SGM Command Reference

This appendix provides the following information:

SGM Commands and Descriptions

Table B-1 provides the format and a brief description of each SGM command. Each command is available in both Solaris and Windows, except as indicated.

Table B-1 SGM Commands

Command	Description
sgm	Displays the command syntax for the **sgm** command and all of its options. The function of this command is identical to **sgm help**. For a sample output for this command, see the "Viewing the SGM Technical Documentation" section on page 7-81.

sgm ?	Displays the command syntax for the **sgm** command and all of its options. The function of this command is identical to **sgm help**. For a sample output for this command, see the "Viewing the SGM Technical Documentation" section on page 7-81.
	
	To see the command syntax for a specific keyword, enter **sgm ?** followed by that keyword. For example, if you enter **sgm help restart**, SGM displays:
	
	`sgm restart - Restarts all SGM Servers on the local host.`
	`sgm restart web - Restarts Web servers on the local host.`
	`sgm restart jsp - Restarts JSP servers on the local host.`
	`sgm restart pm - Restarts Process Manager on the local host.`

Table B-1 SGM Commands (continued)

Command	Description
sgm accstats [*node-list* [*id-tag*]] [*sort-option*] [**quiet**]	(Solaris only) Generate SGM accounting statistics reports: • To include or exclude specific nodes or linksets in the reports, use the *node-list* argument: – To include all nodes, specify **all**. – To include a single node, specify a single node name as the *node-list* argument. The node name must match exactly the node name as discovered by SGM, including the domain name, such as **sgm-2600a.cisco.com**. – To include or exclude nodes or linksets based on the contents of the user-defined *nodes.include*, *linksets.include*, *nodes.exclude*, and *linksets.exclude* files, create the files, then specify **default**. This is also the default setting for this command; you only need to specify **default** if you also want to specify an *id-tag*, *sort-option*, or **quiet**. – To include a group of nodes other than the one specified in the *nodes.include* file, create a file that contains the list of nodes to included and specify the full path and name of the file as the *node-list* argument. If you specify a *node-list*, you can also specify an *id-tag* to identify the reports. The *id-tag* can be any meaningful character string, but it cannot contain any spaces. The default value for *id-tag* is the process ID of the **sgm accstats** command. • To specify the sort order for the reports, specify one of the following keywords for the *sort-option* argument: – **-sdp**—Sort based on the destination point code (DPC) of the node, in descending order. – **-sno**—Sort based on the node name, in ascending order. – **-sop**—Sort based on the originating point code (OPC) of the node, in descending order. – **-srb**—Sort based on number of bytes received, in descending order.

Table B-1 SGM Commands (continued)

Command	Description
sgm accstats [*node-list* [*id-tag*]] [*sort-option*] [**quiet**] (continued)	– **-srm**—Sort based on number of MTP3 MSUs received, in descending order.**-ssb**—Sort based on number of bytes sent, in descending order. – **-ssi**—Sort numerically based on service indicator (SI), in ascending order. – **-ssm**—Sort based on number of MTP3 MSUs sent, in descending order. • To disable automatic output to the terminal when running this command in a script, specify the **quiet** keyword. SGM generates the report in export format, which you can view using the SGM Web interface. The first time you use the **sgm accstats** command to generate a report, you must enter the command at least three times: • The first entry gets the first set of raw data. • The second entry calculates begins calculating useful accounting statistics. • The third entry continues to calculate statistics, calculates long-term averages, and, if the data being collected appears valid, begins generating the report. Thereafter, you need only enter this command once to generate the report. See the "Generating and Viewing Custom SGM Statistics Reports" section on page 3-254 for more information on the use of this command. You must be logged in as the root user or as a super user to use this command.

Table B-1 SGM Commands (continued)

Command	Description
sgm adduser [*username*]	(Solaris only) If SGM User-Based Access is enabled, adds the specified user to the authentication list. When you add a user, SGM prompts you for the following information: • User's password. When setting the password, follow the rules and considerations in the "Creating Secure Passwords" section on page 4-5. • Whether to force the user to change the password at the next login. The default is not to force the user to change the password. • Authentication level for the user. Valid levels are: – **1**—Basic User – **2**—Power User – **3**—Network Operator – **4**—Network Administrator – **5**—System Administrator See the "Implementing SGM User-Based Access (Solaris Only)" section on page 4-2 for more information on authentication levels, and on the use of this command. You must be logged in as the root user or as a super user to use this command.

Table B-1 SGM Commands (continued)

Command	Description
sgm authtype [**local** | **solaris**]	(Solaris only) Configures SGM security authentication, as follows: • **local**—Allows creation of user accounts and passwords local to the SGM system. When using this method, usernames, passwords, and access levels are managed using SGM commands. • **solaris**—Uses standard Solaris-based user accounts and passwords, as specified in the */etc/nsswitch.conf* file. Authentication can be provided by the local */etc/passwd* file or from a distributed Network Information Services (NIS) system. You can use all SGM User-Based Access commands except the following commands: – **sgm disablepass** – **sgm passwordage** – **sgm userpass** You must use Solaris commands to manage passwords. Users also cannot change their passwords using the SGM client. Instead, they must manage their passwords on the external authentication servers, using Solaris commands. All new passwords take effect the next time SGM automatically synchronizes local SGM passwords with Solaris. In addition, you must be logged in as the root user, not a super user, to use the following SGM commands: – **sgm adduser** – **sgm disableuser** – **sgm enableuser** – **sgm updateuser** See the "Implementing SGM User-Based Access (Solaris Only)" section on page 4-2 for more information on the use of this command. You must be logged in as the root user or as a super user to use this command.

Table B-1 SGM Commands (continued)

Command	Description
sgm backup	(Solaris only) Backs up SGM data files to the SGM installation directory. SGM automatically backs up all data files at 11:59 PM each night, but you can use this command to back up the files at any other time. • If you installed SGM in the default directory, */opt*, then the locations of the backup files are */opt/sgm22-client-backup.tar.Z* and */opt/sgm22-server-backup.tar.Z*. • If you installed SGM in a different directory, then the backup files are located in that directory. To restore the SGM data files from the previous night's backup, use the **sgm restore** command. Do not try to manually extract the backup files. You must be logged in as the root user (not as a super user) to use this command.
sgm backupdir [*directory*]	(Solaris only) Enables you to change the directory in which SGM stores its nightly backup files. The default backup directory is the directory in which SGM is installed: • If you installed SGM in the default directory, */opt*, then the default backup directory is also */opt*. • If you installed SGM in a different directory, then the default backup directory is that directory. If you specify a new directory that does not exist, SGM does not change the directory, and issues an appropriate message. **Note** The **sgm backupdir** command does not change the directory in which SGM stores GTT files, ITP route table files, report files, or sound files. To change those directories, you must use the **sgm gttdir**, **sgm repdir**, **sgm routedir**, and **sgm sounddir** commands, respectively. You must be logged in as the root user or as a super user to use this command.

Table B-1 SGM Commands (continued)

Command	Description
sgm badloginalarm [*number-of-attempts* | **clear**]	(Solaris only) If SGM User-Based Access is enabled, number of unsuccessful login attempts allowed before SGM generates an alarm. The valid range is 1 unsuccessful attempt to an unlimited number of unsuccessful attempts. The default value is 5 unsuccessful attempts. SGM records alarms in the system security log file. The default path and filename for the system security log file is */opt/CSCOsgm/logs/sgmSecurityLog.txt*. If you installed SGM in a directory other than */opt*, then the system security log file is located in that directory. To view the system security log file, enter **sgm seclog**. You can also view the system security log on the SGM System Security Log Web page. For more information, see the "Viewing the SGM System Security Log" section on page 7-73. To disable this function (that is, to prevent SGM from automatically generating an alarm after unsuccessful login attempts), enter **sgm badloginalarm clear**. See the "Automatically Disabling Users and Passwords (Solaris Only)" section on page 4-9 for more information on the use of this command. You must be logged in as the root user or as a super user to use this command.

Table B-1 SGM Commands (continued)

Command	Description
sgm badlogindisable [*number-of-attempts* | **clear**]	(Solaris only) If SGM User-Based Access is enabled, number of unsuccessful login attempts by a user allowed before SGM disables the user's authentication. SGM does not delete the user from the authentication list, SGM only disables the user's authentication. To re-enable the user's authentication, use the **sgm enableuser** command. The valid range is 1 unsuccessful attempt to an unlimited number of unsuccessful attempts. The default value is 10 unsuccessful attempts. To disable this function (that is, to prevent SGM from automatically disabling a user's authentication after unsuccessful login attempts), enter **sgm badlogindisable clear**. See the "Automatically Disabling Users and Passwords (Solaris Only)" section on page 4-9 for more information on the use of this command. You must be logged in as the root user or as a super user to use this command.
sgm browserpath	(Solaris only) Sets a user-defined SGM Web browser path, and verifies that the browser specified by the user exists. You must be logged in as the root user (not as a super user) to use this command.
sgm certgui	(Solaris only) If Secure Sockets Layer (SSL) is implemented in your SGM system, opens the SGM Certificate Tool window, which enables you to manage SSL certificates on the SGM client. **Note** If you installed the SGM server and client on the same workstation, this command is unnecessary. Instead, when you use the **sgm keytool** command to manage SSL certificates on the server, SGM automatically manages the certificates on the client. You must be logged in as the root user (not as a super user) to use this command in Solaris.

Table B-1 SGM Commands (continued)

Command	Description
sgm certtool [**clear** | **delete** *alias* | **export** *alias* [**-file** *filename*] | **import** *alias* [**-file** *filename*] | **list**]	If Secure Sockets Layer (SSL) is implemented in your SGM system, enables you to manage SSL certificates on the SGM client from the command line. **Note** If you installed the SGM server and client on the same workstation, this command is unnecessary. Instead, when you use the **sgm keytool** command to manage SSL certificates on the server, SGM automatically manages the certificates on the client. Use the following keywords and arguments with this command: • **import** *alias* [**-file** *filename*]—Imports a signed SSL certificate in X.509 format. This is the most common use for this command. The *alias* argument can be any character string; the host name of the server from which you are importing the certificate is a good choice. To import the certificate from a file, specify the optional **-file** keyword and a filename. • **export** *alias* [**-file** *filename*]—Exports the specified SSL certificate in X.509 format. To export the certificate to a file, specify the optional **-file** keyword and a filename. • **list**—Lists all SSL certificates on the SGM client. • **delete** *alias*—Removes the specified SSL certificate from the SGM client. • **clear**—Removes all SSL certificates from the SGM client. (Solaris only) You must be logged in as the root user (not as a super user) to use this command in Solaris.

