



# Trusted Solaris 7 Transition Guide

---

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

Part Number 805-8059  
November 1999

Copyright 1999 Sun Microsystems, Inc. 901 San Antonio Road, Palo Alto, California 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, Solstice AdminSuite, 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 1999 Sun Microsystems, Inc. 901 San Antonio Road, Palo Alto, Californie 94303-4900 Etats-Unis. 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, Trusted Solaris, Solstice AdminSuite, 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.



# Preface

---

The *Trusted Solaris 7 Transition Guide* describes the differences between Trusted Solaris 2.5.1 and Trusted Solaris 7. For the details of procedures that have changed, refer to the appropriate book in the Trusted Solaris 7 document set.

---

## Who Should Use This Book

The *Trusted Solaris 7 Transition Guide* is designed to enable users of Trusted Solaris 2.5.1, Solaris 2.5.1, and Solaris 7 to find their way around the Trusted Solaris 7 operating environment more easily. All users should find the book useful.

---

## How This Book Is Organized

Chapter 1 provides an overview and details of the differences. At the end of the chapter are summaries of interface changes from Trusted Solaris 2.5.1 to Trusted Solaris 7.

---

## 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*. It is available online at the docs.sun.com<sup>SM</sup> Web site in the *Trusted Solaris 2.5.1 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<sup>SM</sup> 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>.

---

## Typographic Conventions

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.
<b>AaBbCc123</b>	What you type, contrasted with on-screen computer output	<code>machine_name%</code> <b>su</b> Password:
<i>AaBbCc123</i>	Command-line placeholder: replace with a real name or value	To delete a file, type <b>rm</b> <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.



## Transition to Trusted Solaris 7

---

Trusted Solaris 7 is a security-enhanced version of the Solaris 7 operating environment. It upgrades Trusted Solaris 2.5.1 software, and includes:

- “Trusted Solaris 7 Changes to SunOS 5.7 (Solaris 7)” on page 7
- “Trusted Solaris 7 Changes to CDE 1.3” on page 9
- “Trusted Solaris 2.5.1 Changes to Solstice AdminSuite 2.3” on page 9
- “Changes from Trusted Solaris 2.5.1 to Trusted Solaris 7” on page 9
- “Trusted Solaris 7 Changes to Support the Sun Enterprise 10000 and Intel Platform” on page 8

Trusted Solaris 7 runs on hardware that was unsupported in Trusted Solaris 2.5.1:

- Intel architecture is supported.
- The Sun Enterprise™ 10000, a sun4u machine, is supported.

---

## Trusted Solaris 7 Changes to SunOS 5.7 (Solaris 7)

Unless explicitly stated otherwise, Trusted Solaris 7 supports the new features in the Solaris 7 release, such as 64-bit support and Sendmail version 8.8.8. The following Solaris 7 features function differently in the Trusted Solaris environment:

- Network printers use sockets, not pipes. See “Printing” on page 12 for more information.

- Trusted Solaris 7 does not update the Solaris `SUNWrdm` package. For late-breaking news, see the *Trusted Solaris 7 Release Notes*.
- The Trusted Solaris version of the Solaris 7 `traceroute(1M)` command follows Trusted Solaris security policy. The doors interfaces from Solaris 7 are enhanced for security; see the man pages `door_create(3x)` and `door_tcred(3x)`.
- The following Solaris interfaces are not supported in Trusted Solaris 7:
  - `bsmconv(1M)` and `bsmunconv(1M)`
  - `rexecd(1M)`
  - `rusers(1)`
  - `spell(1)`
  - `talk(1)`

---

## Trusted Solaris 7 Changes to Support the Sun Enterprise 10000 and Intel Platform

To run securely on the Sun Enterprise 10000 and on the Intel platform, Trusted Solaris 7 enhances installation and administration for security.

For the Sun Enterprise 10000:

- For remote (headless) workstation administration, see the new `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 7 Reference Manual*.
- There is no command line login. Administration of a newly installed Sun Enterprise 10000 is done remotely, using CDE. See the *Trusted Solaris Installation and Configuration for the Sun Enterprise 10000 Guide*.

For the Intel Platform:

- There is no WebStart installation.
- The equivalent of protecting the PROM on Intel is to protect the BIOS.



---

## Trusted Solaris 7 Changes to CDE 1.3

Trusted Solaris 7 supports the new features in the CDE 1.3 release, such as the new front panel configuration, 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 1.3 function more securely in the Trusted Solaris environment, and are available in the System\_Admin folder:

- Front panel device actions, such as Open Floppy and Open CD-ROM are protected by device allocation. The Trusted Solaris Device Allocation Manager is available from the Trusted Desktop subpanel.
- The System\_Admin folder contains more administrative actions than in Trusted Solaris 2.5.1.

---

**Note** - The Application Manager is now invoked from the Applications subpanel on the left side of the front panel. A terminal can be invoked from the Workspace menu, a right-button menu from the workspace background.

