



Trusted Solaris Installation and Configuration

Trusted Solaris 8 4/01

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

Part No: 816-1040-10
November 2001

Copyright 2001 Sun Microsystems, Inc. 901 San Antonio Road Palo Alto, CA 94303-4900 U.S.A. All rights reserved.

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

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

Sun, Sun Microsystems, the Sun logo, docs.sun.com, AnswerBook, AnswerBook2, Trusted Solaris, OpenWindows, Solaris Management Console, JumpStart, Solaris Web Start, Netra, and Solaris are trademarks, registered trademarks, or service marks of Sun Microsystems, Inc. in the U.S. and other countries. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.

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

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

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

Copyright 2001 Sun Microsystems, Inc. 901 San Antonio Road Palo Alto, CA 94303-4900 U.S.A. Tous droits réservés

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

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

Sun, Sun Microsystems, le logo Sun, docs.sun.com, AnswerBook, AnswerBook2, OpenWindows, Solaris Management Console, JumpStart, Solaris Web Start, Netra, et Solaris sont des marques de fabrique ou des marques déposées, ou marques de service, de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays. Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux Etats-Unis et dans d'autres pays. Les produits portant les marques SPARC sont basés sur une architecture développée par Sun Microsystems, Inc.

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

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



011026 @2471



Contents

Preface	15
1 Security Overview	23
Planning for Security	23
Understanding the Trusted Solaris Environment	24
Understanding Your Site's Security Policy	24
Devising an Administration Strategy	25
Devising a Label Strategy	26
Planning User Security	27
Planning System Hardware and Capacity	28
Planning Your Network	29
Planning Auditing	30
Devising an Installation and Configuration Strategy	31
Collecting Information	31
Backing Up the System	32
Installing the Trusted Solaris Software	32
Configuring the Software	32
Differences From Solaris Installation and Configuration	34
Installation Results from an Administrator's Perspective	34
2 Installation and Configuration Task Maps	37
Preparing for Installation (Task Map)	37
Installing a System From CD-ROM (Task Map)	38
Installing Systems Over the Network (Task Map)	38
Configuring Headless Systems (Task Map)	39

3	Installing the Trusted Solaris Operating Environment	41
	Install Team Responsibilities	41
	Differences from the Solaris 8 Installation Program	42
	Recommendations for the Trusted Solaris Environment	42
	Shutting Down the System to be Installed	42
	▼ Shut Down a Trusted Solaris System	43
	Installing From a CD-ROM	43
	▼ Insert the First Trusted Solaris 8 4/01 CD and Boot	43
	▼ Read Booting Messages	44
	▼ Answer Installation Questions	44
	▼ Enter a root Password	45
	▼ Insert the Second Trusted Solaris 8 4/01 CD	45
	▼ Read the Log	46
	▼ Configure the Trusted Solaris System	46
	Troubleshooting	47
	Installing Over the Network	47
	▼ Boot Over the Network or with Custom Files	47
	▼ Finish Configuring Systems Installed Over the Network	48
4	Configuring a System with No Name Service	49
	Who Does What	49
	No Name Service Configuration Tasks	49
	Logging In and Launching a Terminal	50
	▼ Log In	50
	▼ Assume the root Role	51
	▼ Launch a Terminal	52
	Protecting the Machine	52
	▼ SPARC: Protect Machine Hardware	53
	▼ IA: Protect the BIOS	53
	Setting Up Labels	53
	▼ Create an Admin_High Workspace	54
	▼ Allocate the Appropriate Device	54
	▼ Check and Install Your Label Encodings File	55
	▼ Deallocate the Device	56
	Initializing the Solaris Management Console	56
	▼ Initialize the SMC Server	56
	▼ (Optional) Save the Current Toolbox	58

(Optional) Configuring Routing	59
▼ Set Up Simple Static Routing	59
▼ Set up Static Routing Using Extended Metrics	60
Configuring Network Files	60
▼ Add Hosts to the System's Known Network	60
▼ (Optional) Remove the 0.0.0.0 Network	61
▼ Add a Remote Host Template	61
▼ Assign a Template to a Remote Host	62
▼ (Optional) Set Up DNS	63
Creating Roles and Users	64
▼ Create Administrative Roles	64
▼ Create Users Who Will Assume Roles	66
Verifying That Roles Work	69
▼ Reboot the Computer	69
▼ Verify that the Roles secadmin and admin Work	69
▼ Verify that the Role primaryadmin Works	70
Finishing Up Configuration	70
▼ Set Up Auditing	70
▼ (Optional) Share File Systems	70
▼ (Optional) Mount File Systems	71
▼ (Optional) Delete the User install	71
▼ Other Setup	72
 5 Configuring a Name Service Master	 73
Who Does What	73
Name Service Master Configuration Tasks	73
Initial Configuration	74
▼ Initially Configure the Machine	74
(Optional) Configuring Routing	75
▼ Set Up Simple Static Routing	75
▼ Set up Static Routing Using Extended Metrics	76
Configuring the Network	76
▼ Add Hosts to a Machine's Known Network	76
▼ (Optional) Remove the 0.0.0.0 Network	77
▼ Add a Remote Host Template	77
▼ Assign a Template to a Remote Host	78
Trusted Network Summary	80

Setting Up the Name Server and Domain	80
▼ Set Up Files to be Name Service Databases	80
▼ Modify the /yp/Makefile (NIS domains only)	82
▼ Create NIS Maps from the Staging Area (NIS domains only)	82
▼ Create NIS+ Tables from the Staging Area (NIS+ domains only)	83
▼ Edit SMC Toolbox Definitions for the Name Service	84
▼ (Optional) Set Up DNS	85
▼ Reboot the Computer	86
Name Service References	86
Setting Up Critical Servers	86
▼ Install and Configure the Home Directory and Mail Servers	87
Creating Roles and Users	87
▼ Create Domain-wide Roles and Users	87
▼ Add Roles to the NIS+ Admin Group (NIS+ domains only)	88
Verifying That Roles Work	88
▼ Log Out	88
▼ Verify that the Roles secadmin and admin Work	89
▼ Verify that the Role primaryadmin Works	89
Finishing Up Configuration	89
▼ Set Up Auditing	89
▼ Copy Configuration Files for Distribution to Clients	90
▼ (Optional) Share File Systems	90
▼ (Optional) Mount File Systems	91
▼ (Optional) Delete the User install	91
▼ Other Setup	92
 6 Configuring a Name Service Client	 93
Who Does What	93
Client Configuration Tasks	93
Initial Configuration	95
▼ Log In	95
▼ SPARC: Protect Machine Hardware	95
▼ IA: Protect the BIOS	96
▼ Install the Name Service Master's label_encodings File	96
▼ Mount the Diskette With Configuration Files	97
▼ Initialize the SMC Server	97
(Optional) Configuring Routing	97

▼ Configure to Match the Name Server's Routing Method	98
Configuring the Network	98
▼ Add Hosts to be Contacted During Booting	98
▼ (Optional) Remove the 0.0.0.0 Network	99
▼ Copy the Name Service Master's Tnrhtp Database	99
▼ Assign Templates to Remote Hosts	99
Summary of Client Network Files	100
Connecting to the Name Server	100
▼ Verify Communication with the Name Service Master	100
▼ Add Client to the NIS+ Domain	101
▼ Add Client to the NIS Domain	102
▼ Copy the SMC Name Server Toolbox Definitions to the Client	102
▼ Copy Network Files to the /etc Directory	102
▼ Reboot the Computer	103
▼ Enable the Slave Server (NIS domain only)	103
▼ Add the IMAP Server (NIS+ domain only)	103
Sharing Critical File Systems	104
▼ Share Home Directories	104
▼ Share Mail Server Directories	104
Finish Configuring the System	105
▼ Set Up Auditing to Match the Master Server	105
▼ (Optional) Set Security Attributes on Mounted File Systems	106
▼ (Optional) Mount and Share File Systems	106
▼ (Optional) Delete the Install User	106
7 Installing a Trusted Solaris System Over a Network	107
Setting Up Network Installation	107
▼ Give Mounted Media All Allowed Privileges	108
▼ Allocate the CD-ROM Device	108
▼ Modify Permissions of Mount Point Parent	109
▼ Load Trusted Solaris Images from CDs	109
▼ Share the Network Install Directory	110
▼ Add Client Information to the Install Server	111
Trusted Solaris Modifications to Network Installation	112
Setting Up Custom JumpStart Installation	113
▼ Create a JumpStart Diskette	113
▼ Edit a JumpStart Profile	114

▼ Use pfinstall to Test a Profile	115
▼ Edit a Rules File	115
▼ Validate a Rules File	115
▼ Copy a Rules File	116
Modifying Optional Custom JumpStart Procedures	116
▼ Create Begin and Finish Scripts	116
Trusted Solaris Script Examples	116
Modifications to Creating a Disk Configuration File	117
▼ SPARC: To Create a SPARC Disk Configuration File	118
▼ IA: To Create an Intel Disk Configuration File	118
Modifying a Solaris JumpStart Example	118
▼ Set up the engineering systems for installation	119
▼ Set up the marketing systems for installation	119
8 Configuring a Headless Trusted Solaris System	121
Headless System Configuration Tasks	121
▼ To Set Up Remote CDE Login to a Headless System	122
▼ To Set Up Remote SMC Login to a Headless System	123
▼ To Set Up Administration by Serial Login	125
▼ To Set Up Administration by Remote Login	125
9 Common Procedures	127
Logging In as a User	127
▼ To Log In as a Regular User	127
Ending a Session	128
▼ To Lock the Screen	128
▼ To Log Out	128
▼ To Reboot the System	129
Running Administrative Actions	129
How To Use System_Admin Actions	129
Using the Solaris Management Console	132
Copying to and from a Portable Medium	135
▼ To Copy Files to a Diskette	135
▼ To Copy Files From a Diskette	135
Modifying a Role's Rights	136
▼ To Add a Command to a Role's Rights	136

▼ To Verify That a Command is Available to a Role	137
▼ To Remove a Command from a Role's Rights	137
Saving and Restoring Trusted Solaris Databases	138
▼ To Save Profile and User Attribute Information	138
A Site Security Policy	141
Site Security Policy and the Operating Environment	142
Computer Security Recommendations	142
Physical Security Recommendations	143
Personnel Security Recommendations	144
Common Security Violations	145
Additional Security References	146
U.S. Government Publications	146
UNIX Security Publications	147
General Computer Security Publications	147
General UNIX Publications	148
B Checklists for a Secure Trusted Solaris Environment	149
Site Summary Checklist	149
Reading List	149
Checklist Summaries	149
Planning Labels	150
Label Decisions	150
Planning the Network	151
Open Network Security Information	151
Name Service Domain Information	151
Labels of Communicating Machines	151
Planning Auditing	152
Auditing Security Information	152
Auditing System Information	152
Planning System Configuration	152
Required System Information	152
Security Information for Each Machine	153
C Example Worksheets	155
How to Use the Examples	155

Root NIS+ Master Installation Program Example	155
Root NIS+ Master Disk Partitioning Example	157
Services Provided by Servers Example	158
Audit Server Installation Program Example	159
Audit Server Disk Partitioning Example	162
Audit Server Configuration Worksheet	162

Glossary	165
-----------------	------------

Index	179
--------------	------------

Tables

TABLE 1-1	Trusted Solaris Security Defaults for User Accounts	27
TABLE 1-2	Possible Servers in a Trusted Solaris Environment	29
TABLE 1-3	Templates Provided with Trusted Solaris Network Software	30
TABLE 4-1	secadmin Values in Add Role Dialog	65
TABLE 4-2	secadmin Values in Properties/Modify Dialog	65
TABLE 4-3	User Values in Add User Dialog	67
TABLE 4-4	User Values in Properties/Modify Dialog	68
TABLE 6-1	Task Map for Clients Installed from CD-ROM	94
TABLE 6-2	Task Map for Clients Installed Over a Network	94
TABLE 6-3	Task Map for Clients Installed Using JumpStart	95
TABLE 6-4	Client Static Routing Entry	98
TABLE 7-1	Trusted Solaris Differences in Network Installation	112
TABLE 7-2	Modified Network Commands	113
TABLE 9-1	Trusted Solaris Actions in the System_Admin Folder	130

Figures

FIGURE 1-1	Two Roles Administering a System	32
FIGURE 4-1	The Enable Logins Dialog Box	50
FIGURE 4-2	A Trusted Solaris User Workspace	51
FIGURE 4-3	Solaris Management Console Tools	58
FIGURE 9-1	Solaris Management Console Tools in the Navigation Pane	132

Preface

This book is for knowledgeable system administrators and security administrators who are installing the Trusted Solaris™ operating environment at networked or non-networked sites. Level of trust required by site security policy and level of expertise will determine who can perform the tasks required to install Trusted Solaris software.

Implementing Site Security

Successfully installing and configuring a Trusted Solaris system consistent with site security requires understanding the security features of the Trusted Solaris operating environment and your site security policy. Before attempting to install the Trusted Solaris 8 4/01 software, read Chapter 1 for information on how to ensure site security when installing and configuring the Trusted Solaris environment.

Using Installation Books

Installing the Trusted Solaris operating environment requires Solaris installation books as well as Trusted Solaris ones. See Chapter 2 for information on which books cover which tasks. Because Trusted Solaris software modifies Solaris software for security, Trusted Solaris books often supplement Solaris ones. Administrators should have access to both.

For example, to install the first one or two systems, Chapter 3 supplements the Solaris installation guides.

If you are installing and configuring a network of hosts, you can choose from several installation methods after installing the first system. *Solaris 8 Advanced Installation Guide*, 806-0957-10, contains background information for networked installation, and describes interactive installations: network, JumpStart, and custom JumpStart. Some of the instructions are modified in the Trusted Solaris environment. See “Trusted Solaris Modifications to Network Installation” on page 112 for a list of commands and procedures that the Trusted Solaris environment secures or enhances for network and JumpStart installations.

Note – Instructions for setting up hardware and peripherals are provided in hardware guides, such as the *Solaris 8 Sun Hardware Platform Guide*.

How This Book is Organized

This section describes the chapters in this book.

Chapter 1 describes the security issues when installing the Trusted Solaris operating environment on one or more systems.

Chapter 2 contains task maps for installing and configuring non-networked and networked systems.

Chapter 3 provides instructions for shutting down a Trusted Solaris system and installing the Trusted Solaris 8 4/01 operating environment.

Chapter 4 provides step-by-step instructions for installing a system that will use files, not a naming service, for administration.

Chapter 5 provides step-by-step instructions for installing the master server for a name service.

Chapter 6 provides step-by-step instructions for installing a client for the naming services. It includes instructions for setting up a NIS slave server.

Chapter 7 describes the differences between Trusted Solaris network installation from Solaris network installation, including JumpStart and Custom JumpStart.

Chapter 8 describes how to configure and administer the Trusted Solaris environment on a headless system.

Chapter 9 describes procedures and administration tools specific to Trusted Solaris software that are useful to know when configuring the operating environment .

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

Appendix B provides a checklist for the install team when installing and configuring the Trusted Solaris environment.

Appendix C provides sample answers to Trusted Solaris installation program questions.

Glossary defines selected terms and phrases used in this book.

Related Books from Sun Microsystems

The following books contain information useful when installing Trusted Solaris software. The Solaris 8 AnswerBook CD and the Trusted Solaris 8 4/01 AnswerBook CD are shipped with the product. Solaris 8 books are available from the Solaris 8 AnswerBook CD.

Release Notes

Trusted Solaris 8 Release Notes – Describes late-breaking news about installing and running Trusted Solaris software, including known problems.

Solaris 8 (Intel Platform Edition) 4/01 Release Notes – Describes bugs, known problems, software being discontinued, and patches related to the Solaris release on the SPARC™ platform.

Solaris 8 (SPARC Platform Edition) 4/01 Release Notes Update – Describes bugs, known problems, software being discontinued, and patches related to the Solaris release on the Intel platform.

Hardware and Devices Guides

Solaris 8 Sun Hardware Platform Guide, 806-2221-10 – Describes hardware supported in the Solaris and Trusted Solaris environments.

Solaris 8 (Intel Platform Edition) Device Configuration Guide, 806-1053-10 – Describes Intel hardware configurations supported in the Solaris and Trusted Solaris environments.

Solaris 8 (Intel Platform Edition) 4/01 Hardware Compatibility List, 816-1455-10 – Describes Intel hardware compatibility with the Solaris and Trusted Solaris environments.

Installation Guides

Trusted Solaris Label Administration – Describes labels and includes a copy of *Compartmented Mode Workstation Labeling: Encodings Format* issued by the U.S. government.

Solaris 8 (SPARC Platform Edition) Installation Guide, 806-0955-10 – Describes how to install the Solaris environment on a SPARC platform. See *Trusted Solaris 8 4/01 Documentation Roadmap* for additional AnswerBook2 server setup required for the Trusted Solaris environment.

Solaris 8 (Intel Platform Edition) Installation Guide, 806-0956-10 – Describes how to install the Solaris environment on an Intel platform. See *Trusted Solaris 8 4/01 Documentation Roadmap* for additional AnswerBook2 server setup required for the Trusted Solaris environment.

Solaris 8 Advanced Installation Guide, 806-0957-10 – Describes interactive installations: network, JumpStart, and custom JumpStart. Contains background information for networked installation. Forms the basis for Trusted Solaris interactive installation—see Chapter 7 for Trusted Solaris modifications to the Solaris procedures.

Configuration Guides

Trusted Solaris Audit Administration – Describes how to set up and administer auditing on one or more Trusted Solaris systems.

Trusted Solaris Administrator's Procedures – Describes administration tasks in the Trusted Solaris environment in detail.

“Planning Your TCP/IP Network” in *System Administration Guide, Volume 3*, 805-7229-10 – Describes how to set up a network. Required for networked sites only.

Solaris Naming Administration Guide, 806-1391-10 – Describes how to administer naming services.

Solaris Naming Setup and Configuration Guide, 806-1386-10 – Describes how to set up and configure naming services.

Other Books

Solaris 8 4/01 What's New, 816-0014-10 – Describes new features in the Solaris environment.

System Administration Guide, Volume 1: Basic Administration, 806-7228-10 – Describes basic administrative tasks in the Solaris 8 operating environment, such as creating and mounting file systems.

System Administration Guide, Volume 2: Advanced Administration, 805-7229-10 – Describes more advanced administrative tasks in the Solaris 8 operating environment, such as print management.

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.

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

Automating Solaris® Installations: A Custom JumpStart™ Guide by Paul Anthony Kasper and Alan L. McClellan, published by Prentice Hall (SunSoft Press), 1995. – Describes how to set up “hands-off” network installations. ISBN .0-13-312505-X

Ordering Sun Documents

Fatbrain.com, the Internet's most comprehensive professional bookstore, stocks select product documentation from Sun Microsystems, Inc.

For a list of documents and how to order them, visit the Sun Documentation Center on Fatbrain.com at <http://www1.fatbrain.com/documentation/sun>.

Accessing Sun Documentation Online

The docs.sun.comSM Web site enables you to access Sun technical documentation online. You can browse the docs.sun.com archive or search for a specific book title or subject. The URL is `http://docs.sun.com`.

What Typographic Conventions Mean

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

TABLE P-1 Typographic Conventions

Typeface or Symbol	Meaning	Example
AaBbCc123	The names of commands, files, and directories; on-screen computer output	Edit your <code>.login</code> file. Use <code>ls -a</code> to list all files. <code>machine_name%</code> you have mail.
AaBbCc123	What you type, contrasted with on-screen computer output	<code>machine_name%</code> su Password:
<i>AaBbCc123</i>	Command-line placeholder: replace with a real name or value	To delete a file, type rm <i>filename</i> .
<i>AaBbCc123</i>	Book titles, new words, or terms, or words to be emphasized.	Read Chapter 6 in <i>User's Guide</i> . These are called <i>class</i> options. You must be <i>root</i> to do this.

Shell Prompts in Command Examples

The following table shows the default system prompts for administrative roles.

TABLE P-2 Shell Prompts

Shell	Prompt
administrative role prompt	\$
root role prompt	#

Security Overview

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

- "Planning for Security" on page 23 – For administrators of the Trusted Solaris operating environment, this section provides an overview of necessary planning before installation.
- "Differences From Solaris Installation and Configuration" on page 34 – For experienced Solaris administrators. Addresses specific differences from the Solaris operating environment.
- "Installation Results from an Administrator's Perspective" on page 34 – Describes the security features in effect after a host is installed.

See Appendix B for a checklist of Trusted Solaris 8 4/01 configuration tasks. If you are interested in localizing your site, see "For International Customers" on page 26. If you are interested in running an evaluated configuration, see "Understanding Your Site's Security Policy" on page 24.

Planning for Security

This section outlines the planning required before installing and configuring the Trusted Solaris operating environment.

1. "Understanding the Trusted Solaris Environment" on page 24
2. "Devising an Administration Strategy" on page 25
3. "Devising a Label Strategy" on page 26
4. "Planning User Security" on page 27
5. "Planning System Hardware and Capacity" on page 28

6. "Planning Your Network" on page 29
7. "Planning Auditing" on page 30
8. "Devising an Installation and Configuration Strategy" on page 31
9. "Collecting Information" on page 31
10. "Backing Up the System" on page 32
11. "Installing the Trusted Solaris Software" on page 32
12. "Configuring the Software" on page 32

Understanding the Trusted Solaris Environment

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

- Superuser has been eliminated. No one can log in as or use `su` to become root.
- Capabilities formerly assigned to superuser are available to discrete administrative *roles* to be assigned to a limited number of users.
- Users are limited to those applications necessary for performing their jobs.
- In addition to UNIX permissions, access to data is controlled by special security tags called sensitivity labels which are assigned to users and objects (such as data files and directories).
- The ability to override security policy can be assigned to specific users and applications.

To familiarize yourself with the Trusted Solaris environment, you should at a minimum read the *Trusted Solaris User's Guide* and *Trusted Solaris Administration Overview*. You should also be familiar with the rest of the documentation set, which is described in the *Trusted Solaris 8 4/01 Documentation Roadmap*.

Understanding Your Site's Security Policy

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

The Trusted Solaris operating environment is configured by default to conform with the ITSEC evaluation certificate FB1 (and FC2 which is less stringent). To meet these evaluated levels, you must:

- Select NIS+ as the naming service.
- Select multiple-label environment operation for the FB1 level. The FC2 level permits single- or multiple-label operation.

Note that your configuration may no longer conform with the ITSEC security levels if you do any of the following:

- Change the kernel switch settings in the `/etc/system` file, other than those switches and their values documented in this manual.
- Provide security-relevant execution profiles to non-administrative users.
- Change the default entries in these configurable files:
 - `/usr/openwin/server/tsol/*`
 - `/usr/dt/app-defaults/C/Sel_Mgr`
 - `/usr/dt/bin/Xsession`
 - `/usr/dt/bin/Xtsolusersession`
 - `/usr/dt/config/sel_config`
 - `/usr/dt/app-defaults/C/Dtwm`
 - `/usr/dt/app-defaults/C/Dt`
 - `/usr/dt/config/C/sys.dtwmrc`

Devising an Administration Strategy

The root role is mainly responsible for installing the Trusted Solaris 8 4/01 CD-ROM. After the initial Trusted Solaris installation, the root role is mostly not useful. In place of root or superuser, the Trusted Solaris environment suggests creating three or four administrative roles for managing the environment.

- 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.
- A less trusted role called “oper” for operator is responsible for backing up files.

As part of your administration strategy, you need to decide:

- Which users will be handling which administration responsibilities
- Which non-administrative users will be allowed to run trusted applications, that is, will be permitted to override security policy when necessary
- Which users will 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 environment. The label encodings file contains this type of information for your organization. You can use one of the label_encodings files supplied on the Trusted Solaris CD-ROM, modify one of the supplied files, or create a new label encodings file specific to your site. The file should include the Sun-specific local extensions (at least the COLOR NAMES section) when used in the Trusted Solaris environment.



Caution – You must have the final version of the label_encodings(4) file ready prior to configuring the first system. The file should be on a diskette. It will be read and installed at the label ADMIN_HIGH.

To learn more about the label encodings file, see *Trusted Solaris Label Administration*. You can also refer to *Compartmented Mode Workstation Labeling: Encodings Format*.

Planning labels also involves planning label configuration. After installation, you need to make the following decisions regarding the use of labels:

- Single- or multiple-label environment – If all of your non-administrative users can operate at the same security label, select a single-label system. Multiple-label environments are required for the FB1 level. If you want a no-label system, select single-label and then hide the labels for all users.
- Hide or display upgraded names in directories – This prevent a user (or intruder) from viewing the names of files or directories at higher levels than the current sensitivity label.

After installation, you can make the following label configuration display changes using User Accounts:

- Display administrative label names – You can show the actual administrative label names, or show substitute names for the labels.
- Hide or display labels – You can hide or display labels on a per-user basis.

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 Trusted Solaris label_encodings file.

Note – Each site should replace the `label_encodings` file provided on the Trusted Solaris CD with their own. Their file should have appropriate values for the label encodings keywords.

Planning User Security

The software ships with reasonable security defaults for users. The security defaults are listed in the two files 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 will inherit the established defaults. See the `label_encodings(4)` and `policy.conf(4)` man pages for descriptions of the keywords and values.

The system administrator can set up a standard user template that will set appropriate system defaults for users. 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. See the Solaris Management Console online help for User Accounts for more information.

TABLE 1-1 Trusted Solaris Security Defaults for User Accounts

File name	Keyword	Value
<code>/etc/security/policy.conf</code>	IDLECMD	lock logout
	IDLETIME	30
	LABELVIEW	showsl hidesl
	LOCK_AFTER_RETRIES	yes no
	PASSWORD	manual auto
	PROFS_GRANTED	Basic Solaris User
LOCAL DEFINITIONS section of <code>/etc/security/tsol/label_encodings</code>	Default User Clearance	c
	Default User Sensitivity Label	u
	Admin Low Name	ADMIN_LOW
	Admin High Name	ADMIN_HIGH
	Default Label View	External Internal

Planning System Hardware and Capacity

System hardware includes the system itself and its attached devices (tape drives, microphones, CD drives, and disk packs). Its capacity includes its memory, its network interfaces, and its disk space.

Consult the *Solaris 8 Sun Hardware Platform Guide* for a list of hardware that supports the Trusted Solaris environment. Any exceptions are noted in *Trusted Solaris 8 4/01 Release Notes*.

Peripheral hardware and capacity required for initial installation on a SPARC include:

- 128 MBytes minimum memory – 256 MBytes memory recommended to handle Solaris Management Console requests
- Local CD-ROM drive

Memory over the minimum is required on Trusted Solaris systems that:

- Are used as servers: name servers, file servers, audit servers, boot servers
- Run graphics or other large applications
- Run compilers
- Run number-crunching applications
- Run at more than one sensitivity label
- Are used by users who can assume an administrative role

Similarly, disk space requirements are greater for some systems. See “Disk Space Planning” in *Solaris 8 Advanced Installation Guide* for a list of factors that affect disk space. Particular Trusted Solaris features that require more disk space include:

- Disks with files stored at more than one label
- Disks whose users can assume administrative roles

For each Trusted Solaris system, you need to determine the following:

- Name and IP address
- Ethernet address (for network installations)
- Sun architecture (for network installations)
- Root password
- PROM security level: maintenance password only, or boot password
- PROM password (for Intel Architecture: BIOS protection)
- What devices may be attached to the system
- Which users may use the system
- Which printers at what labels are accessible from the system

Planning Your Network

If you are installing a non-networked system, you can skip this step.