Table B-1 SGM Commands (continued)

Command	Description
sgm clean	(Solaris only) Removes all SGM data from the SGM server, **excluding** message log files, backup files, and report files. This command restores the SGM server to a "clean" state, such as would exist after a new installation of SGM, except for the presence of the retained files. Data removed includes all SGM data, notes, preferences, route files, and views, as well as any user-created files stored in SGM directories. You must be logged in as the root user (not as a super user) to use this command.
sgm cleanall	(Solaris only) Removes all SGM data from the SGM server, **including** message log files, backup files, and report files. This command restores the SGM server to a "clean" state, such as would exist after a new installation of SGM. Data removed includes all SGM data, notes, preferences, route files, views, message log files, backup files, and report files, as well as any user-created files stored in SGM directories. You must be logged in as the root user (not as a super user) to use this command.
sgm cleandiscover [*seed-node*] [*seed-node*]...	(Solaris only) Enables you to delete all current network data and begin a clean discovery of the ITP network from the command line. Use the *seed-node* arguments to specify the DNS names or IP addresses of one or more seed nodes. **Note** When you begin a clean discovery, SGM stops any real-time polls that are running and issues appropriate messages. Running this command does not remove any notes, preferences, route files, views, message log files, backup files, or report files, nor any user-created files stored in SGM directories. You must be logged in as the root user or as a super user to use this command.

Table B-1 SGM Commands (continued)

Command	Description
sgm client [*hostname*]	(Solaris only) Starts an SGM client on the specified host. If no host name is specified, starts an SGM client on the default host, as specified during installation. See the "Connecting to a New Server" section on page 3-284 for information about determining the default host. If you Telnet into a remote workstation, the DISPLAY variable must be set to your local display, or you cannot use this command. If the DISPLAY variable is not set automatically, you must set it manually. See the "Setting the DISPLAY Variable (Solaris Only)" section on page 5-44 for details.
sgm clientlogs	(Solaris only) Uses PAGER to display the SGM client log files. The SGM client log files contain client console output for all SGM clients, one file per local or remote client. The file for a client is created by SGM automatically when the client starts. • If you installed SGM in the default directory, */opt*, then the SGM client log file is located in the */opt/CSCOsgm/logs/clientLogs* directory. • If you installed SGM in a different directory, then the file is located in that directory.
sgm clientpass	(Solaris only) Sets an SGM password to control starting an SGM client from the command line. This password is independent of, and in addition to, any passwords configured using SGM User-Based Access. See the "Implementing a Client Password (Solaris Only)" section on page 4-37 for more information. You must be logged in as the root user (not as a super user) to use this command.

Table B-1 SGM Commands (continued)

Command	Description
sgm clitimeout [*number-of-minutes* | **clear**]	(Solaris only) Specifies how long, in minutes, an SGM client can be inactive before being disconnected automatically by SGM. This function is disabled by default. If you do not specify this command, clients are never disconnected as a result of inactivity. If you enter the **sgm clitimeout** command, the valid range is 1 minute to an unlimited number of minutes. There is no default value. If you have enabled this function and you want to disable it (that is, never disconnect a client as a result of inactivity), enter the **sgm clitimeout clear** command. See the "Automatically Disabling Users and Passwords (Solaris Only)" section on page 4-9 for more information on the use of this command. You must be logged in as the root user or as a super user to use this command.
sgm cmdlog [**clear** | **-r**]	(Solaris only) Uses PAGER to display the contents of the system command log. The system command log lists all **sgm** commands that have been entered for the SGM server, the time each command was entered, and the user who entered the command. To clear the log and restart the server, enter **sgm cmdlog clear**. To display the contents of the log in reverse order, with the most recent commands at the beginning of the log, enter **sgm cmdlog -r**. You must be logged in as the root user or as a super user to use this command.
sgm console	(Solaris only) Displays the contents of the console log file, *sgmConsoleLog.latest*. The console log file contains unexpected error and warning messages from the SGM server, such as those that might occur if the SGM server cannot start. You must be logged in as the root user or as a super user to use this command.

Table B-1 SGM Commands (continued)

Command	Description
sgm cw2ksetup [**install** | **uninstall**]	(Solaris only) Manages the integration of SGM with CiscoWorks2000: • **install**—Checks to see which CiscoWorks2000 files are installed, and installs additional files as necessary. Use this command to integrate SGM and CiscoWorks2000 in the following instances: – You installed CiscoWorks2000 after you installed SGM. – SGM and CiscoWorks2000 are no longer integrated for some reason. • **uninstall**—Removes SGM files from the CiscoWorks2000 area. *Always* run **sgm cw2ksetup uninstall** before uninstalling CiscoWorks2000 from your system. You must be logged in as the root user (not as a super user) to use this command.
sgm delete [**all** | **node** [**all** | *node* [*node*] [*node*]...] | **linkset** [**all** | *node*/*linkset*] [*node*/*linkset*]...]	(Solaris only) Deletes objects from the SGM database. • **all**—Deletes all nodes and linksets from the SGM database. • **node all**—Deletes all nodes from the SGM database. • **node** [*node*] [*node*]...—Deletes one or more nodes from the SGM database. Use the *node* arguments to specify one or more nodes. • **linkset all**—Deletes all linksets from the SGM database. • **linkset** [*node*/*linkset*] [*node*/*linkset*]...—Deletes one or more linksets from the SGM database. Use the *node*/*linkset* arguments to specify one or more linksets associated with specific nodes. See the "Deleting a Linkset" section on page 3-77 and the "Deleting a Node" section on page 3-105 for more information. You must be logged in as the root user or as a super user to use this command.

Table B-1 SGM Commands (continued)

Command	Description
sgm deluser [*username*]	(Solaris only) If SGM User-Based Access is enabled, deletes the specified user from the authentication list. To add the user back to the list, use the **sgm adduser** command. See the "Manually Disabling Users and Passwords (Solaris Only)" section on page 4-13 for more information on the use of this command. You must be logged in as the root user or as a super user to use this command.
sgm disablepass [*username*]	(Solaris only) If SGM User-Based Access is enabled and **sgm authtype** is set to **local**, disables the specified user's authentication and password. SGM does not delete the user from the authentication list, SGM only disables the user's authentication and password. • To re-enable the user's authentication with the same password as before, use the **sgm enableuser** command. • To re-enable the user's authentication with a new password, use the **sgm userpass** command. If **sgm authtype** is set to **solaris**, you cannot use this command. Instead, you must manage passwords on the external authentication servers. See the "Manually Disabling Users and Passwords (Solaris Only)" section on page 4-13 for more information on the use of this command. You must be logged in as the root user or as a super user to use this command.

Table B-1 SGM Commands (continued)

Command	Description
sgm disableuser [*username*]	(Solaris only) If SGM User-Based Access is enabled, disables the specified user's authentication. SGM does not delete the user from the authentication list, SGM only disables the user's authentication. • To re-enable the user's authentication with the same password as before, use the **sgm enableuser** command. • To re-enable the user's authentication with a new password, use the **sgm userpass** command. See the "Manually Disabling Users and Passwords (Solaris Only)" section on page 4-13 for more information on the use of this command. You must be logged in as the root user or as a super user to use this command.
sgm discover [*seed-node*] [*seed-node*]...	(Solaris only) Enables you to discover the ITP network from the command line. Use the *seed-node* arguments to specify the DNS names or IP addresses of one or more seed nodes. **Note** This command does not perform a clean discovery. To do so, see the **sgm cleandiscover** command. You must be logged in as the root user or as a super user to use this command.
sgm enableuser [*username*]	(Solaris only) If SGM User-Based Access is enabled, re-enables the specified user's authentication, which had been disabled either automatically by SGM or by a super user. The user's authentication is re-enabled with the same password as before. See the "Enabling and Modifying Users and Passwords (Solaris Only)" section on page 4-15 for more information on the use of this command. You must be logged in as the root user or as a super user to use this command.

Table B-1 SGM Commands (continued)

Command	Description
sgm eventconfig [**edit** | **master** | **restore** | **view**]	(Solaris only) Manages the SGM event configuration file, *SgmEvent.conf*. This file determines the size of the SGM event database, the maximum length of time SGM is to retain events, the default severity and color associated with each type of event, and all other aspects of SGM event processing. To manage the *SgmEvent.conf* file, specify one of the following keywords: • **edit**—Open and edit the *SgmEvent.conf* file directly. • **master**—Restore the *SgmEvent.conf* file to the default settings. • **restore**—Restore the *SgmEvent.conf* file from the previous version that was used. • **view**—View the current contents of the *SgmEvent.conf* file. Any changes you make take effect when you restart the SGM server. SGM reflects the changes on the SGM server and on all SGM clients that connect to that server. The changes are reflected in all SGM GUI and Web event displays, even in displays of archived events. SGM even reflects any new or changed categories and severities in its Web display navigation bars. See the "Modifying the SGM Event Configuration File (Solaris Only)" section on page 5-25 for important considerations to keep in mind when modifying the *SgmEvent.conf* file, and for more information about using this command. You must be logged in as the root user or as a super user to use this command.
sgm eventlog [**clear** | **-r**]	(Solaris only) Uses PAGER to display the contents of the SGM event automation log. The event automation log lists all messages generated by scripts launched by event automation. To clear the log and restart the server, enter **sgm eventlog clear**. To display the contents of the log in reverse order, with the most recent events at the beginning of the log, enter **sgm eventlog -r**. You must be logged in as the root user or as a super user to use this command.

