

# Release Notes for Cisco Service Control Management Suite Subscriber Manager (SCMS SM) 2.2.1

---

**Dec 14, 2004**

Cisco Release Notes for Service Control Management Suite Subscriber Manager (SCMS SM) 2.2.1

Supports: SCMS SM 2.2, SCMS SM 2.2.1

OL-7017-02

These release notes for the Cisco SCMS SM describe the enhancements provided in Cisco Release SCMS SM 2.2.1 and SCMS SM 2.2. These release notes are updated as needed.

For a list of the software caveats that apply to Cisco Release SCMS SM 2.2.1 see “Open Caveats – Cisco Release SCMS SM 2.2,” page 8.



---

**Corporate Headquarters:**

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

Copyright © 2004 Cisco Systems, Inc. All rights reserved.

# Contents

<b>INTRODUCTION.....</b>	<b>3</b>
SCMS SM 2.2.1.....	3
<i>Check Lease Period when Replying to Pull Requests</i> .....	3
<i>Default Package Property in the Radius Listener LEG</i> .....	3
<i>Correction of Default Value in Configuration File of SM 2.2</i> .....	3
<i>Radius Listener LEG Login of Existing Subscribers</i> .....	4
NEW FUNCTIONALITY IN CISCO RELEASE SCMS SM 2.2 .....	4
<i>SM Fail-Over</i> .....	4
<i>SM Configuration Changes</i> .....	7
<b>CAVEATS .....</b>	<b>8</b>
OPEN CAVEATS – CISCO RELEASE SCMS SM 2.2 .....	8
<b>OBTAINING TECHNICAL ASSISTANCE.....</b>	<b>10</b>
CISCO TECHNICAL SUPPORT WEBSITE .....	10
SUBMITTING A SERVICE REQUEST .....	10
DEFINITIONS OF SERVICE REQUEST SEVERITY .....	11
<b>OBTAINING ADDITIONAL PUBLICATIONS AND INFORMATION .....</b>	<b>11</b>

# Introduction

Cisco is proud to release version 2.2.1 of its SM infrastructure.

SCMS SM 2.2.1 is a point release of SCMS SM 2.2. This point release includes some very important fixes of various bugs and issues that were identified in SCMS SM 2.2.

SCMS SM 2.2 presents an important step forward in the management infrastructure at the subscriber management level, and includes fail-over capabilities for the SM module using two SMs connected in a Veritas cluster.

This document outlines the new features and enhancements to the Management Infrastructure, and assumes the reader already has a good working knowledge of Cisco's solution. For additional information, please refer to Cisco's User Guides.

## SCMS SM 2.2.1

Various bugs and issues were fixed in release SCMS SM 2.2.1:

### Check Lease Period when Replying to Pull Requests

In SM 2.2, when the SM receives a Pull request from the SE, it responds with the details of the subscriber that is mapped to the IP address in the Pull request, without checking whether the lease period of the IP address was expired (this is relevant only for Cable or Satellite deployments, where IP addressees are allocated with a lease period)

In SM 2.2.1, when the SM receives a Pull request, it performs the relevant checks, and in case the IP address's lease period expired, the SM does not reply to the Pull request. The SE then applies a default policy to this IP address.

### Default Package Property in the Radius Listener LEG

Several issues which relate to the functionality of default value for the Package property in the Radius Listener LEG in SM 2.2 were resolved. The default Package property functionality can now be safely used.

### Correction of Default Value in Configuration File of SM 2.2

SM 2.2 configuration file was released with a *false* default value for the *push\_mode\_auto\_resync* parameter, instead of a *true* default value.

SM 2.2.1 configuration file is now released with the correct *true* default value.

## Radius Listener LEG Login of Existing Subscribers

In SM 2.2, when a log-in operation is performed through the Radius Listener LEG for a subscriber that already exists in the SM, and when this subscriber already has an assigned package, the repetitive login operation fails.

This issue was fixed in SM 2.2.1.

## New Functionality in Cisco Release SCMS SM 2.2

The following new functionalities are supported by Cisco for Cisco Release SCMS SM 2.2.

### SM Fail-Over

Recognizing that the SM plays a critical role in Cisco's SCAS BB solution that is deployed in Tier-one service provider environments, Cisco added fail-over capabilities to the SM.

The fail-over topology is based on two SUN servers that run the SM software, and operate as a Veritas Cluster.

The cluster components on each of the SUN machines exchange heartbeat information, and the primary SM also constantly replicates the content of its TimesTen database to the TimesTen database on the secondary SM. The two SM s use a virtual IP address for their communications with the SCE platforms and the AAA server. In case the primary SM fails, the secondary SM takes over, and starts operating with an updated database of subscriber information. The SCE platforms and the AAA server start communicating with the secondary SM.

