Release Notes for Cisco Signaling Gateway Manager Release 4.1.2

CDC Date: March 31, 2007

These release notes describe the caveats for Cisco Signaling Gateway Manager (SGM) Release 4.1.2.

Note You can access the most current Cisco documentation, including these release notes, online:
http://www.cisco.com/en/US/products/sw/wirelssw/ps2153/tsd_products_support_series_home.html
You can find the latest updates for SGM software and additional documentation online:
http://www.cisco.com/go/sgm

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Contents

These release notes contain the following sections:

Bugs Fixed in SGM 4.1.2

The following bugs have been fixed in SGM 4.1.2:

Bug ID	Description
CSCsd92735	The scroll position of the linkset troubleshooting output in the linkset real-time window resets after a window update.
CSCse35408	When creating an address table in the Address Table Editor, the network name is sometimes not displayed and the message log on the server reports an error.
CSCse40842	SGM user authentication with restricted passwords set in a custom dictionary file fails to honor the restricted passwords.
CSCse41814	The java client fails to launch from a CLI on Windows with SSL.
CSCse44542	A signaling point with no network name is not handled properly.

Bug ID	Description
CSCse53244	Setting the clitimeout causes the client to exit even if there is activity in the client window.
CSCse53247	The GTT and Address Table clients do not timeout after the clitimeout has been set.
CSCse55790	The sgmTrapReceiver process fails to start when SGM User Access is enabled on a multi-home box.
CSCse55795	When SSL is enabled and you are launching web reports from the SGM client, the web browser may point to the "http://" URL prefix, but not the correct "https://" URL prefix.
CSCse88193	SGM route table and GTT table deployment wizard shows “unexpected error” or "IndexOutOfBoundsException."
CSCse89318	Need to update how certain SGM CLI commands work when super user is enabled for a user.
CSCsg07406	The Edit Properties dialog for a node does not allow you to add a valid domain name in the Name field. For example, if the original name is ems1941kmt and you change it to ems1941kmt.cisco.com and save, you get an error.
CSCsg08590	After a switchover, the time display in the switchover history is invalid.
CSCsg16648	When installing the SGM 4.1.1 patch on a 4.1.0 system with SSL installed, the patch will not install.
CSCsg18842	The ciscoGspCongestionChange trap triggers a cItpSpCongestionChange event, which causes event customizations made with the SGM Event Configurator for link congestions traps to not be displayed by SGM.
CSCsg52230	Downloading the ITP route table to a device with a period (.) in its hostname fails and causes a client timeout.
CSCsg60674	If you open a link or linkset troubleshooting window and add or remove credentials for its corresponding node, the credentials change is only reflected in one of the two troubleshooting subtabs.
CSCsg60798	SGM web reports provide no output even if the reports run properly on the server when a volume manager is in use on the server.

Bug ID	Description
CSCsg93174	After upgrading from SGM 4.1 to SGM 4.1.1 on Linux, you cannot access any JSP pages on the SGM web interface.
CSCsg93232	Certain application server and/or application server process configurations cause SGM to aggregate states incorrectly when a detail poller is active.
CSCsh14085	When a statistical or accounting report has no data, a blank page appears with only the page URLs at the bottom. In this case, an informative message such as "No entries found" should appear.
CSCsh17366	The cleanall command does not clear out user access for the SGM web client in 4.1.1.
CSCsh25487	If you supply an invalid username and/or password for troubleshooting credentials, the SGM client can sometimes appear to never complete and an exception is logged in the sgmConsoleLog.
CSCsh30393	The point code mask does not appear in bits in the route details table even though it is set to appear in bits in the SGM client preferences.
CSCsh35821	Deploying an address table file with an invalid enable password eventually times out instead of reporting that a bad password was supplied.
CSCsh41930	The GTT client fails to load a GTT table with more than 10,000 lines from an ITP.
CSCsh58420	There is an exception when deploying a route table, GTT, or MLR address table configuration file to an ITP, if the target ITP has a full flash filesystem.
CSCsh74772	When you issue the sgm tac command on a Linux server running SGM, a message similar to the following appears: line 10462: [: sgmLinkStats.debug.zip: The resulting cisco_sgm_tshoot.log.zip file does not contain any files with the debug extension (.debug) found in /opt/CSCOsgm/tmp.

