Focal Point™ 3.0 Management Application

for

ION System & Point System
Chassis and Standalones

Serial Number: 3245

Cabinet Description: ION Chassis

Device Model: ION219

Focal Point 3.0 Management Application
Version: Alpha release revision 3.0.3

Copyright © 2002 - 2011 Transition Networks, Inc
All Rights Reserved

http://www.transition.com
Tel 1-800-526-9267, 1-952-941-7600 Fax 952-941-2322

User Guide

33293 Rev E

Trademarks

Copyright Notice/Restrictions

Printed in the U.S.A.

Focal Point™ 3.0 Management Application User Guide for the ION System & PointSystem Chassis and Standalones, PN 33293 Rev E

Contact Information

Transition Networks
10900 Red Circle Drive
Minnetonka, MN 55343 USA
Tel: 952- 941-7600 or 1-800-526-9267
Fax: 952-941-2322

Revision History

Rev	Date	Description
A	03/02/04	First release.
B	01/25/07	Revised for FP software version 2.1.
C	06/12/09	Revised for FP software version 2.2.
D	12/06/11	Revised for Focal Point™ 3.0.1.
E	04/19/12	Revised for Focal Point™ 3.0.3 which adds 1) ION hardware support. 2) SNMP V3 support. 3) New Trap Server. 4) New PS and ION cards (PS 10G CTGFF, 4xT1). 5) Fixes for bugs found in FP2.2. 6) IP Discovery status. 7) Auto refresh function. Clarified "Discovery" procedure 10/03/12.

Table of Contents

Figures

Chapter 1 - Introduction

About Focal Point

Transition Networks' Focal Point management software is an implementation of SNMP that installs on a networked computer to provide a graphical user interface (GUI) to monitor the ION System and/or Point System chassis and related modules. The Focal Point management software GUI lets an administrator monitor and control an ION System and/or Point System chassis and related modules from a remote NMS.

The FP 3.0 application works in both ION and Point System (PS) environments:

- Point System (PS) chassis and cards
- ION chassis (Chassis II) and cards
- Point System card(s) in an ION chassis with IONADP adapter

About this Manual

This manual explains how to set up Transition Networks' (TN) Focal Point (FP) management software to monitor and manage one or more Point System chassis, or ION system chassis populated with TN slide-in cards (SICs), or ION standalone devices.

This manual includes a table of contents, five chapters, three appendixes, a glossary, and an index.

Related Documents and Online Help

A printed documentation card is shipped with each ION device. Context-sensitive Help screens and cursor-over-help (COH) facilities are built into the Web interface. A substantial set of technical documents, white papers, case studies, etc. are available on the Transition Networks web site at www.transition.com. Note that this manual provides links to third part web sites for which Transition Networks is not responsible.

ION System and related manuals are listed below.

1. FocalPoint 3.0 User Guide, 33293 (this manual)
2. ION System x323x Remotely Managed NID User Guide, 33342
3. ION Management Module (IONMM) User Guide, 33457
4. ION Systems CLI Reference Manual, 33461
5. ION219-A 19-Slot Chassis Installation Guide, 33412
6. ION System Release Notes (software version specific)
7. TN Product Support Postcard, 33504

Point System and related manuals are listed below.

1. CPSMC0100-210 User's Guide, 33305
2. CPSMC19xx-100 User's Guide, 33242
3. CPSMC08xx-100 User's Guide, 33270
4. CPSMM-200-210 User's Guide, 33189
5. CETTF10xx-105 User's Guide, 33204
6. CFETF10xx-105 User's Guide, 33205
7. CFBRM10xx-1xx & SFBRM10xx-1xx Quick Reference Guide, 33345
8. CRS4Fxxxx-10x User's Guide, 33280

Note: Information in this document is subject to change without notice. All information was deemed accurate and complete at the time of publication. This manual documents the latest software/firmware version. While all screen examples may not display the latest version number, all of the descriptions and procedures reflect the latest software/firmware version, noted in the Revision History on page 2.

About the Point System

A Point System can include the following products:

- Point System chassis (single, dual, 8, 13, 18 or 19 slot)
- Point System slide-in cards
- Point System Management modules
- Focal Point 3.x management software (see www.transition.com for current version)
- Point System power supply module
- Point System accessories

Visit www.transition.com and the related documents for complete details on Point System chassis products.

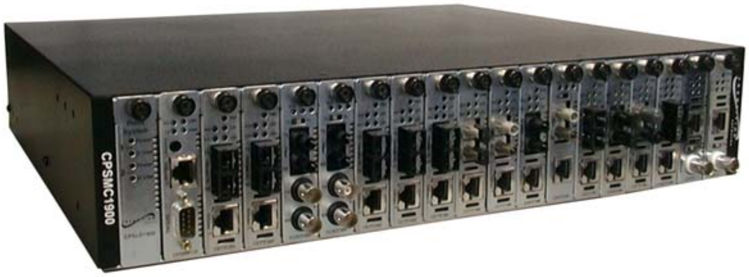


Figure 1: Point System™ Chassis

About the ION System

An ION System can include the following products:

- ION System chassis
- ION System slide-in cards (SICs)
- ION System standalone cards
- ION Management Module (IONMM)
- Focal Point 3.x Management software (see www.transition.com for current version)
- ION System power supply module(s)
- ION System accessories

Visit www.transition.com and the related documents for complete details on ION System chassis products.

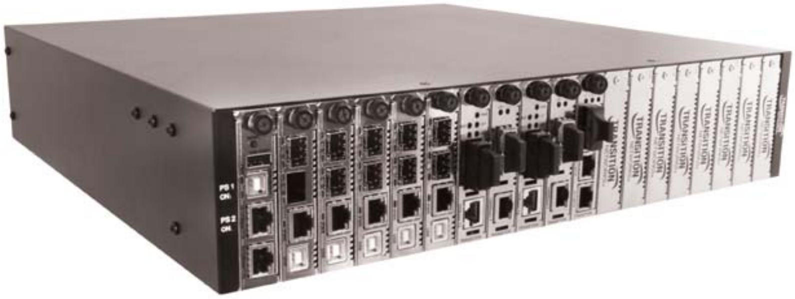


Figure 2: ION System™ Chassis

CPSMM100-xxx Firmware Overview

See the TN web site at www.transition.com for current CPSMM100-xxx version, location, module and firmware PNs, Firmware contents, and PS Cabinets/Devices supported.

Focal Point Management Software Overview

Focal Point description: Transition Networks' Focal Point management software is an implementation of SNMP that installs on a networked computer to provide a graphical user interface (GUI) to monitor the Point System or ION System chassis and its slide-in cards and standalone NIDs.

Management methods: In a network that includes one or more management module(s), the administrator can monitor and manage the Point System / ION System chassis and its individual slide-in cards via:

- A CLI at an attached terminal
- A CLI at a remote Telnet connection
- A remote Web browser
- SNMP software, such as TN Focal Point management software, installed on a remote PC or workstation

Features: The Focal Point software includes these features:

- Graphical user interface (GUI) tools:
  - Trap Server tool
  - Trap Viewer tool
  - Transition Agents Discovery tool
  - Text Editor tool
  - System Monitor tool
- Status monitoring
- Enable/disable converter features
- One-click telnet
- Rules for Alerts via beep, email, hints, and/or process group control string
- SMTP server support (authenticated and non-authenticated)
- Authentication (SHA and MD5) and Privacy (DES and AES) protocol support

The integrated Trap Receiver has the following features:

- Receive all traps - including traps from third party devices
- Display all traps on console
- Log all traps to disk
- Convert traps to email messages
- Send emails, audio alert beep, etc. on detection of traps
- All features configurable

Simple Network Management Protocol (SNMP) Overview

SNMP definition: SNMP is a request-response protocol that defines network communication between a managed device and a PC or workstation.

How is SNMP managed? SNMP is anything but simple. The good news is that the details of SNMP are managed very well by Transition Networks management module firmware and the Focal Point management software. A more lengthy and detailed explanation of SNMP can be found at www.transition.com/pshelp/snmp.html.

SNMP terms: The following terms will help enable a better understanding of SNMP.

Managed Device - A managed device is a hardware unit with embedded firmware connected to a Point System network with SNMP management capabilities. An example of a managed device is Transition Networks' 19-slot chassis with an installed management module and one or more installed slide-in cards shown in Figure 1 in the "About Focal Point" section on page 6.

Management Information Base (MIB) - The MIB is a set of variables used to monitor and control a managed device.

Managed Object or ***MIB variable*** - The individual variables that make up the MIB are called managed objects or MIB variables. These variables are the individual features of the managed device. The administrator can use these variables to monitor and configure the managed device. For example, a slide-in card from Transition Networks can have up to 20 or more managed objects (MIB variables) associated with it. Some examples are:

- Power ON/OFF the slide-in card
- Enable the AutoCross feature
- Display activity on the fiber link, etc.

SNMP Operations: SNMP v1 has four defined operations. These operations allow the administrator to monitor and control a managed device from a remote location. The four operations are the following:

GET and ***GET-NEXT*** - To monitor (or read) the managed device, the administrator initiates, through the user interface to the network management software, the GET and GET-NEXT operations. This is done on selected called instances of managed objects (variables) in the MIB of the managed device.

SET - To control (or write) the managed device, the administrator initiates, via the user interface to the NMS software on a PC or laptop, the SET operation on selected instances of managed objects in the MIB of the managed device.

TRAP - To alert the administrator about instances of MIB-defined asynchronous events on the managed device, the SNMP agent initiates the TRAP operation through the user interface to the network management application on a PC or Laptop.

SNMP v3 operations also include the ***Get Bulk*** operation.

Chapter 2 - Installation

Introduction

This chapter covers the setup and installation of Transition Networks' Focal Point management software that allows the administrator to monitor and control a Point System or ION System chassis and its slide-in cards from a remote PC or workstation.

FP 3.0 Environments

The FP 3.0 application supports:

- Point System (PS) chassis and cards
- ION chassis (Chassis II) and cards
- Point System card(s) in an ION chassis (with IONADP adapter)

Point System Hardware Setup

The Point System hardware setup begins with one or more Transition Networks' management modules (CPSMM-200 or CPSMM-120) installed in one or more Transition Networks' Point System™ chassis:

- CPSMC0200-2xx 2-slot chassis
- CPSMC0800-100 8-slot chassis
- CPSMC13xx-100 13-slot chassis
- CPSMC18xx-xxx 18-slot chassis
- CPSMC19xx-100 19-slot chassis

Next, connect the management module via an Ethernet port to a TCP/IP network that is accessible via IP from a PC or Laptop. See the figure below.

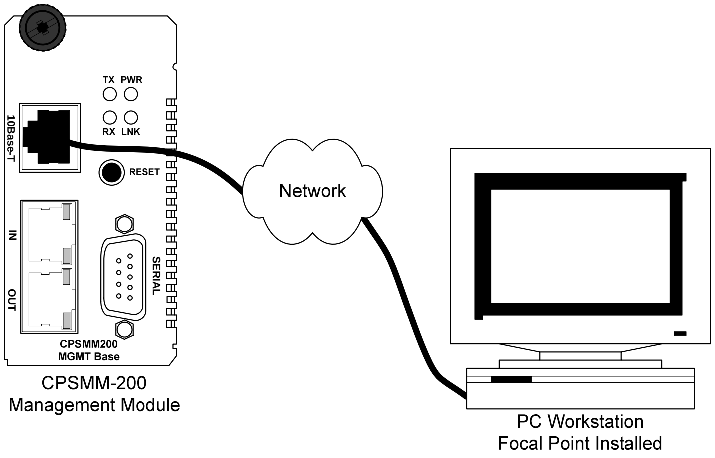


Figure 3: CPSMM-200 Management via PC with Focal Point Software Installed

ION System Hardware Setup

The ION System hardware setup begins with a Transition Networks' IONMM management module installed in a Transition Networks' ION System chassis. Refer to the ION system documentation for hardware installation information.

Each slide-in module for the ION Chassis has specific features and functions that can be controlled via the IONMM. A network administrator can configure, monitor and troubleshoot ION modules remotely via the IONMM. Remote access to management information helps reduce operating expenses by reducing technician dispatches and lowering the mean-time-to-repair by proactively looking for potential issues and receiving detailed SNMP traps if a problem occurs.

A simple ION System configuration is shown in the figure below.

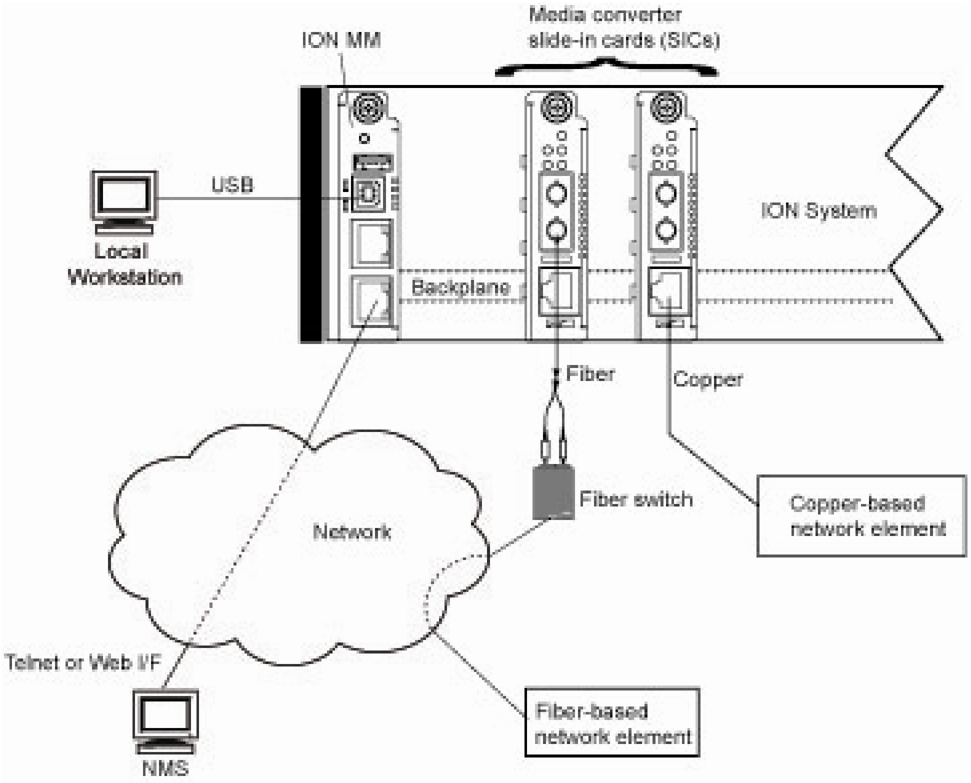


Figure 4: Sample ION System Configuration

Focal Point Software Installation

This section provides the procedures to install the Focal Point software on a Windows PC.

The Focal Point 3.0 software is free of charge to users with any TN Chassis or Management card purchase.
You can download FP 3.0 from http://www.transition.com/focalpoint/ (registration required).

FP 3.0 can only run one instance at a time on one management platform (PC, laptop, workstation).
If you want to restart FP 3.0, stop the first FP 3.0 instance. Otherwise a second FP 3.0 instance cannot start up. Note that Point System can only use SNMP v1.

Downloading Focal Point 3.0

1. Go to the TN web site at http://www.transition.com/focalpoint/.
2. Register, and then click on the Download Focal Point 3.0 link.
3. At the **File Open** dialog box, click **Save**.
4. At the **Save As** dialog box, select a Save in location and verify the name of the file displayed in the **File name**: area.
5. Click the **Save** button. The **Focal Point 3.0 zip** file is saved to the specified location.
6. Continue to the applicable install procedure for your OS.

Operating Systems Supported

Focal Point supports the following software platforms:

- Microsoft Windows® 7, Windows 7 x64,
- Windows Server 2008, Windows 2000, Windows 2003 32 bit,
- Windows XP® 32 bit and Windows XP 64 bit.

JRE v 1.6 is included in the FP 3.0 installation, so Focal Point 3.0 can be installed without any Java™ Runtime Engine (JRE™) installed in the target machine before running FP 3.0 setup.

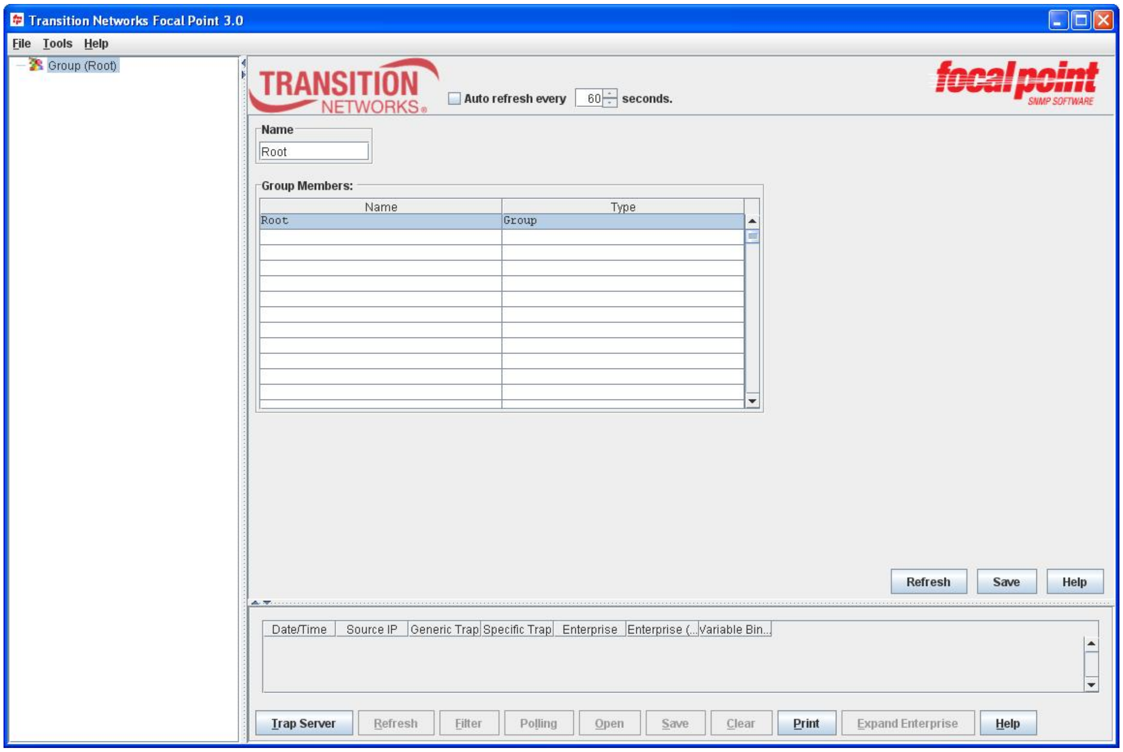
Windows XP Installation

To install the Focal Point 3.0 under Windows XP Service Pack 2 (SP2), or Service Pack 3 (SP3):

1. Double-click the *FocalPointApp* file in the download location (e.g., *C:\Program Files\FocalPoint3.0\bin*). The FP 3.0 banner displays with a series of *Loading* ... messages.

Loading plug-ins ...

2. When the loading is complete, the FP 3.0 main screen displays.



□ Auto refresh every 60 seconds.

Name: Root

Group Members:

Name	Type
Root	Group

Date/Time	Source IP	Generic Trap	Specific Trap	Enterprise	Enterprise (...	Variable Bin...

If a Windows Security Alert message displays (e.g., *Windows Firewall has blocked some features of this program*), click **OK** to clear the message, and continue the installation.

3. Review the "Focal Point Main Window pull-down menus" section below, and continue with FP 3.0 operation as discussed in the rest of this section.

Windows 7 Installation

Perform the steps below to install FP 3.0 in Windows 7 Starter, Home Premium, Professional, or Ultimate edition.

1. Log in to Windows 7 as "Administrator". For other login users, the installation path must NOT be under the default path (i.e. "C:\Program Files\...") and you must change to another path.
2. In your web browser, click the link to the program.
3. Do one of the following:

   To install the program immediately, click **Open** or **Run**, and then follow the instructions on your screen. If you're prompted for an administrator password or confirmation, type the password or provide confirmation.

   To install the program later, click **Save**, and then download the installation file to your computer. When you're ready to install the program, double-click the file, and then follow the instructions on your screen.

FP3.0 Installed in Default Location

Because of Windows 7 privilege control, if Focal Point is not installed in the default position “*C:\Program Files\FocalPoint3.0*”, it can run successfully. If Focal Point is installed in the default position, right-click on the short cut “Focal Point 3.0 Management Application”, and select “Run as Administrator” to start it.

Turn UAC Off

1. Open **User Account Control Settings** by clicking the **Start** button and then clicking **Control Panel**.

2. In the search box, type **uac**, and then click **Change User Account Control setting**s.

3. Turn UAC off. Move the slider to the **Never notify** position, and then click **OK**. If prompted for an administrator password or confirmation, type the password or provide confirmation.

4. Restart your computer to turn off UAC.

To turn UAC on, move the slider to choose when you want to be notified, and then click **OK**.
If prompted for an administrator password or confirmation, type the password or provide confirmation.

See also: http://msdn.microsoft.com/en-us/library/dd446675(v=ws.10).aspx
http://technet.microsoft.com/en-us/library/dd835564(WS.10).aspx
http://technet.microsoft.com/en-us/library/dd919180(WS.10).aspx

Chapter 3 - Operation

Introduction

This chapter covers FP 3.0 startup and operation. It assumes that the Chapter 2 installation process is complete.

Start the FP 3.0 Application in Windows

1. To start and run the FP 3.0 program after successful installation in Windows, either:

   a) Go to Windows **Start** > **All Programs** > **Transition Networks** > **Focal Point 3.0 Management Application**; the *Loading* ... messages display momentarily, and then the FP 3.0 Main screen displays.

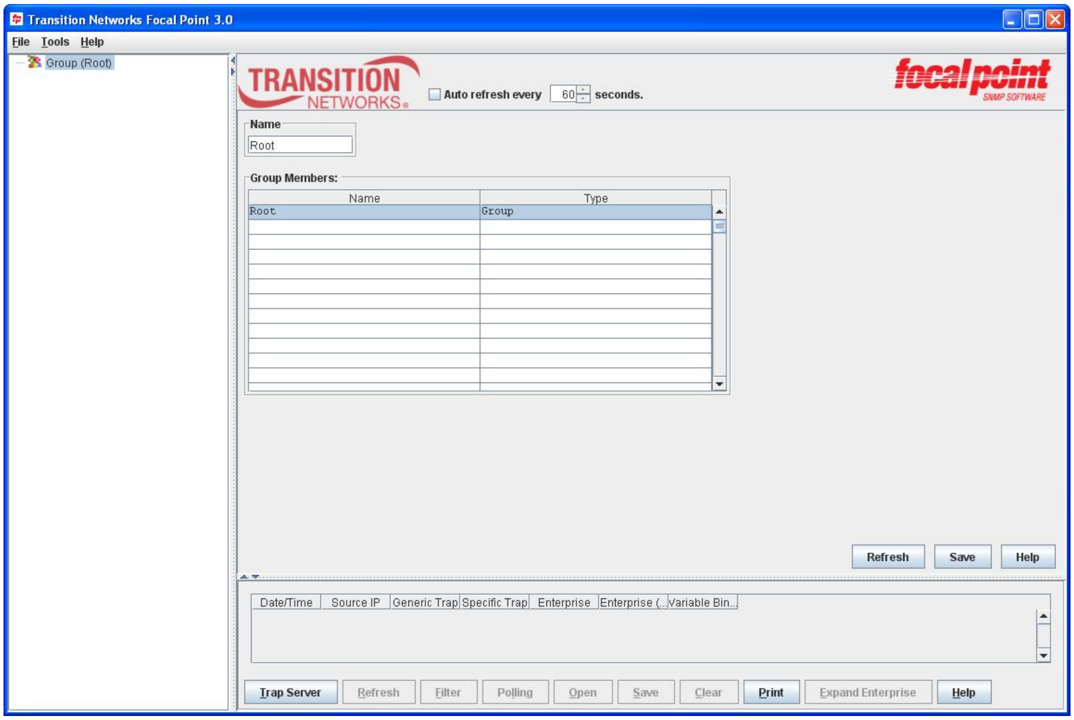
   <u>or</u>

   b) Go to the install location (e.g., *C:\Program Files|FocalPoint3.0\bin*) and double-click on **FocalPoint.bat**.
   The *Loading* ... messages display momentarily, and then the FP 3.0 Main screen displays.

   <u>or</u>

   c) Double-click the *FocalPointApp* file in the download location (e.g., *C:\Program Files\FocalPoint3.0\bin*). The FP 3.0 banner displays with a series of *Loading* ... messages.

   When the loading is complete, the FP 3.0 main screen displays.

   ☐ Auto refresh every 60 seconds.

   Name: Root

   Group Members:

Name	Type
Root	Group

Date/Time	Source IP	Generic Trap	Specific Trap	Enterprise	Enterprise (...	Variable Bin...

   If a Windows Security Alert message displays (e.g., *Windows Firewall has blocked some features of this program*), click **OK** to clear the message, and continue the installation.

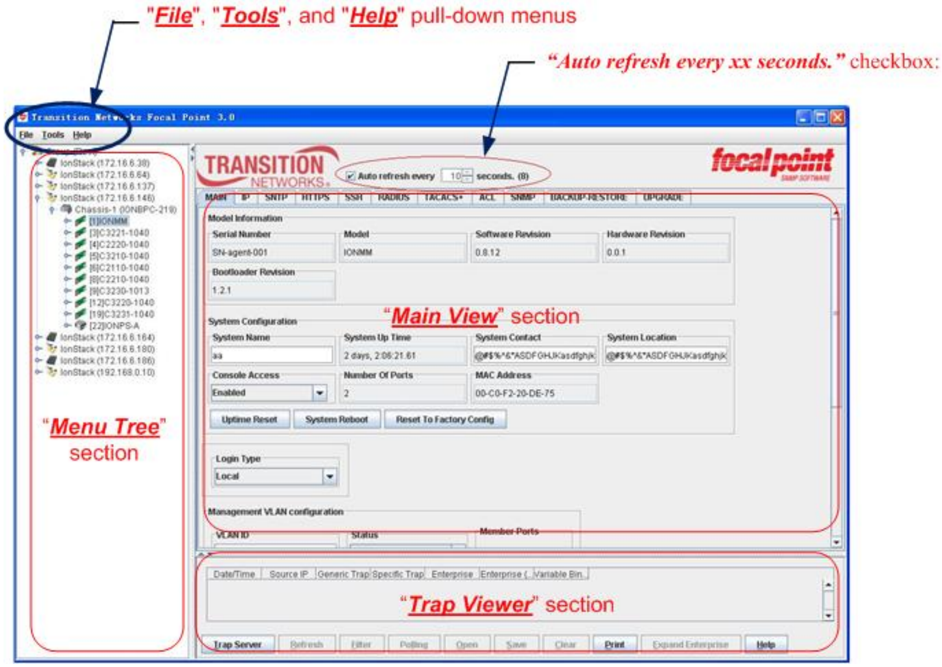
2. Review the "Focal Point Main Window Pull-down Menus" section below, and continue with FP 3.0 operation as discussed in the rest of this section.

