EMC²

RELEASE NOTES

EMC® Ionix™ IP Management Suite

Version 7.0 Service Pack 4

Release Notes

P/N 300-011-427
REV A01

November 03, 2010

These release notes contain information about the EMC Ionix IP Management Suite 7.0.4 release, referred to as Service Pack 4 or SP4. Topics include:

- Revision History 2
- Introduction 2
- Product description 2
- New features and changes 3
- Fixed problems 46
- Environment and system requirements 54
- Known problems and limitations 58
- Technical notes 73
- Documentation 74
- Software media, organization, and files 77
- Troubleshooting and getting help 79

Note: On July 8th, 2009, EMC announced that EMC® Ionix™ is the family name that unifies the family of products: EMC® Smarts®, EMC® Voyence®, and EMC® ControlCenter®. In addition to the new family name, individual products will be renamed in future releases. The title of this document uses the new Ionix name, however references to earlier product releases and supporting documentation use EMC Smarts.

Revision History

The following table presents the revision history of this document.

Revision	Date	Description
A01	November 03, 2010	First release

Introduction

These release notes supplement the release notes provided with the Ionix IP Management Suite 7.0 release. Unless indicated otherwise in these release notes, all enhancements, fixes, and limitations described in the 7.0 release notes are still applicable to the IP Management Suite 7.0 products.

Service Pack 4 contains all the contents of IP Management Suite 7.0 which includes all the enhancements and fixes of IP Management Suite 7.0 service packs 1, 2, and 3 and new enhancements and fixes. You may use Service Pack 4 to install a new 7.0.4 installation of the IP Management Suite, or upgrade an existing 7.0.1, 7.0.2, or 7.0.3 installation to 7.0.4.

Note: For EMC Smarts software prior to version 7.0.1, service packs were referred to as SmartPacks. Like service packs, SmartPacks contained enhancements and fixes to known problems, but unlike service packs, SmartPacks did not contain base product files.

Product description

Service Pack 4 delivers enhancements and fixes to the following products:

- IP Availability Manager
- IP Performance Manager
- IP Server Performance Manager
- IP Discovery Manager

IP Server Performance Manager is an enhanced version of IP Performance Manager and is available through a feature license.

Note: In this document, "IP Manager" is used to collectively represent IP Availability Manager, IP Performance Manager, IP Server Performance Manager, and IP Discovery Manager.

Installation executables

As with all service packs, Service Pack 4 is distributed as individual platform-specific installation executable files. A service pack installation executable contains base product files, new and replacement files, and a Java-based installation program.

The following base installation executables for Service Pack 4 are available for download from EMC Powerlink®:

- setup-IP-7_0_4_0-sol.bin
- setup-IP-7_0_4_0-linux.bin
- setup-IP-7_0_4_0-hpux.bin
- setup-IP-7_0_4_0-win.exe

The names of the files comply with the following naming convention for EMC Smarts installation executables:

```
setup-<suite>-<version>-<os>.<bin|exe>
```

JRE bundled in installation executable

As with all service packs, the Java Runtime Environment (JRE) is bundled with the Service Pack 4 installation executable. The installation executable installs the JRE and starts a Java-based installation program that accesses the JRE to run.

New features and changes

In addition to new product enhancements, Service Pack 4 includes the product enhancements provided by service packs.

- "Product enhancements in Service Pack 4" on page 4
- "Product enhancements in Service Pack 3" on page 29
- "Product enhancements in Service Pack 2" on page 36
- "Product enhancements in Service Pack 1" on page 37

Product enhancements in Service Pack 4

The following enhancements are new in Ionix IP Management Suite 7.0 Service Pack 4:

- "Support for additional operating systems" on page 4
- "Enhanced support for VMware" on page 4
- "Support for new device certifications" on page 5
- "Support Virtual Router Redundancy Protocol (VRRP)" on page 5
- "Support for Link Layer Discovery Protocol (LLDP)" on page 11
- "Thresholds for individual devices and filesystem instances" on page 16
- "New directory to backup user-modified files during an upgrade" on page 27
- "Changes in creation of Card Redundancy groups for Cisco devices" on page 28
- "New groups added for devices of type MediaGateway for performance polling" on page 28
- "New flag RetainStaleConnections introduced to retain stale connections in the topology" on page 29

Support for additional operating systems

Ionix IP Management Suite 7.0 Service Pack 4 supports the following additional operating systems:

- Microsoft Windows Server 2008 Enterprise Edition SP1, SP2, and R2
- Red Hat Enterprise Linux Server 5

Enhanced support for VMware

Ionix IP Management Suite 7.0 Service Pack 4 adds support for VMware ESX 3.5 and VMware vSphere™ 4 that run the following operating systems for virtual machines:

- Microsoft Windows Server 2008 Enterprise Edition SP1, SP2, and R2
- Red Hat Enterprise Linux Server 5

IMPORTANT

To run IP 7.0.4 on Red Hat Enterprise Linux Server 5, ensure that *compat-libstdc++-33-3.2.3-61* is installed.

Support for new device certifications

Ionix IP Management Suite 7.0 Service Pack 4 adds support for new device certifications. The new certifications have been added to the *EMC Ionix IP Certification Matrix for 7.0.4* device certification document (.xls file) and are highlighted with a blue background.

Support Virtual Router Redundancy Protocol (VRRP)

Virtual Router Redundancy Protocol (VRRP) is a standard protocol that provides virtual standby redundancy for routers. This redundancy ensures that user traffic recovers from first hop failures immediately and transparently in network edge devices or access circuits. The Availability Manager can monitor routers in VRRP configurations and indicate the availability of the VRRP routers in normal, switchover, and failure scenarios.

VRRP is designed to eliminate the single point of failure that is inherent in a static default routed environment. It specifies an election protocol that dynamically assigns responsibility of a virtual router to one of the VRRP routers on a LAN. The VRRP router that controls the IP addresses associated with a virtual router is called the master. The master router forwards packets sent to these IP addresses.

Should the master become unavailable, the election process provides dynamic failover in the forwarding responsibility. Any of the virtual router's IP addresses on a LAN can then be used as the default first hop router by end-hosts. The advantage of using VRRP is a higher availability default path without requiring the configuration of dynamic routing or router discovery protocols on every end-host.

Creation of VRRP groups

During discovery of the VRRP-enabled routers, IP Availability Manager creates a new redundancy group called VRRP group. The VRRP group is created for each Virtual Router Identifier (VRID). It is composed of a logical element that is defined per interface, per VRRP group, on a VRRP router called VRRP endpoint. VRRP endpoints belonging to the same VRRP group (that is, having the same VRID) have a common virtual IP and a virtual media access control (MAC). The virtual MAC is defined as xx-xx-xx-xx-xx-VRID. The

VRRP-enabled router with the highest priority is considered to be the master router. All other routers are considered to be backup routers.

IMPORTANT

Virtual IP of VRRP is derived from vrrpAssoIpAddrRowStatus, which is part of indexes in the vrrpAssoIpAddrTable. If the vrrpAssoIpAddrTable does not contain values in the MIB, then VRRP group will not be created.

IMPORTANT

If ipNetToMediaTable does not contain values with current Virtual IP for that VRRP group, then relationships like HostedBy, LayeredOver, ConnectedVia, Underlying, ConcreteDependency_Dependent will not be created.

Basic VRRP configuration

Figure 1 on page 6 illustrates the basic VRRP configuration.

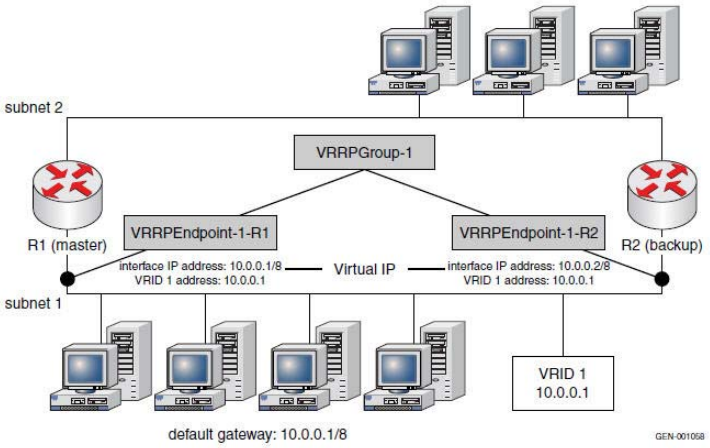

Figure 1 **Basic VRRP configuration**

The VRRP configuration uses a single Virtual Router Identifier (VRID 1). Router R1 is the address owner and serves as the master router and router R2 serves as the backup router. The four end-hosts on subnet 1 are configured to use 10.0.0.1/8 as the default router. IP address 10.0.0.1 is associated with VRID 1.

In this example, if R1 becomes unavailable, R2 takes over VRID 1 and its associated IP addresses. Packets sent to IP destinations outside the 10.x.x.x subnet that use 10.0.0.1 as the router are then forwarded by R2. Even though R2 assumes the forwarding responsibilities of R1, it may or may not process any packet with destination address (DA) 10.0.0.1, depending on the accept-data configuration. When R1 becomes active again, it takes over as the master router and R2 reverts as the backup router.

Enable VRRP support for IP Management Suite 7.0.4 in Service Assurance Management Suite 8.1

By default, VRRPGroup instances are not imported in Service Assurance Management Suite from IP 7.0.4.

To enable the import of VRRPGroup in SAM, add the following lines in the dxa configuration files and reconfigure the corresponding InCharge Domain.

```
class   VRRPGroup                    VRRPGroup
attr    DisplayName
attr    Description
attr    VirtualIP
attr    VirtualRouterID
rel     ComposedOf
rel     PartOf
rel     LayeredOver
sub     VRRPEndpoint::.*::SwitchOver/e
sub     VRRPGroup::.*::SwitchOverFailed/e
#VRRP
sev VRRPGroup          SwitchOverFailed     Availability   1
sev VRRPEndpoint       SwitchOver           Availability   3
```

The dxa configuration files to modify are:

- local/conf/ics/dxa-conn.conf
- local/conf/ics/dxa-conn-per.conf

If Aggregate SAM has VRRPGroup instances, you must add the following lines in the local/conf/dxa-sam.conf file in Presentation SAM to import the VRRPGroup instances. Note that VRRPGroup is not available in SAM 7.2 and SAM 8.0.

class VRRPGroup VRRPGroup

attr DisplayName

attr Description

attr VirtualIP

attr VirtualRouterID

rel ComposedOf

rel PartOf

rel LayeredOver

Containment map changes in SAM

Due to containment map changes in SAM (smarts/conf/maps/MAP-CONTAINMENT.import), you need to also modify two entries in the MAP-CONTAINMENT.import file. This is because SAM now requires the "type" of the domain to be specified in the configuration entries.

Using the sm_edit utility, modify the $SM_HOME/conf/maps/MAP-CONTAINMENT.import file to ensure that the following line matches with what is in the import file: "INCHARGE-SA | INCHARGE-AM | INCHARGE-AM-PM | INCHARGE-PM | IP-Perspective"

Example

```
MapViews += {
"VRRP Systems",
"VRRPGroup",
"LayeredOver",
"UnitaryComputerSystem",
"DisplayName",
"Vendor",
"Model",
"Description",
"IsUnresponsive",
"Location",
```

```
"PrimaryOwnerName",
"PrimaryOwnerContact",
"INCHARGE-SA|INCHARGE-AM|INCHARGE-AM-PM|INCHARGE-PM|IP-Perspective"
}
MapViews += {
"VRRP Interfaces",
"VRRPGroup",
"ComposedOf",
"VRRPEndpoint",
"DisplayName",
"Priority",
"State",
"InterfaceName",
"InterfaceNumber",
"InterfaceAdminStatus",
"InterfaceOperStatus",
"SystemName",
"INCHARGE-SA|INCHARGE-AM|INCHARGE-AM-PM|INCHARGE-PM|IP-Perspective"
}
```

IMPORTANT

After making the required changes in the MAP-CONTAINMENT.import file, save and close the file, and then restart the SAM server.

Any errors regarding duplicate entries can be ignored.

Discovery and monitoring of VRRP-enabled routers

Figure 2 on page 10 illustrates an example of VRRP monitoring in the Domain Manager Administration Console.

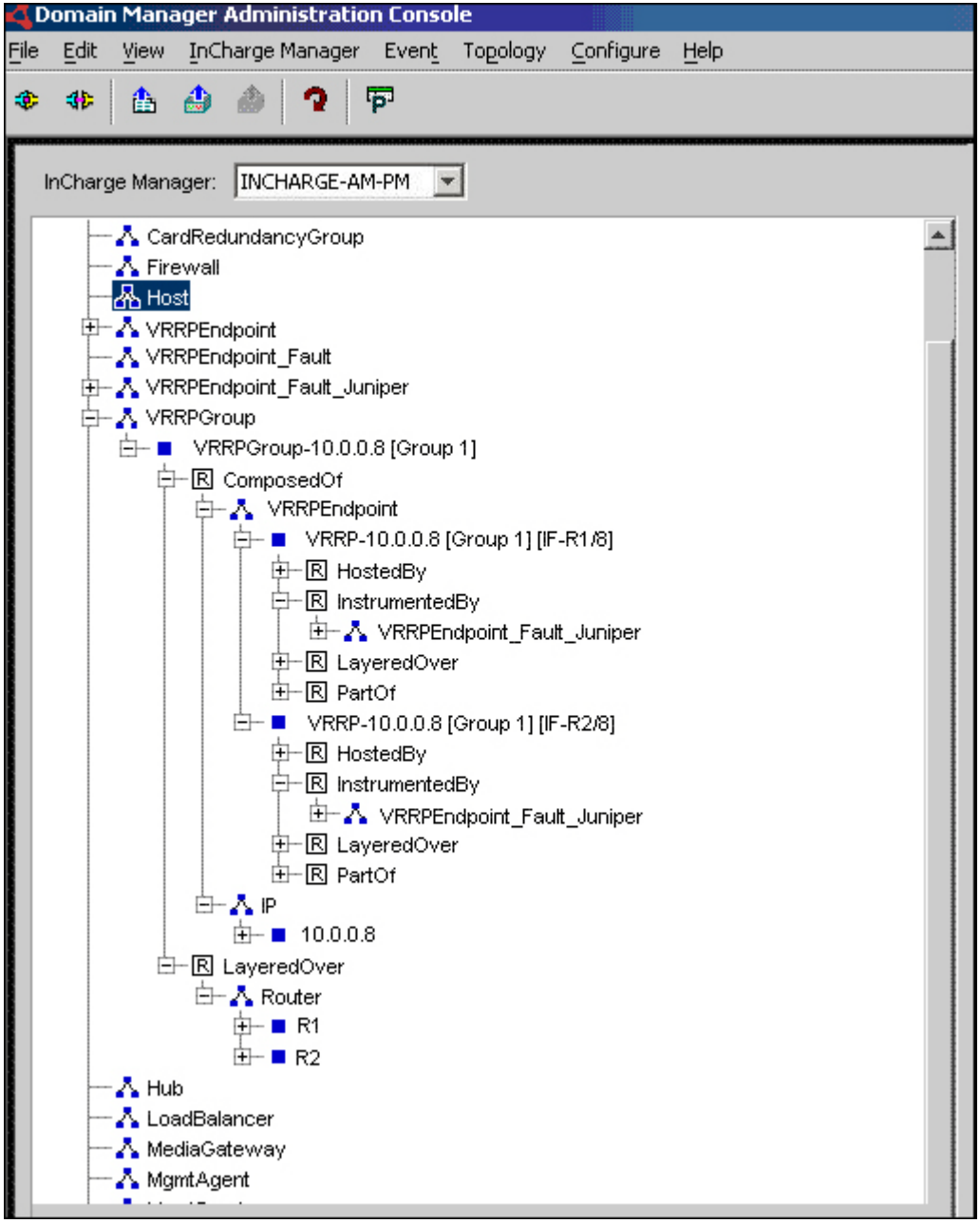

Figure 2 VRRP Discovery and monitoring

VRRP events

Table 1 on page 11 lists the VRRP events and their descriptions.