Table B-1 SGM Commands (continued)

Command	Description
sgm evilstop	(Solaris only) Forcefully stops all SGM servers on the local host. This command can be useful if a normal **sgm stop** does not stop the servers. You must be logged in as the root user (not as a super user) to use this command.
sgm export [**all** | **links** | **linksets** | **nodes**]	(Solaris only) Exports current SGM data, with fields separated by vertical bars (|). • **all**—Export all current SGM data. • **links**—Export only link data. • **linksets**—Export only linkset data. • **nodes**—Export only node data. For a sample output for this command, see the "Output of sgm export Command" section on page B-66. You must be logged in as the root user or as a super user to use this command.
sgm gttcheck [**list** | **semantics** *nodename filename*| **syntax** *filename*]	(Solaris only) Checks the semantics or syntax of the specified GTT file. • **list**—List all current GTT filenames. • **semantics** *nodename filename*—Check the semantics of the specified GTT file on the specified node. • **syntax** *filename*—Check the syntax of the specified GTT file. For a sample output for this command, see the "Output of sgm gttcheck Command" section on page B-66. You must be logged in as the root user or as a super user to use this command.

Table B-1 SGM Commands (continued)

Command	Description
sgm gttclient [*hostname*]	(Solaris only) Starts an SGM GTT client on the specified host. If no host name is specified, starts an SGM GTT client on the default host, as specified during installation. See the "Connecting to a New Server" section on page 3-284 for information about determining the default host. If you Telnet into a remote workstation, the DISPLAY variable must be set to your local display, or you cannot use this command. If the DISPLAY variable is not set automatically, you must set it manually. See the "Setting the DISPLAY Variable (Solaris Only)" section on page 5-44 for details.
sgm gttdir [*directory*]	(Solaris only) Sets the directory in which SGM stores GTT files. See the "Editing a Global Title Translation Table" section on page 3-188 for information about GTT files. The default directory for GTT files is located in the SGM installation directory: • If you installed SGM in the default directory, */opt*, then the default directory is */opt/CSCOsgm/gtt*. • If you installed SGM in a different directory, then the default directory is located in that directory. Use this command if you want to use a different directory for GTT files, such as */tftboot*, or such as a Network File System location on another server, used as the Trivial File Transfer Protocol (TFTP) server for server configuration files for routers in the network. **Note** This command copies all files in the current directory to the new directory. If you are logged in as the super user, and you do not own the new directory, you might not be able to copy the files. If that is the case, you must specify a directory that you own, or you must log in as the root user. You must be logged in as the root user or as a super user to use this command.

Table B-1 SGM Commands (continued)

Command	Description

sgm help [*keyword*]	Displays the command syntax for the **sgm** command and all of its options. The function of this command is identical to **sgm ?**. For a sample output for this command, see the "Viewing the SGM Technical Documentation" section on page 7-81.
	
	To see the command syntax for a specific keyword, enter **sgm help** followed by that keyword. For example, if you enter **sgm help restart**, SGM displays:
	
	`sgm restart - Restarts all SGM Servers on the local host.`
	`sgm restart web - Restarts Web servers on the local host.`
	`sgm restart jsp - Restarts JSP servers on the local host.`
	`sgm restart pm - Restarts Process Manager on the local host.`

sgm inactiveuserdays [*number-of-days* | **clear**]	(Solaris only) If SGM User-Based Access is enabled, number of days a user can be inactive before disabling that user account. This function is disabled by default. If you do not specify this command, user accounts are never disabled as a result of inactivity. If you enter the **sgm inactiveuserdays** command, the valid range is 1 day to an unlimited number of days. There is no default setting. If you have enabled this function and you want to disable it (that is, prevent SGM from automatically disabling user accounts as a result of inactivity), enter **sgm inactiveuserdays clear**. To re-enable the user's authentication, use the **sgm enableuser** command. See the "Automatically Disabling Users and Passwords (Solaris Only)" section on page 4-9 for more information on the use of this command. You must be logged in as the root user or as a super user to use this command.
sgm iosinfo	(Solaris only) Displays the versions of IOS with which SGM is compatible.

Table B-1 SGM Commands (continued)

Command	Description
sgm installlog [**server** | **client**]	(Solaris only) Displays the latest install log for the **server** or **client**. If you do not specify **server** or **client**, displays the latest install log for both the server and client. You must be logged in as the root user or as a super user to use this command.

Table B-1 SGM Commands (continued)

Command	Description
sgm ipaccess [**add** [*ip-addr*] | **clear** | **edit** | **list** | **rem** [*ip-addr*] | **sample**]	(Solaris only) Enables you to create and manage a list of client IP addresses allowed to connect to the SGM server. The list of allowed client IP addresses is contained in the *ipaccess.conf* file. By default, when you first install SGM, the *ipaccess.conf* file does not exist and SGM allows all client IP addresses to connect to the SGM server. To create the *ipaccess.conf* file and work with the list of allowed client IP addresses, specify one of the following keywords: • **add**—Add the specified client IP address to the *ipaccess.conf* file. If the *ipaccess.conf* file does not already exist, this command creates a file with the first entry. • **clear**—Remove all client IP addresses from the *ipaccess.conf* file, and allow connections from any SGM client IP address. • **edit**—Open and edit the *ipaccess.conf* file directly. If the *ipaccess.conf* file does not already exist, this command creates an empty file. • **list**—List all client IP addresses currently in the *ipaccess.conf* file. If no client IP addresses are listed (that is, the list is empty), connections from any SGM client IP address are allowed. • **rem**—Remove the specified client IP address from the *ipaccess.conf* file. • **sample**—Print out a sample *ipaccess.conf* file. Any changes you make take effect when you restart the SGM server. See the "Limiting SGM Client Access to the SGM Server (Solaris Only)" section on page 4-39 for more information about using this command. You must be logged in as the root user or as a super user to use this command.

Table B-1 SGM Commands (continued)

Command	Description
sgm jspport [*port-number*]	(Solaris only) Sets a new port number for the JSP server, where *port-number* is the new, numeric port number. SGM verifies that the new port number is not already in use. This command is needed only if you must change the port number after you install SGM, because another application must use the current port number. The new port number must contain only numbers. If you enter a port number that contains non-numeric characters, such as **sgm13**, SGM displays an error message and returns to the command prompt without changing the port number. You must be logged in as the root user (not as a super user) to use this command.

Table B-1 SGM Commands (continued)

Command	Description
sgm keytool [**clear** | **genkey** | **import_cert** *cert_filename* | **import_key** *key_filename cert_filename* | **list** | **print_csr** | **print_crt**]	(Solaris only) If SSL is implemented in your SGM system, manages SSL keys and certificates on the SGM server. If you installed the SGM server and client on the same workstation, also automatically manages the certificates on the client. Use the following keywords and arguments with this command: • **clear**—Stops the SGM server, if necessary, and removes all SSL keys and certificates from the server. Before restarting the server, you must either generate new SSL keys using the **sgm keytool genkey** command, or you must completely disable SSL using the **sgm ssl disable** command. • **genkey**—Stops the SGM server, if necessary, and generates a new self-signed public/private SSL key pair on the SGM server. The new keys take effect when you restart the server. • **import_cert** *cert_filename*—Imports the specified signed SSL certificate in X.509 format. • **import_key** *key_filename cert_filename*—Imports the specified SSL key in OpenSSL format and the specified signed SSL certificate in X.509 format. • **list**—Lists all SSL key/certificate pairs on the SGM server. • **print_csr**—Prints a certificate signing request (CSR) in X.509 format. • **print_crt**—Prints the SGM server's SSL certificate in X.509 format. See the "Implementing SSL Support in SGM" section on page 4-24 for more information on the use of this command. You must be logged in as the root user (not as a super user) to use this command.
sgm killclients	(Solaris only) Forcefully stops all SGM clients, including all GTT clients, on the local host. You must be logged in as the root user (not as a super user) to use this command.

Table B-1 SGM Commands (continued)

Command	Description
sgm linkstats [*node-list* [*id-tag*]] [*sort-option*] [**quiet**]	(Solaris only) Generate SGM link and linkset statistics summary reports: • To include or exclude specific nodes or linksets in the reports, use the *node-list* argument: – To include all nodes, specify **all**. – To include a single node, specify a single node name as the *node-list* argument. The node name must match exactly the node name as discovered by SGM, including the domain name, such as **sgm-2600a.cisco.com**. – To include or exclude nodes or linksets based on the contents of the user-defined *nodes.include*, *linksets.include*, *nodes.exclude*, and *linksets.exclude* files, create the files, then specify **default**. This is also the default setting for this command; you only need to specify **default** if you also want to specify an *id-tag*, *sort-option*, or **quiet**. – To include a group of nodes other than the one specified in the *nodes.include* file, create a file that contains the list of nodes to included and specify the full path and name of the file as the *node-list* argument. If you specify a *node-list*, you can also specify an *id-tag* to identify the reports. The *id-tag* can be any meaningful character string, but it cannot contain any spaces. The default value for *id-tag* is the process ID of the **sgm linkstats** command. • To specify the sort order for the reports, specify one of the following keywords for the *sort-option* argument: – **-sis**—Sort based on average in-service percentage for each link (**Daily InSrv**), in descending order. – **-sls**—Sort based on the linkset name, in ascending order. – **-sos**—Sort based on the average out-of-service percentage for each link, in descending order.

Table B-1 SGM Commands (continued)

Command	Description
sgm linkstats [*node-list* [*id-tag*]] [*sort-option*] [**quiet**] (continued)	– **-sru**—Sort based on the average Receive Utilization for each link (**Avg Receive Util** or **Avg Receive Erls**), in descending order. – **-ssu**—Sort based on the average Send Utilization for each link (**Avg Send Util** or **Avg Send Erls**), in descending order. This is the default setting. • To disable automatic output to the terminal when running this command in a script, specify the **quiet** keyword. SGM generates the report in export format, which you can view using the SGM Web interface. The first time you use the **sgm linkstats** command to generate a report, you must enter the command at least three times: • The first entry gets the first set of raw data. • The second entry calculates begins calculating useful link and linkset statistics. • The third entry continues to calculate statistics, calculates long-term averages, and, if the data being collected appears valid, begins generating the report. Thereafter, you need only enter this command once to generate the report. See the "Generating and Viewing Custom SGM Statistics Reports" section on page 3-254 for more information on the use of this command. You must be logged in as the root user or as a super user to use this command.

