CHAPTER 2

Managing BTS Users and Commands Using EMS

Revised: July 2010, OL-23032-01

Introduction

This chapter describes operator interfaces to the BTS and how to manage access and users.

The Element Management System (EMS) database holds up to 256 logins and up to 50 active user sessions.Using the command line interface (CLI) you can locally connect to the EMS in an interactive session.The EMS system administrator can:

- Add a new user.
- Assign a user's privilege level—10 is for the system administrator. BTS has predefined user accounts:

Username		Permission
btsadmin	btsadmin	like MAINT shell user—MAINT shell is an enhanced CLI interface and does not log off an idle user)
secadmin	secadmin	like MAINT shell user
btsuser	btsuser	lower access permissions than btsadmin and secadmin, good for generic provisioning access

- Reset a user's password.
- Enter a description for each security class and privilege level.
- Manage security log reporting.

Logging into the EMS Using CLI

SSH is a way to access the BTS CLI or maintenance (MAINT) modes. SSH provides encrypted communication between a remote machine and the EMS/CA for executing CLI or MAINT commands. The SSH server runs on EMSs and CAs. To connect the client and server sides run the secure shell daemon (SSHD). With SSH, new users must enter a new password and reenter that password during the first login. In future logins they are prompted once for a password only.

The “ciscouser” login is a high-level security login for TAC and other BTS support personnel that restricts access to certain commands. Anyone else trying to execute such commands receives an error message.

After installation, on the EMS, the system prompts you to change the passwords of **root**, **btsadmin**, **btsuser** and **calea** if they have default passwords. On the CA, the system prompts you to change the passwords of **root** if it has default password. There are no default passwords for Operations, Administration and Maintenance applications.

When logging in for the first time system administrators log in as **btsadmin** (the default password is **btsadmin**). Change the password.

Step 1 To log in from the client side for the first time: **ssh btsadmin@<ipaddress>** .

Note If you are logged in to the system as **root**, enter: **btsadmin@0**

On the first SSH login from the client side, expect a message like this:

```
The authenticity of host [hostname] can't be established.
Key fingerprint is 1024 5f:a0:0b:65:d3:82:df:ab:42:62:6d:98:9c:fe:e9:52.
Are you sure you want to continue connecting (yes/no)?
```

Step 2 Enter **yes**.

The password prompt appears, now all communications are encrypted.

Step 3 Enter your password.

The system responds with a CLI> prompt. You can now send commands to the EMS.

Step 4 Enter provisioning commands.

Step 5 To log off, enter **exit** .

Managing Users

You must have a user privilege level of 9 or higher to add, show, change, or delete a user.

Caution Do not add, change, or delete username **root**, this prevents proper EMS access.

Table 2-1 Managing Users

Task	Sample Command
Adding a user	1. **add user name=UserABC; command-level=9; warn=10; days-valid=30; work-groups=somegroup;** 2. Supply a default password: **reset password name=<user name>; new-password=<user password>;**
Viewing a user	**show user name=UserABC;**

Table 2-1 Managing Users (continued)

Task	Sample Command
Viewing user activity	**show ems;**
Changing a user	**change user name=UserABC; command-level=1; work-groups=somegroup;**
Deleting a user	**delete user name=UserABC;** You cannot delete **optiuser**.
Changing a user's password	**reset password name=username; days-valid=<number of days the new password will be valid>; warn=<number of days before password expiration to warn user>;** **reset password name=username; days-valid=30; warn=4;** A password must: • Have 6-8 characters • Have at least two alphabetic characters • Have at least one numeric or special character • Differ from the user's login name and any combination of the login name • Differ from the old password by at least three characters Change the password for user **optiuser** on each BTS.
Adding a new work-group	**change command-table noun=mgw; verb=add; work-groups=latex;**
Adding a user to a work-group	**change user name=trs80nut; work-groups=+rubber;**
Removing a user from a work-group	**change user name=trs80nut; work-groups=-latex;**
Viewing all currently active users	**show session**
Viewing an active user	**show session terminal**

