



Trusted Solaris 8 HW 12/02 Transition Guide

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

Part No: 817-0878-10
May 2003

Copyright 2003 Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 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, Solstice AdminSuite, Solaris Management Console, Solaris Web Start, Sun Enterprise, Sun Fire, Java, Trusted Solaris, and Solaris are trademarks, registered trademarks, or service marks of Sun Microsystems, Inc. in the U.S. and other countries. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.

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 2003 Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 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, Solstice AdminSuite, Solaris Management Console, Solaris Web Start, Sun Enterprise, Sun Fire, Java, Trusted Solaris, et Solaris sont des marques de fabrique ou des marques déposées, ou marques de service, de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays. Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux Etats-Unis et dans d'autres pays. Les produits portant les marques SPARC sont basés sur une architecture développée par Sun Microsystems, Inc.

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.



030331 @ 5533



Preface

The *Trusted Solaris 8 HW 12/02 Transition Guide* describes the differences among the following releases:

- The Trusted Solaris™ 7 release
- The Trusted Solaris 8 release
- The Trusted Solaris 8 4/01 release
- The Trusted Solaris 8 HW 12/02 release
- The Solaris™ operating environment releases that correspond to the preceding Trusted Solaris releases

The differences include the operating system, the modified desktop, the modified windowing system, and the modified administration tools.

The most recent changes to the software are described in “Changes From the Trusted Solaris 8 4/01 to the Trusted Solaris 8 HW 12/02 Release” on page 5.

Who Should Use This Book

The *Trusted Solaris 8 HW 12/02 Transition Guide* is designed for users who are familiar with the Trusted Solaris 7 release, Trusted Solaris 8 releases, and Solaris 8 releases. The book enables these users to find their way more easily around the Trusted Solaris 8 HW 12/02 operating environment. All users should find the book useful.

Related Books

If you have used the Trusted Solaris 2.5 release, but you have not used the Trusted Solaris 2.5.1 release, read the *Trusted Solaris 2.5.1 Transition Guide*, 805-8030-10. The guide is available online at the docs.sun.comSM Web site in the Trusted Solaris 2.5.1 AnswerBook collection. The URL is <http://docs.sun.com>. This guide can also be viewed using the `/usr/openwin/bin/answerbook` command with the books in the Trusted Solaris 2.5.1 library.

If you have used the Trusted Solaris 2.5.1 release, but you have not used the Trusted Solaris 7 release, read the *Trusted Solaris 7 Transition Guide*, 805-8059-10. The guide is available online at the docs.sun.com Web site in the Trusted Solaris 7 AnswerBook collection.

Accessing Sun Documentation Online

The docs.sun.com 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>.

Transition to the Trusted Solaris 8 HW 12/02 Release

The Trusted Solaris 8 HW 12/02 operating environment is based on the Solaris 8 HW 12/02 release. The Trusted Solaris 8 HW 12/02 software updates Trusted Solaris 8 4/01 software and Solaris 8 2/02 software.

This book covers the following topics:

- “Changes From the Trusted Solaris 8 4/01 to the Trusted Solaris 8 HW 12/02 Release” on page 5
- “Changes From the Trusted Solaris 8 to the Trusted Solaris 8 4/01 Release” on page 7
- “Changes to SunOS 5.8 (Solaris 8 4/01 Release)” on page 8
- “Changes to Support the Sun Enterprise 10000 and Intel Platform” on page 9
- “Changes to CDE 1.4.4” on page 9
- “Changes in Administration Tools” on page 10
- “Changes From the Trusted Solaris 7 to the Trusted Solaris 8 Release” on page 11

Changes From the Trusted Solaris 8 4/01 to the Trusted Solaris 8 HW 12/02 Release

The following table lists features that changed between the Trusted Solaris 8 4/01 and Trusted Solaris 8 HW 12/02 releases. The table also lists differences between the software that the Solaris 8 2/02 release supports and the software that the Trusted Solaris 8 HW 12/02 release supports.

