Trusted Solaris 8 Transition Guide

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

Part Number 805-8118-10
December 2000

Preface

The *Trusted Solaris 8 Transition Guide* describes the differences between Trusted Solaris 7 (including its modified desktop, windows, and administration tools), Solaris 8 6/00, and Trusted Solaris 8.

Who Should Use This Book

The *Trusted Solaris 8 Transition Guide* is designed to enable users familiar with Trusted Solaris 7 and Solaris 8 to find their way more easily around the Trusted Solaris 8 operating environment. All users should find the book useful.

Related Books

If you have used Trusted Solaris 2.5 but not Trusted Solaris 2.5.1, please read the *Trusted Solaris 2.5.1 Transition Guide*, 805–8030–10. It is available online at the docs.sun.com℠ Web site in the *Trusted Solaris 2.5.1 AnswerBook*. It 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 Trusted Solaris 2.5.1 but not Trusted Solaris 7, please read the *Trusted Solaris 7 Transition Guide*, 805–8059–10. It is available online at the docs.sun.com℠ Web site in the *Trusted Solaris 7 AnswerBook*.

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.com[SM] 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`.

CHAPTER 1

Transition to Trusted Solaris 8

Trusted Solaris 8 is a security-enhanced version of the Solaris 8 6/00 operating environment. It updates Trusted Solaris 7 software, and includes:

Changes to SunOS 5.8 (Solaris 8 6/00)

Unless explicitly stated otherwise, Trusted Solaris 8 supports the new features in the Solaris 8 release, such as IPv6, IPsec, role-based access control (RBAC), and new media types, such as Zip, Jaz, and DVD. It does not support Smart Card technology. The following Solaris 8 features function differently in the Trusted Solaris environment:

- Trusted Solaris 8 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 Release Notes*.
- The Trusted Solaris version of selected Solaris 8 man pages are enhanced for Trusted Solaris security policy.
- The following Solaris interfaces are not supported in Trusted Solaris 8:

- `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), Trusted Solaris 8 enhances installation and administration for security.

For the Sun Enterprise 10000:

- 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*, 835–8114–10.
- There is no command line login. Administration of a newly installed Sun Enterprise 10000 is done remotely, using CDE. See the *Trusted Solaris 8 Installation and Configuration on the Sun Enterprise 10000*.

For the Intel platform:

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

Changes to CDE 1.4.1

Trusted Solaris 8 supports the new features in the CDE 1.4.1 release, such as new actions, and it 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 1.4.1 have been modified for security in the Trusted Solaris environment, and are available in the `System_Admin` folder:

- The Style Manager is not available from the Workspace menu in Trusted Solaris 8 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 has 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 from Solstice AdminSuite 2.3 to Solaris Management Console 2.0

Trusted Solaris 8 replaces the administration tools that in Trusted Solaris 7 were based on Solstice AdminSuite 2.3. The `Solstice_Apps` folder is removed and replaced with the `Solaris Management Console` action. 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 shells.

The Solaris Management Console action invokes a GUI based on Java 1.2.2_05a. 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 1–1 Trusted Solaris Administrative Programs

Trusted Solaris 7 Solstice Programs	Trusted Solaris 8 SMC Programs
Database Manager	
— Aliases	Users > Mailing Lists
— Tnidb	Interface Manager
— Tnrhdb, Tnrhtp	Computers and Networks > Security families
Group Manager	Users > Groups
Host Manager	Computers and Networks
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 1–2 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 Trusted Solaris 7 to Trusted Solaris 8

Changes from Trusted Solaris 7 affect users, administrators, and developers. Changes are in the areas of:

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. Trusted Solaris 8 supports the name services that are fully supported in the Solaris 8 6/00 and Solaris Management Console 2.0 releases. The following lists the exceptions:

- Solaris Web Start is not supported

- Upgrade is not supported. However, administrators who want to retain Trusted Solaris database information (`tsoluser`, `tsolprof`, `tnrhdb`, `tnrhtp`) 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 Trusted Solaris 8. See the URL `http://www.sun.com/software/solaris/trustedsolaris/ts_tech_faq/` for the `tsolconvert` utility and procedure.
- The second installation CD-ROM is displayed in a text-only interface.
- The Solaris Management Console requires that the install team allocate approximately 148MB more swap to the host running the console. For example, if the previous swap was 256MB, the Trusted Solaris 8 swap should be at least 404MB.
- Installing and configuring the Sun Enterprise™ 10000 (E10000) 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 installation in Trusted Solaris 8 requires a customized JumpStart installation that calls a site-created script to install the file at `admin_high`.