This way, the continuity in providing subscriber information to the SCEs and backing up subscriber's states is preserved, making the SM a reliable carrier-grade solution.

### *Fail-Over Topology*

For implementing fail-over, Cisco is using the Veritas Cluster Server SW 3.5, with Replicated Data architecture. In this architecture, a replication mechanism is used for creating a copy of the primary SM's subscriber database on the secondary SM, leveraging the synchronization capabilities of the TimesTen In-Memory database.

The following types of information are backed-up:

- Mappings of Network-ID to Subscriber-ID
- Subscriber properties, such as policy index
- Subscriber states, such as the level of consumed volume of some service

This architecture was preferred over using an external storage device, mainly in order to enable support of seamless fail-over and minimal fail-over time.

The two SM servers should be deployed in the same NOC, and connected using two dedicated redundant types of connections, such as:

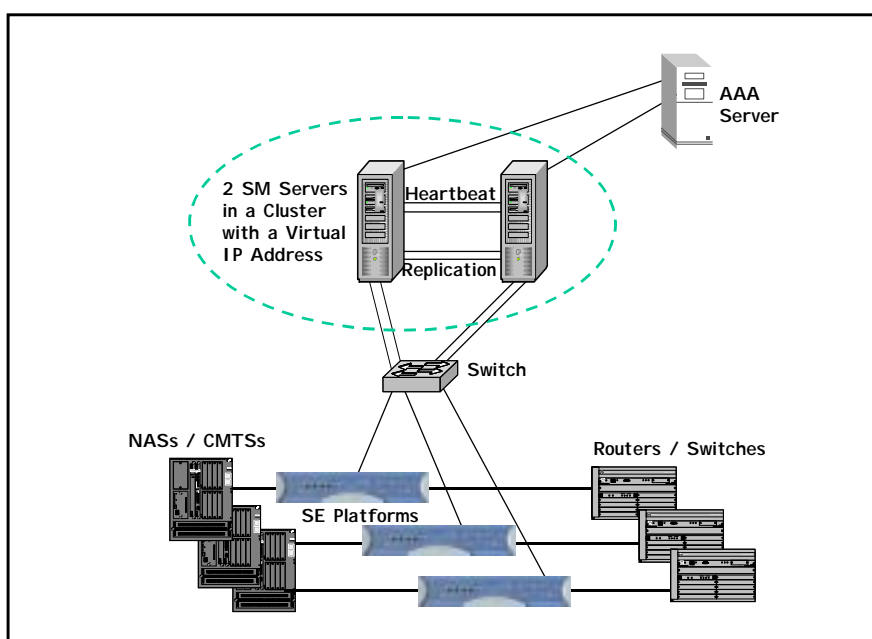
- Two Redundant heartbeat Fast Ethernet connections
- Two redundant replication Fast Ethernet connections

The two SMS support two additional NICs for management communications.

The two SM servers operate in hot-standby configuration, i.e. only one SM server is active at a given time. The active server processes the information coming to the AAA server, and communicates with the SCE platforms. The cluster of two SM servers uses a virtual IP address for communicating with the AAA servers and the SCEs, and two separate NICs are used for this communication.

The following figure presents two SM servers in a cluster-based fail-over configuration:

**Figure 1** *Fail-Over Configuration*



## Fail-Over


During normal operation, the Cluster Server mechanism automatically selects one of the SM servers to be primary and the other to be secondary.

The primary SM server performs all the normal SM functionality. The two servers maintain the heartbeat mechanism between them, and the primary server periodically replicates the subscriber database to the secondary server's database.

The secondary SM server acts as a hot-standby machine, so it is completely ready for taking-over at a minimum fail-over time.

The following types of failures trigger the fail-over mechanism:

- SM application failure including failure of the TimesTen database.
- SUN server failure, due to failure of one of the resources of the server.
- Primary cluster node failure – a failure of the primary SM as a node in the Veritas Server Cluster mechanism.

	
Note	Since each SUN machine has 2 NICs for connecting to external devices, a failure of one of the NICs just results in a move to the redundant NIC, without activating the fail-over mechanism

Once a failure is detected, the secondary SM takes over and performs the following:

- Takes over the IP resources of the virtual IP mechanism
- Creates IP connections with the SCEs and the AAA server.
- Starts processing information that is sent from the AAA server and forwards it to the SCEs.

## Recovery

The original primary SM server recovers manually or automatically, according to the type of failure that occurred.

The various types of recovery procedures are:

- Reboot recovery – this is an automatic recovery process, where the failed SM server reboots, and after establishing a connection with the other server, and synchronizing the databases, the cluster of the two SM servers is ready again for fail-over.
- Replacing an SM server – this is a manual recovery, where the failed SM server is physically replaced. After the new SM server machine is connected to the network and configured, and the two databases synchronize, the cluster of the two SM servers is ready again for fail-over.