TABLE 1-1 Trusted Solaris 8 HW 12/02 Changes to Trusted Solaris 8 4/01 Software

Area of Change	Description of Change
Audit Token	<p>The <code>praudit</code> output for the header token in earlier Trusted Solaris releases had the following form:</p> <pre>header,131,4,login - local,,Wed Dec 11 14:23:54 2002, + 471 msec</pre> <p>The header token in this release includes the machine name, as shown in the following example:</p> <pre>header,162,4,login - local,,enigma,Fri Mar 07 22:27:49 2003, + 770 msec</pre> <p>The host audit token is no longer generated. Instead, the expanded header token contains host information. Customized scripts or tools which parse <code>praudit</code> output might need to be updated to handle this change.</p>
Hardware	<p>The Trusted Solaris 8 HW 12/02 release supports the hardware platforms that the Solaris 8 HW 12/02 release supports.</p> <p>On the Sun Fire 15K and the Sun Fire 12K servers, Trusted Solaris software installs on domains and runs domains. To run on the system controller, install Solaris software.</p>
Licensing	<p>A Trusted Solaris License Agreement dialog box displays when the <code>install</code> user enters CDE. When the user clicks Accept, the dialog box does not display again. Until the license agreement is accepted, the Window Manager displays “Not Licensed” at the far right on the trusted stripe.</p> <p>After the license agreement is accepted, the trusted stripe shows which edition of the Trusted Solaris release is running. This information is also available by using the <code>uname -v</code> command.</p>
Packaging	<p>The Solaris packages that the Trusted Solaris product does not enhance remain unmodified. Therefore, you can apply Solaris patches to those Solaris packages that remain unmodified.</p> <p>Use the <code>showrev -p</code> command in a terminal window to list the patches that have been applied to the system.</p>
Patches	Use the <code>patchadd</code> command to install patches. The <code>patchadd</code> command prevents the installation of a patch that would overwrite a Trusted Solaris feature.
KCMS server	The <code>kcms_server</code> service is disabled by default in the <code>inetd.conf</code> file. The server is vulnerable to security violations.
Upgrade	Upgrade is supported from Trusted Solaris 8 releases to the Trusted Solaris 8 HW 12/02 release.
x86 Network Boot	Trusted Solaris software does not support x86 network boot.

Changes From the Trusted Solaris 8 to the Trusted Solaris 8 4/01 Release

Features that changed between the Trusted Solaris 8 and Trusted Solaris 8 4/01 releases are described in the following table.

TABLE 1–2 Trusted Solaris 8 4/01 Additions to Trusted Solaris 8 Software

Area of Change	Description of Change
Sun Blade™ hardware	The Trusted Solaris 8 4/01 release runs on the Sun Blade 100 and Sun Blade 1000 hardware.
SMC Auditing	The Solaris Management Console GUI is now fully audited.
SMC Rights Manager	Supports copy and paste of security attributes of commands and actions.
SMC Computer and Networks tool	Supports a Default setting for the label and clearance in a security family template definition. When the Default button is selected, the label and clearance values of the interface are applied to unlabeled packets. The label and clearance values are not provided in a template.
SMC Toolbox files	Toolbox files (*.tbx) require the <Scope> tag in addition to the <URL> tag within the <ToolBoxURL> tag. The <Scope> tag indicates the scope that the sub-toolbox will use. The scope value must match the value that is specified in the <Scope> tag of the respective sub-toolbox. A freshly installed Trusted Solaris 8 4/01 system has already implemented the <Scope> tag. When you upgrade a system from the Trusted Solaris 8 release to the Trusted Solaris 8 4/01 release, you must enter the correct scope value. You must manually modify the /var/sadm/smc/toolbox/tsol_smc/tsol_smc.tbx toolbox to add the <Scope> tag for each <ToolBoxURL> tag in the file. Similarly, users are required to modify any toolboxes created in any location other than the default SMC toolbox location.
Smart Card technology	The Trusted Solaris 8 4/01 release supports Smart Card technology on Sun Blade hardware.

TABLE 1–2 Trusted Solaris 8 4/01 Additions to Trusted Solaris 8 Software (Continued)

Area of Change	Description of Change
Man Pages	<p>References to information labels (ILs) have been removed from all man pages except the <code>label_encodings(4)</code> man page.</p> <p>Man pages specific to ILs have been removed.</p> <p>The <code>allocate(1)</code>, <code>deallocate(1)</code>, and <code>list_devices(1)</code> man pages have been moved from Section 1m to Section 1.</p> <p>The <code>mkdevdb(1)</code> man page describes the device allocation interfaces.</p> <p>The streams man pages (<code>tsol_put*ctl*(9f)</code>) have been removed. Trusted Solaris differences are handled in the Solaris versions (<code>put*ctl*(9f)</code>) of the man pages.</p>
NIS+ actions	Actions to handle NIS+ groups have been added to the <code>System_Admin</code> folder.
Upgrade	Upgrade is supported from Trusted Solaris 8 to Trusted Solaris 8 4/01 only.