Configuration Differences

See the topics below for the configuration differences. Of particular interest are “Security Policy” on page 18, “Labels” on page 16, “Roles” on page 18, “Auditing” on page 10, “Devices” on page 15 and “Trusted Networking” on page 19.

Auditing

Trusted Solaris 8, as well as Solaris 8, 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 Solaris 8. Therefore, Trusted Solaris 7 authorizations have been renamed in Trusted Solaris 8 to correspond to their Solaris 8 counterparts. See the file `/etc/security/auth_attr` for a full list of authorizations, and `auth_attr`(4) 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 1–3 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
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.*

TABLE 1–3 Authorizations 1 through 27 *(continued)*

No.	Trusted Solaris 7 Names	Trusted Solaris 8 Equivalents
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 1–4 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

TABLE 1–4 Authorization Numbers 28 through 55 *(continued)*

No.	Trusted Solaris 7 Names	Trusted Solaris 8 Equivalents
42	TSOL_AUTH_DB_TIMEZONE	None
43	TSOL_AUTH_DB_TNIDB	solaris.network.security.write
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 due to technical changes in the product and 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 14). The library functions for authorizations have also been replaced by Solaris functions, which have been extended for the Trusted Solaris environment. See

Table 1–6 for the database man page correspondences. The following table shows the function name man page correspondences.

TABLE 1–5 Trusted Solaris 8 Man Pages for User, Profile, and Authorization Functions

Trusted Solaris 7 Database Functions	Trusted Solaris 8 Man Page
getuserent, setuserent, getuserentbyname, getuserentbyuid, free_userent, enduserent	`getuserattr`(3secdb)
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 environment. Therefore, Trusted Solaris 8 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`.

Profiles are administered through the Solaris Management Console. The Profile Manager is now the Rights tool, under Users (the User Manager). The Rights tool does not recognize symlinked commands.

Profiles are now hierarchical. Profiles can subsume other profiles, though they do not have to. 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 1–6 Database Changes from Trusted Solaris 7 to Trusted Solaris 8

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 allocating within and without the trusted path. For security, Trusted Solaris software keeps track of the allocating username. The Device Allocation Manager GUI can display and edit the device_maps(4) entry for an allocatable device, and 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

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

The Label Builder used by administrators is now Java-based and accessed through the Solaris Management Console. Users are presented with the same Motif label builder as they were in Trusted Solaris 7.

In Trusted Solaris 8, 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, independent of the label of the original profile shell. This is a change to the profile shell from Trusted Solaris 7, although it 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 Trusted Solaris 8:

- `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 `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 has 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 1–7 Man Pages Newly Created or Modified for Trusted Solaris 8

Man Page Section	Man Page	
Section 1	`auths`(1) `crle`(1) `date`(1) `nca`(1) `ncakmod`(1)	`nispasswd`(1) `profiles`(1) `roles`(1)
Section 1M	`coreadm`(1M) `devfsadm`(1M) `init.wbem`(1M) `mkdevalloc`(1M) `mkdevmaps`(1M) `nisclient`(1M) `pkgchk`(1M) `rmmount`(1M), `rpc.yppasswdd`(1M) `rpc.ypupdated`(1M) `su`(1M) `ypbind`(1M) `ypserv`(1M) `ypxfr`(1M)	`smc`(1M) `smcron`(1M) `smexec`(1M) `smgroup`(1M) `smhost`(1M) `smmaillist`(1M) `smmultisuer`(1M) `smnetidb`(1M) `smnettmpl`(1M) `smnetwork`(1M) `smuser`(1M)
Section 2	`acct`(2)	
Section 3	`getauthattr`(3SECDB) `getauusernam`(3BSM)	`grantpt`(3C)
Section 4	`exec_attr`(4) `logindevperm`(4) `nca.if`(4) `policy.conf`(4)	`prof_attr`(4) `shadow`(4) `user_attr`(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

Trusted Solaris 8 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 Trusted Solaris 8 there are five recommended roles. Only the root role is provided on the installation CD-ROM. 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 Trusted Solaris 8 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. 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 (label defaults are set in the `label_encodings` file).

Trusted Solaris 7 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` is administered using the Interface Manager program. The `tnrhtp` and `tnrhdb` databases are administered using the Security Families program. All trusted networking databases are extended to handle IPv6, and the `tnrhdb` handles variable-length netmasks.

Trusted Solaris 8 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 in the `tnrhtp` database has been removed.

The following fields have been removed from the `tnrhtp` templates. For interoperability, they 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 1–8 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`, 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 Trusted Solaris 8 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 `tnd` 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
```