Table 2-1 Managing Users (continued)

Task	Sample Command
Blocking an active user	1. Select operation mode: • MAINTENANCE—(default) for regular maintenance • UPGRADE—for upgrades 2. `block session terminal=USR16;` **Note** You cannot block the session of a user with higher privileges than yours. Prevent BTS provisioning during an upgrade or maintenance window from the following interfaces: • CLI • FTP • CORBA • SNMP **Note** The software will support blocking HTTP interfaces in a future release. If you block provisioning before performing an SMG restart or EMS reboot, blocking is still enforced when these applications return to in-service state. There are two levels of blocking: • PROVISION—Prevents all provisioning commands from executing • COMPLETE—Prevents all commands from executing Only terminal type MNT users can use these blocking and unblocking commands. MNT users are never blocked. MNT users issue these commands from either active or standby EMS. A blocking command applies to all non-MNT users on terminals on either active or standby EMS. Commands do not execute for: • Logged-in users • Users who login after the block command Commands are not queued for execution after unblock. The CLI user prompt changes when blocked, notifying the user their commands will not execute.
Unblocking a user	`unblock session terminal=USR16;` **Note** You cannot unblock the session of a user with higher privileges.
Resetting a user's idle time	Idle time is how many minutes (1-30) a user can be idle before being logged off the BTS. `change session idle-time=30;`
Stopping a user's session	`stop session terminal=USR16;`

Note All commands should be assigned to a work-group. If a command is not assigned to a work-group, a user will able to execute that command, which is not recommended. You can also assign users and the commands to multiple work-groups.

Managing Commands

Each command (verb-noun combination) has a security class of 1-10; 1 is lowest, 10 is highest. Each time a user enters a command, the system compares the user's privilege level to the command's security class. EMS denies the command if the user level is less than the command level.

The Command Level (command-level) table shows the 10 command security classes. BTS has the following presets:

- 1 (lowest level)
- 5 (mid-level)
- 10 (highest level)—These commands require a system administrator with a security level of 10 to execute.

