP1, the name of the LDAP client is myhost, and the value for cn is the default, Directory Manager.

```
# /usr/sadm/bin/dtsetup storeCred
Administrator DN:cn=Directory Manager
Password:abcde1;!
Password (confirm):abcde1;!
# /usr/sadm/bin/dtsetup scopes
Getting list of manageable scopes...
Scope 1 file:/myhost/myhost
Scope 2 ldap:/myhost/cd=myhost,dc=example,dc=com
```

▼ Enable an LDAP Client to Administer LDAP

By default, systems are installed to not listen on ports that present security risks. Therefore, you must explicitly turn on network communication with the LDAP server. You should perform this procedure only on systems from which you plan to administer your network of systems and users.

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

▶ **Enable the system to administer LDAP.**

```
# svccfg -s wbem setprop options/tcp_listen=true
```

▼ Edit the LDAP Toolbox in the Solaris Management Console

Before You Begin   You must be the root user.

Specifically, you must know the output of the /usr/sadm/bin/dtsetup scopes command. For details, see "Register LDAP Credentials With the Solaris Management Console" on page 91.

1 Find the LDAP toolbox.

```
# cd /var/sadm/smc/toolboxes/tsol_ldap
# ls *tbx
tsol_ldap.tbx
```

2 Provide the LDAP server name.

a. Open the Admin Editor.

b. Copy and paste the full pathname of the `tsol_ldap.tbx` **toolbox into the dialog box.**

For example, the following path is the default location of the LDAP toolbox:

`/var/sadm/smc/toolboxes/tsol_ldap/tsol_ldap.tbx`

c. Replace the scope information.

Replace the `server` tags between the `<Scope>` and `</Scope>` tags with the output of the `ldap:/......` line from the `/usr/sadm/bin/dtsetup scopes` command.

`<Scope>ldap:/<`*myhost*`>/<dc=`*domain*`,dc=`*suffix*`></Scope>`

d. Replace `server`.

Replace every instance of `<?server?>` or `<?server ?>` with the LDAP server, as in:

```
<Name> ldap-server-name: Scope=ldap, Policy=TSOL</Name>
services and configuration of ldap-server-name.</Description>
and configuring ldap-server-name.</Description>
<ServerName>ldap-server-name</ServerName>
<ServerName>ldap-server-name</ServerName>
```

e. Save (`:wq!`) **and close the file.**

3 Stop and start the daemon.

The `smc` daemon is controlled by the `wbem` service.

```
# svcadm disable wbem
# svcadm enable wbem
```

Example 5–2 Configuring the LDAP Toolbox

In this case, the name of the LDAP server is LDAP1.

```
<Name>LDAP1: Scope=ldap, Policy=TSOL</Name>
services and configuration of LDAP1.</Description>
and configuring LDAP1.</Description>
<ServerName>LDAP1</ServerName>
<ServerName>LDAP1</ServerName>
```

▼ Initialize the Solaris Management Console Server

Before You Begin   You must be the root user.

To view the LDAP toolbox, you must have completed "Edit the LDAP Toolbox in the Solaris Management Console" on page 92.

1   Start the Solaris Management Console server process.

```
# /usr/sbin/smc &
```

Note – The first time the Solaris Management Console server is launched, it performs several registration tasks. These tasks can take a few minutes.

2   Do one of the following if toolbox icons do not appear in the Solaris Management Console.

- **If the Navigation pane is not visible:**

  a.   In the Open Toolbox dialog that is displayed, click Load next to this machine's name under Server.

  If this machine does not have the recommended amount of memory and swap, it might take a few minutes for the toolboxes to display. For recommendations, see "Installing or Upgrading the Solaris OS for Trusted Extensions (Tasks)" on page 33.

  b.   From the list of toolboxes, select one whose Policy=TSOL.

  Your choice depends on which scope you want to influence. To edit local files, choose the Files scope. To edit LDAP databases, choose the LDAP scope. Do not choose the computer that has no policy.

  c.   Click Open.

- **If the Navigation pane is visible, but the toolbox icons are stop signs:**

  a.   Exit the Solaris Management Console.

  Choose Exit from the Console pull-down men

  b.   Restart the Solaris Management Console.

  ```
  # /usr/sbin/smc &
  ```

  c.   Follow the instructions in Step 3.
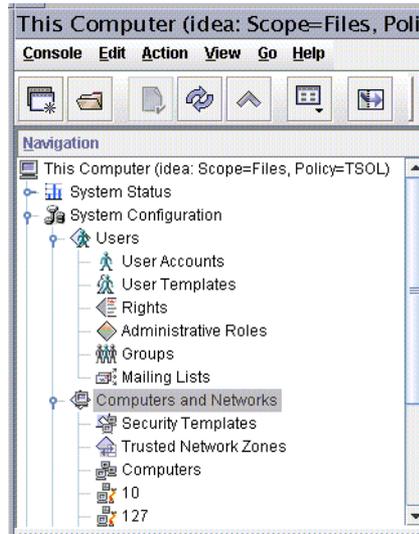
FIGURE 5–1 Solaris Management Console Tools

3   (Optional) Save the current toolbox.

Saving a `Policy=TSOL` toolbox enables a Trusted Extensions toolbox to load by default. Preferences are saved per role, per host. The host is the Solaris Management Console server.

a.   From the Console menu, choose Preferences.

The Home Toolbox is selected.

b.   Define a `Policy=TSOL` toolbox as the home toolbox.

Put the current toolbox in the Location field by clicking the Use Current Toolbox button.

c.   Click OK to save the preferences.

4   Close the Solaris Management Console.

5   Register the LDAP credentials with the Solaris Management Console.

```
# /usr/sadm/bin/dtsetup scopes
Getting list of managable scopes...
Scope 1 file:/myhost/myhost <../../../../myhost/myhost>
Scope 2 ldap:/myhost/dc=example-domain,dc=com <ldap:///myhost/dc=example-domain,dc=com>
```

Your LDAP server setup determines the LDAP scopes that are listed. Once the server is registered, the LDAP toolbox can now be used.

▼ Verify That the Solaris Management Console Contains Trusted Extensions Information

Before You Begin   You must be logged in to an LDAP client in an administrative role, or as superuser. To make a system an LDAP client, see "Make the Global Zone an LDAP Client" on page 45.

To use the LDAP toolbox, you must have completed "Edit the LDAP Toolbox in the Solaris Management Console" on page 92 and "Initialize the Solaris Management Console Server" on page 94.

1   Start the Solaris Management Console.

```
# /usr/sbin/smc &
```

2   Open a Trusted Extensions toolbox.

A Trusted Extensions toolbox has the value Policy=TSOL.