<u>**Note**</u>: you can also start the FP 3.0 Trap Server application separately by double-clicking the TS icon.

Main Window Description

Focal Point Main Window Pull-down Menus and Sections

Click the Focal Point icon at the remote PC or Laptop and the Focal Point main window displays as shown below. The Focal Point main window is divided into three sections: ***Menu Tree***, ***Main View***, and ***Trap Viewer*** sections. The three pull-down menus are **File**, **Tools** and **Help**.



"File", "Tools", and "Help" pull-down menus

"Auto refresh every xx seconds." checkbox:

"Main View" section

"Menu Tree" section

"Trap Viewer" section

Transition Networks Focal Point 3.0

☑ Auto refresh every 10 seconds. (8)

Model Information

Serial Number: SN-agent-001

Model: IONMM

Software Revision: 0.8.12

Hardware Revision: 0.0.1

Bootloader Revision: 1.2.1

System Configuration

System Name: aa

System Up Time: 2 days, 2:06:21.61

System Contact: @#$%^&*ASDFGHJKasdfghjk

System Location: @#$%^&*ASDFGHJKasdfghjk

Console Access: Enabled

Number Of Ports: 2

MAC Address: 00-C0-F2-20-DE-75

Login Type: Local

Management VLAN configuration

Figure 5: Focal Point Main Window

Auto refresh every xx seconds Checkbox

If desired, check the **Auto refresh every xx seconds.** checkbox to have the current screen refreshed at the selected interval. The auto refresh function will take effect immediately. The default is auto refresh disabled and the selector set to 60 seconds. The valid range is 5 - 1000 seconds. The “count down” from the current setting displays in parenthesis next to the selector. The time interval value will not be saved. It will be reset to default value when the Focal Point is reopened.

File Pull-down Menu

On the 'File" pull-down menu "Exit" is the only item. Select **Exit** to close the Focal Point Main window.

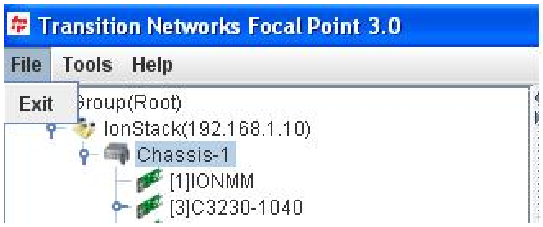


Figure 6: File Pull-Down Menu Item Exit

Tools Pull-down Menu

The 'Tools' pull-down menu items are **Trap Server**, **Text Editor**, **Initiate System**, **Discover Transition Agents..**. and **System Monitor**.

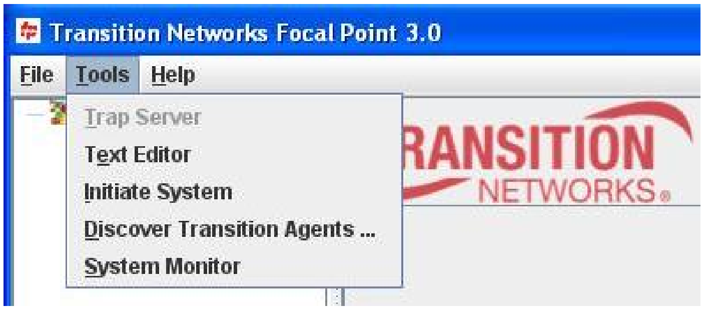


Figure 7: Tools Pull-Down Menu

The items on the "Tools" pull-down menu are explained below.

Trap Server: Select "**Trap Server…**" to pop open the Trap Server application and display the Transition Network icon (TN)in the bottom-right corner of the screen to show that the Trap Server application is running.
The Trap Server application collects and displays SNMP traps. It consists of a receiver component that listens for traps, and a viewer that displays them in a readable format.

Text Editor: Opens a simple text editor. Enter the text via the keyboard. It can be copied from one application (using the *Ctrl-C* keys), pasted to another application (using the *Ctrl-V* keys), and then saved by selecting File\Save from the text-editor menu bar. Only one such file can be saved at a time, so there is no need to name the file. When the Focal Point software closes, the information is saved. The information can be retrieved when Focal Point reopens.

Initiate System: Clears the local database of all stored information. **Note**: A confirmation message displays noting that the Initiate System function will delete all information in the system. If you are sure this is what you want to do, select **Yes**.

Discover Transition Agents: Locates (discovers) a chassis associated with a single IP address or a range of IP addresses. In IPv4, FP can discover a chassis in a range. For IPv6, FP can discover a single chassis. The text in light gray color ("IPv4/IPv6" or "IPv4") provides a hint as to what kind of IP address is supported to discover.

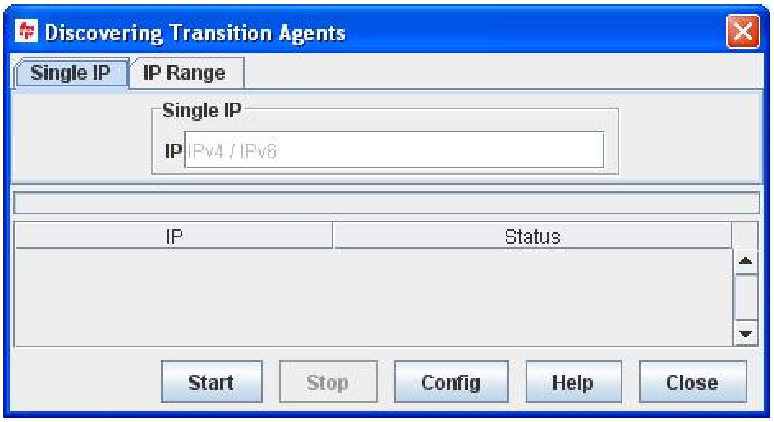


Figure 8: Discovering Transition Agents - Single IP (IPv4/IPv6)

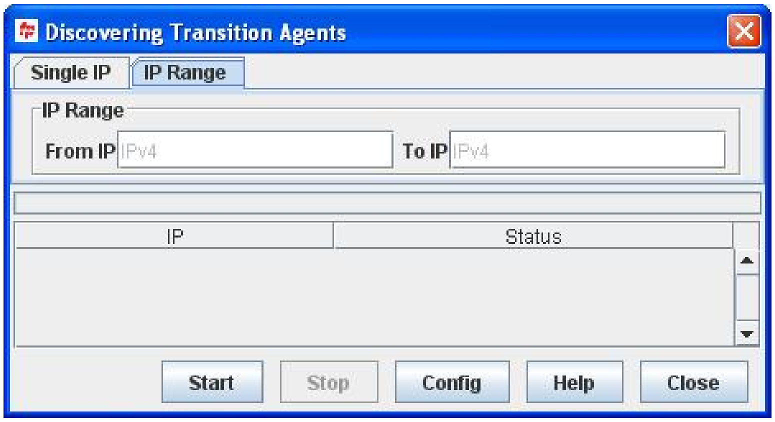
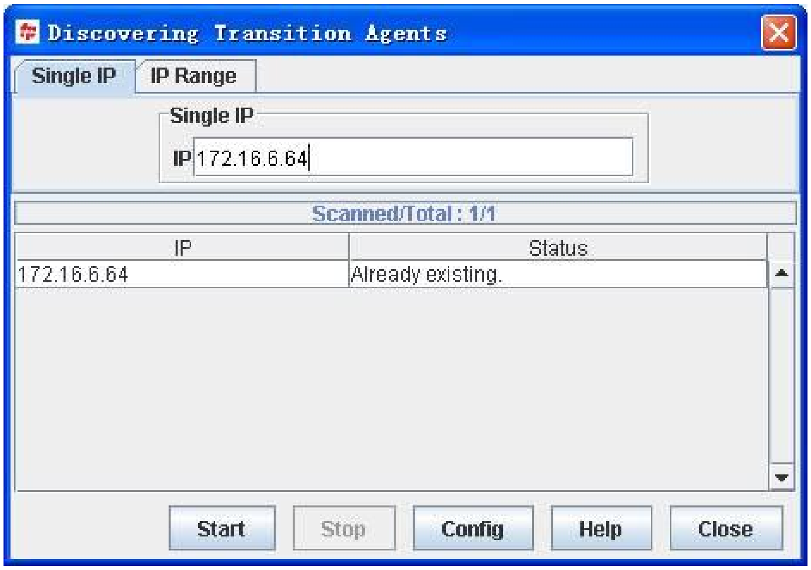


Figure 9: Discovering Transition Agents - IP Range (IPv4)

A table displays to show the discovery process status.



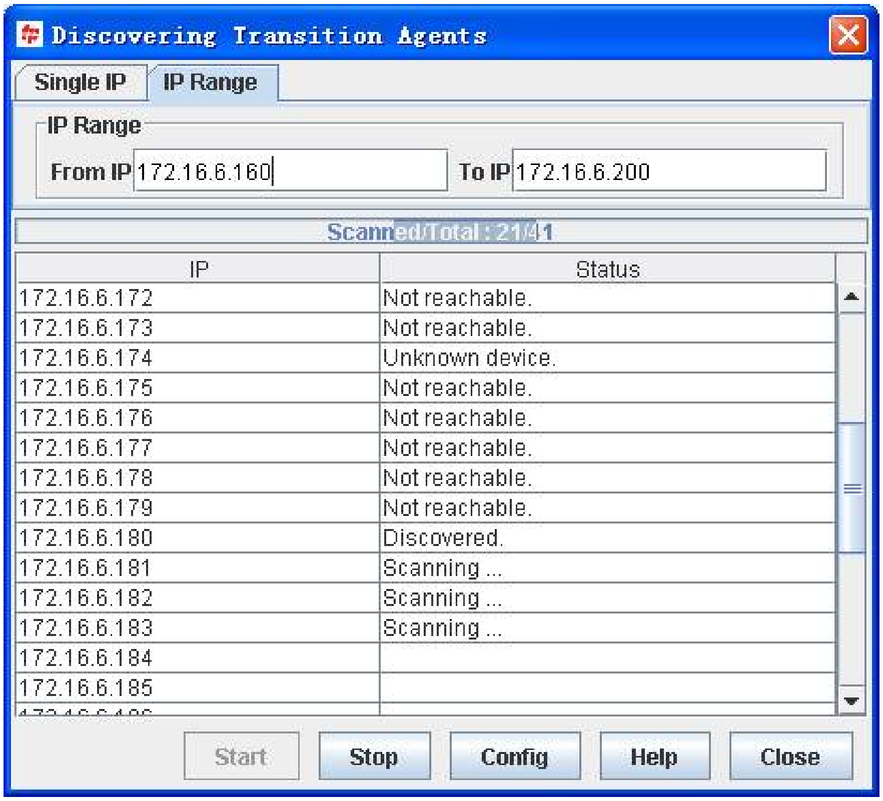
IP 172.16.6.64

Scanned/Total : 1/1

IP	Status
172.16.6.64	Already existing.

The following Discovery result statuses may display:

- *Scanning…*: To detect if the device is found.
- *Already existing*: If the device has already been discovered and is displayed on the tree view.
- *Not reachable*: The network is not reachable. Failed to ping.
- *Unknown device*: The network is reachable, but the destination is not an SNMP agent or not a recognized ION System or Point System device. May display if the SNMP version selected does not match the PointSystem's SNMP version.
- *Discovered*: An ION System or Point System device is found and is added to the tree view.
- *Timeout*: Timeout to detect the destination.



IP Range

From IP 172.16.6.160 To IP 172.16.6.200

Scanned/Total : 21/41

IP	Status
172.16.6.172	Not reachable.
172.16.6.173	Not reachable.
172.16.6.174	Unknown device.
172.16.6.175	Not reachable.
172.16.6.176	Not reachable.
172.16.6.177	Not reachable.
172.16.6.178	Not reachable.
172.16.6.179	Not reachable.
172.16.6.180	Discovered.
172.16.6.181	Scanning ...
172.16.6.182	Scanning ...
172.16.6.183	Scanning ...
172.16.6.184	
172.16.6.185	

System Monitor: Displays system monitor information for debugging purposes, typically by, or at the direction of, a TN tech support specialist. This function is only useful for the Point System devices.

The "**Poll Now**" button starts a polling process.

The "**Enable Polling / Disable Polling**" button alternately allows or disallows the polling process.

The "**Dump Detail**" button sends the polling details to the SnmpPolling log file on the PC's hard drive at *C:\Program Files\FocalPoint3.0\* (the default location). See "FP 3.0 Logs" on page 78.

The "***SNMP Packages***" area displays the IP address, Wait Set, Wait Get, and Sent data. In the sample System Monitor screen below, the "***SNMP Packages***" area displays **192.168.1.10: Wait Set: 0 Wait Get: 0 Sent: 0**.

The "***Polling Status***" area displays the stack name and IP address and chassis name and status information. In the sample System Monitor screen below, the "***Polling Status***" area displays:

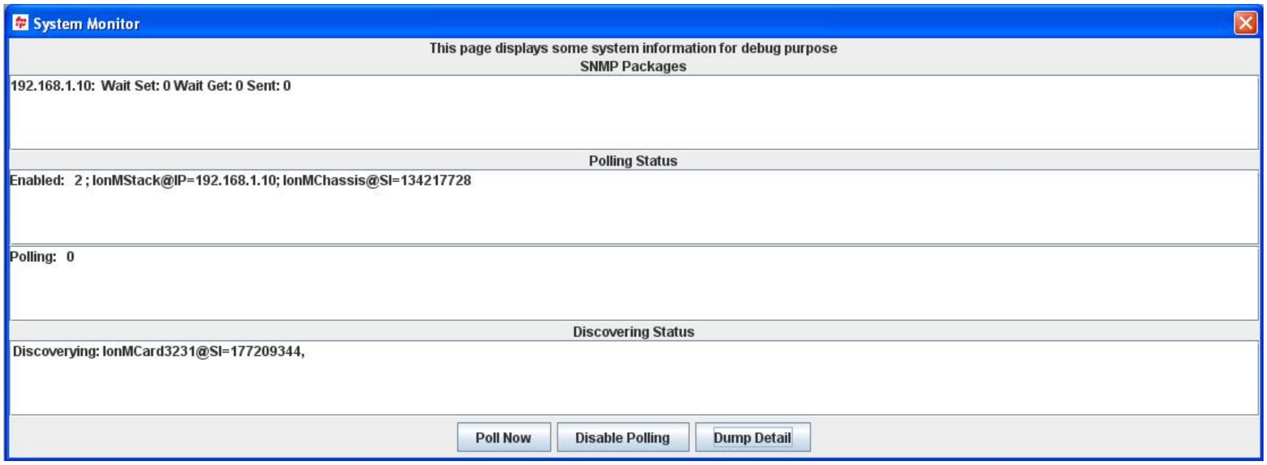
Enabled: 2; IonMStack@IP=192.168.1.10; **IonMChassis@SI-134217728**

where IP is the stack's IP address, and SI is the 'SNMP index' on agent side.

The "***Discovering Status***" area displays the Point System card information (card type and status information). In the sample System Monitor screen below, the "***Discovering Status***" area displays

Discovering: PS CardCGFEB@SI=177209344,

where "PS CardCGFEB" indicates a CGFEB card, and SI is the 'SNMP index' on the agent side.



This page displays some system information for debug purpose

```
192.168.1.10:  Wait Set: 0 Wait Get: 0 Sent: 0
```

```
Enabled:   2 ; IonMStack@IP=192.168.1.10; IonMChassis@SI=134217728
```

```
Polling:   0
```

```
Discoverying: IonMCard3231@SI=177209344,
```

Figure 10: System Monitor

Help Pull-down Menu

Main window ‘Help’ pull-down menu items are **Tech Support**, **Check Updates**, **Contents**, and **About**. See Figure 10.

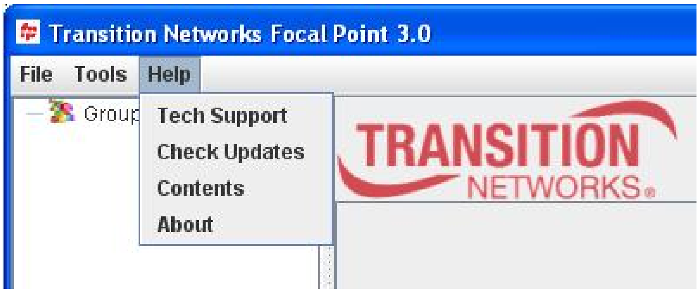


Figure 11: Help Pull-Down Menu

The ‘Help’ pull-down menu items are described below.

Tech Support: Displays Transition Networks’ contact Tech Support page.

Check Updates: Displays Transition Networks’ Software Update page, where the lasted versions of the software are available for downloading.

Contents: Opens the Web browser to the Focal Point help pages. These help pages were installed onto the computer’s hard drive when the application was installed. The files are current to the date the software was produced. For the most current Help files go to http://www.transition.com/pshelp/.

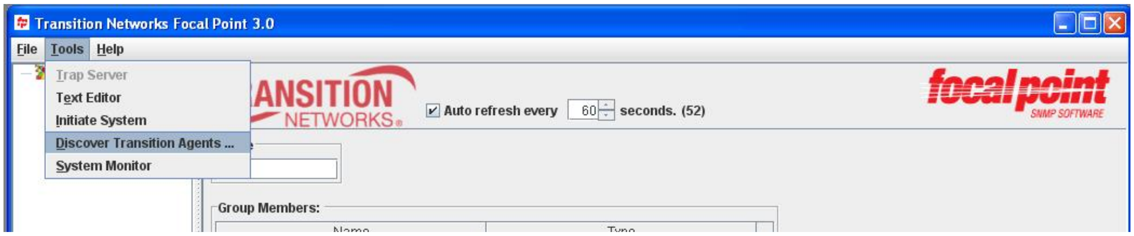
About: Lists the Focal Point software version, copyright, and contact information for Transition Networks.

Run the FP 3.0 Software

Accessing a Chassis via Focal Point

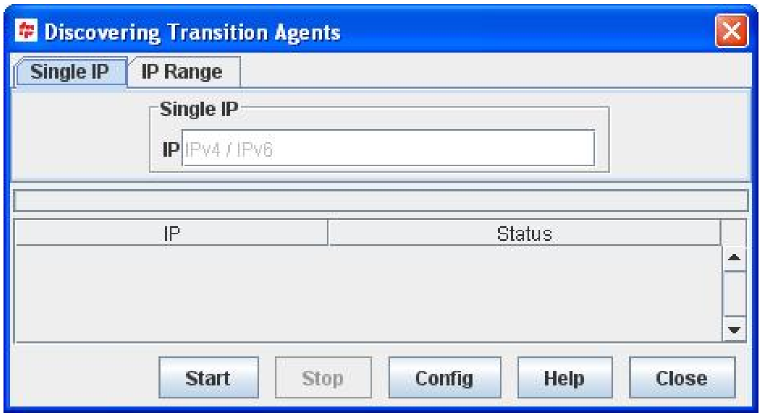
To access a Transition Networks' ION chassis on the network:

1. From the **Tools** pull-down menu select item "**Discover Transition Agents ...**" to launch the Discovering Transition Agents dialog box, shown below.



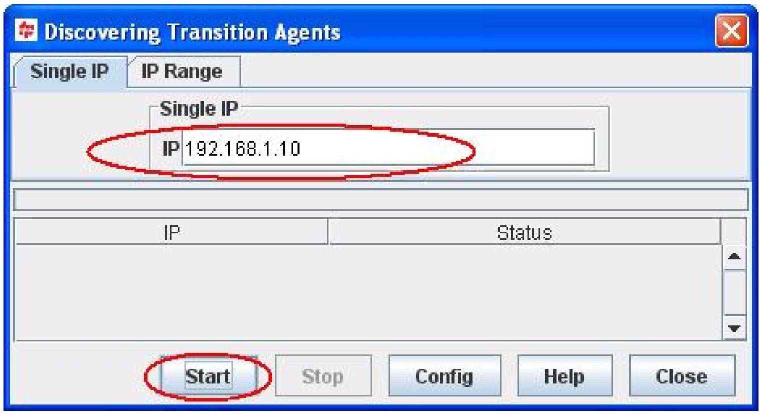
☑ Auto refresh every 60 seconds. (52)

The "Discovering Transition Agents" popup window displays.



2. If you are running SNMPv1 with PointSystem, click the **Config** button, and then click the **Save** button. If you are running SNMPv2c with the ION system, skip this step since SNMPv2c is the default setting for PointSystem.

3. Enter a single IPv4 or IPv6 address in the **IP** field, or select the "**IP Range**" tab and enter a range of IPv6 addresses to search / discover.

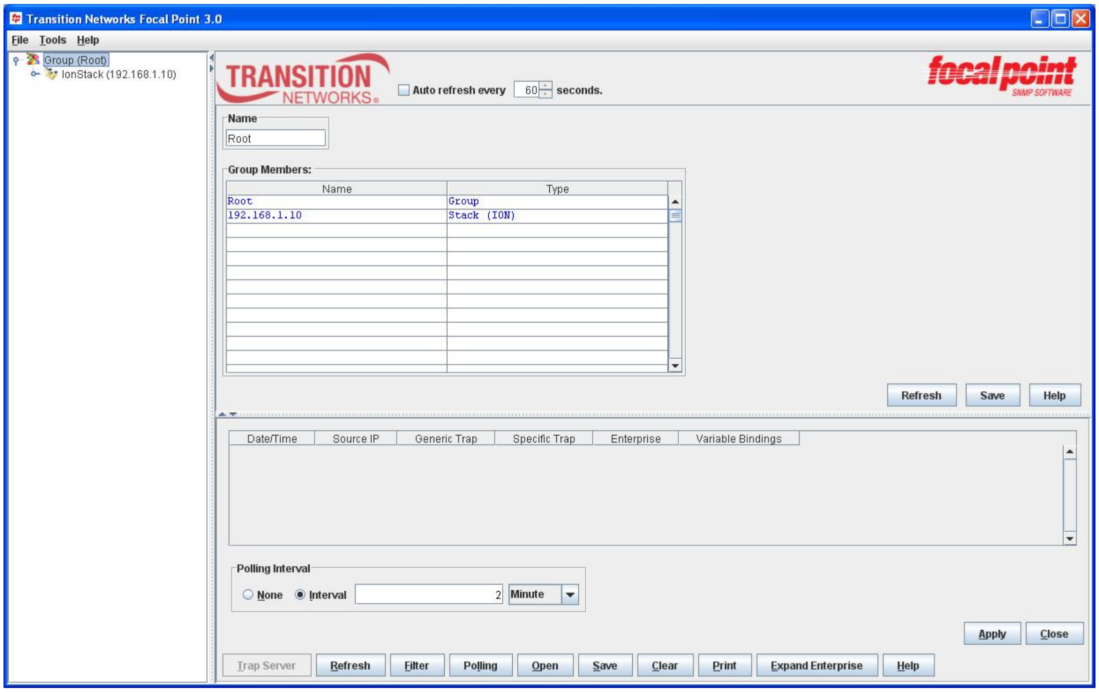


IP 192.168.1.10

Figure 12: Discovering Transition Agents Dialog Box

4. Click the **Start** button to access the stack associated with the IP address, as shown below.

5. Click the **Close** button on the “Discovering Transition Agents” popup window to display the “Main View” window shown below.



□ Auto refresh every 60 seconds.

Name: Root

Group Members:

Name	Type
Root	Group
192.168.1.10	Stack (ION)

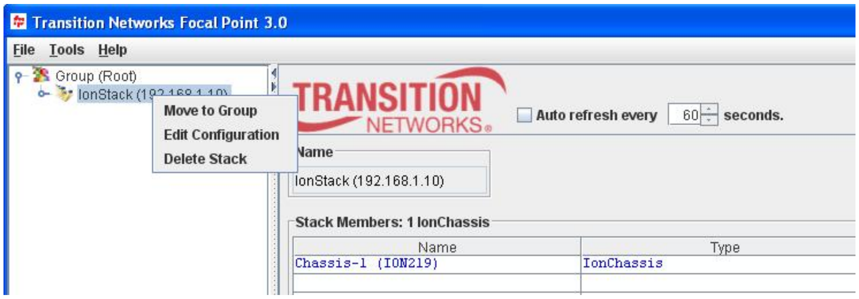
Date/Time	Source IP	Generic Trap	Specific Trap	Enterprise	Variable Bindings

Polling Interval: ○ None ● Interval 2 Minute

Figure 13: Main View Window

6. After Discovery you may change the SNMP version at the Edit Configuration menu. SNMP **V2C** is enabled by default. See “Edit Configuration’ below.

7. Right-click on a discovered Stack to display the **Move to Group / Edit Configuration / Delete Stack** dropdown.



□ Auto refresh every 60 seconds.

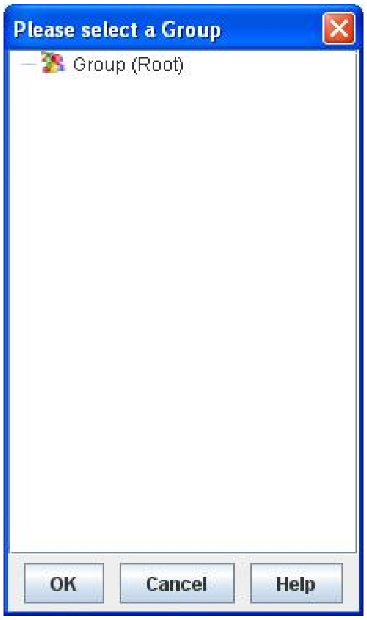
Name: IonStack (192.168.1.10)

Stack Members: 1 IonChassis

Name	Type
Chassis-1 (ION219)	IonChassis

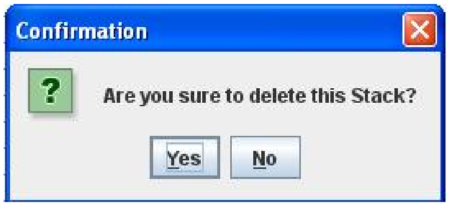
The three dropdown selections are explained below. Note that these Group Management functions work on the Point System only.