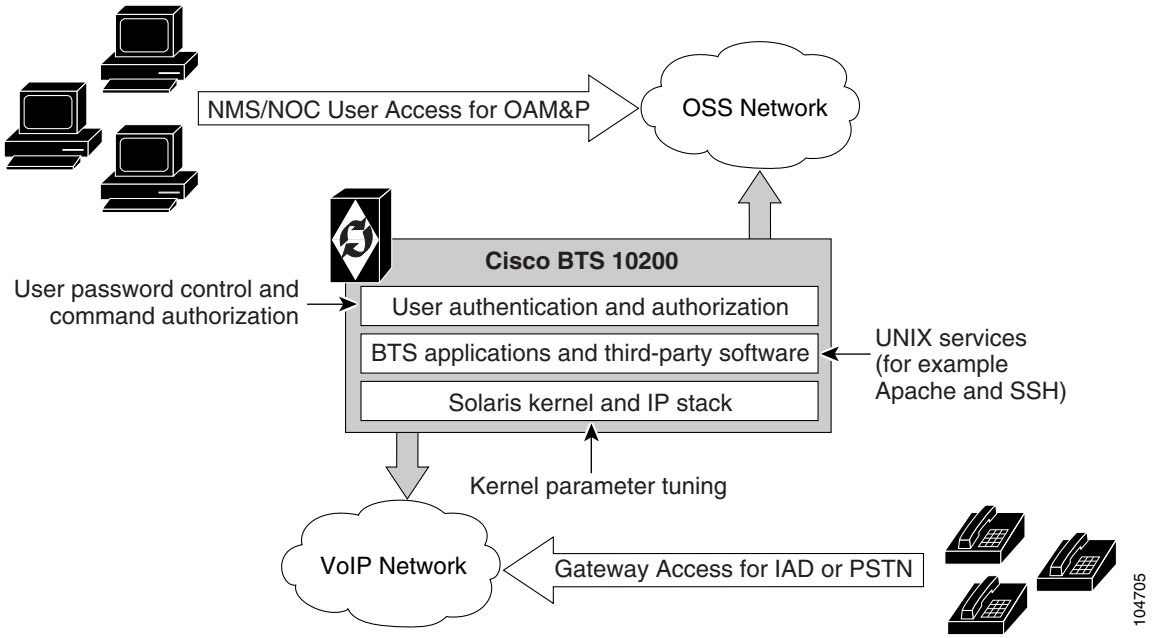
Table 2-2 Managing Commands

Task	Sample Command
Viewing a command's security class	`show command-level id=10;`
Adding a description to a command's security class	`change command-level id=10; description=This is the highest level administration access;`
Changing a command's privilege level	`change command-table noun=mgw; verb=add; sec-level=9;`
Resetting a command's privilege level	`reset command-table noun=mgw; verb=add;`
Viewing all executed commands	`show history;`
Sending all executed commands to a report file	`report history;` **Note** Results may take a few minutes to display.
Viewing the report of all executed commands	1. In a web browser enter http://server name. 2. Click Reports. 3. Click history.html.
Viewing a security summary	`report security-summary start-time=2002-09-26 00:00:00; end-time=2002-09-27 00:00:00; source=all;` **Note** Results may take a few minutes to display.
Viewing security summary reports	In a web browser enter https:// <ems ip addr>.

This chapter details the behaviors and attributes of the various security packages in the BTS 10200. The sources for the items are derived from many dynamic sources. Included in these sources are security bulletins from third-party vendors to the BTS 10200 as well as security agencies and open source organizations.

Security is an important part of the BTS 10200. The BTS 10200 has interfaces to customer premise equipment (CPE) as well as northbound Operations Support System (OSS) interfaces. All of these interfaces are subject to attacks. In addition, users who are allowed onto the BTS 10200 can also find ways to exploit applications that can lead to service-affecting situations. Therefore, many precautions are taken to ensure the solidity of the BTS 10200 defenses while avoiding a system that is difficult to manage.

Figure 2-1 BTS 10200 Access and Related Security



Adapter and User Security

This section describes requirements that generally involve adapter and user level of security. In the BTS 10200, adapters are any external, northbound interfaces of the BTS 10200. However, some extrapolated requirements involve adapter technology based on the current deployment:

- Support termination of a session once a provisionable inactivity timeout has occurred. An event report is issued upon each timeout expiry. The inactivity time ranges from 10 to 30 minutes.
- Restrict access as “root” to the BTS 10200 in all cases except Cisco TAC and customer “administrator”. This is a broad statement that includes the addition of command-line interface (CLI) commands to help manage the system. In addition, UNIX services are restricted to harden the operating system (OS). The service restriction is listed in the Solaris OS Security and BTShard Package section. The process of restricting root access is an ongoing process.
- Use of “sudo" is acceptable and the formal Sun-built and packaged version is located in /opt/sfw/bin/.

Solaris OS Security and BTShard Package

This section details the security packages for the BTS 10200 OS. These packages are automatically installed at installation. These packages are derived from both Sun Microsystems security bulletins and Cisco internal policies for safety of the OS and its applications. All services can be reactivated for the lifetime of the current kernel instance. All settings are reset on reboot of the kernel. These settings are contained in the BTShard Solaris package delivered with the BTS 10200.

