InCharge™

Release Notes

Version 6.0

Cisco Part Number: OL-6202-01

INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARITES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. JfreeChart library (included herein as .jar files) is provided in accordance with, and its use is covered by the GNU Lesser General Public License Version 2.1, which is set forth at http://www.object-refinery.com/lgpl.html/.

BMC – product library

The Software contains technology (product library or libraries) owned by BMC Software, Inc. ("BMC Technology"). BMC Software, Inc., its affiliates and licensors (including SMARTS) hereby disclaim all representations, warranties and liability for the BMC Technology.

Crystal Decisions Products

The Software may contain certain software and related user documentation (e.g., Crystal Enterprise Professional, Crystal Reports Professional and/or Crystal Analysis Professional) that are owned by Crystal Decisions, Inc., 895 Emerson Street, Palo Alto, CA 94301 ("Crystal Decisions"). All such software products are the technology of Crystal Decisions. The use of all Crystal Decisions software products is subject to a separate license agreement included with the Software electronically, in written materials, or both. YOU MAY NOT USE THE CRYSTAL DECISIONS SOFTWARE UNLESS AND UNTIL YOU READ, ACKNOWLEDGE AND ACCEPT THE TERMS AND CONDITIONS OF THE CRYSTAL DECISIONS' SOFTWARE LICENSE AGREEMENT. IF YOU DO NOT ACCEPT THE TERMS AND CONDITIONS OF THE CRYSTAL DECISIONS' SOFTWARE LICENSE, YOU MAY RETURN, WITHIN THIRTY (30) DAYS OF PURCHASE, THE MEDIA PACKAGE AND ALL ACCOMPANYING ITEMS (INCLUDING WRITTEN MATERIALS AND BINDERS OR OTHER CONTAINERS) RELATED TO THE CRYSTAL DECISIONS' TECHNOLOGY, TO SMARTS FOR A FULL REFUND; OR YOU MAY WRITE, CRYSTAL WARRANTIES, P.O. BOX 67427, SCOTTS VALLEY, CA 95067, U.S.A.

GNU eTeks PJA Toolkit

Copyright © 2000-2001 Emmanuel PUYBARET/eTeks info@eteks.com. All Rights Reserved.

The eTeks PJA Toolkit is resident on the CD on which the Software was delivered to you. Additional information is available at eTEks' web site: http://www.eteks.com. The eTeks PJA Toolkit program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License (GPL) as published by the Free Software Foundation; version 2 of the License. The full text of the applicable GNU GPL is available for viewing at http://www.gnu.org/copyleft/gpl.txt. You may also request a copy of the GPL from the Free Software Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA. The eTeks PJA Toolkit program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

For a period of three years from the date of your license for the Software, you are entitled to receive under the terms of Sections 1 and 2 of the GPL, for a charge no more than SMARTS' cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code for the GNU eTeks PJA Toolkit provided to you hereunder by requesting such code from SMARTS in writing: Attn: Customer Support, SMARTS, 44 South Broadway, White Plains, New York 10601.

IBM Runtime for AIX

The Software contains the IBM Runtime Environment for AIX(R), Java™ 2 Technology Edition Runtime Modules © Copyright IBM Corporation 1999, 2000 All Rights Reserved.

HP-UX Runtime Environment for the Java™ 2 Platform

The Software contains the HP-UX Runtime for the Java™ 2 Platform, distributed pursuant to and governed by Hewlett-Packard Co. ("HP") software license terms set forth in detail at: http://www.hp.com. Please check the Software to determine the version of Java runtime distributed to you.

DataDirect Technologies

Portions of this software are copyrighted by DataDirect Technologies, 1991-2002.

NetBSD

Copyright (c) 2001 Christopher G. Demetriou. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
   This product includes software developed for the NetBSD Project. See http://www.netbsd.org/ for information about NetBSD.
4. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. <<Id: LICENSE, v 1.2 2000/06/14 15:57:33 cgd Exp>>

Contents

1 InCharge Version 6.0 1

SmartPack 1
Changes to InCharge Software 2
New Products 5
Enhancements That Impact All Products 5
New Features of InCharge IP Management Products 6
New Features of InCharge Service Assurance Management Products 9
New Features of InCharge Software Development Kit 11
New Features of InCharge Security Infrastructure Management Products 12

2 Release Notes for All Products 13

Platform Support 13
Deprecated Platform Support 13
Platform Support Restrictions for InCharge Adapters 14
Platform Support Restrictions for the Global Console 14
AIX 14
Changes to AIX Patch Requirements 14
Patching the C++ Run Time Library 15
Name Resolution Problem for Discovery on AIX 17
AIX Shutdown 18
Solaris 19
sm_logerror Process 19
HP-UX 19
Change to HP-UX 11.11 Patch Requirements 19
Windows 20
Embedded Spaces 21
Recovery Options Prohibited for Failover 21
Running Multiple Brokers or Domain Managers 21

Directory Naming Convention 22
Windows Diagnostic Tool Recommendation 22
SMARTS Client Program Issues 22
Client Connection Attempts Timeout After 60 Seconds 23
Unexpected Exit by Client Disables Terminal Echo (UNIX) 23
Supported and Unsupported Broker Configurations 24
Supported Configurations 24
Unsupported Configurations 24
InCharge Broker 25
SM_BROKER_DEFAULT Variable 25
Trap Processing 25
Forwarding Traps 25
Documentation Errata 27
Correction for Location of HTML Documents 27
Correction for runcmd_env.sh File 27
Associating InCharge Files With sm_edit on Windows 27
Corrections to Trap Adapter and Application Connectivity Monitor Examples 28
Format Change for the -D Option 28
Direct Telephone Number for SMARTS Technical Support 28

3 Release Notes for Service Assurance Management Suite 29

Global Console 29
Client Tool May Not Stop 29
User Unable to Configure Web Portal From Global Console 30
Map Console 30
IP Network Map Node 30
Unable to Load the Java Applet 30
Java Applet May Not Attach to Broker 31
Console Forces You to Abandon Unapplied Changes 31
Expanded Topology and Node Visibility 32
Topology Browser Console and Unapplied Changes 32
Program Tool Issue 32
Ping and Telnet Tools Have Access Constraints 33
SAM Adapters 33

Configuration Parameters in Notifiers 33
sm_ems Issue 34
sm_ems Does Not Prompt for Authentication Credentials 34
Java Issues 35
Adjusting Memory for Java Dynamic Memory Allocation 35
Default User Profile Requirement 36
Documentation Errata 37
InCharge Adapter for TIBCO Rendezvous Version Support 37
Correction for Modifying mail-custom.asl 37
Corrections for XML insert and put Methods 38
Correction to a Tool Example 38
Correction to an ASL Filter Example 39
Correction to Syntax for an Import Option 39
Correction to Syntax for the sm_config Command 40
Corrections for the InfoVista Adapter 40
Correction for Web Portal 40

4 Release Notes for IP Management Suite 41

InCharge Applications 41
"Illegal" Device Names 41
Error Message Displayed While Setting Full Discovery Below 60 Minutes via Topology Tab 42
Certified Device Support 43
Changed Certifications for ICIP 6.0 SP1 43
Incorrect Directory for IDS Certified Device List 43
Cisco 2948G and 4232 L3 Module Conflict 44
Availability Manager Application 45
Diagnosis of Card Down Problems on Cisco LS1010 Switches 45
Card Status Not Updated When Card Is Reinserted 45
Connections Between Foundry and Cisco Switches 46
Disabling SNMP Polling Through Special Read Community String 46
Discovery Pending Interval 47
Performance Manager Application 47
Changed Method for Determining Duplex Mode 47

Excessive Fragmentation and Cisco Catalyst Switches 48
Exceed Issues 48
Exceed and Minimized Windows 49
Exceed and Repeated Console Closure 49
HP OpenView Pathname Not Converted Properly During Installation 49
Adapters Fail to Create Log Files 50
Documentation Errata 51
Correction for Extracting a Seed File 51

5 Release Notes for Security Infrastructure Management Suite 53
Discovery Options Are Not Supported 53
Concord SystemEDGE SNMP Agent Version 4.2 Causes Erroneous Results 54
Login Session Notifications Do Not Clear for Disconnected Security Adapters 54
Nokia IPSO Agent Issue 55
Nokia Firewalls Time Out 55

1

InCharge Version 6.0

InCharge version 6.0 delivers major enhancements and improvements to SMARTS core products—InCharge Service Assurance Manager, InCharge IP Availability Manager, and InCharge IP Performance Manager—and introduces an updated InCharge Software Development Kit, several new products which are summarized in *New Products* on page 5, and a Security Infrastructure Management Suite.

This chapter begins by summarizing changes to InCharge software that will be of interest to existing InCharge customers. It then goes on to identify new products and features.

Note: 6.0 refers to the InCharge software platform version. The InCharge products described in this document are based on this version of the InCharge software platform. InCharge product versions vary and do not always match the software platform version number. Refer to the *InCharge 6.0 Read Me First* document for a complete list of product version numbers.

SmartPack

Beginning with platform version 6.0, SMARTS periodically distributes SmartPacks which consist of InCharge software updates and newly certified devices. A SmartPack™ can modify the software platform as well as products of one or more product suites. SmartPacks are cumulative for each release, so you do not have to install earlier SmartPacks. For example, SmartPack 2 for InCharge Service Assurance Management Suite 6.0 will include SmartPack 1 for InCharge Service Assurance Management Suite 6.0. When a SmartPack is available, customers will be notified by e-mail. At the present time, SmartPack 1 is available.