Table B-1 SGM Commands (continued)

Command	Description
sgm listusers [*username*]	(Solaris only) If SGM User-Based Access is enabled, lists all currently defined users in the authentication list, including the following information for each user: • Username • Last time the user logged in • User's authentication access level • User's current authentication status, such as **Account Enabled** or **Password Disabled** To list information for a specific user, use the *username* argument to specify the user. See the "Maintaining Your SGM Security System (Solaris Only)" section on page 4-17 for more information on the use of this command. You must be logged in as the root user or as a super user to use this command.
sgm logger	(Solaris only) Displays the system messages *messageLog.txt* file with tail -f. To stop the display, enter **Ctrl-c**.
sgm logtimemode [**12** | **24**]	(Solaris only) Sets the time mode for dates in log files: • **12**—Use 12-hour time, with AM and PM. 1:00 in the afternoon is 1:00 PM. • **24**—Use 24-hour time, also called military time. 1:00 in the afternoon is 13:00. This is the default setting. You must be logged in as the root user or as a super user to use this command.

Table B-1 SGM Commands (continued)

Command	Description
sgm maxasciirows [*number-of-rows*]	(Solaris only) Sets the maximum number of rows for SGM ASCII Web output, such as displays of detailed debugging information. If you enter this command without the *number-of-rows* argument, SGM displays the current maximum number of rows. You can then change that value, or leave it as-is. The valid range is 1 row to an unlimited number of rows. The default value is 6000 rows. You must be logged in as the root user or as a super user to use this command.
sgm maxhtmlrows [*number-of-rows*]	(Solaris only) Sets the maximum number of rows for SGM HTML Web output, such as displays of statistics reports, status change messages, or SNMP trap messages. If you enter this command without the *number-of-rows* argument, SGM displays the current maximum number of rows. You can then change that value, or leave it as-is. The valid range is 1 row to an unlimited number of rows. The default value is 500 rows. You must be logged in as the root user or as a super user to use this command.

Table B-1 SGM Commands (continued)

Command	Description
sgm mldebug [*mode*]	(Solaris only) Sets the mode for logging SGM debug messages: • **normal**—Logs all action, error, and info messages. Use **sgm mldebug normal** to revert to the default settings if you accidentally enter the **sgm mldebug** command. • **all**—Logs all messages, of any type. • **none**—Logs no messages at all. • **minimal**—Logs all error messages. • **action**—Logs all action messages. • **debug**—Logs all debug messages. • **dump**—Logs all dump messages. • **error**—Logs all error messages. • **info**—Logs all info messages. • **snmp**—Logs all SNMP messages. • **trace**—Logs all trace messages. This command can adversely affect SGM performance. Use this command **only** under guidance from the Cisco TAC. You must be logged in as the root user or as a super user to use this command.

Table B-1 SGM Commands (continued)

Command	Description
sgm motd [**cat** | **disable** | **edit** | **enable**]	(Solaris only) Manages the SGM message of the day file, which is a user-specified SGM system notice. You can use the message of the day to inform users of important changes or events in the SGM system. The message of the day also gives users an opportunity to exit the SGM or GTT client before launching. If the message of the day is enabled, it is displayed whenever a user attempts to launch an SGM or GTT client: • If the user accepts the message, the client launches. • If the user declines the message, the client does not launch. Use the following keywords with this command: • **enable**—Enables the message of the day function. Initially, the message of the day file is blank; use the **sgm motd edit** command to specify the message text. • **edit**—Enables you to modify the message of the day. • **cat**—Displays the contents of the message of the day file. • **disable**—Disables this function (that is, stops displaying the message of the day whenever a user attempts to launch an SGM or GTT client). See the "Maintaining Your SGM Security System (Solaris Only)" section on page 4-17 for more information on the use of this command. You must be logged in as the root user or as a super user to use this command.
sgm msglog [**clear** | **-r**]	(Solaris only) Uses PAGER to display the contents of the system message log. To save the current contents of the log, clear the log, and restart the server, enter **sgm msglog clear**. To display the contents of the log in reverse order, with the most recent messages at the beginning of the log, enter **sgm msglog -r**. You must be logged in as the root user or as a super user to use this command.

Table B-1 SGM Commands (continued)

Command	Description
sgm msglogage [*number-of-days*]	(Solaris only) Sets the maximum number of days to archive system message log files before deleting them from the SGM server. If you enter this command without the *number-of-days* argument, SGM displays the current maximum number of days. You can then change that value, or leave it as-is. The valid range is 1 day to an unlimited number of days. The default value is 31 days. You must be logged in as the root user or as a super user to use this command.
sgm msglogdir [*directory*]	(Solaris only) Changes the default location of all SGM system message log files. By default, the system message log files are located on the SGM server at */opt/CSCOsgm/logs*. You must be logged in as the root user or as a super user to use this command. If you are changing to a default location outside SGM, you must have appropriate permissions for that location.
sgm msglogsize [*number-of-lines*]	(Solaris only) Sets the maximum number of messages to write to the message log file before starting a new file. If you enter this command without the *number-of-lines* argument, SGM displays the current maximum number of messages. You can then change that value, or leave it as-is. The valid range is 1000 messages to an unlimited number of messages. The default value is 10000 messages (approximately 2 MB). Therefore, the default message log file and its copy require approximately 4 MB, combined. If you specify a larger message log file size, the message log file and its copy require proportionally more space. When changing the number of messages to display, keep in mind that every 5000 messages require approximately 1 MB. You need to balance your need to refer to old messages against the amount of space they take up. You must be logged in as the root user or as a super user to use this command.

Table B-1 SGM Commands (continued)

Command	Description
sgm netlog [**clear** | **-r**]	(Solaris only) Uses PAGER to display the contents of the network status log. To save the current contents of the log, clear the log, and restart the server, enter **sgm netlog clear**. To display the contents of the log in reverse order, with the most recent network status messages at the beginning of the log, enter **sgm netlog -r**. You must be logged in as the root user or as a super user to use this command.
sgm netlogger	(Solaris only) Displays the current contents of the network status log file with tail -f. To stop the display, enter **Ctrl-c**.
sgm newlevel [*username*]	(Solaris only) If SGM User-Based Access is enabled, changes the authentication level for the specified user. Valid levels are: • **1**—Basic User • **2**—Power User • **3**—Network Operator • **4**—Network Administrator • **5**—System Administrator See the "Enabling and Modifying Users and Passwords (Solaris Only)" section on page 4-15 for more information on the use of this command. You must be logged in as the root user or as a super user to use this command.

Table B-1 SGM Commands (continued)

Command	Description
sgm passwordage [*number-of-days* | **clear**]	(Solaris only) If SGM User-Based Access is enabled and **sgm authtype** is set to **local**, number of days allowed before forcing users to change passwords. This function is disabled by default. If you do not specify this command, users never need to change their passwords. If you enter the **sgm passwordage** command, the valid range is 1 day to an unlimited number of days. There is no default setting. If you have enabled this function and you want to disable it (that is, prevent SGM from forcing users to change passwords), enter **sgm passwordage clear**. **Note** If **sgm authtype** is set to **solaris**, you cannot use this command. Instead, you must manage passwords on the external authentication servers. See the "Automatically Disabling Users and Passwords (Solaris Only)" section on page 4-9 for more information on the use of this command. You must be logged in as the root user or as a super user to use this command.

Table B-1 SGM Commands (continued)

Command	Description
sgm pcformat {**ansi** | **china** | **itu** | *string*}	(Solaris only) Sets the point code format to be used for this SGM server, and for all associated SGM clients. Normally, you need to set the point code format only once, after installation. Valid formats are: • **ansi**—Formats point codes using the 24-bit format American National Standards Institute (ANSI) standard, *xxx.yyy.zzz* format, where: – *xxx* is the 8-bit network identification – *yyy* is the 8-bit network cluster – *zzz* is the 8-bit network cluster member • **china**—Formats point codes using the 24-bit format China standard, *xxx.yyy.zzz* format, where: – *xxx* is the 8-bit network identification – *yyy* is the 8-bit network cluster – *zzz* is the 8-bit network cluster member • **itu**—Formats point codes using the 14-bit format International Telecommunication Union (ITU) standards, *x.yyy.z* format, where: – *x* is the 3-bit zone identification – *yyy* is the 8-bit region identification – *z* is the 3-bit signal-point This is the default setting.

Table B-1 SGM Commands (continued)

Command	Description
sgm pcformat {**ansi** | **china** | **itu** | *string*} (continued)	• *string*—Formats point codes using a user-specified variation on the ANSI or ITU standard, with each bit-number segment separated from the next by either a dot (.) or a dash (-). Valid formats are: – *x*.*x*.*x* or *x*-*x*-*x* – *x*.*x* or *x*-*x* – *x* Where *x* is the number of bits in that segment. The number of bits must total either 14 bits (for the ITU standard) or 24 bits (for the ANSI or China standards). For example, **sgm pcformat 4.6.4** specifies a 14-bit ITU point code format with a 4-bit segment, a 6-bit segment, and a 4-bit segment. You must be logged in as the root user or as a super user to use this command.
sgm pcinfo [**edit** | **view**]	(Solaris only) Enables you to edit or view the SGM point code mappings file, *pcinfo.conf*. This file contains a list of point codes mapped to node names for the server to which you are connected, and which is currently running the SGM server. To work with the *pcinfo.conf* file, specify one of the following keywords: • **edit**—Open and edit the *pcinfo.conf* file directly. • **view**—View the current contents of the *pcinfo.conf* file. You must be logged in as the root user or as a super user to use this command.
sgm pclist	(Solaris only) Lists all point codes that are currently being used by all nodes that are known to SGM. You must be logged in as the root user or as a super user to use this command.