Move to Group - lets you select an existing Group to move this Stack to. Displays the list of available Groups from which to select.


Please select a Group

Select a Group from the list and click the **OK** button.

Delete Stack – lets you select and delete (remove) an existing configured and discovered Stack from the FP 3.0 configuration. A confirmation message displays asking *Are you sure to delete this Stack?*. Note that deleting a Stack deletes any attached, previously configured Chassis / devices under it.


Confirmation

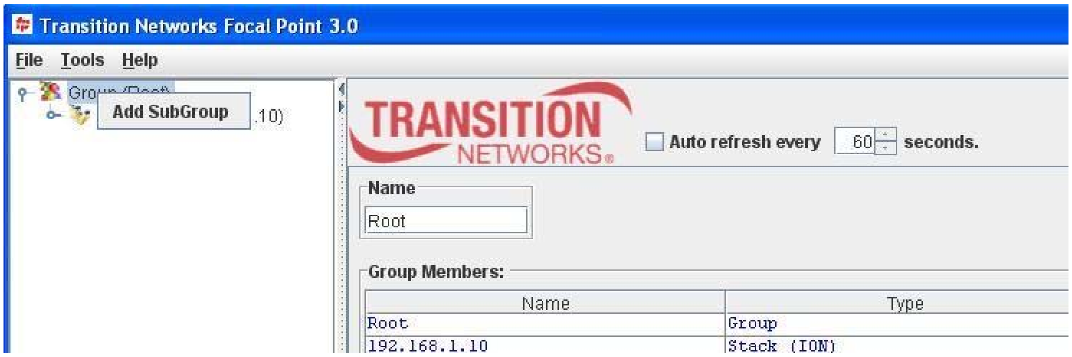
Are you sure to delete this Stack?

If you are sure you want to immediately delete the selected Stack and any Chassis / devices under it, click the **OK** button. Otherwise click the **Cancel** button.

You can use the **Tools** > **Discover Transition Agents** path to re-discover and re-display an ION and/or PS Stack. You can right-click a remaining **Group** to display the **Add SubGroup** dropdown to add subgroups.

Adding a SubGroup via Focal Point

1. Right-click on the **Group(Root)** stack item. The **Add SubGroup** dropdown displays.

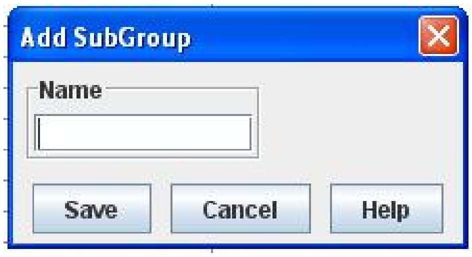


Name: Root

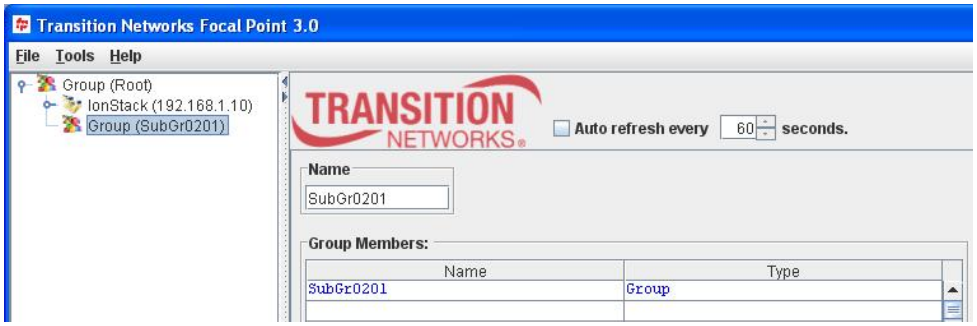
Group Members:

Name	Type
Root	Group
192.168.1.10	Stack (ION)

2. At the **Add SubGroup** dropdown enter a sub-group name and click the **Save** button.



The new sub-group displays.



Name: SubGr0201

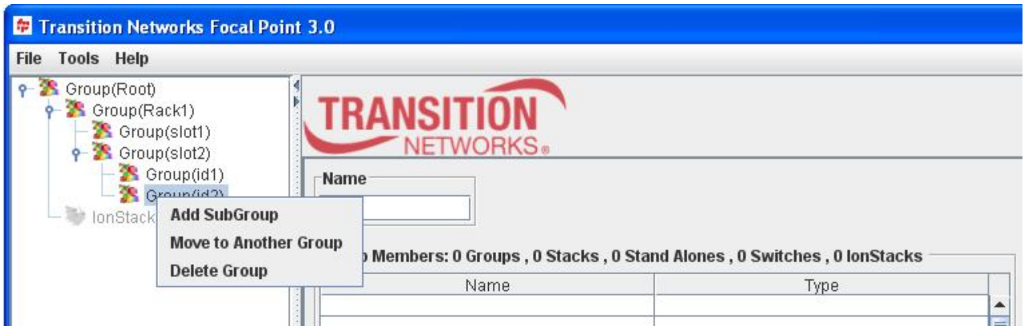
Group Members:

Name	Type
SubGr0201	Group

3. Click the **Refresh** button. The new Group displays.

Moving a SubGroup via Focal Point

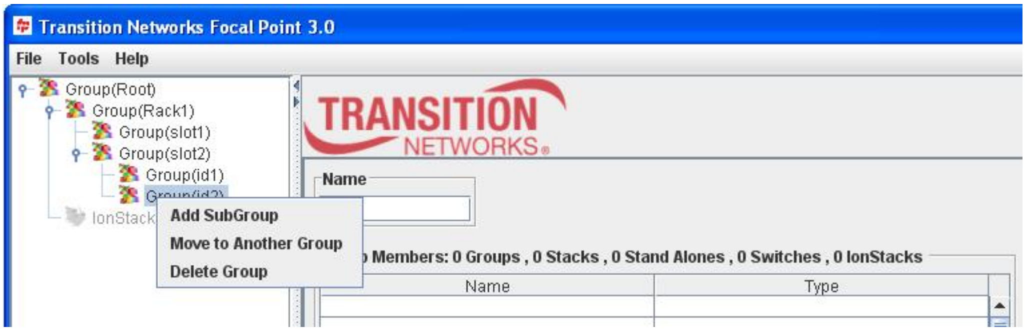
1. Highlight a stack item.
2. Right-click on the **Group(Root)** stack item. The **Add**-**Move**-**Delete** dropdown displays.



3. Select **Move to Another Group**. A list of Groups displays from which to select.
4. Select a Group from the list and click the **OK** button. The selected SubGroup is moved to the specified Group.
5. Expand the Group if necessary and verify the new SubGroup listed.

Deleting a SubGroup via Focal Point

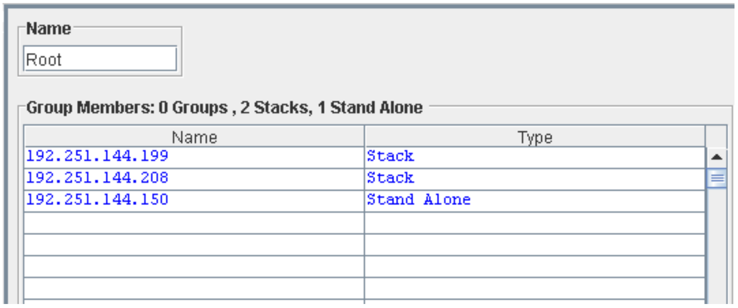
1. Highlight a stack item.
2. Right-click on the **Group(Root)** stack item. The **Add**-**Move**-**Delete** dropdown displays.



3. Select **Delete Group**. The confirmation message "*Are you sure to delete this Group?*" displays.
4. Click the **OK** button. The selected Group is deleted from the stack list.
5. Expand the Group if necessary and verify the SubGroup is no longer listed. The root group can not be deleted. After a sub group is deleted, all devices under this group will be moved to the root group automatically. So deleting a group will not result in deleting any stack.

Viewing IP Address History

Focal Point also saves all previously entered IP addresses to a local database, which will be displayed on the Root screen, as shown below.



Name: Root

Group Members: 0 Groups , 2 Stacks, 1 Stand Alone

Name	Type
192.251.144.199	Stack
192.251.144.208	Stack
192.251.144.150	Stand Alone

Figure 14: IP Address History Root Screen

Chassis / Device Views

To show the Point System chassis or device view, do the following:

1. Click the desired Stack in the left panel Group (Root) tree to show the available chassis or devices, as shown below.

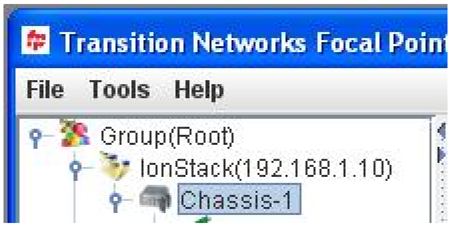
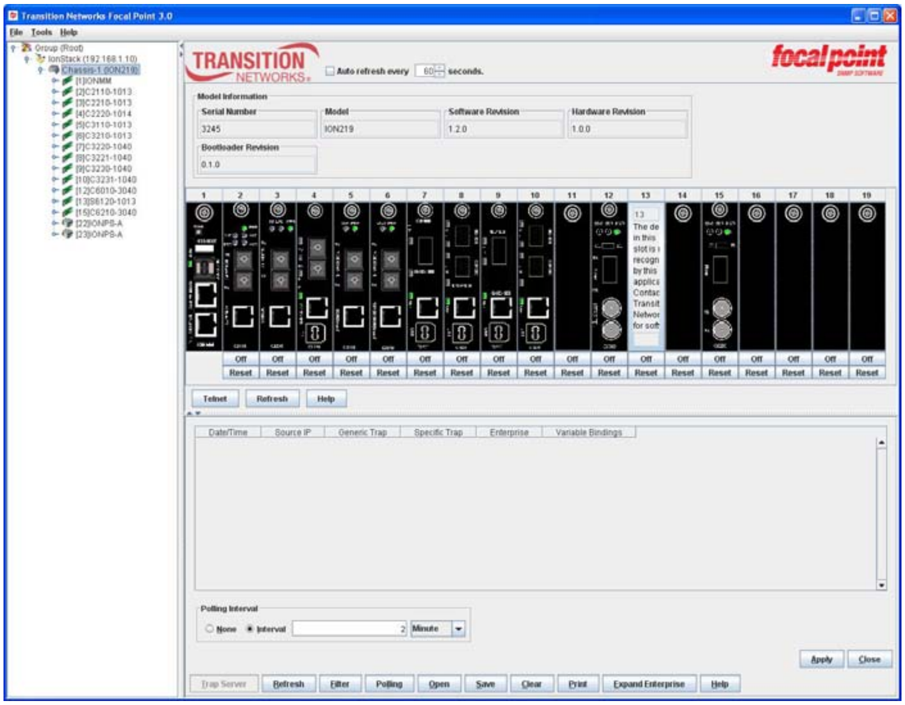


Figure 15: Chassis View Panel *(shows all installed cards)*

2. Click the desired chassis or device listed under the selected stack to view its contents, as shown below.



☐ Auto refresh every 60 seconds.

Model Information

Serial Number	Model	Software Revision	Hardware Revision
3245	ION219	1.2.0	1.0.0

Bootloader Revision: 0.1.0

Polling Interval: ○ None ● Interval 2 Minute

Figure 16: Chassis View

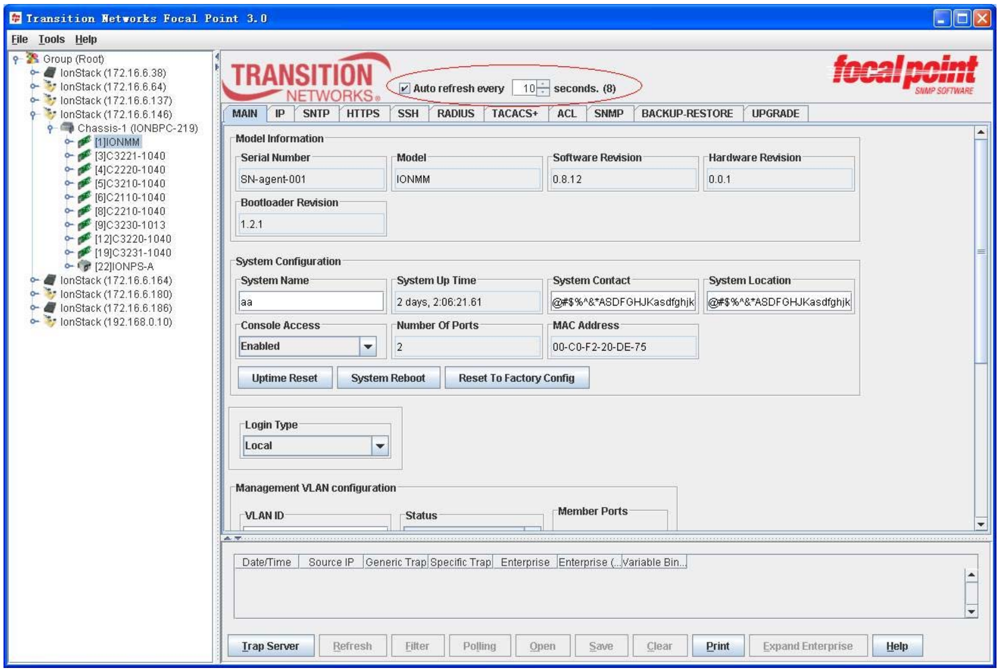
Chassis View

The main feature of the "Chassis View" is the graphical display of the chassis cards. The view displays white-on-black line drawings of all slide-in cards in the ION system chassis at discovery time. The slide-in cards that display include:

1. IONMM Management Module
2. ION System Slide-In Cards
3. Point System Slide-In Cards with IONADP extenders
4. ION System Power Supplies

The COH function lets you hover the cursor over a card / slot to enlarge the graphic for better legibility.

Double-click on a particular card to display the **MAIN** tab for that particular card / slot in the chassis (see below).



Transition Networks Focal Point 3.0

- Group (Root)
  - IonStack (172.16.6.38)
  - IonStack (172.16.6.64)
  - IonStack (172.16.6.137)
  - IonStack (172.16.6.146)
    - Chassis-1 (IONBPC-219)
      - [1]IONMM
      - [3]C3221-1040
      - [4]C2220-1040
      - [5]C3210-1040
      - [6]C2110-1040
      - [8]C2210-1040
      - [9]C3230-1013
      - [12]C3220-1040
      - [19]C3231-1040
      - [22]IONPS-A
  - IonStack (172.16.6.164)
  - IonStack (172.16.6.180)
  - IonStack (172.16.6.186)
  - IonStack (192.168.0.10)

☑ Auto refresh every 10 seconds. (8)

Model Information

Serial Number: SN-agent-001
Model: IONMM
Software Revision: 0.8.12
Hardware Revision: 0.0.1
Bootloader Revision: 1.2.1

System Configuration

System Name: aa
System Up Time: 2 days, 2:06:21.61
System Contact: @#$%^&*ASDFGHJKasdfghjk
System Location: @#$%^&*ASDFGHJKasdfghjk
Console Access: Enabled
Number Of Ports: 2
MAC Address: 00-C0-F2-20-DE-75

Login Type: Local

Management VLAN configuration

VLAN ID
Status
Member Ports

Date/Time	Source IP	Generic Trap	Specific Trap	Enterprise	Enterprise (...	Variable Bin...

Chassis View Slide-in Card Alerts

Yellow ALERT tags show that a particular slide-in card has a connection problem and cannot be configured via the Focal Point software (see below). See the individual slide-in card manual for more information.

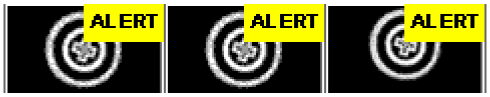
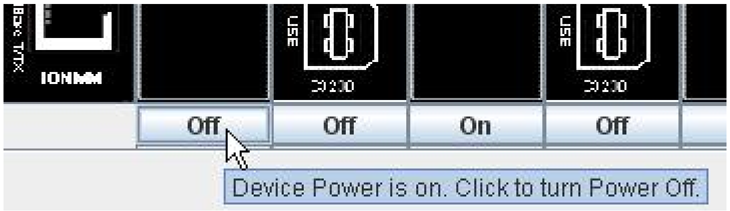


Figure 17: Slide-In Card Alert

The Chassis View Yellow ALERTS are only supported on the PointSystem (Chassis II).

Chassis View Slide-in Card Reset and Power OFF

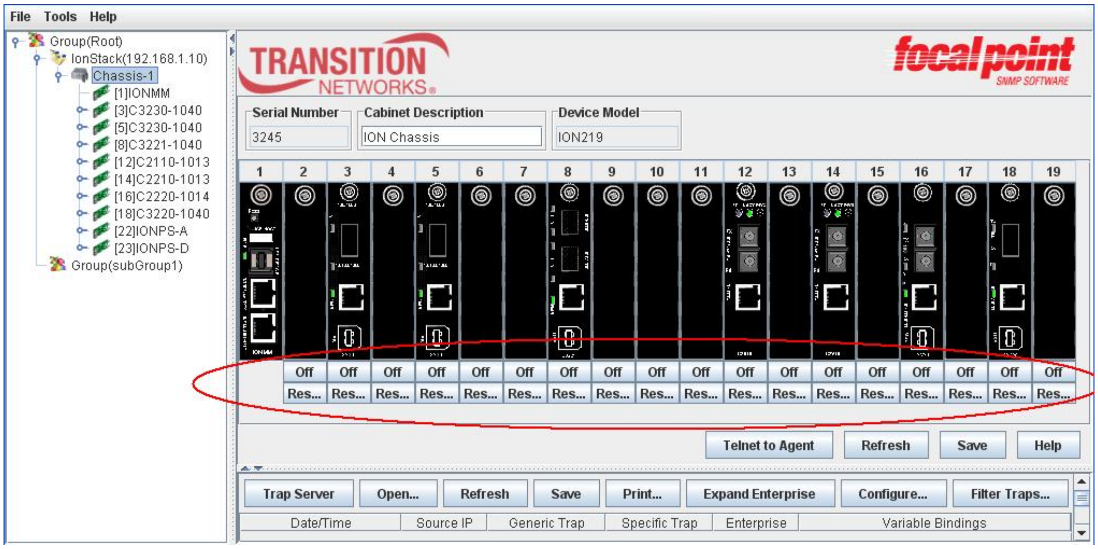
The current Power status (Off or On) displays for each card. Click the **Off** or **On** button beneath a card to switch its status to the displayed status.



Device Power is on. Click to turn Power Off.

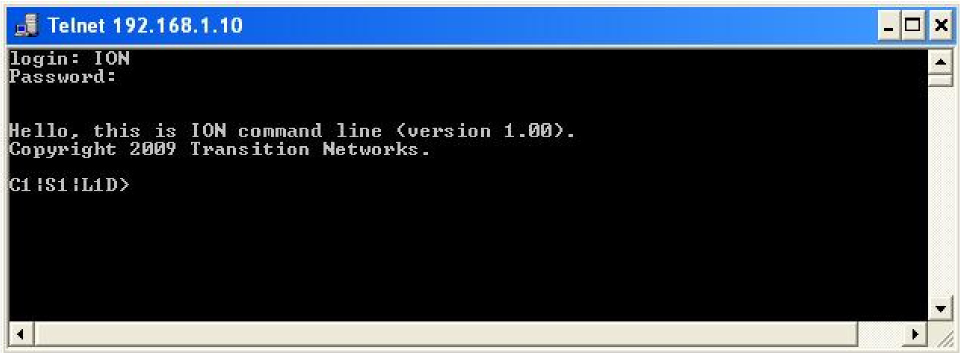
The confirmation dialog "*Are you sure you want to change the Power Status of this Slot?*" displays. Note that Point System cards in an ION chassis cannot be powered off.

A Reset button lets you reset power to an individual slot / card in the chassis. The confirmation dialog "*Are you sure to Power Reset this slot?*" displays.



Serial Number: 3245
Cabinet Description: ION Chassis
Device Model: ION219

Telnet To Agent: Click this button to open a Telnet session, which will bring up the password display for the chassis agent (see below).



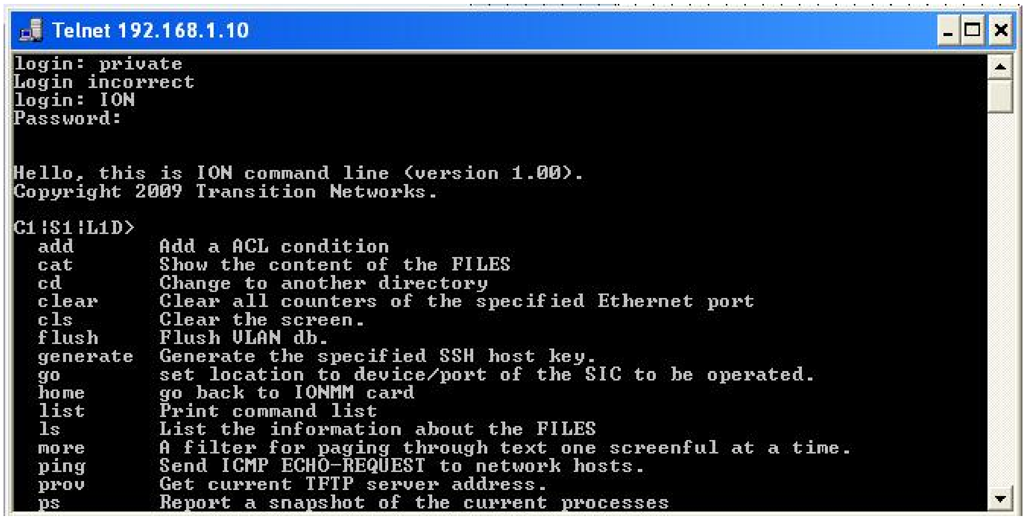
```
login: ION
Password:


Hello, this is ION command line (version 1.00).
Copyright 2009 Transition Networks.

C1|S1|L1D>
```

Figure 18: Telnet Screen

After you successfully log in, you can enter the full set of CLI commands supported. An example of the ION **Help** command (**?** command) is shown below.



```
login: private
Login incorrect
login: ION
Password:


Hello, this is ION command line (version 1.00).
Copyright 2009 Transition Networks.

C1|S1|L1D>
  add       Add a ACL condition
  cat       Show the content of the FILES
  cd        Change to another directory
  clear     Clear all counters of the specified Ethernet port
  cls       Clear the screen.
  flush     Flush VLAN db.
  generate  Generate the specified SSH host key.
  go        set location to device/port of the SIC to be operated.
  home      go back to IONMM card
  list      Print command list
  ls        List the information about the FILES
  more      A filter for paging through text one screenful at a time.
  ping      Send ICMP ECHO-REQUEST to network hosts.
  prov      Get current TFTP server address.
  ps        Report a snapshot of the current processes
```

Refer to the applicable *ION Command Line Interface (CLI) Reference Guide* for details on the set of CLI commands supported.

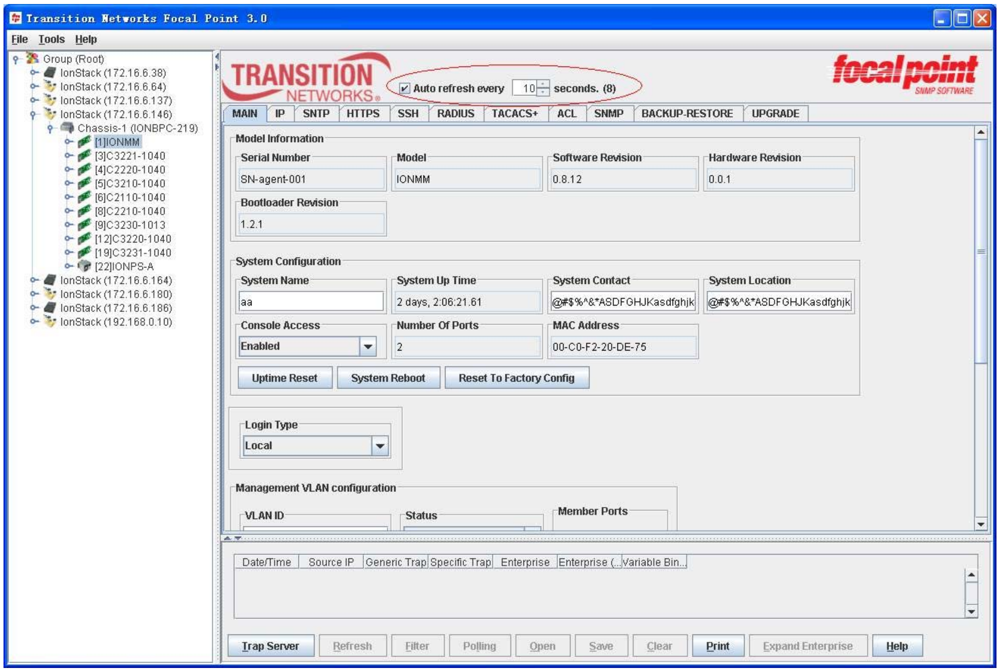
Refresh: Click this button to reflect changes to the Name or the group members table on this page. Another application could change these, at which time, clicking the “Refresh” button will reflect that change also.

Save: Saves the chassis description only, if changed.

Help: Click the **Help** button to display web-based links to an integrated set of help files that present instructions for using Focal Point software. You can view and print the help files from any standard HTML browser. Help screen files are only current to the date of the FP release. The most current files are at www.transition.com/pshelp.

View a Slide-in-Card

To launch the **MAIN** tab for any slide-in-card (SIC), in the Group (Root) tree, click on a chassis number containing a slide-in card, and then double-click on the card / slot (see below).