For help in planning network hardware, see “Planning Your TCP/IP Network” in *System Administration Guide, Volume 3*.

As in any client-server network, you need to identify hosts by their function (server or client) and configure the software appropriately. The following table lists servers you may need to create and their function. For more information, see *System Administration Guide: Basic Administration*.

TABLE 1–2 Possible Servers in a Trusted Solaris Environment

Server	Function
Audit data server	Enable auditing
Audit administration server	Analyze the audit trail
File server	Centrally locate files for general use
Install server	Install over the network or use Custom JumpStart scripts
DNS server	Resolve internet names and addresses outside your local network
Home directory server	Enable remote mounting of users’ home directories. Required in a name service environment.
Mail server	Funnel mail to end user hosts from a central location
Network gateway	Operate an open network
Name Service Servers	Establish a NIS or NIS+ domain
Print server	Print hard copy

To plan the system administration aspects of servers, see the administration guides in the *Solaris 8 System Administrator Collection* including:

- *System Administration Guide, Volume 1*
- *System Administration Guide, Volume 2*

Trusted Solaris-specific administration is covered in *Trusted Solaris Administrator’s Procedures*.

Additional Planning for Open Networks

If your network is open to other networks, you need to specify accessible domains and hosts, and identify which Trusted Solaris hosts will serve as gateways to access them.

You need to identify the Trusted Solaris accreditation range for these gateways, and the sensitivity label at which data from other hosts may be viewed. Trusted Solaris software recognizes four labeled host types, including a Trusted Solaris host type (`sun_tsol`), and provides eleven templates by default, as shown in Table 1–3. The unlabeled template names correspond to the label names in the demo `label_encodings(4)` file installed from the Trusted Solaris CD.

TABLE 1–3 Templates Provided with Trusted Solaris Network Software

Host Type	Template Name	Purpose
Unlabeled	admin_low	For initial boot, before the host is configured with Trusted Solaris software.
	unclassified	For hosts or networks that send unlabeled packets, for example, Sun systems running Solaris software.
	confidential	
	secret	
	top_secret	
Labeled		
Trusted Solaris (sun_tsol)	tsol	For Trusted Solaris 2.5.1, 7, and 8 hosts or networks.
	tsol_ripso	For Trusted Solaris 2.5.1, 7, and 8 hosts or networks that label packets with the RIPSO security option.
	tsol_cipso	For Trusted Solaris 2.5.1, 7, and 8 hosts or networks that label packets with the CIPSO security option.
TSIX	tsix	For TSIX(RE1.1) hosts or networks.
CIPSO	cipso	For hosts or networks that send CIPSO packets.
RIPSO	ripso_top_secret	For hosts or networks that send RIPSO Top Secret packets.

The `tnrhttp(4)` man page gives complete descriptions of each host type with several examples.

Planning Auditing

Auditing requires the storage and analysis of a potentially huge amount of data. Before you set up auditing, you need to:

- Decide which classes of activity you need to audit. Try to keep these to a minimum.
- Plan how you are going to handle the storage and administration of the auditing data.

Each host should have a disk dedicated to audit data collection with a primary partition and a second partition for overflow records.

If you are auditing a network, you should dedicate at least one server to data collection and another server to data administration and analysis. Ideally, you should have your primary and secondary data collection areas on different hosts. In addition, you should reserve a fallback partition on the local hosts in case the network goes down.

- Read *Trusted Solaris Audit Administration* for step-by-step assistance.

Devising an Installation and Configuration Strategy

The Trusted Solaris software is initially loaded by root. Since root cannot log into the Trusted Solaris environment, a local user named “install” has been provided for the first part of the configuration process. Subsequent configuration is a two-person process (by default) using the security administrator and the system administrator roles. Once the roles have been assigned to users, and the computer is rebooted, the software enforces task division by role.

If two-person installation is not a site security requirement, assigning the two administrative roles to one person enables that person to configure both security and system information.

In a name service environment, you should install and configure systems in the order:

1. Name service master
2. Home directory server
3. Install server
4. Other name service servers
5. Other servers
6. End user systems

Collecting Information

Each role needs to gather the information for the tasks particular to the role. Concrete examples are in Appendix B.

Backing Up the System

If your system has any files on it that you want to save, make sure you 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 Trusted Solaris 2.5, Trusted Solaris 2.5.1, or Trusted Solaris 7 to the Trusted Solaris 8 4/01 release, and you want to retain some profile and user information, be sure to convert the `tsoluser` and `tsolprof` databases to their Trusted Solaris 8 4/01 formats *before* installing Trusted Solaris 8 4/01 software. See the `tsolconvert` man page that you download from the Trusted Solaris web site, <http://www.sun.com/software/solaris/trustedsolaris>, on the Technical FAQs page under Transitions Between Environments. Backup and conversion *must be completed* before running the Trusted Solaris 8 4/01 installation program.

Installing the Trusted Solaris Software

Installing the Trusted Solaris operating environment can be done interactively using CD-ROM disks, over the network, or with Custom JumpStart™ scripts. The first three systems, the name service master (NIS or NIS+), the home directory server, and the install server (if you want to do network or Custom JumpStart installs) must be installed from the CD. Subsequent systems can be installed using the server.

Installing over the network requires network setup. The installation program prompts the install team for needed information. Using Custom JumpStart requires some knowledge of Bourne shell scripting to automate installation. However, you can write scripts where no human interaction with the installation program is required.

For security reasons, the installation program does not offer some of the options that are available for Solaris 8 software. See “Differences From Solaris Installation and Configuration” on page 34 for details.

Configuring the Software

After the installation image is installed, the install team logs in as the user “install” and assumes the root role to configure initial security, network, and administrative role information, as shown in the following figure.

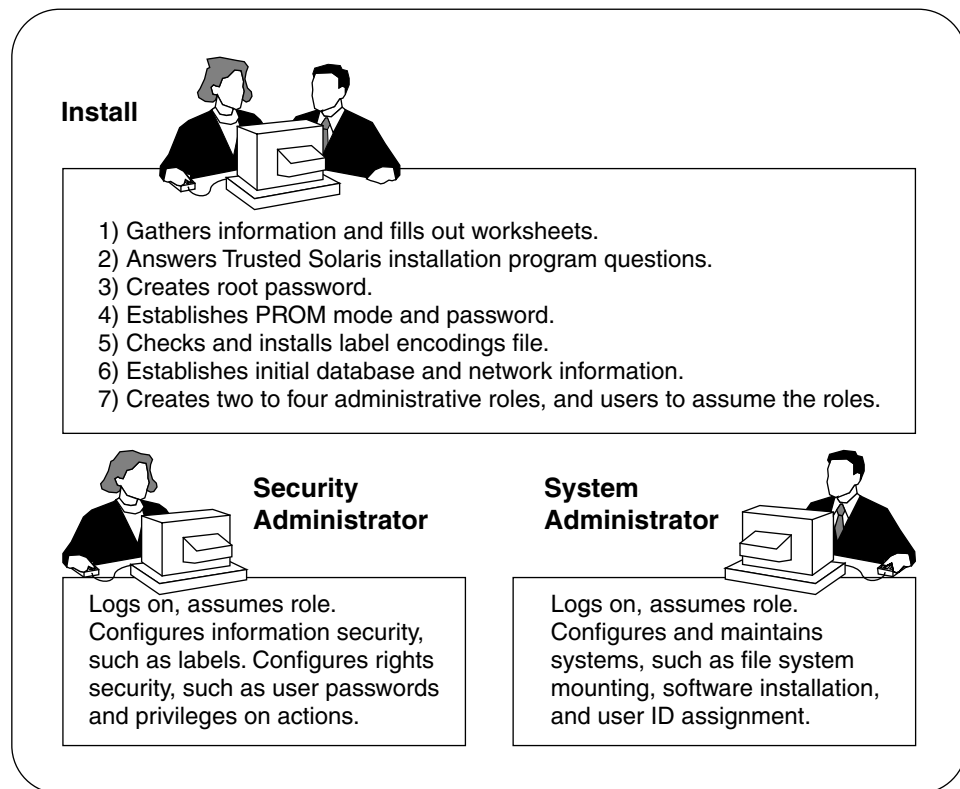


FIGURE 1-1 Two Roles Administering a System

Once users who can assume the administrative roles are created, the install team reboots the computer. Further configuration tasks are then partitioned by the software to a particular role.

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.

Differences From Solaris Installation and Configuration

CDE is the only desktop supported and installed by Trusted Solaris software. The Solaris Management Console™ Java-based tools must be used to manage local and network administrative databases.

Some options that are available when installing Solaris 8 software are not available when installing Trusted Solaris 8 4/01 software. Specifically,

- No remote file system mounting during installation. File systems are mounted after installation.
- Upgrade is supported between Trusted Solaris 8 and Trusted Solaris 8 4/01 only. However, there are manual steps to perform for keeping user and profile databases from earlier Trusted Solaris releases.
- Solaris™ Web Start install is not supported.

Note – Trusted Solaris 8 4/01 software supports the Volume Manager and the name services that are supported by the Solaris 8 release, including the NIS name service.

Installation Results from an Administrator's Perspective

After installing Trusted Solaris 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.
- Rights profiles for Trusted Solaris administrative roles are defined. It is the install team's job to create the roles.
- The Solaris Management Console enables administrative roles to administer user, rights profile and other system databases.
- A trusted editor enables administrators to modify local administrative files. It is implemented as a CDE action named Admin Editor.

- Trusted Solaris-defined CDE actions to view and edit local administrative files in a trusted editor are available to users in administrative roles.
- The Device Allocation Manager manages attached devices.
- Three Trusted Solaris-defined databases, `tnidb`, `tnrhttp`, and `tnrhdb`, handle trusted networking. They are administered using the Interface Manager and Security Families tools in the Solaris Management Console.

Installation and Configuration Task Maps

This chapter outlines the tasks for installing and configuring the Trusted Solaris operating environment, and where the tasks are documented.

Note that some tasks require that you use a Solaris book for the main steps of the task, and a Trusted Solaris book for security modifications. Modifications include assuming a role, operating at a label, and using trusted programs.

Preparing for Installation (Task Map)

Task	For Instructions
Find out what hardware is supported in this release.	<i>Solaris 8 Sun Hardware Platform Guide</i>
Use data from Trusted Solaris 2.5, Trusted Solaris 2.5.1 or Trusted Solaris 7 trusted databases in the Trusted Solaris 8 and Trusted Solaris 8 4/01 releases.	"Saving and Restoring Trusted Solaris Databases" on page 138
Back up a Trusted Solaris system.	<i>Trusted Solaris Administrator's Procedures</i>
Back up a Solaris system.	<i>System Administration Guide, Volume I</i>

Installing a System From CD-ROM (Task Map)

Task	Description	For Instructions
1. Install from a CD-ROM.	Use the Trusted Solaris 8 4/01 CD-ROM set in the CD drive of the machine you are installing.	"Installing From a CD-ROM" on page 43
After installation, do ONE of the following:		
Set up a system with no name service	Configure the computer to be administered with local files only.	"No Name Service Configuration Tasks" on page 49
Set up a name service master	Configure the master server of a NIS or NIS+ domain, and populate the name service databases for central administration of a network.	"Name Service Master Configuration Tasks" on page 73
Set up a name service client	Configure a system that is administered by the name server.	"Client Configuration Tasks" on page 93
Set up a name service client as an OS server	Configure a system to serve as the source of the Trusted Solaris installation program.	"Setting Up Network Installation" on page 107

Installing Systems Over the Network (Task Map)

Task	Description	For Instructions
1. Create an OS Server	Copy the Trusted Solaris installation disks to a name service client's hard disk.	"Setting Up Network Installation" on page 107

Task	Description	For Instructions
2. Enter client machines' details	Enter network information about every client that is going to be installed from the OS server.	"Add Client Information to the Install Server" on page 111
3. Install the client	Boot the client machine from the net.	"Boot Over the Network or with Custom Files" on page 47
4. Finish configuring the client	Configure the machine by assuming administrative roles.	"Client Configuration Tasks" on page 93

Configuring Headless Systems (Task Map)

Task	Description	For Instructions
Set Up Remote CDE Login	Enable the headless system to be configured from a desktop system.	"To Set Up Remote CDE Login to a Headless System" on page 122
Set Up Remote SMC Login	Enable the headless system to be configured remotely from the Solaris Management Console.	"To Set Up Remote SMC Login to a Headless System" on page 123
Set Up Serial Console Administration	Enable the headless system to be administered over a serial line.	"To Set Up Administration by Serial Login" on page 125
Set Up Remote Administration	Enable the headless system to be administered after <code>telnet</code> and <code>rlogin</code> access.	"To Set Up Administration by Remote Login" on page 125

Installing the Trusted Solaris Operating Environment

This chapter describes Trusted Solaris exceptions to the Solaris installation procedures and recommendations. It also describes Trusted Solaris requirements that are optional in a Solaris environment. For example, an evaluated configuration must collect auditing records. The partitions for those audit records are created during installation.

Note – If you are planning to use data from Trusted Solaris 7 or Trusted Solaris 2.5.1 databases on your new Trusted Solaris 8 4/01 system, do *not* start installing. Follow the instructions in “Backing Up the System” on page 32 before you install the Trusted Solaris 8 or Trusted Solaris 8 4/01 release.

Install Team Responsibilities

Trusted Solaris 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 users who can assume Trusted Solaris roles. Since roles and users are not created until after installation, we recommend that an install team of at least two persons be present during the installation of a system.

During Trusted Solaris installation, the team should:

- Partition the disks with security in mind: name the partitions so as not to disclose security information, and provide space for audit records.
- A root password is *required*. Type a root password when prompted.

Differences from the Solaris 8 Installation Program

In the Trusted Solaris 8 4/01 release, upgrade and patch analysis are not supported. Trusted Solaris software supports fewer locales than does Solaris software.

Recommendations for the Trusted Solaris Environment

On *all systems*, for audit records...

- Create at least one audit partition named `/etc/security/audit/system_name`.

On a system that will run the Solaris Management Console to administer the site...

- Provide at least 256 MBytes of memory. Provide swap space. Install the Developer or Entire cluster. Do *not* install the End User cluster.

On *all systems*, for users who can assume a role...

- Create sufficient swap space. Swap space that is double the size of the system's memory is a good rule of thumb.

On a system that will be the *home directory server*...

- Create an `/export/home` partition large enough for the users' home directories.

On a system that will *not be* a home directory server...

- Create a small `/export` partition to hold some temporary configuration files. It also serves as a mount point.

Shutting Down the System to be Installed

For basic information on installation, see the *Solaris 8 Start Here* booklet and the platform-specific books described in "Installation Guides" on page 18.

▼ Shut Down a Trusted Solaris System

Trusted Solaris systems are shut down differently from Solaris systems.

1. Click the right mouse button over the middle of the Front Panel and select Shut Down from the TP (Trusted Path) menu.
2. If the screen displays the > prompt, type `n` and press Return to display the ok prompt.

On a SPARC, if the PROM is protected, type `login` and when prompted, the root password.

Installing From a CD-ROM

See your hardware manual, such as the *Solaris 8 Sun Hardware Platform Guide* for full instructions. The following are examples.

▼ Insert the First Trusted Solaris 8 4/01 CD and Boot

Installing the first two systems requires using the 2 Trusted Solaris 8 4/01 installation CDs. The following are examples of booting from a CD on a SPARC and on an Intel machine.

- Insert the first of two (2) Trusted Solaris 8 4/01 Installation CDs and type the boot command.

EXAMPLE 3-1 SPARC: Typical Boot Command

```
boot cdrom
```

For more detail, see the *Solaris 8 (SPARC Platform Edition) Installation Guide*.

EXAMPLE 3-2 IA: Typical Boot Procedure

1. Do one of the following:
 - OPTION 1: Enable the system to boot from a CD by using the system's BIOS setup tool.
 - OPTION 2: Insert the provided floppy, then insert the first CD.
2. For more detail, see the *Solaris 8 (Intel Platform Edition) Installation Guide*. Keep in mind that Solaris Web Start and upgrade are not supported, and that you are using Trusted Solaris CDs, not Solaris CDs.

▼ Read Booting Messages

After you type the boot command, the system goes through a booting phase where hardware and system components are checked. The following screen provides an example of what you see. You may have to answer a language and a locale question.

```
Type b (boot), c (continue), or n (new command mode)
>n
Type help for more information
ok boot cdrom Rebooting with command: boot cdrom
Boot device: /pci@1f,0/pci@1,1/ide@3/cdrom@2,0:f    File and args:
SunOS Release 5.8 Version Trusted_Solaris_8 64-bit
Copyright 1983-2001, Sun Microsystems, Inc. All rights reserved.
Configuring /dev and /devices
Skipping interface hme0
Select a Language
Please make a choice (0-9): 0
Select a Locale
Please make a choice (0-47) or press ? or help: 45
Starting OpenWindows...
```

The booting phase will last for a few minutes. Then a Welcome to Trusted Solaris screen briefly appears, then the screen turns blue-gray and a Solaris Install Console is displayed in the upper left corner. Messages display in the Install Console during installation.

The Trusted Solaris installation program is running.

▼ Answer Installation Questions

If you are installing from CD-ROM, the program guides you step by step through installing Trusted Solaris software. Online help is also available.

- **Use “Root NIS+ Master Installation Program Example” on page 155 for guidance in answering the questions the first time that you install. In particular, note the following:**
 - When asked whether to use DHCP (Dynamic Host Configuration Protocol), choose No, unless you have a reason to select it.
 - When installing the name service master, choose None when asked for the name service. The name service domain is configured after installing the first system.
 - Implement the “Recommendations for the Trusted Solaris Environment” on page 42 during installation.

For screenshots of the installation program questions, see “Using the Solaris 8 Interactive Installation Program” in *Solaris 8 Advanced Installation Guide*.

▼ Enter a root Password

Users must not disclose their passwords to another person, as that person may 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 Trusted Solaris software provides protection against insecure passwords, but cannot prevent a user disclosing her/his password or writing it down.



Caution – A Trusted Solaris system *must* have a root password in order for the root role to work. The root role is required for successful configuration.

1. **Choose a root password by answering the password prompts.**

Root password: *rootpassword*
Re-enter your root password: *rootpassword*



Caution – Do not forget the root password. The software cannot be configured without it.

System identification is completed.

2. **When asked if you want the system to automatically shut down after 30 minutes of idle time, type y or n.**

The Web Start Launcher starts in command-line mode.

▼ Insert the Second Trusted Solaris 8 4/01 CD

The second CD installs packages only; it does not contain installation questions.

1. **When prompted, type 1 to continue installing using a CD.**

Note – The prompts are misleading. The installation program asks for Solaris 8 CD-ROM #2. You should insert Trusted Solaris 8 4/01 CD-ROM #2.

2. **Insert the second Trusted Solaris 8 4/01 installation CD.**

Upon insertion, the CD prints out that it is a Solaris 8 CD-ROM. If you inserted a CD-ROM with the Trusted Solaris 8 4/01 Installation CD label, you inserted the correct CD.

Note – The screen may display overwriting for the second CD. However, the packages are installing.

3. Answer yes to installing the software.

Package installation is displayed in 25% increments:

```
Installing Solaris Software 2
| -1%-----25%-----50%-----75%-----100%
```

4. Type 1 or 2 when prompted.

5. Remove the CD and press Return.

6. If you manually reboot your system, type:

```
# halt
ok    boot disk
```

▼ Read the Log

Before reboot, the install log is in the file `/tmp/install_log`. After reboot, the install log is in the file `/var/sadm/system/logs/install_log`.

- **Read the install log and check for successful package installation.**

▼ Configure the Trusted Solaris System

Finish system setup by configuring the system. To work properly, a Trusted Solaris system requires machine, label, and network configuration after installation.

- **To configure the system, follow the instructions for the system you are installing:**

A system that will be administered through its local files only
“No Name Service Configuration Tasks” on page 49

A system that will be the master server for a name service domain
“Name Service Master Configuration Tasks” on page 73

A system that will be a client on the name service domain
“Client Configuration Tasks” on page 93

Troubleshooting

Errors you encounter during installation are described and debugged in the Troubleshooting section of the *Solaris 8 Advanced Installation Guide* (see <http://docs.sun.com/ab2/coll.241.7/SPARCINSTALL>).

Installing Over the Network

The admin role is in charge of installing over a network. The secadmin role is called upon to modify or set up files or profiles to enable the admin role to complete software installation.

▼ Boot Over the Network or with Custom Files

Prerequisite: The network and/or custom files are correctly set up.

See the *Solaris 8 Advanced Installation Guide*, 806-0957-10, which describes network installations. The Solaris network installation procedures apply to Trusted Solaris network installations, with the Trusted Solaris security protections described in “Trusted Solaris Modifications to Network Installation” on page 112 and “Setting Up Custom JumpStart Installation” on page 113.

1. Boot using the appropriate boot command on the system being installed.

EXAMPLE 3-3 SPARC: Boot command for a network installation

```
boot net
```

EXAMPLE 3-4 SPARC: Boot command for a custom JumpStart installation

```
boot net - install
```

A space is required between the minus sign and install.

After you type the boot command, the system checks hardware and system components, then connects with the install server. The following screen provides an example of what you see.

```
Rebooting with command: boot net - install
Boot device: /pci@1f,0/pci@1,1/ide@3/network@1,1      File and args:
```

EXAMPLE 3-4 SPARC: Boot command for a custom JumpStart installation (Continued)

```
SunOS Release 5.8 Version Trusted_Solaris_8 64-bit
Copyright 1983-2001, Sun Microsystems, Inc. All rights reserved.
Configuring /dev and /devices
Using RPC Bootparams for network configuration information.
Configured interface hme0
Using sysid configuration file
192.168.114.1:/export/install/jumpstart/sysidcfg/siysidcfg
Starting OpenWindows...
```

2. Answer any prompts that appear.

For JumpStart installations—If you have set them up correctly, you are not prompted for information.

For network installations—If you have set them up correctly, you are prompted for disk partitioning and other information after system identification is completed.

▼ Finish Configuring Systems Installed Over the Network

- **Complete Trusted Solaris configuration.**

For JumpStart installations—You must connect the client to the domain and initialize SMC, as described in “Connecting to the Name Server” on page 100.

For network installations—You must do the procedures in “Client Configuration Tasks” on page 93, except you do *not* have to add the client to the domain.

Configuring a System with No Name Service

This chapter covers how to configure a system without a name service. Administration is through local files.

Note – Installation and configuration commands and actions are limited to particular roles and particular labels. Read each task for the administrative role that can perform it, and the label required.

Who Does What

Trusted Solaris software is designed to be installed and configured by an install team. Once the team has created users who can assume Trusted Solaris roles, and has rebooted the computer, the software enforces task division by role. If two-person installation is not a site security requirement, you can assign the administrative roles to one person.

No Name Service Configuration Tasks

A system that is administered using local files instead of a name service is configured much like a name server, except that only local files are used for administration rather than name service tables or maps.

If you are configuring the system to satisfy criteria for an evaluated configuration, read “Understanding Your Site’s Security Policy” on page 24 before continuing.

Task	Description
Initial Configuration — from “Logging In and Launching a Terminal” on page 50 through “Initializing the Solaris Management Console” on page 56	Covers how to protect the hardware, set up the labels, and initialize the administration tools.
“(Optional) Configuring Routing” on page 59	Covers how to set up static routing.
“Configuring Network Files” on page 60	Covers how to specify all hosts that can communicate with the system.
“Creating Roles and Users” on page 64	Covers how to create administrative roles and users to those roles.
“Verifying That Roles Work” on page 69	Covers how to test that the roles are effective.
“Finishing Up Configuration” on page 70	Covers how to share and mount file systems, and how to delete the install user. Points you to auditing and further setup information,

Logging In and Launching a Terminal

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.

▼ Log In

The predefined user `install` logs in immediately after installation to configure the system.

1. **Enter `install` as the user name and press the Return key.**

The Password dialog box is displayed.

2. **Enter `install` for the password.**

The Enable Logins dialog offers four choices, as shown in the following figure:

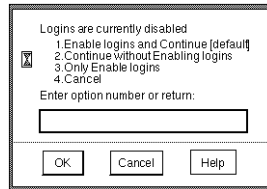


FIGURE 4-1 The Enable Logins Dialog Box

3. **Depending on site security requirements, enter 1 or 2, then click OK.**

The Message Of the Day (MOTD) dialog box is displayed; the label is ADMIN_LOW.

4. **Click OK to dismiss the MOTD dialog box.**

The Trusted Solaris screen appears briefly. Then you are in a CDE workspace, as shown in Figure 4-2. The trusted stripe below the front panel shows the window sensitivity label.

Note – The install team must log off or utilize the lockscreen functionality before leaving a system unattended. Otherwise a person may have access to the system without having to pass identification and authentication, and that person would not be uniquely identified or accountable.

▼ Assume the root Role

An administrative role configures the system, however, a role cannot log in. Users log in, and assume one or more of their assigned roles. The root role has been pre-assigned to the user `install`.

1. **Right click on the middle of the Front Panel.**
2. **Select Assume root Role from the TP (Trusted Path) menu.**

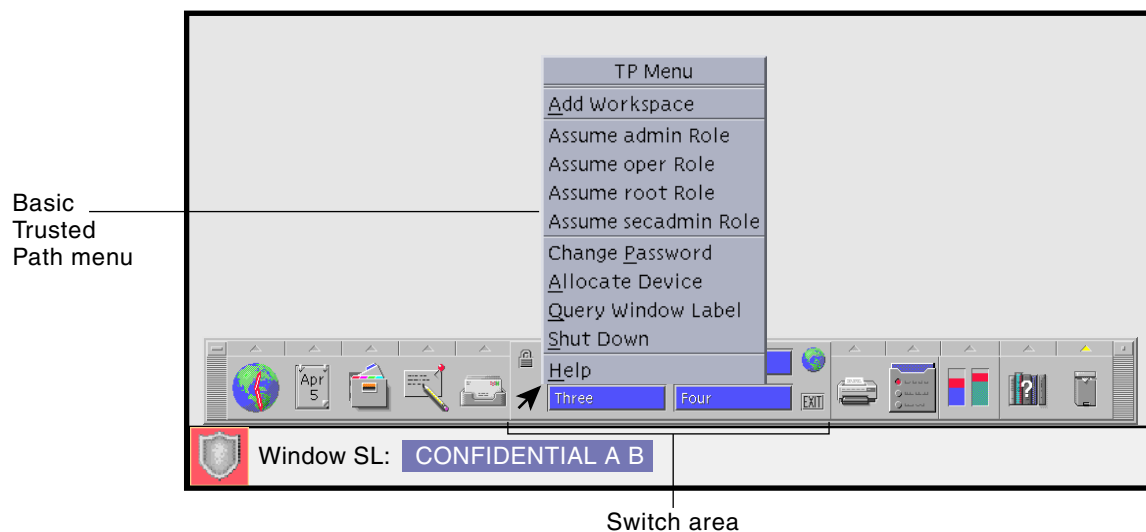


FIGURE 4-2 A Trusted Solaris User Workspace

After initial installation from a CD-ROM, only the root role will be displayed on the TP menu, since no other roles have been created.

3. At the password prompt, enter the password for the root role.

The password for the root role is the password that the install team entered for root when prompted during the installation program.

▼ Launch a Terminal

- **Right-click on the screen background and select Tools → Terminal from the Workspace Menu.**

The terminal's Options menu enables you to customize the appearance of the terminal. Customizations for the install user are not saved.