Table 1 VRRP Events

VRRP Event	Description
SwitchOver	A VRRP endpoint event. The status of the VRRP endpoint has changed since the last polling.
AllComponentsDown	A VRRP group event. Indicates that all of the components in the redundancy group are down.
AtRisk	A VRRP group event. Indicates that the number of functioning components is less than or equal to the threshold.
ReducedRedundancy	A VRRP group event. Indicates at least one component is not functioning. The total number of functioning components is above the threshold.
SwitchOverFailed	A VRRP group event. Indicates that the switchover failed and no active device is available.

VRRP support

The key features of VRRP support in Ionix IP Management Suite are as follows:

- IP 7.0.4 release supports only standard VRRP implementation for IPv4 protocol.
- The MIBs for VRRP follow RFC 2787.
- VRRP-supported vendors:
  - Juniper Routers on JunOS 9.1 and higher, Juniper JunOSE
  - Nortel Routers

Support for Link Layer Discovery Protocol (LLDP)

The Link Layer Discovery Protocol (LLDP) is a neighbor discovery protocol used by network devices to advertise their identity, capabilities, and interconnections on an IEEE 802 LAN network. LLDP is vendor-neutral. The protocol defines a standard way for

Ethernet devices to advertise information about themselves to their network neighbors, and store the information they discover from other devices.

LLDP operates above the MAC service layer and can be used in any networking device that implements a MAC service. Information gathered with LLDP is stored in the device in a standard management information database (MIB) and can be queried with the Simple Network Management Protocol (SNMP). For example, a LAN switch and a router advertise chassis/port IDs and system descriptions to each other. The devices store the information they learn about each other in local MIB databases accessible through SNMP. The network management system retrieves the data stored by each device and builds a network topology map.

Frame structure

LLDP supports a set of attributes that it uses to discover neighboring devices. These attributes contain type, length, and value descriptions and are referred to as TLVs. LLDP frames are sent by each device on each port at a fixed frequency. A frame contains a Link Layer Discovery Protocol Data Unit (LLDPDU) which is a set of type-length-value (TLV) structures. LLDP supported devices use TLVs to send to and receive information from their immediate neighbors.

The LLDP frame starts with the following mandatory TLVs:

- Chassis ID
- Port ID
- Time to live (TTL)

The LLDP frame ends with a special TLV named “End of LLDPDU”. Refer the IEEE 802.1AB specification for a description of all the TLV types.

Information that may be retrieved includes:

- System name and description
- Port name and description
- VLAN ID
- IP management address
- System capabilities (switching, routing, and so on)
- MAC/PHY information

- Link aggregation

Transmission and reception

The transmission and reception of LLDPDUs are enabled when LLDP is enabled on a port. The LLDP agent operates in any of the following modes:

- Transmit-only mode
- Receive-only mode
- Transmit-and-receive mode

When LLDP transmission is enabled, the LLDP agent advertises information to neighbors at regular, user-configured intervals. When LLDP reception is enabled on a port, the LLDP agent receives advertised information from remote neighboring devices and stores this data in the remote systems' MIB.

Note: On Cisco devices, if both LLDP and the Cisco Discovery Protocol (CDP) are enabled, connections may be created by using LLDP or CDP. Further, if LLDP is enabled on a device, and CDP is enabled on a different device, connection is created only as a bridge. LLDP must be enabled on both devices to create the LLDP connection.

LLDP configuration

Table 2 on page 13 shows the default LLDP configuration. To change the default settings, use the LLDP global configuration and LLDP interface configuration commands.

Table 2 Default LLDP configuration

Feature	Default setting
LLDP global state	Enabled
LLDP holdtime (before discarding)	120 seconds
LLDP timer (packet update frequency)	30 seconds
LLDP reinitialization delay	2 seconds
LLDP tlv-select	Enabled to send and receive all TLVs
LLDP interface state	Enabled
LLDP receive	Enabled
LLDP transmit	Enabled

You can configure the frequency of LLDP updates, the amount of time to hold the information before discarding it, and the initialization delay time. You can also select the LLDP TLVs to be sent and received.

Implementation

Table 3 on page 14 lists various connection scenarios when LLDP is enabled or disabled between two devices A and B.

Table 3 LLDP Implementation

System B		LLDP enabled		LLDP not enabled
System A		Full MIB support for LLDP	LLDP MIB not supported	
LLDP enabled	Full MIB support for LLDP	Create the connection by using information from either system A or system B	Create the connection using information only from system A	No connection
	LLDP MIB not supported	Create the connection by using information only from system B	No connection	
LLDP not enabled		No connection		

Configuration impact

Changes are made to the following configuration files:

- DISCOVERY_CISCO.import
- DISCOVERY_GENERIC.import
- DISCOVERY_JUNIPER.import
- oid2type_Cisco.conf
- oid2type_Juniper.conf
- oid2type_force10.conf

Changes are made to the following ASL files:

- discovery-init.asl
- ic-lldp.asl
- ic-lldp-post-processor.asl

Devices supported

- Cisco - CAT2960
- Juniper - EX4200 (JUNOS 9.2R3)

- Force 10 - E600

LLDP supports multiple physical connections.

Installation impact

Make files are changed in order to incorporate the following new ASL files:

- ic-lldp-post-processor.asl
- ic-lldp.asl

Connectivity relationship

Figure 3 on page 15 shows an LLDP connection.

In the example, the LLDP connection is created between two switches under the TrunkCable class. The Description attribute is set to LLDP.

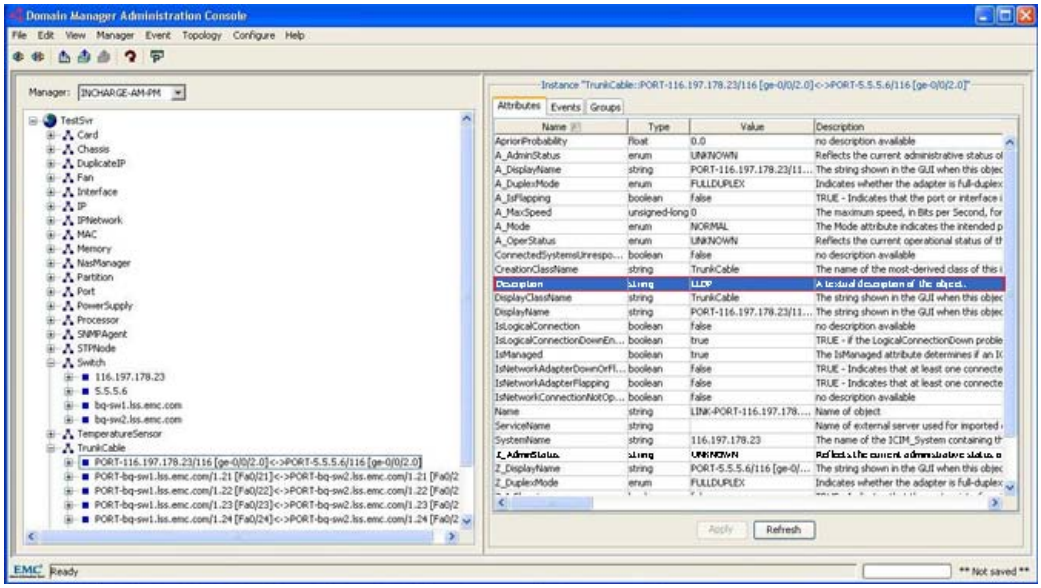

Figure 3 **LLDP connection**

Impact on discovery

A new probe named LLDP probe has been added.

Post-processing impact

The IP Availability Manager discovers LLDP-enabled devices, and the global data structure is loaded with the connection details. This data structure is processed during the post-processing phase in the IP Availability Manager. The IP Availability Manager runs the ic-lldp-post-processor.asl file to do the post-processing.

Trunk cable connections are created in the IP Availability Manager which processes the global data structure based on data gathered during discovery.

MIBs polled

LLDP MIB — The LLDP supported devices are listed in the following configuration files:

- oid2type_Cisco.conf
- oid2type_Juniper.conf
- oid2type_force10.conf

Based on whether the device supports LLDP, the LLDP SNMP OIDs are probed.

Thresholds for individual devices and filesystem instances

This section describes the monitoring of sensors and file system instances.

- "Thresholds for temperature and voltage sensors" on page 16
- "Filesystem management and thresholds" on page 22
- "Impact on an upgrade installation" on page 27

Thresholds for temperature and voltage sensors

In the earlier version, a single threshold value is set for all voltage and temperature sensors within a device using the System Resource group. The disadvantage is that voltage and temperature sensors within a device cannot be monitored individually. In the 7.0.4 release, you can configure separate thresholds for different voltage and temperature sensors in the same device.

By default, the following are available:

- Groups called VoltageSensors and TemperatureSensors.
- These groups are empty and do not match any temperature or voltage sensors.
- All the sensors in 7.0.4 retain the same monitoring as in 7.0.3.
- The thresholds defined in the System Resource Group serve as the default and may be overwritten by values in one of the new groups.

If a temperature sensor or voltage sensor belongs to a particular group, it inherits the group's threshold setting. In case it does not belong to any group, the thresholds in the System Resource group will apply.

To create separate thresholds for different voltage and temperature sensors (or a group of sensors), you must create groups by using appropriate matching criteria.

The threshold behavior for temperature sensors is different. "Discovery of thresholds for temperature sensors using EntitySensor MIB" on page 20 provides more details.

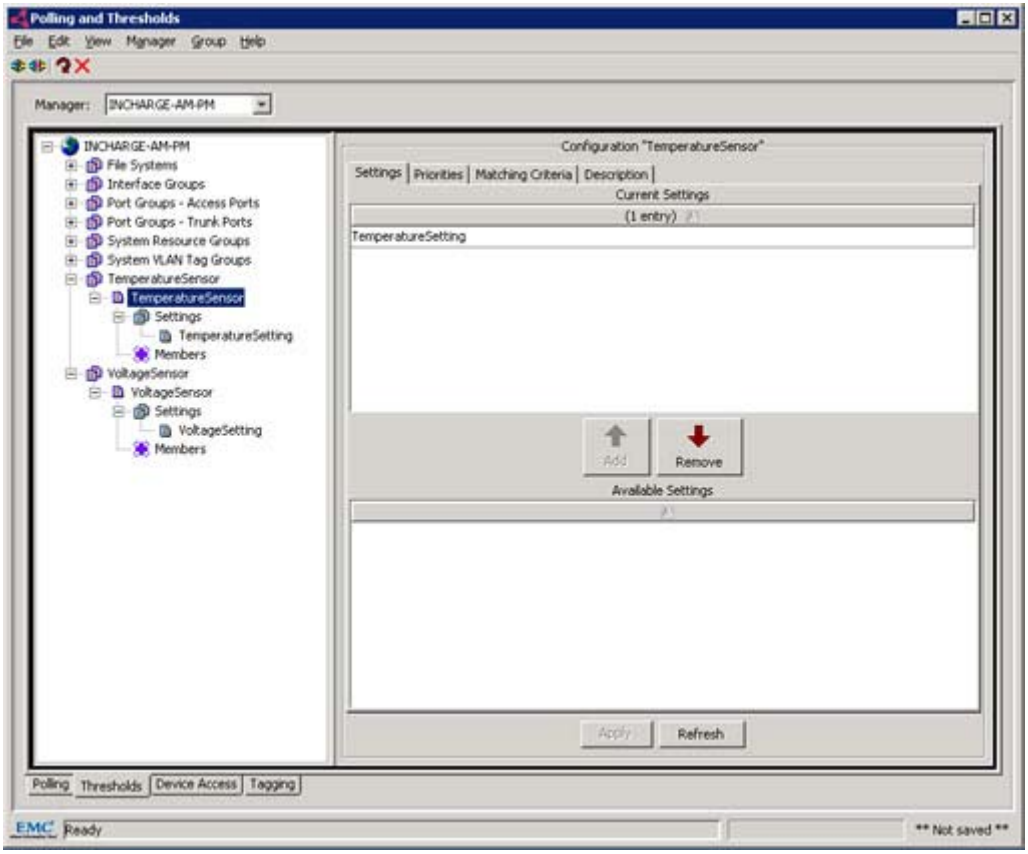

Figure 4 Groups for temperature and voltage sensors

The following sections cover more details regarding thresholds and events for the sensors:

- "Default thresholds and events" on page 19
- "Discovery of thresholds for temperature sensors using EntitySensor MIB" on page 20
- "Temperature sensor threshold attributes explained" on page 20

Default thresholds and events

Table 4 on page 19 gives the default threshold setting and events generated for temperature and voltage sensors.

Table 4 Events and thresholds for temperature and voltage sensors

Event	Utilization threshold	Description of threshold	Default value	Condition
OutOfRange	RelativeTemperature	How close the current temperature value can be to the value that triggers an emergency shutdown, expressed as a percentage of the emergency shutdown value.	10% Range: 0 to 100%	If the shutdown temperature is 50 degrees C and the RelativeTemperatureThreshold is 10%, the OutOfRange event is notified if the temperature exceeds 45 degrees C.
OutOfRange	TemperatureHigh Threshold	High threshold value of the temperature sensor, in degrees C.	50 degrees C Range: 0 to 100 degrees C	This event is generated when the temperature exceeds the configured threshold value.
OutOfRange	RelativeVoltage Threshold	How close the current voltage value can be to the value that triggers an emergency shutdown, expressed as a percentage of the emergency shutdown value.	0 % Range: 0 to 5%	If the shutdown value is +30V, and the RelativeVoltageThreshold is 10%, the OutOfRange event is notified if the voltage exceeds +27V.