- Remove unnecessary UNIX systems services. These services are listed below. Management of these facilities must allow for each service to be enabled or disabled on an individual basis. This service management must also be accomplished through the BTS 10200 adapter interface.
  - FTP—FTP server is disabled and SFTP (Secure FTP) should be used. This impacts the Bulk Data Provisioning interface. It does not impact the Billing Bulk Data transfer. The FTP client code will still be available on the EMS node.
  - Telnet—This terminal protocol is disabled and SSH (Secure Shell) should be used. The telnet server and client code are still available on the EMS node.
  - Echo—This service is to be disabled. This capability has been replaced with Internet Control Message Protocol (ICMP) “ping” facilities.
  - Discard—This service is to be disabled.
  - Printer—This service is to be disabled. No printer services are supplied in the BTS 10200 product description.
  - Daytime—This service is to be disabled.
  - Chargen—This service is to be disabled.
  - SMTP—This service is to be disabled.
  - Time—This service is to be disabled.
  - Finger—This service is to be disabled. No network user facilities are required. The BTS 10200 tracks users internally and on a single BTS basis.
  - Sun RPC—This service is to be disabled. This may be enabled in a lab environment for Tooltalk usage in debugging application programs.
  - Exec—This service is to be disabled.
  - Login—This service is to be disabled.
  - Shell—This service is to be disabled. This may be required for some lab activity; however, there is no field usage for rlogin, rcp, and rsh facilities.
  - UUCP—This service is to be disabled.
  - NFS—This service is to be disabled.
  - Lockd—This service is to be disabled.
  - X11—This service is available for the near term *only*.
  - DTSCP—This service is to be disabled.
  - Font-services—This service is to be disabled.
  - HTTP—This service is to be enabled. This is used by the BTS 10200 to offer results of report generation. This will migrate to HTTPS.

- The following UNIX accounts are to be LOCKED but not removed from the system: lp, uucp, nuucp, nobody, listen, and any other Cisco support accounts not used in the normal course of field operation. Services managed by root are the only accounts allowed to utilize one of these identities. This is the default behavior.
- Modifications to the Solaris kernel parameters were made to close potential breeches in the OS. These types of security precautions are most often geared toward "denial of service" attacks. These types of attacks create situations that degrade the performance of a system and as a result, prohibit the critical applications from delivering the service they are designed to provide.
- The TCP protocol uses random initial sequence numbers.
- All failed login attempts are logged.
- The following users are not allowed direct FTP access to the machine: root, daemon, bin, sys, adm, nobody, and noaccess.
- A root user cannot telnet directly to the machine. Direct root user access is granted to the console only. A user who wants to access the root account must use the **su** command from a nonprivileged account.
- The break key (<STOP> <A>) on the keyboard is disabled.
- IP_FORWARD_DIRECTED_BROADCASTS—This option determines whether to forward broadcast packets directed to a specific net or subnet, if that net or subnet is directly connected to the machine. If the system is acting as a router, this option can be exploited to generate a great deal of broadcast network traffic. Turning this option off helps prevent broadcast traffic attacks. The Solaris default value is 1 (True). For example:

  ```
  ip_forward_directed_broadcasts=0
  ```

- IP_FORWARD_SRC_ROUTED—This option determines whether to forward packets that are source routed. These packets define the path the packet should take instead of allowing network routers to define the path. The Solaris default value is 1 (True). For example:

  ```
  ip_forward_src_routed=0
  ```

- IP_IGNORE_REDIRECT—This option determines whether to ignore the ICMP packets that define new routes. If the system is acting as a router, an attacker may send redirect messages to alter routing tables as part of sophisticated attack (man-in-the-middle attack) or a simple denial of service. The Solaris default value is 0 (False). For example:

  ```
  ip_ignore_redirect=1
  ```

- IP_IRE_FLUSH_INTERVAL—This option determines the period of time at which a specific route will be kept, even if currently in use. Address Resolution Protocol (ARP) attacks may be effective with the default interval. Shortening the time interval may reduce the effectiveness of attacks. The default interval is 1200000 milliseconds (20 minutes). For example:

  ```
  ip_ire_flush_interval=60000
  ```

- IP_RESPOND_TO_ADDRESS_MASK_BROADCAST—This option determines whether to respond to ICMP netmask requests, typically sent by diskless clients when booting. An attacker may use the netmask information for determining network topology or the broadcast address for the subnet. The default value is 0 (False). For example:

  ```
  ip_respond_to_address_mask_broadcast=0
  ```