- **To check that local files can be accessed, open the This Computer (***this-host***:** Scope=Files, Policy=TSOL**) toolbox.**

- **To check that databases on the LDAP server can be accessed, open the This Computer (***this-host***:** Scope=LDAP, Policy=TSOL**) toolbox.**

3   Navigate to Computers and Networks, then Security Templates.

4   Check that the correct templates and labels have been applied to remote hosts.

5   To troubleshoot LDAP configuration, see Chapter 13, "LDAP Troubleshooting (Reference)," in *System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)***.**

6

Configuring a Headless System With Trusted Extensions

Configuring and administering Trusted Extensions software on headless systems like the Netra™ series require different procedures than the same tasks on systems that have monitors. Trusted Extensions software divides administrative responsibilities into roles, which cannot be assumed remotely. The software also provides an administrative tool GUI. The GUI does not display on a serial line.

Note – The configuration methods that headless systems require do not satisfy the criteria for an evaluated configuration. For more information, see "Understanding Your Site's Security Policy" on page 18.

Headless System Configuration (Task Map)

On headless systems, a console is connected by means of a serial line to a terminal emulator window. The line is typically secured by the `tip` command. Depending on what type of second system is available, you can use one of four methods. The methods are listed from most desirable to least desirable in the following table.

Tasks	Description	For Instructions
1. Identify the headless system as a CIPSO system.	On the desktop system where you are going to configure the headless system, make the headless system of host type CIPSO.	If you have not already made the headless system part of the trusted network, assign to it the appropriate security template in "Specify Labels for Network Interfaces" on page 57
2. Enable remote login.	As root, enable remote logins to the headless system.	"Enable Remote Login" on page 98

Tasks	Description	For Instructions
3. Choose a configuration and administration method to set up the headless system. The choice is based on available hardware and software on a second system that communicates with the headless system. The choices are listed in descending order of ease and security.	You can remotely display the Application Manager by using dtappsession.	If you have a desktop system that is running Trusted Extensions, go to "Use dtappsession to Log In to a Headless System" on page 100.
	You can remotely display the Solaris Management Console. In this method, the CDE actions are reached through Legacy Applications.	If you have a desktop system that is running Solaris Management Console 2.1 client software, go to "Set Up Remote Solaris Management Console Login to a Headless System" on page 101.
	You can use rlogin, then administer on the command line.	If you are logging in remotely using the rlogin command, go to "Enable Remote Login" on page 98.
	If you have no windowing system, you can use serial login. This procedure is insecure.	If you do not have a desktop system, and must use serial login to configure and administer the headless system, go to "Set Up Administration by Serial Login" on page 102 .
4. Configure Trusted Extensions on the headless system.	Having logged in, continue configuration.	See Chapter 4, and use the methods that are possible given your login method.
5. Administer the headless system.	Remotely log in to administer the system.	See *Solaris Trusted Extensions Administrator's Procedures*, and use the methods that are possible given your login method.

▼ Enable Remote Login

Follow this procedure *only if* you do not have a desktop system with which to configure the headless system and you plan to administer the headless system by using rlogin or ssh. This procedure is not secure.

Configuration errors can be debugged remotely.

Before You Begin   Consult your security policy for which methods of remote login are permissible at your site.

1   **Launch a terminal.**

Bring up the Workspace Menu by clicking with mouse button 3 on the screen background. Select Tools → Terminal.

2 Choose one or more of the following methods of remote entry.

- **Enable remote login by the** root **user.**

  a. Comment out the CONSOLE= **line in the** /etc/default/login **file.**

     #CONSOLE=/dev/console

  b. Permit root logins for the ssh **service.**

     Modify the /etc/ssh/sshd_config file. By default, ssh is enabled on a Solaris system.

     PermitRootLogin **yes**

- **Enable roles to log in remotely.**

  If root is a role, this modification is required for remote logins by the root role.

  a. Open the pam.conf **file in an editor.**

     # vi **/etc/pam.conf**

  b. Find other account requisite **toward the end of the file.**

  c. Add allow_remote **to the roles module.**

     Use the TAB key between fields.

     other account requisite pam_roles.so.1 **allow_remote**

     After your edits, this section looks similar to the following:

     ```
     other account requisite  pam_roles.so.1        allow_remote
     other account required        pam_unix_account.so.1
     other account required        pam_tsol_account.so.1
     ```

- **Allow remote entry from an unlabeled host.**

  a. Open the pam.conf **file in an editor.**

     # vi **/etc/pam.conf**

  b. Find other account requisite **toward the end of the file.**

  c. Add allow_unlabeled **to the** tsol_account **module.**

     Use the TAB key between fields.

     other account required   pam_tsol_account.so.1 **allow_unlabeled**

     After your edits, this section looks similar to the following:

     ```
     other account requisite  pam_roles.so.1        allow_remote
     other account required        pam_unix_account.so.1
     other account required        pam_tsol_account.so.1 allow_unlabeled
     ```

- **Allow specific users to log in to the global zone.**

  Assign to these users an administrative label range in the user_attr file.

  username:::::idlecmd=lock;lock_after_retries=yes;idletime=5;\
  type=normal;labelview=showsl;\
  clearance=**ADMIN_HIGH**;min_label=**ADMIN_LOW**

  The backslashes are for purposes of display only. The entry should be on one line.

- **Enable remote login from other labels.**

  a. Enable remote login to the global zone.

  Add port 513 as a multilevel port (MLP). Port 513 enables remote login.

  ```
  # cat /etc/security/tsol/tnzonecfg
  ...
  global:ADMIN_LOW:1:111/tcp;111/udp;513/tcp;...
  ```

  b. Verify the syntactic accuracy of the tnzonecfg **file.**

  ```
  # tnchkdb
  ```

  Fix any errors before continuing.

  c. Read the tnzonecfg **changes into the kernel.**

  ```
  # tnctl -fz /etc/security/tsol/tnzonecfg
  ```

  d. Restart the remote login service.

  ```
  # svcadm restart svc:/network/login:rlogin
  ```

▼ Use dtappsession **to Log In to a Headless System**

This procedure enables you to use Trusted Extensions GUIs to administer a headless system.

Before You Begin   The headless system must have enough memory to use the Solaris Management Console. The requirements are the same as for the Solaris OS. For details, see "System Requirements and Recommendations" in *Solaris Express Installation Guide: Basic Installations*.

The headless system is identified as a CIPSO system on the administrator's desktop host. For details, see "Specify Labels for Network Interfaces" on page 57.

You have completed "Enable Remote Login" on page 98.

You are a user who is enabled to log in to the headless system.

1   **On a Trusted Extensions desktop host, remotely log in to the headless system.**

admin-host $ rlogin *headless-host*
    Password: /*type the remote password*/

2   Assume a role.

If you are not in the global zone on the headless system, assume a role in the same terminal:

headless-host # su *role-name*
        Password: *Type the role password*

You are now in the global zone.

3   Display the Application Manager on the administrator's desktop.

In the same terminal, use the dtappsession command.

headless-host # dtappsession *admin-host*
        Password: *Type the remote password*

You can now administer the headless system by using CDE actions and the Solaris Management Console.