Table 4 Events and thresholds for temperature and voltage sensors

Event	Utilization threshold	Description of threshold	Default value	Condition
OutOfRange	VoltageSensorHigh Threshold	High threshold value of the voltage sensor test point, in volts.	5 volts 0 to 100 volts	This event is generated when the voltage exceeds the configured threshold value.
OutOfRange	VoltageSensorLow Threshold	Low threshold value of the voltage sensor test point, in volts.	1 volt 0 to 100 volts	This event is generated when the voltage exceeds the configured threshold value.
StateNotNormal	N/A	N/A	N/A	Indicates that the temperature or voltage sensor test point for this system is in the CRITICAL or WARNING state. The sensor state can be in one of four states: NORMAL, WARNING, CRITICAL, or SHUTDOWN.

Discovery of thresholds for temperature sensors using EntitySensor MIB

Temperature sensor thresholds can be set during discovery for devices that are certified in the IP Management Suite using **EntitySensor MIB** for **Environment**. To verify if threshold values are discovered from the MIB, you must enable **MetaClass** and verify the **Instrumentation Class** (TemperatureSensor_Fault_CiscoEntityFRU) of the specific temperature sensor object.

There are two possibilities for setting the threshold value of the temperature sensors:

- If the threshold values returned by the agent are greater than 0, discovery reads in the threshold values from the EntitySensor MIB and automatically sets the thresholds in the instrumentation object to the values from the agent.
- If the device agent does not return a positive value for the threshold reading, then the threshold value falls back to the default setting defined in either the TemperatureSensor group or in the System Resource group.

Temperature sensor threshold attributes explained

The following attributes are explained:

- MajorAlarmThreshold
- MibEntSensorThreshold
- CurrentValue

- RelativeTemperatureThreshold
- TemperatureHighThreshold
- HighThreshold

MajorAlarmThreshold

The attribute **MajorAlarmThreshold** is a value directly polled from the MIB. Temperature sensors are created based on **entPhysicalIndex** from the entPhysicalClass OID (1.3.6.1.2.1.47.1.1.1.1.5) having value of sensor(8). For each **entPhysicalIndex**, the **entSensorThresholdIndex** having a value of minor(10) from the entSensorThresholdSeverity OID (1.3.6.1.4.1.9.9.91.1.2.1.1.2) is selected. This is used to obtain the corresponding threshold value from the entSensorThresholdValue OID (1.3.6.1.4.1.9.9.91.1.2.1.1.4). Threshold value OIDs are part of the CISCO-ENTITY-SENSOR-MIB.

MibEntSensorThreshold

The attribute **MibEntSensorThreshold** is a value after computing Precision from **entSensorPrecision**. The precision is obtained from Entity MIB's **entSensorPrecision** attribute OID (1.3.6.1.4.1.9.9.91.1.1.1.1.3). The **entSensorPrecision** indicates the number of decimal places of precision in fixed-point sensor values.

- If the **entSensorPrecision** is 1, the **entSensorValue** is divided by 10.
- If the **entSensorPrecision** is 2, the **entSensorValue** is divided by 100.
- If the **entSensorPrecision** is 3, the **entSensorValue** is divided by 1000.
- If the **entSensorPrecision** is zero, the **MibEntSensorThreshold** will be zero.

CurrentValue

The attribute **CurrentValue** is a polled value from the MIB attribute **entSensorValue** after considering the **entSensorPrecision** attribute value. The **entSensorPrecision** indicates the number of decimal places of precision in fixed-point sensor values. The **entSensorPrecision** indicates the number of decimal places of precision in fixed-point sensor values.

- If the **entSensorPrecision** is 1, the **entSensorValue** is divided by 10.
- If the **entSensorPrecision** is 2, the **entSensorValue** is divided by 100.
- If the **entSensorPrecision** is 3, the **entSensorValue** is divided by 1000.
- If the **entSensorPrecision** is zero, the **entSensorValue** is considered as such for **CurrentValue**.

RelativeTemperatureThreshold

The attribute **RelativeTemperatureThreshold** is from the user specified Threshold Group. It indicates how close the current temperature value can be to the value that triggers an emergency shutdown, expressed as a percentage of the emergency shutdown value. For example, if the shutdown temperature is 50 degrees C and the **RelativeTemperatureThreshold** is 10%, the **OutOfRange** event is notified if the temperature exceeds 45 degrees C.

TemperatureHighThreshold

The attribute **TemperatureHighThreshold** value is populated from the Threshold Group. Though the **TemperatureHighThreshold** value is populated, it is considered only for the computation of **HighThreshold** when the **MibEntSensorThreshold** value is negative.

HighThreshold

The value for the attribute **HighThreshold** is computed from the **MibEntSensorThreshold** attribute's value if it is greater than zero. If the value of **MibEntSensorThreshold is negative, then the value is computed** from attribute **TemperatureHighThreshold**'s value.

Filesystem management and thresholds

Filesystem is treated as a logical network object. The File System Management functionality allows you to define and configure thresholds for filesystem space utilization.

In the earlier version, a single threshold value is set for all filesystems using the System Resource group. The disadvantage is that each filesystem cannot be monitored individually.

The following enhancements are added:

- Ability to define thresholds for each filesystem instance
- Ability to manage and unmanage filesystems

The following sections describe the enhancement:

- "Define thresholds for individual filesystem instances" on page 23
- "Events and thresholds for filesystems" on page 24
- "Managing or unmanaging filesystems" on page 27

Define thresholds for individual filesystem instances

In the 7.0.4 release, you can configure thresholds for individual filesystem instances. A default group called FileSystem is available.

The utilization thresholds can be configured for each filesystem instance. As a result, a host with multiple filesystems can have different thresholds defined individually for each filesystem instance. Each filesystem instance is monitored individually.

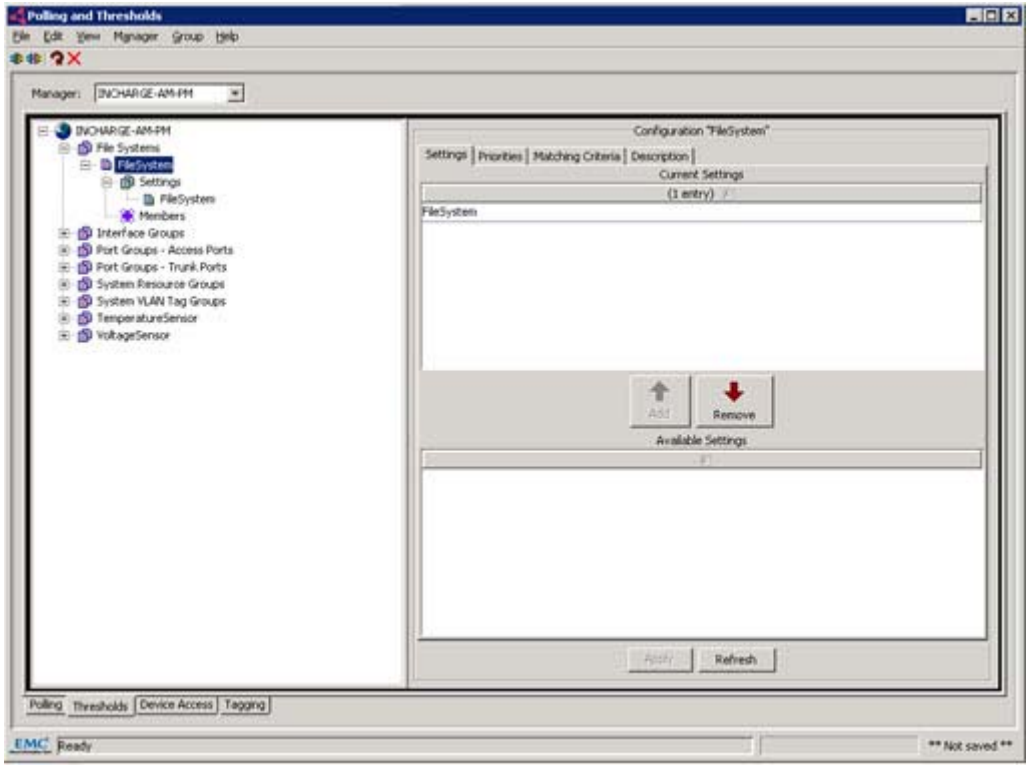

Figure 5 **Groups for filesystem instances**

- You can configure two types of utilization thresholds (in percentage) for each filesystem instance. They are *MaxUtilizationPct* and *ModerateUtilizationPct*.
- The events generated are *HighUtilization* and *ModerateUtilization*.

Note: The *ModerateUtilization* alert is new and available only in IP 7.0.4.

Events and thresholds for filesystems

Table 5 on page 24 provides the events and thresholds along with their description.

Table 5 Events and thresholds for filesystems

Events	Utilization threshold	Description of threshold	Default value	Condition
HighUtilization **Note:** Severity level: Major	MaxUtilizationPct	The percentage of total size currently in use.	95% **Note:** User can change this value for each filesystem instance.	This event is generated when the utilization threshold exceeds the configured threshold value. **Note:** This threshold has greater priority over the ModerateUtilization event.
ModerateUtilization **Note:** Severity level: Minor	ModerateUtilizationPct	Moderate threshold for percentage of total size currently in use.	80% **Note:** User can change this value for each filesystem instance.	This event is generated when the utilization threshold exceeds the configured threshold value.
LowAvailableSpace **Note:** Security level: Minor	MinAvailableSpace	The available space is less than the minimum available space.	1024 **Note:** User can change this value for each filesystem instance.	This event is generated when the utilization threshold exceeds the configured threshold value.

The thresholds defined in the System Resource Group serve as the default and may be overwritten by values in one of the new FileSystem groups. If a filesystem instance belongs to a particular

group, it inherits the group's threshold settings. In case it does not belong to any group, the thresholds in the System Resource group that the device belongs to will apply.

When new filesystem groups are created, they do not have any matching criteria and are empty. You can add new matching criteria and configure the thresholds for each filesystem group. This can be done in the **Matching Criteria** tab for the selected filesystem group in the **Polling and Thresholds** window.

Each filesystem group is placed in the order of priority in the **Polling and Thresholds** window. You can change the priority from the Priority tab. The matching of the filesystem instances begin from the highest priority group and continues in the order of priority. A filesystem instance that matches a group is not considered for matching with the remaining groups.

Sample filesystem groups and matching criteria

Table 6 on page 26 lists sample filesystem groups along with their matching criteria. You can use these as a guide to create filesystem groups manually.

Table 6 Sample filesystem groups and matching criteria

Filesystem group	Description	Matching Criteria
Whole Drive File Systems	Configures all Windows drive filesystem instances that match the criteria.	The default matching criteria is the Filesystem attribute "Root" to match the value *:*. All filesystem instances with the "Root" attribute value beginning with any number of characters, followed by a ":" (colon), followed by "\\" and then followed by any number characters will fall in this group.
OS Only File Systems	Configures all Linux filesystem instances that match the criteria.	The default matching criteria is the Filesystem attribute "Root" to match the value /. All filesystem instances with the "Root" attribute value as "/" (single forward slash) will fall in this group.
Writable File Systems	Configures all Linux filesystem instances that match the criteria.	The default matching criteria is the Filesystem attribute "Root" to match the value "/var". All filesystem instances with the "Root" attribute value as "/var" will fall under this group.
Temporary File Systems	Configures all Linux filesystem instances that match the criteria.	The default matching criteria is the Filesystem attribute "Root" to match the value "/temp". All filesystem instances with the "Root" attribute value as "/temp" will fall under this group.
Non Critical File Systems	Configures all Linux filesystem instances that match the criteria.	No default matching criteria provided, and will match all the filesystem instances.
Unclassified File Systems	Configures all Linux filesystem instances that match the criteria.	No default matching criteria provided, and will match all the filesystem instances.

Managing or unmanaging filesystems

You can manage or unmanage an individual filesystem instance. When a filesystem is rendered managed, that filesystem instance is monitored. On the other hand, when a filesystem instance is rendered unmanaged, that filesystem instance is not monitored.

Follow these steps to manage or unmanage a filesystem instance:

1. In the Domain Manager Administration Console, select the appropriate server from the **Manager** drop-down list.
2. Right-click on the filesystem instance and select **Manage** or **Unmanage,** as applicable.
3. If you have chosen to manage a filesystem instance, click **Reconfigure**.
   This renders the filesystem to be managed.

Table 7 on page 27 describes the attribute for a filesystem instance.

Table 7 Attribute of Filesystem

Attribute	Description	Allowed values
IsManaged	Determines if a filesystem instance should be monitored by the management system. An unmanaged object does not have any associated instrumentation. This attribute is read-only.	Boolean: True or False Default: True

Impact on an upgrade installation

If you are upgrading from an earlier version of the IP Management Suite, start the server with the repository file (.rps) from the old installation. All customization settings that you might have made in the old version are retained and available. The new threshold groups are also available in the server.

New directory to backup user-modified files during an upgrade

In the previous versions of the product, the installer renamed and saved all the customized files under <BASEDIR>/smarts/local. In the 7.0.4 version, the installer moves all the old customizations into a folder at this location: <BASEDIR>/smarts/.local.bkp.7.0.X. This is an efficient way of separating the old customizations.

CAUTION

Do not copy the old configuration files from the backup directory to the upgraded installation.

You can manually merge those customizations that you wish to retain from this location to the local folder of the 7.0.4 installation. Use the sm_edit utility to make suitable changes.

Changes in creation of Card Redundancy groups for Cisco devices

CQ 571608

In the 7.0.4 release, a new condition check for MIB value cRFStatusPrimaryMode to create cards for Cisco devices is introduced. This check did not exist in the previous version of the IP Management Suite.

IP 7.0.4 will discover less cards when compared to the same topology discovered in pre IP 7.0.4 domains. Cards are created only if the corresponding card index's cRFStatusPrimaryMode has a value of 1 (TRUE).

New groups added for devices of type MediaGateway for performance polling

CQ 571603

To enable configuration of specific Polling settings for devices of type MediaGateway, a new group named as MediaGateways is added under Polling groups. The MediaGateways group has default settings similar to the existing Router and Switch groups.

Also, under Threshold Settings -> SystemResource Groups, a new group named as MediaGateways is added. This group has default Threshold settings similar to the existing Switch | Router type.

The MediaGateways group is not observed if you are restoring the domain from a pre 7.0.4 RPS file. In this case, manually create the MediaGateways group.

If you upgrade from an earlier version of IP Management Suite, that is, from 7.0.1, 7.0.2, or 7.0.3, but start a new domain that did not have a pre 7.0.4 RPS, the MediaGateways group will be created.

This is done to enable users to migrate the existing settings related to MediaGateways to the new servers.