Table B-1 SGM Commands (continued)

Command	Description
sgm poll [*node*] [*node*]...	(Solaris only) Enables you to poll one or more known nodes from the command line. Use the *node* arguments to specify the DNS names or IP addresses of one or more known nodes. You must be logged in as the root user or as a super user to use this command.
sgm print {**all** | **data** | **snmp** | **task**}	(Solaris only) Displays information about server internal data, SNMP settings, running tasks, or all three. You must be logged in as the root user or as a super user to use this command.
sgm props	(Solaris only) Displays the contents of the *System.properties* files for both SGM server and client installs. You must be logged in as the root user or as a super user to use this command.
sgm readme	Displays the contents of the README file for SGM.
sgm reboot	(Solaris only) Reboots the Solaris SGM system. You must be logged in as the root user (not as a super user) to use this command.
sgm repcustage [*number-of-days*]	(Solaris only) Maximum number of days SGM is to archive custom reports. If you enter this command without the *number-of-days* argument, SGM displays the current maximum number of days. You can then change that value, or leave it as-is. The valid range is 1 day to an unlimited number of days. The default value is 10 days. See the "Modifying the Way SGM Handles Statistics Reports (Solaris Only)" section on page 3-220 for more information on the use of this command. You must be logged in as the root user or as a super user to use this command.

Table B-1 SGM Commands (continued)

Command	Description
sgm repdailyage [*number-of-days*]	(Solaris only) Maximum number of days SGM is to archive daily reports. If you enter this command without the *number-of-days* argument, SGM displays the current maximum number of days. You can then change that value, or leave it as-is. The valid range is 1 day to an unlimited number of days. The default value is 90 days. See the "Modifying the Way SGM Handles Statistics Reports (Solaris Only)" section on page 3-220 for more information on the use of this command. You must be logged in as the root user or as a super user to use this command.
sgm repdir [*directory*]	(Solaris only) Sets the directory in which SGM stores report files. See the "Working with SGM Statistics Reports" section on page 3-218 for information about SGM reports. The default directory for report files is located in the SGM installation directory: • If you installed SGM in the default directory, */opt*, then the default directory is */opt/CSCOsgm/reports*. • If you installed SGM in a different directory, then the default directory is located in that directory. Use this command if you want to use a different directory for report files, such as a Network File System location on another server. **Note** This command copies all files in the current directory to the new directory. If you are logged in as the super user, and you do not own the new directory, you might not be able to copy the files. If that is the case, you must specify a directory that you own, or you must log in as the root user. You must be logged in as the root user or as a super user to use this command.

Table B-1 SGM Commands (continued)

Command	Description
sgm rephelp	(Solaris only) Displays help for all commands related to SGM reports. You must be logged in as the root user or as a super user to use this command.
sgm rephourlyage [*number-of-days*]	(Solaris only) Maximum number of days SGM is to archive hourly reports. If you enter this command without the *number-of-days* argument, SGM displays the current maximum number of days. You can then change that value, or leave it as-is. The valid range is 1 day to an unlimited number of days. The default value is 31 days. See the "Modifying the Way SGM Handles Statistics Reports (Solaris Only)" section on page 3-220 for more information on the use of this command. You must be logged in as the root user or as a super user to use this command.
sgm replog [**clear** | **-r**]	(Solaris only) Uses PAGER to display the contents of the system reports log. The reports log lists all messages related to the creation and maintenance of SGM reports. To clear the log and restart the server, enter **sgm replog clear**. To display the contents of the log in reverse order, with the most recent commands at the beginning of the log, enter **sgm replog -r**. The default path and filename for the system reports log file is */opt/CSCOsgm/reports/sgmReportLog.txt*. If you installed SGM in a directory other than */opt*, then the system reports log file is located in that directory. See the "Modifying the Way SGM Handles Statistics Reports (Solaris Only)" section on page 3-220 for more information on the use of this command. You must be logged in as the root user or as a super user to use this command.

Table B-1 SGM Commands (continued)

Command	Description
sgm restart [**jsp** | **pm** | **web**]	(Solaris only) Restarts SGM servers on the local host: • **jsp**—Restarts the SGM JSP Server. • **pm**—Restarts the SGM Process Manager and all managed processes. • **web**—Restarts the SGM Web Server. • If you do not specify a keyword, **sgm restart** restarts all SGM servers. You must be logged in as the root user or as a super user to use this command.
sgm restore [**logs** | **reports** | **security**]	(Solaris only) Restores the SGM data files from the previous night's backup, stored in the SGM installation directory: • If you installed SGM in the default directory, */opt*, then the locations of the backup files are */opt/sgm22-client-backup.tar.Z* and */opt/sgm22-server-backup.tar.Z*. • If you installed SGM in a different directory, then the backup files are located in that directory. To restore only specific parts of the SGM data files, use the following keywords: • **logs**—Restores only SGM log files, such as the message log files. • **reports**—Restores only SGM report files, such as the statistics report files. • **security**—Restores only the security-related parts of the SGM data files. This command is useful if you inadvertently delete your user accounts or make other unwanted changes to your SGM security information. You must be logged in as the root user (not as a super user) to use this command.

Table B-1 SGM Commands (continued)

Command	Description
sgm restoreprops	(Solaris only) Restores the SGM server and client *System.properties* files, and other important configuration files, to "clean" backup versions of the files. You must be logged in as the root user (not as a super user) to use this command.
sgm rootvars	(Solaris only) Displays the contents of the */etc/CSCOsgm.sh* file, which determines the root location of the SGM server and client installation.
sgm routedir [*directory*]	(Solaris only) Sets the directory in which SGM stores ITP route table files. See the "Editing an ITP Route Table File" section on page 3-180 for information about ITP route table files. The default directory for ITP route table files is located in the SGM installation directory: • If you installed SGM in the default directory, */opt*, then the default directory is */opt/CSCOsgm/routes*. • If you installed SGM in a different directory, then the default directory is located in that directory. Use this command if you want to use a different directory for ITP route table files, such as */tftboot*, or such as a Network File System location on another server, used as the Trivial File Transfer Protocol (TFTP) server for server configuration files for routers in the network. **Note** This command copies all files in the current directory to the new directory. If you are logged in as the super user, and you do not own the new directory, you might not be able to copy the files. If that is the case, you must specify a directory that you own, or you must log in as the root user. You must be logged in as the root user or as a super user to use this command.

Table B-1 SGM Commands (continued)

Command	Description
sgm sechelp	(Solaris only) Displays help for all commands related to SGM security. You must be logged in as the root user or as a super user to use this command.

Table B-1 SGM Commands (continued)

Command	Description
sgm seclog [**clear** | **-r**]	(Solaris only) Uses PAGER to display the contents of the system security log. The following security events are recorded in the log: • All changes to system security, including adding users • Login attempts, whether successful or unsuccessful, and logoffs • Attempts to switch to another user's account, whether successful or unsuccessful • Attempts to access files or resources of higher authentication level • Access to all privileged files and processes • Operating system configuration changes and program changes, at the Solaris level • SGM restarts • Failures of computers, programs, communications, and operations, at the Solaris level To clear the log and restart the server, enter **sgm seclog clear**. To display the contents of the log in reverse order, with the most recent security events at the beginning of the log, enter **sgm seclog -r**. The default path and filename for the system security log file is */opt/CSCOsgm/logs/sgmSecurityLog.txt*. If you installed SGM in a directory other than */opt*, then the system security log file is located in that directory. See the "Maintaining Your SGM Security System (Solaris Only)" section on page 4-17 for more information on the use of this command. You must be logged in as the root user or as a super user to use this command.

Table B-1 SGM Commands (continued)

Command	Description
sgm secondaryserver [*hostname* [*naming-port*] | **list**]	(Solaris only) Configures a secondary SGM server, where: • *hostname* is the name of the host on which the secondary SGM server is installed. • *naming-port* is the SGM Naming Server port number for the secondary SGM server. The default port number is 44742. For best results, Cisco recommends that you configure the primary server and the secondary server as secondaries for each other. If you use the **sgm secondaryserver** command to configure a secondary SGM server, but the primary SGM server fails before you launch the SGM client, then the SGM client has no knowledge of the secondary server. To list the secondary SGM server that has been configured for this primary SGM server, enter the **sgm secondaryserver list** command. You must be logged in as the root user or as a super user to use this command.

Table B-1 SGM Commands (continued)

Command	Description
sgm servername [*hostname*]	Resets the default host name, where *hostname* is the new default host name: • Make sure the new default host name is valid and is defined in your */etc/hosts* file. If it is not, you might not be able to start the SGM server. • If you are *not* logged in as the root user or as a super user when you enter this command from an SGM client, the default host name is changed only for that SGM client, and for the user who entered the command. • If you *are* logged in as the root user or as a super user when you enter this command, the default host name is changed for the SGM server and for the client, and the SGM server is restarted. The new default host name is used by the SGM server to register RMI services, and by SGM clients to connect to the server. • If you are logged into a *client-only* installation as the root user or as a super user when you enter this command, the default host name is changed only for that SGM client. The new default host name is used by the SGM client to connect to the SGM server.
sgm services	(Solaris only) Displays the processes started and managed by the Process Manager, as set in the *Services.conf* file. You must be logged in as the root user or as a super user to use this command.
sgm snmpcomm [*name*]	(Solaris only) Enables you to set a new default SNMP read community name. SGM automatically updates the name in the SNMP parameters file. The default path and filename for the SNMP parameters file is */opt/CSCOsgm/etc/communities.conf*. You must be logged in as the root user or as a super user to use this command.

Table B-1 SGM Commands (continued)

Command	Description
sgm snmpconf [*filename*]	(Solaris only) Sets the file used for SNMP parameters, such as community names, timeouts, and retries. The default path and filename for the SNMP parameters file is */opt/CSCOsgm/etc/communities.conf*. If you installed SGM in a directory other than */opt*, then the file is located in that directory. When you specify a new path or filename, SGM restarts the servers. **Note** The SNMP parameters file uses the HP OpenView format. Therefore, you can set this path and filename to point to the HP OpenView *ovsnmp.conf* file in an existing OpenView system. For information about exporting SNMP community names from CiscoWorks2000 Resource Manager Essentials (RME), see the "Importing SNMP Community Names from CiscoWorks2000 (Solaris Only)" section on page 5-2. You must be logged in as the root user or as a super user to use this command.
sgm snmpget [*hostname*] [*oid*] [*oid*]...	(Solaris only) Queries the specified *hostname* using SNMP GetRequests. Use the *oid* arguments to specify one or more OIDs or variable names. You must be logged in as the root user or as a super user to use this command.
sgm snmphelp	(Solaris only) Displays help for all commands related to SNMP queries. You must be logged in as the root user or as a super user to use this command.
sgm snmpnext [*hostname*] [*oid*] [*oid*]...	(Solaris only) Queries the specified *hostname* using SNMP GetNextRequests. Use the *oid* arguments to specify one or more OIDs. You must be logged in as the root user or as a super user to use this command.