For detailed information, SMARTS provides the following documentation:

- SmartPack Release Notes—Summarizes major software issues resolved by a SmartPack.
- SmartPack Change Log file (one per product suite)—Lists the files that are updated.
- A Certified Device List (distributed as HTML)—Is provided by SmartPack 1 for the InCharge IP Management Suite.

Before you install a SmartPack, make sure that all of the desired suite products are installed, because, after you install a SmartPack, you cannot install additional products using the InCharge 6.0 CD-ROM(s). SmartPack installation instructions are provided in the *InCharge 6.0 Read Me First* document.

Changes to InCharge Software

The following summarizes changes to the distribution, directory structure, licensing and installation introduced by InCharge 6.0 software.

Product Suite and CD-ROM Distribution

InCharge products, although purchased, installed, and licensed separately, are now distributed as product suites on separate CD-ROMs. Also, in previous releases, the media was operating-system specific. Now, all supported operating system versions are installable from the same product suite media. Product suites include:

- InCharge IP Management Suite – includes InCharge IP Availability Manager, InCharge IP Performance Manager, InCharge Discovery Manager, InCharge Adapter for HP OpenView NNM, and InCharge Adapter for IBM/Tivoli NetView. Also includes IDS-009, InCharge device certification.
- InCharge Service Assurance Management Suite – includes Service Assurance Manager, Global Console, Business Impact Manager, Failover System, Generic Notification Adapters and InCharge (Notification) Adapter for TIBCO Rendezvous, Service Assurance Manager Adapter Platform (previously referred to as the Open Integration Server), InCharge Syslog Adapter, InCharge SNMP Trap Adapter, InCharge Adapter for Remedy, InCharge XML Adapter, InCharge Adapter for Concord eHealth, and InCharge Adapter for InfoVista

- InCharge Application Management Suite – includes Application Connectivity Monitor. Other products in this suite are available as pre-6.0 InCharge software
- InCharge Software Development Kit – includes InCharge run-time product, programmatic APIs, and the MODEL compiler
- InCharge Security Infrastructure Management Suite – includes Security Infrastructure Manager, Firewall Performance Manager, and security adapters such as InCharge Adapter for Check Point/Nokia and InCharge Adapter for Cisco Security.

For a description of each product or component, refer to the product's installation guide or user's guide. For information about product enhancements, refer to the remaining sections of this chapter.

New Directory Structure

Each InCharge product suite is installed to a separate subdirectory under the InCharge installation root directory. The root directory is */opt/InCharge6* for UNIX and *C:\InCharge6* for Windows systems or is user specified. Table 1 identifies the directories under the InCharge root directory where the software for each product suite resides.

PRODUCT SUITE	DIRECTORY UNDER ROOT
InCharge Service Assurance Management	/SAM
InCharge IP Management	/IP
InCharge Application Management	/APP
InCharge Security Infrastructure Management	/SIM
InCharge Software Development Kit	/SDK

Table 1: Directories Under InCharge Root Directory

The directories under the InCharge root directory cannot be user specified.

Licensing

All InCharge products (including InCharge IP Availability Manager and Performance Manager) are now licensed using FLEXlm licensing software, version 7.2. The licensing process has changed slightly. For example, SMARTS no longer provides a trial license on the InCharge CD-ROM. You must have a license before you can run InCharge software. Instructions on how to acquire a trial (temporary) or permanent license are provided in the *InCharge System Administration Guide*. Also, InCharge no longer uses the SMARTS.licserv file to identify the location of the FLEXlm license server. Instead, SM_LICENSE, a new environment variable, is used to set the license server location.

Other InCharge Products

Several InCharge 5.0.x products and adapters are not included in the version 6.0 distribution. However, these products and adapters are available as pre-6.0 software and are compatible with 6.0 InCharge Managers. The following suites and their products are available on the InCharge 5.0.1 CD-ROM:

- InCharge Service Assurance Applications Suite
  - SQL Data Interface Adapter
  - Web Portal
  - Report Manager
- InCharge Application Management Suite
  - InCharge Application Services Manager
  - InCharge Adapter for Concord SystemEDGE
  - InCharge Adapter for BMC Patrol

Installation

Previously, the Global Console was included on every InCharge CD-ROM. In 6.0, the console is only installable from the Service Assurance Management CD-ROM.

Start-up Scripts

Start-up scripts are no longer provided for most InCharge applications. The sm_service utility replaces the functionality provided by the start-up scripts. (The installation and Service Assurance Manager Failover System start-up scripts are exceptions.)

New Products

The following summarizes the new 6.0 product offerings:

- InCharge Discovery Manager – distributed as part of the InCharge IP Management Suite, the Discovery Manager discovers IP networks, provides topology browser and map views of the discovered network, and utilities that can export the topology into other applications. This discovery process is identical to that used by IP Availability Manager.
- InCharge XML Adapter – distributed as part of the InCharge Service Assurance Management Suite, the XML Adapter exchanges topology elements between InCharge and other systems. The adapter transfers data expressed in an XML document, which complies with the ICIM/XML standard DTD.
- InCharge Application Connectivity Monitor (ACM) – distributed as part of the InCharge Application Management Suite, ACM is deployed with Application Services Manager to discover TCP application services and measure their availability. The ACM then reports its findings to the Global Manager.
- InCharge Adapter for Concord eHealth – distributed as part of the InCharge Service Assurance Management Suite, this adapter integrates with Concord eHealth and liveHealth.
- InCharge Adapter for InfoVista – also distributed as part of the InCharge Service Assurance Management Suite, this adapter notifies Service Assurance of InfoVista performance events and provides operators with direct in-context access to InfoVista performance reports.

Enhancements That Impact All Products

The following enhancements are applicable to all products:

- New Operating System Support – InCharge products are now supported on Red Hat Linux Advanced Server ES, AS, or WS 2.1, Solaris 9, and HP-UX 11.11. For complete information about operating system support, including operating systems no longer supported, refer to *Platform Support* on page 13.
- Improved Performance – The InCharge protocol has been enhanced to operate more efficiently over high-latency links.

- Improved Java Applet support – The console Java applet is now more secure. It runs as a cryptographically signed applet. Also, users can optionally run the applet using Java Web Start, which caches the Java code on the client side and shortens applet launch time.
- New, User-friendly Multi-platform Installation – An easy-to-use InstallShield wizard streamlines installation on all platforms for all product suites.
- Local Directory – Beginning with InCharge 5.0, all user modifiable files (such as ASL rule sets, configuration files, and template files) reside in a local directory and original versions of these files are always retained by InCharge.
- InCharge Common Information Model™ (ICIM) 1.2.1 – The model has been updated to include firewall and redundancy group classes.
- New Service Controller – A new, operating system-independent utility is available to set up an InCharge application's environment and launch the application. Services can be installed automatically during installation.

The remaining sections are organized by product suite and provide details about the new features and enhancements specific to each.

New Features of InCharge IP Management Products

Version 6.0 InCharge IP products offer improved problem analysis, a more flexible discovery mechanism, and improved representation and management of topology.

New and Improved IP Availability Manager Analysis

- Improved Performance – The Availability Manager analysis model takes advantage of correlation performance improvements, consumes less memory resources, which results in faster correlation of problems and less transient conclusions.
- New LogicalConnectionDown – This new problem definition improves fault isolation in situations involving wide area outages.

- New Analysis of Redundancy Groups – Availability Manager now analyzes the availability of system, card, network adapter, and network connection redundancy groups. This is a useful feature for those managing high availability networks. The redundancy group analysis is determined by At Risk Thresholds. InCharge generates notifications when a group's redundancy is at risk, has been reduced, or when all of the group's components are down.
- Also, for Card Redundancy, a Card Switchover notification is generated when a card redundancy status changes from inactive to active.
- Improved Analysis of ISDN Interfaces – Availability Manager now differentiates between the status of the physical interface versus the ISDN B channel (which carries the data) and the ISDN D channel (which carries signalling and other control information). In addition, new Threshold Groups are used to monitor the physical ISDN interfaces.
- Improved Analysis for Unstable Network Adapters – Since some devices do not generate LinkDown traps, Availability Manager now processes both LinkUp and LinkDown traps to determine if a network adapter is flapping (or unstable). Also, Availability Manager no longer uses LinkUp traps to set the OperStatus for NetworkAdapter elements. This improves performance when Availability Manager is flooded with LinkUp traps from a device.
- Improved Analysis for Disabled Ports and Interfaces – Normally, you do not need to be alerted when a network adapter is administratively down. Now, however, Availability Manager is able to discern when such an event is important and notifies you.
- Improved Analysis for Subcards – Availability Manager is now able to correlate subcard(s) to the parent card when there is a failure on the parent card.
- Ability to Manage and Unmanage Card Objects

New and Improved IP Performance Manager Analysis

- Improved Analysis for High Error Rates – A new threshold, ErrorTrafficThreshold has been added to the Interface/Port Performance Threshold Setting to improve the analysis of this fault.

Process Control Improvement

- Availability Manager and Performance Manager can now be more easily deployed separately or together as one process.