Changes to SunOS 5.8 (Solaris 8 4/01 Release)

Unless explicitly stated otherwise, the Trusted Solaris 8 4/01 environment supports the new features in the Solaris 8 release. Feature support includes IPv6, IPsec, role-based access control (RBAC), and new media types, such as Zip, Jaz, and DVD.

The following Solaris 8 features function differently in the Trusted Solaris environment:

- The Trusted Solaris release does not update the Solaris `SUNWrdm` README package. Many items in that package apply to the Trusted Solaris environment. However, for late-breaking news particular to the Trusted Solaris environment, see the *Trusted Solaris 8 4/01 Release Notes*.
- The Trusted Solaris versions of selected Solaris man pages are enhanced for Trusted Solaris security policy.
- The following Solaris interfaces are not supported in the Trusted Solaris 8 environment:
 - `bsmconv(1M)` and `bsmunconv(1M)` – See *Trusted Solaris Audit Administration* for how to manage auditing. See *Trusted Solaris Administrator's Procedures* for how to manage devices.
 - `rexecd(1M)`
 - `rusers(1)`

- `ncad(1M)`
- `spell(1)`
- `talk(1)`

Changes to Support the Sun Enterprise™ 10000 and Intel Platform

To run securely on the Sun Enterprise 10000 and on Intel Architecture (IA), the Trusted Solaris 8 release enhances installation and administration for security.

Trusted Solaris changes for the Sun Enterprise 10000 include the following:

- Solaris™ Web Start installation is not supported.
- For remote (headless) workstation administration, use the Solaris Management Console™, or see the Trusted Solaris `dtappsession(1)` page in the CDE man package (installed in the directory `/usr/dt/man`). The man page is also printed in the *Trusted Solaris 8 Reference Manual*, 805-8124-10.
- There is no command line login. Administration of a newly installed Sun Enterprise 10000 is done remotely, using CDE. See *Trusted Solaris 8 Installation and Configuration on the Sun Enterprise 10000*.

Trusted Solaris changes for the Intel platform include the following:

- BIOS protection is the equivalent of PROM protection on the SPARC® platform.

Changes to CDE 1.4.4

The Trusted Solaris 8 environment supports the new features in the CDE 1.4.8 release, such as new actions. The Trusted Solaris 8 environment continues to support the visible Trusted Solaris features in CDE, such as labels, trusted stripe, privilege assignment to files, Admin Editor, and so on. Administrative actions that are new to CDE 1.4.8 have been modified for security in the Trusted Solaris environment. The new actions are available in the `System_Admin` folder:

- The Style Manager is not available from the Workspace menu in the Trusted Solaris 8 environment because it must be run from the trusted path. It is available from the Front Panel, where it runs securely.
- The Solaris Suspend System command on the Workspace menu and the This Host subpanel have been modified to check for the shutdown authorization.

Note – The Application Manager can be invoked from the Applications > Application Manager item on the Workspace menu. A terminal can be invoked from the Tools > Terminal and the Hosts > This Host items on the Workspace menu.

Changes in Administration Tools

The Trusted Solaris 8 release replaces the administration tools that in the Trusted Solaris 7 release were based on Solstice AdminSuite™ 2.3. The `Solstice_Apps` folder is removed. The `Solaris Management Console` action replaces the `Solstice_Apps` folder. CDE online help for these administrative databases is replaced by online help in the Solaris Management Console GUI.

Note – The SMC online help refers to the profile shell as the administrator’s shell. There are now three profile shells: Bourne, Korn, and C.

The Solaris Management Console action invokes a GUI based on Java™ 1.2.2_07a. The SMC GUI enables administrators to manage user, network, execution profile (now called “rights” or “rights profiles”), and other databases. After opening the Solaris Management Console (SMC), the administrator chooses a “toolbox”, which is a collection of programs, and then uses the programs permitted to the administrative role. The SMC does not support the Lightweight Directory Access Protocol (LDAP).

The following tables show the correspondences between Trusted Solaris 7 programs and SMC programs. Note that some actions in the `System_Admin` folder have been superseded by SMC tools.