Table B-1 SGM Commands (continued)

Command	Description
sgm snmpwalk [*hostname*] [*oid*] [*oid*]...	(Solaris only) Queries the specified *hostname*, using SNMP GetNextRequests to "walk" through the MIB. Use the *oid* arguments to specify one or more OIDs. You must be logged in as the root user or as a super user to use this command.
sgm sounddir [*directory*]	(Solaris only) Sets the directory in which the SGM server stores event automation sound files. See the "Automating Events" section on page 5-31 for information about sound files. The default directory for sound files is located in the SGM installation directory: • If you installed SGM in the default directory, */opt*, then the default directory is */opt/CSCOsgm/sounds*. • If you installed SGM in a different directory, then the default directory is located in that directory. Use this command if you want to use a different directory for SGM server event automation sound files, such as a Network File System location on another server. **Note** This command copies all files in the current directory to the new directory. If you are logged in as the super user, and you do not own the new directory, you might not be able to copy the files. If that is the case, you must specify a directory that you own, or you must log in as the root user. You must be logged in as the root user or as a super user to use this command.

Table B-1 SGM Commands (continued)

Command	Description
sgm ssl [**enable** | **disable** | **status**]	(Solaris only) If SSL is implemented in your SGM system, manages SSL support in SGM: • **enable**—Enables SSL support. If you enter this command and SSL has not been implemented in your SGM system, SGM prompts you to contact Cisco TAC or your Cisco Account Team for help in implementing SSL. • **disable**—Disables SSL support. • **status**—Displays the current status of SSL support in SGM, including whether SSL support is enabled or disabled and which SSL keys and certificates exist. See the "Implementing SSL Support in SGM" section on page 4-24 for more information on the use of this command. You must be logged in as the root user (not as a super user) to use this command.
sgm sslstatus	(Solaris only) If SSL is implemented in your SGM system, displays current status for SSL support in SGM, including whether SSL support is enabled or disabled and which SSL keys and certificates exist. See the "Implementing SSL Support in SGM" section on page 4-24 for more information on the use of this command. You must be logged in as the root user (not as a super user) to use this command.
sgm start	(Solaris only) Starts all SGM servers on the local host. You must be logged in as the root user or as a super user to use this command.

Table B-1 SGM Commands (continued)

Command	Description
sgm start client [*hostname*]	(Solaris only) Starts an SGM client on the specified host. If no host name is specified, starts an SGM client on the default host, as specified during installation. See the "Connecting to a New Server" section on page 3-284 for information about determining the default host. If you Telnet into a remote workstation, the DISPLAY variable must be set to your local display, or you cannot use this command. If the DISPLAY variable is not set automatically, you must set it manually. See the "Setting the DISPLAY Variable (Solaris Only)" section on page 5-44 for details. This command has the same function as the **sgm client** command.
sgm start gttclient [*hostname*]	(Solaris only) Starts an SGM GTT client on the specified host. If no host name is specified, starts an SGM GTT client on the default host, as specified during installation. See the "Connecting to a New Server" section on page 3-284 for information about determining the default host. If you Telnet into a remote workstation, the DISPLAY variable must be set to your local display, or you cannot use this command. If the DISPLAY variable is not set automatically, you must set it manually. See the "Setting the DISPLAY Variable (Solaris Only)" section on page 5-44 for details. This command has the same function as the **sgm gttclient** command.
sgm start jsp	(Solaris only) Starts the SGM JSP Server on the local host. You must be logged in as the root user or as a super user to use this command.
sgm start pm	(Solaris only) Starts the SGM Process Manager and all managed processes on the local host. You must be logged in as the root user or as a super user to use this command.

Table B-1 SGM Commands (continued)

Command	Description
sgm start web	(Solaris only) Starts the SGM Web Server on the local host. You must be logged in as the root user or as a super user to use this command.
sgm statreps [**acct** | **noacct**]	(Solaris only) Specifies whether SGM is to generate accounting statistics reports: • **acct**—Generate accounting statistics reports. • **noacct**—Do not generate accounting statistics reports. This is the default setting. See the "Viewing SGM Accounting Statistics Reports" section on page 3-248 for more information on the use of this command. You must be logged in as the root user or as a super user to use this command.
sgm statreps clean	(Solaris only) Removes all data from SGM network statistics reports, restoring the reports to a "clean" state. See the "Modifying the Way SGM Handles Statistics Reports (Solaris Only)" section on page 3-220 for more information on the use of this command. You must be logged in as the root user or as a super user to use this command.
sgm statreps cleancustom [*tag*]	(Solaris only) Removes all data from one or more SGM custom statistics reports, restoring the reports to a "clean" state: • To clean all custom reports, enter **sgm statreps cleancustom**. • To clean a single custom report, enter **sgm statreps cleancustom** *tag*, where *tag* is the ID tag of the custom report you want to clean. See the "Modifying the Way SGM Handles Statistics Reports (Solaris Only)" section on page 3-220 for more information on the use of this command. You must be logged in as the root user or as a super user to use this command.

Table B-1 SGM Commands (continued)

Command	Description
sgm statreps dailyage [*number-of-days*]	(Solaris only) Maximum number of days SGM is to archive daily network statistics reports. If you enter this command without the *number-of-days* argument, SGM displays the current maximum number of days. You can then change that value, or leave it as-is. The valid range is 1 day to an unlimited number of days. The default value is 90 days. See the "Modifying the Way SGM Handles Statistics Reports (Solaris Only)" section on page 3-220 for more information on the use of this command. This command has the same function as the **sgm repdailyage** command. You must be logged in as the root user or as a super user to use this command.
sgm statreps [**disable** | **enable**]	(Solaris only) Enables SGM to generate network statistics reports: • **enable**—Generate network statistics reports. This is the default setting. • **disable**—Do not generate network statistics reports. See the "Modifying the Way SGM Handles Statistics Reports (Solaris Only)" section on page 3-220 for more information on the use of this command. You must be logged in as the root user or as a super user to use this command.

Table B-1 SGM Commands (continued)

Command	Description
sgm statreps [**diskcheck** | **nodiskcheck**]	(Solaris only) Specifies whether SGM is to verify that a disk has at least 10 MB of space remaining before generating network statistics reports: • **diskcheck**—Verify the disk space. This is the default setting. • **nodiskcheck**—Do not verify the disk space. If your system does not return the necessary amount of free space, in a correct format that SGM can parse, this command enables SGM to disable checking to allow reporting to continue. See the "Modifying the Way SGM Handles Statistics Reports (Solaris Only)" section on page 3-220 for more information on the use of this command. You must be logged in as the root user or as a super user to use this command.
sgm statreps [**export** | **noexport**]	(Solaris only) Specifies whether SGM is to generate network statistics reports in export format: • **export**—Generate network statistics reports in export format. This is the default setting. • **noexport**—Do not generate network statistics reports in export format. See the "Modifying the Way SGM Handles Statistics Reports (Solaris Only)" section on page 3-220 for more information on the use of this command. You must be logged in as the root user or as a super user to use this command.

Table B-1 SGM Commands (continued)

Command	Description
sgm statreps hourlyage [*number-of-days*]	(Solaris only) Maximum number of days SGM is to archive hourly network statistics reports. If you enter this command without the *number-of-days* argument, SGM displays the current maximum number of days. You can then change that value, or leave it as-is. The valid range is 1 day to an unlimited number of days. The default value is 31 days. See the "Modifying the Way SGM Handles Statistics Reports (Solaris Only)" section on page 3-220 for more information on the use of this command. This command has the same function as the **sgm rephourlyage** command. You must be logged in as the root user or as a super user to use this command.
sgm statreps [**iplinks** | **noiplinks**]	(Solaris only) Specifies whether SGM is to include links that use the Stream Control Transmission Protocol (SCTP) IP transport protocol in network statistics reports: • **iplinks**—Include SCTPIP links. This is the default setting. • **noiplinks**—Do not include SCTPIP links. See the "Modifying the Way SGM Handles Statistics Reports (Solaris Only)" section on page 3-220 for more information on the use of this command. You must be logged in as the root user or as a super user to use this command.

Table B-1 SGM Commands (continued)

Command	Description
sgm statreps [**nullcaps** | **nonullcaps**]	(Solaris only) Specifies whether SGM is to include links that do not have planned send and receive capacities in network statistics reports: • **nullcaps**—Include links that do not have planned send and receive capacities. This is the default setting. • **nonullcaps**—Do not include links that do not have planned send and receive capacities. See the "Modifying the Way SGM Handles Statistics Reports (Solaris Only)" section on page 3-220 for more information on the use of this command. You must be logged in as the root user or as a super user to use this command.
sgm statreps servratio [*factor*]	(Solaris only) Displays a gray background in the InSrv cell in a network statistics report, if the following condition is met: **Current In-Service <** *factor* *** Long-Term In-Service** The default value for *factor* is **0.95**. See the "Modifying the Way SGM Handles Statistics Reports (Solaris Only)" section on page 3-220 for more information on the use of this command. You must be logged in as the root user or as a super user to use this command.
sgm statreps status	(Solaris only) Displays the current status of all SGM network statistics report parameters. These are the parameters that are set using the other **sgm statreps** commands, such as **sgm statreps** [**disable** | **enable**] and **sgm statreps** [**diskcheck** | **nodiskcheck**]. See the "Modifying the Way SGM Handles Statistics Reports (Solaris Only)" section on page 3-220 for more information on the use of this command. You must be logged in as the root user or as a super user to use this command.