New flag RetainStaleConnections introduced to retain stale connections in the topology

CQ 502823 / CQ 572014

When a port is down, the TrunkCable and Cable down alarm is triggered. However, if a rediscovery is performed on the topology, the IP Manager determines non-existence of the connections based on Cisco Discovery Protocol (CDP) and Address Resolution Protocol (ARP) calculations and deletes the TrunkCable and Cable connections from the topology. This switches off the alarm and the state of the port is changed from Managed to Unmanaged. To retain the TrunkCable and Cable connections in the topology along with the alarm, and the state of the port as Managed, set the flag *RetainStaleConnections* to TRUE, and reload the tpmgr-param.conf file using the following command:

```
./sm_tpmgr.exe -s <servername>
--load-conf=tpmgr-param.conf -b <host:port>
```

In connection with the above, the following ASL error may be observed:

```
[25-Oct-2010 11:32:15 PM+562ms Pacific Daylight Time]
t@4196 ProbeCompletedRunner
ASL-W-ERROR_RULE_SOURCE-While executing rule set
'\IP\704\IP\smarts\rules\discovery\ic-post-cleanup.asl'
ASL-ERROR_ACTION-While executing action at:
ASL-CALL_STACK_RULE-   RuleName: __INIT__, Line: 18
ASL-ERROR_INIT_ACTION-While executing initialization
actions
ASL-ERROR_STRING_AS_BOOLEAN-Attempted to use a string
value as a boolean value
```

The error has no impact on the functionality and can be ignored.

Product enhancements in Service Pack 3

The following enhancements were released in IP Management Suite 7.0 Service Pack 3:

- "Support for new device certifications" on page 30
- "Improved performance through reduced discovery time" on page 30
- "New setting for Cisco free memory thresholds" on page 31
- "New attributes for network Containment views" on page 34

- "FallbackInterfaceMonitoringToMIB2 configuration parameter" on page 35

Support for new device certifications

Service Pack 3 adds support for more than 120 new device certifications. The certifications extend both the functionality of the IP Management Suite products and the cross-dependency of other EMC Smarts products such as EMC Smarts MPLS Manager, EMC Smarts Network Protocol Manager, and EMC Smarts VoIP Availability Manager.

The new certifications have been added to the Excel (xls) and HTML (html) versions of the *EMC Smarts IP Certification Matrix for 7.0.3* device certification document. In the Excel version of the *EMC Smarts IP Certification Matrix for 7.0.3*, the new certifications are highlighted with a blue background.

Improved performance through reduced discovery time

The following optimization techniques have been applied to many of the discovery-related Adapter Scripting Language (ASL) files in Service Pack 3 to significantly reduce the IP Manager discovery time:

- "Replace "if—else" statements with "switch" statements" on page 30
- "Implement early loop breaking" on page 30
- "Reduce repeated SNMP Get operations on devices" on page 30

Replace "if—else" statements with "switch" statements

In the if() statement, if the last case is required, all previous cases are tested first. The switch statement eliminates this extra work.

Implement early loop breaking

Processing the entirety of a loop is often not necessary. As an example, when the software is searching an array for a particular item, it is always good practice to implement early loop breaking so that the software breaks out of the loop as soon as the item is found.

Reduce repeated SNMP Get operations on devices

Of all the optimization techniques applied to Service Pack 3, the reducing of repeated SNMP Get operations on devices has proven to have the most impact on reducing the IP Manager discovery time.

As explanation, previous to Service Pack 3, different rules in the IP Manager ASL files did Get operations on the ifTable MIBs again and again to retrieve the same interface information. (A device's ifTable MIB can contain thousands of entries.) Accessing the ifTable MIBs again and again is costly in terms of CPU time.

With Service Pack 3, often-used interface information is stored in a global table, and the rules in the ASL files have been changed to access the information in the global table. The new global table and the modified interface-data-retrieval algorithm have reduced IP Manager discovery time significantly.

New setting for Cisco free memory thresholds

A new polling and thresholds setting named "Cisco Processor and Memory" enables users to set the free memory thresholds for two different memory types:

- Fast memory
- Non-volatile memory (NVRAM)

In releases before Service Pack 3, the free memory threshold of instrumentation Memory objects was controlled by a single parameter named FreeMemoryThreshold in the "Memory and Processor" setting.

Note: The Cisco Processor and Memory setting is intended for Cisco devices only.

The Cisco Processor and Memory setting is not the default setting for any threshold group but is available to any performance System Resource Group shown in Table 8 on page 32. The matching-criteria target class for System Resource Groups is UnitaryComputerSystem.

Table 8 Performance System Resource Groups

Polling group	Matching criteria
Switches	UnitaryComputerSystem attributes: • Type = Switch
Routers	UnitaryComputerSystem attributes: • Type = Router
Hubs and Bridges	UnitaryComputerSystem attributes: • Type = Hub or Bridge
Other Systems	UnitaryComputerSystem attributes: • No attributes

When a user adds the Cisco Processor and Memory setting to a System Resource Group, the user also adds the "Vendor=Cisco" matching criteria to the group, to limit the group's membership to just Cisco devices. "Vendor" (like "Type") is one of the many attributes of the UnitaryComputerSystem class.

Table 9 on page 32 lists the Cisco Processor and Memory threshold setting parameters.

Table 9 Default values for the Cisco Processor and Memory threshold setting

Parameter	Default value	Description
FastMemoryThreshold	15%	Sets the lower threshold for the acceptable amount of free Fast memory as measured by the ratio of free Fast memory to the total Fast memory.
NvramMemoryThreshold	15%	Sets the lower threshold for the acceptable amount of free NVRAM memory as measured by the ratio of free NVRAM memory to the total NVRAM memory.

The following two procedures provide instructions for adding and removing the Cisco Processor and Memory setting and for adding and removing the Vendor=Cisco matching criteria.

Adding the Cisco Processor and Memory setting and the Vendor=Cisco matching criteria

1. In a **Domain Manager Administration Console** attached to the IP Manager, choose **Configure > Polling and Thresholds** to open the **Polling and Thresholds Console.**

   The example display in Figure 6 on page 33 shows the **Cisco Processor and Memory** setting in the **Settings** tab of a **Routers** threshold group, available through the **Thresholds** tab of a **Polling and Thresholds Console** attached to an IP Performance Manager. In the display, the **Cisco Processor and Memory** setting is shown as removed from the group (the default).

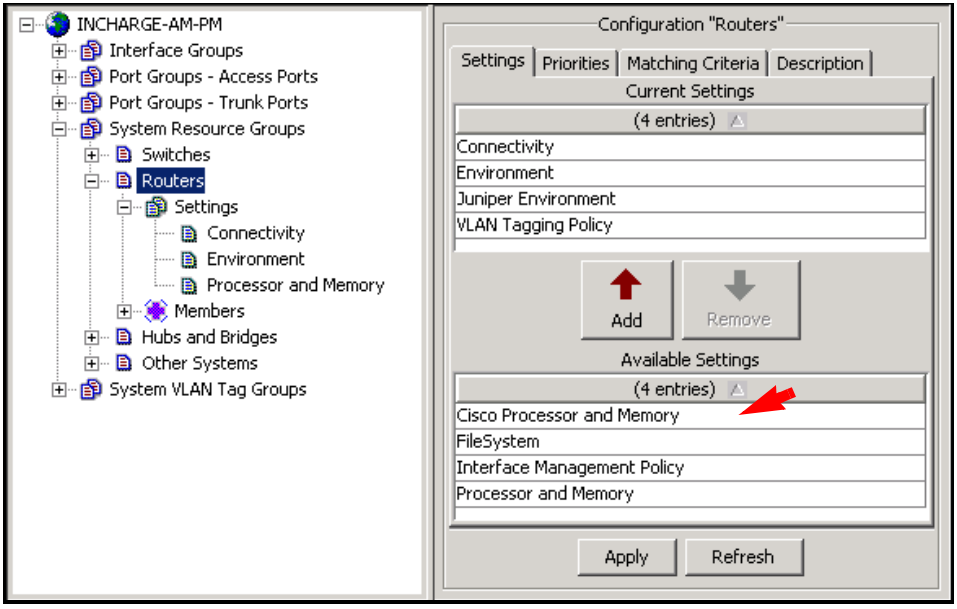

Figure 6 **Cisco Processor and Memory setting in the Routers threshold group**

2. In the **Settings** tab, select the **Cisco Processor and Memory** setting in the **Available Settings** list.
3. Click **Add** to move the setting to the **Current Settings** list.
4. Click **Apply** to save your changes.
5. Click **Matching Criteria** to display the **Matching Criteria** tab.

6. In the **Disabled Criteria** area of the **Matching Criteria** tab, select the **Vendor** criterion.
7. Click **Enable** to activate the criterion, which moves it to the top of the **Matching Criteria** tab.
8. Type **Cisco** in the **Value** matching pattern field.
9. Click **Apply** to save your changes.
10. Click the **Reconfigure** toolbar button to make your changes take effect.

Removing the Cisco Processor and Memory setting and the Vendor=Cisco matching criteria

1. In the **Settings** tab, select the **Cisco Processor and Memory** setting in the **Current Settings** list.
2. Click **Remove** to move the setting to the **Available Settings** list.
3. Click **Apply** to save your changes.
4. Click **Matching Criteria** to display the **Matching Criteria** tab.
5. In the **Enabled Criteria** area of the **Matching Criteria** tab, select the **Vendor** criterion.
6. Click **Disable** to deactivate the criterion, which moves it to the bottom of the **Matching Criteria** tab.
7. Click **Apply** to save your changes.
8. Click the **Reconfigure** toolbar button to make your changes take effect.

New attributes for network Containment views

With the Global Console attached to the Global Manager, users can view a network object's Containment view in a dialog box that organizes the information for the object into tab pages and tables. The intent of the Containment view is to allow users to examine detailed component topology of an individual object.

The attributes identified as new in Table 10 on page 35 have been added to the Memory, Cards, and Network Adapters tabs of Containment views for Service Pack 3.

Table 10 New attributes in Memory, Cards, and Network Adapters tabs

Network tab name	Attributes in tab page
Memory (Available only if IP Performance Manager or IP Server Performance Manager is in the deployment)	Description **(new)** DisplayName TotalMemory FreeMemory BufferMissPct BufferUtilizationPct LargestFreeBuffer TotalBufferAllocationFailures
Cards	Description **(new)** DisplayName Status
Network Adapters	DisplayName AdminStatus OperStatus Type **(new)** Name **(new)** Mode CurrentUtilization PeerSystemName

FallbackInterfaceMonitoringToMIB2 configuration parameter

In releases before Service Pack 3, the IP Manager did not monitor interface performance for a device when the following two conditions were both in effect:

- Interfaces had maximum speed (MaxSpeed) greater than 20 megabytes (MB).
- No 64-bit counters were available in the device's MIB.

Available with Service Pack 3 is a new parameter to control whether the IP Manager monitors interfaces under these circumstances. The parameter is named FallbackInterfaceMonitoringToMIB2 and is contained in the tpmgr-param.conf file.

You can assign the following values to the parameter:

- A value of TRUE forces the IP Manager to use 32-bit counters to monitor greater than 20 MB interfaces when 64-bit counters are not available in the MIB.
- A value of FALSE allows the IP Manager to resort to its previous behavior: Do not monitor greater than 20 MB interfaces when 64-bit counters are not available in the MIB. The default value is FALSE.

Use the sm_edit utility to modify the smarts/conf/discovery/tpmgr-param.conf file. For example, go to the BASEDIR/smarts/bin directory in the IP Management Suite installation area and type the following command to open the tpmgr-param.conf file:

```
sm_edit conf/discovery/tpmgr-param.conf
```

Press **Enter**.

After modifying the file, you must restart the IP Manager.

When you set the value to TRUE, and no 64-bit counters are available in the MIB, the IP Manager will monitor interfaces within a MaxSpeed range of greater than 20 MB and less than 650 MB.

Product enhancements in Service Pack 2

The following product enhancements were introduced in IP Management Suite 7.0 Service Pack 2:

- "Support for new device certifications" on page 36
- "Creation of multiple connections for a shared MAC address" on page 37

Support for new device certifications

Service Pack 2 added support for more than 130 new device certifications. The certifications extend both the functionality of the IP Management Suite products and the cross-dependency of other EMC Smarts products such as EMC Smarts MPLS Manager and EMC Smarts Network Protocol Manager.

Creation of multiple connections for a shared MAC address

(PR 22474) In a fault-tolerant multihoming network, a network device such as a host or router has interfaces to two or more networks that serve the same purpose; for example, to two or more Internet service providers (ISPs). The two or more interfaces on the host or router share a virtual IP address and a MAC address for redundancy purposes; only one of the interfaces can be active at any given time.

A new algorithm available with Service Pack 2 determines which interface on a host or router involved in a multihoming network is the one that connects to the active network, for example, to the active ISP.

With this Service Pack 2 enhancement, the IP Manager creates a "LayeredOver/Underlying" relationships between each of the interfaces and the shared MAC address during the initial discovery of the host or router, and creates a network connection for each of the interfaces to the shared MAC address during the post-processing phase of the discovery process. The IP Manager is able to track which network connection is active and which network connection or connections are in standby.

Note: For Cisco routers, the protocol for multihoming is Hot Standby Router Protocol (HSRP). Other manufacturers have similar proprietary protocols that work in a similar way.

Product enhancements in Service Pack 1

The following product enhancements were introduced in IP Management Suite 7.0 Service Pack 1:

- "Version output enhancement" on page 38
- "UTF-8 character set support" on page 38
- "New default value for SNMPv3 authentication protocol" on page 39
- "Enhanced support for BladeCenter server" on page 39
- "New setting to cleanup unused monitoring instances" on page 40
- "New settings to disable analysis for interfaces or ports" on page 43

- "EnableDNSLookupInReconfigure configuration parameter" on page 45
- "Enhanced support for VMware" on page 45
- "Enhanced naming convention for installation executables" on page 45

Version output enhancement

(CQ 278190) The output of the sm_server --version command was enhanced, as explained in "Version numbers" on page 56.

UTF-8 character set support

Service Pack 1 provides limited UTF-8 encoding support for the IP Manager.

