



Trusted Solaris 8 HW 12/02 Release Notes

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

Part No: 817-0877-10
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, Trusted Solaris, SunScreen, 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, Trusted Solaris, SunScreen, 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.



030327 @ 5533



Contents

Trusted Solaris 8 HW 12/02 Release Notes	5
Getting Help	6
Reading About the Changes and Features in the Trusted Solaris 8 HW 12/02 Release	6
Supported Hardware	7
Solaris Bug Fixes Incorporated Into This Release	7
Trusted Solaris 8 4/01 Bugs Fixed in This Release	9
Expanded Audit header Token	10
Known Problems With the Software	10
x86: Installation Difference Between the Trusted Solaris 8 4/01 Release and the Trusted Solaris 8 HW 12/02 Release	10
Enabling Smart Card Removes PAM Entries From pam.conf File (4827207, 4830611)	10
Languages CD Is Not Supported	11
Communication Between TSIX Host Types With IPsec AH Is Broken (4471447)	11
IKE Does Not Work With the TSOL Host Type (4548783)	11
nisaddent Causes a SIGSEGV Error When Adding to tnrhdb (4491941)	12
File System Label Ranges Are Not Enforced for Unlabeled NFS File Systems (4150441)	12
Graphical Window Manager Controls Do Not Work (4462771)	12
niscat Command Hangs and Spawns Multiple nisd Processes on an NIS+ Server (4430740)	13
Trusted Solaris Label Encodings File Requires Coding for ILs (4329208)	13
smossservice Command Fails to Create OS Server (4378498)	13
Drag-and-Drop Operations Do Not Work for OPEN LOOK Applications (4095021)	14
Nonexistent Location ID: FileManagerLabelsHelp (4477399)	14

Solaris Management Console Mounts and Shares Tools Do Not Set or Modify
Trusted Solaris Attributes (4496897) 14

Trusted Solaris 8 HW 12/02 Release Notes

Note – Read and use *Trusted Solaris Installation and Configuration* (PN 816–1040–10) to guide you in configuring the Trusted Solaris™ operating environment. The differences between a Trusted Solaris operating environment and a Solaris™ operating environment require planning and guidance during installation and configuration. Differences occur in labels, clearance confirmations, obligatory passwords, security configuration choices, name service domain setup, secure network setup, and no superuser.

The Trusted Solaris 8 HW 12/02 operating environment upgrades the Trusted Solaris 8 4/01 release. The operating environment also enhances the following software with security:

- Solaris 8 HW 12/02 operating environment
- X Windows, version 11.0
- CDE 1.4.8 (Common Desktop Environment)
- Solaris Management Console 2.0.0 administrative interface

The release incorporates patches that were released for the Trusted Solaris 8 4/01 operating environment. The release also incorporates patches to the window system, and patches for the Solaris, CDE, and the Solaris Management Console releases.

Note – As of this release, you can safely apply many patches that are available for the standard releases of Solaris software, CDE, X Windows, or the Solaris Management Console. Trusted Solaris software is repackaged to reflect differences from Solaris software packages only where such differences exist. Use the command `showrev -p` to list the patches that have been applied to the system.

The sections in this document are as follows:

- “Getting Help” on page 6
- “Reading About the Changes and Features in the Trusted Solaris 8 HW 12/02 Release” on page 6
- “Supported Hardware” on page 7
- “Solaris Bug Fixes Incorporated Into This Release” on page 7
- “Trusted Solaris 8 4/01 Bugs Fixed in This Release” on page 9
- “Known Problems With the Software” on page 10

Getting Help

For assistance in using the Trusted Solaris document set, see the *Trusted Solaris 8 HW 12/02 Roadmap* (PN 817-1392-10) document.

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>.

For additional information about the Trusted Solaris product, visit the <http://www.sun.com/trustedsolaris> web site.

Reading About the Changes and Features in the Trusted Solaris 8 HW 12/02 Release

Read the following books:

- *Trusted Solaris 8 HW 12/02 Release Notes* – This document. For bugs that have been fixed between the Trusted Solaris 8 4/01 and Trusted Solaris 8 HW 12/02 releases.
- *Trusted Solaris 8 HW 12/02 Transition Guide* – For changes from the Trusted Solaris 7, Trusted Solaris 8, and Trusted Solaris 8 4/01 releases to the current release. Also, for differences between the Trusted Solaris releases and their Solaris counterparts.
- *Solaris 8 2/02 What's New* – For features that the Trusted Solaris 8 HW 12/02 release inherits from the Solaris 8 software release.
- *Solaris 8 (SPARC Platform Edition) 2/02 Release Notes* – For information about the Solaris 8 software release.
- *Solaris 8 (Intel Platform Edition) 2/02 Release Notes* – For information about the Solaris 8 software release.