TABLE 1–3 Trusted Solaris Administrative Programs

Trusted Solaris 7 Solstice Programs	Trusted Solaris 8 SMC Programs
Database Manager	Users > Mailing Lists
— Aliases	Interface Manager
— Tnldb	Computers and Networks > Security families
— Tnrhdb, Tnrhtp	
Group Manager	Users > Groups
Host Manager	Computers and Networks

TABLE 1-3 Trusted Solaris Administrative Programs (Continued)

Trusted Solaris 7 Solstice Programs	Trusted Solaris 8 SMC Programs
Printer Manager	Printer Administrator (in System_Admin folder)
Profile Manager	Users > Rights
Serial Manager	Devices and Hardware > Serial Ports
Storage Manager	Storage > Mounts and Shares
	Storage > Disks
User Manager	Users > User Accounts
	Users > User Templates
	Users > Administrative Roles

TABLE 1-4 Trusted Solaris Administrative Actions

Trusted Solaris 7 System_Admin Actions	Trusted Solaris 8 SMC Programs
Set Mount Points	Storage > Mounts and Shares > Mounts
Share File Systems action	Storage > Mounts and Shares > Shares

Changes From the Trusted Solaris 7 to the Trusted Solaris 8 Release

Changes from the Trusted Solaris 7 release affect users, administrators, and developers. Changes affect the following areas:

- “Installation and Configuration” on page 12
- “Auditing” on page 13
- “Authorizations” on page 13
- “Commands and Functions” on page 15
- “Databases — Users, Profiles, and Authorizations” on page 16
- “Devices” on page 17
- “File Systems and Mounting” on page 17
- “Labels” on page 17
- “Man Pages” on page 17
- “Printing” on page 19
- “Roles” on page 19
- “Security Policy” on page 20
- “Serial Ports” on page 20
- “Trusted Networking” on page 20

Installation and Configuration

Trusted Solaris 8 installation and configuration requires more disk and swap space than the Trusted Solaris 7 release required. Files to create local administrative roles are no longer provided on the installation CD-ROM. The root role creates the initial roles, then assigns the roles to the initial users.

Installation Differences

Installation on most hardware is identical to Solaris 8 installation. The Trusted Solaris 8 environment supports the name services that are fully supported in the Solaris 8 and Solaris Management Console 2.0 releases. The following lists the exceptions:

- Solaris Web Start is not supported.
- Upgrade is not supported. Administrators who want to retain Trusted Solaris 2.5.1 or 7 database information (`tsoluser`, `tsolprof`, `tnrhdb`, `tnrhttp`) should back up these files. The files whose format and names have changed (`tsoluser` and `tsolprof`) should be converted on a Trusted Solaris 7 system before installing the Trusted Solaris 8 release. For the `tsolconvert` utility and procedure, see the following URL:

http://www.sun.com/software/solaris/trustedsolaris/ts_tech_faq/

- The second installation CD-ROM is displayed in a text-only interface.
- The Solaris Management Console requires that the install team allocate approximately 148 MBytes more swap to the host running the console. For example, if the previous swap was 256 MBytes, the Trusted Solaris 8 swap should be at least 404 MBytes.
- Installing and configuring the Sun Enterprise 10000 is modified for Trusted Solaris security. See *Trusted Solaris 8 Installation and Configuration on the Sun Enterprise 10000* for explanation and procedures.

Note – To distribute a site label encodings file during Trusted Solaris 8 network installation requires a customized JumpStart installation that calls a site-created script to install the file at `admin_high`.

Configuration Differences

The Trusted Solaris 8 release introduces significant configuration differences from earlier releases. Of particular interest are “Security Policy” on page 20, “Labels” on page 17, “Roles” on page 19, “Auditing” on page 13, “Devices” on page 17 and “Trusted Networking” on page 20.

Auditing

The Trusted Solaris 8 environment, as well as the Solaris 8 environment, enables the administrator to set up network-wide user audit flags. The `audit_user` file can now be administered using a name service through the Solaris Management Console.

Authorizations

Authorizations are now part of the Solaris 8 environment. Therefore, Trusted Solaris 7 authorizations have been renamed in the Trusted Solaris 8 environment to correspond to their Solaris 8 counterparts. See the file `/etc/security/auth_attr` for a full list of authorizations, and the `auth_attr(4)` man page for an explanation of the syntax. The following tables show the Trusted Solaris 7 to Trusted Solaris 8 authorization name correspondences, ordered by authorization number.