- IP_RESPOND_TO_ECHO_BROADCAST—This option determines whether to respond to ICMP broadcast echo requests (ping). An attacker may try to create a denial of service attack on subnets by sending many broadcast echo requests to which all systems will respond. This also provides information on systems that are available on the network. The Solaris default value is 1 (True). For example:

  ```
  ip_respond_to_echo_broadcast=1
  ```

- IP_RESPOND_TO_TIMESTAMP—This option determines whether to respond to ICMP timestamp requests, that some systems use to discover the time on a remote system. An attacker may use the time information to schedule an attack at a period of time when the system may run a cron job (or other time-based event) or otherwise be busy. It may also be possible predict ID or sequence numbers that are based on the time of day for spoofing services. The Solaris default value is 1 (True). For example:

  ```
  ip_respond_to_timestamp=0
  ```

- IP_RESPOND_TO_TIMESTAMP_BROADCAST—This option determines whether to respond to ICMP broadcast timestamp requests, that are used to discover the time on all systems in the broadcast range. This option is dangerous for the same reasons as responding to a single timestamp request. Additionally, an attacker may try to create a denial of service attack by generating many broadcast timestamp requests. The default value is 1 (True). For example:

  ```
  ip_respond_to_timestamp_broadcast=0
  ```

- IP_SEND_REDIRECTS—This option determines whether to send ICMP redirect messages, that can introduce changes into the routing table of the remote system. It should only be used on systems that act as routers. The Solaris default value is 1 (True). For example:

  ```
  ip_send_redirects=0
  ```

- IP_STRICT_DST_MULTIHOMING—This option determines whether to enable strict destination multihoming. If this is set to 1 and ip_forwarding is set to 0, then a packet sent to an interface from which it did not arrive will be dropped. This setting prevents an attacker from passing packets across a machine with multiple interfaces that is not acting a router. The default value is 0 (False). For example:

  ```
  ip_strict_dst_multihoming=1
  ```

- TCP_CONN_REQ_MAX_Q0—This option determines the size of the queue containing half-open connections. This setting provides protection from SYN flood attacks. Solaris 2.6 and 7 (and 2.5.1 with patch 103582-12 and higher) include protection from these attacks. The queue size default is adequate for most systems but should be increased for busy web servers. The default value is 1024. For example:

  ```
  tcp_conn_req_max_q0=4096
  ```

- The following startup files are removed from the level “3” runtime environment of the BTS 10200. These services can still be started manually if required in laboratory circumstances. They are not required for field operations.
  - S71rpc
  - S73cachefs.daemon
  - S73nfs.client
  - S74autofs
  - S80lp
  - S80spc

- S88sendmail
- S93cacheos.finish
- S99dtlogin

Operator Interface

Additional commands have been added to manage the UNIX services in the BTS 10200. These commands are available from the CLI/MAINT interface. In addition, these same commands are also available from the CORBA and bulk-provisioning interface. There are no schemas and tables associated with these commands. They directly control the UNIX services. These services are only enabled for the lifetime of the current kernel instance. They are reset to the installed defaults when a kernel reboot is performed.

Table 2-3 describes the system services available using the node command.

Table 2-3 Node Command for UNIX Services

Noun	Verb	Options	Description
Node	Change	SERVICE [Required] Must be one of the following: FTP, TELNET, ECHO, DISCARD, PRINTER, DAYTIME, CHARGEN, SMTP, TIME, FINGER, SUNRPC, EXEC, LOGIN, SHELL, UUCP, NFS, LOCKD, X11, DTSCP, FONT-SERVICES, HTTP.	Defines the service to change.
Node	Change	ENABLE [Required]	A Boolean flag [Y/N] that indicates whether to turn this service on or off.
Node	Change	NODE [Required]	The node name in the BTS 10200 where the service is managed.