Discovery Enhancements

- New Methods for Configuring Discovery Properties – InCharge 6.0 provides more control over what systems are found and discovered and how the systems are accessed.
    - New Seed File and Add Agent Format. Users can specify the community strings, alternate SNMP port, version of SNMP (V1, V2C) or have InCharge automatically detect the version, and what protocols InCharge uses to access the system (ICMP only, SNMP only, ICMP and SNMP). This last feature is useful for organizations with limited ability or permissions to poll or ping certain IP addresses.
    - Improved Autodiscovery Filters. In addition to being able to set all of the above, the filters can also use the Sys Object ID as matching criteria.
- New Option to Use Loopback IP Address to Access Devices – Users can specify that the loopback address be used for ICMP and SNMP polls during discovery and for monitoring and analysis. The address used to access devices can either be set globally or on a system-by-system basis.
- New Methods to Update Community String – Network administrators often change the read community strings for devices at regular intervals as a security precaution. In version 6.0, you can now routinely make InCharge aware of the updates to the read community strings and ensure that devices continue to be properly monitored.
- Customize Discovery post-processing – You can specify ASL scripts to perform custom post-processing discovery tasks. The postprocessing occurs before discovered elements are monitored (SNMP polls and ICMP pings). For example, you might include an ASL script that creates redundancy group memberships.
- Control PING Bursts – To reduce the burst of ICMP pings sent during discovery, InCharge version 6.0 introduces a sleep time to control the flow of ICMP packets into the network during discovery. The sleep time causes the discovery process to wait a short interval between ICMP pings.
- Improved Discovery Error Analysis – InCharge now reports a discovery error when a system is unreachable during discovery. Additional discovery errors include:
    - Device is Unreachable During Discovery

- SNMP Agent is Not Responding
- Qualified access address not found

Enhancements to Topology Representation

- Improved Representation of Non-SNMP Devices – Interfaces are created for each IP address that resolves to the device. Also, cables may be created between switches and non-SNMP devices.
- Improved Control of Display Names – you have more flexibility regarding a system's display name and can either use the MIB-II SysName variable or the InCharge DisplayNameFormat attribute to derive the display name.
- Improved Event Details – More useful and complete information is now available from the Details tab.
- Improved Containment Information – Containment information is now available for all managed elements.

New Certified Device Support

- Certification Updates – The 6.0 version includes all devices certified up to and including IDS-009. For a complete list of certified devices, refer to the IDS9_Certification.html.
- Discovery of Subcards for Juniper Devices

New Features of InCharge Service Assurance Management Products

Version 6.0 InCharge Service Assurance Manager (SAM) adds a rich set of facilities to define automated escalation policies and corrective actions, offers a unified Global Console that interfaces with all InCharge Managers, and enhanced configuration and administration features.

New Escalation Policy

- An Escalation Policy leverages InCharge tools to automatically execute actions when a notification meets a set of criteria. Time intervals and tools are configured by administrators so that when the desired condition is not met, the notification is escalated to the next level of priority and action. SAM administrators can create, copy, edit, and view escalation policies.

Global Console Enhancements

- Consolidation of the Console – The Global Console now consolidates the features and functionality of previous consoles. For example, InCharge administrators can manage objects in any InCharge Manager, including underlying domains. This means an administrator can configure a Global Manager, perform discovery of underlying domains, and set polling and threshold values of those domains – all through the Global Console. The console enables all InCharge users to browse, in context, the detailed topology of an underlying domain as well as view detailed codebook and aggregate data for an event of interest.
- Enhanced Service Assurance Manager Administration – InCharge administrators can now configure notification lists, users, user profiles, tools, and escalation policies through a new graphical interface.
- Support for Multiple User IDs – The Global Console now allows users to log in to underlying domains using different User IDs. This is helpful since the Global Manager and underlying InCharge Managers may potentially have a different set of users and user identifications.

Configuration and Migration Enhancements

- Optional Command-line Interface (sm_config) – While the easiest way to create and manage repository objects (such as notification lists and user profiles) is through the Global Manager Administration Console, sm_config allows you to create them through the command line. Using XML files to define the properties of the objects, administrators can batch process the uploading of multiple objects. In addition, this utility can be used to duplicate repository objects in a separate Global Manager.
- New Migration Utility (sm_migrate) – This utility allows you to transfer your Service Assurance Manager 5.0 and later configurations into your 6.0 environment. Specifically, this utility migrates the information in your old configuration files so that they are now displayed and configurable from the new Global Manager Administration Console. For example, by migrating information from the NotificationSection of a 5.0 or 5.0.1 *ics.conf* file, administrators will be able to view and modify individual notification lists in the Global Manager Administration Console.

New Features of InCharge Software Development Kit

Version 6.0 InCharge Software Development Kit offers new and improved documentation, new Remote APIs, MODEL enhancements, as well as new compiler support.

New Documentation

- Remote API Documentation – Distributed as HTML, the *InCharge Software Development Kit Remote API for Java* describes the programmer's interface to the Java classes used to develop remote applications. Also, the *InCharge Software Development Kit Remote API Programmer's Guide* (distributed as PDF) provides a description of the development environment and procedures needed to create application programs using the Remote API.
- ICIM Documentation – Distributed as HTML, the *InCharge Software Development Kit ICIM Reference* describes the ICIM schemata and provides general concepts related to InCharge information modeling and ICIM classes.

New Remote APIs

- getClassHierarchy(SM_Sequence<SM_ClassHierarchy>&) – New API that constructs the entire class hierarchy with a single API call.
- getAllProperties(const SM_String& className...) – New API that retrieves all the properties of a given class.
- getProperties(const SM_String& className...) – New API that retrieves a specified list of attributes. For example, when the console displays network elements it needs to retrieve certain attributes such as DisplayName and DisplayClassName. The console client can use the getProperties() to obtain these in a single API call.
- getProblemSymptomState(SM_EventName, SM_Sequence<SM_SymptomData>) – New API that returns the state of the symptoms for a given problem even when the symptoms have not been subscribed to. Use this call to display the codebook properties for an event in the console.

MODEL Enhancements

- More Flexible MODEL Rate – The repository now allows the MODEL rate (target_attribute, window_size) to use window sizes larger than the polling interval on the target_attribute.

- New synch_rates Method – The repository's accessor interface has a new method, synch_rates (instance), which will cause the accessor to check the values of attributes used for window sizes and update the corresponding rate calculation interval.
- Improved Handling of Default Polling Periods – The handling of default polling periods has been improved so that attributes polled at the default period will adjust their polling periods when the default is changed.
- Static Stored Attributes – In MODEL, you can now declare static stored attributes, whose value will be shared by all instances of an interface. The syntax is: [static] [readonly] [stored] attribute.
- Ability to Mark Interfaces as Unique – In MODEL, you can now mark an interface as unique, which means that the repository will only permit one instance of the interface or any derived interfaces to exist at a time. The syntax is: [abstract] [unique] interface

C++ Compiler Support Upgrades

In addition to continuing support for the Microsoft Visual C++ v6.0 and the AIX 4.3.3 ibmcxx 3.6.6 (packaged with Visual Age C++ V4.0), the 6.0 InCharge SDK has upgraded C++ compiler support as follows:

- Upgraded Solaris C++ Compiler Support – On Solaris 8 and 9, SDK now supports the Forte Developer 7 C++ 5.4 compiler.
- Upgraded HP-UX C++ Compiler Support – On HP-UX 11.00 and 11.11, SDK now supports aCC A.03.45 or the latest version.
- New Linux C++ Compiler Support – On Red Hat Linux Advanced Server ES, AS, or WS 2.1, SDK supports g++ 3.2.2.

New Features of InCharge Security Infrastructure Management Products

InCharge Security Infrastructure Management products support additional types of firewalls. For a complete list of supported devices or software components that act as firewalls, refer to the *SIM_SupportedFirewalls.html* file in the ***BASEDIR****/smarts/doc/html* directory.

2

Release Notes for All Products

This chapter describes issues and resolutions pertinent to all InCharge products.

Platform Support

The following are supported operating systems for InCharge 6.0 products:

- Solaris 8 and 9 on SPARC
- HP-UX 11.0 and 11.11 on PA-RISC
- AIX 4.3.3
- Red Hat Linux Advanced Server ES, AS, or WS 2.1
- Windows 2000, SP3 or later
- Windows XP (console only)

Deprecated Platform Support

The following operating systems are no longer supported:

- Solaris 2.6 and 2.7
- HP-UX 10.20
- Windows NT

Platform Support Restrictions for InCharge Adapters

Operating system restrictions apply to the following adapters:

- InCharge Adapter for Concord eHealth is not supported on HP-UX or AIX.
- InCharge Adapter for InfoVista is not supported on HP-UX or AIX.
- SAM or IP Adapters that interface with third-party applications are not supported on Linux. The following adapters do support Linux: Syslog Adapter, SNMP Trap Adapter, and XML Adapter.
- InCharge Adapter for Check Point/Nokia is not supported on Solaris 9, HP-UX, AIX, or Linux.

Platform Support Restrictions for the Global Console

The Global Console is not supported on AIX.

AIX

The following issues are specific to running InCharge on the AIX platform.

Changes to AIX Patch Requirements

For AIX 4.3.3, the required patch level for two patches changed:

PATCH	OLD REQUIRED LEVEL	NEW REQUIRED LEVEL
xlC.rte	5.0.0.0	6.0.0.0
xlC.aix43.rte	5.0.0.4	6.0.0.8

Table 2: Updated Patch Levels

Table 3 provides a complete list of patches as of September 16, 2003.

For information on updating AIX systems, see the IBM Web site at *http://www.ibm.com*.

The filesets in Table 3 are required. Your system *must be* at or above the specified level for each fileset.

PATCH ID	DESCRIPTION
bos.rte.libc 4.3.3.18	C library update
bos.rte.libpthreads 4.3.3.12	Thread library
xlC.rte 6.0.0.0	C++ library
xlC.aix43.rte 6.0.0.8	C++ library for AIX 4.3
bos.iocp.rte 4.3.3.0	I/O Completion Ports API Base Operating System
bos.mp 4.3.3.79	Multiprocessor Runtime
bos.net.tcp.client 4.3.3.78	TCP/IP Client Support

Table 3: Patch Requirements for AIX

Patching the C++ Run Time Library

Issue:

You receive an error message while you are attempting to apply the xlC.aix43.rte 6.0.0.8 patch (the C++ library for AIX 4.3) in order to satisfy InCharge 6.0 pre-installation requirements.