☑ Auto refresh every 10 seconds. (8)

Serial Number: SN-agent-001
Model: IONMM
Software Revision: 0.8.12
Hardware Revision: 0.0.1
Bootloader Revision: 1.2.1

System Name: aa
System Up Time: 2 days, 2:06:21.61
System Contact: @#$%^&*ASDFGHJKasdfghjk
System Location: @#$%^&*ASDFGHJKasdfghjk
Console Access: Enabled
Number Of Ports: 2
MAC Address: 00-C0-F2-20-DE-75

Login Type: Local

Figure 19: MAIN Menu for Slot One [1]IONMM

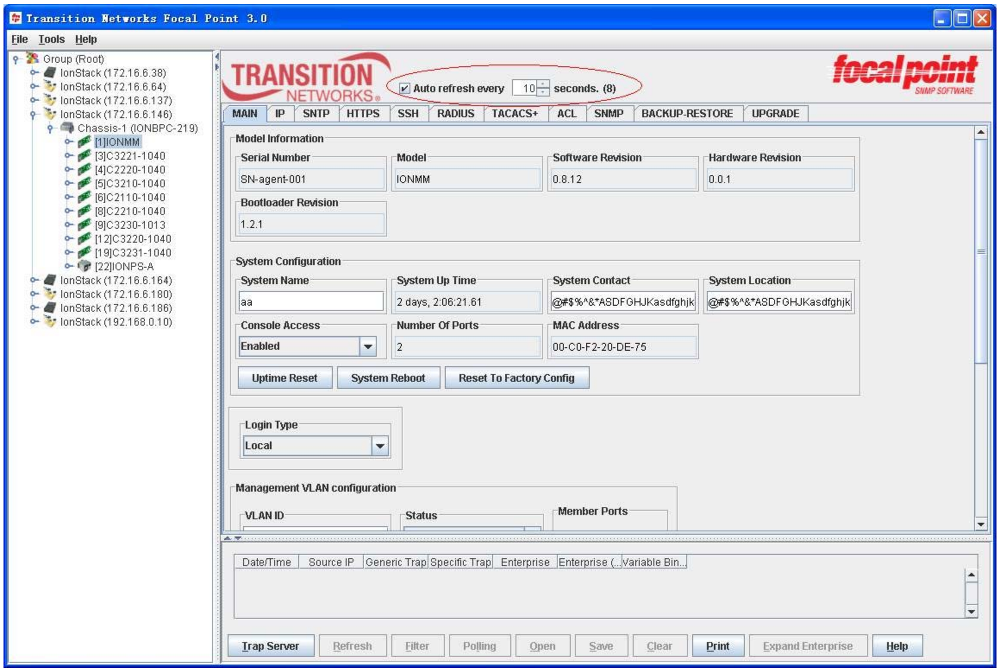
The remaining buttons shown in the figure above are described below.

Help button: Click the **Help** button to display web-based links to an integrated set of help files that present instructions for using Focal Point software. You can view and print the help files from any standard HTML browser. The most current files are on the TN website at www.transition.com/pshelp.

Refresh button: Click this button to reflect changes to the Name or the group members table on this page. Another application could change these, at which time clicking the **Refresh** button will reflect that change also.

MAIN Tab - Device Details

From the "Chassis View" menu, double-click any graphical card to open the **MAIN** tab for that slide-in card as shown below.



Transition Networks Focal Point 3.0

☑ Auto refresh every 10 seconds. (8)

Model Information

Serial Number: SN-agent-001

Model: IONMM

Software Revision: 0.8.12

Hardware Revision: 0.0.1

Bootloader Revision: 1.2.1

System Configuration

System Name: aa

System Up Time: 2 days, 2:06:21.61

System Contact: @#$%^&*ASDFGHJKasdfghjk

System Location: @#$%^&*ASDFGHJKasdfghjk

Console Access: Enabled

Number Of Ports: 2

MAC Address: 00-C0-F2-20-DE-75

Login Type: Local

Management VLAN configuration

VLAN ID

Status

Member Ports

Date/Time	Source IP	Generic Trap	Specific Trap	Enterprise	Enterprise (...	Variable Bin...

Figure 20: Device Main Tab

The Device **MAIN** tab displays device details for the selected device. **Note**: The **MAIN** device details tab will have a different format for different slide-in card types; however, the functions described apply to all card types.

Main Tab - Device Details Buttons

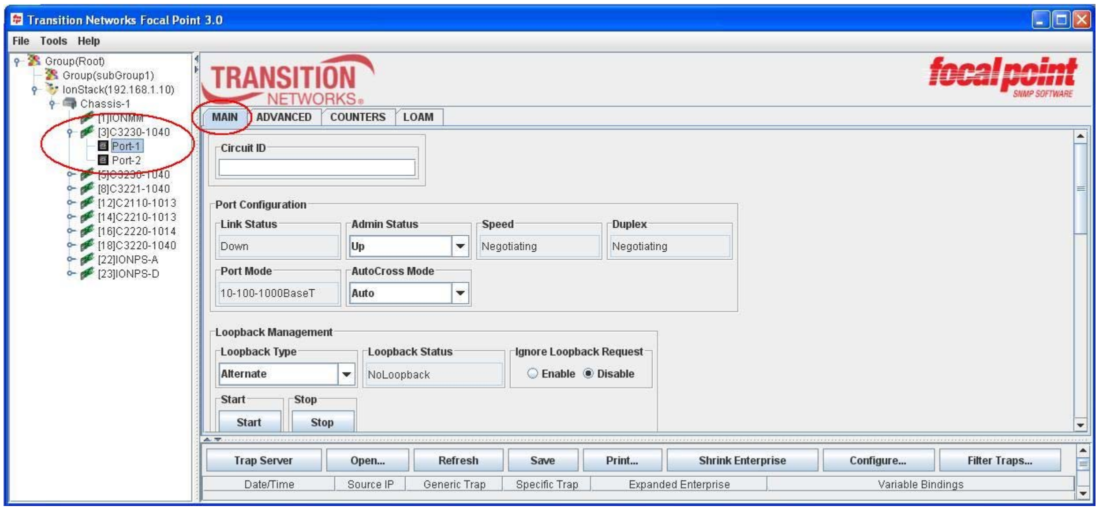
Refresh: Click this button to reflect changes to the Name or the group members table on this page. Another application could change these, at which time, clicking the **Refresh** button will reflect that change also.

Save: Saves the changes made to any parameter listed. Only those parameters that appear in text boxes or drop-down lists can be changed. (**Note**: changes made on the display are saved in non-volatile memory of the card(s), so the modified configuration follows the slide-in card if it is moved from one slot to another.)

Help: Click this button to display web-based information about this device.

MAIN Tab - Port Details

From the “Chassis View” menu, double-click any graphical card to open the **MAIN** tab for that slide-in card.
Click on the desired device to display its Ports view.
Click on the desired Port to display the Device Port’s **MAIN** tab.

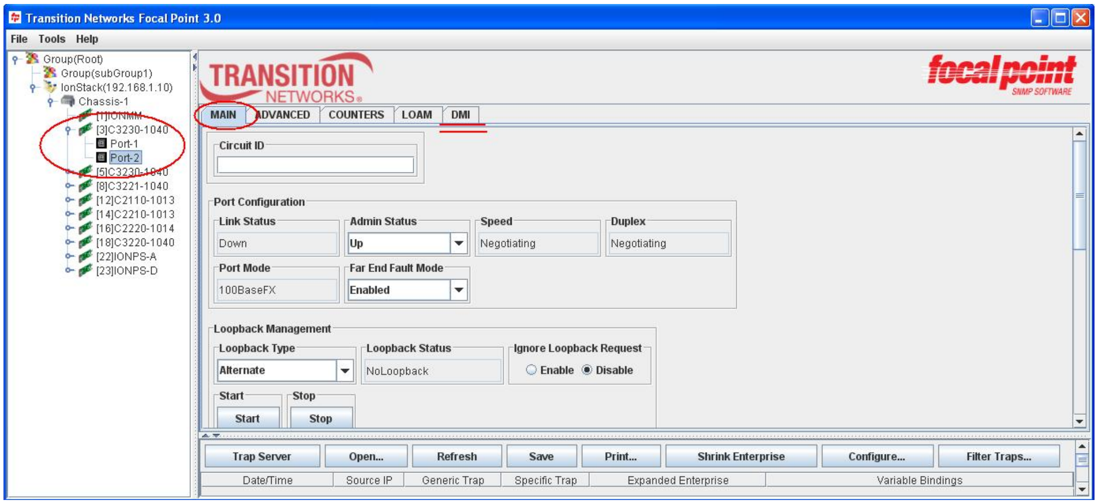


Circuit ID:

Port Configuration
- Link Status: Down
- Admin Status: Up
- Speed: Negotiating
- Duplex: Negotiating
- Port Mode: 10-100-1000BaseT
- AutoCross Mode: Auto

Loopback Management
- Loopback Type: Alternate
- Loopback Status: NoLoopback
- Ignore Loopback Request: ○ Enable ● Disable

Figure 21: Port 1 MAIN Tab



Circuit ID:

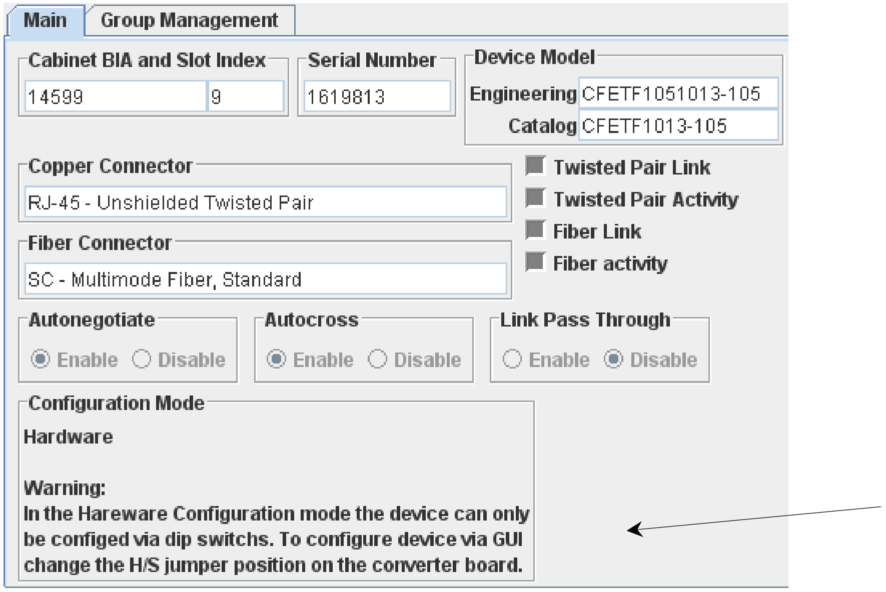
Port Configuration
- Link Status: Down
- Admin Status: Up
- Speed: Negotiating
- Duplex: Negotiating
- Port Mode: 100BaseFX
- Far End Fault Mode: Enabled

Loopback Management
- Loopback Type: Alternate
- Loopback Status: NoLoopback
- Ignore Loopback Request: ○ Enable ● Disable

Figure 22: Port 2 MAIN Tab

Main Device Details Window Configuration Mode

Configuration Mode Details shows that this particular slide-in card is in Hardware configuration mode and cannot be configured via the Focal Point software. For additional information see the specific manual for the selected slide-in card (SIC).



Cabinet BIA and Slot Index: 14599 | 9

Serial Number: 1619813

Device Model
Engineering: CFETF1051013-105
Catalog: CFETF1013-105

Copper Connector: RJ-45 - Unshielded Twisted Pair

Fiber Connector: SC - Multimode Fiber, Standard

■ Twisted Pair Link
■ Twisted Pair Activity
■ Fiber Link
■ Fiber activity

Autonegotiate: ● Enable ○ Disable

Autocross: ● Enable ○ Disable

Link Pass Through: ○ Enable ● Disable

Configuration Mode
Hardware

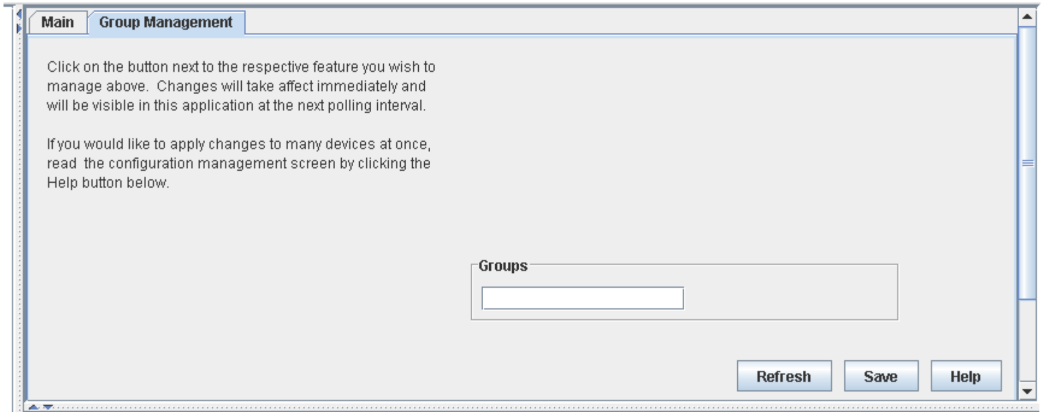
Warning:
In the Hareware Configuration mode the device can only be configed via dip switchs. To configure device via GUI change the H/S jumper position on the converter board.

Attention Tag

Figure 23: Main Configuration Mode Details

Group Management

The Group Management dialog box allows placing devices in groups. The Point System SNMP agent can be used to apply a single configuration change to a group of the same slide-in card types. Note that this function applies only to Point System chassis and SICs.



Click on the button next to the respective feature you wish to manage above. Changes will take affect immediately and will be visible in this application at the next polling interval.

If you would like to apply changes to many devices at once, read the configuration management screen by clicking the Help button below.

Figure 24: Group Management Portion of the Details Dialog Box

Help button: Click a **Help** button to display a web-based help screen that shows detailed instructions for using the group management function—view or print the help screens from any standard HTML browser. See Figure 24 above. Help-screen files are only current to the date of the FP release. The most current files are help files are at www.transition.com/pshelp. **Note**: Both **Help** buttons show the same information.

Group String Text Field: The Group String text field is used to select the previously defined Group strings, or to add new strings by entering a new name into the text field and then clicking the **Save** button. See Figure 24 above.

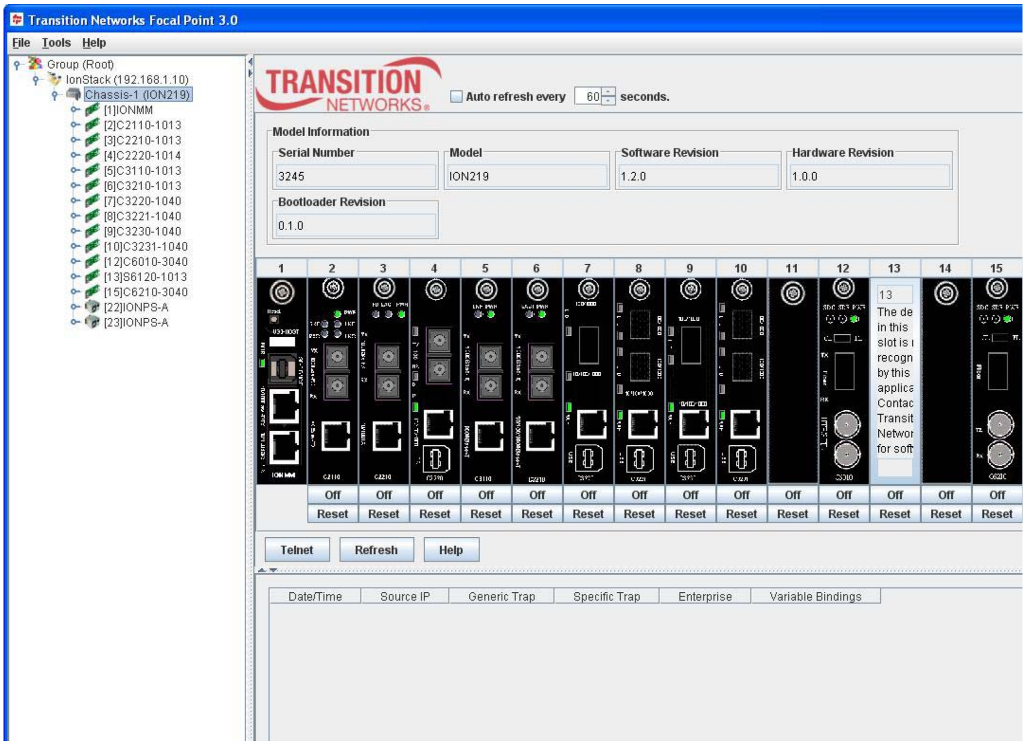
Save: Click this button to save the changes made to group string.

Refresh: Click this button to reflect changes to the Name or the group members table on this page. Another application could change these, at which time, clicking the **Refresh** button will reflect that change also.

Note: For additional information go to www.transition.com/pshelp/configmgmt2.html and click the Group Control String link.

FP3.0 Startup Screens

A sample FP 3.0 startup screen is shown below with an ION Chassis.



- Group (Root)
  - IonStack (192.168.1.10)
    - Chassis-1 (ION219)
      - [1]IONMM
      - [2]C2110-1013
      - [3]C2210-1013
      - [4]C2220-1014
      - [5]C3110-1013
      - [6]C3210-1013
      - [7]C3220-1040
      - [8]C3221-1040
      - [9]C3230-1040
      - [10]C3231-1040
      - [12]C6010-3040
      - [13]S6120-1013
      - [15]C6210-3040
      - [22]IONPS-A
      - [23]IONPS-A

Model Information

Serial Number: 3245

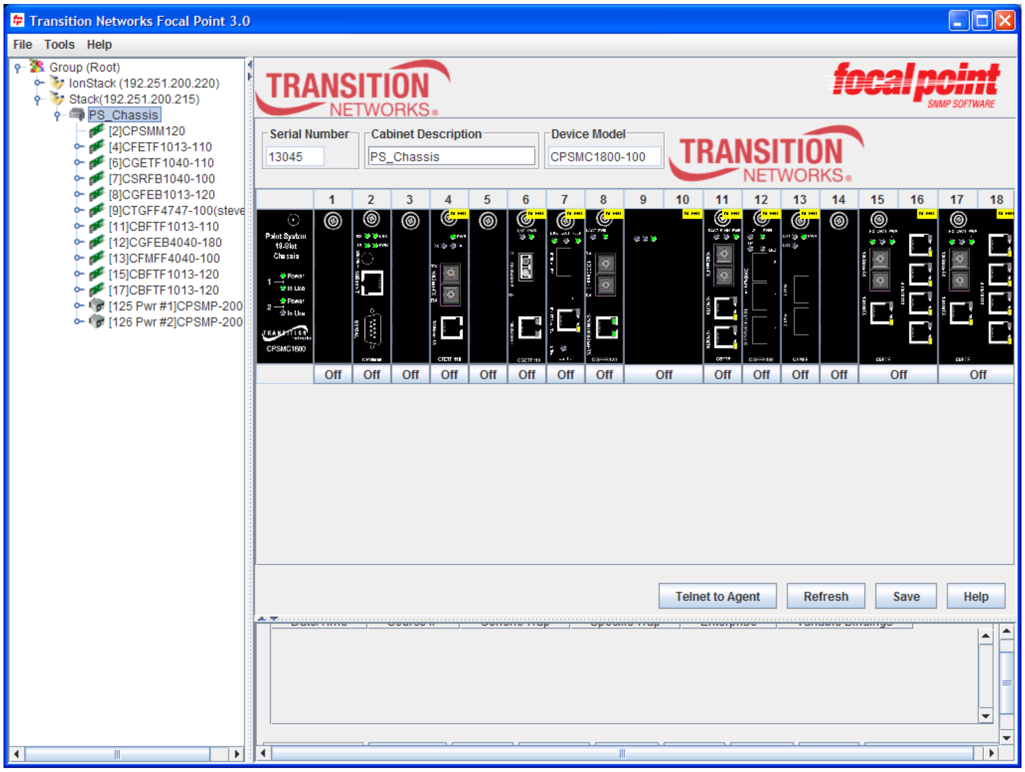
Model: ION219

Software Revision: 1.2.0

Hardware Revision: 1.0.0

Bootloader Revision: 0.1.0

A sample FP 3.0 startup screen is shown below with a Point System (PS) Chassis.



- Group (Root)
  - IonStack (192.251.200.220)
  - Stack(192.251.200.215)
    - PS_Chassis
      - [2]CPSMM120
      - [4]CFETF1013-110
      - [6]CGETF1040-110
      - [7]CSRFB1040-100
      - [8]CGFEB1013-120
      - [9]CTGFF4747-100(steve
      - [11]CBFTF1013-110
      - [12]CGFEB4040-180
      - [13]CFMFF4040-100
      - [15]CBFTF1013-120
      - [17]CBFTF1013-120
      - [125 Pwr #1]CPSMP-200
      - [126 Pwr #2]CPSMP-200

Serial Number: 13045

Cabinet Description: PS_Chassis

Device Model: CPSMC1800-100

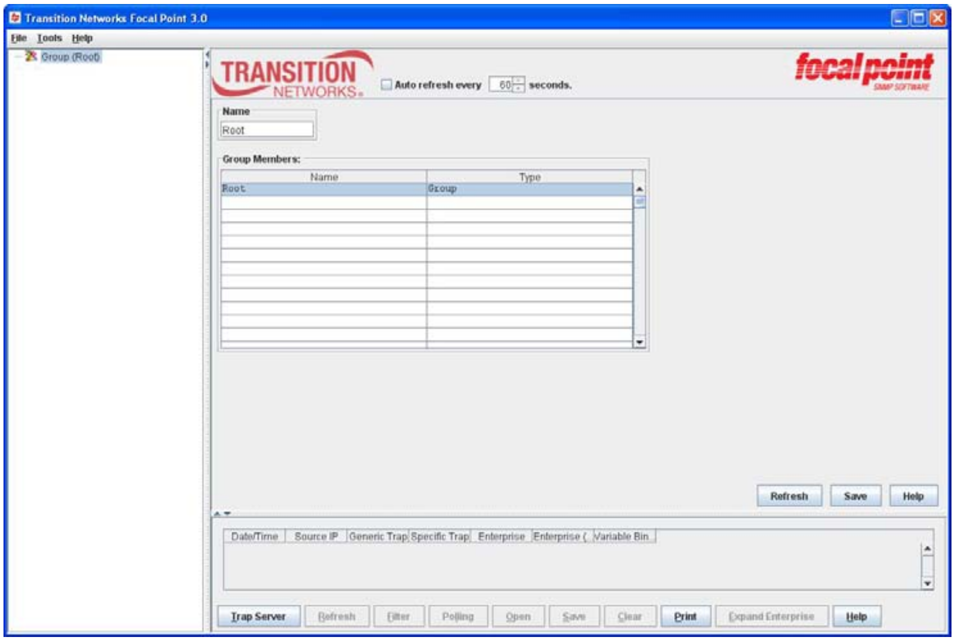
Start the FP 3.0 Trap Server Application

1. Navigate to the **Start** > **All Programs** > **Transition Networks** > **Focal Point 3.0 Management Application** menu path, or at Windows Explorer > *C:\Program Files\FocalPoint_3.0\FocalPoint3.0\bin* double-click on the *FocalPointApp.bat* file.

Or double-click on the **TMStartup.bat** file installed by default at *C:\Program Files\FocalPoint_3.0\FocalPoint3.0\bin*.

If the Windows Security Alert dialog box opens, 1) Check your Windows Firewall settings. 2) Check the "For this program, don't show this message again" checkbox. 3) Click the **OK** button to clear the Windows Security Alert message and continue operation.

The FP 3.0 startup screen displays.



☐ Auto refresh every 60 seconds.

Name: Root

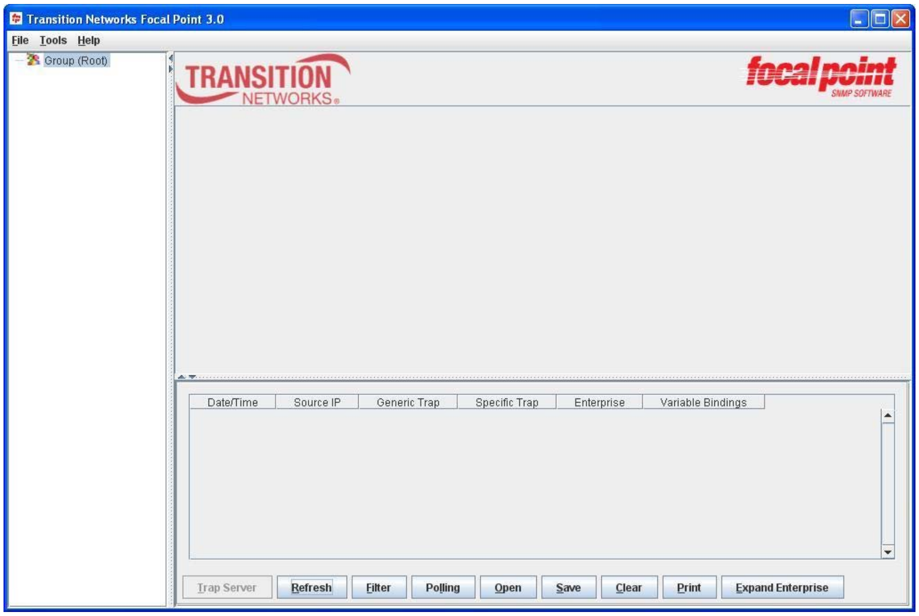
Group Members:

Name	Type
Root	Group

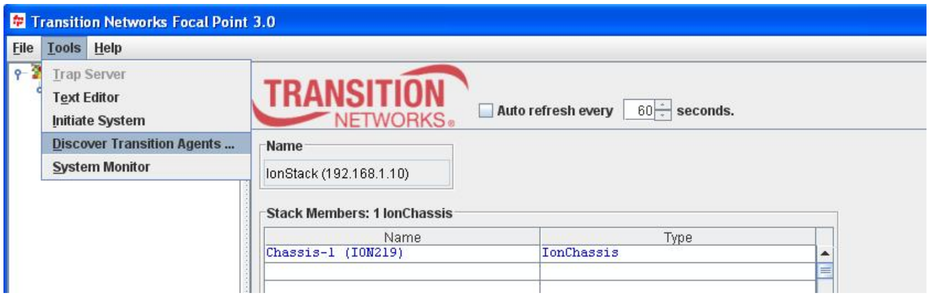
2. Go to the "Discover Transition Agents" section on the next page.

Discover Transition Agents

1. After you start the FP 3.0 Management Application, the startup screen displays with the Trap Server button grayed out.



2. Click **Tools** > **Discover Transition Agents ...** menu path. The Discovering Transition Agents dialog displays.



☐ Auto refresh every 60 seconds.