Table 2-3 Node Command for UNIX Services (continued)

Noun	Verb	Options	Description
Node	Show	SERVICE [Required] Must be one of the following: FTP, TELNET, ECHO, DISCARD, PRINTER, DAYTIME, CHARGEN, SMTP, TIME, FINGER, SUNRPC, EXEC, LOGIN, SHELL, UUCP, NFS, LOCKD, X11, DTSCP, FONT-SERVICES, HTTP.	Defines the service to display.
Node	Show	Node [Required]	Defines the node to display for the state of the service.

Vulnerabilities in H.323 Message Processing

During 2002 the University of Oulu Security Programming Group (OUSPG) discovered a number of implementation-specific vulnerabilities in the Simple Network Management Protocol (SNMP). Subsequent to this discovery, the National Infrastructure Security Coordination Centre (NISCC) performed and commissioned further work on identifying implementation specific vulnerabilities in related protocols that are critical to the United Kingdom Critical National Infrastructure. One of these protocols is H.225, that is part of the H.323 family and is commonly implemented as a component of multimedia applications such as Voice over IP (VoIP).

OUSPG produced a test suite for H.225 and employed it to validate their findings against a number of products from different vendors. The test results have been confirmed by testing performed by NISCC and the affected vendors contacted with the test results. These vendors' product lines cover a great deal of the existing critical information infrastructure worldwide and have therefore been addressed as a priority. However, the NISCC has subsequently contacted other vendors whose products employ H.323 and provided them with tools with which to test these implementations.

Authentication, Authorization and Accounting Support

These extensions represent modifications to the current scheme of user account management on the system. It includes support for the following two protocols; these protocols are not required to be mutually inclusive.

- Radius Protocol
- Lightweight Directory Access Protocol (LDAP)

Prior to Release 4.4, user account management for the BTS 10200 used the standard Solaris password management facilities without the use of the Authentication Dial-In User Service Network Information Service (NIS). All accounts are stored locally and referenced locally. This security feature begins support for a complete AAA model for user account management. This model impacts several internal subsystems of the BTS 10200 Element Management System (EMS) application. It also impacts the core login support on the other nodes of the BTS 10200.

Pluggable Authentication Module Support

The BTS 10200 deploys a Secure Shell (SSH) package with Pluggable Authentication Module (PAM) support. The package includes the PAM support required to utilize the Radius and LDAP servers.

The supporting configuration allows local accounts to fall through if the Radius and LDAP servers are not available. These default local accounts for the BTS 10200 are the btsuser, btsadmin and secadmin accounts. These are the standard default accounts provided in the base product and use the native password management.

A UNIX-based user provides access to the operating system on all nodes. The oamp user is defined for package management purposes. The account is locked and no password is available. However, to grant UNIX access to all nodes of the BTS 10200, a default password is provided.

When PAM support is used, SSH transfers the control of authentication to the PAM library, that then loads the modules specified in the PAM configuration file. Finally, the PAM library tells SSH whether the authentication was successful. SSH is not aware of the details of the actual authentication method employed by PAM. Only the final result is of interest.

User Security Account Management

The BTS 10200 EMS contains an application program known as User Security Management (USM). This program determines if an account is local or off-board. Password management facilities are disabled for all accounts on the BTS 10200 when an AAA deployment is configured. The AAA deployment transfers the responsibility for these existing facilities to the end-user AAA servers. These facilities include the following attributes:

- Password aging, warning, and expiration
- Password reset and automatic account locking
- Local account management (password and shadow files) for new accounts

Sun Microsystems Configurations

Table 2-4 lists the Solaris 10 architecture-specific or hardware specific packages for certain Sun Microsystems configurations.