EMC Smarts products based on the EMC Smarts 7.0 product foundation have the following limited support for UTF-8 encoding:

- The Service Assurance Global Manager and Adapter Platform support events containing UTF-8 encoded text from outside sources for EventText and UserDefined attributes used in notifications. Other attributes in the event object (ICS_Notification) do not support UTF-8 encoded text. Hostnames and topology object names can only appear in ASCII characters.
- The Service Assurance Global Console displays UTF-8 encoded text for the EventText and UserDefined attributes. For example, if these attributes contain UTF-8 encoded Japanese characters, the Japanese characters appear in the columns of the Notification Log View. Hostnames and topology object names can only appear in ASCII characters. Console components such as menus and toolbars remain in ASCII characters.
- If outside sources, such as an SNMP MIB, provide discovery data in a natural language (a human language—English or Japanese, for example—as opposed to a computer language), an IP Manager with Service Pack 1 applied does not transcode the encoding of the natural language text into UTF-8; for example, does not transcode SJIS encoded Japanese text into UTF-8 encoded Japanese text. The following fields are likely to contain natural language text:
  - sysContact
  - sysName

- sysLocation

- Installation and configuration of EMC Smarts products continue to use ASCII input, including filenames and directory paths.
- Command Line Interface (CLI) continues to use ASCII input. If a user enters data in a natural language text encoded with a character set other than ASCII, the Global Console does not display the text properly.

Configuration for this enhancement is predefined. No user action is required to configure this enhancement.

New default value for SNMPv3 authentication protocol

Service Pack 1 changes the default value for the authentication protocol parameter, AuthProtocol, from MD5 to NONE. The discovery process uses the AuthProtocol parameter to authenticate SNMP requests and responses when communicating with an SNMPv3 agent, and to authenticate SNMP traps received from an SNMPv3 agent. The other valid values for this protocol are MD5 and SHA.

Enhanced support for BladeCenter server

An IP Manager with Service Pack 1 applied is able to discover the individual blades of an IBM BladeCenter server as hosts and switches, and is able to identify the individual blades as being part of the BladeCenter server. In releases before Service Pack 1, the IP Manager was able to discover a BladeCenter server and its individual blades but was not able to identify the individual blades as being part of the BladeCenter server.

When an IP Manager with Service Pack 1 applied discovers a BladeCenter server (System ObjectID: 1.3.6.1.4.1.2.6.158.3), it represents the server as a host having the BladeCenter's chassis name. The discovery represents the server as a whole and also identifies the individual blades that are part of the server.

In the topology tree of a Global Console attached to the IP Manager, the hosts, switches, fan, power, temperature, and voltage associated with a BladeCenter instance are represented under the ComposedOf relationship. An example is shown in Figure 7 on page 40.

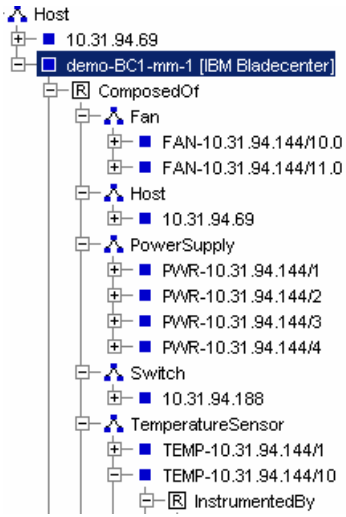

Figure 7 **IBM BladeCenter server as host and the ComposedOf relationship**

Note: The IBM BladeCenter Chassis Management module maintains a list of IP addresses of the switch modules connected to the individual blades. Hence, if you enable autodiscovery, the IP Manager discovers the switch modules during the autodiscovery process and shows them as part of the chassis.

When the BladeCenter Chassis Management module (chassis agent) is down, the IP Manager cannot identify the individual blades as being part of the BladeCenter server. You must ensure that the BladeCenter Chassis Management module is up and running before you discover the network.

When individual blades of a BladeCenter server are down, they are displayed separately as down. When all individual blades of a BladeCenter server are down, the BladeCenter server itself is displayed as down.

To retrieve information about the IBM BladeCenter server, the IP Manager polls the vendor-specific MIB, BLADE-MIB.

New setting to cleanup unused monitoring instances

A new polling and thresholds setting named “Cleanup Unused Monitoring Instances” controls the removal of instrumentation objects that no longer have an associated object (a Card, Interface, Port, or Memory instance, for example) to monitor. This situation

occurs when an originally enabled polling and thresholds setting for a polling or threshold group is disabled by the user. In releases before Service Pack 1, instrumentation objects created by enabling a particular polling and thresholds setting were not removed after the setting was disabled.

The Cleanup Unused Monitoring Instances setting is available to any polling or threshold group for which the matching-criteria target class is UnitaryComputerSystem. The setting is enabled by default.

Table 11 on page 41 lists the settings that are affected by the Cleanup Unused Monitoring Instances setting.

Table 11 Settings affected by the Cleanup Unused Monitoring Instances setting

Polling group setting	Threshold group setting	Instrumentation objects created for these classes
Connectivity Polling	Connectivity	• Card • Interface • Port
Performance Polling - Ports and Interfaces	N/A	• Interface • Port
Performance Polling - Processor and Memory	Cisco Processor and Memory	• Memory • Processor
Environment Polling	Environment	• Fan • PowerSupply • TemperatureSensor • VoltageSensor
FileSystem Polling	FileSystem	• Disk • FileSystem
Connectivity Polling for IPv6 Addresses	N/A	• IPv6

Removing the Cleanup Unused Monitoring Instances setting

1. In a **Domain Manager Administration Console** attached to the IP Manager, choose **Configure > Polling and Thresholds** to open the **Polling and Thresholds Console**.

   The example display in Figure 8 on page 42 shows the **Cleanup Unused Monitoring Instances** setting in the **Settings** tab of a **Routers** polling group, available through the **Polling** tab of a **Polling and Thresholds Console** attached to an IP Performance Manager. In the display, the **Cleanup Unused Monitoring**

Instances setting is shown as added to the group (the default), thereby enabling the cleanup of unused monitoring instances for the **Routers** group.

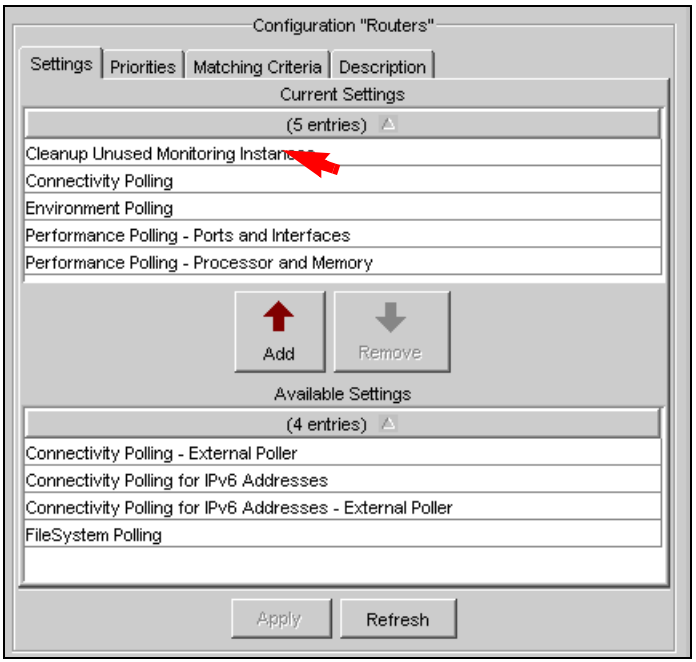

Figure 8 Cleanup Unused Monitoring Instances setting in the Routers polling group

2. In the **Settings** tab, select the **Cleanup Unused Monitoring Instances** setting in the **Current Settings** list.
3. Click **Remove** to move the setting to the **Available Settings** list.
4. Click **Apply** to save your changes.
5. Click the **Reconfigure** toolbar button to make your changes take effect.

Adding the Cleanup Unused Monitoring Instances setting

1. In the **Settings** tab, select the **Cleanup Unused Monitoring Instances** setting in the **Available Settings** list.
2. Click **Add** to move the setting to the **Current Settings** list.
3. Click **Apply** to save your changes.

4. Click the **Reconfigure** toolbar button to make your changes take effect.

New settings to disable analysis for interfaces or ports

The polling and thresholds setting named "Disable Interface/Port Analysis" is now represented by two settings named "Disable Performance Analysis for Interface/Port" and "Disable Fault Analysis for Interface/Port". The Disable Performance Analysis for Interface/Port setting allows a user to disable the performance analysis of interfaces and ports, and the Disable Fault Analysis for Interface/Port setting allows a user to disable the fault analysis of interfaces and ports.

Both settings are available to any threshold group for which the matching-criteria target class is Interface or Port. For any of these groups, a user can specify the Disable Performance Analysis for Interface/Port setting, the Disable Fault Analysis for Interface/Port setting, or both. Both settings are disabled by default.

The following two procedures provide instructions for adding and removing the Disable Fault Analysis for Interface/Port setting. The same procedures can be used to add and remove the Disable Performance Analysis for Interface/Port setting.

Adding the Disable Fault Analysis for Interface/Port setting

1. In a **Domain Manager Administration Console** attached to the IP Manager, choose **Configure > Polling and Thresholds** to open the **Polling and Thresholds Console.**

   The example display in Figure 9 on page 44 shows the **Disable Fault Analysis for Interface/Port** setting in the **Settings** tab of a **1 GB Ethernet** threshold group, available through the **Thresholds** tab of a **Polling and Thresholds Console** attached to an IP Performance Manager. In the display, the **Disable Fault Analysis**

for Interface/Port setting is shown as removed from the group (the default), thereby enabling fault analysis for the interfaces that become members of the **1 Gb Ethernet** group.

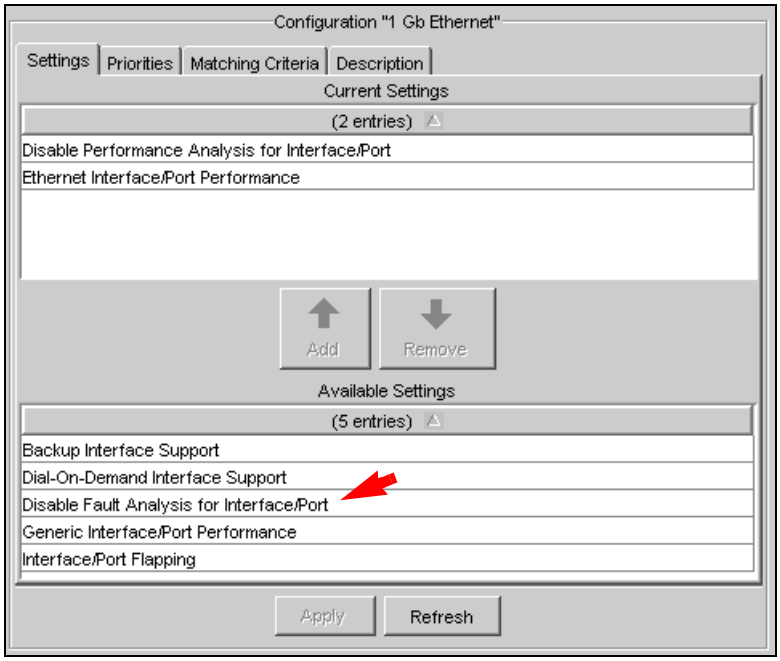

Figure 9 Disable Fault Analysis for Interface/Port setting in the 1 Gb Ethernet threshold group

2. In the **Settings** tab, select the **Disable Fault Analysis for Interface/Port** setting in the **Available Settings** list.
3. Click **Add** to move the setting to the **Current Settings** list.
4. Click **Apply** to save your changes.
5. Click the **Reconfigure** toolbar button to make your changes take effect.

Removing the Disable Fault Analysis for Interface/Port setting

1. In the **Settings** tab, select the **Disable Fault Analysis for Interface/Port** setting in the **Current Settings** list.
2. Click **Remove** to move the setting to the **Available Settings** list.
3. Click **Apply** to save your changes.

4. Click the **Reconfigure** toolbar button to make your changes take effect.

EnableDNSLookupInReconfigure configuration parameter

Available with Service Pack 1 is a new parameter to control whether the DNS lookup is used during a reconfiguration. The parameter is named EnableDNSLookupInReconfigure and is contained in the tpmgr-param.conf file.

You can assign the following values to the parameter:

- A value of TRUE indicates that DNS lookup is used during a reconfiguration.
- A value of FALSE indicates that DNS lookup is not used during a reconfiguration. The default value is FALSE.

Note: Use the sm_edit utility to modify the tpmgr-param.conf file. After modifying the file, you must restart the IP Manager.

Ensure that when you set the value to TRUE and DNS provides wrong IP addresses, the wrong addresses might be used for polling. Thus, polling might result in incorrect alarms.

A value of FALSE improves discovery time. If you have frequent DNS changes, and a full discovery takes a long time, you can set the value to TRUE to synchronize the AgentAddressList.

Enhanced support for VMware

There is new support for VMware ESX 3.0.1 when configured with Windows 2003 Enterprise Edition SP1, R2, or Red Hat Enterprise Linux AS 3 Update 5.

Enhanced naming convention for installation executables

Available with Service Pack 1 is a new naming convention for installation executables. The convention is:

```
setup-<suite>-<version>-<os>.<exe|bin>
```

An example for Windows for IP Management Suite 7.0.1 is:

```
C:\setup-IP-7_0_1_0-win.exe
```

An example for Solaris, HP-UX, or Linux for IP Management Suite 7.0.1 is:

```
setup-IP-7_0_1_0-<os>.bin
```

Where <os> is operating system: `sol`, `hpux`, or `linux`.

The new naming convention makes it easy for customers to identify the EMC Smarts product suite and version number associated with an installation executable.

Fixed problems

In addition to new software fixes, Service Pack 4 includes the software fixes provided in Service Packs 1, 2, and 3. This section lists the software fixes and the service pack in which it was initially introduced.

Table 12 on page 47 lists the software fixes provided by Service Pack 4 for the IP Management Suite.