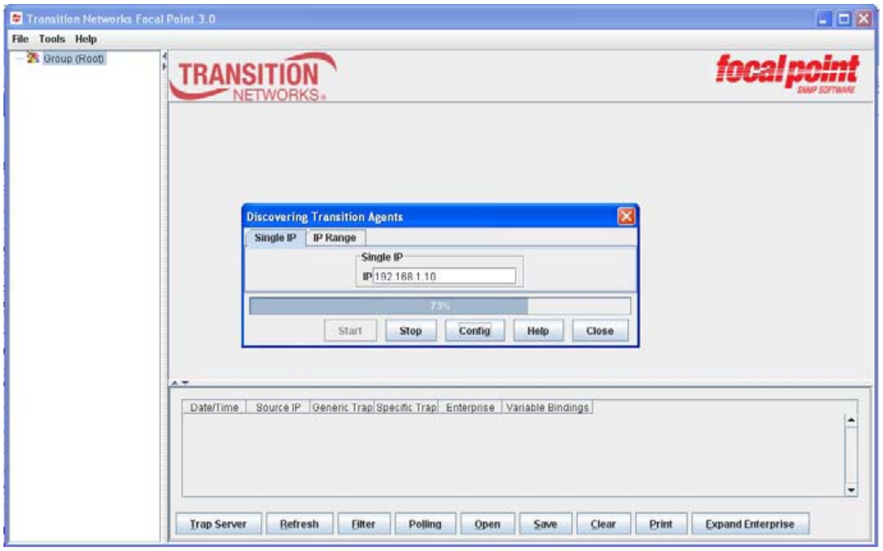
Name

IonStack (192.168.1.10)

Stack Members: 1 IonChassis

Name	Type
Chassis-1 (ION219)	IonChassis

3. Enter the Single IP address or IP Range of addresses an click the **Start** button. The discovery action displays for a short time. (Note that discovery for a range of IP addresses will take longer than discovery for a single IP address.)

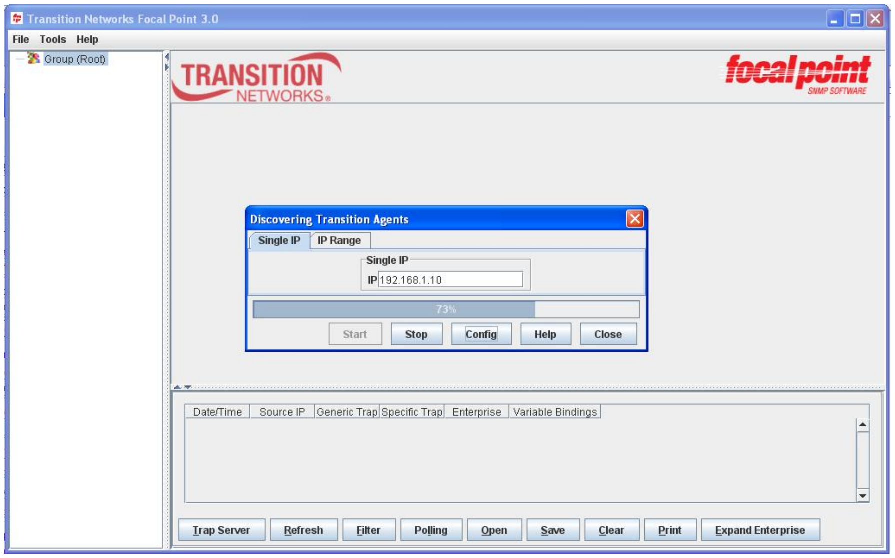


Single IP

IP 192.168.1.10

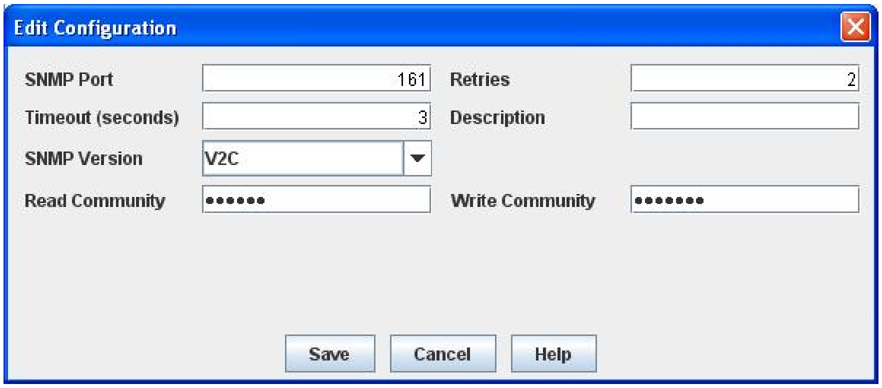
73%

4. When discovery completes, the Group tree displays, click **Tools** > **Discover Transition Agents ...** menu path again.
The **Discovering Transition Agents** dialog displays again.



Single IP
IP 192.168.1.10
73%

5. Click the **Config** button. The default **Edit Configuration** screen displays with SNMP Version **V2C** selected by default.



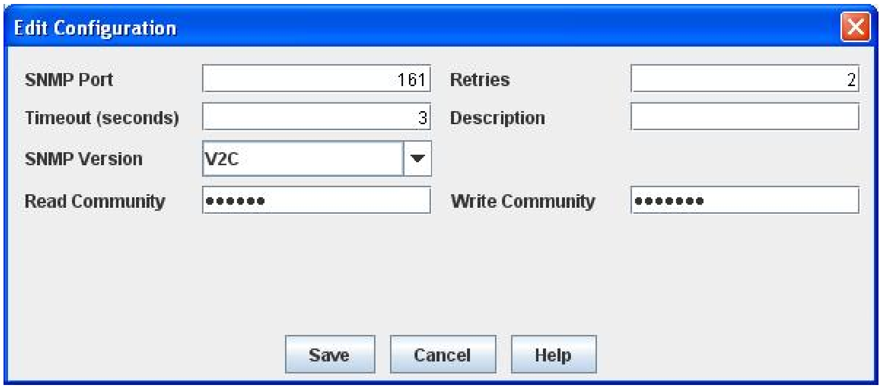
SNMP Port	161	Retries	2
Timeout (seconds)	3	Description	
SNMP Version	V2C		
Read Community	••••••	Write Community	•••••••

6. Continue with the **Edit Configuration** section below.

Edit Configuration

The **Edit Configuration** menu lets you change the current SNMP configuration. Here you may edit the configuration information of stacks and stand alone devices in terms of Port number, Retries, Timeout, SNMP version, security, authentication protocol, and privacy protocol.

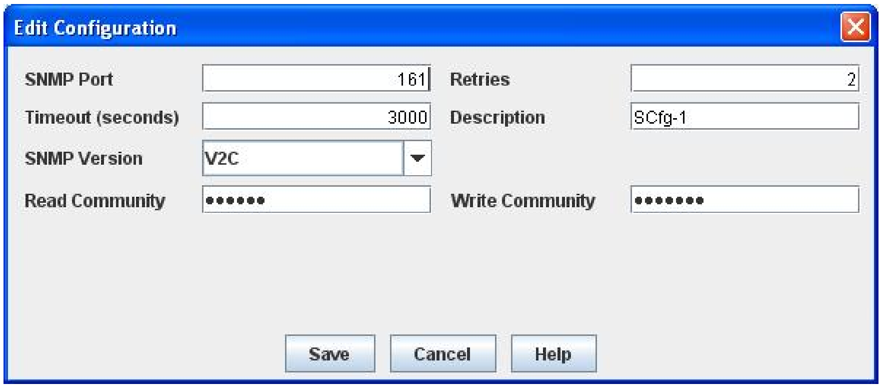
1. In the **SNMP Port** entry field, enter a valid, unused port number. The default is Port number 161.
2. In the **Retries** entry field, enter the number of attempts to be made before stopping further attempts.
3. In the **Timeout (seconds)** entry field, enter the amount of time in seconds to elapse before stopping further attempts.
4. In the **Description** entry field, enter text to help identify this configuration.
5. The Edit Configuration screen displays SNMP Version 1 (v1) by default. For either SNMP Version 1 or Version 2c, enter the **Get Community** and **Set Community** names and press **Save** when done.



SNMP Port: 161
Retries: 2
Timeout (seconds): 3
Description:
SNMP Version: V2C
Read Community: ••••••
Write Community: •••••••

In SNMPv1 and v2c the community string is used to authenticate the SNMP management station and SNMP agent.
So whenever any SNMP management station sends a request to get or set some data on an SNMP agent, it also sends the community string, which is configured in the string along with the request. When the request reaches the SNMP agent, it tries to match the sent community string with the one you have defined in the agent. If the two strings match, the SNMP agent answers the request. If not, the request is rejected as unauthorized. This helps stop unauthorized SNMP management stations from changing parameters on your SNMP agent.
You should not leave the community string set to 'public' on your SNMP agent. This is the default community string, and if left unchanged, exposes your SNMP agent to any SNMP management station. Anyone with SNMP manager software on their PC could make changes to your SNMP agents.

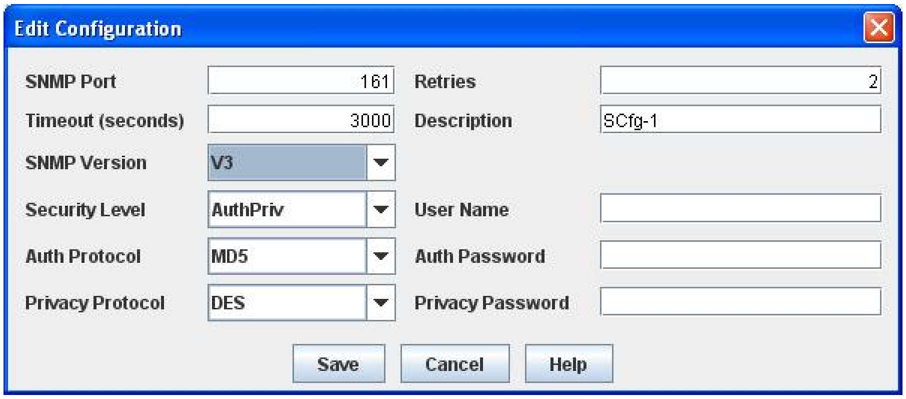
6. In the **SNMP Version** field, select the desired SNMP version for FP 3.0 operation. The selections are SNMP **V1**, **V2C**, or **V3**. SNMP **V2C** is enabled by default.
a) For SNMP V1 or V2C, enter the **Get Community** and **Set Community** names and press **Save** when done.



SNMP Port: 161
Retries: 2
Timeout (seconds): 3000
Description: SCfg-1
SNMP Version: V2C
Read Community: ••••••
Write Community: •••••••

In SNMPv1 and v2c, the community string is used to authenticate the SNMP management station and SNMP agent. So whenever any SNMP management station sends a request to get or set some data on an SNMP agent, it also sends the community string, which is configured in the string along with the request. When the request reaches the SNMP agent, it tries to match the sent community string with the one you have defined in the agent.

If the two strings match, the SNMP agent answers the request. If not, the request is rejected as unauthorized. This helps stop unauthorized SNMP management stations from changing parameters on your SNMP agent.
Warning: You should not leave the **Get Community** string at the default (**public**) or leave the default **Set Community** default (**private**). These are the default community strings, and if left unchanged, exposes your SNMP agent to any SNMP management station. Anyone with SNMP manager software on their PC could make changes to your SNMP agents.
Note: You can toggle between different SNMP configurations if you are managing different devices that support different versions of SNMP.
Note: Any change made in Focal Point should also be made at the Management Module (e.g., IONMM or CPSMM-200).
b) If SNMP **V3** is required, at the **SNMP Version** dropdown, select **V3**. Several additional configuration entry fields and dropdowns display.



Edit Configuration

SNMP Port	161	Retries	2
Timeout (seconds)	3000	Description	SCfg-1
SNMP Version	V3		
Security Level	AuthPriv	User Name	
Auth Protocol	MD5	Auth Password	
Privacy Protocol	DES	Privacy Password	

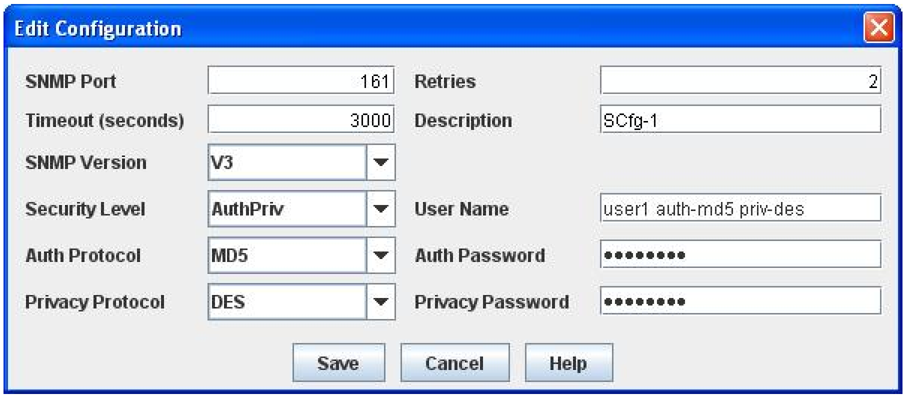
7. At the **Security Level** dropdown, select **Auth Priv**, **Auth No Priv**, or **No Auth No Priv**, where:

   Auth Priv = Authentication and Privacy are both configured.

   Auth No Priv = Authentication configured, but No Privacy configured.

   No Auth No Priv = No Authentication and No Privacy configured.

8. In the **User Name** field, enter a name to help identify this user.
9. At the **Auth Protocol** dropdown, select **MD5** or **SHA** as the Authentication Protocol.
10. In the **Auth Password** field, enter an Authentication password of 8 - 64 alphanumeric characters.
11. At the **Privacy Protocol** dropdown, select **DES** or **AES** as the Privacy Protocol.
12. In the **Privacy Password** field, enter a Privacy password of 8 - 64 alphanumeric characters.
13. Verify your configuration settings.



Edit Configuration

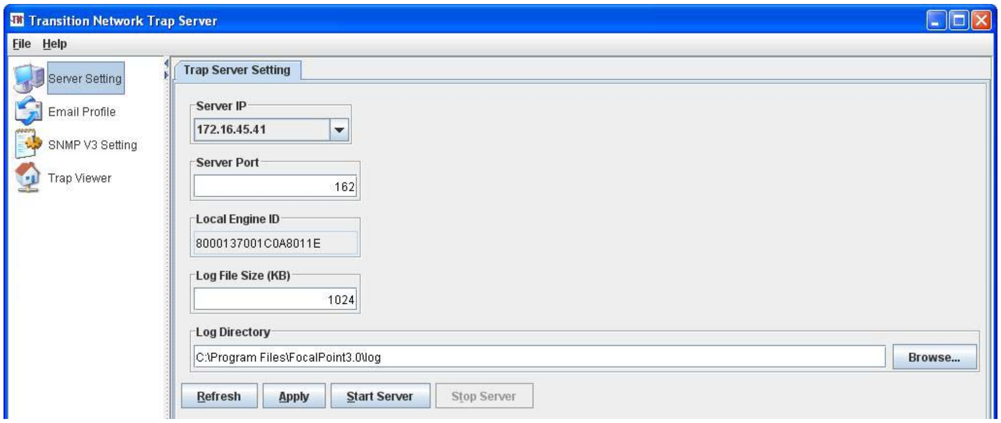
SNMP Port	161	Retries	2
Timeout (seconds)	3000	Description	SCfg-1
SNMP Version	V3		
Security Level	AuthPriv	User Name	user1 auth-md5 priv-des
Auth Protocol	MD5	Auth Password	••••••••
Privacy Protocol	DES	Privacy Password	••••••••

14. When done click the **Save** button. The **Discovering Transition Agents** dialog displays again.
15. Click the **Close** button.
16. Continue with the **Trap Server Setup** section below.

1. Trap Server Setup

The **Trap Server** > **Server Setup** menu path lets you define the necessary trap server settings.

1. Navigate to the **Trap Server** > **Server Setup** > **Trap Server Setting** menu path.



Server IP: 172.16.45.41

Server Port: 162

Local Engine ID: 8000137001C0A8011E

Log File Size (KB): 1024

Log Directory: C:\Program Files\FocalPoint3.0\log

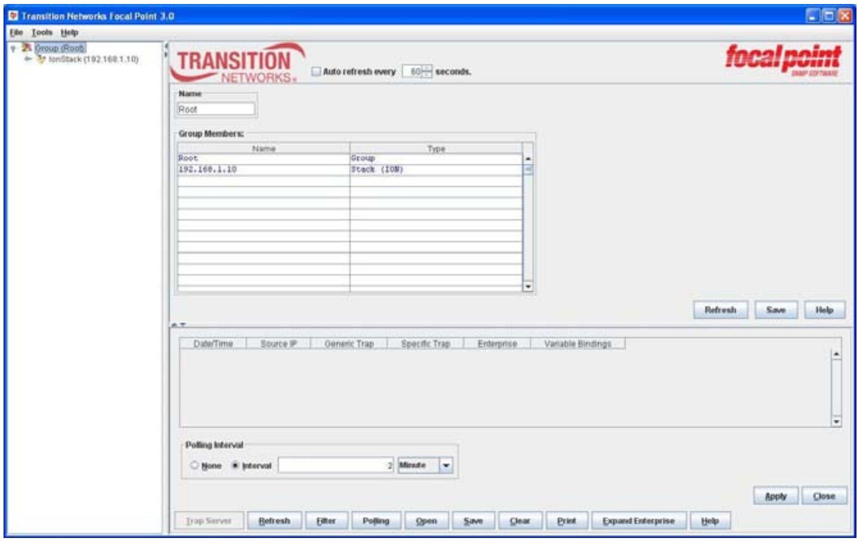
2. First enter/select new settings, then click the **Apply** button to save the settings, and then click the **Start Server** button to listen the traps with the new settings. The new settings include:

- Select a **Server IP** address from the dropdown (e.g., **172.16.45.41** shown above). This window lists all IP addresses available in the local PC (loopback IP 127.0.0.1 is excluded).
- Enter a **Server Port** number. The default is port number **162**.
- Enter a valid Local Engine ID (e.g., **80000137001C0A8011E** in the sample screen above). The local Engine ID is calculated by the Trap Server automatically and is not editable. This value is used as the remote engine ID when to receive the inform traps from the equipments.
- Enter a valid **Log File Size** limit in kilobytes (e.g., **1024** KB shown above). The received traps are saved in a default log file named "TN_TrapServer.log" which is located in the Log Directory.

3. Click the **Browse** button and locate a **Log Directory** location for storing FP 3.0 log files (e.g., ***C:\Program Files\FocalPoint_3.0\log*** shown above).

4. When done click the **Apply** button to save the settings.

5. Click the **Start Server** button to start the Trap Server. The startup screen displays again with the **Trap Server** button grayed out, but several other buttons available.



☐ Auto refresh every 60 seconds.

Name: Root

Group Members:

Name	Type
Root	Group
192.168.1.10	Stack (ION)

Polling Interval: ○ None ● Interval 2 Minute

8. Use the other available buttons as desired (Refresh, Filter, Polling, Open, Save, Clear, Print, and/or Expand Enterprise):

Refresh: updates the screen data.

Filter: lists Generic Traps selectable from the dropdown on the Filter tab (49 total; 17 ION traps plus 32 PS traps).

See 'FP 3.0 Traps List' on page 75 for the list of supported trap types.

Polling: lets you define polling interval (None or Interval), and select a unit of measure if 'Interval' is selected. There is no limitation for the maximum intervals; enter a value greater than zero.

Open: opens an 'Open' dialog box which lets you select a trap from a list on which to open a Traps Log View window.

Save: Opens a Save dialog box which lets you select a log file save location.

Clear: Clears all of the existing traps.

Print: Lets you print to a local or networked printer. This prints the traps table including the table header and grid lines.

Expand Enterprise: Expand Enterprise / Shrink Enterprise button. Click the 'Expand Enterprise' button to change the "Enterprise" column to the "Expanded Enterprise" with additional information capacity. If the "Expanded Enterprise" is currently displayed, click the Shrink Enterprise button to display the narrower "Enterprise" column.

9. When done click the **Stop Server** button to stop the Trap Server and continue with the **Email Profile Configuration** section below.

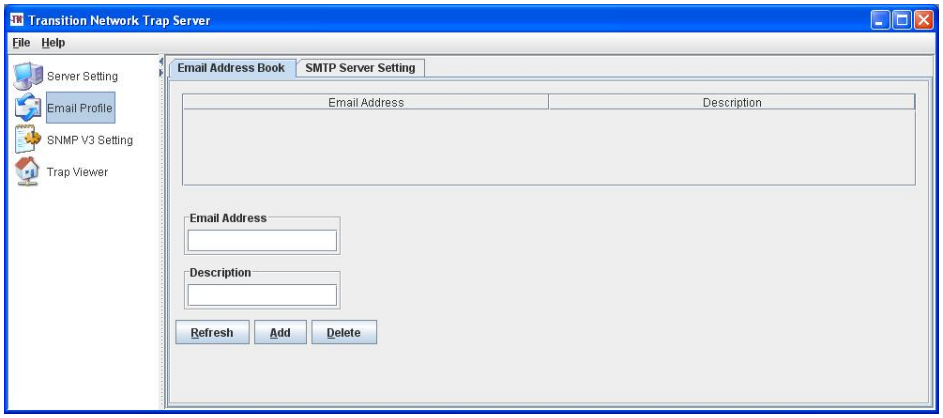
2. Email Profile Configuration

The **Trap Server** > **Email Profile** menu path lets you define the necessary **Email Address Book** and **SMTP Server Setting**s for email or other notification.

Email Address Book Configuration

Here you set up email addresses for trap notifications.

1. Select the **Email Address Book** tab.



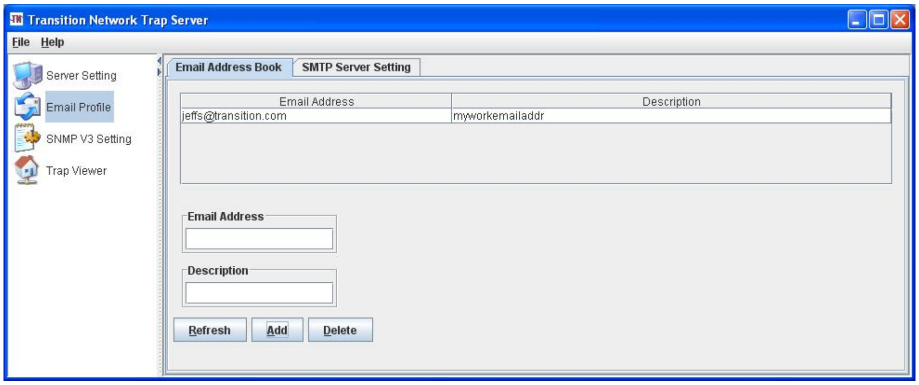
2. In the **Email Address** entry field, enter an active email address in a valid email address format.

3. In the **Description** entry field, enter some descriptive text to help describe this email address / person.

4. Click the **Add** button to list this email address / description in the Email Address Book table.

5. Repeat steps 2-4 for each email address to receive notifications.

6. Click the **Refresh** button when done and verify the Email Address Book table entries.



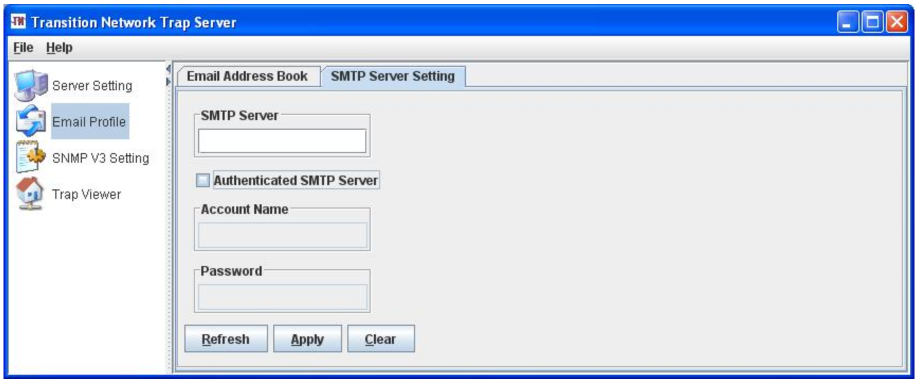
Email Address	Description
jeffs@transition.com	myworkemailaddr

7. To delete an entry from the table, highlight the entry and click the **Delete** button.

SMTP Server Setting

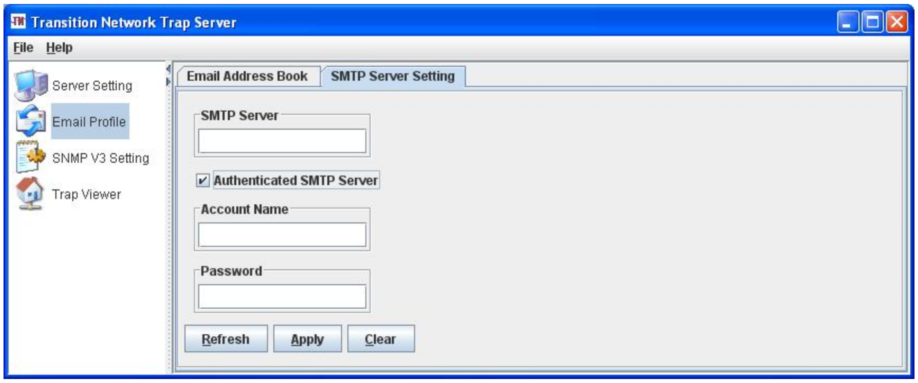
An SMTP server is a computer used for or dedicated to SMTP server functions; it may or may not use uthentication. An Authenticated SMTP Server is an SMTP server that provides user authentication, and requires an account name and password. The service extension (per IETF RFC 4954) allows SMTP sessions to be authenticated.

1. Navigate to the **Trap Server** > **Email Profile** > **SMTP Server Setting** menu path.



2. In the **SMTP Server** entry field, enter the IP address of the SMTP server to be configured. Because an SMTP server address may contain non-digital (alpha) characters, something like "127.0.com" will be regarded as valid (“127.0.com” will be regarded as a domain name, not an IP address). If all characters between two "." characters are numeric characters, the SMTP server will be treated as an IP and checked in another way.

3. Check or uncheck the **Authenticated SMTP Server** checkbox. If checked (enabled), the **Account Name** and **Password** fields become active.