Supported Hardware

The Trusted Solaris 8 HW 12/02 release supports the workstation, server, and peripherals hardware supported by the Solaris 8 HW 12/02 release. See the following books:

- *Solaris 8 HW 12/02 Sun Hardware Platform Guide* in the Solaris 8 HW 12/02 on Sun Hardware Collection
- *Solaris 8 (Intel Platform Edition) 2/02 Hardware Compatibility List*

Solaris Bug Fixes Incorporated Into This Release

The Trusted Solaris 8 HW 12/02 release includes all product patches and bug fixes incorporated into the Solaris 8 HW 12/02 release. Use the `showrev -p` command to see the list of patches that are included in the release.

Additional bug fixes that are included in the Trusted Solaris 8 HW 12/02 release are listed in the following table. Most of the fixes are security bug fixes.

TABLE 1–1 Solaris Bug Fixes Incorporated Into the Trusted Solaris 8 HW 12/02 Release

Solaris Bug Number	Synopsis
1159193	<code>fmodsw</code> needs to be dynamically allocated
1255897	Arbitrary data attributes are being printed by <code>praudit</code> in a confusing way
1262891	<code>fbconsole</code> core dumps if incorrect permissions on <code>/tmp</code>
4059965	<code>praudit</code> has problems displaying paths with non-ASCII characters
4280870	<code>pcmcia</code> is writing a directory and file that is owned by <code>root</code>
4367223	In certain erroneous conditions the <code>mount ()</code> call leaves kernel locks held
4382410	“Missing message #18022” displays on front panel at installation
4397459	<code>*ed*</code> creates temporary files in an insecure manner
4457722	MLD general queries with maximum report delay of 0 can panic the Solaris x86 kernel

TABLE 1–1 Solaris Bug Fixes Incorporated Into the Trusted Solaris 8 HW 12/02 Release
(Continued)

Solaris Bug Number	Synopsis
4464517	RED State Exception on SB100/SB1000 while booting with Addonics USB DVD
4508268	praudit and auditreduce do not work with RBAC profile entries
4545809	mount () system call can panic machine
4545858	mount(2) man page is incorrect with several issues
4548739	Security vulnerability involving pmconfig
4617380	Panic: assertion failure pm_cfb_comps_off
4619275	pmconfig does not check bounds while processing user input
4619526	powerd does not check bounds while processing user input
4621278	IPv6 home address option has security concerns
4621760	ftp debug output includes passwords in clear text form
4649509	fdformat reads any file as boot sector
4649511	fdformat contains a race condition
4655066	crle: -u with nonexistent config file does not work
4661997	Buffer overflow in dbm_open ()
4664152	TPI connection response is extremely hazardous
4668699	Buffer overflow in dbm_open () and dbminit ()
4677620	Security issue in sysinfo ()
4680691	Doctored rpc calls over UDP can bring down machines through rpcbind
4702931	Ordinary user can panic machine using crafted /dev/arp messages
4708822	priocntl () can load a user module and gain access to system
4712864	TCP_IOC_ABORT_CONN leaks kernel memory
4725286	Panic: recursive rw_enter caused by sendfilev ()
4728754, 4777632	sad needs to validate input
4729683	modload () could do some checking before loading a module
4732677	TCP_IOC_ABORT_CONN leaks kernel memory
4737417	ypxfrd security issue with map handling
4737861	IP module allows an unprivileged process to generate raw IP packet

TABLE 1–1 Solaris Bug Fixes Incorporated Into the Trusted Solaris 8 HW 12/02 Release
(Continued)