Bug ID	Description
CSCsh77803	When a trigger is configured with no action, or a trigger or a subtrigger is configured with a 'result' action, the MLR trigger and subtrigger statistics reports may list an incorrect action.
CSCsh81431	When you select the CPU Utilization tab for a node, and the slot-specific process utilization tab is selected, the Time Created column lists incorrect creation times for the processes running on a device.
CSCsh84394	Within the Deploy from Archive window, when you select a configuration type (such as GTT, Route, or MLR) and no archived configurations exist, an error window appears that says, “Failed to update model.”
CSCsf09209	When you change the default server name on the Windows client by using the **sgm servername** command or the **Start > Cisco SGM Client > Modify Default SGM Server Name** option, the action fails and an exception appears.

Note SGM 4.1 has been successfully integrated with HP OpenView 6.0, 6.1, and 6.2. Other versions of HP OpenView may or may not integrate successfully.

Caveats and Known Bugs in SGM 4.1.2

The following caveat and known bug exists in SGM 4.1.2:

Exception occurs within topology window

- CSCef67144

  Sometimes when using the client on a Solaris multi-processor computer, an exception occurs when having the topology window displayed and manipulating views.

  Workaround: Close the topology window and re-open.

Related Documentation

Refer to the following publications for additional information, available online at http://www.cisco.com/en/US/products/sw/wirelssw/ps2153/tsd_products_support_series_home.html:

- *Cisco Signaling Gateway Manager Installation Guide, Release 4.1*
- *Cisco Signaling Gateway Manager User Guide, Release 4.1*

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a library of technical product documentation on a portable medium. The DVD enables you to access installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the HTML documentation and some of the PDF files found on the Cisco website at this URL:

http://www.cisco.com/univercd/home/home.htm

The Product Documentation DVD is created and released regularly. DVDs are available singly or by subscription. Registered Cisco.com users can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at the Product Documentation Store at this URL:

http://www.cisco.com/go/marketplace/docstore

Ordering Documentation

You must be a registered Cisco.com user to access Cisco Marketplace. Registered users may order Cisco documentation at the Product Documentation Store at this URL:

http://www.cisco.com/go/marketplace/docstore

If you do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Documentation Feedback

You can provide feedback about Cisco technical documentation on the Cisco Support site area by entering your comments in the feedback form available in every online document.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to do the following:

- Report security vulnerabilities in Cisco products
- Obtain assistance with security incidents that involve Cisco products
- Register to receive security information from Cisco

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For emergencies only—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*x*.

Never use a revoked encryption key or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT to find other means of encrypting the data before sending any sensitive material.

Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can receive these announcements by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information.

To access the Product Alert Tool, you must be a registered Cisco.com user. Registered users can access the tool at this URL:

http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en

To register as a Cisco.com user, go to this URL:

http://tools.cisco.com/RPF/register/register.do

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Support website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Support Website

The Cisco Support website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day at this URL:

http://www.cisco.com/en/US/support/index.html

Access to all tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Before you submit a request for service online or by phone, use the **Cisco Product Identification Tool** to locate your product serial number. You can access this tool from the Cisco Support website by clicking the **Get Tools & Resources** link, clicking the **All Tools (A-Z)** tab, and then choosing **Cisco Product Identification Tool** from the alphabetical list. This tool offers three search options: by product ID or model name; by tree view; or, for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Tip **Displaying and Searching on Cisco.com**

If you suspect that the browser is not refreshing a web page, force the browser to update the web page by holding down the Ctrl key while pressing **F5**.

To find technical information, narrow your search to look in technical documentation, not the entire Cisco.com website. After using the Search box on the Cisco.com home page, click the **Advanced Search** link next to the Search box on the resulting page and then click the **Technical Support & Documentation** radio button.

To provide feedback about the Cisco.com website or a particular technical document, click **Contacts & Feedback** at the top of any Cisco.com web page.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411
Australia: 1 800 805 227
EMEA: +32 2 704 55 55
USA: 1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The Cisco Online Subscription Center is the website where you can sign up for a variety of Cisco e-mail newsletters and other communications. Create a profile and then select the subscriptions that you would like to receive. To visit the Cisco Online Subscription Center, go to this URL:

  http://www.cisco.com/offer/subscribe

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco channel product offerings. To order and find out more about the *Cisco Product Quick Reference Guide*, go to this URL:

  http://www.cisco.com/go/guide

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- Cisco Press publishes a wide range of general networking, training, and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Internet Protocol Journal* is a quarterly journal published by Cisco for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website where networking professionals share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- "What's New in Cisco Documentation" is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of "What's New in Cisco Documentation" at this URL:

  http://www.cisco.com/univercd/cc/td/doc/abtunicd/136957.htm

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.