Resolution:

You need to apply the base xlC runtime library software (xlC.rte 6.0.0.0 patch for C++ library) before you apply the xlC.aix43.rte 6.0.0.8 patch.

You can obtain the base xlC runtime library software from two sources, SMARTS or IBM. SMARTS recommends that you use its specially-prepared tar file which is based on IBM's redistributable tar file and contains only relevant files (omits unnecessary files for earlier versions of AIX) for a more simplified patch installation. Information for obtaining the base xlC runtime library software from both sources is provided here.

First, verify that you need to install the base xlC runtime library software. Type:

```
$ lslpp -l xlC.aix43.rte
```

If you receive one of the following results, the necessary base software has *not* been installed on your system:

- The message:

```
lslpp: 0504-132  Fileset xlC.aix43.rte not installed.
```

- Level displayed is less than 5.0.0.0

If you receive either result, you must obtain and install the base xlC runtime library software.

SMARTS Tar File

SMARTS provides a tar file on its FTP site. Perform these steps to obtain and install it:

1. Obtain the tar file from the SMARTS FTP site.
   - FTP to the SMARTS FTP site. (Type: **ftp** *ftp.smarts.com*).
   - Log in as user anonymous with your e-mail address as the password.
   - Make sure the transfer mode is binary (type: **binary**).
   - Change the directory to the *out.going* directory (**cd** *out.going*).
   - Then, get the file vacpp5_runtime_base_43.tar.Z (Type: **get** *vacpp5_runtime_base_43.tar.Z)*.

Note: You must specify the **get** command with the exact file name. You will not be able to list the contents of the *out.going* directory.

2. Uncompress the tar file and untar it into an empty directory on the target machine.
3. Execute **smit**. The smit utility displays a series of menus.
   - Choose Software Installation and Management.
   - Choose Install and Update Software.
   - Choose Install and Update From ALL Available software.
   - Provide the directory path in which you untarred the file.
   - Choose as "SOFTWARE to install" xlC.rte, xlC.aix43, and at least one of the message files (for example, xlC.msg.EN_US for US English messages).
   - Allow **smit** to install the software. No reboot should be required.

Once you have installed the base xlC runtime library software, you can continue by applying the required xlC.aix43.rte 6.0.0.8 patch.

IBM Location

The base xlC runtime library software is not available from the usual IBM patch servers. You can obtain it directly at this IBM URL:

http://www-4.ibm.com/software/ad/vacpp/service/csd.html#redistribute

Under the topic "Redistributable Filesets," download the VisualAge C++ professional V5.0 C++ Runtime Libraries tar file and the README file.

Note: If you download the patch from IBM, you must follow the IBM installation procedure as described in the *README* file. The installation procedure described in the *README* file is not the same as the SMARTS procedure described above.

Once you have installed the base xlC runtime library software, you can continue by applying the required xlC.aix43.rte 6.0.0.8 patch.

Name Resolution Problem for Discovery on AIX

PR 6582

Issue:

The discovery process hangs. Or, the InCharge Domain Manager crashes and this message appears in the log file:

```
The assert subroutine failed: vc_cv != (cond_t *) NULL,
file clnt_vc.c, line 192
```

Resolution:

There is a problem in the IBM name resolution routines. The problem is triggered only when all of the following conditions apply:

- You discover a hostname NAME that can be translated using DNS
- The address to which NAME is translated does not have a reverse translation
- NISPLUS translations for hosts are enabled
- NAME does not appear in the NISPLUS hosts map

Use IBM's patch level "bos.net.tcp.client 4.3.3.84" with the abstract description "NISPLUS NOT THREADSAFE WITHOUT LIBNSL" to solve the problem.

To check for the first two conditions, use the AIX command /usr/*bin*/***host***. For example, first do the forward translation:

```
$ host NAME
NAME.EXAMPLE.COM is 172.16.1.98
```

Now, attempt the reverse translation:

```
$ host 172.16.1.98
host: 0827-803 Cannot find address 172.16.1.98.
```

AIX Shutdown

PR 7617

Issue:

SMARTS programs started automatically at boot are not shut down cleanly when the system shuts down.

Resolution:

During shutdown, AIX sends a SIGTERM to running processes, gives them 10 seconds to shut down cleanly, and then sends a SIGKILL which unconditionally stops them. SMARTS processes handle SIGTERM and will attempt to shut down cleanly, but may not be able to complete within the 10 seconds allotted to them.

AIX provides a mechanism, the */etc/rc.shutdown* script, that allows you to define actions to be taken at shutdown. Because this is a single script that can contain arbitrary shell code, it is impractical for SMARTS to attempt to modify it to include the necessary shutdown actions. You can, however, edit it by hand.

Execute the following command within */etc/rc.shutdown*:

```
/etc/rc.smarts stop
```

For further information, see the comments in */etc/rc.smarts*.

Solaris

The following issue relates to running InCharge on the Solaris platform.

sm_logerror Process

Issue:

Starting with InCharge version 5.0, every running SMARTS program is accompanied by a child process running a SMARTS program, *sm_logerror*.

Resolution:

This process is used to safely print the stack trace of its parent process. On other operating systems, it is possible to print a stack trace from within the running program. On Solaris systems, stack traces are printed by a standalone program, */usr/bin/pstack*.

Previous versions of InCharge created a process to run *pstack* each time a stack trace was requested—usually when a process was about to crash. In certain error states, it may be impossible to create the subprocess; worse, attempting to do so can cause a deadlock, hanging the server. The new design avoids these problems. *sm_logerror* processes do nothing except when asked to print a stack trace, and exit automatically when their parent exits.

HP-UX

The following issue is specific to running InCharge on the HP-UX platform.

Change to HP-UX 11.11 Patch Requirements

Issue:

Installation of InCharge on an HPUX 11.11 system calls for the application of patch PHSS_28436. The installation enforces this requirement. However, HP has associated severe warnings with this patch, and installing it can cause failures on some systems.

Resolution:

If you have already installed PHSS_28436 and have not seen problems, you do not need to do anything.

HP recommends that, should you be unable to install PHSS_28436, you should install PHSS_26560. This patch level should be sufficient to allow the InCharge software to run.

HP has very recently issued a replacement for the incorrect patch: PHSS_28871. HP does not list it as "Recommended" at this time. Should HP do so in the future, you can install it in place of PHSS_26560 and proceed with a normal installation.

SMARTS recommends the following steps:

1. Run the InCharge installation, allowing it to report any missing patches.
2. If the installation complains about any missing patches other than PHSS_28436, resolve those complaints first.
3. Check to see that PHSS_26560 or later has been installed on the system. To do so, issue the command:

   ```
   $ what /usr/lib/dld.sl
   ```

   You will see output similar to the following:

   ```
   SMART_BIND
   92453-07 dld dld dld.sl B.11.33 020617
   ```

   The version number—just after dld.sl—must be B.11.33 or later.

   If the version number is not B.11.33 or later, PHSS_26560 or later has not been installed. Contact SMARTS Technical Support for assistance.

Windows

The following issues relate to running InCharge on the Windows platforms.

Embedded Spaces

Issue:

In previous versions of SMARTS software, command line arguments that contained embedded spaces were not handled properly. This was especially the case for services installed with *sm_service*, since the command line is interpreted multiple times.

As of InCharge version 5.0, such arguments are handled properly. However, users of earlier InCharge versions might have used various work-arounds to get the older code to produce the correct results. Those work-arounds typically will now produce the wrong result, since extra characters incorrectly stripped off by the old code are now preserved.

Resolution:

SMARTS is not aware of any instances of this in the standard, shipped code, but it might occur in customized code developed either by SMARTS or by users. All such code needs to be examined and may need to be modified for InCharge version 5.0 and later versions.

Recovery Options Prohibited for Failover

Issue/Limit:

For the Windows 2000 platforms (Professional, Server, and Advanced Server), users should not set recovery options for any InCharge services. Recovery options are set in the Recovery Tab under *Administrative Tools > Services*. The options, First Failure, Second Failure, and Subsequent Failure, must not be changed. InCharge services must use the default setting, Take No Action, for all these options.

Running Multiple Brokers or Domain Managers

Issue:

On the Windows 2000 platform (Professional, Server, and Advanced Server), it is possible to start several InCharge Brokers or InCharge Domain Managers listening on the same port. This is due to an incompatibility between the UNIX and 2000 implementations of the Internet Protocol stacks. Running more than one copy of the Broker or the Domain Manager may cause unpredictable results.

Resolution:

Terminate all InCharge Brokers and Domain Managers using the same port and start only one copy.

Directory Naming Convention

Issue:

On the Windows 2000 platform (Professional, Server, and Advanced Server), InCharge does not install properly or InCharge services do not start up properly.

Resolution:

The directory names used in ***BASEDIR*** cannot contain spaces (for example, *Program Files*). Do not install InCharge in directories that have names containing spaces.

Windows Diagnostic Tool Recommendation

Issue/Limit:

If you are running InCharge on the Windows 2000 platform (Professional, Server, and Advanced Server), SMARTS recommends that you use the Dr. Watson diagnostic tool as your debugger. Dr. Watson gathers information about your computer when a problem occurs with a program, and is typically the default tool on computers running Windows operating systems. If Dr. Watson is not currently set as your computer's diagnostic tool, you can set it with the command:

```
c:\>drwtsn32 -i
```

If you are using a different diagnostic tool, SMARTS Technical Support may not be able to acquire as much diagnostic information if problems occur. For more information about Dr. Watson, refer to your Microsoft documentation.

SMARTS Client Program Issues

The following issues are applicable if you are using SMARTS client programs from the terminal. For example, these issues apply to the execution of the dmctl program from an xterm Window.