Protecting the Machine

For more information on PROM values that you can set, see *OpenBoot 2.x Command Reference Manual* or *OpenBoot 3.x Command Reference Manual*.

▼ SPARC: Protect Machine Hardware

1. In the terminal, enter the PROM security mode.

```
# eeprom security-mode=command
```

Changing PROM password:

New password: *password*

Retype new password: *password*

Choose the value `command` or `full`. See the `eeprom(1M)` man page for more details.

2. If you are not prompted to enter a PROM password, the system already has a PROM password. To change the PROM password, run the command:

```
# eeprom security-password=Return
```

Changing PROM password:

New password: *password*

Retype new password: *password*

The new PROM security mode and password are in effect immediately, but are most likely to be noticed at the next boot.



Caution – Do not forget this password. The hardware is unusable without it.

▼ IA: Protect the BIOS

On Intel architecture, the equivalent to protecting the PROM is to protect the BIOS.

- Refer to your machine's manuals for how to protect the BIOS.

Setting Up Labels

Note – The default `label_encodings` file is useful for demos, but it is not a good choice for use by a customer site. However, if you plan to use it, you can skip this step.

The Trusted Solaris `label_encodings(4)` file has been checked and is installed. Note that it must be compatible with any Trusted Solaris host with which you are communicating.

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

You can edit the placeholder `label_encodings(4)` file that the Trusted Solaris installation program installed, or install your own. The security administrator is responsible for editing, checking, and maintaining the `label_encodings` file.



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

▼ Create an Admin_High Workspace

The `label_encodings` file is protected at the label `ADMIN_HIGH`. For security, you copy, edit, check and install your label encodings file at `ADMIN_HIGH`.

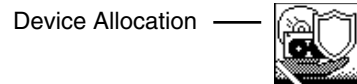
1. **Click the right menu button over the `root` workspace switch to bring up the TP menu, and select **Add Workspace**.**
A second workspace, named `root_1`, is created and active.
2. **Click the right menu button over the `root_1` workspace switch, and choose **Change Workspace Label** from the menu.**
3. **Click the `ADMIN_HIGH` label in the Label Builder and click **OK**.**

The color of the workspace switch changes to the color associated with the label `ADMIN_HIGH`. Actions, terminals, commands and windows originating from this workspace run at the label `ADMIN_HIGH`.

▼ Allocate the Appropriate Device

1. **In the `ADMIN_HIGH` workspace, click the left mouse button on the triangle above the **Style Manager** icon on the **Front Panel**.**

Its Tools subpanel includes the Device Allocation icon.



2. **Click the **Device Allocation** icon once.**

3. **Double-click the device you want to allocate.**

`floppy_0` indicates a diskette.

4. **Click Yes to mount the device.**

A File Manager pops up showing the mount point. If it does not pop up, open a File Manager from the Front Panel, navigate to `/`, and double-click `floppy`.

▼ Check and Install Your Label Encodings File

1. **If you plan to tweak the label encodings file, make sure that the file itself is writable.**
2. **In the `ADMIN_HIGH` workspace, open the Application Manager by clicking the right mouse button on the background to bring up the Workspace menu.**
3. **Choose Applications → Application Manager from the top of the menu.**
4. **Double-click the `System_Admin` folder icon —**



5. **Check the syntax of the new label encodings file by double-clicking the Check Encodings action.**

You can ignore any Trash Can Error dialog error messages.

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

`/floppy/floppy0/label-encodings-filename`

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

The `chk_encodings(1M)` command checks the syntax of the file.

8. **If the file passes the check, answer `yes` to overwrite the currently-installed `label_encodings` file.**

The Check Encodings action creates a backup copy (naming it `label_encodings.orig`), installs the checked version, then restarts the label daemon.

CONTINUE

Only if it reports no errors can you continue installing.

RESOLVE ERRORS

If it reports errors, they *must* be resolved before continuing with installation.

Consult “Creating or Editing the Encodings File” in *Trusted Solaris Label Administration* for troubleshooting assistance.



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

▼ Deallocate the Device

1. In the workspace where the Device Allocation action is displayed, double-click the device to be deallocated from the list of allocated devices.
2. Remove the diskette and click OK in the Deallocation dialog box.
3. Return to root’s ADMIN_LOW workspace by clicking the root workspace switch.

Initializing the Solaris Management Console

▼ Initialize the SMC Server

1. In the root role in an ADMIN_LOW workspace, start the SMC server process in the terminal window.

```
# smc
```

Note – The `smc` command initializes the SMC server. The first time the server is launched, it performs several registration tasks, which can take a few minutes.

2. If toolbox icons do not appear in the Solaris Management Console,
And the Navigation pane is not visible:
 1. In the Open Toolbox dialog that is displayed, click Load next to where this machine’s name is listed under Server.
If this machine does not have the recommended amount of memory and swap, it may take a few minutes for the toolboxes to display. See “Recommendations for the

Trusted Solaris Environment” on page 42.

2. From the list of toolboxes, select Trusted Solaris Management Console, then click the Open button.

And the Navigation pane is visible, but the toolbox icons are stop signs:

1. Exit the SMC by choosing Exit from the Console pull-down menu
2. Restart the SMC

smc

3. Open the Trusted Solaris Management Console toolboxes by choosing Open from the Console menu, then selecting Trusted Solaris Management Console. The following figure shows the Navigation Pane of the Solaris Management Console in

the Files scope.

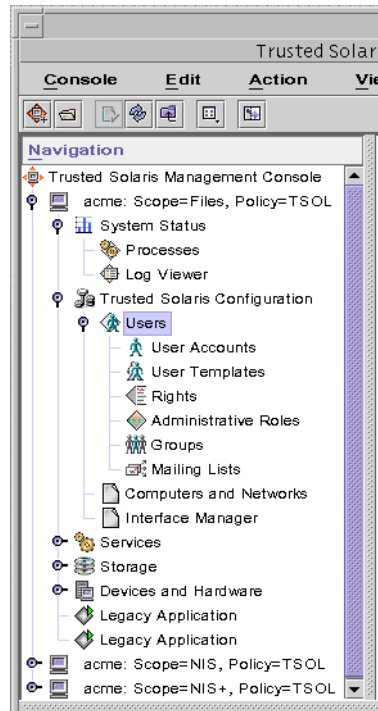


FIGURE 4-3 Solaris Management Console Tools

▼ (Optional) Save the Current Toolbox

Saving the toolbox preference enables the Trusted Solaris Management Console toolboxes to load by default. The preferences are saved per role, per host (SMC server).

1. **From the Console menu, choose Preferences.**
2. **Click the Use Current Toolbox button, then click OK.**

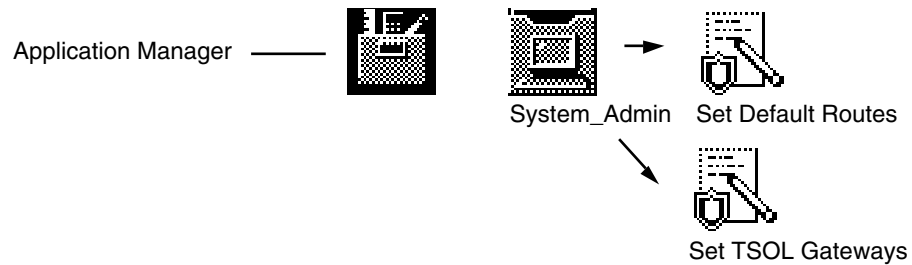
If you are configuring the name service master, return to “(Optional) Configuring Routing” on page 75 in Chapter 5. Otherwise, continue.

(Optional) Configuring Routing

Set up static routing only if the security administrator has planned for an open network and you do not plan to use dynamic routing. Dynamic routing is the default, and requires no setup.

See “Administering Trusted Networking” in *Trusted Solaris Administration Overview* for more information.

For static routing, do *one* of “Set Up Simple Static Routing” on page 59 or “Set up Static Routing Using Extended Metrics” on page 60.



▼ Set Up Simple Static Routing

For small networks, an `/etc/defaultrouter` file provides a simple routing method.

1. **Double-click the Set Default Routes action in the System_Admin folder.**

See “To Open a File that has a Defined Action” on page 132 if you are unfamiliar with using trusted actions.

An empty `/etc/defaultrouter` file appears in the trusted editor.

2. **Enter the name or the IP address of the defaultrouter. If there is more than one, enter them all, one per line, and then save the file.**

For example, if the hosts `trustworthy` and `forwardho` are routers, enter them, one per line:

```
trustworthy
forwardho
```

▼ Set up Static Routing Using Extended Metrics

If your host or site accesses a complex network of gateways, the `/etc/tsolgateways` file offers more routing options. See the `tsolgateways(4)` man page for examples.

1. **Double-click the Set TSOL Gateways action in the System_Admin folder.**

See “To Open a File that has a Defined Action” on page 132 if you are unfamiliar with using trusted actions.

An empty `/etc/tsolgateways` file appears in the trusted editor.

2. **Enter the IP address of the subnet, the name of the gateway and its metric. Repeat for every gateway and save the file.**

For example, if the hosts `trustworthy` and `forwardho` are gateways:

```
192.168.15.0 trustworthy 1
192.168.8.0 forwardho 2
```

Note – If the system has an `/etc/defaultrouter` file and an `/etc/tsolgateways` file, only the `/etc/tsolgateways` file is used for routing decisions.

Configuring Network Files

▼ Add Hosts to the System’s Known Network

1. **In the root role at the label ADMIN_LOW, return to the Solaris Management Console or re-open it if it is closed.**

```
# smc
```

2. **Click *this-host*: Scope=Files, Policy=TSOL under Trusted Solaris Management Console in the Navigation pane.**

See Figure 9–1 for what tools should display in the Navigation pane .

3. **Display the computers known to this host by clicking Trusted Solaris Configuration, then clicking Computers and Networks.**

Note – If toolbox icons display as red stop signs, the toolboxes will not load. To load them, see step 2 in “Initialize the SMC Server” on page 56.

4. **Provide a password when prompted., then double-click Computers.**
This computer should already be in the database. You should add every host that his system may contact, including static routers (if any), and any audit servers.
5. **Add a host that this computer may contact by choosing Add Computer from the Action menu.**
6. **Click Apply to add the host, and click OK when the entries are complete.**

▼ (Optional) Remove the 0.0.0.0 Network

The network wildcard 0.0.0.0 may present a security risk. See “Modifying the Boot-time Trusted Network Databases” in *Trusted Solaris Administrator’s Procedures* for more information.

- **Follow the instructions in the “To Replace the 0.0.0.0 Entry in the Local Tnrhdb File” procedure under “Managing Trusted Networking (Tasks)” in *Trusted Solaris Administrator’s Procedures*.**

▼ Add a Remote Host Template

If you used the Trusted Solaris `label_encodings` file, you can skip this step.

If this host is going to contact unlabeled hosts, the `tnrhtp` file must have an appropriate unlabeled template for those unlabeled hosts. See Table 1–3 in “Additional Planning for Open Networks” on page 29 for host types and their associated templates provided by Trusted Solaris software.

The `tnrhtp(4)` file installed by the Trusted Solaris installation program contains examples of templates that match the `label_encodings(4)` file installed during Trusted Solaris installation. If you installed a site-specific `label_encodings` file, it is highly likely that the existing `tnrhtp` templates will not work with your file.

1. **In the root role at the label ADMIN_LOW, double-click Security Families under Computers and Networks in the Solaris Management Console.**

The existing templates are displayed in the View pane.



Caution – Sites that install a site-specific `label_encodings` file *must* create templates that reflect the labels of machines and networks that the Trusted Solaris network can contact.

You should have templates for:

1. The Trusted Solaris hosts that this machine can contact.
2. Any unlabeled hosts/networks that this machine can contact..

2. **To create a single-label template to assign to unlabeled hosts, choose Add Template from the Action menu.**

Consult the online help as you create the template.

- a. **In the Basic Information tab, create a template named `unlab_min-user-label`, of host type Unlabeled, with an `ADMIN_HIGH` clearance and a process label of `min-user-label`.**

The default clearance must dominate the default label. The label `ADMIN_HIGH` dominates all labels.

- b. **Click OK when the template is complete.**

3. **Create any other templates your site needs before continuing.**

▼ Assign a Template to a Remote Host

The trusted network remote host database, `tnrhdb`, enables this host to communicate with remote hosts. The `tnrhdb(4)` man page describes the format of the entries, and suggests how to minimize the number of entries required.

Assign a remote host template to every host or network that this machine may contact. Include every host in the `/etc/hosts` file.

See Table 1–3 in “Additional Planning for Open Networks” on page 29 for host types and their associated templates provided by Trusted Solaris software.

1. **In the root role at the label `ADMIN_LOW`, double-click Security Families under Computers and Networks in the Solaris Management Console.**
2. **Double-click the Trusted Solaris security family, `tsol`.**
3. **Choose Add Host(s) from the Action menu.**

4. In the Add Host(s) dialog box, click Add Wildcard to assign this template to all hosts on your Trusted Solaris subnet.

- a. Enter the subnet IP address and choose the template name.

For example, enter 192.168.10.0 and tsol. The final zero signifies a subnet address; all hosts on that subnet are recognized as tsol hosts.

Note – The number zero (0) is the wildcard. Do not use a star (*).

- b. Click OK.

5. Choose Add Host(s) from the Action menu and click Add Host in the Add Host(s) dialog box to enter any exceptions to the subnet template assignment. Click OK to end the entry.

For example, enter 192.168.10.3 and unlabeled_min-user-label. This host on the subnet is an unlabeled host, an exception to the tsol wildcard entry.

6. Choose Add Host(s) from the Action menu and click Add Host to enter the IP address of every host in your /etc/defaultrouter or /etc/tsolgateways file, and assign to each an appropriate template name. Click OK to end each entry.

7. Enter the details of other subnets and hosts.

- a. Enter the wildcard designation of each subnet and choose its appropriate template by choosing Add Host(s) → Choose Wildcard.

- b. Individually assign a different template to any host that is an exception to its subnet's assigned template by choosing Add Host(s) → Choose Host.

Use the details provided by your system administrator, then choose the appropriate template name from the menu.

8. Open a terminal to reload and verify the updated tnrhdb database.

```
# tnctl -H /etc/security/tsol/tnrhdb
# tninfo -h
```

▼ (Optional) Set Up DNS

Skip this procedure if the security administrator has planned a closed network. For detailed information about DNS, see the *Solaris Naming Setup and Configuration Guide*.

- If your system is going to use DNS, click the Set DNS Servers action in the System_Admin folder and enter the nameservers by IP address, one per line.

The file looks something like:

```
nameserver nnn.nnn.nnn.nnn
nameserver nnn.nnn.nnn.nnn
```

Creating Roles and Users

The install team creates the administrative roles (other than root) to be used at the site. The team assigns each role its rights profiles. Initial rights profiles are provided on the installation CD-ROM.

The appropriate toolbox scope for creating roles and users in a non-networked environment is *this-host*: Scope=Files, Policy=TSOL.

▼ Create Administrative Roles

1. In the root role at label **ADMIN_LOW**, start the Solaris Management Console if it is not running.
2. Select the appropriate toolbox.
3. Click Trusted Solaris Configuration, then click Users.
4. When prompted, enter the root role password.
5. Double-click Administrativ... (Administrative Roles).
6. Choose Add Administrative Role from the Action menu.

The Add Administrative Role wizard enables you to enter all values that are required for a role to work well. Values that you are not prompted to enter receive a default value. If you want to view or modify a role, double-click the role after creating it.
7. Create the secadmin role to be the security administrator. Use the following table as a guide when creating the role.

The secadmin password, 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.

TABLE 4–1 secadmin Values in Add Role Dialog

Tab	Role Field	(Recommended) Value
Role Name	Role name	secadmin
	Full Name	Security Administrator
	Description	No proprietary info here.
	Role ID Number	≥100
	Role shell	Administrator’s Bourne (profile shell)
	Create a role mailing list	checked
Password	Password and confirm	Assign a password of at least 6 alphanumeric characters.
Rights	Available and Granted	Information Security
		Rights Security
Home Directory	Server	<i>home directory server</i>
	Path	<i>/mount_path</i>
Assign Users	Add and Delete	This will be automatically filled in when you assign a role to a user.

8. After creating the role, select it and double-click it to modify it. Use information from the following table as a guide.

TABLE 4–2 secadmin Values in Properties/Modify Dialog

Tab	Role Field	(Recommended) Value
Password	Set password by Type in or Choose from list	(Set in Table 4–1.)
	Update password by Choose from list or Type in	
Group	Available Groups	

TABLE 4-2 secadmin Values in Properties/Modify Dialog (Continued)

Tab	Role Field	(Recommended) Value
Trusted Solaris Attributes	Minimum Label: Edit	Default value is correct.
	Clearance: Edit	Default value is correct.
	View: External or Internal	The default value is External.
	Label: Show or Hide	If your site is a no-label site, choose Hide.
	Lock account ...	Default value, No, is correct.
Audit	Excluded and Included	Set flags per site security policy

9. Using the preceding tables as a guide, create the following three roles. Give each role a unique ID, and assign to it the correct rights profile, as shown below:

Role Name	Granted Rights
admin	System Administrator
primaryadmin	Primary Administrator
oper	Operator



Caution – You must create the administrative roles before you create the users, since you will assign a role to each user.

▼ Create Users Who Will Assume Roles

The install team in the root role creates users to assume the roles secadmin, admin, and primaryadmin. Where site security policy permits, the team can choose to create one user who can assume more than one administrative role.

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 you add.

3. Begin to create a user who can assume the secadmin role and use Table 4–3 to fill out the fields.

The Add User → Use Wizard dialog boxes create most aspects of a user.

4. After creating the user, double-click the created user to modify some user properties.

Use Table 4–4 as a guide.

5. Read the (Recommended) Value columns for guidance.

Parentheses enclose suggestions. Requirements or defaults are not enclosed in parentheses.

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.

TABLE 4–3 User Values in Add User Dialog

Tab	User Field	(Recommended) Value
User Name	User name	
	Full name	
	Description	No proprietary info here.
	User ID number	(1001 or higher)
Password	Set password by Type in or Choose from list	Assign a password of at least 6 alphanumeric characters.
	Confirm	
Group	Primary group	Staff
Home directory	Server	<i>home directory server</i>
	Path	
Mail	Server	
	Path	

For the user who can assume the secadmin role, select “Always Available” for “Account Availability” under General, below. Choose an appropriate account availability for other users.

TABLE 4-4 User Values in Properties/Modify Dialog

Tab	User Field	(Recommended) Value
General	Shell	
	Account Availability	Always Available
Password	Set password by Type in or Choose from list	(Set in Table 4-3.)
	Update password by Choose from list or Type in	
Group	Additional Groups	
Roles	Available Roles and Assigned Roles	secadmin
Trusted Solaris Attributes	Minimum Label: Edit	Default value is correct.
	Clearance: Edit	Default value is correct.
	View: External or Internal	
	Label: Show or Hide	If your site is a no-label site, choose Hide.
Account Usage	Idle time	
	Idle action	
	Lock account ...	No — for any user who will assume a role.
Rights	Available and Granted	Enable Login ... and see Note below.
Audit	Excluded and Included	Set flags per site security policy

Note – Although Basic Solaris User does not appear in the Granted column, this right is assigned automatically to a user that is created using the Add User wizard. Do not assign the right explicitly.

6. **Create and modify another user, one who can assume the admin role.**
7. **(Optional) Create and modify third and fourth users to assume the primaryadmin and oper roles, and provide them with unique IDs and appropriate Rights.**
These first users should each have at least the Enable Login right — user can enable logins after a system reboot.

After checking your site security policy, you may want to add the Convenient Authorizations right — user can allocate devices, enable logins, print PostScript files, print without labels, remotely log in, and shut down the system.

Note – Do not create any more users at this time. Setting up users is a two-role, trusted procedure.

See “Managing User Accounts” in *Trusted Solaris Administrator’s Procedures* and “Managing Users and Rights With SMC” in *Trusted Solaris Administrator’s Procedures* for details on setting up users and user files.

In a multilabel environment, users and roles are set up with a useful file, `.link_files`. See “Managing Initialization Files” in *Trusted Solaris Administrator’s Procedures* for further discussion.

Verifying That Roles Work

▼ Reboot the Computer

If you have not set up DNS or static routing, you can skip this step.

- Shut down the computer from the TP (Trusted Path) menu, and reboot it.

▼ Verify that the Roles secadmin and admin Work

1. For each role, log in as a user who can assume the role and assume it.
2. In the role workspace, open the Solaris Management Console, select the Trusted Solaris Management Console with the appropriate scope for your site, and click Users.
3. Provide the role password when prompted, then double-click User Accounts.
4. Click a user.
 - The admin role should be able to modify fields under the tabs General, Home Directory, and Group.
 - The secadmin role should be able to modify fields under all tabs.

▼ Verify that the Role primaryadmin Works

1. Log in as a user who can assume the primaryadmin role and assume it.
2. In the role workspace, open the Solaris Management Console, select the Trusted Solaris Management Console with the appropriate scope for your site, and click Users.
3. Provide the role password when prompted, and double-click Rights.
4. Creating a new right by choosing Add Right from the Action menu.
5. Save the new right, then delete it before continuing.

Finishing Up Configuration

▼ Set Up Auditing

The security administrator is responsible for auditing decisions.

- **Configure or disable auditing by doing *one* of the following.**

Disable auditing—if site security does not require auditing. To disable auditing in the Trusted Solaris environment, follow the procedures described in *Trusted Solaris Audit Administration*.

Configure auditing—by following the procedures in *Trusted Solaris Audit Administration*.

▼ (Optional) Share File Systems

If a directory is being shared before the admin role is created, the install team performs the procedure in the root role.



Caution – Do not use proprietary names for shared file systems. The names of shared file systems are visible to every user.

1. In the admin role, (or root if the admin role does not exist), at label **ADMIN_LOW**, under **Trusted Solaris Management Console**, click *this-host: Scope=Files*,

Policy=TSOL.

2. Click **Storage**, and provide a password if prompted.
3. Double-click **Mounts and Shares**, and then double-click **Shares**
4. Choose **Add Shared Directory** from the **Action** menu.
5. Follow the online help to share the directory.
The tool shares the directory and starts the NFS daemons,
6. To modify the attributes of the shared directory, double-click the **Properties** tab and use the online help to guide you.

▼ (Optional) Mount File Systems

In the Trusted Solaris environment, unlabeled and labeled hosts can be mounted on a Trusted Solaris labeled host.



Caution – Do not use proprietary names for mounted file systems. The names of mounted file systems are visible to every user.

1. In the **admin** role at label **ADMIN_LOW**, under **Trusted Solaris Management Console**, click *this-host: Scope=Files, Policy=TSOL*.
2. Click **Storage** and provide a password if prompted.
3. Double-click **Mounts and Shares**, and then double-click **Mounts**.
4. Choose **Add NFS Mount** from the **Action** menu.
5. Follow and answer the prompts to mount the file system.
You are prompted to allow creation of the mount point if it does not exist. The tool adds an entry in the `/etc/vfstab` file, creates the mount point, and mounts the file system.

▼ (Optional) Delete the User install

When a user is deleted from the system, the administrator must ensure that the user's home directory and any objects owned by that user are also deleted. As an alternative to deleting objects owned by the user, the administrator may change the ownership of these objects to another user who is defined on the system.

The administrator must also ensure that all batch jobs that are associated with the deleted user are also deleted. The administrator must ensure that there are no objects or processes belonging to a deleted user that remain on the system.

Note – If you plan to use the `tsolconvert` utility, do not delete the `install` user until you have completed the required conversion steps on a Trusted Solaris 8 or Trusted Solaris 8 4/01 system. See “Saving and Restoring Trusted Solaris Databases” on page 138 for more information on converting Trusted Solaris 7 to Trusted Solaris 8 4/01 databases.

1. **In the admin role at label `ADMIN_LOW`, in the Solaris Management Console, choose the `this-host: Scope=Files, Policy=TSOL`, and click **Users**.**
2. **Provide a password if prompted, then double-click **User Accounts**.**
The user “install” is defined locally.
3. **Select the user to be deleted and click the **Delete** button.**
For the user `install`, you do not have mail files to delete. Other local users may have home directories and mail files to delete.

▼ Other Setup

- **See *Trusted Solaris Administrator's Procedures* for tasks such as handling mail, setting up printers, and protecting file systems.**

Configuring a Name Service Master

This chapter covers how to configure the name service server and the home directory server at a networked site.

Note – Installation and configuration commands and actions are limited to particular roles and particular labels. Read each task for the administrative role that can perform it, and the label required.

Who Does What

Trusted Solaris software is designed to be installed and configured by an install team. Once the team has created users who can assume Trusted Solaris roles, and has rebooted the computer, the software enforces task division by role. If two-person installation is not a site security requirement, you can assign the administrative roles to one person.

Name Service Master Configuration Tasks

The first system installed on a network has special status. It must be installed interactively from the CD-ROM, and it must be configured as the name service master.

If you are configuring a site that satisfies criteria for an evaluated configuration, please read “Understanding Your Site’s Security Policy” on page 24.

The procedures are listed in order. Depending on your site configuration, some procedures can be omitted.

Task	Description
“Logging In and Launching a Terminal” on page 50 to “Protecting the Machine” on page 52	Covers how to protect the hardware, set up the labels, and initialize the administration tools.
“(Optional) Configuring Routing” on page 75	Covers how to set up static routing.
“Configuring the Network” on page 76	Covers how to specify all hosts that can communicate with the system.
“Setting Up the Name Server and Domain” on page 80	Covers how to set up the name service.
“Setting Up Critical Servers” on page 86	Covers how to create a separate home directory server.
“Creating Roles and Users” on page 87	Covers how to create administrative roles and users to assume those roles.
“Verifying That Roles Work” on page 88	Covers how to test that the roles are effective.
“Finishing Up Configuration” on page 89	Covers how to share and mount file systems, and how to delete the install user. Points you to auditing and further setup information,

Initial Configuration

▼ Initially Configure the Machine

- Do the following procedures in “No Name Service Configuration Tasks” on page 49, then return to this chapter.
 - “Log In ” on page 50
 - “Assume the root Role” on page 51
 - “Launch a Terminal” on page 52
 - One of: “SPARC: Protect Machine Hardware” on page 53 or “IA: Protect the BIOS” on page 53

- “Create an Admin_High Workspace” on page 54
- “Allocate the Appropriate Device” on page 54
- “Check and Install Your Label Encodings File” on page 55
- “Deallocate the Device” on page 56
- “Initialize the SMC Server” on page 56
- “(Optional) Save the Current Toolbox” on page 58

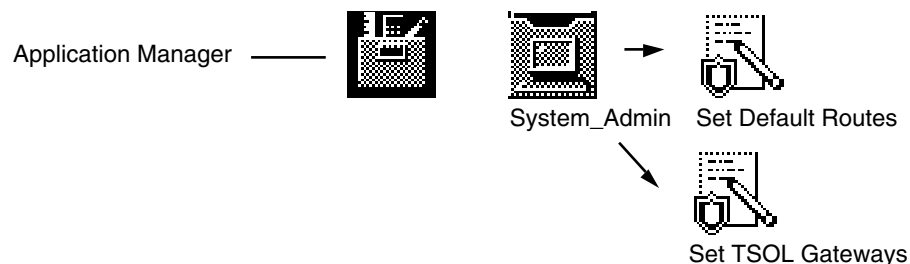
(Optional) Configuring Routing

If you configure the name service master to use static routing, you must configure the clients to use the same routing method.