4. In the **Account Name** entry field, enter the email account name of the SMTP server (if authenticated).

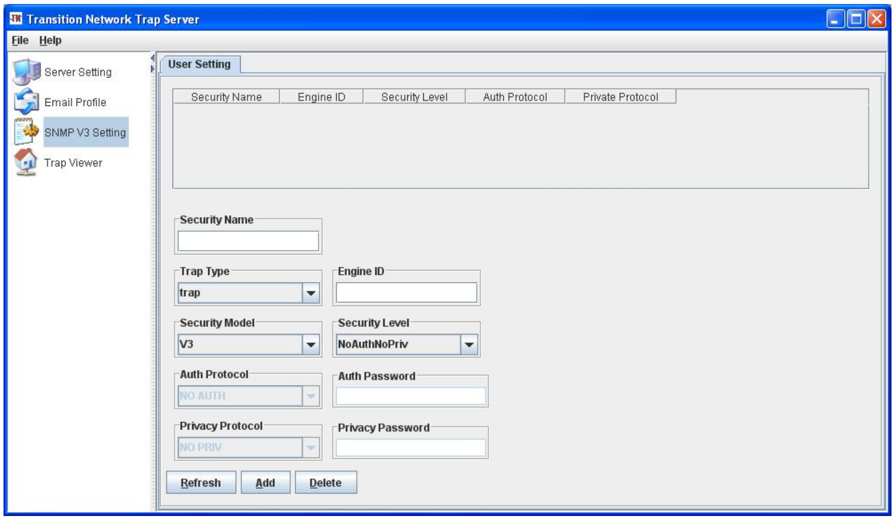
5. In the **Password** entry field, enter the password for the SMTP server (if authenticated). This entry displays in ciphertext.

6. When done at the **SMTP Server Settings** tab, click the **Apply** button. You can use the "**Clear**" button to clear the entry before saving.

3. SNMP V3 Setting

SNMP V3 User Settings

1. Navigate to the **Trap Server** > **SNMP V3 Setting** > **User Setting** menu path.



Security Name:

Trap Type: trap

Engine ID:

Security Model: V3

Security Level: NoAuthNoPriv

Auth Protocol: NO AUTH

Auth Password:

Privacy Protocol: NO PRIV

Privacy Password:

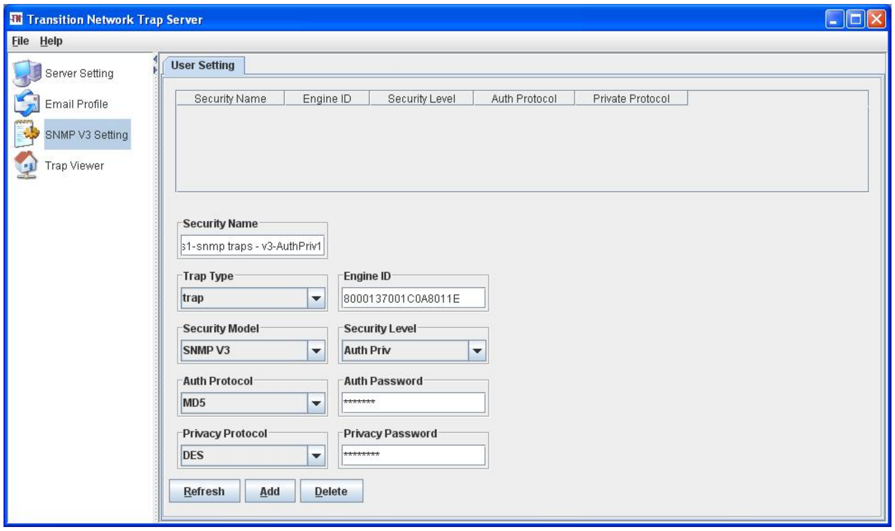
2. In the **Security Name** field, enter a unique, valid security name for this user.
3. At the **Trap Type** dropdown, select **trap** or **inform**.
4. In the **Engine ID** field, enter a valid, defined SNMP Engine ID (not needed if '**inform**' was selected in step 3 above).
   If "inform" is selected in the "Trap Type" field, the Engine ID will be forced to be the remote Engine ID which is displayed in the "Trap Server Setting" panel.
   If "trap" is selected in the "Trap Type" field, the Engine ID can automatically detected by the Trap Server if it is kept blank.
   Or you can input a specific Engine ID which is defined in the equipment. Normally this case happens when multiple equipments are using the same security name.
5. At the **Security Model** dropdown, select **SNMP V3**.
6. At the Security Level dropdown, select **Auth Priv**, **Auth No Priv**, or **No Auth No Priv**, where:

   Auth Priv = Authentication and Privacy

   Auth No Priv = Authentication but No Privacy

   No Auth No Priv = No Authentication and No Privacy
7. At the **Auth Protocol** dropdown, select MD5 or SHA as the Authentication protocol.
8. In the **Auth Password** field, enter an authentication password of 8 - 16 alphanumeric characters.
9. At the **Privacy Protocol** dropdown, select DES or AES as the privacy protocol.
10. In the **Privacy Password** field, enter a privacy password of 8 - 16 alphanumeric characters.

11. When done, verify your entries and selections and then click the **Add** button.



Security Name	Engine ID	Security Level	Auth Protocol	Private Protocol

Security Name: s1-snmp traps - v3-AuthPriv1

Trap Type: trap

Engine ID: 8000137001C0A8011E

Security Model: SNMP V3

Security Level: Auth Priv

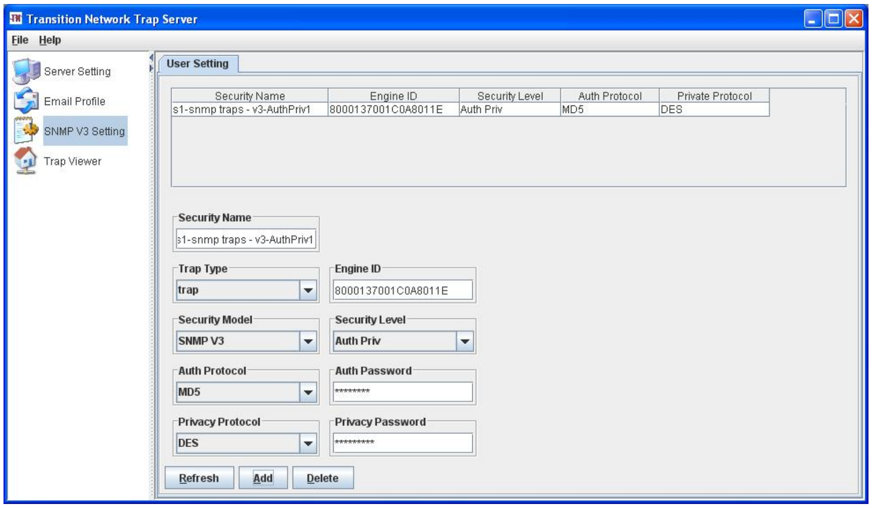
Auth Protocol: MD5

Auth Password: *******

Privacy Protocol: DES

Privacy Password: ********

12. Click the **Add** button. The new user setting is added to the table.



Security Name	Engine ID	Security Level	Auth Protocol	Private Protocol
s1-snmp traps - v3-AuthPriv1	8000137001C0A8011E	Auth Priv	MD5	DES

Security Name: s1-snmp traps - v3-AuthPriv1

Trap Type: trap

Engine ID: 8000137001C0A8011E

Security Model: SNMP V3

Security Level: Auth Priv

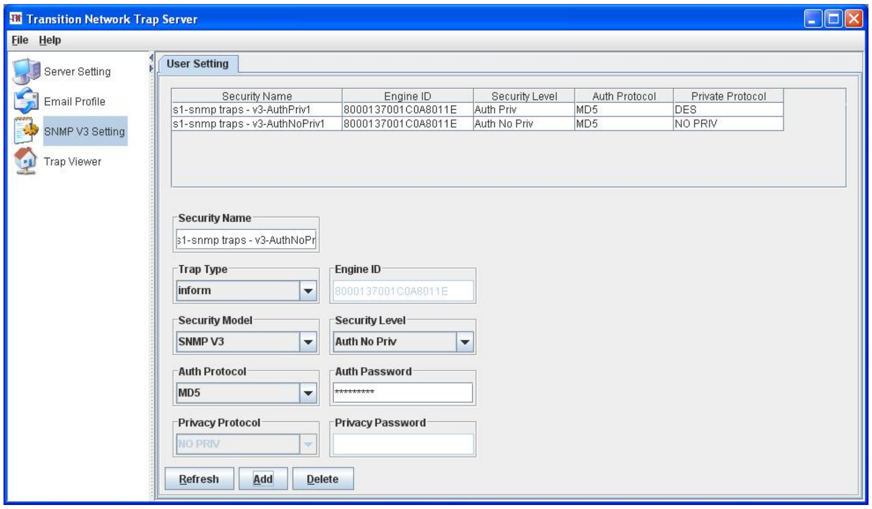
Auth Protocol: MD5

Auth Password: ********

Privacy Protocol: DES

Privacy Password: *********

13. Repeat steps 2 through 12 for each user to be configured.



Security Name	Engine ID	Security Level	Auth Protocol	Private Protocol
s1-snmp traps - v3-AuthPriv1	8000137001C0A8011E	Auth Priv	MD5	DES
s1-snmp traps - v3-AuthNoPriv1	8000137001C0A8011E	Auth No Priv	MD5	NO PRIV

Security Name: s1-snmp traps - v3-AuthNoPr

Trap Type: inform

Engine ID: 8000137001C0A8011E

Security Model: SNMP V3

Security Level: Auth No Priv

Auth Protocol: MD5

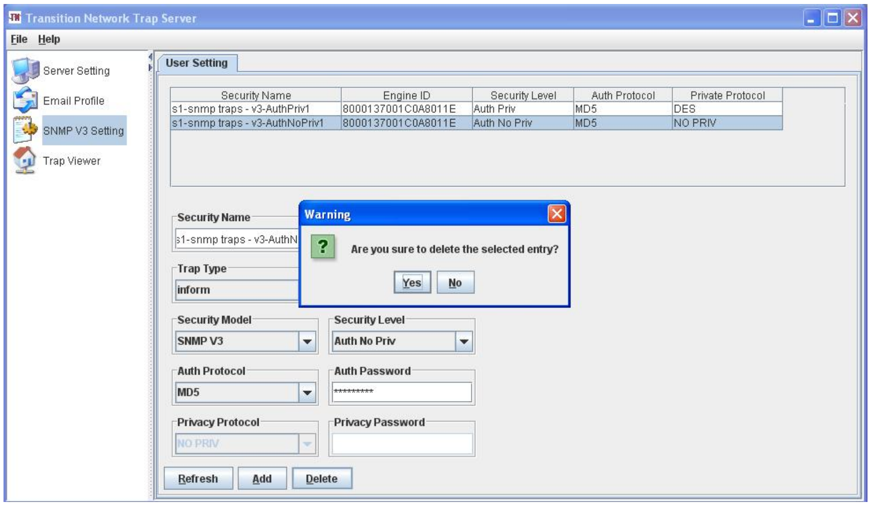
Auth Password: *********

Privacy Protocol: NO PRIV

Privacy Password:

Delete a User Setting Entry

To delete an existing entry from the table, highlight the entry and click the **Delete** button. At the *Warning* message, click the **Yes** button. The selected message is removed from the table.



Security Name	Engine ID	Security Level	Auth Protocol	Private Protocol
s1-snmp traps - v3-AuthPriv1	8000137001C0A8011E	Auth Priv	MD5	DES
s1-snmp traps - v3-AuthNoPriv1	8000137001C0A8011E	Auth No Priv	MD5	NO PRIV

Security Name: s1-snmp traps - v3-AuthN

Trap Type: inform

Security Model: SNMP V3

Security Level: Auth No Priv

Auth Protocol: MD5

Auth Password: *********

Privacy Protocol: NO PRIV

Privacy Password:

Warning

Are you sure to delete the selected entry?

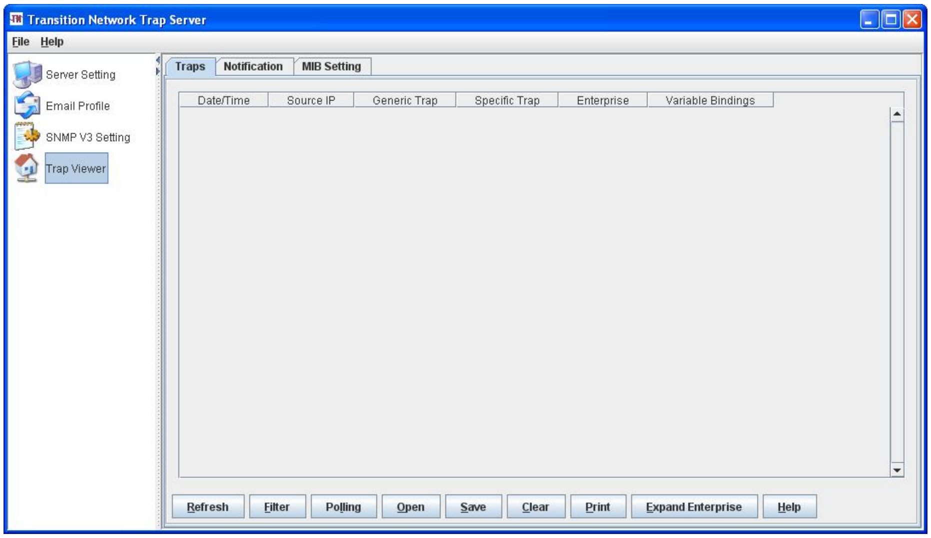
Yes No

4. Trap Viewer Configuration

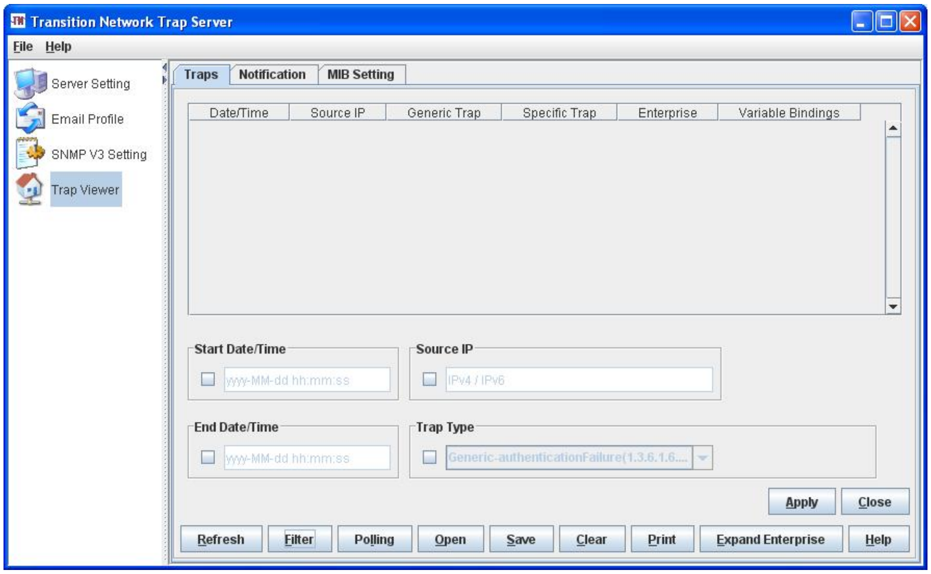
The **Trap Server** > **Trap Viewer** menu path lets you define traps and notifications and open MIB settings.
You can elect to be notified of the selected conditions via Audio beep, E-mail, Process Group Control String, or by Hints. The email function uses the JavaMail API to send email via SMTP. The Trap Server uses SMTP as a client to send simple emails.

Configure Traps

1. Navigate to the **Trap Server** > **Trap Viewer** > **Traps** menu path. The initial **Trap Viewer** > **Traps** tab screen displays.

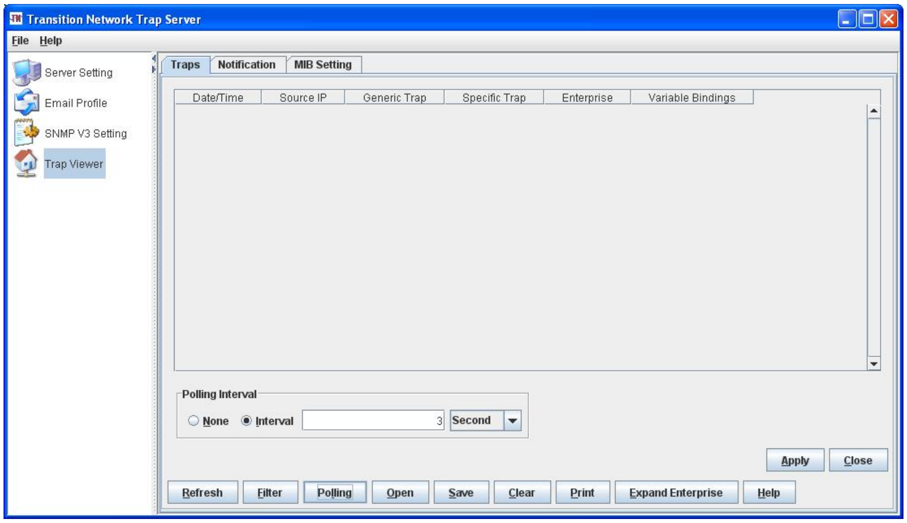


2. Click the **Filter** button. The filter parameters display.



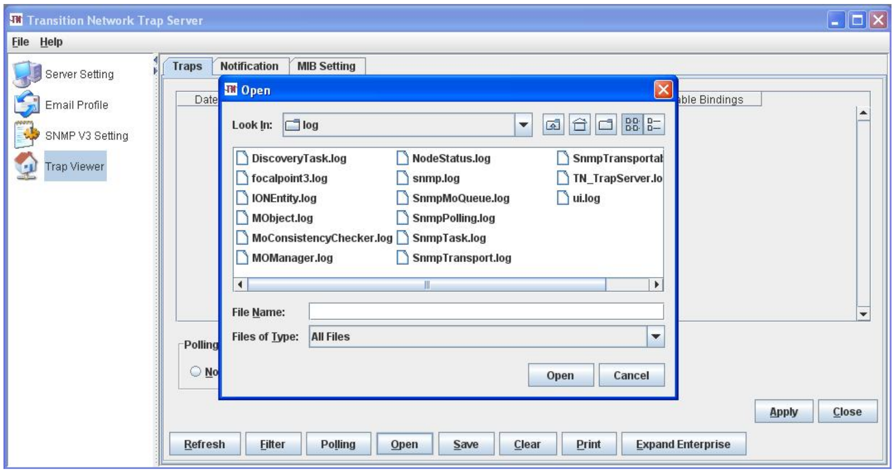
3. Check the **Start Date / Time** checkbox and enter a date and time in the required format (*yyyy-mm-dd hh-mm-ss*).
   A light gray hint text is provided. When you put the mouse cursor in the text field, the hint message clears. Once you input a wrong format, the text displays in red to indicate an incorrect format entry.
4. Check the **End Date / Time** checkbox and enter a date and time in the required format (*yyyy-mm-dd hh-mm-ss*).

5. Check the **Source IP** checkbox and enter an IPv4 or IPv6 source IP address in the required format (e.g., 192.168.1.10). The Source IP address box can be used to show traps from a particular IP address. By default, traps from all IP addresses are shown.
6. Check the **Trap Type** checkbox and select a trap from the dropdown (e.g., **ION_authenticationFailure** shown above). There are 51 traps in total (ION traps plus Point System traps). See 'FP 3.0 Traps List' on page 75 for the full list of supported trap types.
7. Click the **Apply** button. The **Polling Interval** configuration page displays.



Polling Interval
○ None ● Interval 3 Second

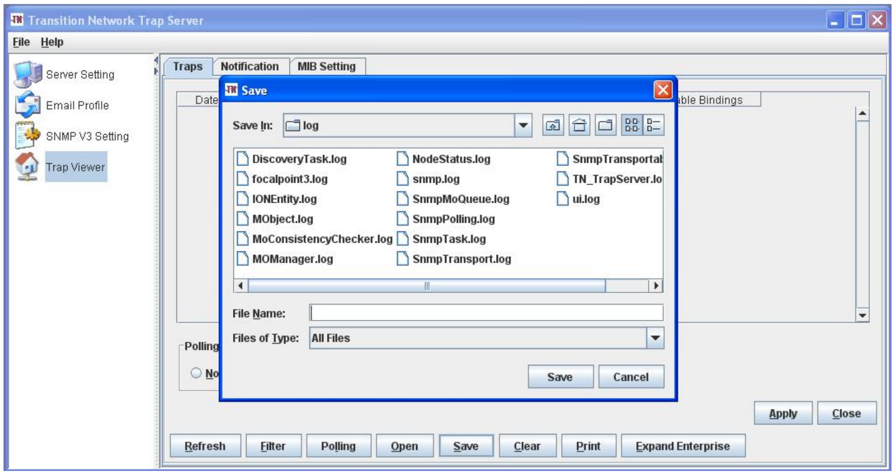
8. Click the **Polling** button. The **Polling Interval** configuration page displays.
9. Click the desired polling interval (**None** or **Interval**) radio button. If you want to define the polling interval, select **Interval** and enter a value and select a unit of measure from the dropdown (e.g., **3 Seconds** shown above). There is no limitation for the maximum intervals; enter a value greater than zero. The default polling value is every **3** seconds. Here you can define how long to wait to refresh the table view automatically, by reading data from the log file (not the device).
The mechanism is: 1) the Trap Server sets up a server socket (UDP) to listen to the traps received from the device in a passive way (not polling data to get traps from device).
2) once a trap is received, this trap will be translated and written to the log file (i.e., *TN_TrapServer.log*).
3) there is a polling thread running to read data from the log file and display it in the table view at the interval defined.
10. Click the **Apply** button.
11. Click the **Open** button. The **Open** dialog box displays.



Look In: log
Files of Type: All Files

12. Select a File Name and click the **Open** button.
13. Click the **Apply** button.

14. Click the **Save** button. The **Save** dialog box displays.


Transition Network Trap Server
File Help
Server Setting
Email Profile
SNMP V3 Setting
Trap Viewer
Traps Notification MIB Setting
Date
ble Bindings
Polling
No
Save
Refresh Filter Polling Open Save Clear Print Expand Enterprise
Apply Close
Save Cancel

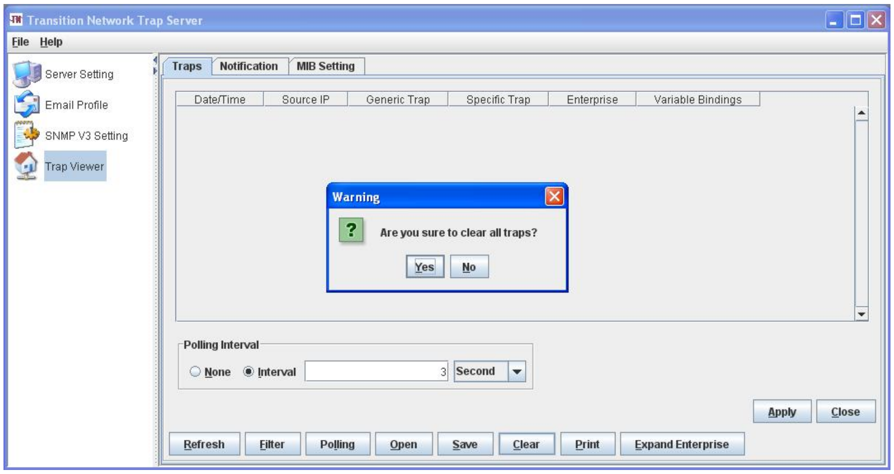
Save In: log

DiscoveryTask.log
focalpoint3.log
IONEntity.log
MObject.log
MoConsistencyChecker.log
MOManager.log
NodeStatus.log
snmp.log
SnmpMoQueue.log
SnmpPolling.log
SnmpTask.log
SnmpTransport.log
SnmpTransportat
TN_TrapServer.lo
ui.log

File Name:

Files of Type: All Files

15. Enter a File Name and click the **Save** button.
16. Click the **Apply** button.
17. Click the **Clear** button. The message "*Are you sure you want to clear all traps*? displays.

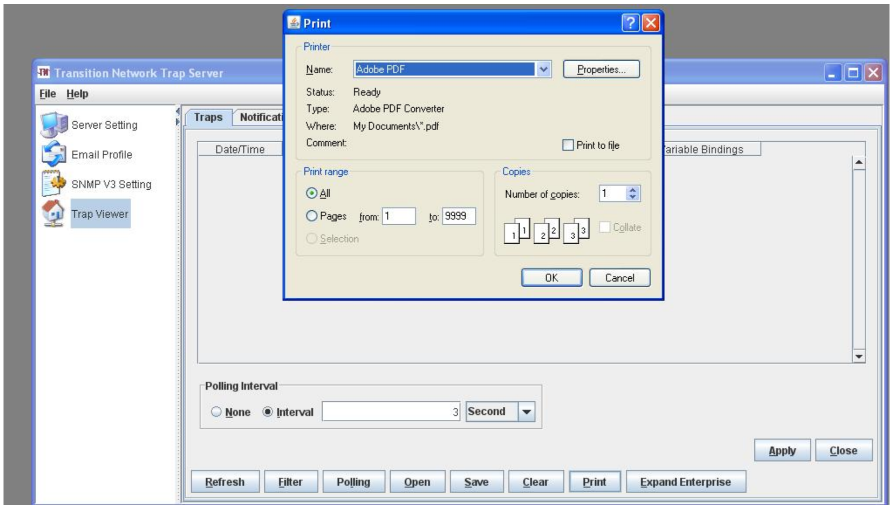

Transition Network Trap Server
File Help
Server Setting
Email Profile
SNMP V3 Setting
Trap Viewer
Traps Notification MIB Setting
Date/Time Source IP Generic Trap Specific Trap Enterprise Variable Bindings
Warning
Yes No
Apply Close
Refresh Filter Polling Open Save Clear Print Expand Enterprise

Are you sure to clear all traps?

Polling Interval

○ None ● Interval 3 Second

18. If you want to clear all of the traps click **Yes**. Otherwise click **No**.
19. Click the **Apply** button.
20. Click the **Print** button. The **Print** dialog box displays.