Client Connection Attempts Timeout After 60 Seconds

PR 6325

Issue:

When <PROMPT> is specified for the InCharge username field of the *clientConnect.conf* file, a user must type a username, and possibly a password, when invoking a client program. If the username and password (if required) are not entered within 60 seconds, the operation will time-out and report an I/O error. This timeout only affects clients started from the command line; it does not affect the Global Console.

Resolution:

Type the username and password before 60 seconds elapse. If the operation cannot be completed before the timeout, you can re-invoke the command. If 60 seconds elapse, you will also have to restore the terminal's echo state (see below).

Unexpected Exit by Client Disables Terminal Echo (UNIX)

PR 6328

Issue:

When the *clientConnect.conf* file is configured to prompt the user for a password, the terminal echo is disabled so that the typed password is not displayed. If the client program exits during the password prompt, the terminal's echo state is not reset.

Resolution:

To restore the terminal's echo state, type the following command:

```
% stty echo icanon
```

Because the terminal echo is disabled, you will not be able to see the command as you type it.

Supported and Unsupported Broker Configurations

Beginning with InCharge version 5.0.1, due to improvements in security, InCharge version 5.0 and later components (brokers, clients, and servers) authenticate to each other differently than pre-5.0 versions. As a result, not all combinations of InCharge versions are supported. This section describes which configurations are supported for InCharge version 5.0 or later.

Supported Configurations

If the deployment includes any InCharge version 5.0 or later software, you must use the version 5.0 or later InCharge Broker to obtain a supported configuration. The following configurations are supported:

- A version 5.0 or later InCharge Broker in nonsecure mode (the default) supports connections from any combination of versions of clients and servers (5.0.1 and previous versions).
- A version 5.0 or later InCharge Broker in secure mode supports:
  - InCharge version 4.1 and 4.1.1 clients or servers configured with security *enabled*. It cannot support version 4.1 and 4.1.1 clients or servers configured with security disabled.
  - Clients and servers of Service Assurance versions 4.5, 4.5.1, and 4.6, except for consoles.

    The *clientConnect.conf* file for clients and servers must be modified to send credentials to the version 5.0 or later broker and those credentials must correspond to the entries in the *serverConnect.conf* file. (The same modification must be made to the version 5.0 or later *clientConnect.conf* file.)

For information about security modes and the InCharge Broker, see the *InCharge System Administration Guide*.

For information about deployment, see the *InCharge Service Assurance Manager Configuration Guide*.

Unsupported Configurations

For a version 5.0 or later InCharge Broker in secure mode, the following configurations are unsupported and do not function:

- Consoles prior to version 5.0.
- Clients or servers prior to version 4.1.

InCharge Broker

The following issue relates to the InCharge Broker.

SM_BROKER_DEFAULT Variable

PR 9287

Issue/Limitation:

The variable SM_BROKER_DEFAULT is not defined in ***BASEDIR****/smarts/local/conf/runcmd_env.sh*. Instead, the variable SM_BROKER is defined. This prevents the user from overriding the SM_BROKER value on an InCharge product suite basis by presetting the SM_BROKER environment variable. For example:

```
SM_BROKER=localhost:427 ./sm_server [args]
```

Resolution:

In order to have the ability to override the SM_BROKER variable for a program, the variable name in *runcmd_env.sh* must be changed from SM_BROKER to SM_BROKER_DEFAULT.

Trap Processing

The following issue relates to trap processing.

Forwarding Traps

PR 8155

Issue:

Prior to InCharge version 5.0.1, for some configurations, the default settings for trap forwarding might have enabled the forwarding of all traps.

For the system that receives the traps, the processing of extraneous traps might result in high resource (CPU and memory) usage. Specifically, for IP Availability Manager, it has been observed that forwarding all traps can cause, in extreme cases, delayed startup times of the domain manager and sometimes excessive CPU utilization.

Resolution:

The configuration file that controls trap processing, *trapd.conf*, has been revised to provide better control over which types of traps are forwarded to the system where Availability Manager and/or Performance Manager is running.

To forward traps more efficiently, open the *trapd.conf* file for the trap processor that forwards traps to Availability Manager and/or Performance Manager and uncomment the lines of code (beginning with FORWARD) for specific types of traps. The types of traps are listed in the file.

For example, if the Service Assurance Manager Adapter Platform is deployed, you can modify the *trapd.conf* file for the InCharge SNMP Trap Adapter to forward Cisco or 3Com traps to Availability Manager.

There are many different InCharge applications that forward traps. Examples of trap processors are: the InCharge SNMP Trap Forwarder and the InCharge SNMP Trap Adapter. You only need to modify the *trapd.conf* file for the processor that transfers traps to Availability Manager and Performance Manager. Depending upon your configuration, the file may be:

- ***BASEDIR****/smarts/conf/trapd/trapd.conf* for the InCharge SNMP Trap Forwarder
- ***BASEDIR****/smarts/conf/icoi/trapd.conf* for the InCharge SNMP Trap Adapter

SMARTS recommends the forwarding of a particular subset of traps, rather than all traps.

As with previous InCharge versions, traps will not be forwarded unless you uncomment lines of code.

The *trapd.conf* file still retains the code to forward all traps if it is appropriate for your configuration. The file does not contain code to forward traps to the Service Assurance Manager Adapter Platform or to Application Services Manager.

Documentation Errata

The following issues describe corrections to documents.

Correction for Location of HTML Documents

HTML documents are not accessible from the CD-ROM, but they are installed on the host machine and are available from the ***BASEDIR****/smarts/doc/html* directory. The *InCharge Documentation Roadmap* erroneously states that the HTML documents can be accessed from the CD-ROM.

Correction for runcmd_env.sh File

Pages 75 through 76 of the *InCharge System Administration Guide* erroneously state that if you add a SMARTS environment variable to the *runcmd_env.sh* file, it sets the variable for all InCharge software that runs on that system. Since a *runcmd_env.sh* file exists for each suite of InCharge products, the environment variables you set in the file will only be used by the products in the product suite.

If you have multiple product suites installed on a system and you want to set a system-wide environment variable, you must add the desired environment variable to each suite's *runcmd_env.sh* file.

Associating InCharge Files With sm_edit on Windows

The *InCharge System Administration Guide* describes how to associate InCharge configuration files with the sm_edit utility on Windows systems. The procedure to associate InCharge configuration files with sm_edit is correct as described. However, if you install multiple product suites (for example, IP and SAM) on the same host, you can only associate the sm_edit utility from one product suite with InCharge configuration files. Opening an InCharge configuration file from a different suite by double-clicking on it in Windows Explorer will result in an error. Instead, invoke the sm_edit utility at the command prompt from the ***BASEDIR****/smarts/bin* directory of the product suite that includes the configuration file you want to edit.

Corrections to Trap Adapter and Application Connectivity Monitor Examples

Two examples in the *InCharge System Administration Guide* are incorrect.

Page 40, in the Trap Adapter code example, the last line incorrectly reads:

```
icoi-trapd/trap_mgr_parse.asl
```

The last line should read:

```
--rules=icoi-trapd/trap_mgr_parse.asl
```

Page 42, in the Application Connectivity Monitor code example, the third line incorrectly reads:

```
/opt/InCharge6/APP/smarts/bin/sm_adapter
```

The third line should read:

```
/opt/InCharge6/APP/smarts/bin/sm_server
```

Format Change for the -D Option

Page 121 of the *InCharge Operator's Guide* states that the `-D` option should be specified once, followed by comma delimited pairs of properties and values. Instead, you must specify the `-D` option before each pair and commas are no longer necessary. For example, to change the font to Arial and set the font to 20 points, specify:

```
sm_gui -D com.smarts.font=Arial -D com.smarts.fontSize=20
```

Direct Telephone Number for SMARTS Technical Support

In addition to SMARTS main telephone number, which is provided in the preface of all InCharge documents, you can also contact SMARTS Technical Support directly by dialing 1-914-798-8600.

3

Release Notes for Service Assurance Management Suite

This chapter describes issues and resolutions for products of the InCharge Service Assurance Management (Service Assurance) Suite.

Global Console

The following issues relate to running the Service Assurance Global Console.

Client Tool May Not Stop

Issue:

For client tools, when you press the **Stop** button in the Tool Output window, the client process may not stop. Processes (such as shell scripts) that do not respond to a SIGTERM signal will not stop.

Resolution:

Use a script that responds to a SIGTERM signal. Or, terminate the client process manually from the command line or by using the Task Manager.

User Unable to Configure Web Portal From Global Console

Issue:

The user will not be able to configure the Web Portal from the 6.0 Global Console.

Resolution:

The Web Portal is not distributed in the InCharge 6.0 release. The Web Portal is only available as a 5.0.x version. So, you should use the 5.0.x Global Console to configure the Web Portal.

Map Console

Issue/Limit:

The Map Console is not supported with the Java applet for any platform. However, this can be configured by a SMARTS Professional Services Representative.

IP Network Map Node

Issue:

In a map, the node for an IP network is always green, even if the network is inaccessible.

Resolution:

SMARTS intends to address this issue in a future release of the product.

Unable to Load the Java Applet

Issue/Limitation:

If you install your broker with the InCharge IP Management Suite instead of with the InCharge Service Assurance Management Suite, you will not be able to load the Java applet from the broker URL.

Resolution:

You must download the Java applet by using the URL of the Global Manager. This will only work if the console is installed with the Global Manager.

Java Applet May Not Attach to Broker

PR 9450

Issue:

The Java applet defaults to using smarts-broker:426 as the broker. If "smarts-broker" is not configured as a host name by the customer, the applet will not attach to the broker by default.