▼ Set Up Remote Solaris Management Console Login to a Headless System

This procedure enables you to use the Solaris Management Console to administer the headless system. Terminals and the Application Manager are available through Legacy Applications on the Solaris Management Console.

Before You Begin   For this procedure to work, one of the following systems must be available:

- A Solaris desktop system that is configured to run the Solaris Management Console 2.1 client process
- A Windows client that is running the Solaris release and can run the Solaris Management Console 2.1 client process

1   After installation, boot the headless system into single-user mode.

2   Add the Solaris desktop machine with Solaris Management Console 2.1 running on it, to the headless system's /etc/hosts **file.**

For example,

192.168.168.77   soldesktop77

3   On the Windows client or Solaris desktop system, add the headless system's address to the c:\windows\system\hosts **or** /etc/hosts **file, respectively.**

For example,

192.168.168.111   headless1

4 Modify the /usr/sadm/lib/smc/bin/smcwbemserver **file on the headless system to include the** -u **option.**

Follow the procedure, To Enable Remote Role Assumption From Untrusted Systems under "Administering Remotely (Tasks)" in *Solaris Trusted Extensions Administrator's Procedures*, then return here.

5 On the headless system, exit single-user mode and let the system complete the boot process.

6 On the Windows client or Solaris desktop system, start the Solaris Management Console server process.

```
# /usr/sbin/smc &
```

7 In the Solaris Management Console Console menu, select the Preferences dialog box.

8 Click the Authentication tab, and click Enable advanced login, then OK.

9 Open the Files toolbox of the headless system, and log in specifying an administrative role.

Provide the role password.

10 Bring up a Terminal or the Application Manager window from the Legacy tools set in the Navigation Pane.

11 Configure the headless system.

▼ Set Up Administration by Serial Login

Follow this procedure *only if* you do not have a desktop system with which to configure the headless system. This procedure is not secure.

Before You Begin The serial port must be allocated before the port can be used. For details, see the serial login procedure in "Managing Devices in Trusted Extensions (Tasks)" in *Solaris Trusted Extensions Administrator's Procedures*.

You must be root in single user mode on the headless system.

1 Modify the /etc/inittab **file to spawn a console login on the serial console.**

Use the vi command to change the last line of /etc/inittab to:

```
co:234:respawn:/usr/lib/saf/ttymon -g -h -p "'uname -n' console login: " \
 -T sun -d  /dev/console -l console -m ldterm,ttcompat
```

The preceding line is broken with a backslash for display purposes. You should not break the line in the /etc/inittab file.

2 You can administer the system as root or by assuming a role.

Modify the /etc/security/user_attr entry for the install user, as in:

```
install...;profiles=...,Primary Administrator;
```

The Primary Administrator profile includes privileged shells. The install user can now run privileged commands.

- **Create a user and a role.**

  The user install is a conventional name.

  ```
  # grep install /etc/passwd
  install:x:111:111:Headless Configuration:/:/sbin/sh
  ```

  a. Supply a user password for the user.

  ```
  # grep install /etc/shadow
  install:wqI2HKYC2t41E:6445::::::
  ```

  b. Create the Primary Administrator role and supply a role password.

  The Primary Administrator role includes the Primary Administrator profile.

  ```
  # grep primadmin /etc/passwd
  primadmin:x:101:101:Primary Administrator:/:/sbin/sh

  # grep primadmin /etc/shadow
  primadmin:q64IHHW297x9e:6445::::::

  # grep primadmin /etc/user_attr
  primadmin:::::profiles=Primary Administrator
  ```

  c. Assign the role to the user.

  ```
  # grep install /etc/user_attr
  install:::::roles=primadmin
  ```

  You can now configure the system by logging in as the install user, and assuming the Primary Administrator role.

- **Administer the system as root.**

  This method of configuration is insecure. For a modicum of security, two people should be present while the system is being configured.

7

Common Procedures

This chapter contains common administrative procedures that are useful to know when configuring Trusted Extensions software. Each procedure, or part of it, is specific to Trusted Extensions.

Running Administrative Actions

Trusted Extensions administrative programs are located on the Front Panel of CDE, and in the Application Manager. The following table shows the icons and describes the administrative programs.

TABLE 7–1 Administrative Program Icons and Locations

Icon	Name and Location	Use
	The Application Manager is reached from the Workspace menu.	Holds desktop applications.
	The Trusted_Extensions folder is in the Application Manager.	Holds administrative applications for the local machine.
	The Solaris Management Console GUI is in the Application Manager.	Administers local and network databases.

TABLE 7–1 Administrative Program Icons and Locations   *(Continued)*

Icon	Name and Location	Use
	In CDE, the Device Allocation Manager is on the Front Panel.	Administers devices. Used to allocate and deallocate devices.

Using Trusted_Extensions Actions (Tasks)

The Trusted_Extensions folder contains CDE actions for administering the local system. For a full list of Trusted_Extensions actions, read the CDE online help.

▼ How to Find CDE Online Help for Trusted Extensions

1 Click the online help icon on the front panel.

2 In the Help Viewer, click the Solaris Trusted Extensions Desktop.

On-item help is also available.

3 If the Help Viewer does not display the Solaris Trusted Extensions Desktop, find Trusted **in the index.**

    a. Click the Index ... button.

    b. Click All Volumes.

    c. In the Entries with: field, type trusted.

    d. Click one of the index entries that is returned.

▼ How to Run a Trusted_Extensions Action

Before You Begin   You must be in a role workspace.

1 Open the Application Manager.

Right-click the background to bring up the Workspace menu. Choose Applications → Application Manager from the top of the menu.

2 Double-click the Trusted_Extensions folder icon.

3 Double-click the appropriate action.

For more details, see "How to Create or Open a File from the Trusted Editor" on page 107, Example 7–1 and Example 7–2.

Example 7–1   Opening a File That Has a Defined Action

You double-click the file's action in the Trusted_Extensions folder. The Admin Editor invokes the file.

Files that have their own action include the audit configuration files, the label_encodings file, and the nsswitch.conf file.

Example 7–2   Running a Script From the Trusted_Extensions Folder

You double-click the script's action in the Trusted_Extensions folder, then follow the instructions. The script is finished when its windows have been dismissed.

Actions that invoke scripts include Initialize Client for LDAP, Start Zone, Install Zone, and Check Label Encodings.

▼ How to Create or Open a File from the Trusted Editor

Actions that open files in an editor use the Admin Editor icon that is shown in the following graphic.

Before You Begin   You must be in a role workspace.

1   To create or open a file that does not have its own action, double-click the Admin Editor action.

A prompt appears for you to specify the file to be opened.

2   Type the name of the file to be opened.

If the file exists, it is opened. If the file does not exist, it is created. You can create an empty file (touch) by exiting the editor.

Note – You cannot save a file to a different name from the trusted editor.