Table 12 Fixes applicable to the IP Management Suite (page 1 of 7)

CQ or SR ticket number	Summary	Fixed in	Problem Report number
CQ 571495 CQ 566083	Discrepancies in the creation of STPNodes and Cable connections were observed. In earlier releases, there could be wrong connections created in the topology based on BridgeMIB data. This could possibly lead to incorrect root cause analysis. The wrong connections may have been created due to duplicate PortNumber across more than one port of the same device. This could happen in cases such as Link Aggregation. Code is changed such that if the PortNumber is duplicated, the BridgedVia relationship is not created on that port and the connection is skipped. The corresponding STPNode is also not created when there is duplication in the PortNumber.	SP4	N/A
CQ 571454 CQ 565232	The AllComponentsDown event for redundancy groups HSRP and VRRP was generated if both the interfaces of a group were administratively down. The event should be generated for operation down of the interface and not Admin down. The AllComponentsDown event is now not generated if the member Endpoints of the Group's underlying interface Admin Status is disabled since the explicit configuration of the components of a redundancy group to be administratively disabled, did not constitute an operational failure of the group itself.	SP4	N/A

Table 12 Fixes applicable to the IP Management Suite (page 2 of 7)

CQ or SR ticket number	Summary	Fixed in	Problem Report number
CQ 570746	As a result of the fix provided for CQ 565138, some valid Serial ifTypes were not being handled properly when making WAN NetworkConnections during post processing. This results in fewer WAN NetworkConnections formed after the migration from 7.0.3 to 7.0.4. Additional Serial ifType values are introduced to compensate for the loss of WAN NetworkConnections. These Serial IfType values are added to the tpmgr-param.conf configuration file as follows: • WANLINK_PPP TRUE • WANLINK_L3IPVLAN TRUE • WANLINK_RFC1483 TRUE Due to the limited availability of sample Serial IfType values, the above list may not cover all the potential Serial ifTypes in the topology. As a result of upgrading from 7.0.3 to 7.0.4, if there are fewer WAN NetworkConnections than earlier, contact Customer Support.	SP4	N/A
CQ 565138	Connections were created even when only one interface of a WAN NetworkConnection satisfied the criteria to establish a connection. As a result, depending on the order the interfaces were evaluated in, there was a possibility of making a connection incorrectly. This is fixed by ensuring that both the end adapter interfaces of the WAN NetworkConnection satisfy the criteria to create a connection.	SP4	N/A
CQ 562319	The interface Underlying and LayeredOver relationships were not created in Netscreen devices. Since the discovery of SSG and ISG series of firewalls was differentiated from others, the relationships were not created. This problem is fixed by creating interface layering relationships based on the interface description.	SP4	N/A

Table 12 Fixes applicable to the IP Management Suite (page 3 of 7)

CQ or SR ticket number	Summary	Fixed in	Problem Report number
CQ 530164 SR 36171202	The OID .1.3.6.1.4.1.9.1.672 misidentified the model number. The correct model number should be ASA5540 instead of ASA5405. The correct model number ASA5540 is updated for OID .1.3.6.1.4.1.9.1.672 in the oid2type_Cisco.conf file.	SP4	N/A
CQ 526382 SR 35135320	Removal of the Standby Routing Engine Card did not generate an event for Juniper MX960 devices. The Juniper Devices Redundancy Card status must be polled from the jnxFruState, jnxOperStatus and jnxRedundancyState MIB attributes. When a Standby Routing Engine Card is pulled out from the slot, the jnxFurState MIB attribute value becomes empty. The problem is fixed by generating a Critical Event for Standby Routing Engine Card when the jnxFruState MIB attribute's polled value is empty.	SP4	N/A
CQ 524573 SR 34857564	During Cisco CDP post-processing, the findIP() call was used to find if the Remote IP address polled from the Cisco CDP MIB was available in the topology. To get the Remote IP Address, the cdpCacheAddress was polled. If the Remote IP address was not found for a particular port number of the local host, the cdpCacheDeviceId was used, instead of the Remote IP address. As a result, the CDP post-processing took more time than expected. The CDP DeviceID table contains the IP address or the system name. Modified the code to check the contents of this table and if the CDP DeviceID is a system name, the findIP() call is not performed. This reduces the time taken for CDP post-processing.	SP4	N/A

Table 12 Fixes applicable to the IP Management Suite (page 4 of 7)

CQ or SR ticket number	Summary	Fixed in	Problem Report number
CQ 519281 SR 33919514	During discovery of unisphere devices, the following ASL error occurred: 20-Mar-2010 6:49:40 AM+945ms EDT] t@62 Discovery #5 ASL-W-ERROR_RULE_SOURCE-While executing rule set '/opt/InCharge7/IP/smarts/local/rules/discovery/ic-unisphere-data.asl' ASL-ERROR_ACTION-While executing action at: ASL-CALL_STACK_RULE- RuleName: JUNI_INTERFACE, Line: 519 ASL-CALL_STACK_RULE- RuleName: START, Line: 507 ASL-ERROR_UNDEFINED_VARIABLE_ACCESS-Variable 'interfaceDone' has not been assigned a value. The error occurred due to a return statement in the INIT rule. This has been fixed.	SP4	N/A
CQ 501420 SR 33588292	The criteria by which critical status of the voltage sensors was identified was too strict. If the voltage varied by the smallest amount, the status showed as critical and an alarm was generated. The preference was to have the thresholds populated in the GUI and to be able to use the relative voltage threshold to control out-of-range alarms. An OutOfRange alarm is provided for all Redback devices based on threshold values set by the user. The StateNotNormal event has been removed.	SP4	N/A
CQ 501026 SR 33242006	Trunk cable connections were not created between Force10 E600 devices. Modified code to create trunk cable connections.	SP4	N/A

Table 12 Fixes applicable to the IP Management Suite (page 5 of 7)

CQ or SR ticket number	Summary	Fixed in	Problem Report number
CQ 494517 SR 35089680	After adding a device in the pending list, the DiscoverState and Description attributes did not get updated in the AD_PendingData class instance. The problem is fixed by adding a call updateDiscoveryState() to assign correct values to the DiscoveryState and Description attributes for the pending device.	SP4	N/A
CQ 493965 SR 34120716	VLANs were numbered by internal index on Juniper EX4200 and EX8216 devices instead of being tagged. Added a new driver to create VLANs based on Juniper Vlan MIB OID jnxExVlanTag for device EX4200 of sysOID 1.3.6.1.4.1.2636.1.1.1.2.31. If jnxExVlanTag OID is empty, then the jnxExVlanNameOID index is used to create VLANs.	SP4	N/A
CQ 493718 SR 33543048	The HighThreshold value set for Temperature on Cisco MDS device was invalid and resulted in OutofRange events being generated. The attribute HighThreshold is now calculated by using the value from entSensorThresholdValue (1.3.6.1.4.1.9.9.91.1.2.1.1.4.21912) with index "1". If the OID populates negative units or NULL value, the default TemperatureHighThreshold will be considered.	SP4	N/A
CQ 289624	Memory, Disks, and Filesystems tabs are missing in the Containment views for discovered Solaris 9 or 10 host systems managed by NETsnmp 5.4 agents. Fixed code in the shared MAP-CONTAINMENT.import file to display the Memory, Disks, and Filesystems tabs. Also, for the Disks tab entry in the file, changed the names of the AvgDataRate and AvgQueueDepth attributes to: • MaxAvgDataRate • MaxAvgQueueDepth	SP3	N/A

Table 12 Fixes applicable to the IP Management Suite (page 6 of 7)

CQ or SR ticket number	Summary	Fixed in	Problem Report number
CQ 341651	The IP Manager crashed due to a deadlock. The deadlock occurred when a monitoring-system thread made a call to the accessor to get values of instrumented attributes. The reason for the deadlock was that the thread attempted to acquire locks in an incorrect order. Changed the lock acquisition order in the “monitor” class file to ensure that threads acquire locks in the correct order.	SP3	N/A
CQ 303622	Shadow IP addresses, that is, IP objects that have their IsShadow parameter set to TRUE, appear in the IP Addresses tab of Containment views for discovered network objects. Added code to the shared MAP-CONTAINMENT.import file to filter out IP addresses that have their IsShadow parameter set to TRUE.	SP2	N/A
CQ 211819 SR 15959764	Adapter Scripting Language (ASL) script does not work as context filter for Server Tool. Fixed ASL parsing to avoid exception when checking parameter values.	SP1	20689
CQ 216220 SR 5490394	When the Global Manager reconnects to clients, an error might occur that causes the Global Manager to crash. Fixed error that caused a recursion in the Global Manager’s reconnect code.	SP1	19728
CQ 236802	The Data Exchange Adapter (DXA) Configuration Syntax HTML page has been updated to reflect enhanced functionality for filtering capabilities. The DXAConfigurationSyntax.html file is located in the BASEDIR/smarts/doc/html/usage directory. The index.html file provides an index to the various commands.	SP1	20829

Table 12 Fixes applicable to the IP Management Suite (page 7 of 7)

CQ or SR ticket number	Summary	Fixed in	Problem Report number
CQ 240546	Relationship change notifications are not generated during a transaction commit. Symptom: Deleting an IP tag group in the Global Console did not cause the icons in the console to be removed. The handling of relationship changes during a transaction commit is fixed.	SP1	20944
CQ 275605	The trapCount and trapRate are not calculated correctly in the Network Protocol Manager 2.0 release. Fixed: The fetch_trapCount properly returns a failure code when no callback is bound.	SP1	21517
CQ 275984	When the glob function in ASL returns a parse error, it is not outputting the offending pattern. Fixed: Improved ASL error message to contain the glob pattern that failed.	SP1	21641
CQ 278481 SR 16090272	Perl API Check scripts do not work with ActivePerl 5.8.8.819. Fixed: Modified Perl scripts to work with newest version of Active Perl as well as older versions previously supported.	SP1	N/A

Environment and system requirements

Platform support

Ionix IP Management Suite 7.0.4 supports the following operating systems:

- Solaris 8, 9, and 10
- HP-UX 11.11
- Red Hat Enterprise Linux AS 3 or 4
- Red Hat Enterprise Linux Server 5
- Windows 2003 Enterprise Edition, SP1, SP2, and R2
- Microsoft Windows Server 2008 Enterprise Edition SP1, SP2, and R2

Platform Support Notes

Red Hat Enterprise Linux (RHEL) 5

When you start IP Management Suite in a system with RHEL 5, you might see the following error:

```
[09-Sep-2010 12:05:11 AM+383ms EDT] t@-143386224 <Primary
Thread> CI-E-EPRGNOTLOAD-Program "dmboot" could not be
loaded CI-ESYSINFO-System information:
/opt/InCharge/IP/smarts/local/lib/libsm_license.so:
cannot restore segment prot after reloc: Permission
denied RTLD-SI_ELOADERR-Dynamic loader error
```

The error message appears if the **SELinuxSetting** security setting is enabled. To correct the problem, run the following command from the command prompt:

```
chcon -t textrel_shlib_t
/opt/InCharge/IP/smarts/local/lib/libsm_license.so
```

Solaris 10

If you are running IP Management Suite on Solaris 10, the **tcp_fusion** setting must be disabled. If it is enabled, there may be a degradation in the performance of IP Management Suite.

To disable **tcp_fusion**, add the following lines at the bottom of the /etc/system file and restart the system for the new setting to take effect:

```
Disable tcp fusion
set ip:do_tcp_fusion = 0x0
```

Patch levels of supported platforms

The following patch levels have been identified as critical to the proper functioning of the EMC Smarts software. Because patch levels are continually being updated, ensure that your operating systems are patched to the most recent levels recommended by the OS vendors.

Note: These patch levels have changed since the 7.0 product release.

- Solaris 8
  - 108434-22 C++ runtime library (32-bit)
  - 108435-22 C++ runtime library (64-bit)
  - 111721-04 libm patch
  - 116965-23 (to fix an ACK storm bug in Solaris that prevents it from transmitting urgent data TCP packets)
  - 121972-02 (to fix a Socksfs bug)

- Solaris 9
  - 111711-23 C++ runtime library (32-bit)
  - 111712-23 C++ runtime library (64-bit)
  - 111722-04 libm patch
  - 114344-36 (TCP patches)
  - 118335-06 (to fix a Socksfs bug)
- Solaris 10
  - 119963-08 C++ patch
  - 120011-14 - Network stack patches, tcp fusion on loopback hangs. This is part of a set of patches which must be installed in a specific order. Install the Solaris 10 patch set for Sparc that includes 120011-14 or newer.
- Red Hat Enterprise Linux AS 4
  - compat-libstdc++-33-3.2.3
- Red Hat Enterprise Linux Server 5

  - compat-libstdc++-33-3.2.3-61
- HP-UX 11.11 (PA-RISC)
  - PHCO_36082 1.0 (libc manpage cumulative patch)
  - PHCO_36184 1.0 (libc cumulative patch)
  - PHNE_35865 1.0 (libnss_dns DNS backend patch)
- HP-UX 11.23 (Itanium)
  - PHSS_36347 1.0 (assembler patch)
  - PHSS_37552 1.0 (Aries cumulative patch)
  - PHSS_38134 1.0 (linker + fdp cumulative)
  - PHSS_38140 1.0 (aC++ Runtime (IA: A.06.20, PA: A.0)
- Windows 2003 Enterprise Edition SP1
  - Hotfix KB 927493

Deprecated platform support

Ionix IP Management Suite 7.0 is not supported on the following platforms:

- Windows 2000 Server and Advanced Server, SP4
- HP-UX 11.0

Version numbers

When you run a utility to report the version number of the software, you will see both the version number for the product suite as well as the version number for the underlying EMC Smarts 7.0 product foundation software. These two version numbers may differ.

Checking the version number

From the BASEDIR/smarts/bin directory, enter the following command:

```
sm_server --version
```

The EMC Smarts output displays the following:

```
<Suite>: V<Number>(<InternalBuild>), <Date>
Copyright 1995-2008, EMC Corporation - Build <Build>
Foundation V<Number>(<InternalBuild>), <Date>
Copyright 1995-2008, EMC Corporation - Build <Build>
```

For example, for IP Management Suite 7.0.4, the output might look similar to:

```
sm_server.exe:
IP_NETWORK_SUITE: V7.0.4.0(101808), 13-Oct-2010 13:33:22
Copyright 1995-2010, EMC Corporation - Build 42
Foundation V7.0.2.1(101037), 11-Sep-2010 08:55:09
Copyright 1995-2010, EMC Corporation - Build 121
```

Note: Product versions vary and do not always match the EMC Smarts version number. For example, if you select the About from the Help menu in the Global Console, you may see a different number.

The product version number is displayed during installation on the InstallShield screen.

Product and version compatibility

IP Management Suite 7.0.4 is compatible with the versions of the products listed in Table 13 on page 57.

Table 13 IP Management Suite 7.0.4 interoperability chart (page 1 of 2)

Smarts or Ionix product suite	Versions
Application Connectivity Monitor	2.1.x, 2.2.x, 2.3
ATM/Frame Relay Availability Management Suite	1.0, 1.1, 2.0.x
Optical Transport Management Suite	2.0.0.1, 5.0
Multicast Manager	1.1.x, 1.2, 2.0
MPLS Management Suite	2.1, 3.0, 3.1
Network Protocol Management Suite	2.1, 3.0
Service Assurance Management Suite	7.1, 7.2.0.25, 8.0.0.4, 8.1.0.x
Storage Insight for Availability	1.0.0.2, 1.0.0.3, 2.0.x, 2.1, 2.3
Service Assurance Management Adapter Suite	1.0, 1.1, 1.2
ITOps Performance Reporter	1.0, 1.2, 2.0.x, 8.1.0.3
Voice over Internet Protocol (VOIP) - AM	2.0, 3.0, 4.0

Table 13 IP Management Suite 7.0.4 interoperability chart (page 2 of 2)

Smarts or Ionix product suite	Versions
Alcatel 5620 SAM Adapter (ASAM)	2.1, 3.0, ,3.1, 3.2
IP Management Suite	6.5.x, 7.0.x
Server Manager (EISM)	1.1, 2.0

FLEXnet 10.1.3 licensing

Upgraded License Support – EMC Smarts products based on the EMC Smarts 7.0 product foundation now use the FLEXnet version 10.1.3. If users have FLEXlm version 9.2 for other EMC Smarts products, their 9.2 licenses will work with the 10.1.3 FLEXnet License Server. See the *FLEXnet Licensing End User Guide* for information about FLEXnet version 10.1.3. For information about licensing EMC Smarts products, see the *EMC Smarts System Administration Guide*.