Resolution:

Using sm_edit, change *classes/unzipped/config.properties* on the machine that serves the applet. Change the line that says:

```
smarts.remote.broker=smarts-broker:426
```

to:

```
smarts.remote.broker=<broker host>:<broker port>
```

where <***broker host***> is the machine that the broker is on and <***broker port***> is the port it is running on.

Console Forces You to Abandon Unapplied Changes

PR 9316

Issue:

Administration Consoles (Global and Domain) force you to abandon unapplied changes when you switch domains.

If you are editing a configuration from one of the administration consoles or from Polling and Thresholds Console and you select a new domain from the InCharge Manager pull-down menu while you have unapplied changes, a warning dialog pops up. The dialog says "Do you want to abandon unapplied changes?" You must select "Yes". If you select "No", the same dialog will pop up two or three more times, and afterwards the dialog will pop up each time you select an new instance, until you respond "Yes".

Resolution:

Close the offending console and re-open it.

Expanded Topology and Node Visibility

PR 9714

Issue:

While using UNIX, in the event that the topology is expanded such that more than approximately 2200 nodes are visible in the tree, the tree's background turns gray and the tree is not repainted properly.

Resolution:

Close some class nodes in the tree so that fewer than 2200 nodes are visible.

Topology Browser Console and Unapplied Changes

PR 9693

Issue:

The Topology Browser Console allows you to edit attribute values of topological elements in InCharge Domain Managers, but there is no **Apply** button available to apply these changes. If, after editing an attribute, you select a different instance in the topology tree, you are prompted with a popup dialog that asks whether or not you would like to abandon unapplied changes. You cannot apply the changes, so you must abandon them.

Resolution:

Only edit attributes from the Domain Administration Console. This console has an **Apply** button.

Program Tool Issue

The following issue relates to running Service Assurance program tools.

Ping and Telnet Tools Have Access Constraints

PR 6389

Issue:

The sample scripts for ping and Telnet server tools, located in your ***BASEDIR****/smarts/local/actions/server* directory, may not work properly in all cases.

For example, the sample scripts do not take firewalls into account. If an underlying domain manager running InCharge Availability Manager generates an IP Down notification and a firewall exists between the device and the Service Assurance Global Manager, the Service Assurance Ping tool cannot ping the IP address. The ping script is invoked from the same host as the global manager.

Resolution:

The ping and Telnet tools are sample scripts. You need to customize them to meet the needs of your environment.

SAM Adapters

The following issues relate to adapters.

Configuration Parameters in Notifiers

PR 6452 and 6392

Issue:

Values specified for the MinimumCertainty and eventSmoothingInterval parameters in the configuration file of E-Mail Notifier, File Notifier, SNMP Trap Notifier, Script Notifier, and TIBCO Rendezvous Notifier are ignored.

Resolution:

In the configuration file of the affected adapters, the MinimumCertainty and eventSmoothingInterval parameters are not supported. Also, the notification filters used in adapters for InCharge version 4.0.1 or later are not supported.

You can define a notification list with notification list filters and minimum certainty in the global manager's configuration file (*ics.conf)* and apply them to adapters. You cannot define a smoothing interval using the adapter's configuration file.

For minimum certainty, you can specify a notification list filter that matches the Certainty field against a numeric value.

For example,

```
match("Certainty", "<30->")
```

results in a minimum certainty of 30%.

The name of notification list in the global manager's configuration file (*ics.conf)* must match the NLName parameter value in the adapters' configuration file. Adapters receive notifications as determined by the notification list name specified for the NLName parameter.

sm_ems Issue

The following issue relates to the sm_ems command line interface.

sm_ems Does Not Prompt for Authentication Credentials

PR 7618

Issue:

By default, the sm_ems command line interface does not prompt for authentication credentials.

Resolution:

If you are working in a secure environment, you need to create an entry in the *clientConnect.conf* (using the *sm_edit* utility) that provides the necessary user name and password for the sm_ems interface. The user name in this entry must match a user in the corresponding *serverConnect.conf*. You must edit the *clientConnect.conf* file on the host where sm_ems is running.

Java Issues

The following are Java issues.

Adjusting Memory for Java Dynamic Memory Allocation

PR 5660

Issue:

The host machine is experiencing degraded performance due to memory swapping.

Resolution:

The `-H` option for the **sm_gui** command enables you to adjust the maximum amount of memory space ("heap size") that Java uses for dynamic memory allocation. The default value for the maximum "heap size" is 256 MB.

To improve performance, specify the **sm_gui** command with the `-H` option:

```
sm_gui -H valueM
```

Specify the `-H` option once. One space after the `-H` is required. The value you specify can be greater or less than the 256 MB default, depending upon the host machine. The character "M" (uppercase or lowercase) is required; do not insert a space between the value and the M.

The heap size can be up to the following approximate values:

Operating System	Approximate Maximums
Solaris 8 and 9	4000 MB
HP-UX 11.0 and 11.11	2000 MB
AIX 4.3.3	2000 MB

Table 4: Operating Systems and Their Heap Size Values

For example, if the available memory for a host machine is 256 MB, you can specify 100 MB for the heap size:

```
sm_gui -H 100m
```

Default User Profile Requirement

PR 6632

Issue:

When you log in to a Global Manager, if the specified user name (for example, admin or operator) does not correspond to a defined user profile, the default user profile is used instead. If the default user profile does not exist, you receive an error message and the Global Console does not open. This is proper behavior.

If you are already attached to a Global Manager and you attempt to attach to a second Global Manager that does not have a default user profile, you may observe the following types of behavior:

- The second Global Manager appears to be attached; its name is listed in the Global Manager pull-down menu of the Notification Log Console. However, the Notification Log view is blank.
- If you switch and select the first Global Manager in the Global Manager pull-down menu, notifications that previously displayed in the view no longer appear. (In order to redisplay the notifications, detach from the second Global Manager.)
- If you detach and reattach to the second Global Manager, you may receive messages that the console cannot attach to the Global Manager or that the console is already is attached. If you continue to try to detach and reattach, "None" is listed repeatedly in the Global Manager pull-down menu.

Resolution:

SMARTS provides two user profiles, default-profile and maint-profile. Both profiles, especially the default-profile one, should not be deleted. You must have a default user profile defined for every Global Manager. Or, you can create a profile in Global Manager Administration Console for every user name that is allowed to access the Global Manager.

Documentation Errata

The following issues describe a correction to documents.

InCharge Adapter for TIBCO Rendezvous Version Support

The InCharge Adapter for TIBCO Rendezvous only integrates with TIBCO Rendezvous version 6.8 software. The *InCharge Installation Guide* erroneously states that the InCharge Adapter for TIBCO Rendezvous integrates with TIBCO Rendezvous version 6.x.

Correction for Modifying mail-custom.asl

Page 42 of the *InCharge Service Assurance Manager Notification Adapters User's Guide* incorrectly states to use the following to invoke the use of the *mail-custom.asl* in Step 2:

```
OMIT_CLEAR_EVENTS()
    filter {
        (currentEvent->icType == "CLEAR"
        || currentEvent->icType == "NL_CLEAR")
    }
    do {currentEvent->filterMe = TRUE;}
    do {currentEvent->sentByCustom = TRUE;}
```

The correct code after the START statement should be:

```
/*
 * Filter cleared events.
 */
OMIT_CLEAR_EVENTS()
    do {
        if (currentEvent->icType == "CLEAR"
         || currentEvent->icType == "NL_CLEAR" )
        {         currentEvent->filterMe = TRUE;
                  currentEvent->sentByCustom = TRUE;
        }
    }
```

Corrections for XML insert and put Methods

Page 9, Table 4, of the *InCharge XML Adapter User's Guide* states that attributes may be modified using the insert or put methods. This is not entirely true; only stored attributes may be modified with the insert and put methods. Propagated attributes, instrumented attributes, and computed attributes can not be modified with the insert or put methods.

The document also states that the insert method for attributes adds a value to a set of attributes. This is only true if the attribute allows for multiple values. If the attribute can only have one value, then using the insert method will actually replace the existing single value instead of adding to the set of values.

Correction to a Tool Example

The tool example on page 86 of the *InCharge Service Assurance Manager Configuration Guide* is incorrect.

When using the `--subscribe` option to subscribe to a notification list, append `/n` after the name of the notification list as shown below. Note that the slash at the end of each line indicates that all of the options should be typed on the same line.

```
# BASEDIR/smarts/bin/sm_adapter --server=INCHARGE-SA \
--subscribe=TicketingNL/n \
-DNotifyAction="Open Trouble Ticket" \
-DClearAction="Close Trouble Ticket" \
-DLogActions=TRUE \
--output \
ics/auto-action.asl
```

Correction to an ASL Filter Example

The ASL filter example on page 138 of the *InCharge Service Assurance Manager Configuration Guide* is incorrect. Also, the example script, *nl-sample-filter.asl*, resides in the ***BASEDIR****/smarts/rules/ics directory* and not in the */local* subdirectory. The correct code should be:

```
START do {
      notification = object(NotificationName);
      if (notification->EventName == "Failure")
      {
         Result = TRUE;
      }
      else
      {
         Result = FALSE;
      }
}
```

Correction to Syntax for an Import Option

Page 146 of the *InCharge Service Assurance Manager Configuration Guide* has a typographical error. There should not be a space in the syntax for the option `--addmodify`. The correct text for the "Importing Options" section and an example is as follows:

- `--addmodify`: Use this option (without the `--force` option) and the timestamp of the repository object is monitored. If an object you configured was modified since the last time you exported, the object will not be imported in order to protect the modified configurations.