Set up static routing only if the security administrator has planned for an open network and you do not plan to use dynamic routing. Dynamic routing is the default, and requires no setup.

See “Administering Trusted Networking” in *Trusted Solaris Administration Overview* for more information.

For static routing, do *one* of “Set Up Simple Static Routing” on page 59 or “Set up Static Routing Using Extended Metrics” on page 60.



▼ Set Up Simple Static Routing

For small networks, an `/etc/defaultrouter` file provides a simple routing method.

1. Double-click the Set Default Routes action in the System_Admin folder.

See “To Open a File that has a Defined Action” on page 132 if you are unfamiliar with using trusted actions.

An empty `/etc/defaultrouter` file appears in the trusted editor.

2. Enter the name or the IP address of the default router. If there is more than one, enter them all, one per line, and then save the file.

For example, if the hosts `trustworthy` and `forwardho` are routers, enter them, one per line:

```
trustworthy
forwardho
```

▼ Set up Static Routing Using Extended Metrics

If your host or site accesses a complex network of gateways, the `/etc/tsolgateways` file offers more routing options. See the `tsolgateways(4)` man page for examples.

1. Double-click the **Set TSOL Gateways** action in the **System_Admin** folder.

See “To Open a File that has a Defined Action” on page 132 if you are unfamiliar with using trusted actions.

An empty `/etc/tsolgateways` file appears in the trusted editor.

2. Enter the IP address of the subnet, the name of the gateway and its metric. Repeat for every gateway and save the file.

For example, if the hosts `trustworthy` and `forwardho` are gateways:

```
192.168.15.0 trustworthy 1
192.168.8.0 forwardho 2
```

Note – If the system has an `/etc/defaultrouter` file and an `/etc/tsolgateways` file, only the `/etc/tsolgateways` file is used for routing decisions.

Configuring the Network

▼ Add Hosts to a Machine’s Known Network

1. In the root role at the label `ADMIN_LOW`, return to the Solaris Management Console or re-open it if it is closed.

```
# smc
```

2. Click *this-host*: Scope=Files, Policy=TSOL under **Trusted Solaris Management Console in the Navigation pane**.

See Figure 9–1 for what tools should display in the Navigation pane .

3. Display the computers known to this host by clicking **Trusted Solaris Configuration**, then clicking **Computers and Networks**,
4. Provide a password if prompted, then double-click **Computers**.

Note – If toolbox icons display as red stop signs, the toolboxes will not load. To load them, see step 2 in “Initialize the SMC Server” on page 56.

This computer should already be in the database. You should add the following hosts:

1. Name service master, if any.
 2. Static routers, if any.
 3. Audit servers for this host.
5. Add every host that this computer may contact during boot by choosing **Add Computer** from the **Action** menu.
 - a. Click **Apply** to add each host.
 - b. Click **OK** when the entries are complete.

▼ (Optional) Remove the 0.0.0.0 Network

The network wildcard 0.0.0.0 may present a security risk. See “Modifying the Boot-time Trusted Network Databases” in *Trusted Solaris Administrator’s Procedures* for more information.

- Follow the instructions in the “To Replace the 0.0.0.0 Entry in the Local Tnrhdb File” procedure under “Managing Trusted Networking (Tasks)” in *Trusted Solaris Administrator’s Procedures*.

▼ Add a Remote Host Template

If you used the Trusted Solaris `label_encodings` file, you can skip this step.

If this host is going to contact unlabeled hosts, the `tnrhtp` file must have an appropriate unlabeled template for those unlabeled hosts. See Table 1–3 in “Additional Planning for Open Networks” on page 29 for host types and their associated templates provided by Trusted Solaris software.

The `tnrhttp(4)` file installed by the Trusted Solaris installation program contains examples of templates that match the `label_encodings(4)` file installed during Trusted Solaris installation. If you installed a site-specific `label_encodings` file, it is highly likely that the existing `tnrhttp` templates will not work with your file.

1. **In the root role at the label `ADMIN_LOW`, double-click Security Families under Computers and Networks in the Solaris Management Console.**

The existing templates are displayed in the View pane.



Caution – Sites that install a site-specific `label_encodings` file *must* create templates that reflect the labels of machines and networks that the Trusted Solaris network can contact.

You should have templates for:

1. The Trusted Solaris hosts that this machine can contact.
 2. Any unlabeled hosts/networks that this machine can contact..
2. **To create a single-label template to assign to unlabeled hosts, choose Add Template from the Action menu.**

Consult the online help as you create the template.

- a. **In the Basic Information tab, create a template named `unlab_min-user-label`, of host type Unlabeled, with an `ADMIN_HIGH` clearance and a process label of `min-user-label`.**

The default clearance must dominate the default label. The label `ADMIN_HIGH` dominates all labels.

- b. **Click OK when the template is complete.**

3. **Create any other templates your site needs before continuing.**

▼ Assign a Template to a Remote Host

The trusted network remote host database, `tnrhdb`, enables this host to communicate with remote hosts. The `tnrhdb(4)` man page describes the format of the entries, and suggests how to minimize the number of entries required.

Assign a remote host template to every host or network that this machine may contact. Include every host in the `/etc/hosts` file.

See Table 1–3 in “Additional Planning for Open Networks” on page 29 for host types and their associated templates provided by Trusted Solaris software.

1. In the root role at the label **ADMIN_LOW**, double-click Security Families under Computers and Networks in the Solaris Management Console.
2. Double-click the Trusted Solaris security family, `tsol`.
3. Choose Add Host(s) from the Action menu.
4. In the Add Host(s) dialog box, click Add Wildcard to assign this template to all hosts on your Trusted Solaris subnet.
 - a. Enter the subnet IP address and choose the template name.
For example, enter `192.168.10.0` and `tsol`. The final zero signifies a subnet address; all hosts on that subnet are recognized as `tsol` hosts.

Note – The number zero (0) is the wildcard. Do not use a star (*).

- b. Click OK.
5. Choose Add Host(s) from the Action menu and click Add Host in the Add Host(s) dialog box to enter any exceptions to the subnet template assignment. Click OK to end the entry.
For example, enter `192.168.10.3` and `unlab_min-user-label`. This host on the subnet is an unlabeled host, an exception to the `tsol` wildcard entry.
6. Choose Add Host(s) from the Action menu and click Add Host to enter the IP address of every host in your `/etc/defaultrouter` or `/etc/tsolgateways` file, and assign to each an appropriate template name. Click OK to end each entry.
7. Enter the details of other subnets and hosts.
 - a. Enter the wildcard designation of each subnet and choose its appropriate template by choosing Add Host(s) → Choose Wildcard.
 - b. Individually assign a different template to any host that is an exception to its subnet's assigned template by choosing Add Host(s) → Choose Host.
Use the details provided by your system administrator, then choose the appropriate template name from the menu.
8. Open a terminal to reload and verify the updated `tnrhdb` database.

```
# tnctl -H /etc/security/tsol/tnrhdb
# tninfo -h
```

Trusted Network Summary

The `tnrddb` database must have an IP address and template name for every host or subnet that the hosts in the Trusted Solaris domain can communicate with:

1. The master server (that is, this host)
2. Every client that will be in the Trusted Solaris domain, or its subnet wildcard mechanism `nnn.nnn.nnn.0`
3. Every static router (open network only)
4. Every other host with which the domain can communicate, or a wildcard address for its subnet (open network only)

Setting Up the Name Server and Domain

Setting up the name service master sets up the name service domain for the Trusted Solaris clients. Several name service databases have been created or modified to hold Trusted Solaris data about label configuration, users, and remote hosts.

▼ Set Up Files to be Name Service Databases

1. **As root, create a staging area for files you plan to use to populate the name service databases.**

You can place the staging area wherever you have enough space. Usually a few megabytes is more than enough room to store some files temporarily.

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

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

Most of the files that you need already exist on the installed system and have enough data in them to get you started. The following files in the `/etc` directory are usually not found on a newly installed system: `bootparams`, `ethers`, `netgroup`, `netmasks`, and `timezone`. You can create these with an editor, load them from a backup diskette, or merely create empty versions of these files, so that the name service databases are created all at once. If you choose not to create these files, you can create them later, but a few warning messages may print out.

```
# cd /etc
# touch bootparams ethers netgroup netmasks timezone

# cp bootparams ethers netgroup netmasks timezone \
aliases auto_home auto_master group hosts networks \
```

```

protocols publickey rpc services /setup/files

# cd 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. Create empty files in the staging area of files whose contents should not be distributed.

```

# cd /setup/files
# touch audit_user passwd shadow user_attr

```

All entries in the `passwd`, `shadow`, and `user_attr` files on a newly-installed system are local users who should be restricted to local access. The name service will create empty databases from the empty files, and will not print spurious warning messages.

4. Check that all the files are now in your staging area. There are 25.

```

# ls | wc -l
25

```

5. Edit the `hosts` file in your staging area.

a. Open the Admin Editor and enter `/setup/files/hosts` for editing.

The file already contains the name service master (that is, this host's address) and the static routers, if any.

b. Add every system that will be in the Trusted Solaris domain.

There is no wildcard mechanism here. The IP address of every host to be contacted *must* be in this file.



Caution – Failure to include a host will cause client authentication to fail because the NIS+ client will have no credentials.

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

d. Use the `:wq!` command to write the file and exit the editor.

There is enough information in your staging area to convert your host to a name service master.



Caution – If you have edited any files, you must be very careful to provide all of the information necessary in the correct formats before populating the NIS+ tables. Failure to do so can result in the inability to further administer or use the system.

▼ Modify the /yp/Makefile (NIS domains only)

The `/var/yp/Makefile` file must be modified to point to the staging area and its subdirectories.

1. **Edit the `/var/yp/Makefile` in the Admin Editor.**
2. **Change four variables: `PWDIR`, `DIR`, `INETDIR`, and `RBACDIR`, to point to the `/setup/files` directory.**
3. **To ensure that the NIS master server stores its mail aliases in a NIS map, change the line in the `/var/yp/Makefile` file that begins with `ALIASES` to point to the NIS map.**

The name is in the format `ALIASES = /var/yp/mail-server.NIS-domain-name/mail.aliases`. For example,

```
ALIASES = /var/yp/pigeon.aviary.example.org/mail.aliases
```

The `/etc/mail/aliases` file remains available for mail aliases specific to the NIS master server.

▼ Create NIS Maps from the Staging Area (NIS domains only)

1. **Double-click the Create NIS Server action in the `System_Admin` folder.**
2. **Enter your NIS domain name.**

For example,

Domain Name: **aviary.example.org**

This action creates the domain name, establishes this host as the NIS master server, and copies the `/etc/nsswitch.nis` file over `/etc/nsswitch.conf`.

3. **When prompted for other NIS servers, enter their host names one by one.**

For example,

Host: **tern**

4. **Follow the instructions for ending the prompts.**

The action creates NIS maps from the `/setup/files` directory. It uses your modified `/var/yp/Makefile` to create the `/var/yp/NIS_maps`.

5. **Do not reboot your system yet.**

▼ Create NIS+ Tables from the Staging Area (NIS+ domains only)

1. **Double-click the Create NIS+ server action in the System_Admin folder.**

2. **Enter your NIS+ domain name.**

This host will be the root master. For example,

Domain Name: `aviary.example.org`.

There is a period at the end of the domain name.

3. **Answer the prompts (`y`, `y`, `rootpassword`).**

You can ignore diagnostics printing out that the file `/etc/defaultdomain` cannot be located. The file will be created.

4. **In the `/setup/files` directory, make sure that you have added all NIS+ clients to the hosts file.**

```
# cd /setup/files
# more hosts
```

5. **Populate the standard NIS+ databases from the `/setup/files` directory by running the Populate NIS+ Tables action in the System_Admin folder.**

6. **Enter your staging area when prompted.**

Populate from which directory? `/setup/files`

7. **Answer the prompts (`y`, `y`).**

```
...
Is this information correct? y
...
Do you want to continue? y
```

8. **Load any additional NIS+ tables you may have backed up, such as `auto_home`.**

Procedures vary depending on the format of the backup and on what types of NIS+ tables they are. Refer to the *Solaris Naming Setup and Configuration Guide* for details of how to load your tables.

9. **Do not reboot your system yet.**

▼ Edit SMC Toolbox Definitions for the Name Service

If you are running a name service, you must edit two files: the `tsol_smc.tbx`, and the name service toolbox. These files must be edited on the name service master before it can be used on the domain.

1. In the root role at the label `ADMIN_LOW`, list the toolbox directory.

```
# cd /var/sadm/smc/toolboxes
# ls tsol*/*tbx
tsol_files/tsol_files.tbx      tsol_nis/tsol_nis.tbx
tsol_smc/tsol_smc.tbx         tsol_nisplus/tsol_nisplus.tbx
```

- If you are running the NIS+ name service, your toolbox files are `tsol_smc/tsol_smc.tbx` and `tsol_nisplus/tsol_nisplus.tbx`
- If you are running the NIS name service, your toolbox files are `tsol_smc/tsol_smc.tbx` and `tsol_nis/tsol_nis.tbx`

2. Open the Admin Editor from the `System_Admin` folder.

3. Copy and paste the full pathname to the `tsol_smc.tbx` toolbox into the dialog box, as in:

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

4. Find your name service toolbox name in the file, and replace the Scope line with the name of the master and the name of the domain.

For example, change

```
<ToolBoxURL>
  <URL>../tsol_nisplus/tsol_nisplus.tbx</URL>
  <Scope>nisplus:/<?server?>/<?server?></Scope>
</ToolBoxURL>
```

To:

```
<ToolBoxURL>
  <URL>../tsol_nisplus/tsol_nisplus.tbx</URL>
  <Scope>nisplus:/eagle/aviary.example.org</Scope>
</ToolBoxURL>
```

5. Save (:wq!) and close the file.
6. Edit the name service toolbox in the Admin Editor.

EXAMPLE 5-1 NIS Toolbox

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

EXAMPLE 5-2 NIS+ Toolbox

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

7. In the editor, in the line beginning with <Scope>, replace the first instance of <?server ?> with the name service master, and the second with the fully-qualified domain name.

EXAMPLE 5-3 NIS <Scope>

```
<Scope>nis:/eagle/example.org</Scope>
```

EXAMPLE 5-4 NIS+ <Scope>

```
<Scope>nisplus:/eagle/aviary.example.org</Scope>
```

8. Replace every other instance of <?server?> or <?server ?> with the name service master, as in:

EXAMPLE 5-5 NIS <?server?>

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

EXAMPLE 5-6 NIS+ <?server?>

```
<Name> eagle: Scope=NIS+, Policy=TSOL</Name>
services and configuration of eagle.</Description>
and configuring eagle.</Description>
<ServerName>eagle</ServerName>
<ServerName>eagle</ServerName>
```

9. Write (:wq!) and quit the editor.

▼ (Optional) Set Up DNS

Skip this procedure if the security administrator has planned a closed network. For detailed information about DNS, see the *Solaris Naming Setup and Configuration Guide*.

1. If your system is going to use DNS, click the Set DNS Servers action in the System_Admin folder and enter the nameservers by IP address, one per line.

The file looks something like:

```
nameserver nnn.nnn.nnn.nnn
nameserver nnn.nnn.nnn.nnn
```

2. Using the **Name Service Switch** action, change the `hosts` entry in the `/etc/nsswitch.conf` file to use DNS.

EXAMPLE 5-7 NIS `nsswitch.conf` File

```
~
#hosts:      nis [NOTFOUND=return] files
hosts:      nis files dns
~
```

EXAMPLE 5-8 NIS+ `nsswitch.conf` File

```
~
#hosts:      nisplus [NOTFOUND=return] files
hosts:      files nisplus dns
~
```

▼ Reboot the Computer

- Shut down the system from the **TP (Trusted Path)** menu, and reboot it.

Name Service References

For fuller descriptions of name service setup and administration, and DNS, see

- *Solaris Naming Setup and Configuration Guide*
- *Solaris Naming Administration Guide*

Setting Up Critical Servers

Two servers are critical to the successful creation of users and roles: the home directory server and the mail server. If the name service master also serves as the home directory and mail server, you can skip this step. otherwise, install and configure the two critical servers, reboot them, and share them before adding roles and users.

▼ Install and Configure the Home Directory and Mail Servers

1. Install the system that will become the home directory server and the mail server by following the installation instructions in “Installing From a CD-ROM” on page 43.
2. Then configure each system to be a name service client (see “Client Configuration Tasks” on page 93), before making it a server. Return to configuring the name service master after completing “Sharing Critical File Systems” on page 104.
3. Then, create the administrative roles on the name service master as described in “Creating Roles and Users” on page 87.

Note – The administrative roles are created as network-visible accounts, not as local accounts. Their home directories are mounted from the home directory server.

Creating Roles and Users

The install team creates the administrative roles (other than root) to be used at the site. The team assigns each role its rights profiles. Initial rights profiles are provided on the installation CD-ROM.

Prerequisite: The name service, home directory, and mail server must be set up before you create the administrative roles secadmin, admin, and oper.

Note – In previous releases, roles were local. In the Trusted Solaris 8 4/01 operating environment, every role except root can be distributed. The roles are created by the install team.

▼ Create Domain-wide Roles and Users

- Create roles and users for the domain, following the procedures in “Creating Roles and Users” on page 64 within the appropriate scope.
 - The appropriate scope for NIS domains is *name-server*: Scope=NIS, Policy=TSOL
 - The appropriate scope for NIS+ domains is *name-server*: Scope=NIS+, Policy=TSOL.

▼ Add Roles to the NIS+ Admin Group (NIS+ domains only)

1. Open the `System_Admin` folder in the Application Manager.
2. Double-click the **Add to NIS+ Administrative Group** action.
3. Add the **admin** role to the NIS+ admin group.

Use your domain name with the format *subdomain.domain.suffix..* For example:

Group Name: **admin**

Principal Name: **admin.aviary.example.org.**

Note – Remember to type a period (.) at the end of the principal name.

4. Double-click the **Add to NIS+ Administrative Group** action to add the **secadmin** role.

For example:

Group Name: **admin**

Principal Name: **secadmin.aviary.example.org.**

5. Double-click the **Add to NIS+ Administrative Group** action to add the **primaryadmin** role.

For example:

Group Name: **admin**

Principal Name: **primaryadmin.aviary.example.org.**

Verifying That Roles Work

In the following tests, the appropriate scope for NIS domains is *name-server* :
Scope=NIS, Policy=TSOL. The appropriate scope for NIS+ domains is *name-server* :
Scope=NIS+, Policy=TSOL.

▼ Log Out

- Log out by clicking the **EXIT** button on the Front Panel.

▼ Verify that the Roles secadmin and admin Work

1. For each role, log in as a user who can assume the role and assume it.
2. In the role workspace, open the Solaris Management Console, select the Trusted Solaris Management Console with the appropriate scope for your site, and click Users.
3. Provide the role password when prompted, then double-click User Accounts.
4. Click a user.
 - The admin role should be able to modify fields under the tabs General, Home Directory, and Group.
 - The secadmin role should be able to modify fields under all tabs.

▼ Verify that the Role primaryadmin Works

1. Log in as a user who can assume the primaryadmin role and assume it.
2. In the role workspace, open the Solaris Management Console, select the Trusted Solaris Management Console with the appropriate scope for your site, and click Users.
3. Provide the role password when prompted, and double-click Rights.
4. Creating a new right by choosing Add Right from the Action menu.
5. Save the new right, then delete it before continuing.

Finishing Up Configuration

▼ Set Up Auditing

The security administrator is responsible for auditing decisions.

- **Configure or disable auditing by doing *one* of the following two procedures.**
Disable auditing—if site security does not require auditing. To disable auditing in the Trusted Solaris environment, follow the procedures described in *Trusted Solaris Audit Administration*.

Configure auditing—by following the procedures in *Trusted Solaris Audit Administration*. Every Trusted Solaris system should audit users and events identically.

▼ Copy Configuration Files for Distribution to Clients

1. As root at label **ADMIN_LOW**, create a directory that cannot be deleted between reboots.

```
# mkdir /export/clientfiles
```

2. Copy modified files to the `/export/clientfiles` directory.

For example, most sites will want to copy the `/var/sadm/smc/toolboxes/tsol_smc/tsol_smc.tbx` and the `/var/sadm/smc/toolboxes/tsol_nameservice/tsol_nameservice.tbx` files to the client machines. A site that is using a modified `tnrhttp` file, DNS, and auditing might copy the files `/etc/security/audit_control`, `/etc/security/audit_startup`, `/etc/security/tsol/tnrhttp`, `/etc/resolv.conf`, and `/etc/nsswitch.conf`.

3. Allocate a diskette at **ADMIN_LOW**, and transfer the files to it.

Physically affix a label to the diskette that marks it as containing **ADMIN_LOW** information.

4. Use this diskette, and your `label_encodings` diskette, labeled **ADMIN_HIGH**, when configuring your clients.

▼ (Optional) Share File Systems

If a directory is being shared before the admin role is created, the install team performs the procedure in the root role.



Caution – Do not use proprietary names for shared file systems. The names of shared file systems are visible to every user.

1. In the admin role, (or root if the admin role does not exist), at label **ADMIN_LOW**, under **Trusted Solaris Management Console**, click *this-host*: Scope=Files, Policy=TSOL.
2. Click **Storage**, and provide a password if prompted.

3. Double-click Mounts and Shares, and then double-click Shares
4. Choose Add Shared Directory from the Action menu.
5. Follow the online help to share the directory.
The tool shares the directory and starts the NFS daemons,
6. To modify the attributes of the shared directory, double-click the Properties tab and use the online help to guide you.

▼ (Optional) Mount File Systems

In the Trusted Solaris environment, unlabeled and labeled hosts can be mounted on a Trusted Solaris labeled host.



Caution – Do not use proprietary names for mounted file systems. The names of mounted file systems are visible to every user.

1. In the admin role at label **ADMIN_LOW**, under Trusted Solaris Management Console, click *this-host: Scope=Files, Policy=TSOL*.
2. Click Storage and provide a password if prompted.
3. Double-click Mounts and Shares, and then double-click Mounts.
4. Choose Add NFS Mount from the Action menu.
5. Follow and answer the prompts to mount the file system.
You are prompted to allow creation of the mount point if it does not exist. The tool adds an entry in the `/etc/vfstab` file, creates the mount point, and mounts the file system.

▼ (Optional) Delete the User install



Caution – Do not remove the user install until you are satisfied that the client systems can communicate with the name service master.

When a user is deleted from the system, the administrator must ensure that the user's home directory and any objects owned by that user are also deleted. As an alternative to deleting objects owned by the user, the administrator may change the ownership of these objects to another user who is defined on the system.

The administrator must also ensure that all batch jobs that are associated with the deleted user are also deleted. The administrator must ensure that there are no objects or processes belonging to a deleted user that remain on the system.

Note – If you plan to use the `tsolconvert` utility, do not delete the `install` user until you have completed the required conversion steps on a Trusted Solaris 8 or Trusted Solaris 8 4/01 system. See “Saving and Restoring Trusted Solaris Databases” on page 138 for more information on converting Trusted Solaris 7 to Trusted Solaris 8 4/01 databases.

1. **In the admin role at label `ADMIN_LOW`, in the Solaris Management Console, choose the `this-host: Scope=Files, Policy=TSOL`, and click **Users**.**
2. **Provide a password if prompted, then double-click **User Accounts**.**
The user “install” is defined locally.
3. **Select the user to be deleted and click the **Delete** button.**
For the user `install`, you do not have mail files to delete. Other local users may have home directories and mail files to delete.

▼ Other Setup

- **See *Trusted Solaris Administrator's Procedures* for tasks such as handling mail, setting up printers, and protecting file systems.**

Configuring a Name Service Client

This chapter provides procedures to configure the name service clients at your site interactively, after you have configured the name server.

Who Does What

Trusted Solaris software is designed to be installed and configured by an install team. Once the team has created users who can assume Trusted Solaris roles, and has rebooted the computer, the software enforces task division by role. If two-person installation is not a site security requirement, you can assign the administrative roles to one person.

Client Configuration Tasks

Configuring a name service client is similar to configuring its master, except that configuration details the client receives from the master do not have to be repeated.

If the client machine was installed from a CD-ROM—you should expect to complete the configuration tasks in the following table. Depending on your site configuration, some procedures can be omitted.

TABLE 6-1 Task Map for Clients Installed from CD-ROM

Task	Described
"Initial Configuration" on page 95	Covers protecting the hardware, setting up the labels, and initializing the administration tools.
"(Optional) Configuring Routing" on page 97	Covers how to set up static routing.
"Configuring the Network" on page 98	Covers how to specify the hosts that are contacted during boot.
"Connecting to the Name Server" on page 100	Covers how to connect to the name service.
"Sharing Critical File Systems" on page 104	Covers how to share the home directory and mail server.
"Finish Configuring the System" on page 105	Points you to auditing setup information, how to share and mount file systems, and how to delete the install user.

If the client machine was installed over the network—you should expect to complete the configuration tasks in the following table in the appropriate role.

TABLE 6-2 Task Map for Clients Installed Over a Network

Role	Task Responsibility After Network Installation
secadmin role	
	"SPARC: Protect Machine Hardware" on page 95 or "IA: Protect the BIOS" on page 96
	"Install the Name Service Master's label_encodings File" on page 96
	"Copy the Name Service Master's Tnrhtp Database" on page 99
	"Initialize the SMC Server" on page 97, then "Assign Templates to Remote Hosts" on page 99
	"Set Up Auditing to Match the Master Server" on page 105
	"(Optional) Set Security Attributes on Mounted File Systems" on page 106
admin role	
	"Mount the Diskette With Configuration Files" on page 97
	"(Optional) Configuring Routing" on page 97
	"Initialize the SMC Server" on page 97, then "Add Hosts to be Contacted During Booting" on page 98
	"(Optional) Remove the 0.0.0.0 Network" on page 99

TABLE 6-2 Task Map for Clients Installed Over a Network (Continued)

Role	Task Responsibility After Network Installation
	“Copy the SMC Name Server Toolbox Definitions to the Client” on page 102
	“Copy Network Files to the /etc Directory” on page 102

If the client machine was installed using JumpStart scripts—you should expect to complete the configuration tasks in the following table in the appropriate role.

TABLE 6-3 Task Map for Clients Installed Using JumpStart

Role	Task Responsibility After Network Installation
secadmin role	
	“SPARC: Protect Machine Hardware” on page 95 or “IA: Protect the BIOS” on page 96
	“Set Up Auditing to Match the Master Server” on page 105
admin role	
	“Initialize the SMC Server” on page 97
	“Connecting to the Name Server” on page 100

Initial Configuration

▼ Log In

- Log in as `install`, assume the root role, and open a terminal.
See “Logging In and Launching a Terminal” on page 50 for details.

▼ SPARC: Protect Machine Hardware

1. In the terminal, enter the PROM security mode.