## Management

The configuration of the two SM servers is performed using Command Line Utilities and a Configuration File. The actual configuration is performed for the primary SM and then replicated for the secondary SM.

All the configuration and administration of the Veritas Server Cluster is performed using Veritas tools.

Notifications are enabled through SNMP traps that the Veritas Cluster Server provides.

The Cluster Server supports SNMP traps such as:

- Fatal failure detected (local or remote)
- Secondary node starts fail-over procedure
- Secondary node is operational (end of fail-over)

## SM Configuration Changes

The configuration scheme of the SM was changed in SCMS SM version 2.2. The following changes were made:

- All the configuration operations are now performed via one single configuration file that is loaded to SM using CLU.
- Technician information was moved to hidden parameters that do not appear in the configuration file.
- The interactive configuration commands in the CLU were removed, except for commands that perform subscriber configuration and PQI installation.
- A dedicated folder (*~pcube/sm/server/root/config*) was assigned for configuration files.

Copying this folder to standby SM and loading it, assigns the standby SM with the configuration of the active SM.

# Caveats

## Open Caveats – Cisco Release SCMS SM 2.2

### *Restarting the SM after Changing the Time*

- Cisco number 7426

After changing the time on the machine running the SM SUN machine (SM), you must restart the SM. Not restarting the machine may result in the inability to log into the SM from any of Cisco's Management clients.

There are no known workarounds.

### *Configuring Subscribers Directly to an SCE*

- Cisco number 9134

If an SCE is part of an SM domain, and is also configured directly with the subscriber through CLI, the SM will perform a synchronization of the SCE's subscriber database and will erase the subscribers that were manually configured.

Workaround: you should design and configure your system accordingly.

### *Clearing the Subscriber DB in the SM*

- Cisco number 9570

When the SM- LEG Failure Handling parameter in the SM's configuration file is configured to `clear_all_mappings= true`, the subscriber information that was manually entered using CLU commands is also erased.

Workaround: you should design and configure your system accordingly.

---




## Restarting the SM if the "Auto Resync" Parameter Changes

When changing the parameter `Push_mode_auto_resync` in `p3sm.cfg`, the SM is required to restart in order for this change to take effect. Since this parameter is not supposed to change during SM's lifetime, it is recommended changing the parameter in the configuration file right after installation and prior to starting the SM the first time.

Workaround: change this parameter immediately after installing the SM.

## JRE version


The SM requires installing Sun JRE 1.4.2\_02 for correct and stable operation. The SM CD includes a JRE installation script.

	
Note	In case your server hosts other Java applications, that use a different JRE version, the JRE installation script may cause these applications to stop functioning correctly. Please contact Cisco customer support if this occurs

There are no known workarounds.

## Solaris Time Zone and Locale Prerequisites

The time zone and locale is set by editing the `/etc/TIMEZONE` configuration file.

	
Note	You are required to reboot in order for the changes in the file to take effect.

### Time zone

Setting the OS time zone as offset from GMT in POSIX format is not supported and may lead to corrupted log files.

Workaround: It is recommended to set the time zone by country name, for example:

```
TZ=Israel
```

In case GMT offset must be used, use the "zoneinfo" format by attaching a `:Etc/` prefix, for example:

```
TZ=:Etc/GMT+5
```

### Locale

Setting the locale may cause incorrect time stamping.

Workaround: For correct SM operation, English locale must be used. The easiest way to set it is by adding the following line:

```
LANG=en_US
```

To the `/etc/TIMEZONE` configuration file.

## *Standby SM Failure Status*

- Cisco number 12383

When the standby SM fails, the Veritas agent notifies the user through a “monitor time-out” status notification.

There are no known workarounds.

## Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

## Cisco Technical Support Website

The Cisco Technical 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, 365 days a year at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical 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>

## 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 automatically provides recommended solutions. If your issue is not resolved using the recommended resources, your service request will be assigned to a Cisco TAC 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 TAC 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)**—Your 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 operation 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 your network is impaired, but 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.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:  
<http://www.cisco.com/go/marketplace/>
- The Cisco Product Catalog describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:  
<http://cisco.com/univercd/cc/td/doc/pcat/>
- 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>

- Packet magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

<http://www.cisco.com/packet>

- iQ Magazine is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

<http://www.cisco.com/go/iqmagazine>

- Internet Protocol Journal is a quarterly journal published by Cisco Systems 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>

- 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>

---

CCSP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0411R)

Copyright © 2004 Cisco Systems, Inc. All rights reserved.