For example, you would use the following command to import configurations from a file called *ics-conf.xml* into a Global Manager called INCHARGE-SA and ensure that your configurations do not override any changes made from the Global Manager Administration Console:

```
#./sm_config -s INCHARGE-SA import --addmodify ics-conf.xml
```

Correction to Syntax for the sm_config Command

Pages 145 through 148 of the *InCharge Service Assurance Manager Configuration Guide* have a typographical error regarding the example command lines for the **sm_config** command. In each instance of the command example, it erroneously states that the syntax is:

```
./sm_config -s=<server_name>
```

The correct syntax (no equal sign) for all of these code examples is:

```
./sm_config -s <server name>
```

For example, on page 145 there is a command example in Step 2 of Importing XML Files to the Global Manager. The correct command should read as follows:

```
#./sm_config -s INCHARGE-SA import NewUsers.xml
```

Corrections for the InfoVista Adapter

InCharge Service Assurance Manager User's Guide for InfoVista Adapter provides incorrect locations to the configuration and script files and an incorrect default variable value.

Page 8, the section "Editing the infovista.conf Configuration File" incorrectly states that the *infovista.conf* file, once edited, is copied to the ***BASEDIR****/smarts/local/script/server/infovista* directory. The file is actually copied to ***BASEDIR****/smarts/local/conf/infovista*. There is also a typographical error on the file name. The file name is *infovista.conf,* not *invovista.conf*.

Page 10, Table 6, the default value for the InfoVistaUserName variable is administrator in both client tool files, infoVistaTrapReport and showVistaReport. The default value is not operator for the variable in the showVistaReport file.

Pages 12 and 13, the location of the script file, *runExportImport.sh*, is also incorrect. The *runExportImport* script is located in the ***BASEDIR****/smarts/script/infovista/server* directory, not in the ***BASEDIR****/smarts/script/server/infovista* directory.

Correction for Web Portal

Page 52 of the *InCharge Service Assurance Manager Web Portal Configuration Guide* lists an incorrect directory in an example for copying JDK files in Step 2. The correct directory is ***BASEDIR****/jdk/jre/lib/ext* and not ***BASEDIR****/jdk/lib/ext*.

4

Release Notes for IP Management Suite

This chapter describes issues and resolutions for products of the InCharge IP Management Suite.

InCharge Applications

The following issues apply to all InCharge applications:

- InCharge IP Availability Manager
- InCharge IP Performance Manager
- InCharge IP Discovery Manager

"Illegal" Device Names

Issue:

During the discovery process, InCharge discovers a network element that has the same name as InCharge Information Model (ICIM) class names. InCharge considers these names to be "illegal". A warning is issued to the log file and the device is not added to the topology.

Resolution:

Log files are found in the ***BASEDIR****/logs* directory. All log files have a ".log" file type. The name of a domain manager's log file is based on the domain manager's name. In typical installations, the log file is named *INCHARGE.log*.

The warning message for an "illegal" name reads:

```
<Device IP Address> is resolved to <InCharge Class Name> which
is a class name in INCHARGE.
```

In this warning, <Device IP Address> represents the address of the device and <InCharge Class Name> represents the exact InCharge class name.

For example, if you have a device at IP address 123.12.123.123 named Switch, then the warning will read:

```
123.12.123.123 is resolved to Switch which is a class name in
INCHARGE.
```

If this warning appears in your log file, SMARTS suggests renaming the device before attempting another discovery.

Error Message Displayed While Setting Full Discovery Below 60 Minutes via Topology Tab

PR 9432

Issue:

In the Domain Manager Administration Console from the Topology tab, if the user selects "Enable Full Discovery" and sets an interval time below 60 minutes, an error message displays:

```
Apply changes failed: CI-E-ICF-TopologyManager:
reprobePeriod:constraint MinimumProbePeriod MR-Violation of
hard constraint
```

Resolution:

For "Enable Full Discovery," set an interval time above 60 minutes.

Certified Device Support

The following issues relate to certified device support.

Changed Certifications for ICIP 6.0 SP1

The following changes have been made to previous certifications for ICIP 6.0 SP1.

VENDOR	MODEL NAME	OID	DESCRIPTION
Cisco	VPN 3000 Concentrator	.1.3.6.1.4.1.3076.1.2.1.1.1.2	Changed from a router to a firewall
Cisco	VPN 3000 Concentrator	.1.3.6.1.4.1.3076.1.2.1.1.2.1	Changed from a router to a firewall
Foundry	BigIron15000	.1.3.6.1.4.1.1991.1.3.14.2	Changed from a router to a switch
Foundry	IronRouter	.1.3.6.1.4.1.1991.1.3.7.2	Changed from a router to a switch
Nokia	Nokia2-Firewall-1 3.2-fcs4 releng 783	.1.3.6.1.4.1.94.1.21.2.1.9	Changed from a router to a firewall
Nokia	Nokia IP650	.1.3.6.1.4.1.94.1.21.2.1.8	Changed from a router to a firewall
Nokia	Nokia IPS0	.1.3.6.1.4.1.94.1.21.2.1.1	Changed from a router to a firewall
Nokia	Nokia IP740	.1.3.6.1.4.1.94.1.21.2.1.12	Changed from a router to a firewall
Larscom	Mega-E	.1.3.6.1.4.1.555.2.3.7	Model attribute has changed

Table 5: Summary of Certification Changes for ICIP 6.0 SP1

Incorrect Directory for IDS Certified Device List

PR 9945

Issue:

The IDS-009 Certified Device List is installed to the ***BASEDIR****/smarts/doc/pdf/IDS* directory. It should, instead, be installed to the ***BASEDIR****/smarts/docs/html/IDS* directory.

Resolution:

SMARTS intends to correct the file location in the next release of the InCharge IP Management Suite.

Cisco 2948G and 4232 L3 Module Conflict

Issue:

Cisco 2948G and 4232 L3 module share the same sysObjectID (that is, .1.3.6.1.4.1.9.1.275). Since InCharge uses the sysObjectID to identify the device type, InCharge Availability Manager by default classifies both devices as "Switch."

Even though the 4232 L3 module is classified as a switch, it has all of the router properties (for example, interfaces, IP endpoints, memory, processors, etc.) as defined by InCharge Availability Manager and it is monitored as a router.

For some customers, the device type is critical for creating trouble tickets.

Resolution:

If the device type is critical, you can classify the 4232 L3 module as a router. To do so, modify the field certification file, if it exists, for this unique situation.

The *oid2type_Field.conf* file, located in the ***BASEDIR****/smarts/conf/discovery* directory, contains field certification information. Under normal circumstances, SMARTS recommends editing the file to include only non-network devices such as personal computers or printers. This modification is an exception.

If the *oid2type_Field.conf* file does not exist, use the *oid2type_Field.conf.template* to create it. For instructions about using the template, see the *InCharge IP Discovery Guide*.

If *only* the 4232 L3 module is deployed in the network, to classify the module as a router, add the following device entry to the *oid2type_Field.conf* file:

```
# CAT4232-IN-M L3 (Switch/Router)
.1.3.6.1.4.1.9.1.275 {
   TYPE = Router
   VENDOR = Cisco
   MODEL = 4232 L3
   CERTIFICATION = CERTIFIED
   CONT = Cisco-Router
}
```

For additional information about the *oid2type_Field.conf* file, see the *InCharge IP Discovery Guide*.

Availability Manager Application

The following issues relate to InCharge IP Availability Manager for Networks.

Diagnosis of Card Down Problems on Cisco LS1010 Switches

Issue:

To diagnose a Card Down problem, InCharge needs to query the MIB variable ciscoLS1010ModuleOperStatus. However, this MIB variable is often not implemented on LS1010 switches. As a result, diagnosis of Card Down problems is disabled.

Resolution:

If the MIB variable ciscoLS1010ModuleOperStatus is available in the SNMP agent, contact SMARTS Technical Support for assistance.

Card Status Not Updated When Card Is Reinserted

Issue:

After discovering a switch, InCharge uses the ModuleInsertion trap to monitor the status of cards within the switch. When InCharge receives a ModuleDown trap, it marks the card as OperationallyDown. When InCharge receives a ModuleUp trap, it adds the switch to the Pending Devices List so that the switch is rediscovered and the status of the card is updated. Upon reinsertion of the card, the status may not be updated.

InCharge currently supports the ModuleInsertion trap for the following switches:

- Cisco
- 3Com Corebuilder

Resolution:

If you have a switch where the status of a card in not updated when it is reinserted, contact SMARTS Technical Support. SMARTS routinely adds support for new devices through the Incremental Device Support program.

Connections Between Foundry and Cisco Switches

Issue:

Availability Manager does not discover all connections (trunk cables) between Foundry switches and Cisco switches due to a known bug in the Foundry agent implementation. The bug causes incorrect Spanning Tree Protocol (STP) information which, in turn, causes Availability Manager to make connections to the wrong ports. Because of the known bug, Availability Manager no longer uses the incorrect STP information which is why connections might be missing from the topology.

Resolution:

Perform these steps to rectify the situation:

1. Update all Foundry switches to use MIB version 7.6. (The known bug is fixed in the 7.6 version of the Foundry MIB.)
2. Issue the following command (all on one line) to enable Availability Manager to use STP information to make connections between Foundry and Cisco switches:

```
dmctl -s <domain_manager_name> invoke
ICF_TopologyManager::ICF-TopologyManager insertParameter
STPTRUNK_EnableFoundryCisco TRUE
```

Note: Step 1 is required; otherwise, the command in Step 2 will cause connections to the wrong ports. The command in Step 2 remains in effect even if the domain manager is stopped and restarted.

To disable the use of STP information to make connections, use the above command and specify FALSE instead of TRUE.