TABLE 1-5 Authorizations 1 through 27

No.	Trusted Solaris 7 Names	Trusted Solaris 8 Equivalents
1	TSOL_AUTH_ENABLE_LOGIN	solaris.login.enable
2	TSOL_AUTH_REMOTE_LOGIN	solaris.login.remote
3	TSOL_AUTH_TERMINAL_LOGIN	solaris.login.remote
4	TSOL_AUTH_FILE_AUDIT	solaris.file.audit
5	TSOL_AUTH_FILE_DOWNGRADE_SL	solaris.label.file.downgrade
6	TSOL_AUTH_FILE_UPGRADE_SL	solaris.label.file.upgrade
7	TSOL_AUTH_FILE_OWNER	solaris.file.owner
8	TSOL_AUTH_FILE_CHOWN	solaris.file.chown
9	TSOL_AUTH_FILE_SETPRIV	solaris.file.privs
10	TSOL_AUTH_ALLOCATE	solaris.device.allocate
11	TSOL_AUTH_WIN_DOWNGRADE_SL	solaris.label.win.downgrade
12	TSOL_AUTH_WIN_UPGRADE_SL	solaris.label.win.upgrade
13	TSOL_AUTH_CRON_ADMIN	solaris.jobs.admin
14	TSOL_AUTH_SYS_ACCRED_SET	solaris.label.range
15	TSOL_AUTH_BYPASS_FILE_VIEW	solaris.label.win.noview
16	TSOL_AUTH_SHUTDOWN	solaris.system.shutdown
17	TSOL_AUTH_USER_IDENT	solaris.admin.usermgr.write

TABLE 1-5 Authorizations 1 through 27 (Continued)

No.	Trusted Solaris 7 Names	Trusted Solaris 8 Equivalents
18	TSOL_AUTH_USER_PASSWORD	solaris.admin.usermgr.pswd
19	TSOL_AUTH_USER_SELF	None
20	TSOL_AUTH_USER_LABELS	solaris.admin.usermgr.label
21	TSOL_AUTH_USER_AUDIT	solaris.admin.usermgr.audit
22	TSOL_AUTH_USER_PROFILES	solaris.profmgr.*
23	TSOL_AUTH_USER_IDLE	None
24	TSOL_AUTH_USER_ROLES	solaris.role.assign
25	TSOL_AUTH_USER_HOME	solaris.admin.usermgr.write
26	TSOL_AUTH_PRINT_POSTSCRIPT	solaris.print.ps
27	TSOL_AUTH_PRINT_UNLABELED	solaris.print.unlabeled

TABLE 1-6 Authorization Numbers 28 through 55

No.	Trusted Solaris 7 Names	Trusted Solaris 8 Equivalents
28	TSOL_AUTH_DB_ALIASES	None
29	TSOL_AUTH_DB_AUTO_HOME	solaris.admin.fsmgr.write
30	TSOL_AUTH_DB_BOOTPARAMS	None
31	TSOL_AUTH_DB_ETHERS	solaris.network.hosts.write
32	TSOL_AUTH_DB_GROUP	solaris.admin.usermgr.write
33	TSOL_AUTH_DB_HOSTS	solaris.network.hosts.write
34	TSOL_AUTH_DB_LOCALE	solaris.network.hosts.write
35	TSOL_AUTH_DB_NETGROUP	solaris.network.hosts.write
36	TSOL_AUTH_DB_NETMASKS	solaris.network.hosts.write
37	TSOL_AUTH_DB_NETWORKS	solaris.network.hosts.write
38	TSOL_AUTH_DB_PASSWD	solaris.admin.usermgr.pswd
39	TSOL_AUTH_DB_PROTOCOLS	None
40	TSOL_AUTH_DB_RPC	None
41	TSOL_AUTH_DB_SERVICES	None
42	TSOL_AUTH_DB_TIMEZONE	None
43	TSOL_AUTH_DB_TNIDB	solaris.network.security.write

TABLE 1-6 Authorization Numbers 28 through 55 (Continued)

No.	Trusted Solaris 7 Names	Trusted Solaris 8 Equivalents
44	TSOL_AUTH_DB_TNRHDB	solaris.network.security.write
45	TSOL_AUTH_DB_TNRHTP	solaris.network.security.write
46	TSOL_AUTH_CRON_USER	solaris.jobs.user
47	TSOL_AUTH_AT_ADMIN	solaris.jobs.admin
48	TSOL_AUTH_AT_USER	solaris.jobs.user
49	TSOL_AUTH_PRINT_ADMIN	solaris.print.admin
50	TSOL_AUTH_PRINT_NOBANNER	solaris.print.nobanner
51	TSOL_AUTH_CONFIG_DEVICE	solaris.device.config
52	TSOL_AUTH_REVOKE_DEVICE	solaris.device.revoke
53	TSOL_AUTH_PRINT_CANCEL	solaris.print.cancel
54	TSOL_AUTH_PRINT_LIST	solaris.print.list
55	TSOL_AUTH_PRINT_MAC_OVERRIDE	solaris.label.print

Commands and Functions

Commands and functions have been modified. Some modifications are due to technical changes in the product. Some changes are due to removal of nonstandard interfaces.