Using the Solaris Management Console

The Solaris Management Console program invokes a Java-based administrative GUI for configuring and maintaining users and networks. The GUI lists toolboxes in a Navigation pane, as shown in the following figure.
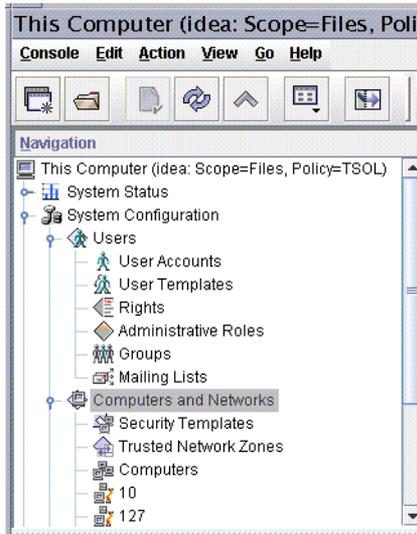
FIGURE 7–1 Solaris Management Console Tools in the Navigation Pane

Trusted Extensions extends the Solaris Management Console to accommodate labels. A toolbox whose name includes `Policy=TSOL` recognizes Trusted Extensions features. The following tools recognize Trusted Extensions features:

User Accounts – Part of the Users tool, for administering users. In Trusted Extensions, the default label and the clearance of a user can be changed here.

Administrative Roles – Part of the Users tool, for administering roles. In Trusted Extensions, the default label and the clearance of a role can be changed here.

Rights – Part of the Users tool, for constructing rights profiles. In Trusted Extensions, actions can be added to rights profiles.

Security Templates – Part of the Computers and Networks tool. This tool creates remote host templates, that is, updates the `tnrhtp` database, and assigns hosts to a template, that is, updates the `tnrhdb` database.

Trusted Network Zones – Part of the Computers and Networks tool. This tool associates zone names with labels, that is, updates the `tnzonecfg` database.

Other tools in the Solaris Management Console work as they do in the Solaris OS.

▼ How to Locate a Solaris Management Console Tool for Trusted Extensions

`Scope=Files, Policy=TSOL` tools modify local files. `Scope=LDAP, Policy=TSOL` tools modify naming service files. Read the online help for what the tool does and how to use it.

Before You Begin   You must be superuser or a role in the global zone.

1   Launch the Solaris Management Console.

   # **/usr/sbin/smc &**

2   Open a Trusted Extensions toolbox.

   Find a toolbox whose name is similar to the following:

   This Computer (*this-host*: Scope=Files, Policy=TSOL)

3   Click the key to the left of System Configuration.

   In the Scope=Files, Policy=TSOL toolbox, under System Configuration, all Trusted Extensions tools are available.

   In the Scope=LDAP, Policy=TSOL toolbox, the Trusted Network Zones tool is not available. This tool operates on labeled zones on the local host only, so is not administered by a naming service.

Allocating and Deallocating Devices

The Device Allocation Manager enables you to allocate and deallocate devices. Devices must be allocated before they can be used.

▼ How to Allocate a Device

Before You Begin   You must be superuser or a role to allocate a device for use in the global zone. You allocate the device from the global zone.

1   Click the Device Allocation icon.

   Click the triangle that is above the Style Manager icon on the Front Panel. Its Tools subpanel includes the Device Allocation Manager icon.
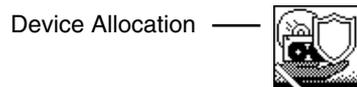
   Device Allocation ————

2   Double-click the device that you want to allocate.

   - audio[*n*] – Is a microphone and speaker.
   - floppy[*n*] – Is a diskette drive.
   - disk[*n*] – Is a removable disk, such as a JAZ or ZIP drive.
   - cdrom[*n*] – Is a CD-ROM drive.
   - tape[*n*] – Is a tape drive.

3   Click Yes to mount the device.

   A File Manager pops up showing the mount point.

Troubleshooting   If a File Manager does not appear, open a File Manager from the Front Panel. Navigate to /, and double-click `floppy`.

▼ How to Deallocate a Device

1   **Deallocate the device.**

    a.   **Find the workspace where the Device Allocation action is displayed**

    b.   **Double-click the device to be deallocated from the list of allocated devices.**

2   **Remove the media and click OK in the Deallocation dialog box.**

Copying To and From Portable Media

When copying to a portable medium, label the medium with the sensitivity label of the information.

Note – During installation, superuser or an equivalent role copies administrative files to and from portable media. Label the media with `Trusted Path`.

▼ How to Copy Files to Portable Media

Before You Begin   To copy administrative files, you must be in a role in the global zone. For this procedure, you are using Solaris Trusted Extensions (CDE).

1   **Allocate the appropriate device.**

Use the Device Allocation Manager, and insert clean media.

For details, see "How to Allocate a Device" on page 109. A File Manager displays the contents of the removable media.

2   **Open a second File Manager from the Front Panel.**

3   **Navigate to the folder that contains the files to be copied**

For example, you might have copied files to an /export/clientfiles folder.

4   **Highlight the icon for a file and drag the file to the File Manager for the removable media.**

Repeat until all files are copied.

5   **Deallocate the device.**

For details, see "How to Deallocate a Device" on page 110.

6 **On the File Manager for the removable media, choose Eject from the File menu.**

Note – Remember to physically affix a label to the medium with the sensitivity label of the copied files.

Example 7–3 Keeping Configuration Files Identical on All Systems

The system administrator wants to ensure that every machine is configured with the same settings. So, on the first machine that is configured, she creates a directory that cannot be deleted between reboots. In that directory, the administrator places the files that should be identical or very similar on all systems.

For example, she copies the Trusted Extensions toolbox that the Solaris Management Console uses for the LDAP scope, /var/sadm/smc/toolboxes/tsol_ldap/tsol_ldap.tbx. She has customized remote host templates in the tnrhtp file, has a list of DNS servers, and audit configuration files. She also modified the policy.conf file for her site. So, she copies the files to the permanent directory.

```
# mkdir /export/commonfiles
# cp  /etc/security/policy.conf \
/etc/security/audit_control \
/etc/security/audit_startup \
/etc/security/tsol/tnrhtp \
/etc/resolv.conf \
/etc/nsswitch.conf \
/export/commonfiles
```

She uses the Device Allocation Manager to allocate a diskette in the global zone, and transfers the files to the diskette. On a separate diskette, labeled ADMIN_HIGH, she puts the label_encodings file for the site.

When she copies the files onto a system, she modifies the dir: entries in the /etc/security/audit_control file for that system.

▼ How to Copy Files From Portable Media

It is safe practice to rename the original Trusted Extensions file before replacing the file. When configuring a system, the root role renames and copies administrative files.

Before You Begin To copy administrative files, you must be superuser or in a role in the global zone. For this procedure, you are using Solaris Trusted Extensions (CDE).

1 **Allocate the appropriate device.**

For details, see "How to Allocate a Device" on page 109.