Disabling SNMP Polling Through Special Read Community String

Issue:

Beginning with InCharge version 6.0, users can specify that InCharge IP Availability Manager uses only ICMP to access devices for discovery and monitoring. This is accomplished by setting the ICMPONLY Access Mode in a discovery filter, the Add Agent command, or a seed File.

Prior to InCharge 6.0, InCharge customers may have used the SM_SNMP_SQUELCH environment variable to restrict discovery and monitoring to ICMPONLY. Although this method is still supported in 6.0, customers should no longer use it. Instead, you should use the new ICMPONLY Access Mode. For more information about the Access Mode, refer to the *InCharge IP Discovery Guide*.

Discovery Pending Interval

PR 9432

Issue:

When the discovery pending interval is shorter than five minutes or the full discovery interval is less than one hour, the following exception is thrown from the Domain Manager Administration Console:

```
Apply changes failed: CI-E-ICF-TopologyManager:
reprobePending_period: constraint MinimumProbePeriod MR-
Violation of hard constraint
```

Resolution:

The discovery pending interval can not be less than five minutes. The full discovery interval can not be less than one hour.

Performance Manager Application

The following issue relates to InCharge IP Performance Manager.

Changed Method for Determining Duplex Mode

Beginning with InCharge 4.1.2, SMARTS changed the method for determining the duplex mode of ports and interfaces. Previously, InCharge IP Performance Manager calculated the duplex mode for ports or interfaces when the duplex mode was not specified. With version 4.1.2 and later, InCharge IP Performance Manager only uses the MIB to determine the duplex mode. If the MIB does not specify the duplex mode, analysis for High Utilization faults is disabled for that port or interface. Such interfaces have a value of UNSPECIFIED for the DuplexMode attribute.

If the value of the DuplexMode attribute for a port or interface is UNSPECIFIED and you know the duplex mode, you can enable the analysis for High Utilization faults. Use the Domain Manager Administration Console or the *dmctl* utility to change the value of the DuplexMode attribute for the port or interface object to the appropriate value. Valid values include FULLDUPLEX, HALFDUPLEX, and UNSPECIFIED. Changes made to the DuplexMode attribute of a port or interface are not overwritten when the device is rediscovered.

Note: This change only affects new devices added to the topology of a running InCharge IP Performance Manager that is upgraded to version 6.0. It also affects new installations of InCharge IP Performance Manager version 6.0.

Excessive Fragmentation and Cisco Catalyst Switches

Issue:

The Excessive Fragmentation fault occurs frequently and inaccurately for Cisco Catalyst switches, due to a fixed value supplied by the Cisco MIB, CISCO-MEMORY-POOL-MIB. The Excessive Fragmentation fault is one of several faults that can trigger a Resource Exception notification.

Resolution:

For Cisco Catalyst switches only, analysis for the Excessive Fragmentation fault is disabled. A related fault, Insufficient Free Memory, for the switches remains enabled.

Note: For Cisco Catalyst routers, analysis for excessive fragmentation remains enabled.

Exceed Issues

The following issues relate to running an InCharge Console from a UNIX platform and displaying through Exceed on a Windows desktop.

Exceed and Minimized Windows

Issue:

When an InCharge console is run from a UNIX platform and displayed through Exceed on a Windows desktop, the windows (popup window, dialog box, etc.) in the console may not be sized correctly. The windows may display in a minimized state.

Resolution:

SMARTS suggests that you install the InCharge Console on the Windows desktop. Or you can run Exceed in single-window mode with the XDMCP-query communication option.

Exceed and Repeated Console Closure

Issue:

When an InCharge console is run from a UNIX platform and displayed through Exceed in multi-window mode on a Windows desktop, opening a console with the **sm_gui** command and closing it repeatedly causes the console to fail and print a stack trace.

Resolution:

SMARTS suggests that you install the InCharge Console on the Windows desktop. Or you can run Exceed in single-window mode with the XDMCP-query communication option.

HP OpenView Pathname Not Converted Properly During Installation

PR 6093

Issue:

When HP OpenView 6.2 is installed on Windows, the pathname may contain spaces which are not converted properly in the InCharge *OV_TOPO.import* file. By default, HP OpenView 6.2 installs itself in *Program Files/HP OpenView*.

Resolution:

The resolution has three steps:

1. Modify the *OV_TOPO.import* file.
2. Register InCharge with HP OpenView.

Modifying the OV_TOPO.import File

The file ***BASEDIR****smarts**conf**OV**OV_TOPO.import* must be modified to state the correct path to the OpenView *ovtopodump* executable.

In the GA_Driver section of *OV_TOPO.import* (below), the command string setting should be changed from:

```
ReadsInputFrom = GA_ProgramFE::OpenView-Topology-FE
{
commandString = "/opt/OV/bin/ovtopodump -rl"
}
```

to:

```
commandString =
"C:\Program Files\HP OpenView\opt\OV\bin\ovtopodump -rl"
```

Registering InCharge with HP OpenView

Next, the InCharge registration files must be registered with OpenView. Use the following command (all on one line):

```
C:\"Program Files\HP OpenView"\NNM\bin\ovaddobj.exe
C:\InCharge\smarts\conf\OV\sm_ovtopo.lrf
```

Repeat for each file: *sm_ovevent.lrf*, *sm_ovfwd.lrf*, *sm_ovlog.lrf*, and *sm_ovtopo.lrf*.

Alternatively, change directory to OpenView and issue the following command (all on one line):

```
cd C:\"Program Files\HP OpenView"\NNM
bin\ovaddobj C:\InCharge\smarts\conf\OV\sm_ovevent.lrf
bin\ovaddobj C:\InCharge\smarts\conf\OV\sm_ovfwd.lrf
bin\ovaddobj C:\InCharge\smarts\conf\OV\sm_ovlog.lrf
bin\ovaddobj C:\InCharge\smarts\conf\OV\sm_ovtopo.lrf
```

Adapters Fail to Create Log Files

Issue:

For Windows 2000, the following adapters will not create a log file: OpenView/NetView Initial Topology Reader, OpenView/NetView Topology Update Reader and OpenView/NetView Forwarder.

Resolution:

SMARTS intends to address this issue in a future release of the product.

Documentation Errata

The following issue describes corrections to documents.

Correction for Extracting a Seed File

Page *77* of the *InCharge IP Discovery Guide* describes how to extract a seed file from an InCharge Domain Manager using the sm_tpmgr utility. The example, and its description, is incorrect. The example should read:

```
#./sm_tpmgr -s INCHARGE-AM --dump-agents --output=seedfile
```

This creates a file named *seedfile.log* in the ***BASEDIR****/smarts/local/logs* directory. You should invoke the sm_tpmgr utility from the location where the InCharge Domain Manager is installed.

5

Release Notes for Security Infrastructure Management Suite

This chapter describes issues and resolutions for products of the InCharge Security Infrastructure Management Suite.

Discovery Options Are Not Supported

PRs 8580 and 8595

Issue:

When you import firewalls into FPM's topology, the options Enable Full Discovery and Enable Auto Discovery are not supported. These options are located on the Topology tab in the Domain Manager Administration Console (accessed from the Global Console).

Resolution:

Firewalls are imported manually into FPM's topology using a seed file or the Add Agent menu option.

Concord SystemEDGE SNMP Agent Version 4.2 Causes Erroneous Results

PRs 8691 and 8701

Issue/Limitation:

Concord SystemEDGE SNMP agent, version 4.2 patch level 2, provides erroneous information. As a result, FPM's discovery and correlation results are also erroneous.

For example, since the MIB-II ifType variable has the incorrect value 1, discovered firewall interfaces are added to FPM's default thresholds group named Other Interfaces instead of the 10/100 Mb Ethernet group. Consequently, the wrong threshold settings might be applied to the interfaces.

FPM's correlation results are also affected when MIB-II is not updated, because related notifications are not generated.

Login Session Notifications Do Not Clear for Disconnected Security Adapters

PR 8737

Issue:

Login notifications are aggregated with other session notifications such as CheckPoint_Database_Locking; therefore, they cannot be cleared by acknowledgement. They stay active when acknowledged.

When a security adapter disconnects from SIM (due to a network outage, for example), the login session notifications from an unavailable security adapter are not updated in the Global Console. If, in addition to the disconnected adapter, SIM also goes down gracefully and is restarted, the Event State column for affected open session notification changes to WAS_ACTIVE.

Resolution:

When the unavailable security adapter reconnects, you can clear the login session notifications in the WAS_ACTIVE state by acknowledging them.

If the SIM server cannot be restarted, please contact SMARTS Technical Support to clear the Session notifications using command line tools or scripts.

Nokia IPSO Agent Issue

Issue/Limitation:

Nokia's IPSO agent does not index the process table from the HOST-RESOURCES MIB using the process ID. It appears to be using a sequence of integers to index the processes. If a new process is added, it gets assigned a low integer index in the table (for example, 2), and the entire process table is shifted down. Similarly, if a process is deleted, the entire table is shifted up. This makes if very difficult, if not impossible, to keep the indices that the SNMP accessor uses for instrumentation synchronized with the most current ones at the agent.

To avoid inconsistent behavior, process monitoring for Nokia devices has been turned off by commenting out all processes of interest on a Nokia firewall from the *ProcessList.conf* file.

Resolution:

This is a known IPSO agent bug. Contact SMARTS Technical Support to find out if this issue has been resolved.

Nokia Firewalls Time Out

PR 8763

Issue:

Nokia firewalls with operating system IPSO 3.6-FCS6 or FCS3 time out during an SNMP MIB walk or a query for invalid OIDs. When this occurs, all subsequent SNMP activity on the firewall ceases.

Resolution:

The operating system Nokia IPSO 3.6-FCS7 is required on Nokia firewalls.