- The Trusted Solaris `/usr/proc/bin/` commands have been moved to `/usr/bin/` to correspond to their Solaris counterparts.
- The library functions for the `tsoluser` and `tsolprof` databases have been replaced by functions for the new databases, `user_attr`, `exec_attr`, and `prof_attr`. See “Databases — Users, Profiles, and Authorizations” on page 16.
- The library functions for authorizations have been replaced by Solaris functions. The functions have been extended for the Trusted Solaris environment. See Table 1-8 for the database man page correspondences. The following table shows the Trusted Solaris 8 man pages that describe Trusted Solaris 7 functionality.

TABLE 1-7 Trusted Solaris 8 Man Pages for User, Profile, and Authorization Functions

Trusted Solaris 7 Database Functions	Trusted Solaris 8 Man Page
<code>getuserent()</code> , <code>setuserent()</code> , <code>getuserentbyname()</code> , <code>getuserentbyuid()</code> , <code>free_userent()</code> , <code>enduserent()</code>	<code>getuserattr(3secdb)</code>

TABLE 1–7 Trusted Solaris 8 Man Pages for User, Profile, and Authorization Functions
(Continued)

Trusted Solaris 7 Database Functions	Trusted Solaris 8 Man Page
getprofent(), setprofent(), getprofentbyname(), getprofstr(), getprofstrbyname(), free_profent(), free_profstr(), endprofent(), endprofstr(), putprofstr()	getprofattr(3secdb)
auth_to_str(), str_to_auth(), auth_set_to_str(), str_to_auth_set(), free_auth_set(), get_auth_text(), chkauth()	getauthattr(3secdb)

Databases — Users, Profiles, and Authorizations

The user, rights profile, and authorization databases are now available in the Solaris 8 environment. Therefore, a Trusted Solaris 8 server can manage the rights and authorizations for Solaris 8 clients as well as Trusted Solaris 8 clients. The Solaris environment changed the name execution profile to rights, or rights profile.

Rights profiles are administered through the Solaris Management Console. The Trusted Solaris 7 Profile Manager is now the Rights tool, under Users (the User Manager). The Rights tool does not recognize symbolically linked commands.

Rights profiles are now hierarchical. Profiles can subsume other profiles, though this is not required. Hierarchical profiles eliminate the need to enumerate all profiles assigned to a user or role.

The names and contents of profiles have changed. Most profiles have been reconfigured. Some profiles have been eliminated.

Trusted Solaris extends the Solaris versions of the user, profile, and authorization databases to include CDE actions and Trusted Solaris security attributes, such as labels and new authorizations. The following table shows the new database names.

TABLE 1–8 Database Changes from the Trusted Solaris 7 to the Trusted Solaris 8 Release

Trusted Solaris 7 Database	Trusted Solaris 8 Man Page
/etc/security/tsol/tsolprof	exec_attr(4) and prof_attr(4)
/etc/security/tsol/tsoluser	user_attr(4)
/usr/lib/tsol/locale/C/auth_name	auth_attr(4)
auth_desc man page	SMC help for the Authorizations tab

Devices

Devices may be allocated outside of the trusted path. Separate authorizations specify that you are allocating within the trusted path and without the trusted path. For security, Trusted Solaris software keeps track of the username of the allocator. The Device Allocation Manager GUI can display and edit the `device_maps(4)` entry for an allocatable device. The GUI enables the administrator to specify if devices should be deallocated at logout or reboot. Device allocation can be done remotely or in shell scripts by authorized users.

File Systems and Mounting

The Trusted Solaris 8 implementation for specifying file system security attributes follows the Solaris 8 implementation. The Solaris 8 implementation has consequences for Trusted Solaris 8 administrators.

Mount-time security attributes may be specified either by using the `mount(1M)` command with the `-o` option on the command line or by specifying the attributes in the `vfstab_adjunct` file. The following mount-time security attributes have been removed: `acl`, `attr_flg`, `uid`, `gid`, and `mode`.

The `vfstab_adjunct` file is protected at the label `admin_high`.

Labels

The Trusted Solaris 8 environment protects the `label_encodings(4)` at the label `admin_high`. The default user label and clearance are defined in the `label_encodings` file.

The Label Builder used by administrators is now Java-based and accessed through the Solaris Management Console. The label builder that is accessed outside the Solaris Management Console is different. The users' label builder is the Motif label builder that was shipped with the Trusted Solaris 7 software.