Printer

Name: Adobe PDF

Status: Ready

Type: Adobe PDF Converter

Where: My Documents*.pdf

Comment:

□ Print to file

Print range

● All

○ Pages from: 1 to: 9999

○ Selection

Copies

Number of copies: 1

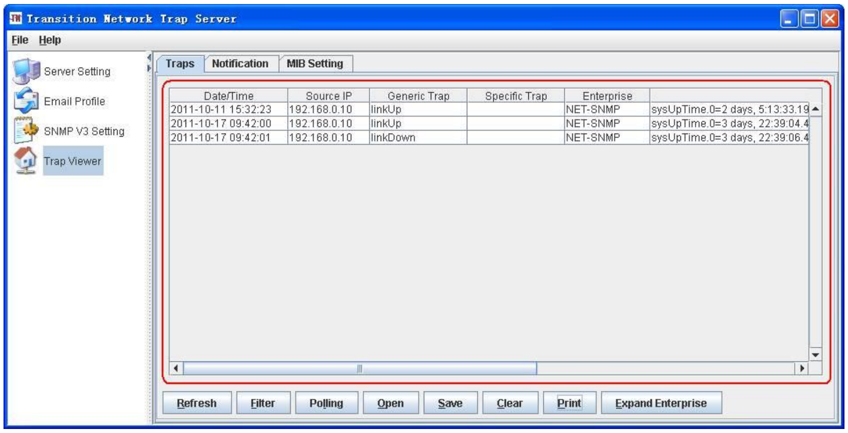
□ Collate

Polling Interval

○ None ● Interval 3 Second

21. Select a Printer Name, optional Properties, Print Range, and Number of copies to print and then click the **OK** button.

    The traps table prints, including the table header and grid lines. On the screen below picture, the circled area will be printed.

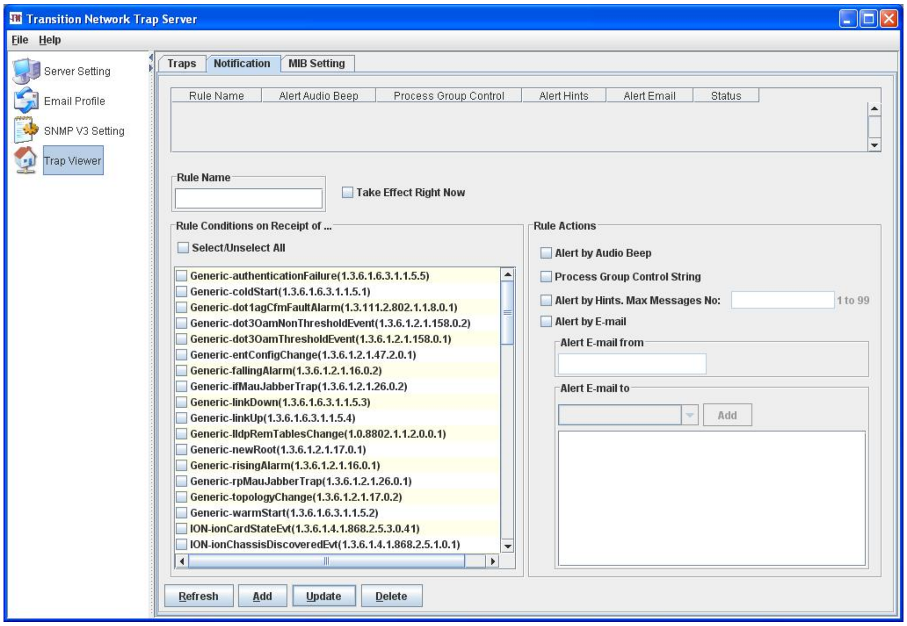


Date/Time	Source IP	Generic Trap	Specific Trap	Enterprise	
2011-10-11 15:32:23	192.168.0.10	linkUp		NET-SNMP	sysUpTime.0=2 days, 5:13:33.19
2011-10-17 09:42:00	192.168.0.10	linkUp		NET-SNMP	sysUpTime.0=3 days, 22:39:04.4
2011-10-17 09:42:01	192.168.0.10	linkDown		NET-SNMP	sysUpTime.0=3 days, 22:39:06.4

22. Alternately click the **Expand Enterprise** button to expand and contract the Enterprise column data displayed.

Configure Notifications

1. Navigate to the **Trap Server** > **Trap Viewer** > **Notification** menu path. The initial **Trap Viewer** > **Notification** tab screen displays.


Transition Network Trap Server
File
Help
Server Setting
Email Profile
SNMP V3 Setting
Trap Viewer
Traps
Notification
MIB Setting
Rule Name
Alert Audio Beep
Process Group Control
Alert Hints
Alert Email
Status
Rule Name
□ Take Effect Right Now
Rule Conditions on Receipt of ...
□ Select/Unselect All
□ Generic-authenticationFailure(1.3.6.1.6.3.1.1.5.5)
□ Generic-coldStart(1.3.6.1.6.3.1.1.5.1)
□ Generic-dot1agCfmFaultAlarm(1.3.111.2.802.1.1.8.0.1)
□ Generic-dot3OamNonThresholdEvent(1.3.6.1.2.1.158.0.2)
□ Generic-dot3OamThresholdEvent(1.3.6.1.2.1.158.0.1)
□ Generic-entConfigChange(1.3.6.1.2.1.47.2.0.1)
□ Generic-fallingAlarm(1.3.6.1.2.1.16.0.2)
□ Generic-ifMauJabberTrap(1.3.6.1.2.1.26.0.2)
□ Generic-linkDown(1.3.6.1.6.3.1.1.5.3)
□ Generic-linkUp(1.3.6.1.6.3.1.1.5.4)
□ Generic-lldpRemTablesChange(1.0.8802.1.1.2.0.0.1)
□ Generic-newRoot(1.3.6.1.2.1.17.0.1)
□ Generic-risingAlarm(1.3.6.1.2.1.16.0.1)
□ Generic-rpMauJabberTrap(1.3.6.1.2.1.26.0.1)
□ Generic-topologyChange(1.3.6.1.2.1.17.0.2)
□ Generic-warmStart(1.3.6.1.6.3.1.1.5.2)
□ ION-ionCardStateEvt(1.3.6.1.4.1.868.2.5.3.0.41)
□ ION-ionChassisDiscoveredEvt(1.3.6.1.4.1.868.2.5.1.0.1)
Rule Actions
□ Alert by Audio Beep
□ Process Group Control String
□ Alert by Hints. Max Messages No:
1 to 99
□ Alert by E-mail
Alert E-mail from
Alert E-mail to
Add
Refresh
Add
Update
Delete

2. In the **Rule Name** field, enter a name for this rule (e.g., '*AskMeOnlyIf*' in the example below).

3. Check the **Take Effect Right Now** checkbox if you want to have the new rule take effect immediately. If left unchecked, the rule the rule will be just kept there (to inhibit the rule temporarily).

4. In the **Rule Conditions on Receipt of ...** area, check the desired checkboxes (e.g., *ION_coldStart*, *ION_fallingAlarm*, etc.). All trap types items have their OID included after the name.

5. In the **Rule Actions** section check one or more checkboxes for how you want to be notified of the selected conditions from step 4 (Alert by Audio Beep, Alert by E-mail, Process Group Control String, Alert by Hints).

   □ At the **Alert by Audio Beep** checkbox, check the box if audio beeps notification is desired. If the received trap matches the rule, a sound is sent from the PC (normally a speaker installed in the PC case).

   □ Check the **Process Group Control String** checkbox to have the Point System groups to which the system should currently be applying all configuration changes be set automatically by your system. This is the Agent II Group Control String function for Chassis 2 configuration management - Group String Processing. This selection does not apply to the ION System.

   Because a Chassis-2 stack may contain dozens of devices, it is useful to have a method for applying a single management operation to more than one device. To this end, it is possible to cause the Chassis-2 SNMP agent to replicate an operation (i.e., one variable binding in an SNMP SET request) and apply it to an entire group of MIB variables. The user does this by assigning one or more user-defined "group" keywords to each managed device, and then using a group control string to direct SET operations to all devices that are in the groups named in the control string. For example: an end user has chosen to assign group keywords that indicate the city and department served by each card in their stack.

   Departments: mfg acct eng mktg
   Locations: ord msp bos atl

   As each device is installed, it is assigned a group string. Given the scheme chosen by this end user, a device serving the accounting department in Atlanta would have the group string "atl acct". These strings remain assigned to the devices until deliberately changed by the system administrator.

   To apply a change to the entire accounting department, the end user would set the group control string to "acct" and then make the changes to individual devices. Changes made to devices while the group control string is not null are applied to all devices with matching group strings, rather than to the individual device whose details screen is used to make the changes.

   Group Control String Functions

The group control string contains one or more user-defined group keywords and special unary operators described below. Note that *all* operations specified in the group control string must be satisfied for a match to occur. Although operators may affect one another, the use of one operator does not make the satisfaction of any other operator "optional."

PICK ONE: allows the specification of one or more keywords, at least one of which must occur in the target string for a match to occur. This requirement must be met regardless of the use of other functions. PICK ONE is invoked by adding a '.' to the beginning of the keyword. The PICK ONE function is the default if no function character is specified.

REQUIRED: allows the specification of keywords that are mandatory for a match to occur. It is invoked by adding a '+' sign to the beginning of the keyword. Every keyword in the group control string that has the REQUIRED operator must be present in the device group string for a match to occur.

PROHIBITED: allows the specification of keywords that are forbidden for a match to occur. It is invoked by adding a '-' or '!' sign to the beginning of the keyword. No keyword in the group control string that has the PROHIBITED operator may be present in the device group string for a match to occur. PROHIBITED takes precedence over REQUIRED and ANY.

WILDCARD: The '*' sign is a wildcard that matches zero or more characters in a keyword. There can be only one '*' sign in any one keyword in the group control string. If more than one '*' is used, the match always fails.

Example group control strings and the devices they match (using the keywords from the previous example):

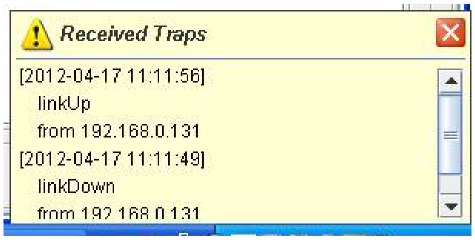
".eng .mktg" - all devices serving either the engineering or marketing departments.

"+atl eng mktg" - all devices that serve either engineering or marketing in Atlanta only. Note the use of the alternate form of the PICK ONE operator.

* -m*" - all devices excluding those that serve marketing or manufacturing, and all of Minneapolis.
"* -m* !eng" - all devices excluding those that serve marketing or manufacturing, and all of Minneapolis except engineering.

- □ Check the **Alert by Hints.** checkbox if you want a popup message to display in the corner of your desktop each time a trap is received.

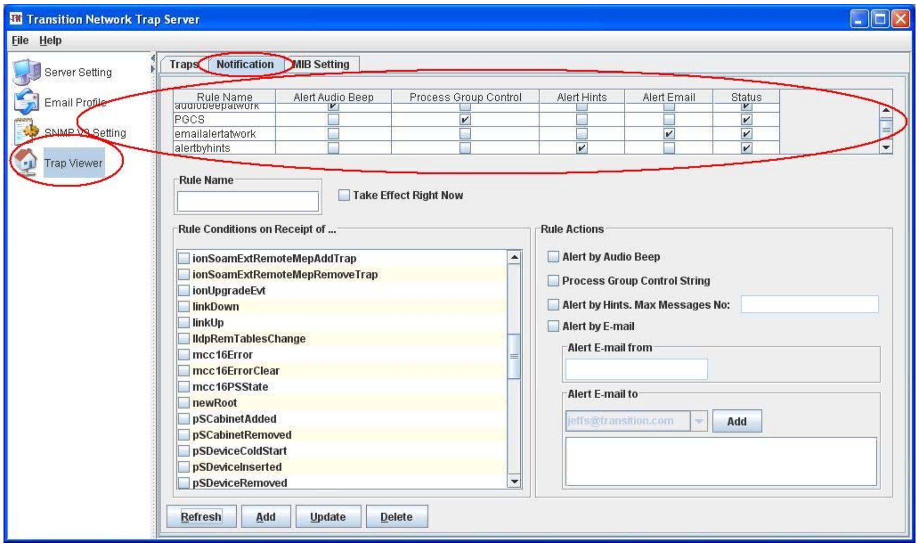
  If checked, enter a number from 1 to 99 in the **Max Messages No:** entry field. For example, if you set it to “3”, there would be a maximum of 3 messages displayed in the popup up window.



[2012-04-17 11:11:56]
linkUp
from 192.168.0.131
[2012-04-17 11:11:49]
linkDown
from 192.168.0.131

- □ At the **Alert by E-mail** checkbox, check the box if email notification is desired. If checked, in the **Alert E-mail from** entry box, enter a valid email address for the displayed source of these email alerts (e.g., TNTrapViewer1@TN.com). This lets your organization create a special email account which is responsible for sending email to corresponding owners when traps are received.
- □ In the **Alert E-mail to** dropdown, enter a valid email address which is to receive email alerts (e.g., jeff_x@transition.com).

6. When done, click the **Add** button. The Rule information is added to the table (see below).



Rule Name	Alert Audio Beep	Process Group Control	Alert Hints	Alert Email	Status
audiobeepatwork	☑	□	□	□	☑
PGCS	□	☑	□	□	☑
emailalertatwork	□	□	□	☑	☑
alertbyhints	□	□	☑	□	☑

Rule Name

□ Take Effect Right Now

Rule Conditions on Receipt of ...

□ ionSoamExtRemoteMepAddTrap
□ ionSoamExtRemoteMepRemoveTrap
□ ionUpgradeEvt
□ linkDown
□ linkUp
□ lldpRemTablesChange
□ mcc16Error
□ mcc16ErrorClear
□ mcc16PSState
□ newRoot
□ pSCabinetAdded
□ pSCabinetRemoved
□ pSDeviceColdStart
□ pSDeviceInserted
□ pSDeviceRemoved

Rule Actions

□ Alert by Audio Beep
□ Process Group Control String
□ Alert by Hints. Max Messages No:
□ Alert by E-mail

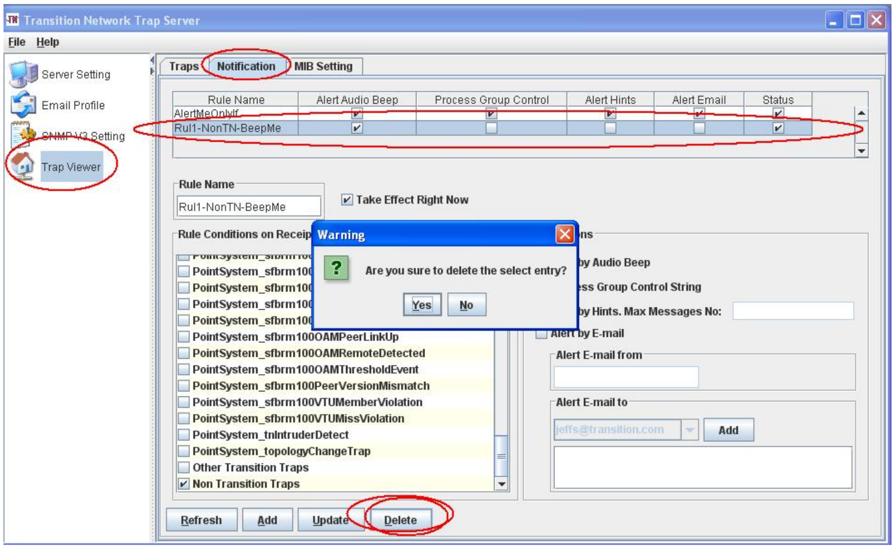
Alert E-mail from

Alert E-mail to: jeffs@transition.com

10. Verify your entries. If necessary, delete one or more notification entries as explained below. Otherwise continue to the 'Configure MIB Setting' section on page 55.

Delete a Notifications Entry

To delete an existing entry from the table, highlight the entry and click the **Delete** button. At the Warning message "*Are you sure to delete the selected entry?*, click the **Yes** button..



Rule Name	Alert Audio Beep	Process Group Control	Alert Hints	Alert Email	Status
AlertMeOnlyIf	☑	☑	☑	☑	☑
Rul1-NonTN-BeepMe	☑	□	□	□	☑

Rule Name: Rul1-NonTN-BeepMe

☑ Take Effect Right Now

Warning

Are you sure to delete the select entry?

Rule Conditions on Receip

□ PointSystem_sfbrm10
□ PointSystem_sfbrm10
□ PointSystem_sfbrm10
□ PointSystem_sfbrm10
□ PointSystem_sfbrm100OAMPeerLinkUp
□ PointSystem_sfbrm100OAMRemoteDetected
□ PointSystem_sfbrm100OAMThresholdEvent
□ PointSystem_sfbrm100PeerVersionMismatch
□ PointSystem_sfbrm100VTUMemberViolation
□ PointSystem_sfbrm100VTUMissViolation
□ PointSystem_tnIntruderDetect
□ PointSystem_topologyChangeTrap
□ Other Transition Traps
☑ Non Transition Traps

□ by Audio Beep
□ ss Group Control String
□ by Hints. Max Messages No:
□ Alert by E-mail

Alert E-mail from

Alert E-mail to: jeffs@transition.com

The selected entry is removed from the table.

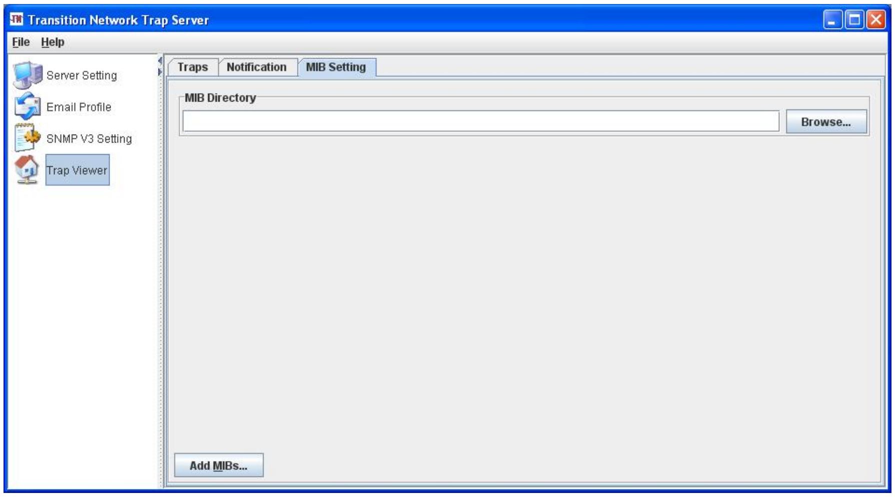
Configure MIB Setting

Here you can select a directory which will contain the MIB files to parse. Note that only the directories are visible, because the file chooser hides all files in the directory.

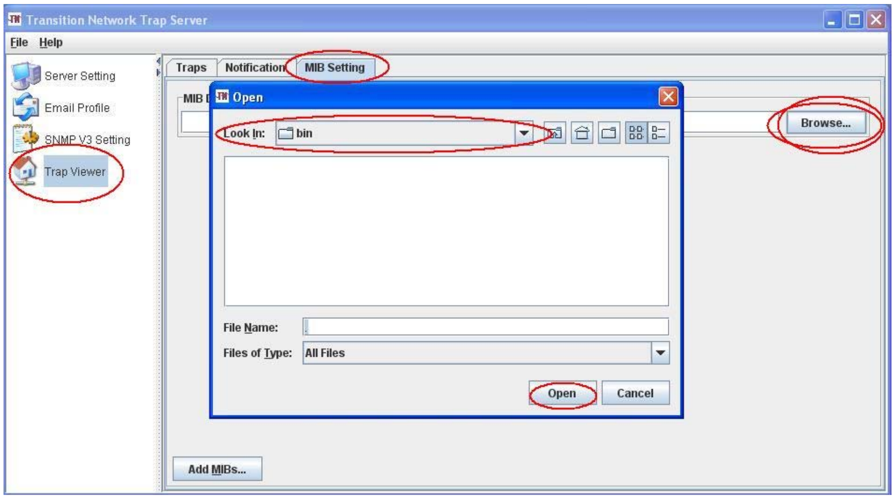
The MIB Directory parameter can be used to change the location of MIB files which are to be loaded by the Receiver. The **Browse** button can be used to select the new location. New MIBs can be added to the list of MIBs loaded by the Receiver by clicking the **Add MIBs**... button. This allows selection of multiple MIB files using mouse and control keys. The file chooser only allows you to choose a directory which may contains multiple MIB files. You cannot select MIB files under the directory.

Unless the **Save Configuration** button is pressed, changes to configuration are not saved.

1. Navigate to the **Trap Server** > **Trap Viewer** > **MIB Setting** menu path.



2. Click the **Browse ...** button. The **Open** dialog box displays.



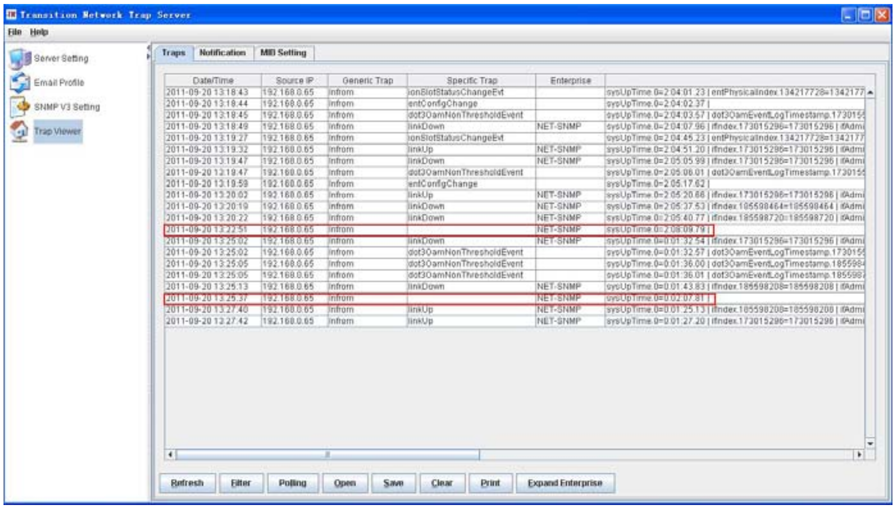
3. Navigate to and select a directory to contain the MIB files to parse (*e.g. D:\Other Devices\MIB\*).
4. In the filename entry field, enter a valid MIB filename to be uploaded (e.g., with a *.bin* file extension).
5. Click the **Open** button.
6. Click the **Add MIBs...** button to add a selected directory which will contain the MIB files to parse.
7. If you navigate to and select an invalid MIB directory and then click the **Add MIBs...** button to select it, an error message displays along with the **Clear** button. Click the **Clear** button to clear the error message, and then navigate to and select a valid MIB directory.

Interpret Traps

Two categories of traps exist: generic and enterprise-specific. There are several generic trap numbers defined for conditions ranging from system reboots (coldStart) and interface state changes (linkUp and linkDown) to generic traps (e.g., enterpriseSpecific). Enterprise-specific traps extend the trap mechanism's power; anyone with an enterprise number can define enterprise-specific traps for whatever conditions they consider worth monitoring.

An enterprise-specific trap is identified by two pieces of information: the enterprise ID of the organization that defined the trap and a specific trap number assigned by that organization. The notion of an enterprise-specific trap is extremely flexible, because organizations are allowed to subdivide their enterprises as much as they like. For example, if your enterprise number is 2789, your enterprise ID is .1.3.6.1.4.1.2789. But you can further subdivide this, defining traps with enterprise IDs such as .1.3.6.1.4.1.2789.5000, .1.3.6.1.4.1.2789.5001, and so on.

Sample Trap results are displayed as shown below.



Date/Time	Source IP	Generic Trap	Specific Trap	Enterprise	
2011-09-20 13:18:43	192.168.0.65	infrom	ionSlotStatusChangeEvt		sysUpTime.0=2:04:01.23 | entPhysicalIndex.134217728=1342177
2011-09-20 13:18:44	192.168.0.65	infrom	entConfigChange		sysUpTime.0=2:04:02.37 |
2011-09-20 13:18:45	192.168.0.65	infrom	dot3OamNonThresholdEvent		sysUpTime.0=2:04:03.57 | dot3OamEventLogTimestamp.173015
2011-09-20 13:18:49	192.168.0.65	infrom	linkDown	NET-SNMP	sysUpTime.0=2:04:07.96 | ifIndex.173015296=173015296 | ifAdmi
2011-09-20 13:19:27	192.168.0.65	infrom	ionSlotStatusChangeEvt		sysUpTime.0=2:04:45.23 | entPhysicalIndex.134217728=1342177
2011-09-20 13:19:32	192.168.0.65	infrom	linkUp	NET-SNMP	sysUpTime.0=2:04:51.20 | ifIndex.173015296=173015296 | ifAdmi
2011-09-20 13:19:47	192.168.0.65	infrom	linkDown	NET-SNMP	sysUpTime.0=2:05:05.99 | ifIndex.173015296=173015296 | ifAdmi
2011-09-20 13:19:47	192.168.0.65	infrom	dot3OamNonThresholdEvent		sysUpTime.0=2:05:06.01 | dot3OamEventLogTimestamp.173015
2011-09-20 13:19:59	192.168.0.65	infrom	entConfigChange		sysUpTime.0=2:05:17.62 |
2011-09-20 13:20:02	192.168.0.65	infrom	linkUp	NET-SNMP	sysUpTime.0=2:05:20.66 | ifIndex.173015296=173015296 | ifAdmi
2011-09-20 13:20:19	192.168.0.65	infrom	linkDown	NET-SNMP	sysUpTime.0=2:05:37.53 | ifIndex.185598464=185598464 | ifAdmi
2011-09-20 13:20:22	192.168.0.65	infrom	linkDown	NET-SNMP	sysUpTime.0=2:05:40.77 | ifIndex.185598720=185598720 | ifAdmi
2011-09-20 13:22:51	192.168.0.65	infrom		NET-SNMP	sysUpTime.0=2:08:09.79 |
2011-09-20 13:25:02	192.168.0.65	infrom	linkDown	NET-SNMP	sysUpTime.0=0:01:32.54 | ifIndex.173015296=173015296 | ifAdmi
2011-09-20 13:25:02	192.168.0.65	infrom	dot3OamNonThresholdEvent		sysUpTime.0=0:01:32.57 | dot3OamEventLogTimestamp.173015
2011-09-20 13:25:05	192.168.0.65	infrom	dot3OamNonThresholdEvent		sysUpTime.0=0:01:36.00 | dot3OamEventLogTimestamp.185598
2011-09-20 13:25:05	192.168.0.65	infrom	dot3OamNonThresholdEvent		sysUpTime.0=0:01:36.01 | dot3OamEventLogTimestamp.185598
2011-09-20 13:25:13	192.168.0.65	infrom	linkDown	NET-SNMP	sysUpTime.0=0:01:43.83 | ifIndex.185598208=185598208 | ifAdmi
2011-09-20 13:25:37	192.168.0.65	infrom		NET-SNMP	sysUpTime.0=0:02:07.81 |
2011-09-20 13:27:40	192.168.0.65	infrom	linkUp	NET-SNMP	sysUpTime.0=0:01:25.13 | ifIndex.185598208=185598208 | ifAdmi
2011-09-20 13:27:42	192.168.0.65	infrom	linkUp	NET-SNMP	sysUpTime.0=0:01:27.20 | ifIndex.173015296=173015296 | ifAdmi

The fact that you received a trap and know its generic trap number, enterprise ID, and specific trap number may be all you need to diagnose a problem. But traps also carry additional information. In the case of generic traps, the specific information is predefined and hardwired into the NMS. When you receive a generic trap, the NMS knows how to interpret the information it contains and will be able to display it appropriately, whether it's the time of the reboot or the identity of the interface that just changed state. In contrast, the information carried by an enterprise-specific trap is entirely up to the person who defined the trap. An enterprise-specific trap can contain any number of variable bindings, or MIB object-value pairs.