Solaris Bug Number	Synopsis
4740832	fbconsole creates tmp files unsafely
4756570	sendmail does not handle some .forward constructs correctly
4763520	TCP accepts connection response queue in T_CONN_RES without validation
4756979	uucp contains a buffer overflow
4767276, 4778962	rpcbind can be killed remotely
4776480	at -r job name handling and race conditions
4777715	CERT Advisory CA-2002-31: Multiple Remote Vulnerabilities in BIND
4786593	pkgadd fails with size issue when space file is present
4788209	/usr/dt/bin/dtprintinfo \$HOME environment variable overflow
4788212	/usr/dt/bin/dtsession \$HOME environment variable overflow
4789120	Floating point operations in getfpregs () may cause unexpected traps
4790725	Port of patch 109896 to the Trusted Solaris release
4798301	Ordinary user can panic the Solaris x86 kernel
4804524	getfpregs () spuriously enables FPU on sparcv9
4809539	CERT Advisory CA-2003-07: Remote Buffer Overflow in Sendmail

Trusted Solaris 8 4/01 Bugs Fixed in This Release

The following bugs that are reported in the *Trusted Solaris 8 4/01 Release Notes* have been fixed in the Trusted Solaris 8 HW 12/02 software:

- praudit and auditreduce do not work with RBAC profile entries (4508276)
- Some suser () calls still exist in kernel (4493976)
- Device Allocation: Configuration dialog box does not configure the first device (4533649)

Expanded Audit header Token

The fix for bug, 4825056 host token doesn't support IPv6, changes the contents of the header audit token. See the *Trusted Solaris 8 HW 12/02 Transition Guide* for more information.

Known Problems With the Software

This section identifies known problems in the Trusted Solaris 8 HW 12/02 software, describes the problems, and suggests solutions. These bugs might or might not be fixed in a future release.

x86: Installation Difference Between the Trusted Solaris 8 4/01 Release and the Trusted Solaris 8 HW 12/02 Release

Trusted Solaris Installation and Configuration instructs the installer to remove the boot diskette.

Workaround: If you have booted from a CD-ROM and have not used a diskette, you can ignore the instruction. Leave the CD-ROM in the drive, let the system reboot, and remove the CD-ROM when instructed to. If you are doing an upgrade install, the system will not automatically reboot after the installation of the first CD.

Enabling Smart Card Removes PAM Entries From `pam.conf` File (4827207, 4830611)

The `smartcard -c enable` command updates the `pam.conf` file incorrectly. The result is that the user is unable to log in with a smart card.

Workaround: In the `secadmin` role, do the following steps:

1. Before configuring smart card, save the `/etc/pam.conf` file.

```
$ cp /etc/pam.conf /etc/pam.conf.orig
```
2. Configure smart card using the Smart Card Admin GUI. The executable is `/usr/dt/bin/sdtsmartcardadmin`.
3. Enable smart card with the following command:

```
$ smartcard -c enable
```

4. Before logging out, restore the `/etc/pam.conf` file.

```
$ cp /etc/pam.conf.orig /etc/pam.conf
```

5. Add the following lines to the `/etc/pam.conf` file.

You add lines that contain `pam_smartcard` for both `dtlogin` and `dtsession`. You append `'use_first_pass'` to the `dtlogin` and `dtsession` lines that contain `pam_unix`.

Note – The lines in the `pam.conf` file should not contain continuation characters. For display purposes, the lines below contain continuation (`\`) characters.

```
dtlogin auth requisite /usr/lib/security/$ISA/pam_smartcard.so.1
dtlogin auth requisite /usr/lib/security/$ISA/pam_tp_auth.so.1
dtlogin auth requisite /usr/lib/security/$ISA/pam_unix.so.1 \
  check_retries use_first_pass
...
dtsession auth requisite /usr/lib/security/$ISA/pam_smartcard.so.1
dtsession auth required /usr/lib/security/$ISA/pam_unix.so.1 \
  use_first_pass
```

When a patch is released, you can apply the patch to your system. Once the patch is applied, you do not need the workaround.

Languages CD Is Not Supported

This release supports only the C locale (U.S. English). Thus, no Languages CD is provided.

Communication Between TSIX Host Types With IPsec AH Is Broken (4471447)

Network packets that use the TSIX protocol are not processed correctly when AH headers are present.

Workaround: None.

IKE Does Not Work With the TSOL Host Type (4548783)

Network packets that are labeled with the TSOL protocol are not processed correctly by IKE in the SunScreen™ 3.2 product. The SunScreen log messages show `IKE_INVALID_COOKIE`.

The SunScreen software properly processes TSOL-labeled network traffic that is in clear text. The SunScreen IKE software also behaves correctly in the Trusted Solaris operating environment to protect traffic between unlabeled network connections.