```
# eeprom security-mode=command
```

```
Changing PROM password:
New password: password
```

Retype new password: *password*

Choose the value `command` or `full`. See the `eeeprom(1M)` man page for more details.

2. If you are not prompted to enter a PROM password, the system already has a PROM password. To change the PROM password, run the command:

```
# eeeprom security-password=Return
Changing PROM password:
New password: password
Retype new password: password
```

The new PROM security mode and password are in effect immediately, but are most likely to be noticed at the next boot.



Caution – Do not forget this password. The hardware is unusable without it.

▼ IA: Protect the BIOS

On Intel architecture, the equivalent to protecting the PROM is to protect the BIOS.

- Refer to your machine's manuals for how to protect the BIOS.

▼ Install the Name Service Master's `label_encodings` File



Caution – The `label_encodings` file on the client machine must be identical to the one on the name service master. If you are *sure* it is identical, you may skip this step.

1. In the root role, create an **ADMIN_HIGH** workspace.
See "Create an Admin_High Workspace" on page 54 for details.
2. In the **ADMIN_HIGH** workspace, allocate the floppy device, and insert the name service master's **ADMIN_HIGH** diskette containing the `label_encodings` file.
See "Allocate the Appropriate Device" on page 54 for details.
3. Double-click the Check Encodings action in the **System_Admin** folder of the Application Manager and enter the full pathname of the `label_encodings` file.
4. Answer **yes** to install the the name service master's `label_encodings` file on the client.

5. Deallocate the floppy drive, and return to a root workspace labeled **ADMIN_LOW**.

▼ Mount the Diskette With Configuration Files

You made a diskette for the client in “Copy Configuration Files for Distribution to Clients” on page 90.

1. In the root role at label **ADMIN_LOW**, allocate the floppy device, insert the **ADMIN_LOW** diskette of selected files from the name service master, and mount it.
2. Leave up the File Manager that shows the diskette’s mount point.

▼ Initialize the SMC Server

- In the root role in an **ADMIN_LOW** workspace, start the SMC server process in the terminal window.

```
# smc
```

Note – The `smc` command initializes the SMC server. The first time the server is launched, it performs several registration tasks, which can take a few minutes.

If toolboxes do not load, see step 2 in “Initializing the Solaris Management Console” on page 56 for troubleshooting procedures. If the client was installed with the End User cluster, SMC will not run.

(Optional) Configuring Routing

If you configured the name service master to use static routing, you must configure the clients to use the same routing method.

▼ Configure to Match the Name Server's Routing Method

1. If the name service master is configured for static routing, determine the appropriate static routing for the client.

TABLE 6-4 Client Static Routing Entry

Server Interfaces	Client on same subnet	Client on different subnet
Name service master has 1 network interface	Use same entry as master's	Static routing will be slightly different for the subnet
Name service master has >1 network interface	Enter master's other network interface(s) in static routing file	

2. Configure the client to use the same static routing method as the one used on the master.

Configuring the Network

▼ Add Hosts to be Contacted During Booting

Note that a name service client finds its file servers, home directory server, mail server, and other servers from the name service master.

1. In the root role at the label **ADMIN_LOW**, return to the Solaris Management Console or re-open it if it is closed.

smc

2. Click *this-host*: *Scope=Files*, *Policy=TSOL* under **Trusted Solaris Management Console in the Navigation pane**.

See Figure 9-1 for what tools should display in the Navigation pane .

▼ (Optional) Remove the 0.0.0.0 Network

The network wildcard 0.0.0.0 may present a security risk. See “Modifying the Boot-time Trusted Network Databases” in *Trusted Solaris Administrator’s Procedures* for more information.

- Follow the instructions in the “To Replace the 0.0.0.0 Entry in the Local Tnrhdb File” procedure under “Managing Trusted Networking (Tasks)” in *Trusted Solaris Administrator’s Procedures*.

▼ Copy the Name Service Master’s Tnrhttp Database

You can skip this step if your site did not modify or replace the `label_encodings` file and the `tnrhttp` file that were installed from the Trusted Solaris 8 4/01 Installation CD.

Note – The `tnrhttp(4)` template definition and name for the name service master must be identical on the client and master.

- In the root role at label **ADMIN_LOW**, copy the `tnrhttp` file from the `/diskette-mount-point/export/clientfiles` directory to `/etc/security/tsol/tnrhttp`.

See “To Copy Files From a Diskette” on page 135 if you are unsure how to copy using the File Manager.

▼ Assign Templates to Remote Hosts

The clients get most of their template assignments from the name service. A client’s local `tnrhdb` database must contain servers that are contacted during boot, such as the name service master (or its subnet), static routers, and any audit servers.

1. In the root role at the label **ADMIN_LOW**, double-click **Security Families under Computers and Networks in the Trusted Solaris Configuration**.
The remote host templates display in the View pane.
2. Double-click the remote host template, `tsol`.
3. Choose **Add Host(s)** from the Action menu, click **Add Host**, and enter the IP address and template name (`tsol`) of the Trusted Solaris name service master.
4. Add the audit server by choosing **Add Host(s)** from the Action menu. Then click **Add Host** and enter the IP address of the client’s audit server and `tsol` host type.

5. Again choose **Add Host(s)** from the Action menu, click **Add Host**, and enter the IP address and host type of the static router(s).

A client with one defaultrouter and no audit server would have three entries in its `tnrhdb`:

1. The client and its host type (`tsol`),
2. The name service master and its host type (`tsol`) (or its subnet fallback IP address and `tsol`)
3. The defaultrouter and its host type.

6. Open a terminal to reload and verify the updated `tnrhdb` database.

```
# tnctl -H /etc/security/tsol/tnrhdb
# tninfo -h
```

Summary of Client Network Files

These client files must be compatible with the name service master files:

- `/etc/security/tsol/label_encodings`
- `/etc/security/tsol/tnrhtp`

The client's local `tnrhdb(4)` file must have the IP address and host type of the NIS+ master (or the IP address and host type of the subnet), the client's static routers, and the client.

In addition, the client's address and name, the name service master's name and address, and the static routers' names and addresses must be in the local `hosts` database.

Connecting to the Name Server

▼ Verify Communication with the Name Service Master

Skip this procedure if the client specified the name service, NIS or NIS+, during network install.

1. As root, at label **ADMIN_LOW**, check to see that you can ping the name service master.

```
# ping name-service-master
```

2. Check to see that you can rup the name service master.

```
# rup name-service-master
```

If the rup(1) command succeeds, you may proceed. If it fails, debug your network setup until the rup command succeeds.

Note – If you have added a client that was not initially on the master, you must add it to the master and assign it a template. On the master, the ping and rup commands must work to contact the new client before continuing.

▼ Add Client to the NIS+ Domain

Note – Skip this procedure if the client specified a name service during network install. After JumpStart installation, you must do the procedure to add the client to the domain.

Prerequisite: The rup command must succeed in both directions: from client to master, and master to client.

1. In the root role at label **ADMIN_LOW**, add the host as a NIS+ client using the Create NIS+ Client action in the System_Admin folder.
2. Enter the NIS+ domain name and host name of the root master. There is a period at the end of the domain name.

For example,

```
Domain Name: aviary.example.org.  
Hostname of NIS+ Master: eagle
```

3. Answer the prompts (y, (your-master's-ip-address), nisplus, rootpassword).
You can ignore diagnostics printing out that certain files and directories cannot be located. The files and directories will be created.

4. Do not reboot when the program prints the message:

```
Once initialization is done, you will need to reboot your machine.
```

You will reboot after setting up DNS.

▼ Add Client to the NIS Domain

1. In the root role at label **ADMIN_LOW**, add the host as a NIS client using the Create NIS Client action in the System_Admin folder.

Note – If this is a NIS slave server, make sure you enter this host name and the name of the master server at the prompts.

The action copies the `nsswitch.nis` file to the `nsswitch.conf` file.

2. Do not reboot until after you have set up DNS.

▼ Copy the SMC Name Server Toolbox Definitions to the Client

Note – Administrators who want to administer the name service using SMC from this client system *must* do this procedure

1. In the root role at label **ADMIN_LOW**, copy the name service master's `tsol_nameservice.tbx` file from the `/diskette-mount-point/export/clientfiles` directory to the `/var/sadm/smc/toolboxes/tsol_nameservice` directory.
If you did not copy the files to the client, do the “Edit SMC Toolbox Definitions for the Name Service” on page 84 procedure on the client system.
2. Also copy the name service master's `tsol_smc.tbx` file from the `/diskette-mount-point/export/clientfiles` directory to the `/var/sadm/smc/toolboxes/tsol_smc` directory.

▼ Copy Network Files to the /etc Directory

If you are using DNS to contact hosts outside of your domain, or if you have altered the `resolv.conf` and `nsswitch.conf` files on the name service master, set up DNS before rebooting.

- In the root role at label **ADMIN_LOW**, set up the DNS nameservers and the name service switch by copying the files `resolv.conf` and `nsswitch.conf` from the `/diskette-mount-point/export/clientfiles` directory to the `/etc` directory.
If you did not copy the files to the client, follow the procedure in “(Optional) Set Up DNS” on page 85.

▼ Reboot the Computer

Skip this procedure if the client was installed over the network.

- Shut down the system from the TP (Trusted Path) menu, and reboot it.

▼ Enable the Slave Server (NIS domain only)

1. If this is a NIS slave server, log in, assume the root role, open a terminal, and enable `ypinit`.

```
# /usr/sbin/ypinit -s NIS-master-server
```

2. Before continuing, reboot the machine again to enable it to serve NIS clients.

▼ Add the IMAP Server (NIS+ domain only)

1. If this is an IMAP mail server, go to the NIS+ master and log in.
This procedure enables the mail server to authenticate users.
2. Assume the admin role in an `ADMIN_LOW` workspace, and open the `System_Admin` folder in the Application Manager.
3. Double-click the `Add to NIS+ Administrative Group` action and enter the group name and the full name of your mail server.

Use your domain name with the format *subdomain.domain.suffix*. For example:

Group Name: `admin`

Principal Name: `pigeon.aviary.example.org`.

Note – Remember to type a period (.) at the end of the the principal name.

Sharing Critical File Systems

▼ Share Home Directories

See “Administering NIS+ Groups” in *Solaris Naming Administration Guide* for ways to restrict home directory access to particular groups.

1. In the root role at label **ADMIN LOW**, under **Trusted Solaris Management Console**, click *this-host*: Scope=Files, Policy=TSOL.

Note – If toolbox icons display as red stop signs, the toolboxes will not load. To load them, see step 2 in “Initialize the SMC Server” on page 56.

2. Click **Storage**, provide a password if prompted, then double-click **Mounts and Shares**, then double-click **Shares**.
3. Choose **Add Shared Directory** from the **Action** menu.
4. Follow the online help to share the `/export/home` directory.
The tool shares the directory and starts the NFS daemons,
5. Verify that the directories are shared.

```
$ showmount -e
export list for homedir-server:
/export/home
```

▼ Share Mail Server Directories

1. Repeat the above procedure to share the mail service directory.

For example, when the directories are shared, the `showmount` command would show something like the following:

```
$ showmount -e
export list for mail-server:
```

```
/export/post
```

If the users' home directories and email directories are on the same server, the command would show the following:

```
$ showmount -e
export list for server:
/export/home
/export/post
```

2. If you have not finished configuring the name service master, return to "Creating Roles and Users" on page 87. Otherwise, continue below.

Finish Configuring the System

If you are configuring a site that satisfies criteria for an evaluated configuration, read "Understanding Your Site's Security Policy" on page 24. Users assume the roles that have been created — security administrator and system administrator — to complete system configuration.

▼ Set Up Auditing to Match the Master Server

The client's audit configuration must be identical to the name service master's. The domain should collect auditing records as if one machine were being audited.

1. **To ensure that every system and user is audited identically, in the root role at label ADMIN_LOW, copy the name service master's /etc/security/audit* configuration files to the system from the /diskette-mount-point/export/clientfiles directory.**
2. **In the secadmin role, customize the dir: entries for the local host in the audit_control file.**

Follow the procedures in *Trusted Solaris Audit Administration*.

▼ (Optional) Set Security Attributes on Mounted File Systems

- To set security attributes on an unlabeled file system, assume the role `secadmin`, and in an `ADMIN_LOW` workspace, use the Admin Editor to enter the file system in the `vfstab_adjunct` file.

The `vfstab_adjunct(4)` file is saved and protected at the label `ADMIN_HIGH`.

▼ (Optional) Mount and Share File Systems

The `admin` role handles file system management, and user account creation and deletion.

- In the `admin` role in an `ADMIN_LOW` workspace, finish configuring the system.
 - To share a file system, see “(Optional) Share File Systems” on page 90.
 - To mount a file system, see “(Optional) Mount File Systems” on page 91.

▼ (Optional) Delete the Install User

- Read “(Optional) Delete the User install” on page 91 before deleting the install user.

Installing a Trusted Solaris System Over a Network

When installing Trusted Solaris software over a network, the system administrator uses the *Solaris 8 Advanced Installation Guide* in conjunction with the Trusted Solaris exceptions and additions described in this chapter.

Due to the security features in the Trusted Solaris environment, Trusted Solaris software modifies some of the procedures used for network installation, JumpStart installation, and Custom JumpStart installation. Also, the Trusted Solaris security and system administrators must enable access to commands on the installation CD-ROM or its image.

Setting Up Network Installation

For an overall view of the differences between Trusted Solaris and Solaris installation, see “Trusted Solaris Modifications to Network Installation” on page 112. See the “Preparing to Install Solaris Software Over the Network” in *Solaris 8 Advanced Installation Guide* for the installation procedures themselves.

Steps	Where Described
1. Copy installation CDs to hard disk.	“Give Mounted Media All Allowed Privileges” on page 108
	“Allocate the CD-ROM Device” on page 108
	“Modify Permissions of Mount Point Parent” on page 109
	“Load Trusted Solaris Images from CDs” on page 109
2. Share the install directory.	“Share the Network Install Directory” on page 110

Steps	Where Described
3. Add client information and reboot.	"Add Client Information to the Install Server" on page 111
4. Boot the client machine.	"Boot Over the Network or with Custom Files" on page 47
5. Configure it.	"Client Configuration Tasks" on page 93

▼ Give Mounted Media All Allowed Privileges

Users in administrative roles copy the Trusted Solaris CD-ROMs to a server's hard disk. The secadmin role gives all allowed privileges to the CD-ROM device and modifies profiles where necessary. The admin role allocates the device, changes the permissions on the parent of the mount point, and copies the software to the install server.

1. Log in as a user who can assume the secadmin role and assume it.
2. Open the Admin Editor from the System_Admin folder and type `/etc/rmmount.conf` in the file name field.
3. Assign all allowed privileges to mounted removable media in the `/etc/rmmount.conf` file, as in:

```
mount * hsfs udfs ufs -o nosuid allowed=all
```

4. Write the file with `:wq!` and exit the editor.

▼ Allocate the CD-ROM Device

1. Log in as a user who can assume the admin role and assume it.
2. In the admin role at label **ADMIN_LOW**, open the Device Allocation Manager, allocate the CD-ROM drive and mount it.
After the CD-ROM has been mounted, a File Manager pops up showing the mount point of the CD-ROM.
3. If a File Manager does not appear, bring one up from the Front Panel and navigate to the CD-ROM mount point.

For Trusted Solaris software, the mount point should be one of:

- `/cdrom/admin-cdrom_0/trusted_sol_8_sparc`
- `/cdrom/admin-cdrom_0/trusted_sol_8_ia`

4. In the File Manager, highlight `/cdrom/admin-cdrom_0`, the parent of the mount point.
5. From the Selected menu, choose Properties.
Note that the directory, named CD-ROM_FOLDER, has mode 700, so it is not searchable. The following procedure will fix that.

▼ Modify Permissions of Mount Point Parent

1. In the File Manager, click the Show Access Control List button, then Add ...
2. Highlight the Mask entry and click Change.
3. Change the Mask to Read and Execute, and click Change.
4. Click Add..., and enter root in the User field, giving it Read and Execute.
5. Click Add, then click OK to exit the dialog.
6. Leave the File Manager up, available for the installation setup commands.

▼ Load Trusted Solaris Images from CDs

1. In the File Manager, open the Tools folder, from one of the following:
 - `/cdrom/admin-cdrom_0/trusted_sol_8_sparc/Trusted_Solaris_8/Tools`
 - `/cdrom/admin-cdrom_0/trusted_sol_8_ia/Trusted_Solaris_8/Tools`
2. From the File menu select Open Terminal.
3. Still in the admin role, transfer the files from the first CD to the install server by typing

```
$ ./setup_install_server /export/install/ts8_{sparc,ia}
```

Note – Do not double-click on this tool because the command must be started in a profile shell, not the shell defined in the File Manager.

By default, the Software Installation profile contains the exact pathname for this command. The secadmin role must modify this profile if a different mount point is used. To modify a profile, see “Modifying a Role’s Rights” on page 136.

EXAMPLE 7-1 Admin Role Verifying that a Command is Available

If the commands `add_install_client` and `rm_install_client` are in the admin role's profile, the `profiles(1)` command should display something like the following for a disk image:

```
$ profiles -l | grep install_client
/export/install/ts8_sparc/add_install_client:
    4,5,6,10,11,12,17,30,32,33,35,36,39,52,55,57,61,68,69
/export/install/ts8_sparc/rm_install_client:
    4,5,6,10,11,12,17,30,32,33,35,36,39,52,55,57,61,68,69
```

4. When the pound sign (#) prompt displays, deallocate the CD.
5. Insert the second CD, allocate it and mount it.
6. For the second CD, still in the admin role, repeat step 4 through step 6 of the procedure "Modify Permissions of Mount Point Parent" on page 109.
7. In the File Manager, open the Tools folder on the second CD, one of the following:
 - /cdrom/admin-cdrom_0/trusted_sol_8_sparc/Solaris_8/Tools
 - /cdrom/admin-cdrom_0/trusted_sol_8_ia/Solaris_8/Tools
8. From the File menu select Open Terminal.
9. Transfer the files from the second CD to the install server by typing

```
$ ./add_to_install_server /export/install/ts8_{sparc,ia}
```

Note – Do not double-click on this tool because the command must be started in a profile shell, not the shell defined in the File Manager.

10. Deallocate the second CD and remove it.

▼ Share the Network Install Directory

To complete network installation setup requires a user in the admin role. Follow the instructions for Solaris network installation setup, using the following procedures when needed.

1. In the admin role at **ADMIN_LOW**, start the Solaris Management Console.

```
$ smc &
```
2. Select the *this-host*: Scope=Files, Policy=TSOL toolbox.

3. **Navigate to the Mounts and Shares tool in the Solaris Management Console to share the network install directory for the Trusted Solaris image.**
If you are unsure of the steps, see “(Optional) Share File Systems” on page 90.
4. **Double-click the Properties tab to modify the properties of the shared file system.**
5. **Enter `ro`, `anon=0`, and “`netinstall dir`” for the network install directory, for example, for `/export/ts8_sparc_install`.**

▼ Add Client Information to the Install Server

To modify or create files in the `/etc` directory, use the Admin Editor from the `System_Admin` folder to give the file the correct security attributes.

See “To Create or Open a File from the Trusted Editor” on page 131 for how to create or modify a file using the Admin Editor.

1. **To create an empty `ethers` file, in the admin role at `ADMIN_LOW`, invoke the Admin Editor.**
2. **Enter the full path to the file, `/etc/ethers`.**
3. **Once the editor is open, type `:wq` to save the empty file.**
4. **In a terminal, change the file permissions to 644.**

```
$ chmod 644 /etc/ethers
```
5. **Run the Name Service Switch action from the `System_Admin` folder.**

6. **Change the `ethers`, `netmasks`, and `bootparams` entries in the file to read as follows:**

```
ethers: files name-service dns
netmasks: files name-service dns
bootparams: files name-service dns
```

The variable `name-service` is one of `nis` or `nisplus`.

7. **In the role `admin` at `ADMIN_LOW`, run the `add_install_client` command to add client information to the OS server.**
See the `add_install_client(1M)` for details.
8. **Reboot the install server before attempting to install clients over the network.**

Trusted Solaris Modifications to Network Installation

Trusted Solaris software modifies network installation commands and procedures that require greater security. For example, the Volume Manager adds a mounting-user directory when mounting devices in the Trusted Solaris environment.

TABLE 7-1 Trusted Solaris Differences in Network Installation

Solaris Software	Trusted Solaris Software
You can log in as root.	There is no superuser. You log in as a user who can assume the root role, or as a user who can assume the admin or secadmin role, depending on the task. Then, assume the role to perform the task.
Processes and files do not have a label.	All processes and files are labeled. Commands and actions are run at a particular label. Most administrative tasks are run at the label ADMIN_LOW.
Administrators can often use a command line interface, even if a corresponding GUI equivalent exists.	Many administrative commands are run from a GUI, which calls checking and synchronizing functions.
Administrators can run an administrative command from a CD-ROM or diskette.	Commands that are on a diskette or CD-ROM, or are accessible from an NFS mount, may need to be added to the admin role's profile before they can be run.
Allows you to use a CD-ROM or diskette without allocating it.	Requires you to allocate a peripheral device at a particular label before its use. Before removing the medium, you must deallocate it.

Modifications to Network Installation Commands

The following commands and actions are used when installing Solaris software or Trusted Solaris software over a network, and their use is modified in the Trusted Solaris environment. The following listing describes the additional procedures or security requirements. Commands that do not require a change in procedure are not listed. See the "Preparing to Install Solaris Software Over the Network" in *Solaris 8 Advanced Installation Guide* for the installation procedures themselves.

TABLE 7–2 Modified Network Commands

Network Command or GUI	Trusted Solaris Modification in its Use
setup_install_server(1M) add_install_client(1M) add_to_install_server(1M) rm_install_client(1M)	<p>You must be in the admin role, at label ADMIN_LOW, in a terminal where the command is in a profile assigned to the admin role.</p> <p>If the admin role does not have this <code>/pathname/*install*</code> command in its assigned profiles, the secadmin role, at label ADMIN_LOW, must add it to the Custom Admin Role profile.</p> <p>For the procedure, see “Modifying a Role’s Rights” on page 136.</p>
mount(1M)	<p>The admin role, at label ADMIN_LOW, runs this command.</p> <p>If you are mounting a CD-ROM or diskette on an installed system, the admin role must allocate the device at a particular label, usually ADMIN_LOW. When the medium is removed, the device must be deallocated.</p>

Setting Up Custom JumpStart Installation

In the Trusted Solaris environment, Custom JumpStart procedures are handled by administrative roles. For an explanation of Custom JumpStart, see “Preparing Custom JumpStart Installations” in *Solaris 8 Advanced Installation Guide*. Trusted Solaris software modifies Custom JumpStart procedures as it does other installations, with device allocation and task allocation by role. Note that the Trusted Solaris environment does not support mounting remote file systems during installation.

Note – Factory-installed JumpStart may not be supported by Trusted Solaris software.

▼ Create a JumpStart Diskette

This procedure is done by the admin role at label ADMIN_LOW.

1. In the admin role at label **ADMIN_LOW**, allocate the floppy drive.
See “Allocate the Appropriate Device” on page 54 if you are unsure of the steps.
2. Format the JumpStart diskette by running the **fdformat** command.
3. Create a file system on the diskette by running the **newfs** command.
4. Create a mount point on the diskette by running the **mkdir** command.
5. Run the **mount** command.

EXAMPLE 7-2 Mount a UFS Filesystem on a Diskette

To create a UFS file system on a diskette to be used for Custom JumpStart, as admin at **ADMIN_LOW**:

```
$ mkdir /ts8_jumpstart
$ mount -F ufs /dev/diskette /ts8_jumpstart
```

6. Run the **cp** command to copy the JumpStart sample directory to the diskette.
7. Share the directory.
For details of the procedure, see “(Optional) Share File Systems” on page 90.
8. Use the **-c** option to the **add_install_client** command to add JumpStart details to the install server’s local **bootparams** database.
9. When you are finished with the JumpStart diskette, deallocate the drive and remove the diskette.
See “Deallocate the Device” on page 56 if you are unsure of the steps.

▼ Edit a JumpStart Profile

- When following the procedures in “Creating a Profile” in *Solaris 8 Advanced Installation Guide*, assume the admin role at label **ADMIN_LOW**, and use the Admin Editor action to edit a JumpStart profile.

For how to use the Admin Editor, see “To Create or Open a File from the Trusted Editor” on page 131.

The upgrade keyword is not fully supported in the Trusted Solaris 8 4/01 installation program. If you want to upgrade Trusted Solaris 8 systems, this keyword should work.

▼ Use pfinstall to Test a Profile

Use this procedure to modify the procedures in “Testing a Profile” in *Solaris 8 Advanced Installation Guide* and “pfinstall” in *Solaris 8 Advanced Installation Guide*.

In the Trusted Solaris environment, testing profiles is handled by the admin role, and modifying rights profiles is handled by the secadmin role.

1. **On an installed and configured Trusted Solaris system, log in as a user who can assume the admin role.**
2. **As admin at label ADMIN_LOW, launch a terminal and see that the pfinstall(1M) command is available in the role’s profile shell.**

```
$ profiles -l | grep pfinstall
```

The name profile shell refers to a shell that recognizes rights profiles. It does not refer to the machine profiles being tested here.

3. **If the command is not in the profile, the secadmin role must add it to the admin role’s rights, and then the admin role launches a new terminal in which to run the command.**

See “Modifying a Role’s Rights” on page 136 for how to add the pfinstall command to the admin role’s rights profile.

▼ Edit a Rules File

1. **When following the procedures in “Creating the rules File” in *Solaris 8 Advanced Installation Guide*, assume the admin role at label ADMIN_LOW, and edit the rules file with the Admin Editor action.**

2. **To use a Trusted Solaris-specific value for the *version* keyword:**

For the installed option, the *version* keyword.

version - A version name, such as Trusted_Solaris_8, or the special word any. If any is used, any Trusted Solaris or SunOS release is matched.

For the osname option, the *version* keyword.

version — A version of Trusted Solaris the Trusted Solaris environment installed on the system: for example, Trusted Solaris 7.

▼ Validate a Rules File

- **In the admin role at label ADMIN_LOW, run the check script.**

▼ Copy a Rules File

- In the admin role at label **ADMIN_LOW**, copy the file.

Modifying Optional Custom JumpStart Procedures

Use the Trusted Solaris information that follows to modify the procedures in “Using Optional Custom JumpStart Features” in *Solaris 8 Advanced Installation Guide*.

▼ Create Begin and Finish Scripts

Use this information to modify the procedures in “Creating Begin Scripts” in *Solaris 8 Advanced Installation Guide* and “Creating Finish Scripts” in *Solaris 8 Advanced Installation Guide*.

1. **In the admin role at label **ADMIN_LOW**, create and modify scripts using the Admin Editor action.**
2. **Make sure that the scripts invoke a profile shell, such as `pfsh` or `pfksh`.**
See the `pfexec(1)` man page.

Trusted Solaris Script Examples

The following procedures expand on and modify procedures in “To Add Files With a Finish Script” in *Solaris 8 Advanced Installation Guide*.

▼ Reboot the Computer with a Finish Script

1. **The first line in the script must invoke a profile shell.**

```
#!/bin/pfsh  
...
```

2. **The last line in the finish script reboots the computer.**

```
#!/bin/pfsh
```

```
...  
/usr/sbin/reboot
```

▼ Add label_encodings File with a Finish Script

1. In the admin role at label **ADMIN_HIGH**, place a copy of the site's label_encodings file into the JumpStart directory on the diskette.