---

---

## Trusted Solaris 2.5.1 Changes to Solstice AdminSuite 2.3

Trusted Solaris 7 retains the Trusted Solaris 2.5.1 security enhancements to the Database Manager (tnrhdb, tnrtcp, tnrtb) and User Manager, and retains the Profile Manager, which enables the security administrator to administer execution profiles. Trusted Solaris 7 made no further enhancements to the databases in the Solstice\_Apps folder.

---

## Changes from Trusted Solaris 2.5.1 to Trusted Solaris 7

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

- “Authorization and Privilege Differences” on page 15
- “Commands and Functions” on page 12
- “File Systems and Mounting” on page 14
- “Labels” on page 11
- “Installation and Configuration” on page 10
- “Login and Remote Login” on page 14
- “Man Pages” on page 13
- “Printing” on page 12
- “System Start and Shutdown” on page 14

## Installation and Configuration

Trusted Solaris 2.5.1 installation included labels configuration. In Trusted Solaris 7, the install team configures labels after installation.

### Installation Differences

Installation on most hardware is identical to Solaris 7 installation. The two exceptions are:

- Solaris™ Web Start is not supported
- The Sun Enterprise™ 10000 (E10000), also called Starfire™, is installed for Trusted Solaris security. See *Trusted Solaris Installation and Configuration for the Sun Enterprise 10000 Guide* for complete information.

Solaris installation features that Trusted Solaris 7 supports include:

- Trusted Solaris network and jumpstart installations are identical to Solaris network and jumpstart installations.
- `sys-unconfig(1M)` is supported.
- Unlike Trusted Solaris 2.5.1 installation, Trusted Solaris 7 installation does not offer label configuration options; sensitivity labels are configured after installation, not during. Therefore, the `config_data` file and its corresponding man page do not exist since there are no Trusted Solaris configuration options for network installations.

## Configuration Differences

To change default label configuration values, the security administrator edits the `/etc/system` file.

To enable the Stop-A shutdown mechanism, the security administrator edits the `/etc/default/kbd` file.

The `Check Encodings System_admin` action enables an administrative role to install a site-specific `label_encodings` file.

## Labels

Trusted Solaris 7 does not configure labels during installation (see “Installation and Configuration” on page 10, documents how to create many compartments in labels, and does not support information labels.

## Large Numbers of Compartments

“Bits Available for Classification and Compartment Components” in *Trusted Solaris Label Administration* documents how to create and manage large numbers of compartments in a `label_encodings` file.

## Information Labels

Information labels (ILs) are not supported in Trusted Solaris 7 and later releases. Trusted Solaris software interprets any ILs on communications and files from systems running earlier releases as `ADMIN_LOW`.

Objects still have CMW labels, and CMW labels still include the IL component: `IL[SL]`; however, the IL component is fixed at `ADMIN_LOW`.

As a result, Trusted Solaris 7 has the following characteristics:

- ILs do not display in window labels; SLs (Sensitivity Labels) display alone within brackets.
- ILs do not float.
- Setting an IL on an object has no effect, and getting an object’s IL will always return `ADMIN_LOW`.
- Although certain utilities, library functions, and system calls can manipulate IL strings, the resulting ILs cannot be set on any objects.
- Sensitivity labels, not information labels, display on printer banners and body pages.
- Options related to information labels in the `label_encodings(4)` file can be ignored.

- IL-related privileges are no longer used. See “Authorization and Privilege Differences” on page 15 for a list.
- In auditing, the `ilabel` token is recorded as `ADMIN_LOW`, when it is recorded. The audit event numbers 519 (`AUE_OFLOAT`), 520 (`AUE_SFLOAT`), and 9036 (`AUE_iil_change`) continue to be reserved, but those events are no longer recorded.

## Printing

Adding Trusted Solaris security to Solaris 7 printing changed several things about printing in the Trusted Solaris environment.

- Additional printing authorizations handle printing capabilities. Trusted Solaris 7 checks authorizations where Trusted Solaris 2.5.1 checked for privilege. See “Authorization and Privilege Differences” on page 15.
- Network printers do trusted printing only when directly cabled to a Trusted Solaris print server.
- Network printers can be configured as standalone nodes on the network to print at a single label without labeled output, by assigning the printer an IP address and a host name. See *Trusted Solaris Administrator's Procedures* for the complete procedures.
- Users who print to a single-label printer from a trusted printer cannot list or delete the jobs in the queue.

## Commands and Functions

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

- The Pluggable Authentication Module (PAM) allows the customer to plug in a customized static randomword function.
- The following `/usr/proc/bin/` commands have a standard interface:
  - `pattr(1)`
  - `pclear(1)`
  - `plabel(1)`
  - `ppriv(1)`
- The Trusted Solaris 2.5.1 `mldstat( )` and `mldlstat( )` system calls are library routines in Trusted Solaris 7.
- The `runpd(1M)` command has a slightly changed setup procedure.