Table B-1 SGM Commands (continued)

Command	Description
sgm statreps timemode [**12** | **24**]	(Solaris only) Sets the time mode for dates in network statistics reports: • **12**—Use 12-hour time, with AM and PM. 1:00 in the afternoon is 1:00 PM. • **24**—Use 24-hour time, also called military time. 1:00 in the afternoon is 13:00. This is the default setting. See the "Modifying the Way SGM Handles Statistics Reports (Solaris Only)" section on page 3-220 for more information on the use of this command. You must be logged in as the root user or as a super user to use this command.
sgm statreps timer	(Solaris only) Displays the timer file for SGM network statistics reports. The timer file is useful for identifying how much time SGM spends gathering report data and generating reports. See the "Modifying the Way SGM Handles Statistics Reports (Solaris Only)" section on page 3-220 for more information on the use of this command. You must be logged in as the root user or as a super user to use this command.
sgm statreps utilratio [*factor*]	(Solaris only) Displays a gray background in the Send Utilization or Receive Utilization cell in a network statistics report, if the following condition is met: **Current Utilization >** *factor* *** Long-Term Utilization** The default value for *factor* is **1.50**. See the "Modifying the Way SGM Handles Statistics Reports (Solaris Only)" section on page 3-220 for more information on the use of this command. You must be logged in as the root user or as a super user to use this command.

Table B-1 SGM Commands (continued)

Command	Description
sgm status	(Solaris only) Displays the status of all SGM servers on the local host. For a sample output for this command, see the "Output of sgm status Command" section on page B-65.
sgm stop	(Solaris only) Stops all SGM servers on the local host. You must be logged in as the root user or as a super user to use this command.
sgm stopclients	(Solaris only) Stops all SGM clients running on the local host. You must be logged in as the root user or as a super user to use this command.
sgm stop jsp	(Solaris only) Stops the SGM JSP Server on the local host. You must be logged in as the root user or as a super user to use this command.
sgm stop pm	(Solaris only) Stops the SGM Process Manager and all managed processes on the local host. You must be logged in as the root user or as a super user to use this command.
sgm stop web	(Solaris only) Stops the SGM Web Server on the local host. You must be logged in as the root user or as a super user to use this command.

Table B-1 SGM Commands (continued)

Command	Description
sgm superuser [*username*]	(Solaris only) Enables the specified user to perform most functions that otherwise require the user to be logged in as the root user. (The root user can still perform those functions, too.) The specified user account must exist in the local */etc/passwd* file. You cannot specify a user that is defined in a distributed Network Information Services (NIS) system. **Note** As a super user, you can adversely affect your operating environment if you are unaware of the effects of the commands you use. If you are a relatively inexperienced UNIX user, limit your activities as a super user to the tasks described in this document. For a complete list of the SGM commands that a super user *cannot* use, as well as other super user considerations, see the "Specifying a Super User (Solaris Only)" section on page 4-22. You must be logged in as the root user (not as a super user) to use this command.
sgm syncusers	(Solaris only) If SGM User-Based Access is enabled and **sgm authtype** is set to **solaris**, synchronizes local SGM passwords with Solaris. See the "Maintaining Your SGM Security System (Solaris Only)" section on page 4-17 for more information on the use of this command. You must be logged in as the root user (not as a super user) to use this command.
sgm tac	(Solaris only) Collects important troubleshooting information for the Cisco Technical Assistance Center, and writes the information to the */opt/CSCOsgm/tmp/cisco_sgm_tshoot.log* file. You must be logged in as the root user or as a super user to use this command.

Table B-1 SGM Commands (continued)

Command	Description
sgm telnetpath	Specifies the path to the Telnet application to use for Telnet sessions on the SGM client, as well as any special parameters to pass to the Telnet application. • On Solaris, the default path is */usr/bin/telnet*. • On Windows, you do not need to specify a path. Windows detects and launches the Telnet application wherever it is located. You must be logged in as the root user (not as a super user) to use this command.
sgm testeventconfig [**-print**] [*filename*]	(Solaris only) Parses and validates the specified event configuration file before you load it into SGM. The default filename is *SgmEvent.conf*. If you use a different event configuration file, it must reside in the same directory as the *eventconfiguration.dtd* file. The **-print** keyword dumps the event configuration to STDOUT for visual validation. You must be logged in as the root user or as a super user to use this command.

Table B-1 SGM Commands (continued)

Command	Description
sgm trapaccess [**add** [*ip-addr*] | **clear** | **edit** | **list** | **rem** [*ip-addr*] | **sample**]	(Solaris only) Enables you to create and manage a list of router IP addresses allowed to send traps to the SGM server. The list of allowed router IP addresses is contained in the *trapaccess.conf* file. By default, when you first install SGM, the *trapaccess.conf* file does not exist and SGM allows all IP addresses to send traps to the SGM server. To create the *trapaccess.conf* file and work with the list of allowed client IP addresses, specify one of the following keywords: • **add**—Add the specified IP address to the *trapaccess.conf* file. If the file does not already exist, this command creates the file containing the first entry. • **clear**—Remove all IP addresses from the *trapaccess.conf* file, and allow traps from any SGM client IP address. • **edit**—Open and edit the *trapaccess.conf* file directly. If the *trapaccess.conf* file does not already exist, this command creates an empty file. • **list**—List all IP addresses currently in the *trapaccess.conf* file. If no IP addresses are listed (that is, the list is empty), traps from any SGM IP address are allowed. • **rem**—Remove the specified IP address from the *trapaccess.conf* file. • **sample**—Print out a sample *trapaccess.conf* file. Any changes you make take effect when you restart the SGM server. See the "Limiting Traps by IP Address (Solaris Only)" section on page 5-42 for more information about using this command. You must be logged in as the root user or as a super user to use this command.

Table B-1 SGM Commands (continued)

Command	Description
sgm trapsetup [**disable**]	(Solaris only) Configures SGM to receive SNMP traps, or prevents SGM from receiving traps, then restarts the SGM server. SGM gives you the option to receive traps natively or using HP OpenView. When you select an SNMP trap port number for the SGM server, make sure your ITP routers use the same SNMP trap port number. See the description of the **snmp-server host** command in the "ITP Router Requirements" section of the *Cisco Signaling Gateway Manager Installation Guide* for more information. To prevent SGM from receiving traps, enter the **sgm trapsetup disable** command. SGM restarts the SGM server. You must be logged in as the root user (not as a super user) to use this command.
sgm trapstatus	(Solaris only) Displays the current trap reception configuration for SGM, including: • SNMP trap integration type: – **native**—SGM receives traps natively on a UDP port. – **hpov**—SGM receives traps using HP OpenView. • For **native**, SGM also displays the UDP port number on which SGM receives traps natively. • For **hpov**, SGM also displays the location of the HP OpenView home directory. • Status for the sgmTrapReceiver (such as **Running** or **Stopped**).
sgm uninstall	(Solaris only) Uninstalls SGM. You must be logged in as the root user (not as a super user) to use this command.

Table B-1 SGM Commands (continued)

Command	Description
sgm unknownage [*number-of-days*]	(Solaris only) Sets the maximum number of days to retain **Unknown** nodes, linksets, and links before deleting them from the SGM database. If you enter this command without the *number-of-days* argument, SGM displays the current maximum number of days. You can then change that value, or leave it as-is. The valid range is 1 day to an unlimited number of days. The default value is 7 days. Setting this value to 0 days means delete all **Unknown** nodes, linksets, and links at the next poll. You must be logged in as the root user or as a super user to use this command.
sgm updateuser [*username*]	(Solaris only) If SGM User-Based Access is enabled, changes the authentication level for the specified user. Valid levels are: • **1**—Basic User • **2**—Power User • **3**—Network Operator • **4**—Network Administrator • **5**—System Administrator If **sgm authtype** is set to **local**, this command also enables you to change the following settings: • User's password. When setting the password, follow the rules and considerations in the "Creating Secure Passwords" section on page 4-5. See the "Enabling and Modifying Users and Passwords (Solaris Only)" section on page 4-15 for more information on authentication levels, and on the use of this command. You must be logged in as the root user or as a super user to use this command.

Table B-1 SGM Commands (continued)

Command	Description
sgm useraccess [**disable** | **enable**]	(Solaris only) Enables or disables SGM User-Based Access. User-Based Access provides multi-level password-protected access to SGM features. Each user can have a unique username and password. Each user can also be assigned to one of five levels of access, which control the list of SGM features accessible by that user. You must enable SGM User-Based Access in order to use the associated SGM security commands. See the "Implementing SGM User-Based Access (Solaris Only)" section on page 4-2 for more information. You must be logged in as the root user or as a super user to use this command.
sgm userpass [*username*]	(Solaris only) If SGM User-Based Access is enabled and **sgm authtype** is set to **local**, changes the specified user's SGM security authentication password. If the user's authentication has been disabled, either automatically by SGM or by a super user, this command re-enables the user's authentication with a new password. If **sgm authtype** is set to **solaris**, you cannot use this command. Instead, you must manage passwords on the external authentication servers. See the "Enabling and Modifying Users and Passwords (Solaris Only)" section on page 4-15 for more information on the use of this command. You must be logged in as the root user or as a super user to use this command.
sgm version	(Solaris only) Displays version information for SGM servers and clients on the local host.
sgm viewlog	(Solaris only) Uses PAGER to display the system messages *messageLog.txt* file. This command has the same function as the **sgm msglog** command.

Table B-1 SGM Commands (continued)

Command	Description
sgm wall *message_string*	(Solaris only) Sends a message to all clients connected to the server. For example: **./sgm wall Server going down at 9:00 pm tonight.** sends the following message: **Server going down at 9:00 pm tonight.** SGM ignores quotation marks in *message_string*. To include quotation marks, use the escape character (\) in combination with quotation marks. For example: **./sgm wall Example of the \"sgm wall\" command.** sends the following message: **Example of the "sgm wall" command.** You must be logged in as the root user or as a super user to use this command.
sgm webaccesslog [**clear** | **-r**]	(Solaris only) Uses PAGER to display the SGM system Web access log file for the server to which you are connected, and which is currently running the SGM server. The system Web access log lists all SGM system Web access messages that have been logged for the SGM server. This provides an audit trail of all access to the SGM server via the Web interface. To clear the log and restart the server, enter **sgm webaccesslog clear**. To display the contents of the log in reverse order, with the most recent Web access messages at the beginning of the log, enter **sgm webaccesslog -r**. You must be logged in as the root user or as a super user to use this command.