2 **Insert the media that contains the administrative files.**

3   **If the system has a file of the same name, copy the original file to a new name.**
For example, add .orig to the end of the original file:

`# cp /etc/security/tsol/tnrhtp /etc/security/tsol/tnrhtp.orig`

4   **Open a File Manager from the Front Panel.**

5   **Navigate to the desired destination directory, such as** /etc/security/tsol

6   **In the File Manager for the mounted media, highlight the icon for the file.**
Then drag the file to the destination directory in the second File Manager.

7   **Deallocate the device.**
For details, see "How to Deallocate a Device" on page 110.

8   **When prompted, eject the media.**
Then remove the media.

Site Security Policy

Each Solaris Trusted Extensions site is unique and must determine its own security policy. Perform the following tasks when creating and managing a security policy.

- Establish a security team. The security team should have representation from toplevel management, personnel management, computer system management and administrators, and facilities management. The team should review Trusted Extensions administrators' policies and procedures, and recommend general security policies that apply to all system users.

- Educate management and administration personnel about the site security policy All personnel involved in the management and administration of the site should be educated about the security policy. Security policies should not be made available to ordinary users because this policy information has direct bearing on the security of the computer systems.

- Educate users about Trusted Extensions software and the policy. All users must be familiar with the *Solaris Trusted Extensions User's Guide*. Because the users are usually the first to know when a system is not functioning normally, the user should become acquainted with the system and report any problems to a system administrator. A secure environment needs the users to notify the system administrators immediately if they notice:

    - A discrepancy in the last login time that is reported at the beginning of each session

    - An unusual change to file data

    - A lost or stolen human-readable printout

    - The inability to operate a user function

- Enforce the security policy. If the security policy is not followed and enforced, the data contained in the system that is configured with Trusted Extensions is not secure. Procedures should be established to record any problems and the measures that were taken to resolve the incidents.

- Review the security policy. The security team should perform a periodic review of the security policy and all incidents that occurred since the last review. Adjustments to the policy can then lead to increased security.

Site Security Policy and Trusted Extensions

The security administrator should design the Trusted Extensions network based on the site's security policy. The security policy dictates configuration decisions, such as the following:

- How much auditing is done for all users in the system and for which classes of events
- How much auditing is done for users in roles and for which classes of events
- How audit data is managed, archived, and reviewed
- Which labels are used in the system and whether the ADMIN_LOW and ADMIN_HIGH labels will viewable by ordinary users
- Which user clearances are assigned to individuals
- Which devices (if any) can be allocated by which ordinary users
- Which label ranges are defined for machines, printers, and other devices
- Whether Trusted Extensions is used in an evaluated configuration or not

Computer Security Recommendations

The following list of guidelines provides some things to consider when developing a security policy for your site.

- The maximum label of a system that is configured with Trusted Extensions should not be greater than the maximum security level of work being done at the site.
- System reboots, power failures, and shutdowns should all be recorded manually in a site log.
- File-system damage should be documented and all affected files should be analyzed for potential security-policy violations.
- Operating manuals and administrator documentation should be restricted to individuals with a valid need for access to that information.
- Unusual or unexpected behavior of any Trusted Extensions software should be reported and documented, and the cause should be determined.
- If possible, at least two individuals should administer systems that are configured with Trusted Extensions. One should be assigned security administrator authorization for security-related decisions, and the other should be assigned the system administrator authorization for computer management tasks.
- A regular backup routine should be established.
- Authorizations should be assigned only to users who need them and who can be trusted to use them properly.
- Privileges should be assigned to programs only when the program needs the privileges to do its work, and only when the programs have been scrutinized and proven to be trustworthy in their use of privilege. Review the privileges on existing Trusted Extensions programs for a guide to setting privileges on new programs.

- Audit information should be reviewed and analyzed regularly. Any irregular events should be noted and investigated to determine the cause of the event.
- The number of administration IDs should be minimized.
- The number of setuid and setgid programs should be minimized. Such programs should be employed only in protected subsystems.
- An administrator should regularly verify that ordinary users have a valid login shell.
- An administrator should regularly verify that ordinary users have valid user ID values and not system administration ID values.

Physical Security Recommendations

- Restrict access to the systems that are configured with Trusted Extensions. The most secure locations are generally interior rooms that are not on the ground floor.
- Monitor and document access to systems that are configured with Trusted Extensions.
- Secure computer equipment to large objects such as tables and desks to prevent theft. When equipment is secured to a wooden item, increase the strength of the item by adding metal plates.
- Consider removable storage media for sensitive information. Lock up all removable media when the media are not in use.
- Store system backups and archives in a secure location that is separate from the location of the systems.
- Restrict physical access to the backup and archival media in the same manner as you restrict access to the systems.
- Install a high-temperature alarm in the computer facility to indicate when the temperature is outside the range of the manufacturer's specifications. A suggested range is 10°C to 32°C (50°F to 90°F).
- Install a water alarm in the computer facility to indicate water on the floor, in the subfloor cavity, and in the ceiling.
- Install a smoke alarm to indicate fire, and Install a fire-suppression system.
- Install a humidity alarm to indicate too much or too little humidity.
- Consider TEMPEST shielding if machines do not have it. TEMPEST shielding might be appropriate for facility walls, floors, and ceilings.
- Only certified technicians should open and close TEMPEST equipment to ensure its ability to shield electromagnetic radiation.
- Check for physical gaps that allow entrance to the facility or the rooms containing computer equipment. Look for openings under raised floors, in suspended ceilings, in roof ventilation equipment, and in adjoining walls between original and secondary additions.
- Prohibit eating, drinking, and smoking in computer facilities or near computer equipment. Establish areas where these activities can occur without threat to the computer equipment.
- Protect architectural drawings and diagrams of the computer facility.

■ Restrict the use of building diagrams, floor maps, and photographs of the computer facility.

Personnel Security Recommendations

■ Inspect packages, documents, and storage media entering and leaving a secure site.

■ Require identification badges on all personnel and visitors at all times.

■ Use identification badges that are difficult to copy or counterfeit.

■ Establish areas that are prohibited for visitors and clearly mark the areas.

■ Escort visitors at all times.

Common Security Violations

Because no computer is 100% secure, a computer facility is only as secure as the people who use it. The limitations of an administrator are directly related to the actions of every individual who is involved with the use of computer equipment and its facilities. Most actions that violate security are easily resolved by careful users or additional equipment. However, the following list gives examples of problems that can occur:

■ Users give passwords to other individuals who should not have access to the computer system.

■ Users write down passwords and lose or leave the passwords in nonsecure locations.

■ Users set their passwords to easily guessed words or easily guessed names.

■ Users learn passwords by watching other users typing a password.

■ Unauthorized users remove, replace, or physically tamper with hardware.

■ Users leave their computers or terminals unattended without locking the screen.

■ Users change the permissions on a file to allow other users to read the file.

■ Users change the labels on a file to allow other users to read the file.

■ Users discard sensitive hardcopy documents without shredding them or leave sensitive hardcopy documents in insecure locations.

■ Users leave access doors unlocked.

■ Users lose their keys.