FLEXnet software is backward-compatible. A FLEXnet 10.1.3 license server provided with EMC Smarts version 7.0 software will work with FLEXlm 9.2 license files distributed for EMC Smarts version 6.5.x software, but not vice versa.

Known problems and limitations

The following problems and limitations are known for Service Pack 4:

- "Installation/uninstallation issues" on page 58
- "Ionix IP Management Suite issues" on page 60
- "Documentation errata" on page 67

Installation/uninstallation issues

The following issues relate to the install or uninstall process.

Exception when installing IP Management Suite 7.0.4 on Solaris 9

CQ 571066

Issue

If you install IP Management Suite 7.0.4 on Solaris 9 that does not have all the required patches, an exception is displayed when you exit the installation.

```
java.net.UnknownHostException: linbgn106.lss.emc.com:
linbgn106.lss.emc.com at
java.net.InetAddress.getLocalHost(Unknown Source) at
com.smarts.production.wizardx.panels.ExtendedWelcomePane
l.logInetInfo (ExtendedWelcomePanel.java:193) at
com.smarts.production.wizardx.panels.ExtendedWelcomePane
l.queryEnter(ExtendedWelcomePanel.java:128) at
com.installshield.wizard.console.ConsoleWizardUI.current
BeanChanged(Unknown Source) at
com.installshield.wizard.StandardWizardListener.currentB
eanChanged(Unknown Source) at
com.installshield.wizard.Wizard$RunThread.run(Unknown
Source)
```

Resolution

Ensure that your operating system is patched to the most recent level and perform the installation. For more information regarding patch levels, see the "Patch levels of supported platforms" on page 55 section.

Cannot upgrade from IP Management Suite 7.0.0 to 7.0.4

CQ 570667

Issue

You cannot upgrade directly from IP Management Suite version 7.0.0 to 7.0.4.

Resolution

Upgrade to one of the Service Pack releases of IP Management Suite (7.0.1, 7.0.2, or 7.0.3) before upgrading to IP Management Suite 7.0.4.

Note: If patches for any version are installed, uninstall all patches before performing an upgrade.

Services cannot be selected for products installed previously

CQ 296284

Issue

If you install a product and do not select the corresponding service during installation, you cannot select the service during later installations. The service is disabled on the Service Selection screen for any product that was installed previously. This issue occurs only if installation is on the same host.

Resolution

Manually configure the service for the product as described in the *EMC Ionix IP Management Suite Installation Guide*.

Ionix IP Management Suite issues

The following issues apply to the IP Management Suite applications.

Current processor utilization value is not displayed properly for some Juniper device models

CQ 571898 / CQ 572031

Issue

For Juniper devices running JunOS-8.5R1.13, the processor's current utilization value is polled from the jnxOperatingTable's jnxOperatingCPU MIB attribute. The jnxoperatingCPU MIB attribute is a Gauge 32 bit data type. But for some processor instances, the value reported is more than the 32 bit range. In such cases, the IP Manager reports the current processor utilization value as negative.

Resolution

There is no workaround at this time.

Error message in the log file regarding Juniper_System_Environment_Setting after an upgrade

CQ 502628

Issue

When you upgrade an existing IP Management Suite 7.0.1, 7.0.2, or 7.0.3 installation to 7.0.4, warning messages appear in the log file.

```
27-Sep-2010 4:08:10 PM+627ms Eastern Daylight Time]
t@3152 InCharge Framework
```

```
MR-W-CLASS_NOTDEFINED-Class:
'Juniper_System_Environment_Setting' is no longer defined
in repos.
```

Resolution

The message is displayed because the class Juniper_System_Environment_Setting is no longer used in IP Management Suite 7.0.4. The same functionality is performed by System Resource Groups or Temperature Sensor Groups. You can ignore the warning message.

Error message in the log file regarding the IsProxy attribute after an upgrade

CQ 571267

Issue

When you upgrade an existing IP Management Suite 7.0.1, 7.0.2, or 7.0.3 installation to 7.0.4, warning messages appear in the log file.

```
[27-Sep-2010 09:18:24 PM+306ms IST] t@-1274049616
InCharge Framework
MR-W-ATTRIBUTE_NOTDEFINED-'Partition::IsProxy':
Attribute is no longer defined by class.
```

Resolution

The warning message appears because the attribute IsProxy and all proxy-related code is removed from IP Management Suite 7.0.4. The aim of these changes is for better Root Cause Analysis and performance optimization.

You can ignore this message.

Additional backup directory created after an upgrade

CQ 571085

Issue

When you upgrade an existing IP Management Suite 7.0.1, 7.0.2, or 7.0.3 installation to 7.0.4, the customized files from your old installation are moved to a new folder at this location: <BASEDIR>/smarts/.local.bkp.7.0.X. In addition, another folder is created at this location: <BASEDIR>/smarts/local/.local.bkp.7.0.X.

Resolution

This latter one under the local folder is empty and can be ignored. All the customizations are saved under the <BASEDIR>/smarts/.local.bkp.7.0.X folder.

Additional environment variables in the runcmd_env.sh file

CQ 502640, CQ 502634

Issue

When you install IP Management Suite 7.0.4, you will see the following additional environment variables in the runcmd_env.sh file:

```
SM_IP_VERSIONS=v6v4
SM_ENCODING_OUTPUT=UTF-8
SM_GUI_DISPLAYNAME_CLASSES=CORE_Collection
```

Resolution

None of these variables impact IP Management Suite 7.0.4 and can be ignored.

Crash under Windows Server 2008 Enterprise Edition in licensing code

CQ 502130, CQ 502343

Issue

The licensing code can cause the domain manager to crash under some conditions when licensing is being provided by a file specified with SM_LICENSE.

Resolution

- Inspect the value of the registry key HKEY_LOCAL_MACHINE\SOFTWARE\FLEXlm License Manager and remove any references to directories, or delete the key.
- Set up a license server and set SM_LICENSE as described in the *EMC Ionix ITOps System Administration Guide*. Alternatively, ensure that the file specified with SM_LICENSE exists.

IMPORTANT

The FLEXnet license server version 10.8.5.0 is currently not supported on Microsoft Windows Server 2008.

Mismatch in partition instances and MemberSystems between IP Management Suite versions 7.0.4 and 7.0.3

CQ 565894

In IP Management Suite version 7.0.4, load balancers get connectivity with the switches present in the topology. Hence, load balancers are present in the same partition as the switches. In IP Management Suite version 7.0.3, the load balancers were not connected with switches and formed a separate partition.

Therefore, the number of partitions between the two versions differ. However, the current behavior results in relationships between neighboring devices which is favorable.

Display of high processor utilization percentage

CQ 565231

IP Management Suite displays utilization values for a processor as reported by the device. In some instances, the value returned by the device may be beyond the range of a valid utilization value as per the MIB definition. However, the application will display the value as is. It relies on the agent to provide the appropriate utilization values.

Displaying the values as returned by the agent enables the administrator to identify the issue as a problem with the device.

Card to port mapping relationship for Cisco Nexus 5000 and Nexus 7000 Series

CQ 565305 / CQ 570754

Issue

The entAliasMappingIdentifier OID, which provides the mapping between entityPhysicalIndex and IfIndex, is not supported for Cisco Nexus Switches. Therefore, IP Management Suite 7.0.3 was unable to provide card to port mapping relationships.

Resolution

IP Management Suite 7.0.4 uses a formula provided by the vendor to retrieve the ifIndex from the entityPhysicalIndex and establish the card to port mapping relationships. The formula is applicable for Cards/Modules containing Ethernet, Fex Ports and will not be applicable for Modules/Cards which have both FC and Ethernet Ports (for example: N5K-M1404).

The formula has been tested on the following Device OIDs and restricted to the OS versions:

- Cisco N7000 .1.3.6.1.4.1.9.12.3.1.3.612 | Cisco NX-OS™ n7000, Software (n7000-s1-dk9), Version 4.2(5), Interim version 4.2(4.44)
- Cisco N5020 .1.3.6.1.4.1.9.12.3.1.3.719 | Cisco NX-OS™ n5000, Software (n5000-uk9), Version 4.2(1)N1(1), Interim version 4.2(1)N1(0.329)
- Cisco N5010 .1.3.6.1.4.1.9.12.3.1.3.798 | Cisco NX-OS™ n5000, Software (n5000-uk9), Version 4.2(1)N2(1), RELEASE SOFTWARE Copyright (c) 2002-2010 by Cisco Systems, Inc. Device Manager Version 5.0(4), Compiled 7/28/2010 18:00:00

DSCV-W-PROBE_FAILED message appears in the log file

CQ 378292

Issue

When you discover some devices, messages similar to the following appear in the IP Manager log file:

```
DSCV-W-PROBE_FAILED-'discovery/ic-cisco-cpu.asl: Cisco CPU
Physical Index'
   probe of '10.31.117.89' failed
```

The DSCV-W-PROBE_FAILED is a warning message, and does not indicate an error. The ic-cisco-cpu.asl file was introduced in IP Management Suite 7.0.3 to extract CPU description from the Entity MIB. This was required because in the table cpmCPUTotalTable, in the ciscoProcessMIb, does not contain a description entry.

Though the warning message appears in the system log, it does not point to the cpmCPUTotalTable. Moreover, there is no need for extracting the description from the Entity table.

Resolution

You can ignore the warning message. No user action is required.

Cannot delete router IP address from the IP Manager topology

CQ 212528

Issue

After deleting a router IP address from the IP Manager topology, the object appears to delete successfully but reappears in the IP list when the Reconfigure toolbar button is clicked.

Resolution

No user action is required. EMC Smarts testers cannot reproduce this issue.

DSCV-W-DELETE_COMPONENT-'CARD* messages appear in the log file

CQ 287376, CQ 287150

Issue

DSCV-W-DELETE_COMPONENT-'CARD* messages appear in the IP Manager's log file. After discovering the device, some cards are seen in the topology, but the log file is erroneously saying that some card components are deleted with some different card indexes. This issue will not affect the functionality.

Resolution

No user action is required.

IPSec exception messages appear in the log file

CQ 373854

Issue

IPSec exception messages appear in the IP Manager's log file during IPSec short discovery.

An example of the message is:

```
[11-Mar-2008 2:10:02 PM+000ms PST] t@2276 ShortDiscovery
#6 CI-E-ESRVTHEXCEPTION-Service thread closure for queue
 ShortDiscovery #6 threw exception
  MR-CALL_ON_NULL_OBJECT-Tried to make a call on a NULL
repository
   object; in file "l:\ip-7.0.3\26\smarts\auto-discovery\
   winnt-i386\optimize\TopologyManager. h" at line 13655.
```

The IP Manager will successfully recover from the exception and continue to function properly.

Resolution

No user action is required.

VPN Tagging Server has connection issues with Broker and AM server on Windows platform

CQ 508649

Issue

On a Windows 2003 Service Pack 1 platform, the VPN Tagging Server is unable to establish a connection between the AM server and the Broker.

The VPN Tagging Server fails to connect the AM server and the Broker, displaying ASL errors and write buffer messages. This failure is due to a restriction implemented by Microsoft in Windows 2003 Service Pack 1, allowing a maximum of 10 connections that TCP may open simultaneously to prevent malware.

The following links provide more details:

http://support.microsoft.com/kb/Q324270

http://smallvoid.com/article/winnt-tcpip-max-limit.html

Resolution

Create a registry key to remove the restriction placed by Microsoft on the connection parameter.

To add a new registry key:

1. From the **Start** menu, select **Run**.
2. Type **regedit** and press **Enter**.
3. Go to **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters**
4. Add a new parameter **SynAttackProtect**.
5. Right-click to add a new **DWORD VALUE** with data type as **REG_DWORD**.
6. Double-click the parameter and set the value to **0**.
7. Shut down all servers.
8. Restart the machine.
9. Start the Broker, SAM, AM, VPN Tagging, and MPLS topology servers.

Documentation errata

The following notes list changes to user documentation.

Incorrect command in migration guide

(CQ 310270) Page 2-12 of the *EMC Smarts IP Management Suite Migration Guide* has an incorrect command in step 2b. The sm_rebond command is missing the drive letter for Windows (C:) or the path for UNIX (/opt) of the directory path.

The correct text is:

2. At the conclusion of the installation process, if you have changed your secret phrase from the default, you must change the secret phrase used for encryption to match the one used in the rest of your deployment.

- On Windows:

1. Go to C:\InCharge7\IP\smarts\bin
2. Type the following command:

```
sm_rebond --basedir=C:\InCharge7\IP\smarts
```

or

- On UNIX:

1. Go to /opt/InCharge7/IP/smarts/bin
2. Type the following command:

```
sm_rebond --basedir=/opt/InCharge7/IP/smarts
```

Note: This example of the sm_rebond command assumes you used the default installation path. If you initially installed the application to a different path, use that path.

Authentication protocol default change not documented for the deployment guide

(CQ 284241) As of Service Pack 1, the authentication protocol default for the AuthProtocol attribute changed from MD5 to NONE. This change was not documented in the deployment guide for the IP Management Suite, but it was documented for the configuration guide and discovery guide.

On Page 2-11 of the *EMC Smarts IP Management Suite Deployment Guide*, the bulleted text will be revised as follows:

Authentication protocol (Only MD5, SHA, and NONE are supported. NONE is the default.)

Unclear description of LOOPBACKADDRESS value in the configuration guide

(CQ 373626) Page 2-10 of the *EMC Smarts IP Management Suite Configuration Guide* contains an unclear description of the LOOPBACKADDRESS value for the AccessAddressFormat parameter in the discovery.conf file.

The existing text currently states:

> LOOPBACKADDRESS means that the discovery process uses the loopback address for both ICMP and SNMP for monitoring and discovery. (MIB-II ifType 24). Note that discovery cannot determine the loopback address until after the system has been discovered.
>
> If a qualified IP address is not found, the last known SNMP address is used and a DiscoveryError is notified. The DiscoveryError contains the message: Qualified access address not found.

The text should state:

> LOOPBACKADDRESS means that the discovery process uses the loopback address for both ICMP and SNMP for monitoring and *rediscovery.* (MIB-II ifType 24). Note that discovery cannot determine the loopback address until after the system has been discovered.
>
> If a qualified IP address is not found *during the initial discovery,* the last known SNMP address is used and a DiscoveryError is notified. The DiscoveryError contains the message: Qualified access address not found.