Table 2-4 Solaris Architectural- or Hardware-Specific Optional Package List

Package	Description	Type	Status
SMEvplr	SME platform links	SYSTEM	—
SMEvplu	SME usr/platform links	SYSTEM	—
SUNWaudd	Audio drivers	SYSTEM	—
SUNWauddx	Audio drivers (64-bit)	SYSTEM	—
SUNWced	Sun GigaSwift Ethernet Adapter (32-bit driver)	SYSTEM	—
SUNWcedx	Sun GigaSwift Ethernet Adapter (64-bit driver)	SYSTEM	—
SUNWcg6	GX (cg6) device driver	SYSTEM	—
SUNWcg6x	GX (cg6) device driver (64-bit)	SYSTEM	—
SUNWcsd	Core Solaris devices	SYSTEM	—

Table 2-4 Solaris Architectural- or Hardware-Specific Optional Package List (continued)

Package	Description	Type	Status
SUNWdfb	Dumb Frame Buffer device drivers	SYSTEM	—
SUNWensqr	Ensoniq ES1370/1371/1373 Audio device driver (32-bit) (Root)	SYSTEM	—
SUNWensqx	Ensoniq ES1370/1371/1373 Audio device driver (64-bit) (Root)	SYSTEM	—
SUNWeridx	Sun RIO 10/100 Mb Ethernet drivers (64-bit)	SYSTEM	—
SUNWfcip	Sun FCIP IP/ARP over FibreChannel device driver	SYSTEM	—
SUNWfcipx	Sun FCIP IP/ARP over FibreChannel device driver (64-bit)	SYSTEM	—
SUNWfcp	Sun FCP SCSI device driver	SYSTEM	—
SUNWfcpx	Sun FCP SCSI device driver (64-bit)	SYSTEM	—
SUNWfctl	Sun Fibre Channel Transport layer	SYSTEM	—
SUNWfctlx	Sun Fibre Channel Transport layer (64-bit)	SYSTEM	—
SUNWfruid	FRU ID prtfru Command and libfru library	SYSTEM	—
SUNWfruip	FRU ID Platform Data module and Access libraries	SYSTEM	—
SUNWfruix	FRU ID library (64-bit)	SYSTEM	—
SUNWged	Sun Gigabit Ethernet Adapter driver	SYSTEM	—
SUNWglmr	rasctrl environment monitoring driver for i2c (Root) (32-bit)	SYSTEM	—
SUNWglmx	rasctrl environment monitoring driver for i2c (Root) (64-bit)	SYSTEM	—
SUNWi2cr	device drivers for I2C devices (Root, 32-bit)	SYSTEM	—
SUNWi2cx	device drivers for I2C devices (Root, 64-bit)	SYSTEM	—
SUNWidecr	IDE device drivers	SYSTEM	—
SUNWidecx	IDE device drivers (Root) (64bit)	SYSTEM	—
SUNWider	IDE device driver (Root)	SYSTEM	—
SUNWkmp2r	PS/2 Keyboard and Mouse device drivers (Root((32-bit)	SYSTEM	—
SUNWkmp2x	PS/2 Keyboard and Mouse device drivers (Root) (64-bit)	SYSTEM	—
SUNWmdr	Solstice DiskSuite drivers	SYSTEM	Required by the BTS 10200
SUNWmdx	Solstice DiskSuite drivers(64-bit)	SYSTEM	Required by the BTS 10200
SUNWmdi	Sun Multipath I/O drivers	SYSTEM	—
SUNWmdix	Sun Multipath I/O drivers (64-bit)	SYSTEM	—
SUNWpd	PCI drivers	SYSTEM	—

Table 2-4 Solaris Architectural- or Hardware-Specific Optional Package List (continued)