■ Users do not lock up removable storage media.

■ Computer screens are visible through exterior windows.

■ Network cables are tapped.

■ Electronic eavesdropping captures signals emitted from computer equipment.

■ Power outages, surges, and spikes destroy data.

■ Earthquakes, floods, tornadoes, hurricanes, and lightning destroy data.

■ External electromagnetic radiation interference such as sun-spot activity scrambles files.

Additional Security References

Government publications describe in detail the standards, policies, methods, and terminology associated with computer security. Other publications listed here are guides for system administrators of UNIX systems and are useful in gaining a thorough understanding of UNIX security problems and solutions.

The web also provides resources. In particular, the CERT (`http://www.cert.org`) website alerts companies and users to security holes in the software. The SANS (`http://www.sans.org/index.php`) institute offers training, an extensive glossary of terms, and an updated list of top threats from the Internet.

U.S. Government Publications

The U.S. government makes its publications available on the web. The Computer Security Resource Center (CSRC) of the National Institute of Standards and Technology (NIST) publishes articles on computer security. The following are a sample of the publications that can be downloaded from the NIST (`http://csrc.nist.gov/index.html`) site.

- *An Introduction to Computer Security: The NIST Handbook*, SP 800-12, October 1995.

- *Standard Security Label for Information Transfer*, FIPS-188, September 1994.

- Swanson, Marianne and Barbara Guttman, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, SP 800-14, September 1996.

- Tracy, Miles, Wayne Jensen, and Scott Bisker, *Guidelines on Electronic Mail Security*, SP 800-45, September 2002. Section E.7 concerns securely configuring LDAP for mail.

- Wilson, Mark and Joan Hash, *Building an Information Technology Security Awareness and Training Program*, SP 800-61, January 2004. Includes a useful glossary.

- Grace, Tim, Karen Kent, and Brian Kim, *Computer Security Incident Handling Guidelines*, SP 800-50, September 2002. Section E.7 concerns securely configuring LDAP for mail.

- Souppaya, Murugiah, John Wack, and Karen Kent, *Security configuration Checklists Program for IT Products*, SP 800-70, May 2005.

UNIX Security Publications

Chirillo, John and Edgar Danielyan, *Sun® Certified Security Administration for Solaris™ 9 & 10 Study Guide*, McGraw-Hill/Osborne, 2005.

Garfinkel, Simson, Gene Spafford, and Alan Schwartz, *Practical UNIX and Internet Security, 3rd Edition*, O'Reilly & Associates, Inc, Sebastopol, CA, 2006.

General Computer Security Publications

Brunette, Glenn M. and Schuba, Christoph L., *Toward Systemically Secure IT Architectures*, Sun Microsystems, Inc, June 2005.

Kaufman, Charlie, Radia Perlman, and Mike Speciner, *Network Security: Private Communication in a Public World, 2nd Edition*, Prentice-Hall, 2002.

Pfleeger, Charles P. and Shari Lawrence Pfleeger, *Security in Computing*, Prentice Hall PTR, 2006.

Privacy for Pragmatists: A Privacy Practitioner's Guide to Sustainable Compliance, Sun Microsystems, Inc, August 2005.

Rhodes-Ousley, Mark, Roberta Bragg, and Keith Strassberg, *Network Security: The Complete Reference*, McGraw-Hill/Osborne, 2004.

Stoll, Cliff, *The Cuckoo's Egg*, Doubleday, 1989.

General UNIX Publications

Bach, Maurice J., *The Design of the UNIX Operating System*, Prentice Hall, Englewood Cliffs, NJ, 1986.

Nemeth, Evi, Garth Snyder, and Scott Seebas, *UNIX System Administration Handbook*, Prentice Hall, Englewood Cliffs, NJ, 1989.

B

Configuration Checklist for Trusted Extensions

This checklist provides an overall view of the big configuration tasks. The smaller tasks are outlined within the big tasks. The checklist does not take the place of following the steps in the guide.

Checklist for Configuring Trusted Extensions

The following list summarizes what is required to install and configure Trusted Extensions at your site.

1. Read
   - Read Part 1 of *Solaris Trusted Extensions Administrator's Procedures*
   - Understand site security requirements.
   - Read "Site Security Policy and Trusted Extensions" on page 114.

2. Prepare
   - Decide the root password.
   - Decide the PROM or BIOS security level.
   - Decide the PROM or BIOS password.
   - Decide if attached peripherals are permitted.
   - Decide if access to remote printers is permitted.
   - Decide if access to unlabeled networks is permitted.
   - Decide the zone creation method.

3. Install Trusted Extensions
   a. Install the Solaris OS.
      - For remote administration, install the Developer Group or larger group of Solaris packages.
      - For the Clone Zone creation method, select Custom Install, then lay out a /zone partition.
   b. Add Trusted Extensions packages.
   c. Start any services that are disabled.

4. If using IPv6, enable IPv6 for Trusted Extensions

5. Configure labels

    a. Finalize your site's `label_encodings` file.
    b. Check and install the file.
    c. Reboot.

6. Configure interfaces for the global zone and for labeled zones

7. Configure the Solaris Management Console

8. Configure LDAP

    a. Either create a Trusted Extensions proxy server, or a Trusted Extensions LDAP server.

    b. Register the Solaris Management Console with LDAP.

    c. Create LDAP toolbox for the Solaris Management Console.

9. Configure network connection for LDAP

    ■ Assign LDAP server or proxy server to the `cipso` host type in a remote host template.

    ■ Assign local system to the `cipso` host type in a remote host template.

10. Configure labeled zones

    a. In the Solaris Management Console, associate zone names with particular labels.
    b. Run the Configure Zone action.
    c. (Optional) Create ZFS pool for cloning zones.

11. Create labeled zones

    a. Run the Install Zone action.

    b. Run the Initialize for LDAP action.

    c. Run the Start Zone action.

    d. Customize the running zone.

    e. Run the Shut Down Zone action.

    f. Customize the zone while the zone is shut down.

    g. (Optional) Create ZFS snapshot.

    h. Create the remaining zones from scratch, or by using the Copy Zone or the Clone Zone action.

12. Configure the network
    ■ Identify single-label hosts and limited range hosts.
    ■ Determine the labels to apply to incoming data from unlabeled hosts.
    ■ Customize remote host templates.
    ■ Assign individual hosts to templates.
    ■ Assign subnets to templates.

13. Establish static routing

14. Configure local users and local administrative roles
    ■ Create the Security Administrator role.
    ■ Create a local user who can assume the Security Administrator role.

- Create other roles, and possibly other local users to assume these roles.

15. Create home directories on the NFS server
    - Create home directories for each user at every label that the user can access.
    - (Optional) Prevent users from reading their lower-level home directories.

16. Configure printing

17. Configure devices
    a. Assign the Device Management profile or the System Administrator profile to a role.
    b. To make devices usable, do one of the following:
        - Per machine, make devices allocatable.
        - Assign Allocate Device authorization to selected users and roles.