EnableIPSecDiscovery parameter is missing from documents

(CQ 293321) The EnableIPSecDiscovery parameter is missing from two guides:

- Page 2-20 of the *EMC Smarts IP Management Suite Discovery Guide* describes short discovery for IPSec tunnels, including how to set the discovery interval. It does not describe how to enable discovery for IPSec devices.

- Page 2-12 of the *EMC Smarts IP Management Suite Configuration Guide*, Table 2-4, lists the parameters for the tpmgr-params.conf file. The parameter for enabling IPSec discovery, EnableIPSecDiscovery, is missing.

The correct text for the *EMC Smarts IP Management Suite Discovery Guide*

To enable short discovery for IPSec tunnels, perform these steps:

1. Go to the BASEDIR/smarts/bin directory in the IP Management Suite installation area and use the following command to open the tpmgr-param.conf file.

   ```
   sm_edit conf/discovery/tpmgr-param.conf
   ```

2. In the tpmgr-param.conf file, set the EnableIPSecDiscovery to TRUE.
3. Save the tpmgr-param.conf file. The modified version of the file is saved to the BASEDIR/smarts/local/conf/discovery directory.
4. If IP Availability Manager was running before you edited the tpmgr-param.conf file, restart IP Availability Manager.

The correct text for Table 2-4 of the *EMC Smarts IP Management Suite Configuration Guide*

Parameter	Value	Description
EnableIPSecDiscovery	TRUE FALSE Default: FALSE	Enables or disables short discovery for IPSec tunnels: • A value of TRUE enables short discovery. • A value of FALSE disables short discovery. Short discovery for tunnels is described in the *EMC Smarts IP Management Suite Discovery Guide*.

Minor heading correction in discovery guide

(CQ 302117) Page 3-5 of the *EMC Smarts IP Management Suite Discovery Guide* contains a minor typographical error in the section heading. The heading should read: “TM_USESEEDNAME option for seed-file name resolution.”

Overview table for the local name resolution exceptions for the discovery guide

(CQ 306911, CQ 306874) Page 3-5 of the *EMC Smarts IP Management Suite Discovery Guide* contains a table named "Overview of local name resolution exceptions for individual systems in a seed file", which will be revised as shown in Table 14 on page 70.

Table 14 Overview of local name resolution exceptions for individual systems in a seed file

Automatic name resolution (when you enter NameFormat = "TM_USEAUTONAME" in name-resolver.conf file)	**Seed-name name resolution** (when you enter NameFormat = "TM_USESEEDNAME" in name-resolver.conf file)
Individual automatic name resolution exception using a prioritized list of naming sources: Not applicable	Individual automatic name resolution exception that uses a prioritized list of naming sources: • NAMEFORMAT=TM_USEAUTONAME The resolution process is performed in accordance to the naming source order (0 through 4) specified by the AutoNameOrder entries in the name-resolver.conf file. The default order is: • AutoNameOrder 0 TM_USELOOPBACK • AutoNameOrder 1 TM_USESYSNAME • AutoNameOrder 2 TM_USENONPRIVATEIP • AutoNameOrder 3 TM_USEPRIVATEIP • AutoNameOrder 4 TM_USEAGENTADDRESS If you prefer a different naming source order, edit the name-resolver.conf file and change the AutoNameOrder numbers.
Individual automatic name resolution exceptions using an individual naming source: • NAMEFORMAT=TM_USELOOPBACK • NAMEFORMAT=TM_USESYSNAME • NAMEFORMAT=TM_USENONPRIVATEIP • NAMEFORMAT=TM_USEPRIVATEIP • NAMEFORMAT=TM_USEAGENTADDRESS	Individual automatic name resolution exceptions that use an individual naming source: • NAMEFORMAT=TM_USELOOPBACK • NAMEFORMAT=TM_USESYSNAME • NAMEFORMAT=TM_USENONPRIVATEIP • NAMEFORMAT=TM_USEPRIVATEIP • NAMEFORMAT=TM_USEAGENTADDRESS
Individual seed filename resolution exception that specifies a specific name: • NAMEFORMAT=TM_USESEEDNAME SEEDNAME=<user-specified name>	Individual seed filename resolution exception that specifies a particular name: Not applicable

Missing step in the discovery guide

(CQ 306911, CQ 306885) Page 3-10 of the *EMC Smarts IP Management Suite Discovery Guide* contains a procedure named *Configuring exceptions to seed-name name resolution*, which will be revised to include the following step right after step 1:

> Define the naming source for the system as TM_USEAUTONAME by inserting the following in the seed file entry:
>
> ```
> NAMEFORMAT=TM_USEAUTONAME
> ```
>
> For example:
>
> ```
> 192.168.12.2 NAMEFORMAT=TM_USEAUTONAME
> ```

Correction in extended filter information for the discovery guide

(CQ 282200, CQ 286644) Page 7-5 of the *EMC Smarts IP Management Suite Discovery Guide* contains the following information relevant to extended options:

Access Mode determines what protocols are used to both discover and monitor the system and its components. Valid values for autodiscovery are ICMPSNMP and ICMPONLY. The default is ICMPSNMP, meaning that both ICMP and SNMP protocols are used to discover and manage the system. When ICMPONLY is selected, discovery does not send SNMP polls to the system and cannot, therefore, discover the system and its components. Instead, the system is added to the topology as a host and is monitored only for connectivity.

The text should state:

Access Mode determines what protocols are used to both discover and monitor the system and its components. Valid values for autodiscovery are ICMPSNMP and ICMPONLY. The default is ICMPSNMP, meaning that both ICMP and SNMP protocols are used to discover and manage the system. When ICMPONLY is selected, discovery does not send SNMP polls to the system and cannot, therefore, discover the system and its components. Instead, the system is added to the topology as a host (and the system's SNMP agent is added to the topology as an SNMPAgent). The host is monitored only for connectivity.

Filename correction for the discovery guide

(CQ 286402) Page 9-2 of the *EMC Smarts IP Management Suite Discovery Guide* mentions an incorrect filename in the section Certifying non-network systems.

The existing text currently states:

Editing oid2Type_Field.conf

To certify non-network systems:

1. Go to the BASEDIR/smarts/bin directory in the IP Management Suite installation area and use the following command to open the oid2Type_Field.conf file.

   `sm_edit conf/discovery/oid2Type_Field.conf`

The text should state:

`Editing oid2type_Field.conf`

To certify non-network systems:

1. Go to the BASEDIR/smarts/bin directory in the IP Management Suite installation area and use the following command to open the oid2type_Field.conf file.

   `sm_edit conf/discovery/oid2type_Field.conf`

Incorrect range of values for SM_BACKUP_FILE_LIMIT parameter in the system administration guide

(CQ 302946) Page A-15 of the *EMC Smarts System Administration Guide* mentions an incorrect range of values for the SM_BACKUP_FILE_LIMIT parameter.

The existing text currently states:

> Valid values are 0 through 99. The default value is 3.

The text should state:

> Valid values are 0 through 999. The default value is 3.

Invalid wildcard character description in the system administration guide

(CQ 302948) Page B-2 of the *EMC Smarts System Administration Guide* contains an error in Table B-1, the Wildcard table. The table row describing the \\ wildcard character should be removed.

Technical notes

Perform discovery upon device removal

CQ 563683

If a device is removed from the application, it is necessary to perform a rediscovery of any device in the topology or add a new device. If rediscovery is not done, there might be problems with root cause analysis.

When a device is deleted, devices get separated based on the topology. As part of rediscovery, post-processing creates the partitions based on the new topology.

Set up trap filtering to avoid domain crashes

CQ 527096

Large numbers of traps may be sent by network devices, but typically only a small subset are important to network operators. For example, link up and down traps are sent frequently by devices. However, these traps are not important to the network operator since the IP Availability Manager already supplies authentic, root-cause problems related to these traps.

To prevent crashes due to trap storms and a growing queue size, use the following settings in the smarts/conf/trapd/trapd.conf file:

Table 15 Parameters in the trapd.conf file

Parameter	Description	Value
QUEUE_LIMIT_MEGS	The allowable size of the queue before the process of discarding begins for traps from chatty sources.	• Default: 0 (No limit) • Recommended value: 100
QUEUE_LIMIT_SECONDS	The amount of time the traps can remain in the queue before being discarded.	• Default: 0 (No limit) • Recommended value: 60

Alternatively, you can use the dmctl utility to set the required filtering parameters as follows:

- dmctl -s put SNMP_TrapManager::<trap manager instance>::MegabytesInQueue 100
- dmctl -s put SNMP_TrapManager::<trap manager instance>::SecondsInQueue 60

Note: Setting values for these parameters could result in the dropping of some traps and slowing down the root-cause analysis as the server has to poll for the lost or dropped traps.

Documentation

Documents are updated periodically. Electronic versions of the updated manuals are available on Powerlink at:

Home > Support > Technical Documentation and Advisories > Software ~ E-I ~ Documentation > Ionix Family > Ionix for IT Operations Intelligence > Ionix IP Management Suite.

EMC Smarts documentation

The documents in Table 16 on page 74 are relevant to users of all EMC Smarts products.

Table 16 EMC Smarts products documentation (page 1 of 2)

Part number	Revision	Item
300-004-100	A01	*EMC Smarts Documentation Catalog*
300-003-954	A01	*EMC Smarts ICIM Reference 1.5*
300-004-103	A01	*EMC Smarts Common Information Model Infrastructure Models Chart*
300-004-102	A01	*EMC Smarts Common Information Model Application•Business Models Chart*
300-003-966	A01	*EMC Smarts ASL Reference Guide*
300-003-969	A01	*EMC Smarts Perl Reference Guide*
300-004-101	A01	*EMC Smarts System Administration Guide*

Table 16 EMC Smarts products documentation (page 2 of 2)

Part number	Revision	Item
300-003-967	A01	*EMC Smarts Dynamic Modeling Tutorial* (distributed with IP and SAM only)
300-003-968	A01	*EMC Smarts MODEL Reference Guide* (distributed with IP and SAM only)
N/A	10.1	*FLEXnet Licensing End User Guide*

EMC Smarts IP Management Suite documentation

The documents in Table 17 on page 75 are relevant to users of the Ionix IP Management Suite.

Table 17 Ionix IP Management Suite documentation (page 1 of 2)

Part number	Revision	Item
300-004-060	A01	*EMC Smarts 7.0 Quick Start Guide*
300-004-083	A02	*EMC Smarts IP Management Suite 7.0 Third-Party Copyright Read Me*
300-004-041	A01	*EMC Smarts IP Management Suite Release Notes*
300-011-427	A02	*EMC Ionix IP Management Suite 7.0 Service Pack 4 Release Notes* [a]
300-011-534	A01	*EMC Ionix IP Management Suite 7.0.4 Powerlink and Documentation Updates* [a]
300-004-282	A01	*EMC Smarts IP Management Suite Migration Guide*
300-004-085	A01	*EMC Smarts IP Management Suite Deployment Guide*
300-004-086	A03	*EMC Smarts IP Management Suite Configuration Guide*
300-004-087	A02	*EMC Smarts IP Management Suite Discovery Guide*
300-004-088	A02	*EMC Smarts IP Availability Manager User Guide*
300-004-089	A02	*EMC Smarts IP Performance Manager and Server Performance Manager User Guide*
300-004-090	A01	*EMC Smarts IP Adapters User Guide*

Table 17 Ionix IP Management Suite documentation (page 2 of 2)

Part number	Revision	Item
300-004-095	A01	*EMC Smarts IP Availability Manager Extension for IPv6 User's Guide*
300-004-106	A01	*EMC Smarts IP Availability Manager Extension for NAS User Guide*
300-011- 426	A01	*EMC Ionix IP Management Suite Installation Guide* [a]
300-011- 428	A01	*EMC Ionix IP Certification Matrix for 7.0.4* (xls file) [a]

a. Document was updated for the 7.0.4 release.

Software media, organization, and files

This section lists the individual products in the Ionix IP Management Suite and gives instructions to download this service pack.

- "Ionix IP Management Suite products" on page 77
- "Downloading service pack software" on page 77

Ionix IP Management Suite products

The Ionix IP Management Suite includes the following products:

- IP Availability Manager
- IP Performance Manager
- IP Server Performance Manager
- IP Discovery Manager
- EMC Smarts Adapter for IBM/Tivoli NetView
- EMC Smarts Adapter for HP OpenView NNM
- IP Availability Manager Extension for IPv6
- IP Availability Manager Extension for NAS

You must acquire the appropriate IP Management Suite 7.0 feature licenses in order to use these products. To obtain or update your IP Management Suite product licenses, contact smartslicensing@EMC.com with your request.

You must select the correct executable for your operating system when installing the suite. Or, you can download Service Pack 4 from Powerlink and use it to install both the IP Management Suite and the service pack.

Downloading service pack software

Service packs are available from the EMC Powerlink website. To access the website, you need a Powerlink username and password.

Before you can download software such as product suites, service packs, and patches, you must have a valid support agreement, according to your purchase order (PO), and you need to register your site.

Registering your site

To register your site:

1. In your Web browser, access the Powerlink website:

   http://Powerlink.EMC.com

2. Enter your Powerlink username and password.
3. Select **Support > Product Registration and License Keys > Register your Software Sites**.
4. Type your site numbers (IDs) and click **Submit**. (Use a space to separate each site ID.)

EMC Corporation will send you an email within two business days, notifying you about your registration status and whether you are granted permission to download software. For more information about registering your site, go to the Powerlink website and reference Knowledgebase Solution "emc116045".

Downloading a service pack

To download the service pack:

1. In your Web browser, access the Powerlink website:

   http://Powerlink.EMC.com

2. Enter your Powerlink username and password.
3. On the Powerlink page, select **Support > Software Downloads and Licensing > Downloads E-I > Ionix IP Management Suite**.

   If EMC Smarts product suites are not displayed and you registered your site, you might not have a valid support agreement. For assistance, send an email to the Powerlink Registration Group at esds@EMC.com.

4. Select the latest service pack for the version of your IP Management Suite and your operating system.
5. Save the file to a directory where you typically store patches. You can copy the service pack to the *BASEDIR* directory for your product suite.

Troubleshooting and getting help

EMC support, product, and licensing information can be obtained as follows.

Product information — For documentation, release notes, software updates, or for information about EMC products, licensing, and service, go to the Powerlink website (registration required) at:

http://Powerlink.EMC.com

Technical support — For technical support, go to EMC Customer Service on Powerlink. To open a service request through Powerlink, you must have a valid support agreement. Please contact your EMC sales representative for details about obtaining a valid support agreement or to answer any questions about your account.

Copyright © 2010 EMC Corporation. All rights reserved.

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

For the most up-to-date listing of EMC product names, see EMC Corporation Trademarks on EMC.com. All other trademarks used herein are the property of their respective owners.