# Man Pages

Man pages are in a different format, have a different naming scheme, and can be viewed using AnswerBook2™ technology. Changes in product functionality have caused corresponding changes in the man pages.

- Man pages are in SGML (Standardized General Markup Language). The online man command handles SGML; printed output is in troff.
- Trusted Solaris man pages are part of the SUNWman package; therefore, the tsol extension is not used. To view man pages in the Trusted Solaris environment, use the same syntax as in the Solaris 7 environment:

```
man setfsattr
man -s2 chmod
man ls
```

- Answerbook technology is now browser-based. The Trusted Solaris 2.5.1 answerbook command (/usr/openwin/bin/answerbook) does not support this functionality. To view Sun's Solaris 7 and Trusted Solaris 7 documentation, use the command /usr/dt/bin/answerbook2, or choose the AnswerBook2 option from the Help menu on the Front Panel.
- The following man pages do not have Trusted Solaris specific modifications due to changes in installation:
  - install\_scripts(1M)
  - add\_install\_client(1M)
  - rm\_install\_client(1M)
  - setup\_install\_server(1M)
- The following man pages have been moved or added due to changes in functionality:
  - dtappsession(1) — Added to CDE man pages
  - mldstat(3) and mldlstat(3) — Moved from system calls to library routines.
  - door\_create(3x) and door\_tcred(3x) — Added Trusted Solaris security.
  - pam\_tp\_auth(5) and pam\_tsol(5) — Added Trusted Solaris security.
  - kbd(1) — Added Trusted Solaris security. See “System Start and Shutdown” on page 14.
- The following man pages have been removed due to changes in implementation:
  - config\_data(4TSOL)

- `msgrcv1(2TSOL)`
- `msgsnd1(2TSOL)`
- `semopl(2TSOL)`

## File Systems and Mounting

The Trusted Solaris 7 implementation of file system security attributes is similar to the Solaris 7 implementation instead of the Trusted Solaris 2.5.1 implementation. Instead of attributes stored on a filesystem inode, the operating system manages the filesystem security attributes. The new implementation has consequences for Trusted Solaris 7 administrators:

Mount-time security attributes may be specified either by using the `mount(1M)` command with the `-S` option on the command line or by specifying the attributes in the `vfstab_adjunct` file. Mount-time security attributes override existing security attributes on a file system. However, they never override security attributes on the files and directories within the file system. When access-control decisions are made, security attributes on a file or directory take precedence over security attributes specified either at the filesystem level or at mount time.

- Filesystem security attributes are not assigned using the `tsol_attr` flag; the flag has been removed.

## Login and Remote Login

The Enable Logins dialog box offers more choices to the user.

Roles now have the `remote login` authorization in a profile. The root role has it in the Maintenance and Repair profile. Remote logins by roles requires an additional step on every host where the roles need to remotely log in. See *Trusted Solaris Administrator's Procedures* for the procedure.

In Trusted Solaris 2.5.1, the value for `MAXBADLOGINS` was set by default to 3 was set in the `/etc/default/passwd` file. Trusted Solaris 7 follows the Solaris model: the default of 5 for the variable `RETRIES` is set in the `/etc/default/login` file.

## System Start and Shutdown

In Trusted Solaris 2.5.1, to enable a user to use the Stop-A sequence to bring down the computer, the administrator set the `abort_enable` keyword in the `/etc/system` file to 1. In Trusted Solaris 7, the administrator uncomments the `#KBD_ABORT=enable` line in the `/etc/default/kbd` file. By default, Stop-A is disabled.

# Authorization and Privilege Differences

The lists of authorizations and privileges have changed. There are new authorizations, removed privileges, and new privileges. Authorizations are now handled by number rather than by manifest constant.

The following authorizations have been added for the printing system:

- TSOL\_AUTH\_PRINT\_CANCEL
- TSOL\_AUTH\_PRINT\_LIST
- TSOL\_AUTH\_PRINT\_MAC\_OVERRIDE

The privilege PRIV\_SYS\_SYSTEM\_DOOR has been added.

The following IL-related privileges have been removed:

- PRIV\_FILE\_DOWNGRADE\_IL
- PRIV\_FILE\_NOFLOAT
- PRIV\_FILE\_UPGRADE\_IL
- PRIV\_IPC\_DOWNGRADE\_IL
- PRIV\_IPC\_NOFLOAT
- PRIV\_IPC\_UPGRADE\_IL
- PRIV\_NET\_DOWNGRADE\_IL
- PRIV\_NET\_NOFLOAT
- PRIV\_NET\_UPGRADE\_IL
- PRIV\_PROC\_NOFLOAT
- PRIV\_PROC\_SETIL
- PRIV\_WIN\_DOWNGRADE\_IL
- PRIV\_WIN\_NOFLOAT
- PRIV\_WIN\_UPGRADE\_IL