18. Configure Solaris features
    - Configure auditing.
    - Configure security settings.
    - Enable particular LDAP clients to be LDAP administration systems.
    - Configure users in LDAP.
    - Configure network roles in LDAP.
    - Mount and share file systems.

Glossary

accreditation range	A set of sensitivity labels that are approved for a class of users or resources. A set of valid labels. See also system accreditation range and user accreditation range.
administrative role	A role that gives required authorizations, privileged commands, privileged actions, and the Trusted Path security attribute to allow the role to perform administrative tasks. Roles perform a subset of Solaris superuser's capabilities, such as backup or auditing.
allocation	A mechanism by which access to a device is controlled. See device allocation.
application search path	In CDE, the search path is used by the system to find applications and certain configuration information. The application search path is controlled by a trusted role.
authorization	A right granted to a user or role to perform an action that would otherwise not be allowed by security policy. Authorizations are granted in rights profiles. Certain commands require the user to have certain authorizations to succeed. For example, to print a PostScript file requires the Print Postscript authorization.
CDE	See Common Desktop Environment.
CIPSO label	Common IP Security Option. CIPSO is the label standard that Trusted Extensions implements.
clearance	The upper limit of the set of labels at which a user can work. The lower limit is the minimum label that is assigned by the security administrator. A clearance can be one of two types, a session clearance or a user clearance.
client	A system connected to a network.
closed network	A network of systems that are configured with Trusted Extensions. The network is cut off from any non-Trusted Extensions host. The cutoff can be physical, where no wire extends past the Trusted Extensions network. The cutoff can be in the software, where the Trusted Extensions hosts recognize only Trusted Extensions hosts. Data entry from outside the network is restricted to peripherals attached to Trusted Extensions hosts. Contrast with open network.
Common Desktop Environment	The historical windowing environment for administering Trusted Extensions software. In this release, the Sun Java Desktop System Java DS can also be used.

.copy_files file	An optional setup file on a multilabel system. This file contains a list of startup files, such as `.cshrc` or `.mozilla`, that the user environment or user applications require in order for the system or application to behave well. The files that are listed in `.copy_files` are then *copied* to the user's home directory at higher labels, when those directories are created. See also .link_files file.
DAC	See discretionary access control.
device	Devices include printers, computers, tape drives, floppy drives, CD-ROM drives, DVD drives, audio devices, and internal pseudo terminal devices. Devices are subject to the read equal write equal MAC policy. Access to removable devices, such as DVD drives, are controlled by device allocation.
device allocation	A mechanism for protecting the information on an allocatable device from access by anybody except the user who allocates the device. Until a device is deallocated, no one but the user who allocated a device can access any information that is associated with the device. For a user to allocate a device, that user must have been granted the Device Allocation authorization by the security administrator.
discretionary access control	The type of access that is granted or that is denied by the owner of a file or directory at the discretion of the owner. Solaris Trusted Extensions provides two kinds of discretionary access controls (DAC), UNIX permission bits and ACLs.
domain	A part of the Internet naming hierarchy. It represents a group of systems on a local network that share administrative files.
domain name	The identification of a group of systems on a local network. A domain name consists of a sequence of component names separated by periods (for example: example1.town.state.country.org). As you read a domain name from left to right, the component names identify more general, and usually remote, areas of administrative authority.
evaluated configuration	One or more Trusted Extensions hosts that are running in a configuration that has been certified as meeting specific criteria by a certification authority. In the United States, those criteria are the TCSEC. The evaluating and certifying body is the NSA. Solaris Trusted Extensions software will be certified to the Common Criteria v2.1 [August 1999], an ISO standard, to Evaluation Assurance Level (EAL) 4, and against a number of protection profiles.
	The Common Criteria v2 (CCv2) and protection profiles make the earlier TCSEC U.S. standard obsolete through level B1+. A mutual recognition agreement for CCv2 has been signed by the United States, the United Kingdom, Canada, Denmark, the Netherlands, Germany, and France.
	The Trusted Extensions configuration target provides functionality that is similar to the TCSEC C2 and B1 levels, with some additional functionality.
file system	A collection of files and directories that, when set into a logical hierarchy, make up an organized, structured set of information. File systems can be mounted from your local system or a remote system.

GFI
Government Furnished Information. In this manual, it refers to a U.S. government-provided label_encodings file. In order to use a GFI with Trusted Extensions software, you must add the Sun-specific LOCAL DEFINITIONS section to the end of the GFI. For details, see Chapter 5, "Customizing LOCAL DEFINITIONS," in *Solaris Trusted Extensions Label Administration*.

host name
The name by which a system is known to other systems on a network. This name must be unique among all the systems within a given domain. Usually, a domain identifies a single organization. A host name can be any combination of letters, numbers, and minus sign (−), but it cannot begin or end with a minus sign.

initial label
The minimum label assigned to a user or role, and the label of the user's initial workspace. The initial label is the lowest label at which the user or role can work.

install team
A team of at least two people who together oversee the installation and configuration of Solaris Trusted Extensions software. One team member is responsible for security decisions, and the other for system administration decisions.

IP address
Internet protocol address. A unique number that identifies a networked system so it can communicate by means of Internet protocols. In IPv4, the address consists of four numbers separated by periods. Most often, each part of the IP address is a number between 0 and 225. However, the first number must be less than 224 and the last number cannot be 0.

IP addresses are logically divided into two parts: the network, and the system on the network. The network number is similar to a telephone area code. In relation to the network, the system number is similar to a phone number.

label
A security identifier that is assigned to an object. The label is based on the level at which the information in that object should be protected. Depending on how the security administrator has configured the user, a user can see the sensitivity label, or no labels at all. Labels are defined in the label_encodings file.

label configuration
A Trusted Extensions installation choice of single-label or multilabel sensitivity labels. In most circumstances, label configuration is identical on all systems at your site.

label_encodings file
The file where the complete sensitivity label is defined, as are accreditation ranges, label view, default label visibility, default user clearance, and other aspects of labels.

label range
A set of sensitivity labels that are assigned to commands, zones, and allocatable devices. The range is specified by designating a maximum label and a minimum label. For commands, the minimum and maximum labels limit the labels at which the command can be executed. Remote hosts that do not recognize labels are assigned a single sensitivity label, as are any other hosts that the security administrator wants to restrict to a single label. A label range limits the labels at which devices can be allocated and restrict the labels at which information can be stored or processed when using the device.

label set
See security label set.

labeled host   A labeled host sends network packets that are labeled with CIPSO labels. All Trusted Extensions hosts are labeled hosts.

.link_files file   An optional setup file on a multilabel system. This file contains a list of startup files, such as .cshrc or .mozilla, that the user environment or user applications require in order for the system or application to behave well. The files that are listed in .link_files are then *linked* to the user's home directory at higher labels, when those directories are created. See also .copy_files file.