```
$ cp /etc/security/tsol/label_encodings ${SI_CONFIG_DIR}/label_encodings
```

2. Copy the label_encodings file onto the system during installtion.

For example, if you are using a custom JumpStart diskette to install Trusted Solaris software, the following finish script copies the file from the JumpStart directory into a system's /etc/security/tsol directory during a custom JumpStart installation:

```
#!/bin/pfsh  
cp ${SI_CONFIG_DIR}/label_encodings /a/etc/security/tsol
```

▼ Set the Root Password With a Finish Script

Note – This example modifies the procedures in “Setting the System’s Root Password With a Finish Script” in *Solaris 8 Advanced Installation Guide*.

- In the admin role at label **ADMIN_LOW**, set the variable **PASSWD** to an encrypted root password obtained from an existing entry in a system's /etc/shadow file.



Caution – If you set your root password by using a finish script, be sure to safeguard against those who will try to discover the root password from the encrypted password in the finish script.

Modifications to Creating a Disk Configuration File

In the Trusted Solaris environment, configuration files are handled by the admin role. Use the following information to modify the procedures in “Creating Disk Configuration Files” in *Solaris 8 Advanced Installation Guide*. The Intel architecture procedure also modifies “fdisk” in *Solaris 8 Advanced Installation Guide*.

▼ SPARC: To Create a SPARC Disk Configuration File

1. Log on as a user who can assume the admin role.
2. In the admin role at label **ADMIN_LOW**, launch a terminal and determine the device name for the system's disk.
3. Redirect the output of `prtvtoc` to create the disk configuration file:

```
$ prtvtoc /dev/rdisk/device_name > disk_config
```

▼ IA: To Create an Intel Disk Configuration File

1. As admin at label **ADMIN_LOW**, redirect the output of the following `prtvtoc` command to a file.

```
$ prtvtoc /dev/rdisk/device_name > file1
```

2. Save the output of the following `fdisk` command to a file.

```
$ fdisk -R -d -n /dev/rdisk/device_name 2>file2
```

3. Concatenate the two files to create a disk configuration file.

```
$ cat file1 file2 > disk_config
```

4. Copy the disk configuration file to the JumpStart directory: :

```
$ cp disk_config jumpstart_dir_path
```

Modifying a Solaris JumpStart Example

Use the Trusted Solaris information that follows to modify the example in “Example of Setting Up and Installing Solaris Software With Custom JumpStart” in *Solaris 8 Advanced Installation Guide*.

In the Trusted Solaris environment, the Solaris JumpStart marketing and engineering example requires a user to assume the admin role.

In the Trusted Solaris operating environment:

- The site uses NIS+. The Ethernet addresses, IP addresses, and host names are in NIS+ tables.
- JumpStart information must use “None” for the naming service. Hosts installed by JumpStart are cliented after JumpStart finishes.

Remote file systems are mounted after JumpStart finishes.

- All commands are done by a particular role at a particular label, usually ADMIN_LOW. To execute a command, the role must have the command at that label in its rights profile.
- All directories are created by the admin role at the label ADMIN_LOW, as in:

```
$ cp -r /export/install/ts8_sparc/jumpstart_sample /jumpstart
v
```

- To create a shared directory, in the admin role at label ADMIN_LOW follow the procedure in “Share the Network Install Directory” on page 110 to create a vfstab entry, as in:

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

- To create a profile, the security administrator in the admin role at label ADMIN_LOW uses the Admin Editor action.
- To edit the rules file, the admin role at the label ADMIN_LOW uses the Admin Editor action.
- To execute the check script, the admin role at the label ADMIN_LOW runs the check(1M) script, as in:

```
$ cd /jumpstart
$ ./check
```

▼ Set up the engineering systems for installation

On the install server, the admin role at the label ADMIN_LOW uses the add_install_client(1M) command:

```
$ cd /export/install
$ ./add_install_client -c server_1:/jumpstart host_eng1 sun4u
$ ./add_install_client -c server_1:/jumpstart host_eng2 sun4u
```

▼ Set up the marketing systems for installation

An administrator in the admin role at label ADMIN_LOW then uses the setup_install_server(1M) command that copies the boot software from the CD to the marketing server.

```
$ cd /cdrom/admin-cdrom_0/s0/Trusted_Solaris_8/Tools
$ ./setup_install_server -b /marketing/boot-dir sun4c
```

At label ADMIN_LOW, the admin role uses the `add_install_client` command on the marketing group's boot server.

```
$ cd /marketing/boot-dir
$ ./add_install_client -s server_1:/export/install \
-c server_1:/jumpstart host_mkt1 sun4c
$ ./add_install_client -s server_1:/export/install \
-c server_1:/jumpstart host_mkt2 sun4c    ...
```

Configuring a Headless Trusted Solaris System

Configuring and administering Trusted Solaris software on headless systems like the Netra™ series require different procedures than the same tasks on systems that have monitors. The Trusted Solaris operating environment 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 – If you are configuring a site for an evaluated configuration, please read “Understanding Your Site’s Security Policy” on page 24. The configuration methods dictated by headless systems do not satisfy the criteria for an evaluated configuration.

Headless System Configuration Tasks

On headless systems, a console is connected via 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.

Methods	Where Described
Choose a configuration and administration method. 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.	If you have a desktop system that is running the Trusted Solaris 8 4/01 environment, go to “To Set Up Remote CDE Login to a Headless System” on page 122.
	If you have a desktop system that is running SMC 2.0 client software, go to “To Set Up Remote SMC Login to a Headless System” on page 123.
	If you do not have a desktop system, and must use serial login to configure and administer the headless system, go to “To Set Up Administration by Serial Login” on page 125 .
	If you are logging in remotely using the <code>telnet</code> or <code>rlogin</code> command, go to “To Set Up Administration by Remote Login” on page 125.
2. Set up the communicating systems.	Use one of the methods above.
3. Configure the headless system.	See “Client Configuration Tasks” on page 93, and use the methods possible given your login method.
4. Administer the headless system.	See <i>Trusted Solaris Administrator's Procedures</i> , and use the methods possible given your login method.

▼ To Set Up Remote CDE Login to a Headless System

If you are connecting to a headless system from a Trusted Solaris host, the serial port must be allocated before it can be used. See the serial login procedure in “Managing Devices (Tasks)” in *Trusted Solaris Administrator's Procedures*.

1. **After the headless system is installed, boot it into single-user mode.**
2. **Use the `vi` command to add the Trusted Solaris desktop system to the `/etc/hosts` file on the headless system.**

For example, if a Trusted Solaris desktop system named `admindesktop1` is going to be the configuring system, enter its name and IP address in the `hosts` file, as in:

```
192.168.168.5 admindesktop1
```

3. **Use the `vi` command to add the Trusted Solaris desktop system to the `/etc/security/tsol/tnrddb` file on the headless system.**

For example,

```
192.168.168.5:tsol
```

4. On the headless system, add the entries to the kernel cache with the `tnctl` command.

```
# tnctl -H
```

5. On the Trusted Solaris desktop system, in an administrative role, use the Solaris Management Console Security Families tool to enter the headless system's information in the local `hosts` and `tnrhdb` files.

For example, if the headless system is named `headless1` with an IP address of `192.168.168.111`, the entries would look like:

```
192.168.168.111 headless1    # entry in the hosts file
192.168.168.111:tsol      # entry in the tnrhdb file
```

6. On the Trusted Solaris desktop system, add the entries to the kernel cache with the `tnctl` command.

```
$ tnctl -H
```

7. On the headless system, exit single-user mode and let the system complete the boot process.

8. Log out of the Trusted Solaris desktop system, then on the Login Screen choose **Options** → **Remote Login**.

9. Type in the name of the headless system, and the screen displays “Welcome to *headless-system*”.

For example, if you are connecting to a system named `headless1`, the screen displays “Welcome to `headless1`”.

10. Type `install` for the user name, and type the password for `install` when prompted.
11. When the `install` user's workspace appears, assume the root role.
12. See “Client Configuration Tasks” on page 93 for how to configure a Trusted Solaris system, and *Trusted Solaris Administrator's Procedures* for how to administer a Trusted Solaris system.

▼ To Set Up Remote SMC Login to a Headless System

For this procedure to work, one of the following systems must be available:

- A Solaris desktop system that is running the Solaris 8 4/01 release and can run the SMC 2.0 client process

Note – An End User installation does not include the SMC server software.

- A Windows client that is running the Solaris 8 4/01 release and can run the SMC 2.0 client process

1. After installation, boot the headless system into single-user mode.
2. Add the Solaris 8 4/01 desktop machine with the SMC version 2.0 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 "Managing Roles (Tasks)" in *Trusted Solaris 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 SMC server process.

```
# smc &
```

7. In the SMC 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 the install user and the root role. Provide passwords for both.
10. Bring up a Terminal or the Application Manager window from the Legacy tools set in the Navigation Pane.
11. Configure the headless system.

▼ To 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.

1. **In single user mode on the headless system, modify the `/etc/passwd` entry for the `install` user. Change the `install` user's shell from `/bin/false` to `/bin/pfsh`.**
2. **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 line above is broken with a backslash for printing convenience. You should not break the line in the `/etc/inittab` file.

3. **On the headless system, modify the `/etc/security/user_attr` entry for the `install` user to include the Primary Administrator profile.**

```
install...;profiles=...,Primary Administrator;
```

The Primary Administrator profile includes privileged shells. The `install` user can now run privileged commands.

▼ To Set Up Administration by 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 via `rlogin` or `telnet`. This procedure is not secure.

1. **Follow the steps for “To Set Up Administration by Serial Login” on page 125.**
2. **On the headless system, modify the `/etc/security/user_attr` entry for the `install` user to include the profile Convenient Authorizations.**

```
install...;profiles=...Primary Administrator,Convenient Authorizations;
```

The Convenient Authorizations profile enables the `install` user to log in remotely.

3. **On the headless system, lock the `install` account when it is no longer needed by editing the `/etc/shadow` file.**

```
install:*LK*:6445:::~:
```


Common Procedures

This chapter contains common administrative procedures that are useful to know when configuring a system. Each procedure, or part of it, is specific to the Trusted Solaris environment.

Logging In as a User

▼ To Log In as a Regular User

1. **Log in to the system using your user account name.**
2. **Enter your password.**

Note – Users must not disclose their passwords to another person, as that person may 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. Trusted Solaris software provides protection against insecure passwords, but cannot prevent a user disclosing his/her password or writing it down.

The Enable Logins dialog box, shown in Figure 4–1, is displayed if you are authorized to enable logins.

If you see the error message:

Logins are currently disabled.

Please ask your system administrator to enable logins.

then your user account was not assigned the Enable Login right. To fix, give the user the Enable Login right, or have someone else log in and enable logins.

3. Choose a login option and dismiss the dialog box.

The Message Of the Day dialog box is displayed. In a multilevel session, the default is to log in at the lowest label in your label range. You can also restrict your session to a single label.

4. Click OK to accept the default given to you by the security administrator.

Once the login process is complete, the Trusted Solaris screen appears briefly, and you are in a CDE session with four workspaces. If your user account is configured to display labels, the label of your session (a user account *cannot* be ADMIN_LOW) is displayed in the trusted stripe.

Ending a Session

Users can lock their screen or log out at the end of a session. Users authorized to shut down the system can halt it and reboot.

Note – Users must log off or utilize the lockscreen functionality before leaving a computer unattended. Otherwise a person may have access to the data of a user without having to pass identification and authentication, and that person would not be uniquely identified or accountable.

▼ To Lock the Screen

- Left-click the padlock at the left of the middle section of the Front Panel. >

▼ To Log Out

1. Right-click the workspace background and select Log out... from the Workspace Menu, or left-click the EXIT icon on the Front Panel.
2. When prompted, confirm that you want to log out.

▼ To Reboot the System

1. **Right click the CDE front panel and select Shut Down from the TP (Trusted Path) menu.**

The menu appears when the user or role is authorized to shut down the computer.

2. **Confirm the shutdown.**

3. **Enter `boot` at the `ok` prompt or `b` at the `>` prompt:**

Type `help` for more information

```
<#2> ok boot
```

Type `b` (boot), `c` (continue), or `n` (new command mode)

```
> b
```

Running Administrative Actions

The Application Manager contains a folder that holds administrative applications for the local machine, `System_Admin` and an action, `Solaris Management Console`, for administering local and distributed databases. The Application Manager icon is shown below.



How To Use System_Admin Actions

The `System_Admin` folder contains CDE actions for administering the local system. See the following table for a list of actions used during installation and configuration. For a full list of `System_Admin` actions, read the CDE online help. The `System_Admin` folder icon is shown below.



TABLE 9-1 Trusted Solaris Actions in the System_Admin Folder

Action Name	Action Behavior
Add Allocatable Device	Edit /etc/security/device_maps
Add to NIS+ Administrative Group	Run the nisgrpadm -a command
Admin Editor	Create or edit any file
Audit Classes	Edit /etc/security/audit_class
Audit Control	Edit /etc/security/audit_control
Audit Events	Edit /etc/security/audit_event
Audit Startup	Edit /etc/security/audit_startup
Audit Users	Edit /etc/security/audit_user
Check Encodings	Check syntax (and install) a label encodings file
Check TN Files	Check local tnrhdb and tnrhtp files
Check TN NIS+ Tables	Check NIS+ tnrhdb and tnrhtp databases
Configure Selection Confirmation	Edit /usr/dt/config/sel_config
Create NIS Client	Make this host a NIS client
Create NIS Server	Establish a NIS server with NIS maps
Create NIS+ Administrative Group	Run the nisgrpadm -c command
Create NIS+ Client	Make this host a NIS+ client
Create NIS+ Server	Establish a NIS+ domain
Delete from NIS+ Administrative Group	Run the nisgrpadm -r command
Delete NIS+ Administrative Group	Run the nisgrpadm -d command
Edit Encodings	Edit a label encodings file
List Administrative Group	Run the nisgrpadm -l command
Name Service Switch	Edit /etc/nsswitch.conf
Populate NIS+ Tables	Populate NIS+ tables from a files directory

TABLE 9-1 Trusted Solaris Actions in the System_Admin Folder (Continued)

Action Name	Action Behavior
Printer Administrator	Set up printers
Set Default Routes	Edit /etc/defaultrouter
Set DNS Servers	Edit /etc/resolv.conf
Set Mail Options	Edit the TSOL option in the sendmail.cf file
Set Mount Attributes	Edit /etc/security/tsol/vfstab_adjunct
Set Mount Points	Edit /etc/vfstab
Set TSOL Gateways	Edit /etc/tsolgateways
Share Filesystems	Edit /etc/dfs/dfstab
View NIS Map	View NIS map
View Table Attributes	View NIS+ table attributes
View Table Contents	View NIS+ table contents

▼ To Run a System_Admin Action

1. In an administrative role, open the Application Manager by right-clicking the background to bring up the Workspace menu. Choose Applications → Application Manager from the top of the menu.



2. Double-click the System_Admin folder icon —
3. Double-click the appropriate action. For more details, see “To Create or Open a File from the Trusted Editor” on page 131, “To Open a File that has a Defined Action” on page 132 and “To Run a Script from the System_Admin Folder” on page 132.

▼ To Create or Open a File from the Trusted Editor

Actions that open files in an editor use the Admin Editor icon shown below.



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. Enter 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.

▼ **To Open a File that has a Defined Action**

1. To open a file that has its own action, double-click its action in the System_Admin folder.

The file associated with the action appears in the trusted editor.

2. Enter the required information, write the file, and exit the editor.

▼ **To Run a Script from the System_Admin Folder**

1. To run a script that has its own action, double-click the action in the System_Admin folder.

When the script requires input, the prompts are displayed.

2. Follow the instructions.

The script is finished when all prompt windows have been dismissed.

Using the Solaris Management Console

The Solaris Management Console action in the Application Manager folder invokes a Java-based administrative GUI for configuring and maintaining a Trusted Solaris environment. The GUI lists toolboxes in a Navigation pane, as shown in the following figure.

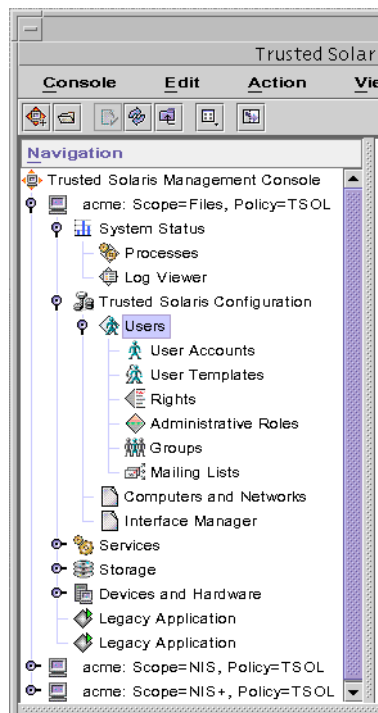


FIGURE 9-1 Solaris Management Console Tools in the Navigation Pane

The following can be configured through the Solaris Management Console, using the Trusted Solaris Management Console > Trusted Solaris Configuration toolboxes in the Navigation pane:

User Accounts—Part of the Users tool, for administering users.

Administrative Roles—Part of the Users tool, for administering roles.

Rights—Part of the Users tool, for constructing rights profiles. A user account is not usable until the user's Rights have been assigned.

Mailing Lists—Part of the Users tool, for administering mail aliases.

Computers and Networks—For setting up networks.

Computers—Part of the Computers and Networks tool, for setting up hosts (the `hosts` database).

Security Families—Part of the Computers and Networks tool, for creating and assigning remote host templates (the `tnrhttp(4)` and `tnrhdb(4)` databases)

Interface Manager—For securing network interfaces (the `tnidb(4)` database). Accessible only when `Scope=Files`.

The following are configured through the Solaris Management Console, using Trusted Solaris Management Console toolboxes:

Mounts—Part of the Storage tool, for mounting file systems. Accessible only when `Scope=Files`.

Shares—Part of the Storage tool, for sharing file systems. Accessible only when `Scope=Files`.

▼ To Locate a Solaris Management Console Tool

`Scope=Files` and `Scope=name-service` contain different tools. Read the online help for what the tool does and how to use it.

1. **To find and use a tool in *this-host*: `Scope=Files`, `Policy=TSOL` in the Navigation pane:**
 - Click the System Status key to view the Processes and Log Viewer tools.
 - Click the Trusted Solaris Configuration key to view the Users, Computers and Networks, and Interface Manager tools.
 - Click the Services key to view the SMC Server and the Scheduled Jobs tools.
 - Click the Storage key to view the Mounts and Shares and Disks tools.
 - Click the Devices and Hardware key to view the Serial Ports tool.
2. **To find and use a tool in the *name-server*: `Scope=name-service`, `Policy=TSOL` toolbox in the Navigation pane, click the Trusted Solaris Configuration key.**

The Users and the Computers and Networks tools are available in the *name-server*: `Scope=name-service`, `Policy=TSOL` scope.
3. **In the Navigation pane, click a toolset icon, such as Users.**
4. **When prompted, enter the role password in the Role Login prompt.**
5. **Double-click the tool, such as User Accounts.**
6. **Read and follow the online help for assistance with each tool.**

Copying to and from a Portable Medium

When copying to a portable medium, label the medium with the sensitivity label of the information.

Note – During installation, the root role copies administrative files to and from portable media. Most files are copied at label ADMIN_LOW.

▼ To Copy Files to a Diskette

1. **First, in a workspace at the target label, allocate the floppy device at the correct label using the Device Allocation action, and insert a clean diskette.**
For a fuller task description, see “Allocate the Appropriate Device” on page 54.
2. **Open a second File Manager from the Front Panel and navigate to the folder that contains the files to be copied, such as /export/clientfiles.**
3. **Highlight the icon for the file and drag the file to the floppy disk folder.**
4. **Deallocate the device.**
5. **On the floppy disk folder, choose Eject from the File menu.**

Note – Remember to physically affix a label to the medium with the sensitivity label of the copied files.

▼ To Copy Files From a Diskette

It is safe practice to rename the original Trusted Solaris file before copying in a file to replace it. When configuring a system, the root role renames and copies administrative files at ADMIN_LOW

1. **Allocate the floppy device using the Device Allocation action and insert the diskette.**
2. **If the system has a file of the same name, copy the original to a new name.**

For example,

```
# cp /etc/security/tsol/tnrhttp /etc/security/tsol/tnrhttp.orig
```

3. Open a second File Manager from the Front Panel and navigate to the desired destination directory, such as `/etc/security/tsol`.
4. Highlight the icon for the file and drag the file from the floppy disk folder to the destination directory.
5. Deallocate the device as described in “Deallocate the Device” on page 56.
6. Click OK on the dialog box when prompted to manually eject the floppy, and remove it.

Modifying a Role's Rights

When setting up a network or custom JumpStart install, some required commands may not be available to the role because they are in a path that is not assigned to the role. To add commands, programs, or scripts to the role's rights, the security administrator must modify the role's rights.

▼ To Add a Command to a Role's Rights

1. Log in as a user who can assume the role `secadmin` and assume it.
2. In the `secadmin` role at `ADMIN_LOW`, invoke the Solaris Management Console from the Application Manager.
3. Click the appropriate toolbox under Trusted Solaris Management Console.
Choose *this-host*: `Scope=Files`, `Policy=TSOL` if you are adding a command for a locally-defined role, or are not using a name service.
Choose *name-server*: `Scope=name-service`, `Policy=TSOL` if you are adding a command for a role defined on the network, such as for the admin role when setting up network install.
4. In the Navigation pane, click **Trusted Solaris Configuration**, then click **Users**.

Note – If toolbox icons display as red stop signs, the toolboxes will not load. To load them, see step 2 in “Initialize the SMC Server” on page 56.

5. Supply a role password if prompted, then double-click **Rights**.
6. In the View pane, scroll to the Custom *Rolename* Role and double-click.

7. Follow the online help for assistance in setting up the Custom *Rolename* Role right.

For a network installation example, use the Commands tab to add the `add_install_client` command from a non-standard directory, such as `/export/ultra_install_tsol/Trusted_Solaris_8/Tools` to the Custom Admin Role right. The command should have all privileges.

8. Make sure that the Custom *Rolename* Role right is assigned to *Rolename*. If it is not, assign it to *Rolename*.

a. Navigate to Administrative Roles.

b. Double-click the *Rolename* role.

c. Click the Rights tab.

d. Open the rights displayed in the Granted Rights column.

If it has already been granted, click the Cancel button. If the Custom *Rolename* Role right is not granted, continue.

e. Add Custom *Rolename* Role to the role's Granted Rights.

f. Click OK to save your work.

▼ To Verify That a Command is Available to a Role

1. Log in as a user who can assume the role whose profile has been updated.

2. Assume the role and launch a terminal from the role's workspace.

3. Verify that the new profile is in effect in the new terminal by using the `profiles(1)` command.

For example, to verify that the `setup_install_server` command is included in the admin role's rights profile with all privileges, in the admin role enter the following:

```
$ profiles -l | grep setup_install_server
/export/ultra_install_tsol//Trusted_Solaris_8/Tools/setup_install_server: all
```

▼ To Remove a Command from a Role's Rights

1. In the secadmin role at ADMIN_LOW, in the Solaris Management Console use the same toolbox that you used to add the command to the rights profile, and navigate to Rights.

2. In the View pane, select the Custom *Rolename* Profile.

3. Follow the online help for how to remove the command from the profile.

Saving and Restoring Trusted Solaris Databases

The Trusted Solaris 8 and Trusted Solaris 8 4/01 user and profile databases are in new formats with new names. To retain the usable data from their previous versions requires an administrator, before installing the Trusted Solaris 8 4/01 operating environment, to run the `tsolconvert` utility on a Trusted Solaris 7 or Trusted Solaris 2.5.1 system, to save the output directory to a safe storage area, and then to restore the files and run a shell script on the Trusted Solaris 8 4/01 system.

The following table shows the name or content difference between earlier releases and the Trusted Solaris 8 4/01 release.

Trusted Solaris Databases	Trusted Solaris 8 4/01 Database Description
<code>/etc/security/tsol/tsoluser</code>	<code>user_attr(4)</code>
<code>/etc/security/tsol/tsolprof</code>	<code>exec_attr(4)</code> and <code>prof_attr(4)</code>
<code>/etc/security/tsol/tnidb</code>	Format is extended for IPv6. No conversion required.
<code>/etc/security/tsol/tnrhtp</code>	Format is extended for IPv6. New templates with <code>doi</code> and <code>ip_label</code> changes. See the <code>tnrhtp(4)</code> man page.
<code>/etc/security/tsol/tnrhdb</code>	Format is extended for IPv6. No conversion required.

▼ To Save Profile and User Attribute Information

1. See the **README file** and **`tsolconvert` man page** that you download from the **Trusted Solaris web site for instructions**.

<http://www.sun.com/software/solaris/trustedsolaris>

2. On the web site, click **Technical FAQs**, then click **Transitions Between Environments**.

Backup and conversion *must be completed* on the Trusted Solaris 2.5.1 or Trusted Solaris 7 NIS+ master before the Trusted Solaris 8 4/01 software is installed.

Site Security Policy

Each Trusted Solaris 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 top level management, personnel management, computer system management and administrators, and facilities management. The team should review Trusted Solaris 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 since this policy information has direct bearing on the security of the computer systems.
- Educate users about the Trusted Solaris operating environment and the policy. All users must be familiar with the Trusted Solaris 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 Trusted Solaris system will not be 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 the Operating Environment

The security administrator should design the Trusted Solaris network based on the site's security policy. The security policy dictates configuration decisions regarding such things as:

- How much auditing will be done for all users in the system and for which classes of events
- How much auditing will be done for users in roles and for which classes of events
- How audit data will be managed, archived, and reviewed
- Which labels will be used in the system and whether the `ADMIN_LOW` and `ADMIN_HIGH` labels will be viewable by ordinary users
- Which user clearances will be assigned to individuals
- Which devices (if any) will be allocatable by which normal users
- Which label ranges are defined for machines, printers, and other devices
- Whether the Trusted Solaris system will be used in an evaluated configuration or in an extended configuration.

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 the Trusted Solaris operating environment (the highest label in the user accreditation range) 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 Solaris software should be reported and documented, and the cause should be determined.
- If possible, at least two individuals should administer a Trusted Solaris system. 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 Solaris 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 install user account should be disabled after an authorized security administrator user is established.
- The number of set user ID and set group ID programs should be minimized. Setuid/setgid programs should be employed only in protected subsystems.
- An administrator should regularly verify that normal users have a valid login shell.
- An administrator should regularly verify that normal users have valid user ID values and not system administration ID values.

Physical Security Recommendations

- Restrict access to the Trusted Solaris system. The most secure locations are generally interior rooms that are not on the ground floor.
- Monitor and document access to the Trusted Solaris system.
- 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 not in use.
- Store system backups and archives in a secure location separate from the location of the Trusted Solaris system.
- Restrict physical access to the backup and archival media in the same manner as access to the Trusted Solaris system.

- Install a high-temperature alarm in the computer facility to indicate when the temperature is outside of 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 may 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 all individuals involved with the use of computer equipment and its facilities. Although most actions that violate security are easily resolved by careful users or additional equipment, 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 names.
- Users learn passwords by watching other users when they enter 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

As a trusted administrator, you should become familiar with the standards established by various government agencies. 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. Some publications listed here describe successful attempts to penetrate computer systems around the world and illustrate real threats to computer security. These publications emphasize the importance of computer systems managed by knowledgeable and capable administrators.

U.S. Government Publications

Computer Security Requirements, Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments, DoD, CSC-STD-003-85, 1985.

Department of Defense Password Management Guideline, DoD, CSC-STD-002-85, 1985.

Department of Defense Trusted Computer System Evaluation Criteria (TCSEC) National Computer Security Center, DoD 520.28-STD, 1985.

Graubart, Richard D., J.L. Berger, and John P.L. Woodward, *Compartmented Mode Workstations Evaluation Criteria, Version 1*, DIA DDS-2600-6243-91, Mitre, Bedford, Massachusetts, March 1991.

Personal Computer Security Considerations, National Computer Security Center, NCSC-WA-002-85, 1985.

Technical Rationale behind CSC-STD-003-85 Computer Security Requirements, Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments, DoD, CSC-STD-004-85, 1985.

Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria, National Computer Security Center, NCSC-TG-005 Version 1, 1987.

Woodward, John P.L., *Security Requirements for System High and Compartmented Mode Workstations*, DIA DDS-2600-5502-87, Mitre, Bedford, Massachusetts, November 1987.

UNIX Security Publications

Farrow, Rik, *UNIX System Security*, Addison-Wesley, Reading, MA, 1991.

Garfinkel, Simson, and Gene Spafford, *Practical UNIX Security*, O'Reilly & Associates, Inc., Sebastopol, CA, 1991.

Gregory, Peter, *Solaris Security*, Sun Microsystems Press, September 1999.

Hayes, Frank, "Is Your System Safe?" *UNIXWORLD*, June 1990.

Wood, Patrick H., and Stephen Kochan, *UNIX System Security*, Hayden Books, Indianapolis, IN, 1986.

General Computer Security Publications

Denning, Peter J., *Computers under Attack: Intruders, Worms and Viruses*, ACM Press, Addison-Wesley, Reading, MA, 1990.

Farrow, Rik, "Inside the Internet Worm," *UNIXWORLD*, June 1990.

Hafner, Katie, and John Markroff, *Cyberpunk: Outlaws and Hackers on the Computer Frontier*, Simon & Schuster, New York, NY, 1991.

Levy, Steven, *Hackers: Heroes of the Computer Revolution*, Dell Books, New York, NY, 1984.

McAfee, John, and C. Haynes, *Computer Viruses, Worms, Data Diddlers, Killer Programs, and Other Threats to Your System*, St. Martin's Press, New York, NY, 1989.

Page, Bob, "A Report on the Internet Worm," University of Lowell, Computer Science Department, November 1988.

Russell, Deborah, and G.T. Gangemi, Sr., *Computer Security Basics*, O'Reilly & Associates, Inc., Sebastopol, CA, 1990.

"Special Report: Computer Security and the Internet", *Scientific American*, October 1998. pp 95–117. Contains articles on hackers, firewalls, encryption, digital signatures, and Java, with extensive bibliographies.

Seeley, Donn, "A Tour of the Worm," University of Utah Department of Computer Science, Technical Report, November 1988.

Spafford, Eugene H., "The Internet Worm: Crisis and Aftermath," *Communications of the ACM*, June 1989.

Stoll, Cliff, *The Cuckoo's Egg*, Doubleday, Garden City, NY, 1989.

Thompson, Ken, "Reflections on Trusting Trust," 1983 ACM Turing Award Lecture, *Communications of the ACM*, August 1984.

General UNIX Publications

Bach, Maurice J., *The Design of the UNIX Operating System*, Prentice Hall, Englewood Cliffs, NJ, 1986.

Kobert, Jeannie Johnstone, *Guide To High Availability: Configuring boot/root/swap*, Sun Microsystems Press, September 1999.

Nemeth, Evi, Garth Snyder, and Scott Seebas, *UNIX System Administration Handbook*, Prentice Hall, Englewood Cliffs, NJ, 1989.

Winsor, Janice, *Solaris 7 Reference*, Sun Microsystems Press, September 1999.

Checklists for a Secure Trusted Solaris Environment

The checklists are for planning and for reference. They provide an overall view of what to remember when installing and configuring the systems at your site, and a record of doing so.

Site Summary Checklist

The following checklists summarize what you have done at your site. Where indicated, there are separate worksheets to plan particular site features, such as servers and labels.

Reading List

- Read *Trusted Solaris Administration Overview*.
- Understand site security requirements.
- Read Appendix A.

Checklist Summaries

Labels	See <i>Trusted Solaris Label Administration</i> . For highlights, see “Planning Labels” on page 150.
Network	See “Planning the Network” on page 151.
Auditing	See <i>Trusted Solaris Audit Administration</i> . For highlights, see “Planning Auditing” on page 152.

Systems or Hosts	See “Planning System Configuration” on page 152.
First Users	See “Planning User Security” on page 27 and Table 4–3.
Administrative Roles	See Table 4–1 for password and account locking considerations.
Users, Roles and Rights Profiles	See <i>Trusted Solaris Administrator’s Procedures</i> .
Printers	See <i>Trusted Solaris Administrator’s Procedures</i> and “Planning System Configuration” on page 152.

Planning Labels

Planning labels requires extensive knowledge. *Trusted Solaris Label Administration* describes in detail the modifications required to the `label_encodings` file you choose.

Label visibility exceptions are implemented per user when creating users.

Label visibility exceptions per system can be done but are not recommended. See *Trusted Solaris Label Administration* for why and how.

Note – When localizing a `label_encodings` file, localize the label names only. However, the names `ADMIN_HIGH` and `ADMIN_LOW` *must not* be localized. All labeled hosts that you contact must have label names that match the label names in the Trusted Solaris `label_encodings` file.

Label Decisions

Choose a `label_encodings` file

1. GFI
2. Site-specific
3. Modified Trusted Solaris single-label
4. Modified Trusted Solaris multilabel

Decide Trusted Solaris configuration

- Create multiple user Sensitivity Labels — Yes, default

	<ul style="list-style-type: none"> ■ Hide upgraded names in directories — No, default
Decide label visibility	Visible to each user, default

Planning the Network

The first decision to make is whether to have an open network or a closed network.

Open Network Security Information

If the network is open:

1. Identify accessible domains
2. Identify accessible hosts
3. Identify Trusted Solaris systems that can access to unlabeled systems or domains

Name Service Domain Information

For the NIS or NIS+ domain:

1. Identify the NIS or NIS+ master
2. Identify the NIS or NIS+ slaves/replicas
3. Identify the NIS+ subdomain masters
4. Identify the file servers
5. Identify the audit servers
6. Identify the print servers
7. Identify the mail servers
8. Identify network routers/gateways
9. Identify end user systems
10. Identify other hosts on the network

Labels of Communicating Machines

Identify the labels at which machines can communicate.

- Identify an single-label or limited range hosts in the Trusted Solaris network.
- Determine the label(s) applied to incoming data from unlabeled hosts

Planning Auditing

Planning auditing can require extensive knowledge. *Trusted Solaris Audit Administration* describes in detail how to set up auditing.

Auditing Security Information

Auditing security decisions include:

- Classes of events to audit for success
- Classes of events to audit for failure
- Classes of events to audit for both
- Users/roles with what additional auditing
- Who has access to the audit administration server
- Who has access to the audit servers
- Who has the rights profile for audit file backup
- Who has the rights profile for audit file review

Auditing System Information

Auditing system decisions include:

- Primary and secondary audit partitions for each host
- Size of audit partitions

Planning System Configuration

Required System Information

List the system information for each host in the Trusted Solaris network:

- name
- kernel architecture
- IP address

Security Information for Each Machine

Determine the security information for each host in the Trusted Solaris network:

- root password
- PROM/BIOS security level
- PROM/BIOS password
- Attached peripherals permitted?
- Access to printers
- Access to unlabeled domains

Example Worksheets

The worksheet examples provide you with samples for your systems, devices, and network.

How to Use the Examples

These are examples only. Do *not* use the IP addresses, names, and other details as they are written here.

Root NIS+ Master Installation Program Example

Dialog Box Title	Answer	Comment
Select a language	0	English
Select a locale	0	English
Networked?	Yes	
Host name	eagle	
IP address	192.168.110.1	
DHCP	No	You should choose DHCP only if this system does not have a permanent IP address and instead gets one from a DHCP server that you have already set up.

Dialog Box Title	Answer	Comment
Primary network interface	le0	You are not prompted for this unless the computer has more than one network card.
Name service	None	You will turn the machine into the name service master later.
Subnet?	Yes	If your LAN is part of a larger network, say yes.
Subnet mask	255.255.255.0	Check that the default is the appropriate mask for your site.
Time zone	Geographical, US Pacific	A time zone map is provided on the WWW.
Date and Time		The default provided is usually the correct clock time.
The answers to the above questions are System ID Information (sysidinfo). When installing over a network, system information is automatically given to the installation program, reducing the installer's interaction with the program.		
Select Geographic Region	North America	Select the regions for which support should be installed.
Install	Install	Upgrade is not supported for this release.
System type	Standalone	
Select Software	Entire software group	For a server, choose Developer or larger.
	Solaris 64-bit support	Choose to enable 64-bit support or not. If you chose IPv6, above, you must choose 64.
Customize?	Yes No	Customizing a software group often results in software dependencies; system administration knowledge is required to fix dependencies.
Select Disks	c0t0d0, c0t1d0, c0t3d0, c0t5d0	See "Root NIS+ Master Disk Partitioning Example" on page 157 for the details of the example.
Preserve Data?	Preserve Continue	Probably Continue.
Auto Layout	Continue	Auto Layout displays the minimum disk amounts required per file system.
File systems to auto-layout	/, /usr, /var	See "Root NIS+ Master Disk Partitioning Example" on page 157
Customize File System and Disk Layout	Customize	Customizing requires advanced system administration skills.

Dialog Box Title	Answer	Comment
Customize Disks	OK Continue	See “Root NIS+ Master Disk Partitioning Example” on page 157
Mount remote file systems	No	Mounting in the Trusted Solaris environment is secure. Remote file systems are mounted after their security attributes are known to this machine.
Begin installation	Begin	Read the disk layout and confirm its accuracy.
Auto Reboot	Auto Manual	
The following prompts are on a plain screen, not in dialog boxes.		
Root password	List it elsewhere	System security requires a root password.
Automatic power-saving shutdown	y n ?	To recover from power shutdown, press the power key at keyboard upper right.
Confirm	Yes No	
The Web Launcher starts in Command Line Mode.		
Continue install: [1] Media [2] Network [3] Skip.	1	The CD drawer opens. Remove the CD.
Insert the CD for Solaris Software 2.	Insert the second CD and press the Return key.	
The screen may be overwritten with messages. Package installation is displayed in 25% increments: -1%---25%---50%---75%---100%		
Enter 1 to review the log, or 2 to end.	2	Press the Return key.
The CD drawer opens. Remove the CD. Press the Return key to reboot the system.		

Root NIS+ Master Disk Partitioning Example

Host Name: eagle

Disk	Slice	Mount point	Size	Disk	Slice	Mount point	Size
c0t0d0	s0	/	80	c0t1d0	s0	/export/Answerbooks	600
	s1	swap	180		s1		
	s2	entire disk	1034		s2	entire disk	1570
	s3	/var	224		s3		
	s4				s4		

Disk	Slice	Mount point	Size	Disk	Slice	Mount point	Size
	s5				s5		
	s6	/usr	520		s6		410
	s7	/export	10		s7	/export/tools	1380

Disk	Slice	Mount point	Size	Disk	Slice	Mount point	Size
c0t3d0	s0			c0t5d0	s0		
	s1				s1		
	s2	entire disk	2028		s2	entire disk	1980
	s3	/etc/security/audit/eagle	1014		s3	/swapfile	600
	s4				s4		
	s5				s5		
	s6				s6		
	s7	/etc/security/audit/eagle.1	1014		s7	/opt	1380

Services Provided by Servers Example

Use	Name	IP address	Shared File Systems	Security Information
NIS+ servers				
Root NIS+ master	eagle	192.168.110.1	/etc/security/audit/eagle	
NIS+ replica	willet	192.168.110.3	/etc/security/audit/willet	nosuid, nodev, [high]
			/etc/security/audit/willet.1	nosuid, nodev, [high]
Network routers				
	willet-118 le1	192.168.118.25		
	stilt-223 ie1	192.168.223.20		
	heron-119 le1	192.168.119.26		
File Servers (Share file systems for mounting by end user systems)				
for home directories	nest	192.168.118.2	/export/home	
for AnswerBooks	worker	192.168.118.7	/usr/all/books	

Use	Name	IP address	Shared File Systems	Security Information
for CodeMgr	ada	192.168.110.5	/opt/utis/cmgr	
for Man Pages	ada	192.168.110.5	/opt/utis/man	
for Utilities	ada	192.168.118.5	/opt/utis/	
for Applications	worker	192.168.118.7	/usr/all/apps	
Audit Servers (Share all audit file systems for mounting by audit administration server and user systems)				
	willet		/etc/security/audit/willet.1	nosuid, nodev, [high]
	egret		.../egret.1,2,3,4	nosuid, nodev, [high]
	stilt		.../stilt.1,2,3	nosuid, nodev, [high]
	tern		.../tern.1,2,3,4	nosuid, nodev, [high]
Audit Administration Server (Shares no file systems; mounts all audit file systems)				
	audacious	192.168.110.7	None	nosuid, nodev, [high]
Install Server (Shares file system that contains Trusted Solaris image)				
	penguin			
Boot Server (One per NIS+ subdomain)				
	penguin			
Mail Server (Share /var/mail file system)				
	willet			
Print Servers				
	cirrus			
	cumulus			

Audit Server Installation Program Example

Note – You will not be prompted for information that you have provided in NIS+ or in the *boot_server:/etc/bootparams* file (during a Custom JumpStart install).

Dialog Box Title	Answer	Comment
Select a language	0	English

Dialog Box Title	Answer	Comment
Select a locale	0	English
Networked?	Yes	
Host name	willett	
IP address	192.168.110.3	
DHCP	No	You should choose DHCP only if this system does not have a permanent IP address and instead gets one from a DHCP server that you have already set up.
Primary network interface	le0	You are not prompted for this unless the computer has more than one network card.
Name service	NIS+ NIS None	Choose the name service if the master is up and running.
Subnet?	Yes	If your LAN is part of a larger network, say yes.
Subnet mask	255.255.255.0	Check that the default is the appropriate mask for your site.
Time zone	Geographical, US Pacific	A time zone map is provided on the WWW.
Date and Time		The default provided is usually the correct clock time.
The answers to the above questions are System ID Information (sysidinfo). When installing over a network, system information is automatically given to the installation program, reducing the installer's interaction with the program.		
Select Geographic Region	North America	Select the regions for which support should be installed.
Install	Install	Upgrade is not supported for this release.
System type	Standalone	
Select Software	Entire software group	For a server, choose Developer or larger.
	Solaris 64-bit support	Choose to enable 64-bit support or not. If you chose IPv6, above, you must choose 64.
Customize?	Yes No	Customizing a software group often results in software dependencies; system administration knowledge is required to fix dependencies.
Select Disks	c0t0d0, c0t1d0, c0t3d0, c0t5d0	See "Audit Server Disk Partitioning Example" on page 162 for the details of the example.

Dialog Box Title	Answer	Comment
Preserve Data?	Preserve Continue	Probably Continue.
Auto Layout	Continue	Auto Layout displays the minimum disk amounts required per file system.
File systems to auto-layout	/, /usr, /var	See “Root NIS+ Master Disk Partitioning Example” on page 157
Customize File System and Disk Layout	Customize	Customizing requires advanced system administration skills.
Customize Disks	OK Continue	See “Audit Server Disk Partitioning Example” on page 162 for the details of the example.
Mount remote file systems	No	Mounting in the Trusted Solaris environment is secure. Remote file systems are mounted after their security attributes are known to this machine.
Begin installation	Begin	Read the disk layout and confirm its accuracy.
Auto Reboot	Auto Manual	
The following prompts are on a plain screen, not in dialog boxes.		
Root password	<i>List it elsewhere</i>	System security requires a root password.
Automatic power-saving shutdown	y n ?	To recover from power shutdown, press the power key at keyboard upper right.
Confirm	Yes No	
The Web Launcher starts in Command Line Mode.		
Continue install: [1] Media [2] Network [3] Skip.	1	The CD drawer opens. Remove the CD.
Insert the CD for Solaris Software 2. Insert the second CD and press the Return key.		
The screen may be overwritten with messages. Package installation is displayed in 25% increments: -1%---25%---50%---75%---100%		
Enter 1 to review the log, or 2 to end.	2	Press the Return key.
The CD drawer opens. Remove the CD. Press the Return key to reboot the system.		

Audit Server Disk Partitioning Example

Note – This system will be configured as a NIS+ client of the NIS+ root master.

Host Name: willet

Disk	Slice	Mount point	Size	Disk	Slice	Mount point	Size
c0t0d0	s0	/	75	c0t1d0	s0		
	s1	swap	160		s1		
	s2	entire disk	1034		s2	entire disk	1980
	s3				s3	/etc/security/audit/willet.1	990
	s4	/var	200		s4		
	s5				s5		
	s6	/usr	350		s6		
	s7	/export/home	250		s7	/etc/security/audit/willet.2	990

Disk	Slice	Mount point	Size	Disk	Slice	Mount point	Size
c0t3d0	s0			c0t5d0	s0		
	s1				s1		
	s2	entire disk	1980		s2	entire disk	1980
	s3	/etc/security/audit/willet.3	990		s3	/etc/security/audit/willet	990
	s4				s4		
	s5				s5		
	s6				s6		
	s7	/etc/security/audit/willet.4	990		s7	/etc/security/audit/willet.5	990

Audit Server Configuration Worksheet

System Administrator Information		Security Officer Information	
Name	willet		root password

System Administrator Information		Security Officer Information	
IP address	192.168.110.3	PROM mode	full
Ethernet address	8:0:20:4c:7e:2f	PROM password	
Sun architecture	sun4m		
Network interfaces	le0		
Network router	willet-118 le1 (192.168.118.25)		
Mount Points (For local file systems)		Security Attributes	
	/		
	/usr		
	/var		
	/export/home		nosuid
for NIS+ utils	/opt/nis/		
Mount Points (For remote file systems)			
for Sol AnswerBks	/usr/AB/Sol8.1/		
for TS AnswerBks	/usr/AB/TS8/		
for ManPages	/usr/share/man		
for CodeMgr	/opt/prog/Code		
for Utilities	/opt/dist/Util		
for Applications	/opt/dist/App		
Audit Mount Points			
Primary	/etc/security/audit/tern.1		nosuid, nodev, [high]
Secondary	/etc/security/audit/egret.1		nosuid, nodev, [high]
Local	/etc/security/audit/willet		nosuid, nodev, [high]
Audit File Systems			
Primary	tern:/etc/security/audit/tern.1/files		
Secondary	egret:/etc/security/audit/egret.1/files		
Local	/etc/security/audit/willet/files		
Mail Server	eagle		

System Administrator Information		Security Officer Information
Attached Devices	CDROM (sd6)	only usable by those whose profile includes the <code>device_allocate</code> command and the <code>solaris.device.allocate</code> authorization
	tape drive (st4)	
Remote Printers	cirrus	Administrator printer [admin_high] only
	cumulus	

Glossary

access control list	One type of discretionary access control based on a list of entries that the owner can specify for a file or directory. An access control list (ACL) can restrict or permit access to any number of individuals and groups, allowing finer-grained control than provided by the standard UNIX permission bits.
accreditation range	A set of sensitivity labels that are approved for a class of users or resources. See also system accreditation range and user accreditation range.
ACL	See access control list.
accreditation range	A set of valid labels. See accreditation range and user accreditation range for more about the two types of accreditation ranges in the Trusted Solaris environment.
administrative role	A <i>role</i> that in the Trusted Solaris environment gives required authorizations, privileged commands, and the Trusted Path security attribute to allow the role to perform part of Solaris superuser's capabilities, such as backup or auditing.
allocation	A device to which access is controlled in the Trusted Solaris environment by making the device allocatable to a single user at a time. Allocatable devices include tape drives, floppy drives, audio devices, and CDROM devices. See device allocation.
allowed privilege set	The allowed set of privileges limits which privileges a process can use. A process that runs a program that has a forced privilege set limits that program to the forced privileges that are also in the process' allowed privilege set.
authorization	A right granted to a user or role to perform an action that would otherwise not be allowed by the Trusted Solaris security policy. Authorizations are granted in rights profiles. Certain commands require the user to have certain authorizations to succeed. Similar to the use of privilege on programs.

application search path	In CDE the search path used by the system to find applications and certain configuration information. The application search path is controlled by a trusted role.
AutoClient system	A system type that caches all of its needed system software from an OS server. Because it contains no permanent data, an AutoClient is a field replaceable unit (FRU). It requires a small local disk for swapping and for caching its individual root (/) and /usr file systems from an OS server. The Trusted Solaris operating environment does not support autoclients.
begin script	A user-defined Bourne shell script, specified within the rules file, that performs tasks before the Trusted Solaris software is installed on the system. Begin scripts can be used only with custom JumpStart installations.
bootparams file	A file that is consulted when a system boots. In the Trusted Solaris operating environment, the bootparams file contains a keyword=value entry that points the boot server to the Trusted Solaris label configuration for the system. A system can have a local bootparams file (/etc/bootparams), or it can use the bootparams NIS+ table. See bootparams(4).
boot server	A server that provides boot services to hosts on the same subnet. A boot server is required if you plan to push Trusted Solaris information from a central location to every host in the network. If the install server is on a different subnet than the hosts that need to install the Trusted Solaris software, you must create a boot server for that subnet.
CDE	See Common Desktop Environment.
clearance	The upper bound of the set of labels at which a user may work, whose lower bound is the minimum label assigned by the security administrator. There are two types of clearance, the session clearance and the user clearance.
client	A system connected to a network.
closed network	A network of Trusted Solaris systems that is cut off from any non-Trusted Solaris host. The cutoff can be physical, where there is no wire that extends past the Trusted Solaris network. The cutoff can be in the software, where the Trusted Solaris hosts recognize only Trusted Solaris hosts. Data entry from outside the network is restricted to peripherals attached to Trusted Solaris systems. Contrast with open network.
cluster	A logical grouping of software packages. The Trusted Solaris software is divided into four main software groups, which are each composed of clusters and packages.
CMW label	Consists of the string ADMIN_LOW followed by a sensitivity label in brackets, in the form: ADMIN_LOW [SENSITIVITY LABEL].

Common Desktop Environment	The required windowing environment for administering the Trusted Solaris software.
.copy_files	An optional setup file in a multilabel environment. The file contains the names of startup files, such as <code>.cshrc</code> or <code>.netscape</code> , that the user environment or user applications require in order for the environment or application to behave well. The files referenced in <code>.copy_files</code> are then <i>copied</i> to the user's home directory at other labels, when those directories are created. See also <code>.link_files</code> .
core	A software group that contains the minimum software required to boot and run the Solaris operating environment on a system. It includes some networking software and the drivers required to run the OpenWindows environment; it does not include the windowing software. The Trusted Solaris installation program does not offer a core software group, since the Common Desktop Environment is the required administration environment.
core file	A file that contains a picture of the state of a system when it crashed. Also called a core dump.
custom JumpStart installation	A type of installation in which the Trusted Solaris software is automatically installed on a system based on a customized profile. You can customize profiles for different types of users.
DAC	See discretionary access control.
derived profile	A profile that is dynamically created by a begin script during a custom JumpStart installation.
device	Devices include printers, computers, tape drives, floppy drives, audio devices, and internal pseudo terminal devices. Devices are subject to the read equal write equal MAC policy.
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 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.
developer system support	A software group that contains the End User System Support software group plus the libraries, include files, man pages, and programming tools for developing software.
discretionary access control	The type of access granted or denied by the owner of a file or directory at the discretion of the owner. The Trusted Solaris environment provides two kinds of discretionary access controls (DAC): permission bits and access control list.

disk configuration file	A file that represents a structure of a disk (for example, bytes/sector, flags, slices). Disk configuration files enable you to use <code>pfinstall</code> from a single system to test profiles on different sized disks.
domain	A part of the Internet naming hierarchy. It represents a group of systems on a local network that share administrative files.
domain address	IP address whose last number is 0.
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: <code>tundra.mpk.ca.us</code>). As you read a domain name from left to right, the component names identify more general (and usually remote) areas of administrative authority.
end user system support	A software group that contains the core software group plus the recommended software for an end user, including OpenWindows and DeskSet software.
entire distribution	A software group that contains the entire Trusted Solaris release.
entire distribution plus OEM support	A software group contains the entire Trusted Solaris release, plus additional hardware support for OEMs. This software group is recommended when installing Trusted Solaris software on servers.
EISA	Extended Industry Standard Architecture. A type of bus on x86 systems. EISA bus standards are “smarter” than ISA bus systems, and attached devices can be automatically detected when they have been configured via the “EISA configurator” program supplied with the system. See ISA.
/etc	A directory that contains critical system configuration files and maintenance commands.
evaluated configuration	<p>One or more Trusted Solaris systems which 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 and the evaluating and certifying body is the NSA. The Trusted Solaris 8 4/01 operating environment 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 which provide functionality similar to the TCSEC C2 and B1 levels, with some additional functionality.</p> <p>One or more Trusted Solaris systems which are running in a configuration that has been certified as meeting specific criteria by a certification authority. The Trusted Solaris 8 4/01 operating environment will be certified to the Common Criteria v2.1 [published in 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.</p>

standard obsolete through level B1+. A mutual recognition agreement for CCv2 has been signed by the United States, the United Kingdom, Canada, the Netherlands, Germany, and France.

The Trusted Solaris 8 4/01 configuration target provides functionality similar to the TCSEC C2 and B1 levels, with some additional functionality.

execution profile	Renamed to rights profiles in the Solaris 8 release.
/export	A file system on an OS server that is shared with other systems on a network. For example, the <code>/export</code> file system can contain the home directories for users on the network.