Workaround: None.

nisaddent Causes a SIGSEGV Error When Adding to tnrhdb (4491941)

A SIGSEGV error is produced when using the `nisaddent -avf` command to add an incorrectly formatted file to the `tnrhdb` NIS+ map. The incorrectly formatted file produces a core dump.

Workaround: The `nisaddent` command works correctly with a valid input file. To ensure that the input file has fields separated by colons and not by spaces, use `niscat -s :` when dumping an NIS+ table that will be used later as input to NIS+.

File System Label Ranges Are Not Enforced for Unlabeled NFS File Systems (4150441)

This bug occurs in a very unusual situation. The administrator must have consciously configured an NFS remote host to be at one label, and the label range to be another label.

Workaround: To prevent the creation of files at the default label for the server, mount the file system as “read-only”. Existing files are unaffected, but the read-only mount option prevents the creation of files at a label outside the label range.

Graphical Window Manager Controls Do Not Work (4462771)

The new utilities `sdtgwm`, `sdtwsm`, and `sdtwinlst` and their corresponding actions in the `Desktop_Apps` folder generate errors, such as `Warning: Query Module Not Running`.

Workaround: None. These tools are inappropriate for users in the Trusted Solaris environment. Thus, the tools are not supported.

niscat Command Hangs and Spawns Multiple nisd Processes on an NIS+ Server (4430740)

The bug is known to occur when the Solaris Management Console is running on an NIS+ client or master and has loaded its toolbox from an NIS+ replica. Next, the replica is shut down and the Solaris Management Console is used to update any NIS+ maps. Since the machine from which the Solaris Management Console loaded its toolbox is down, the Solaris Management Console client has no way to communicate with the Solaris Management Console server, which is the machine from which the toolbox has been loaded.

Workaround: Do not use the Solaris Management Console to update NIS+ databases when an NIS+ replica is down. Use the standard NIS+ command-line interface instead.

Trusted Solaris Label Encodings File Requires Coding for ILs (4329208)

Although Trusted Solaris 8 4/01 software does not support information labels (ILs), the `chk_encodings` command fails with the following error if the `label_encodings` file omits information about ILs.

```
# chk_encodings label_encodings
Label encodings conversion error at line 37:
  Can't find INFORMATION LABELS specification.
  Found instead: "SENSITIVITY LABELS:".
label_encodings: label encodings syntax check failed.
```

Workaround: Copy a valid `SENSITIVITY LABELS:` section in your `label_encodings` file, and rename the section to `INFORMATION LABELS:`, as in:

```
INFORMATION LABELS:
...
WORDS:
...
REQUIRED COMBINATIONS:
...
COMBINATION CONSTRAINTS:
...
```

See the `label_encodings(4)` man page for more information.

smosservice Command Fails to Create OS Server (4378498)

The Solaris Management Console commands `smosservice` and `smdiskless` do not work correctly.

Workaround: Set up diskless service manually. On the OS server, name and allocate the client disk partitions during the installation process.

Drag-and-Drop Operations Do Not Work for OPEN LOOK Applications (4095021)

Drag-and-drop operations do not work reliably for OPEN LOOK applications.

Workaround: Use the copy and paste keys with OPEN LOOK applications.

Nonexistent Location ID: FileManagerLabelsHelp (4477399)

This bug is seen when you perform the following steps:

1. Insert diskette.
 floppy_0 is allocated by Device Allocation Manager.
2. From File Manager, click the File menu and select Removable Media Manager.
3. Select the diskette icon. Click mouse button 3 to open the Labels menu item.
4. In Removable Media Manager - File Labels (the Trusted Solaris Label Builder), click the Help button at bottom right of the dialog box.

Workaround: Perform the following steps:

1. Click mouse button 3 on the Front Panel and select Help from the menu. The Workspace Manager – Help window appears.
2. In the Workspace Manager – Help window, scroll down in the top pane to Trusted Solaris Applications and select that text.
3. In the bottom pane, click Create Labels.

Solaris Management Console Mounts and Shares Tools Do Not Set or Modify Trusted Solaris Attributes (4496897)

The Solaris Management Console Mounts tool and Solaris Management Console Shares tool do not manipulate Trusted Solaris attributes.

Workaround: Use the Set Mount Points action and the Share Filesystems action to handle Trusted Solaris attributes. You can also use the Admin Editor on the /etc/vfstab file and the /etc/dfs/dfstab file.