In the Trusted Solaris 8 environment, the label attributes assigned to commands and actions in a profile no longer represent the restricted label range for execution. Instead, the attributes set the label and clearance of the process that is running the command. The attributes that are set are independent of the label of the original profile shell. This is a change to the profile shell from the Trusted Solaris 7 release. The behavior matches the way the system shell has always worked.

Man Pages

The following Trusted Solaris 7 man pages do not contain Trusted Solaris-specific modifications in the current release due to changes in implementation. The Solaris versions describe their functionality in the Trusted Solaris 8 environment:

- `nstest(1M)`
- `pfsh(1M)`, which points to the `pfexec(1)` man page.

Note – The `clist` command in the profile and system shells no longer exists. See the `smprofile(1M)`, or the `profiles(1)` and `auths(1)` man pages for the command to list the commands, actions, and authorizations in a rights profile.

The `setmnt(1M)` man page and command have been removed from the Solaris and Trusted Solaris environments.

The man pages in the following table contain Trusted Solaris-specific modifications to Solaris 8 man pages, or are Trusted Solaris 8 man pages new to this release:

TABLE 1–9 Man Pages Newly Created or Modified for the Trusted Solaris 8 Environment

Man Page Section	Man Page	
Section 1	<code>auths(1)</code>	<code>nispasswd(1)</code>
	<code>crle(1)</code>	<code>profiles(1)</code>
	<code>date(1)</code>	<code>roles(1)</code>
	<code>nca(1)</code>	
	<code>ncakmod(1)</code>	
Section 1M	<code>coreadm(1M)</code>	<code>smc(1M)</code>
	<code>devfsadm(1M)</code>	<code>smcron(1M)</code>
	<code>init.wbem(1M)</code>	<code>smexec(1M)</code>
	<code>mkdevalloc(1M)</code>	<code>smgroup(1M)</code>
	<code>mkdevmaps(1M)</code>	<code>smhost(1M)</code>
	<code>nisclient(1M)</code>	<code>smaillist(1M)</code>
	<code>pkgchk(1M)</code>	<code>smmultisuer(1M)</code>
	<code>rmmount(1M)</code>	<code>smnetidb(1M)</code>
	<code>rpc.yppasswdd(1M)</code>	<code>smnettpl(1M)</code>
	<code>rpc.ypupdated(1M)</code>	<code>smnetwork(1M)</code>
	<code>su(1M)</code>	<code>smuser(1M)</code>
	<code>ypbind(1M)</code>	
	<code>ypserv(1M)</code>	
	<code>ypxfr(1M)</code>	

TABLE 1–9 Man Pages Newly Created or Modified for the Trusted Solaris 8 Environment
(Continued)

Man Page Section	Man Page	
Section 2	acct(2)	
Section 3	getauthattr(3SECDB)	grantpt(3C)
	getauusernam(3BSM)	
Section 4	exec_attr(4)	prof_attr(4)
	logindevperm(4)	shadow(4)
	nca.if(4)	user_attr(4)
	policy.conf(4)	
Section 5	pam_unix(5)	

Printing

The Printer Administrator action in the System_Admin folder manages printers. To limit the label range of a printer, use the Device Allocation Manager.

Roles

The Trusted Solaris 8 environment has eliminated non-administrative roles. All roles in the Trusted Solaris environment are administrative ones. Roles are managed through the Administrative Roles tool in the Solaris Management Console. With the exception of the root role account, which must be a local account, role accounts are similar to user accounts in that their home directories are not necessarily local. Their home directories can be in the same location as users on the system.

In the Trusted Solaris 8 environment there are five recommended roles. Only the root role is provided on the installation CD-ROM. During system configuration the root role creates four roles (admin, secadmin, oper, and primaryadmin) and assigns existing profiles to them. The new role, primaryadmin, or Primary Administrator, is in fact an emergency administrator, to be used when the security administrator cannot do something. Once roles are created and assigned to users, the root role is no longer required and can be disabled. root is a much weaker role in the Trusted Solaris 8 release than it was in previous releases.

The names and contents of role profiles have changed to enable ease of administration. For example, the system administrator (the role admin) can now install most third-party software packages. The security administrator (secadmin) is only required when the applications being installed affect security. Also, prior to user

account setup, the security administrator can set the security defaults for user accounts. Then when the system administrator sets up user accounts, the security administrator need not be present. It is also possible for the security administrator alone to set up user accounts.