Table B-1 SGM Commands (continued)

Command	Description
sgm weberrorlog [**clear** | **-r**]	(Solaris only) Uses PAGER to display the SGM Web server error log file for the server to which you are connected, and which is currently running the SGM server. The Web server error log lists all SGM Web error messages that have been logged for the SGM Web server. To clear the log and restart the server, enter **sgm weberrorlog clear**. To display the contents of the log in reverse order, with the most recent Web error messages at the beginning of the log, enter **sgm weberrorlog -r**. You must be logged in as the root user or as a super user to use this command.
sgm weblogupdate [*interval* | **disable**]	(Solaris only) Controls how often, in seconds, SGM updates certain Web output. When you enter this command, SGM displays the current interval. You can then change that value, or leave it as-is. The valid range is 1 second to an unlimited number of seconds. The default value is 300 seconds (5 minutes). To disable the update interval, enter the **sgm weblogupdate disable** command. This option lessens SGM's CPU usage on both the server and client. You must be logged in as the root user or as a super user to use this command.
sgm webnames [**display** | **real**]	(Solaris only) Specifies whether SGM is to show real node names or display names in Web pages: • **real**—Show the real DNS names of nodes in Web pages, as discovered by SGM. This is the default setting. • **display**—Show display names in Web pages. Display names are new names that you specify for nodes. For more information about display names, see the "Editing a Node" section on page 3-99. You must be logged in as the root user or as a super user to use this command.

Table B-1 SGM Commands (continued)

Command	Description
sgm webport [*port-number*]	(Solaris only) Sets a new port number for the Web server, where *port-number* is the new, numeric port number. SGM verifies that the new port number is not already in use. The new port number must contain only numbers. If you enter a port number that contains non-numeric characters, such as **sgm13**, SGM displays an error message and returns to the command prompt without changing the port number. You must be logged in as the root user (not as a super user) to use this command.
sgm webutil [**percent** | **erlangs**]	(Solaris only) Specifies whether SGM is to display send and receive utilization for linksets and links as percentages or in Erlangs, in Web pages: • **percent**—SGM displays utilization as a percentage. This is the default setting. • **erlangs**—SGM displays utilization in Erlangs. See the "Working with SGM Statistics Reports" section on page 3-218 for more information on the use of this command. You must be logged in as the root user or as a super user to use this command.
sgm who	(Solaris only) Displays a list of all client user names and processes connected to the server.

Output of sgm status Command

The following example shows the status information displayed when you enter the **sgm status** command:

```
# ./sgm status
============================================================
SGM Server Package Version:      2.2.0
SGM Server Package Build Date:   Sun Oct 27 03:03 EDT 2002
SGM Server Package Hostname:     sgm-sun8
============================================================
   sgmProcessManager:  2.2.0    Sun Oct 27 03:01 EDT 2002
   sgmMsgLogServer:    2.2.0    Sun Oct 27 03:01 EDT 2002
   sgmDataServer:      2.2.0    Sun Oct 27 03:01 EDT 2002
   sgmTrapReceiver:    2.2.0    Sun Oct 27 03:01 EDT 2002
============================================================
SGM Naming  Server  IS Running.
SGM Web     Server  IS Running.
SGM JSP     Server  IS Running.
SGM Process Manager IS Running with processes:

PROCESS              STATUS   PID        Last Message

sgmDataServer        Ready    24785      Running
sgmMsgLogServer      Ready    24771      Running
sgmTrapReceiver      Ready    24799      Running

SSL Support is Disabled.

SGM Server was last restarted:
    Sun Oct 27 12:05:06 EDT 2002

Solaris uptime:
    2:12pm up 26 day(s), 16:29, 1 user, load average: 0.32, 0.14, 0.11

============================================================
SGM Client Package Version:      2.2.0
SGM Client Package Build Date:   Sun Oct 27 03:03 EDT 2002
============================================================

   sgmClient:          2.2.0   Sun Oct 27 03:01 EDT 2002
============================================================

Current time is: 2002/10/31 14:12:52
```

Output of sgm export Command

The following example shows the format of the exported SGM data when you enter the **sgm export** command:

```
# ./sgm export
# v2.2.0
# t1015354083591 | Mon Oct 28 13:48:03 EST 2002
#
# Total 50 nodes
# name | displayname | sgmid | description | cllicode | ipaddress | pointcode |
secondary | capability | state | statetimestamp | devicetype | iconname | sysdes
cr | lastpolltimestamp | lastpolltime | avgpolltime | lasterrormsg | lasterrorti
me | notesexist
sgm-75-70a.cisco.com | null | 1002 | null | code70a | [172.18.16.10, 172.18.16.2
34] | 5.10.1 | 3.10.1 | 2.10.1 | Warning | 1015276286169 | Cisco7507 | null | sy
sDescr | 1015353397341 | 1708 | 1726 | Node sgm-75-70a.cisco.com changed state f
rom Unmanaged to Unknown. | 1015276189446 | false
sgm-75-59a.cisco.com | null | 1006 | null |  | [172.18.16.108] | 5.9.3 | null |
null | Warning | 1015275644164 | Cisco7507 | null | sysDescr | 1015353611179 | 1
549 | 1498 | null | 0 | false
sgm-26-51a.cisco.com | null | 1008 | null | 51a89-   | [172.18.16.34, 172.18.16.
146] | 5.1.1 | 2.1.1 | 3.1.1 | Active | 1015343576992 | Cisco2600 | null | sysDe
scr | 1015353559225 | 1030 | 1032 | null | 0 | false
```

Output of sgm gttcheck Command

The following examples show the output when you enter the **sgm gttcheck** command with the **list**, **semantics**, and **syntax** keywords.

- Output of sgm gttcheck list Command, page B-67
- Output of sgm gttcheck semantics Command, page B-67
- Output of sgm gttcheck syntax Command, page B-69

Output of sgm gttcheck list Command

```
# ./sgm gttcheck list
large.ansi.sample
largest.sample
midsize.sample
small.ansi.sample
small.sample
```

Output of sgm gttcheck semantics Command

```
# ./sgm gttcheck semantics sgm-seed1 small.sample
==================================
Parsing and syntax checking GTT file: small.sample
==================================
Loading GTT file: small.sample
==> parsing GTT file...
==> resolving GTT entries...
Operation completed successfully.
==================================
GTT file info:
==================================
               Version = 1.0
               Variant = itu
      Selector entries = 4
           GTA entries = 8
     App Group entries = 4
           MAP entries = 12
  Concerned PC entries = 4
==================================
Performing semantics checking for GTT file: small.sample
==================================
Validating GTT table for sgm-75-70a.cisco.com
==> retrieving ITP router information from sgm-75-70a.cisco.com
==> validating GTA table ...
Error #1: no route to destination 2.2.2
        gtest,349,1012,gt,100, , ,
Error #2: no route to destination 2.2.2
        gtest,828,1012,gt, ,100, ,
Error #3: no route to destination 2.2.2
        gtest,828258,1012,pcssn,129, , ,
Error #4: no route to destination 2.2.2
        gtest,8282588595,1012,pcssn,100, , ,1
Error #5: no route to destination 1.11.1
        gtest,980,859,pcssn,10, , ,
```

```
==> validating App Group table ...
Error #6: no route to destination 1.12.1
        atest,sha,1,861,gt,
Error #7: no route to destination 1.11.1
        atest,sha,2,859,pcssn,
Error #8: no route to destination 2.2.2
        atest,sha,3,1012,pcssn,10

Error #9: no route to destination 1.12.7
        atest2,sha,1,867,gt,100
==> validating MAP table ...
Error #10: no route to destination 1.1.1
        m809,10,sol, , , ,0,0
Error #11: no route to destination 1.11.1
        m859,10,sol, , , ,0,0
Error #12: no route to destination 1.12.1
        m861,10,sol, , , ,0,0
Error #13: no route to destination 1.12.7
        m867,10,sol, , , ,0,0
Error #14: no route to destination 1.12.7
        m867,100,sol, , , ,0,0
Error #15: no route to destination 2.2.2
        m1012,10,sol, , , ,0,0
Error #16: no route to destination 2.2.2
        m1012,100,sol, , , ,0,0
Error #17: no route to destination 2.2.2
        m1012,129,sol, , , ,0,0
Error #18: no route to destination 1.11.1
        m859,20,sha,861,20,list1,0,1
Error #19: no route to destination 1.12.1
        m859,20,sha,861,20,list1,0,1
Error #20: no route to destination 1.12.1
        m861,20,sha,859,20,list1,0,1
Error #21: no route to destination 1.11.1
        m861,20,sha,859,20,list1,0,1
Error #22: no route to destination 1.11.1
        m859,25,dom,861,25,list7,1,0
Error #23: no route to destination 1.12.1
        m859,25,dom,861,25,list7,1,0
Error #24: no route to destination 1.12.1
        m861,25,dom,859,25,list7,1,0
Error #25: no route to destination 1.11.1
        m861,25,dom,859,25,list7,1,0
```

```
==> validating Concerned PC List table ...
Error #26: no route to destination 1.1.1
        clist1,809
Error #27: no route to destination 1.11.1
        clist1,859
Error #28: no route to destination 2.2.2
        clist3,1012
Error #29: no route to destination 2.2.2
        clist7,1012

Operation completed with errors: Total 29 errors, 0 warnings
====================================
```

Output of sgm gttcheck syntax Command

```
# ./sgm gttcheck syntax small.sample
====================================
Parsing and syntax checking GTT file: small.sample
====================================
Loading GTT file: small.sample
==> parsing GTT file...
==> resolving GTT entries...
Operation completed successfully.
====================================
GTT file info:
====================================
               Version = 1.0
               Variant = itu
      Selector entries = 4
           GTA entries = 8
     App Group entries = 4
           MAP entries = 12
  Concerned PC entries = 4
====================================
```