fdisk partition	A logical partition of a disk drive dedicated to a particular operating system on x86 systems. During the Solaris installation program, you must set up at least one Solaris fdisk partition on an x86 system. x86 systems are designed to support up to four different operating systems on each drive; each operating system must reside on a unique fdisk partition.
file server	A server that provides the software and file storage for systems on a network.
file privilege set	These sets are the allowed and forced privileges specified for use by executable files (programs). The allowed set limits which privileges a process can use, whether the privileges are forced on the executable file or inherited (see inheritable privileges). Any privileges in the forced privilege set are available to any process that invokes the program, as long as they are also in the allowed set.
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.
finish script	A user-defined Bourne shell script, specified within the rules file, that performs tasks after the Trusted Solaris software is installed on the system, but before the system reboots. Finish scripts can be used only with JumpStart installations.
forced privilege set	The forced set of privileges are those placed on a file by the security administrator. Any privileges in the forced privilege set are available to any process that invokes the program, as long as they are also in the allowed privilege set.
GFI	Government Furnished Information. In this manual, it refers to a U.S. government-provided <code>label_encodings</code> file. In order to use a GFI with Trusted Solaris software, you must add the Sun-specific LOCAL DEFINITIONS section to the end of the GFI. Trusted Solaris Label Administration explains the procedure in detail.

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, this means within any 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.
IA	Intel Architecture.
inheritable privilege	The privileges that a process can pass to a program across an <code>execve()</code> without their being affected by the new program's forced or allowed privilege sets. When a new program is executed by a process, the inheritable set of the process is set to be equal to the inheritable set of the old program. The inheritable set is not affected by the forced or allowed privileges on the currently executing program, which allows privileges to be passed from programs that cannot use them to programs that can.
initial label	The minimum label assigned to a user or role, and the label of the user's initial workspace. It is the lowest label at which the user or role can work.
initial installation option	An option presented during the Trusted Solaris installation program that overwrites the disk(s) with the new version of Trusted Solaris software. The initial installation option is the only installation option supported in the Trusted Solaris release.
install server	A server that provides the Trusted Solaris installation image for other systems on a network to boot and install from (also known as a <i>media server</i>). The Trusted Solaris installation image can reside on the install server's CDROM drive or hard disk.
install team	A team of at least two people who together oversee the installation of a Trusted Solaris system. One team member is responsible for security decisions, and the other for system administration decisions.
interactive installation	A type of installation where you have full hands-on interaction with the Trusted Solaris installation program to install the Trusted Solaris software on a system.
IP address	<p>Internet protocol address. A unique number that identifies a networked system so it can communicate via Internet protocols. It 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.</p> <p>IP addresses are logically divided into two parts: the network (similar to a telephone area code), and the system on the network (similar to a phone number).</p>

ISA	Industry Standard Architecture. A type of bus found in x86 systems. ISA bus systems are “dumb” and provide no mechanism the system can use to detect and configure devices automatically. See EISA.
JumpStart directory	When using a diskette for custom JumpStart installations, the JumpStart directory is the root directory on the diskette that contains all the essential custom JumpStart files. When using a server for custom JumpStart installations, the JumpStart directory is a directory on the server that contains all the essential custom JumpStart files.
JumpStart installation	A type of installation in which the Solaris software is automatically installed on a system by using factory-installed JumpStart software. The Trusted Solaris release does not offer this option; all JumpStart installations in the Trusted Solaris installation program are custom JumpStart installations.
kernel architecture	See platform group.
label	A security identifier assigned to a file or directory based on the level at which the information being stored in that file or directory should be protected. Depending on how the security administrator has configured the user, a user may see the complete CMW label, only the sensitivity label portion, only the ADMIN_LOW portion, or no labels at all. See label_encodings file.
label configuration	A Trusted Solaris installation choice of: single- or multilabel sensitivity labels; if multilabel, hide or show upgraded file names. Unless circumstances are unusual, label configuration should be identical on all systems in the Trusted Solaris domain.
labeled host	A labeled host sends labeled network packets, such as RIPS0, CIPS0, and TSIX(RE1.1) packets. All Trusted Solaris hosts are labeled hosts.
label_encodings file	The file where the complete CMW label is defined, as are label view, admin_low and admin_high strings, default label visibility, and all other aspects of labels.
label range	A set of sensitivity labels assigned to commands, file systems, and allocatable devices, specified by designating a maximum label and a minimum label. For commands, the minimum and maximum labels limit the sensitivity labels at which the command may be executed. For file systems, the minimum and maximum labels limit the sensitivity labels at which information may be stored on each file system. Trusted Solaris environments have multilabel file systems configured with a label range from the lowest sensitivity label to the highest sensitivity label. Remote hosts that do not recognize labels are assigned a single sensitivity label, along with any other hosts that the security administrator wishes to restrict to a single label; labels limit the sensitivity labels at which devices may be allocated and restrict the sensitivity labels at which information can be stored or processed using the device.

label view flags	Label view flags control the translation and display of the internal ADMIN_LOW and ADMIN_HIGH labels. A value of External specifies that the actual label ADMIN_LOW displays as the lowest label name in the user accreditation range specified in the label_encodings file, and that the actual label ADMIN_HIGH displays as the highest label name in the user accreditation range. A value of Internal specifies that the ADMIN_LOW and ADMIN_HIGH labels are translated to the Admin Low Name and Admin High Name strings specified in the label_encodings file.
.link_files	An optional setup file in a multilabel environment. The file contains the names of startup files, such as .cshrc or .netscape, that the user environment or user applications require in order for the environment or application to behave well. The files referenced in .link_files are then <i>linked</i> to the user's home directory at other labels, when those directories are created. See also .copy_files.
locale	A specific language associated with a region or territory.
MAC	See mandatory access control.
mandatory access control	Access control 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 — write up, read down (WURD) — applies when a process at one sensitivity label attempts to read or write to a file at another sensitivity label. The MAC rule — write equal, read down — applies when a process at one sensitivity label attempts to write to a directory at another sensitivity label. The MAC rule — read equal, write equal — applies when a process at one sensitivity label attempts to write to a device at another sensitivity label.
MCA	Micro Channel Architecture. A type of bus on IA systems. The MCA bus provides fast data transfer within the computer, and attached devices can be automatically detected when they have been configured using the reference disk provided by the manufacturer. The MCA bus is not compatible with devices for other buses.
media server	See install server.
minimum label	The lower bound of a user's sensitivity labels and the lower bound of all users' sensitivity labels. The minimum label set by the security administrator when specifying a user's security attributes is the sensitivity label of the first workspace that comes up after the user's first login. The sensitivity label specified in the minimum label field by the security administrator in the label_encodings file sets the lower bound for all users.
MLD	See multilevel directory.
mount	The process of making a remote or local file system accessible by executing the mount command. To mount a file system, you need a

	mount point on the local system and the name of the file system to be mounted (for example, <code>/usr</code>).
mount point	A directory on a system where you can mount a file system that exists on the local or a remote system.
multilevel directory	A directory in which information at differing sensitivity label is maintained in separate subdirectories called single-level directories (SLDs), while appearing to most interfaces to be a single directory under a single name. In the Trusted Solaris environment, directories that are used by multiple standard applications to store files at varying labels, such as the <code>/tmp</code> directory, <code>/var/spool/mail</code> , and users' <code>\$HOME</code> directories, are set up to be MLDs. A user working in an MLD sees only files at the sensitivity label of the user's process.
name server	Also called <i>name service master</i> . A server that provides a name service to systems on a network.
name service	A distributed network database that contains key system information about all the systems on a network, so the systems can communicate with each other. With a name service, the system information can be maintained, managed, and accessed on a network-wide basis. Sun supports the following name services: NIS (formerly YP) and NIS+. Without a name service, each system has to maintain its own copy of the system information (in the local <code>/etc</code> files).
network installation	A way to install software over the network—from a system with a CDROM drive to a system without a CDROM drive. Network installations require a name server and an install server.
networked systems	A group of systems (called hosts) connected through hardware and software, so they can communicate and share information; referred to as a local area network (LAN). One or more servers are usually needed when systems are networked.
NIS+	Network Information Service, Plus. The name service for a Trusted Solaris network. NIS+ provides automatic information updating and adds security features such as authorization and authentication.
NIS+ master	See NIS+ root master.
NIS+ root master	The host that contains the master tables for a NIS+ network. Also called a root master or a NIS+ master.
non-networked systems	Computers that are not connected to a network or do not rely on other hosts.
open network	A network of Trusted Solaris systems that is connected physically to other networks and that uses Trusted Solaris software to communicate with non-Trusted Solaris systems. Contrast with closed network.
/opt	A file system that contains the mount points for third-party and unbundled software.

OS server	A system that provides services to systems on a 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, it is described as being <i>outside the evaluated configuration</i> .
package	A functional grouping of files and directories that form a software application. The Trusted Solaris software is divided into four main software groups, which are each composed of clusters and <i>packages</i> .
partition	A disk partition is a slice of the disk.
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 all members of the group specified for the file or directory; and one set for all others.
platform group	The output of the <code>uname -m</code> command. A vendor-defined grouping of hardware platforms for the purpose of distributing specific software. Examples of valid platform names are <code>i86pc</code> , <code>sun4c</code> . Often called kernel architecture.
platform name	The output of the <code>uname -i</code> command. For example, the platform name for the SPARCstation IPX is <code>SUNW, Sun_4_50</code> .
primary administrator	The person 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	A right granted to a process executing a command that allows the command or one or more of its options to bypass some aspect of security policy. A privilege is only granted by a site's security administrator after the command itself or the person using it has been judged to be able to use that privilege in a trustworthy manner.
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 available to the command being executed, the process clearance (which is set to be the same as the session clearance) and the sensitivity label of the current workspace.
profile	A text file used as a template by the custom JumpStart installation software. It defines how to install the Trusted Solaris software on a

	system (for example, initial installation option, system type, disk partitioning, software group), and it is named in the rules file.
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 system that is not part of the Trusted Solaris NIS+ domain. A remote host can be an unlabeled host or a labeled host.
rights profile	Previously, execution profiles. A bundling mechanism for commands and CDE actions and for the security attributes assigned to the commands and CDE actions. Rights profiles allow Trusted 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. Roles are limited to a particular set of commands and CDE actions. See administrative role.
/ (root)	The file system at the top of the hierarchical file tree on a system. The root directory contains the directories and files critical for system operation, such as the kernel, device drivers, and the programs used to start (boot) a system.
root master	See NIS+ root master.
rule	A series of values that assigns one or more system attributes to a profile.
rules file	A text file used to create the rules.ok file. The rules file is a look-up table consisting of one or more rules that define matches between system attributes and profiles.
rules.ok file	A generated version of the rules file. It is required by the custom JumpStart installation software to match a system to a profile. You use the check script to create the rules.ok file.
security administrator	In an organization where sensitive information must be protected, the person or persons who define and enforce the site's security policy and who are cleared to access all information being processed at the site. In the Trusted Solaris software environment, an administrative role that is assigned to one or more individuals who have the proper clearance and whose task is to 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 used in enforcing the Trusted Solaris security policy. Various sets of security attributes, both in the base Solaris and the

	Trusted Solaris environments, are assigned to processes, users, files, directories, hosts on the trusted network, allocatable devices, and other entities.
security policy	In the Trusted Solaris environment, the set of DAC, MAC, and labeling rules that define how information may 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 assigned to a file or directory or process, which is used to limit access based on the security level of the data contained.
single-level directory	A directory within an MLD containing files at only a single sensitivity label. When a user working at a particular sensitivity label changes into an MLD, the user's working directory actually changes to a single-label directory within the MLD, whose sensitivity label is the same as the sensitivity label at which the user is working.
SLD	See single-level directory.
slice	An area on a disk composed of a single range of contiguous blocks. A slice is a physical subset of a disk (except for slice 2, which by convention represents the entire disk). A disk can be divided into eight slices. Before you can create a file system on a disk, you must format it into slices.
software group	A logical grouping of the Solaris software (clusters and packages). During a Solaris installation, you can install one of the following software groups: core, end user system software, developer system support, or entire distribution. In the Trusted Solaris environment, core and end user software are identical.
Solaris Management Console	A Java-based administrative action for Solaris and Trusted Solaris systems. Located in the Application Manager, it contains toolboxes of administrative programs. Most system, network, and user administration is done using the Console toolboxes.
standalone system	A system that has its own / (root) file system, swap space, and /usr file system, which reside on its local disk(s); it does not require boot or software services from an OS server. A standalone system can be connected to a network, but it does not have to be.
subnet	A working scheme that divides a single logical network into smaller physical networks to simplify routing.
subnet mask	A bit mask, which is 32 bits long, used to determine important network or system information from an IP address.
swap space	Disk space used for virtual memory storage when the system does not have enough system memory to handle current processes. Also known as the /swap or swap file system.

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 (well-formed) labels created according to the rules defined by each site's security administrator in the <code>label_encodings</code> file, plus the two administrative labels that are used in every Trusted Solaris environment, <code>ADMIN_LOW</code> and <code>ADMIN_HIGH</code> .
system administrator	In the Trusted Solaris environment, the trusted role assigned to the user or users responsible for performing standard system management tasks such as setting up the non-security-relevant portions of user accounts. In contrast, see security administrator.
system type	One of several different ways a system can be set up to run the Trusted Solaris software. Valid system types are: standalone system and OS server.
time zone	Any of the 24 longitudinal divisions of the earth's surface for which a standard time is kept.
tnrhdb database	The Trusted Network Remote Host DataBase, accessible either as a file in <code>/etc/security/tsol/tnrhdb</code> or as a name service map or table.
tnrhtp database	The Trusted Network Remote Host TemPlate, accessible either as a file in <code>/etc/security/tsol/tnrhtp</code> , or as a name service map or table.
toolbox	A collection of programs in the Solaris Management Console. In the Trusted Solaris environment, administrators are presented with a selection of toolboxes, one for every name service (Files, NIS+, and NIS). Each toolbox has programs usable in the scope of the toolbox. For example, the Interface Manager, which handles the machine's <code>tnidb</code> database, exists only in the Files toolbox, since its scope is always local. The User Accounts program exists in all toolboxes, since an administrator can choose to create a local user (Files), as well as one that can log in to any machine in the name service (NIS+ or NIS toolboxes).
Trusted Network databases	<code>tnrhtp</code> , the Trusted Network Remote Host TemPlate and <code>tnrhdb</code> , the Trusted Network Remote Host DataBase together define the remote hosts that a Trusted Solaris domain can communicate with.
trusted role	See administrative role.
Trusted Solaris installation program	(1) A menu-driven, interactive program that enables you to set up a system and install the Trusted Solaris software on it. (2) Any part of the software that is used to install the Trusted Solaris software on a system.
trusted stripe	A region that cannot be spoofed along the bottom of the screen, which by default provides the following as 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.
prof_attr and exec_attr databases	The profiles attributes database, accessible either as files in <code>/etc/security/prof_attr</code> and <code>/etc/security/exec_attr</code> , or as NIS+ tables. After configuration, it contains rights profiles provided by the Trusted Solaris software.
user_attr database	The User Attributes database, accessible either as a file in <code>/etc/security/user_attr</code> or as a NIS+ table. After configuration, it contains <i>roles</i> provided by the Trusted Solaris software.
upgrade option	An option presented during the Solaris installation program. The upgrade procedure merges the new version of Solaris with existing files on your disk(s), and it saves as many local modifications as possible since the last time Solaris was installed. The upgrade option is not available with the Trusted Solaris 7 release.
unlabeled host	A system that sends unlabeled network packets, such as one running the Solaris 8 operating environment.
user accreditation range	The set of all possible labels at which any normal user may work on the system, as defined by each site's security administrator. The rules for well-formed labels that define the system accreditation range are additionally restricted by the values specified in the ACCREDITATION RANGE section of the site's <code>label_encodings(4)</code> 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 one particular user may work at any time. The user may decide to accept or further restrict that clearance during any particular login session, when setting the session clearance after log in.
/usr	A file system on a standalone system or server that contains many of the standard UNIX programs. Sharing a large file system with a server rather than maintaining a local copy minimizes the overall disk space required to install and run the Trusted Solaris software on a system.
/var	A file system or directory (on standalone systems) containing system files that are likely to change or grow over the life of the system. These include system logs, <code>vi</code> files, mail files, and <code>uucp</code> files.
Volume Management	A program that provides a mechanism to administer and obtain access to the data on CDROMs and diskettes.

Index

A

- accounts
 - creating roles, 64, 87
 - creating the first users, 64, 66, 87
 - planning, 27
- Add to NIS+ Administrative Group action, 88, 103
- add_install_client command
 - custom JumpStart example, 120
 - network installation, 113
- add_to_install_server command
 - network installation, 113
- Admin Editor
 - invoking administrative action, 129, 132
 - running scripts, 132
 - using to create file, 131
- admin group
 - adding IMAP server, 103
- administrative actions
 - Add to NIS+ Administrative Group, 88, 103
 - Check Encodings, 55
 - Device Allocation, 54
 - in System_Admin folder, 55, 131
 - using, 132
- administrative roles
 - administering NIS+, 88
 - creating, 64, 87
 - responsibilities, 32
 - verifying, 69, 88
- administrative scripts
 - running as a role, 115
 - running from Admin Editor, 132

- administrative scripts (*continued*)
 - running in profile shell, 116
- allocate floppy
 - basic procedure, 54
 - during copying, 135
 - during network installation, 114
- Application Manager
 - opening, 129
 - System_Admin folder, 129
- auditing
 - checklist, 152
 - name service client setup, 105
 - NIS+ root master setup, 89
 - no name service setup, 70
 - planning, 30

B

- backup
 - before installation, 32
 - Trusted Solaris database data, 138
- boot information
 - copying during custom JumpStart, 120
- booting
 - from CD-ROM, 43
 - over network, 47
- bootparams file
 - enabling JumpStart directory access, 114

C

- CDE sessions
 - ending, 128
 - starting the computer, 129
- Check Encodings action
 - in System_Admin folder, 55
- checklists for administrators, 149
- computers
 - booting from CD-ROM, 43
 - booting over network, 47
 - protecting, 53, 95
 - screen-locking, 128
 - shutting down, 43
 - starting, 129
- Computers and Networks
 - adding known hosts, 61
 - adding required hosts to the system, 77
 - modifying tnrdhdb, 62, 78
 - modifying tnrdhdp, 61, 78
- configuration
 - headless systems, 121
- configuration files
 - collecting for name service, 80
 - copying, 135
 - copying for distribution, 90
 - creating directory, 90
- copying
 - disk configuration file to JumpStart directory, 118
- cp command
 - in Custom JumpStart, 114
- custom JumpStart installation
 - examples, 119, 120
 - JumpStart directory, 119
 - finish scripts, 117
 - rules file editing, 119
- custom rights profiles
 - verifying, 137

D

- databases
 - collecting for name service, 80
 - converting to new format, 138
- deallocate floppy
 - basic procedure, 56

- deallocate floppy (*continued*)
 - during JumpStart installation, 114
- defaulttrouter
 - setting, 59, 75
- Device Allocation action
 - using, 54, 56
- dfstab file, 119
- DIR variable, 82
- directories
 - for client configuration files, 90
 - for name service setup, 80
 - for network installation, 110, 111
 - JumpStart, 119
 - adding files, 116
 - copying disk configuration files, 118
 - sharing, 119
 - mounting, 71, 91
 - sharing, 70, 90
- disk configuration files
 - copying to JumpStart directory, 118
- diskettes
 - copying files to and from, 135
 - formatting, 114
 - mounting, 114
- disks
 - configuration files, 117
 - partitioning examples, 157, 162
 - partitioning suggestions, 42
- DNS
 - setup on name service client, 102
 - setup on no name service, 63, 85

E

- /etc/dfs/dfstab file, 119
- /etc/hosts file, 61, 77
- /etc/nsswitch.conf file, 102
- /etc/resolv.conf file, 63, 85, 102
- /etc/shadow file, 117
- exec_attr database
 - converting from tsolprof format, 41
- execution profiles
 - updating, 136

F

- fallback mechanism
 - for remote hosts, 62, 63, 78, 79
- fdformat command, 114
- fdisk command, 118
- files
 - collecting for name service, 80
 - copying from floppy, 135
 - copying to diskette, 135
 - creating with Admin Editor, 131
 - disk configuration, 117
 - distributing to clients, 90
 - label encodings in a finish script, 117
- files and file systems
 - mounting, 71, 91
 - naming, 70, 90
 - sharing, 70, 90, 104
 - showing if shared, 104
- finish scripts
 - adding, 116
 - label encodings file, 117
- floppies
 - copying files from, 135
 - copying files to, 135
- formatting diskettes, 114

H

- hardware
 - configuring, 16
 - installation requirements, 28
 - planning, 28
 - protecting, 53, 95
- headless systems
 - configuring, 121
 - task maps, 39
- home directories
 - sharing, 104
- hosts
 - assigning a template, 62, 78, 99
 - entering in network files, 61, 77, 98
 - modifying templates, 61, 78

I

- icons
 - for device allocation, 54
 - for System_Admin actions, 131
- IMAP server
 - adding to NIS+ admin group, 103
- INETDIR variable, 82
- install user
 - deleting, 71, 91
 - justification, 31
 - logging in, 51
- installation
 - boot commands, 43
 - division of tasks, 41
 - log files, 46
 - manual reboot, 45, 46
 - memory requirements, 28
 - name service clients, 93
 - NIS master, 73
 - NIS+ root master, 73
 - NIS slave server, 102
 - no name service, 49
 - over networks, 107
 - planning, 23
 - planning hardware, 28
 - root password creation, 45
 - task maps, 37
 - troubleshooting, 47
- installed rule keyword
 - description and values, 115
- interactive installation
 - CD-ROM drive preparation, 43
 - NIS master, 73
 - NIS+ root master, 73
 - Trusted Solaris requirements, 41
- IP addresses
 - in tnrdhdb file, 62, 78
 - in tsolgateways file, 60, 76

J

- JumpStart directory
 - adding files with finish scripts, 116
 - copying files
 - disk configuration files, 118
 - creating, 119

- JumpStart directory (*continued*)
 - sharing, 119
- JumpStart installation
 - adding files with finish scripts, 116
 - creating in Trusted Solaris system, 114
- Jumpstart installation
 - deallocate floppy, 114
- JumpStart installation
 - modified procedures, 113
- jumpstart_sample directory
 - set_root_pw finish script, 117

L

- label encodings file
 - checking, 55
 - copying, 90
 - distributing using JumpStart, 117
 - installing, 53
 - installing on client, 96
 - localizing, 26, 150
 - modifying, 56
- labels
 - on trusted stripe, 51
 - planning, 26
- log files
 - installation, 46

M

- mkdir command
 - in JumpStart installation, 114
- mount command
 - during network installation, 113
 - example in Custom JumpStart, 114
 - in JumpStart installation, 114
- mounting
 - diskettes, 55, 114
 - file systems, 71, 91

N

- name service
 - client setup, 101

- name service (*continued*)
 - domain setup, 80
 - setup, 80
- names/naming
 - file systems, 70, 90
- network installation
 - add_install_client command, 113
 - add_to_install_server command, 113
 - allocate floppy, 114
 - booting, 47
 - differences from Solaris, 112
 - finish client configuration, 48
 - mount command, 113
 - planning, 29, 30
 - rm_install_server command, 113
 - role assignments, 47
 - setup_install_server command, 113
 - sharing directories, 111
 - task maps, 38
 - Trusted Solaris differences, 112
- newfs command
 - in JumpStart installation, 114
- NIS+
 - adding role to admin group, 88
- NIS+ domain
 - client setup, 101
 - creating roles, 87
- NIS domain
 - DIR variable, 82
 - INETDIR variable, 82
 - PWDIR variable, 82
 - RBACDIR variable, 82
 - root master setup, 73
- NIS+ domain
 - root master setup, 73
- NIS domain
 - setup, 82
- NIS+ domain
 - setup, 83
- NIS domain
 - slave server setup, 102
 - /var/yp directory, 82
 - /var/yp/Makefile, 83
- no name service
 - creating users, 64, 87

O

- osname rule keyword, 115
- output files
 - installation log, 46

P

- PASSWD variable, 117
- passwords
 - root, 117
 - root password creation, 45
- peripheral devices
 - configuring, 16
- privileges
 - on all mounted media, 108
 - on commands in rights profile, 110
- prof_attr database
 - converting from tsolprof format, 41
- PWDIR variable, 82

R

- RBACDIR variable, 82
- reboot
 - computer during configuration, 86, 103
- release of Trusted Solaris software
 - installed rule keyword, 115
- release software
 - osname rule keyword, 115
- remote host templates
 - assigning, 62, 78, 99
 - creating, 61, 78
 - creating new template, 61, 78
- rights
 - assigning, 68
 - updating, 136
 - verifying, 137
- Rights Profile
 - assigning, 65
- rm_install_server command
 - network installation, 113
- roles
 - creating in local files, 64, 87
 - creating in NIS+, 87
 - updating profiles, 136

- roles (*continued*)

- verifying profile contents, 137
- root passwords
 - created, 45
 - in finish scripts, 117
 - why required, 45

- root role
 - assuming, 51
 - updating profiles, 136

- rule keywords
 - installed, 115
 - osname, 115

- rules files
 - custom JumpStart example, 119

S

- screens
 - initial display, 51
 - locking, 128
- scripts
 - adding finish scripts, 116
 - creating finish scripts, 116
 - finish scripts, 117
 - label encodings file, 117
 - network installation modifications, 112
 - running, 132
 - running from Admin Editor, 132
- security
 - common violations, 145
 - computer recommendations, 142
 - install team, 41
 - personnel recommendations, 144
 - physical recommendations, 143
 - publications, 146, 147
 - root password, 45, 117
 - site security policy, 142
- Security Families
 - assigning a template, 61, 78
 - creating a template, 61, 78
 - modifying tnrdhdb, 62, 78
 - modifying tnrdhdb, 61, 78
- sessions
 - ending, 128
- set_root_pw finish script, 117

- setup_install_server command
 - custom JumpStart example, 120
 - network installation, 113
- shadow file, 117
- share command
 - sharing JumpStart directory, 119
- shared directories
 - for network installation, 110, 111
- shutting down
 - before installation, 43
- site security policy, 24, 142, 148
- slave server
 - enabling in NIS, 103
 - setting up in NIS, 102
- Solaris Management Console
 - initializing, 56, 97
 - troubleshooting, 56
- Solaris Management Console action
 - tools, 132
- System_Admin folder
 - using, 129, 132
- systems
 - booting from CD-ROM, 43
 - booting over network, 47
 - logging out, 128
 - protecting hardware, 53, 95
 - screen-locking, 128
 - shutting down, 43
 - starting, 129

T

- task maps
 - administering headless systems, 39
 - configuring headless systems, 39
 - installing from CD-ROM, 38
 - installing over the network, 38
 - preparing to install, 37
- Template Manager
 - modifying tnrrhttp, 61, 78
- /tmp/install_log file, 46
- tnrhdb file
 - configuring, 62, 78
 - fallback mechanism, 62, 78
 - wildcard address, 62, 78
 - wildcard mechanism, 63, 79

- tnrrhttp file
 - copying to the client, 99
 - modifying, 61, 78
- toolboxes
 - copy name service toolboxes, 102
 - description, 133
 - edit name service toolbox, 84
 - open, 56
 - saving preferences, 58
- troubleshooting
 - installation, 47
 - Solaris Management Console, 56
- trusted network
 - editing local files, 61, 62, 78
- Trusted Solaris configuration
 - adding users, 64, 87
 - copying tnrrhttp file to the client, 99
 - creating roles, 64, 87
 - evaluated configuration, 24
 - installing label encodings file on client, 96
 - logging on as a user, 127
 - name service clients, 93
 - no name service, 49
 - protecting computer, 53, 95
 - setting up home directories, 104
- Trusted Solaris differences
 - administrator's perspective, 34
 - Custom JumpStart, 113
 - interactive installation, 42
 - network installation, 112
 - optional Custom JumpStart features, 116
 - overview, 34
- Trusted Solaris installation
 - division of tasks, 41
 - headless systems, 121
 - interactive, 41
 - log files, 46
 - methods, 32
 - name service clients, 93
 - network, 47
 - NIS master, 73
 - NIS+ root master, 73
 - no name service, 49
 - over networks, 107
 - task maps, 37
 - troubleshooting, 47
 - worksheet examples, 155

- tsolgateways
 - setting, 60, 76
- tsolprof database
 - converting to new format, 41
- tsoluser database
 - converting to new format, 41

U

- UNIX publications
 - general, 148
 - security, 147
 - system administration, 19
- unlabeled host type
 - creating, 61, 78
- user_attr database
 - converting from tsoluser format, 41
- users
 - creating the first, 64, 66, 87
 - deleting local user, 71, 91

V

- variables
 - NIS domain, 82
- /var/sadm/system/logs/install_log file, 46
- /var/yp directory, 82
- /var/yp/Makefile, 83
- version of Trusted Solaris software
 - installed rule keyword, 115
 - osname rule keyword, 115

W

- wildcard address
 - using for network configuration, 62, 78
- worksheets
 - answering installation questions, 155, 159
 - examples, 155
 - partitioning examples, 157, 162
 - services that servers provide, 158
- workspaces
 - creating at admin_high, 54
 - initial display, 51

Y

- ypinit command
 - setting up slave server, 103