Roles (and users) can now be prevented from logging in if their password is incorrectly entered a number of times as specified by the value of the `RETRIES` (not the `MAX_BADLOGINS`) flag. For details, see the `passwd(4)` and `shadow(4)` man pages. The default is No, do not lock the account. The defaults can be changed, and individual user and role accounts can be given a non-default value. Note that the NIS name service does not support `RETRIES` or account locking.

Security Policy

Security policy is now configured similarly in the Solaris and Trusted Solaris 8 environments. The configuration file `/etc/security/policy.conf` contains default attributes for users created on the system. Label defaults are set in the `label_encodings` file. The defaults can be added to or overridden, but provide an ease-of-creation mechanism. The security administrator can set up sensible defaults for most users on the system. The Add User wizard in SMC will then create users with sensible defaults.

Trusted Solaris 7 software enabled the security administrator to extend the list of trusted libraries by creating a list of trusted library directories in a file named `/etc/security/tsol/rtld`. The Trusted Solaris 8 release uses a new Solaris 8 mechanism, the `crle(1)` command with the option `-u`. See *Trusted Solaris Administrator's Procedures* for sample procedures.

Serial Ports

The Solaris Management Console Devices and Hardware tool manages serial lines and serial ports. To limit the label range of a serial port, use the Device Allocation Manager.

Trusted Networking

The trusted networking databases are now administered through the Solaris Management Console. The `tnidb` database is administered using the Interface Manager program. The `tnrhtp` database and `tnrhdb` databases are administered using the Security Families program. The `tnrhdb` is extended to handle IPv6 address formats and variable-length netmasks.

The Trusted Solaris 8 environment does not interoperate with hosts or networks that run Trusted Solaris 1.2 software (except as unlabeled). The `msix` template for Trusted Solaris 1.2 hosts in the `tnrhtp` database has been removed.

The following fields have been removed from the `tnrhtp` templates. For interoperability, these are ignored if present: `def_uid`, `def_gid`, `def_audit_auid`, `def_audit_asid`, `def_audit_mask`, and `def_audit_termid`.

The functions `t6last_attr(3NSL)` and `t6peek_attr(3NSL)` no longer return defaults for identity-based attributes.

The `/etc/security/tsol/boot` directory has been removed. To ensure that a Trusted Solaris machine can contact the necessary servers while booting, the security administrator should ensure that each necessary server (name service master, audit server, and so on) is covered by an entry in the machine's local `tnrhdb` file.

The `/etc/security/tsol/tnrhtp` file installed from the Trusted Solaris 8 Installation CD has templates that match the labels in the `/etc/security/tsol/label_encodings` file installed from the Trusted Solaris 8 Installation CD. The following table shows the correspondences between earlier versions of `tnrhtp` and the version shipped with the Trusted Solaris 8 release.

TABLE 1–10 Template Equivalents Between Trusted Solaris 8 and Earlier Releases

Template Names from Earlier Release	Trusted Solaris 8 Replacement Names
unlab	admin_low
	unclassified
	confidential
	secret
	top_secret
tsol	tsol
tsol_1	tsol_ripso
tsol_2	tsol_cipso
ripso	ripso_top_secret
cipso	cipso
tsix	tsix

The `cipso_doi` keyword has been changed to the more general `doi` (Domain of Interpretation) in the `tnrhtp` database, because now it is used in the Trusted Solaris protocol and is not limited to the CIPSO IP options. Matching of the DOI value is enforced for incoming packets. For interoperability with the previous Trusted Solaris releases, the default DOI in the Trusted Solaris 8 release is 0 instead of empty (it is 1 for CIPSO host types), and the keyword `cipso_doi` is interpreted as the more general domain of interpretation.

Packets from unlabeled hosts outside a Trusted Solaris domain can be labeled for trusted routing through the secure domain to another host outside the domain using IP options. Incoming packets are labeled according to their originating host's entry in the `tnrhdb`, and routed through the Trusted Solaris domain according to their sensitivity level (carried in the IP option) and the trusted routing information. The label is then stripped at the exit. Note that trusted routing requires an IPv4 network; IPv6 does not support trusted routing.

The cache files `/var/tsol/tn*_c` are no longer used. The `tn` handles caching and provides `tnrhdb` entries to the kernel on demand.

The software supplies defaults for network interfaces. Therefore, an interface needs to be listed explicitly in the `tnidb` database only when its desired security attributes differ from the defaults:

```
min_sl  ADMIN_LOW
max_sl  ADMIN_HIGH
def_label [ADMIN_LOW]
def_cl  ADMIN_HIGH
forced_privs none
```