Package	Description	Type	Status
SUNWpdx	PCI drivers (64-bit)	SYSTEM	—
SUNWpiclh	PICL Header files	SYSTEM	—
SUNWpiclr	PICL Framework (Root)	SYSTEM	—
SUNWpiclu	PICL libraries and Plugin modules (Usr)	SYSTEM	—
SUNWpiclx	PICL libraries (64-bit)	SYSTEM	—
SUNWqfed	Sun Quad FastEthernet Adapter driver	SYSTEM	—
SUNWqfedx	Sun Quad FastEthernet Adapter driver (64-bit)	SYSTEM	—
SUNWqlc	Qlogic ISP 2200/2202 Fiber Channel device driver	SYSTEM	—
SUNWqlcx	Qlogic ISP 2200/2202 Fiber Channel device driver (64-bit)	SYSTEM	—
SUNWses	SCSI Enclosure Services device driver	SYSTEM	—
SUNWsesx	SCSI Enclosure Services device driver (64-bit)	SYSTEM	—
SUNWsior	SuperIO 307 (plug-n-play) device drivers (Root)	SYSTEM	—
SUNWsiox	SuperIO 307 (plug-n-play) device drivers (Root) (64-bit)	SYSTEM	—
SUNWssad	SPARCstorage Array drivers	SYSTEM	—
SUNWssadx	SPARCstorage Array drivers (64-bit)	SYSTEM	—
SUNWssaop	Administration Utilities and Firmware for SPARCStorage Array	SYSTEM	—
SUNWuaud	USB Audio drivers	SYSTEM	—
SUNWuaudx	USB Audio drivers (64-bit)	SYSTEM	—
SUNWusb	USB device drivers	SYSTEM	—
SUNWusbx	USB device drivers (64-bit)	SYSTEM	—
SUNWxwdv	X Windows System Window drivers	SYSTEM	—
SUNWxwdvx	X Windows System Window drivers (64-bit)	SYSTEM	—

Solaris OS Patches

This chapter describes the BTS 10200 Solaris OS patches.

Trace Normal Forms (TNF) Support

The TNF package provides the Solaris tool suite with enhanced debugging capabilities of applications as they execute in the target environment. TNF supports program execution traces at both the user and kernel level The package includes the following:

- SUNWtnfc—Utilities needed to enable probe points, in the kernel and in applications, that can generate TNF records in a trace file.

- SUNWtnfd—Utilities needed by developers using TNF facilities.
- SUNWtnfx—The 64-bit utilities needed to enable probe points, in the kernel and in applications, that can generate TNF records in a trace file.

XML Libraries

The Sun VTS software requires the use of the XML libraries on the BTS 10200. These are in the supplemental part of the Solaris distribution with the VTS packages. These XML libraries and tools for 32 and 64 bit usage are listed as follows:

- SUNWxmlS
- SUNWlxml
- SUNWlxmlx

Device GLM Patch

The 109885-16 patch corrects several open bug reports on the SCSI device driver GLM in the Solaris OS.

Security CE Patch

The 111883-24 patch corrects Sun GigaSwift Ethernet 1.0 driver.

Security Bad_Trap Patch

The 117000-05 patch is a new generic kernel patch that cumulates many kernel level bug fixes into a single patch. This supersedes the older generic patch 108528-29.

Java SDK Patches

The upgraded version of Java requires some additional patches to the kernel and system libraries to support the required functionality. The patches are listed below. These are the relevant patches from the recommended cluster of patches as produced by Sun Microsystems.

- 109147-30—The SunOS 5.8: linker patch.
- 111308-05—The SunOS 5.8: /usr/lib/libmtmalloc.so.1 patch.
- 112438-03—The SunOS 5.8: /kernel/drv/random patch.
- 108434-17—The SunOS 5.8: 32-Bit Shared library patch for C++.

Note 108435-17 is the corresponding 64-bit patch.

- 108435-17—The SunOS 5.8: 64-Bit Shared library patch for C++ Note: 108434-17 is the corresponding 32-bit patch.
- 111111-04—The SunOS 5.8: /usr/bin/nawk patch.

- 108993-38—The SunOS 5.8: LDAP2 client, libc, libthread and libnsl libraries patch.
- 109326-16—The SunOS 5.8: libresolv.so.2 and in.named patch.
- 110615-13—The SunOS 5.8: sendmail patch.