MAC   See mandatory access control.

mandatory access control   Access control that is based on comparing the sensitivity label of a file, directory, or device to the sensitivity label of the process that is trying to access it. The MAC rule, read equal–read down, applies when a process at one label attempts to read a file at a lower label. The MAC rule, write equal-read down, applies when a process at one label attempts to write to a directory at another label.

minimum label   The lower bound of a user's sensitivity labels and the lower bound of the system's sensitivity labels. The minimum label set by the security administrator when specifying a user's security attributes is the sensitivity label of the user's first workspace at first login. The sensitivity label that is specified in the minimum label field by the security administrator in the label_encodings file sets the lower bound for the system.

naming service   A distributed network database that contains key system information about all the systems on a network, so that the systems can communicate with each other. With a naming service, the system information can be maintained, managed, and accessed on a network-wide basis. Sun supports the LDAP naming service. Without such a service, each system has to maintain its own copy of the system information in the local /etc files.

networked systems   A group of systems that are connected through hardware and software, sometimes referred to as a local area network (LAN). One or more servers are usually needed when systems are networked.

non-networked systems   Computers that are not connected to a network or do not rely on other hosts.

open network   A network of Solaris Trusted Extensions hosts that is connected physically to other networks and that uses Trusted Extensions software to communicate with non-Trusted Extensions hosts. Contrast with closed network.

outside the evaluated configuration   When software that has been proved to be able satisfy the criteria for an evaluated configuration, is configured with settings that do not satisfy security criteria, the software is described as being *outside the evaluated configuration*.

permission bits   A type of discretionary access control in which the owner specifies a set of bits to signify who can read, write, or execute a file or directory. Three different sets of permissions are assigned to each file or directory: one set for the owner, one set for the owner's group, and one set for all others.

primary administrator   The person who is entrusted to create new rights profiles for the organization, and to fix machine difficulties that are beyond the power of the security administrator and system administrator

combined. This role should be assumed rarely. After initial security configuration, more secure sites can choose not to create this role, and not to assign any role the Primary Administrator profile.

privilege Powers that are granted to a process that is executing a command. The full set of privileges describes the full capabilities of the system, from basic capabilities to administrative capabilities. Privileges that bypass security policy, such as setting the clock on a system, can be granted by a site's security administrator.

process An action that executes a command on behalf of the user who invokes the command. A process receives a number of security attributes from the user, including the user ID (UID), the group ID (GID), the supplementary group list, and the user's audit ID (AUID). Security attributes received by a process include any privileges that are available to the command being executed and the sensitivity label of the current workspace.

profile shell A special shell that recognizes privileges. A profile shell typically limits users to fewer commands, but can allow these commands to run with privilege. The profile shell is the default shell of a trusted role.

remote host A different system than the local system. A remote host can be an unlabeled host or a labeled host.

rights profile A bundling mechanism for commands and CDE actions and for the security attributes that are assigned to these executables. Rights profiles allow Solaris administrators to control who can execute which commands and to control the attributes these commands have when they are executed. When a user logs in, all rights assigned to that user are in effect, and the user has access to all the commands, CDE actions, and authorizations assigned in all of that user's rights profiles.

role A role is like a user, except that a role cannot log in. Typically, a role is used to assign administrative capabilities. Roles are limited to a particular set of commands and CDE actions. See administrative role.

security administrator In an organization where sensitive information must be protected, the person or persons who define and enforce the site's security policy. These persons are cleared to access all information that is being processed at the site. In software, the Security Administrator administrative role is assigned to one or more individuals who have the proper clearance. These administrators configure the security attributes of all users and hosts so that the software enforces the site's security policy. In contrast, see system administrator.

security attribute An attribute that is used to enforce Trusted Extensions security policy. Various sets of security attributes are assigned to processes, users, zones, hosts, allocatable devices, and other objects.

security label set Specifies a discrete set of security labels for a tnrhtp database entry. Hosts that are assigned to a template with a security label set can send and receive packets that match any one of the labels in the label set.

security policy	On a Trusted Extensions host, the set of DAC, MAC, and labeling rules that define how information can be accessed. At a customer site, the set of rules that define the sensitivity of the information being processed at that site and the measures that are used to protect the information from unauthorized access.
sensitivity label	A security label that is assigned to an object or a process. The label is used to limit access according to the security level of the data that is contained.
Solaris Management Console	A Java-based administrative GUI that contains toolboxes of administrative programs. In CDE, this GUI can be launched from the Application Manager. Most system, network, and user administration is done by using the Console toolboxes.
system	Generic name for a computer. After installation, a system on a network is often referred to as a host.
system accreditation range	The set of all valid labels that are created according to the rules that the security administrator defines in the label_encodings file, plus the two administrative labels that are used on every system that is configured with Trusted Extensions. The administrative labels are ADMIN_LOW and ADMIN_HIGH.
system administrator	In Trusted Extensions, the trusted role assigned to the user or users who are responsible for performing standard system management tasks such as setting up the non-security-relevant portions of user accounts. In contrast, see security administrator.
tnrhdb database	The trusted network remote host database. This database assigns a set of label characteristics to a remote host. The database is accessible either as a file in /etc/security/tsol/tnrhdb or from the LDAP server.
tnrhtp database	The trusted network remote host template. This database defines the set of label characteristics that a remote host can be assigned. The database is accessible either as a file in /etc/security/tsol/tnrhtp, or from the LDAP server.
toolbox	A collection of programs in the Solaris Management Console. On a Trusted Extensions host, administrators use Policy=TSOL toolboxes. Each toolbox has programs that are usable in the scope of the toolbox. For example, the Trusted Network Zones tool, which handles the system's tnzonecfg database, exists only in the Files toolbox, because its scope is always local. The User Accounts program exists in all toolboxes. To create a local user, the administrator uses the Files toolbox, and to create a network user, the administrator uses the LDAP toolbox.
Trusted Network databases	tnrhtp, the trusted network remote host template and tnrhdb, the trusted network remote host database together define the remote hosts that a Trusted Extensions system can communicate with.
trusted role	See administrative role.
trusted stripe	A region that cannot be spoofed. In CDE, the trusted stripe is at the bottom of the screen, and in Java DS the stripe can be at the top. The stripe provides visual feedback about the state of the window

system: a trusted path indicator and window sensitivity label. When sensitivity labels are configured to not be viewable for a user, the trusted stripe is reduced to an icon that displays only the trusted path indicator.

unlabeled host   A system that sends unlabeled network packets, such as a system that is running the Solaris OS.

user accreditation range   The set of all possible labels at which an ordinary user can work on the system. The site's security administrator specifies the range in the label_encodings file file. The rules for well-formed labels that define the system accreditation range are additionally restricted by the values in the ACCREDITATION RANGE section of the file: the upper bound, the lower bound, the combination constraints and other restrictions.

user clearance   The clearance assigned by the security administrator that sets the upper bound of the set of labels at which a user can work at any time. The user can decide to accept the default, or can further restrict that clearance during any particular login session.

Index