Traps are sorted in ascending order by the column of **Date/Time**. Note that the sorting function is not supported in the Traps Viewer in this release, since data in this viewer could always be refreshed by polling, which will rearrange the sorted data.

To refresh the traps shown, click the **Refresh** button from '**View'** option. The Trap Viewer will read the traps from the log file again.

Change column size as desired by dragging the column markers to left or right. The horizontal scroll bar displays automatically to enable full view of all column data.

By default, the 'Enterprise' column displays the last portion of the Enterprise name. To show the complete Enterprise name, select **Expand Enterprise**.

Each Traps table line provides the following heading information.

Date/Time: The time and date that the trap was received, in the format yyyy-mm-dd hh:mm:ss (for example, *2011-Apr 19 13:53:41*).

Source IP: The IP address where the trap originated (e.g., *192.168.0.65*).

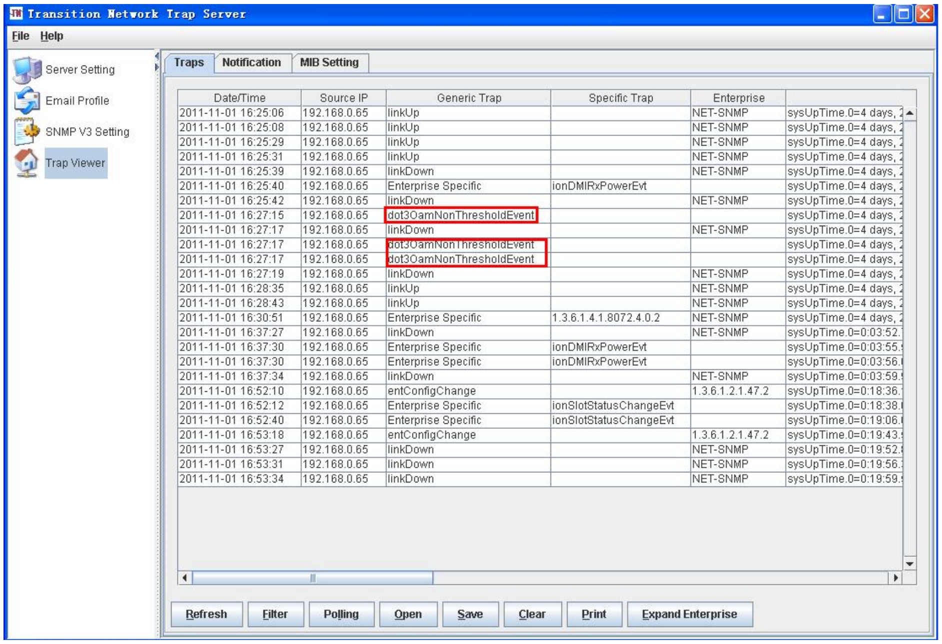
Generic Trap: displays the pre-defined traps in RFC which are implemented by most of the agents (e.g., Cold Start, Warm Start, Link Up, Link Down).

Specific Trap: displays the traps defined by enterprises (e.g., ionChassisDiscoved, ionChassisRemoved).

Enterprise / Expanded Enterprise: By default, the Enterprise column displays the last portion of Enterprise name (e.g., '*NET-SNMP*' shown above). To show complete Enterprise, click Shrink Enterprise or Expand Enterprise. Click the Expand Enterprise button to change the "Enterprise" column to the "Expanded Enterprise" with additional information capacity. If the "Expanded Enterprise" is currently displayed, click the Shrink Enterprise button to display the narrower "Enterprise" column.

Variable Bindings: (VarBinds) the variable number of values included in an SNMP packet. Each varbind has an OID, type, and value (the value for/from that Object ID). Vars (Varbinds, or Variable bindings) display as "*iso.3.6.1.2.1.1.3.0*", or "*entPhysicalIndex.13421*".

Sample Trap results are displayed as shown below.

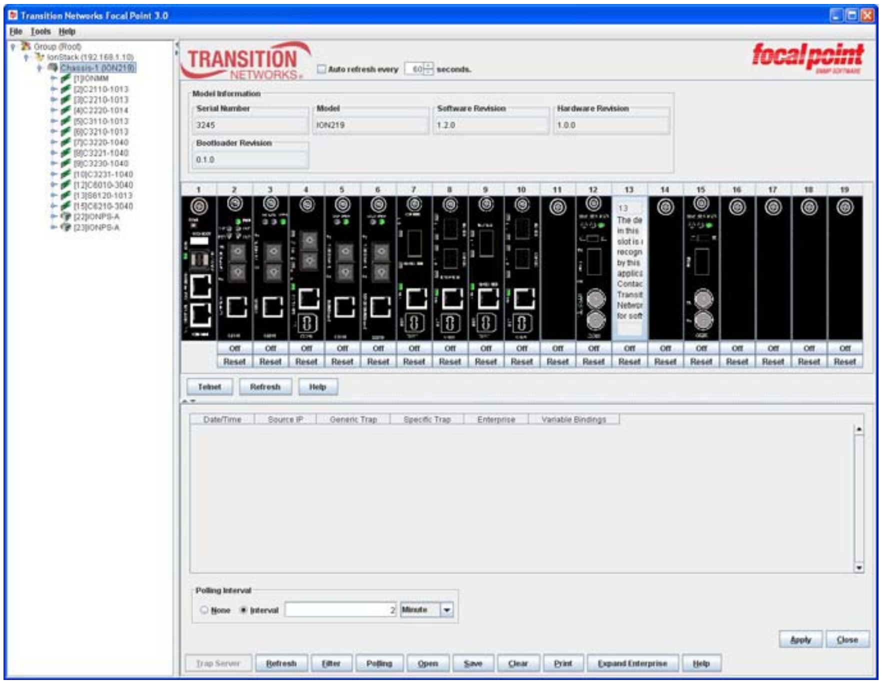


Date/Time	Source IP	Generic Trap	Specific Trap	Enterprise	
2011-11-01 16:25:06	192.168.0.65	linkUp		NET-SNMP	sysUpTime.0=4 days,
2011-11-01 16:25:08	192.168.0.65	linkUp		NET-SNMP	sysUpTime.0=4 days,
2011-11-01 16:25:29	192.168.0.65	linkUp		NET-SNMP	sysUpTime.0=4 days,
2011-11-01 16:25:31	192.168.0.65	linkUp		NET-SNMP	sysUpTime.0=4 days,
2011-11-01 16:25:39	192.168.0.65	linkDown		NET-SNMP	sysUpTime.0=4 days,
2011-11-01 16:25:40	192.168.0.65	Enterprise Specific	ionDMIRxPowerEvt		sysUpTime.0=4 days,
2011-11-01 16:25:42	192.168.0.65	linkDown		NET-SNMP	sysUpTime.0=4 days,
2011-11-01 16:27:15	192.168.0.65	dot3OamNonThresholdEvent			sysUpTime.0=4 days,
2011-11-01 16:27:17	192.168.0.65	linkDown		NET-SNMP	sysUpTime.0=4 days,
2011-11-01 16:27:17	192.168.0.65	dot3OamNonThresholdEvent			sysUpTime.0=4 days,
2011-11-01 16:27:17	192.168.0.65	dot3OamNonThresholdEvent			sysUpTime.0=4 days,
2011-11-01 16:27:19	192.168.0.65	linkDown		NET-SNMP	sysUpTime.0=4 days,
2011-11-01 16:28:35	192.168.0.65	linkUp		NET-SNMP	sysUpTime.0=4 days,
2011-11-01 16:28:43	192.168.0.65	linkUp		NET-SNMP	sysUpTime.0=4 days,
2011-11-01 16:30:51	192.168.0.65	Enterprise Specific	1.3.6.1.4.1.8072.4.0.2	NET-SNMP	sysUpTime.0=4 days,
2011-11-01 16:37:27	192.168.0.65	linkDown		NET-SNMP	sysUpTime.0=0:03:52.
2011-11-01 16:37:30	192.168.0.65	Enterprise Specific	ionDMIRxPowerEvt		sysUpTime.0=0:03:55.
2011-11-01 16:37:30	192.168.0.65	Enterprise Specific	ionDMIRxPowerEvt		sysUpTime.0=0:03:56.
2011-11-01 16:37:34	192.168.0.65	linkDown		NET-SNMP	sysUpTime.0=0:03:59.
2011-11-01 16:52:10	192.168.0.65	entConfigChange		1.3.6.1.2.1.47.2	sysUpTime.0=0:18:36.
2011-11-01 16:52:12	192.168.0.65	Enterprise Specific	ionSlotStatusChangeEvt		sysUpTime.0=0:18:38.
2011-11-01 16:52:40	192.168.0.65	Enterprise Specific	ionSlotStatusChangeEvt		sysUpTime.0=0:19:06.
2011-11-01 16:53:18	192.168.0.65	entConfigChange		1.3.6.1.2.1.47.2	sysUpTime.0=0:19:43.
2011-11-01 16:53:27	192.168.0.65	linkDown		NET-SNMP	sysUpTime.0=0:19:52.
2011-11-01 16:53:31	192.168.0.65	linkDown		NET-SNMP	sysUpTime.0=0:19:56.
2011-11-01 16:53:34	192.168.0.65	linkDown		NET-SNMP	sysUpTime.0=0:19:59.

ION SNMP

Several ION SNMP screens are provided below for reference.

ION Chassis View



Transition Networks Focal Point 3.0

- Group (Root)
  - IonStack (192.168.1.10)
    - Chassis-1 (ION219)
      - [1]IONMM
      - [2]C2110-1013
      - [3]C2210-1013
      - [4]C2220-1014
      - [5]C3110-1013
      - [6]C3210-1013
      - [7]C3220-1040
      - [8]C3221-1040
      - [9]C3230-1040
      - [10]C3231-1040
      - [12]C6010-3040
      - [13]S6120-1013
      - [15]C6210-3040
      - [22]IONPS-A
      - [23]IONPS-A

□ Auto refresh every 60 seconds.

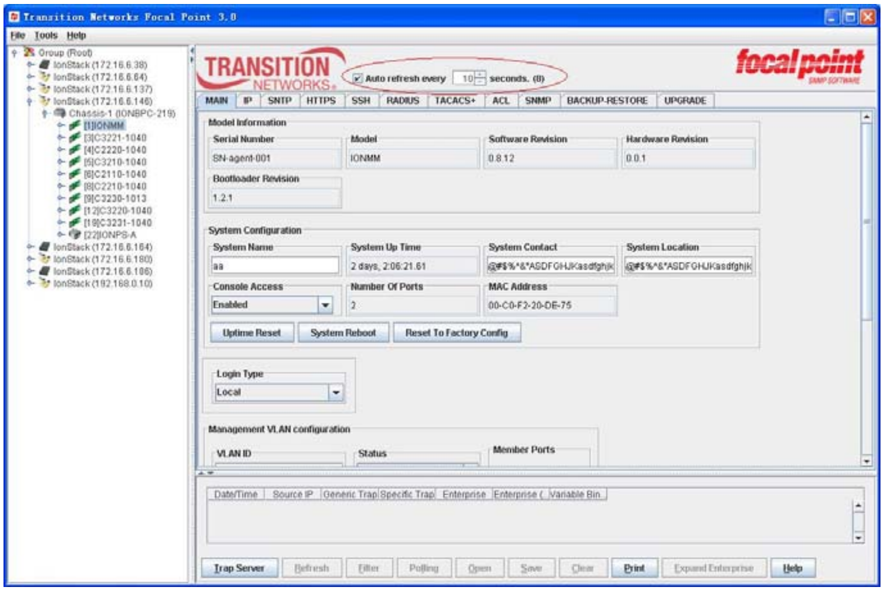
Model Information

Serial Number	Model	Software Revision	Hardware Revision
3245	ION219	1.2.0	1.0.0

Bootloader Revision: 0.1.0

Polling Interval: ○ None ● Interval 2 Minute

IONMM > Tabs



Transition Networks Focal Point 3.0

- Group (Root)
  - IonStack (172.16.6.38)
  - IonStack (172.16.6.64)
  - IonStack (172.16.6.137)
  - IonStack (172.16.6.146)
    - Chassis-1 (IONBPC-219)
      - [1]IONMM
      - [3]C3221-1040
      - [4]C2220-1040
      - [5]C3210-1040
      - [6]C2110-1040
      - [8]C2210-1040
      - [9]C3230-1013
      - [12]C3220-1040
      - [19]C3231-1040
      - [22]IONPS-A
  - IonStack (172.16.6.164)
  - IonStack (172.16.6.180)
  - IonStack (172.16.6.106)
  - IonStack (192.168.0.10)

☑ Auto refresh every 10 seconds. (8)

Model Information

Serial Number	Model	Software Revision	Hardware Revision
SN-agent-001	IONMM	0.8.12	0.0.1

Bootloader Revision: 1.2.1

System Configuration

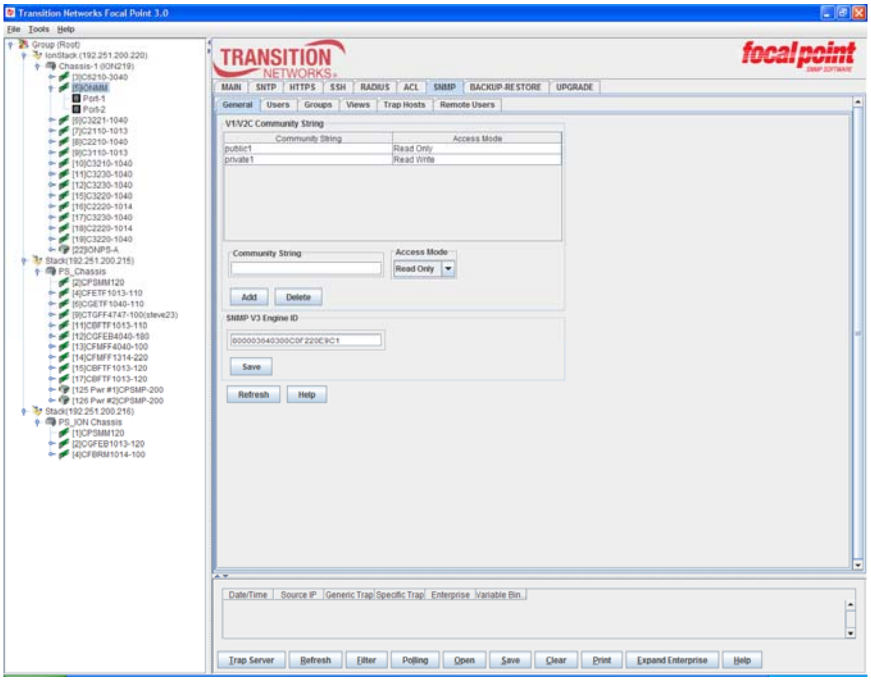
System Name	System Up Time	System Contact	System Location
aa	2 days, 2:06:21.61	@#$%^&*ASDFGHJKasdfghjk	@#$%^&*ASDFGHJKasdfghjk

Console Access	Number Of Ports	MAC Address
Enabled	2	00-C0-F2-20-DE-75

Login Type: Local

Management VLAN configuration

IONMM > SNMP tab > General sub-tab


Transition Networks Focal Point 3.0
File Tools Help
MAIN SNTP HTTPS SSH RADIUS ACL SNMP BACKUP-RESTORE UPGRADE
General Users Groups Views Trap Hosts Remote Users
Add Delete Save Refresh Help
Date/Time Source IP Generic Trap Specific Trap Enterprise Variable Bin.
Trap Server Refresh Filter Polling Open Save Clear Print Expand Enterprise Help

V1/V2C Community String

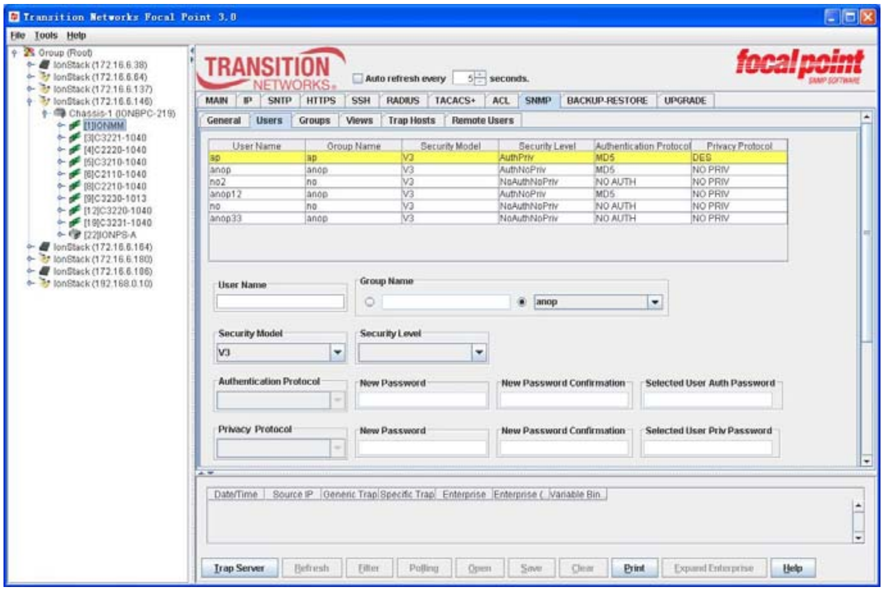
Community String	Access Mode
public1	Read Only
private1	Read Write

Community String:

Access Mode: Read Only

SNMP V3 Engine ID: 800003640300C0F220E9C1

IONMM > SNMP tab > Users sub-tab


Transition Networks Focal Point 3.0
File Tools Help
MAIN IP SNTP HTTPS SSH RADIUS TACACS+ ACL SNMP BACKUP-RESTORE UPGRADE
General Users Groups Views Trap Hosts Remote Users
Date/Time Source IP Generic Trap Specific Trap Enterprise Enterprise (Variable Bin.
Trap Server Refresh Filter Polling Open Save Clear Print Expand Enterprise Help

□ Auto refresh every 5 seconds.

User Name	Group Name	Security Model	Security Level	Authentication Protocol	Privacy Protocol
ap	ap	V3	AuthPriv	MD5	DES
anop	anop	V3	AuthNoPriv	MD5	NO PRIV
no2	no	V3	NoAuthNoPriv	NO AUTH	NO PRIV
anop12	anop	V3	AuthNoPriv	MD5	NO PRIV
no	no	V3	NoAuthNoPriv	NO AUTH	NO PRIV
anop33	anop	V3	NoAuthNoPriv	NO AUTH	NO PRIV

User Name:

Group Name: ○ ● anop

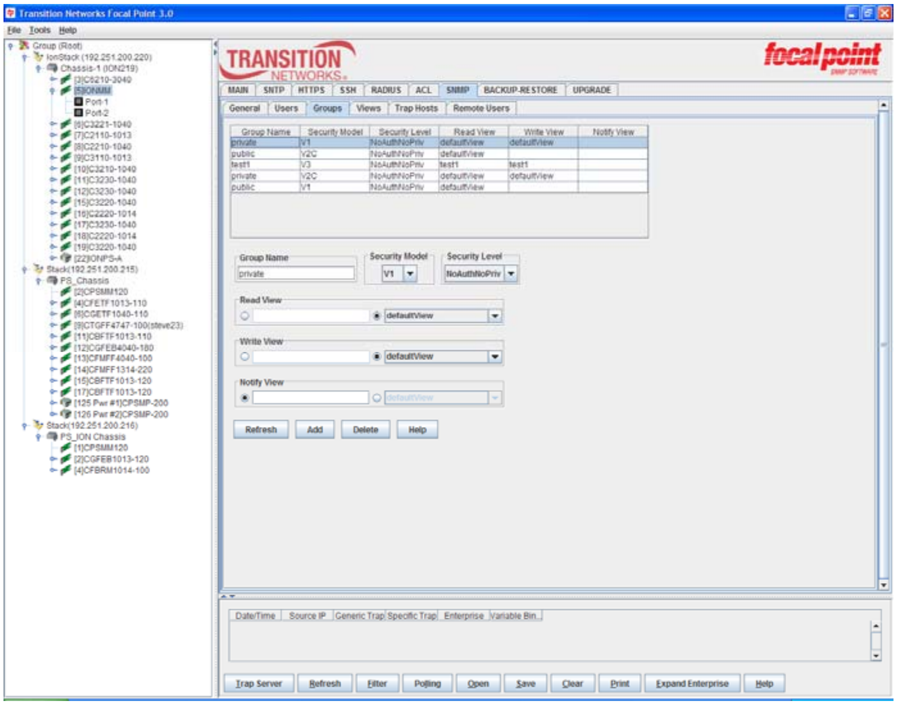
Security Model: V3

Security Level:

Authentication Protocol: New Password: New Password Confirmation: Selected User Auth Password:

Privacy Protocol: New Password: New Password Confirmation: Selected User Priv Password:

IONMM > SNMP tab > Groups sub-tab



Group Name	Security Model	Security Level	Read View	Write View	Notify View
private	V1	NoAuthNoPriv	defaultView	defaultView	
public	V2C	NoAuthNoPriv	defaultView		
test1	V3	NoAuthNoPriv	test1	test1	
private	V2C	NoAuthNoPriv	defaultView	defaultView	
public	V1	NoAuthNoPriv	defaultView		

Group Name: private
Security Model: V1
Security Level: NoAuthNoPriv

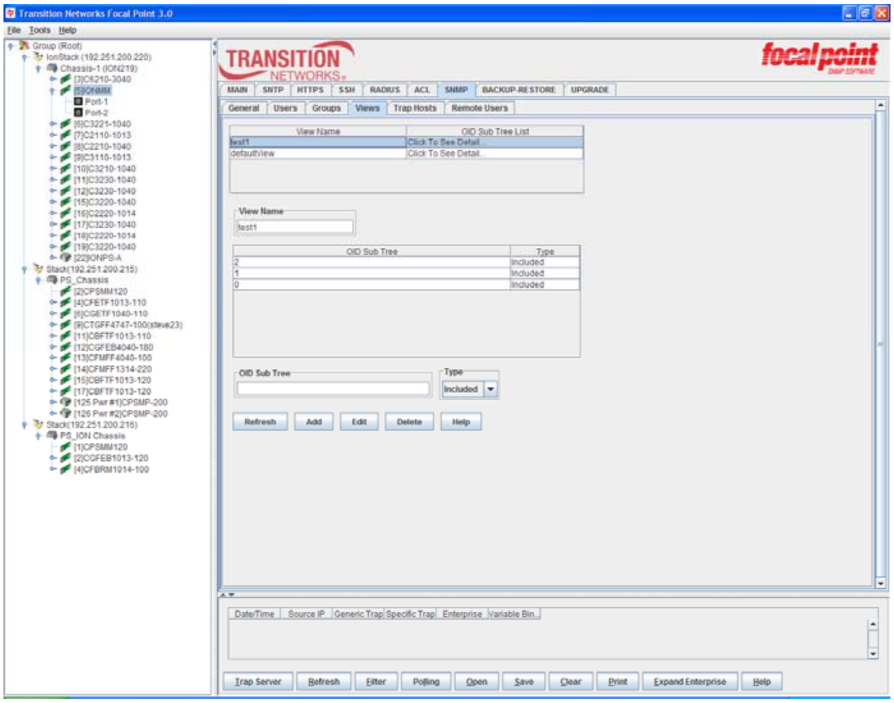
Read View: ○ ● defaultView

Write View: ○ ● defaultView

Notify View: ● ○ defaultView

Date/Time	Source IP	Generic Trap	Specific Trap	Enterprise	Variable Bin...

IONMM > SNMP tab > Views sub-tab



View Name	OID Sub Tree List
test1	Click To See Detail...
defaultView	Click To See Detail...

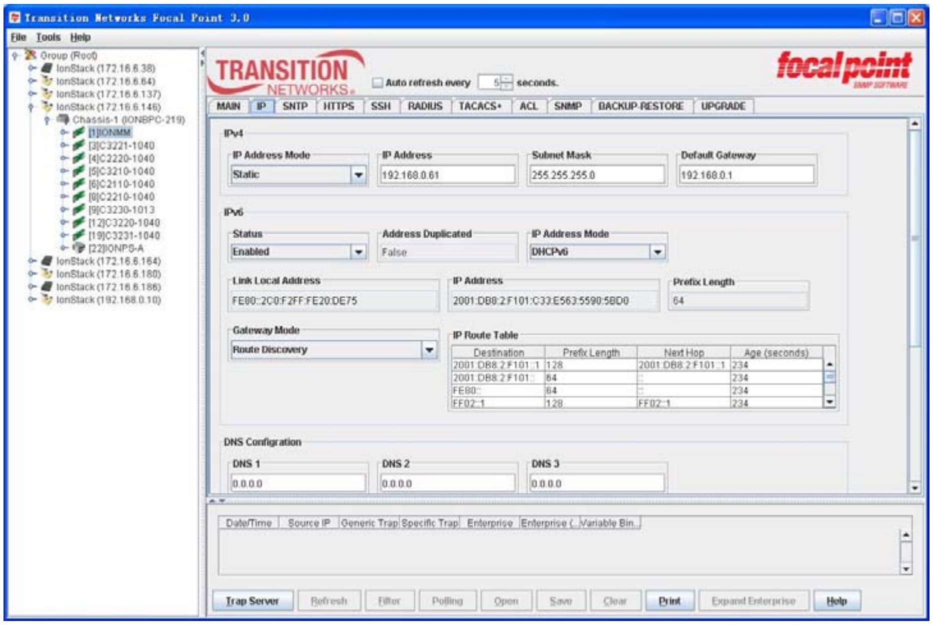
View Name: test1

OID Sub Tree	Type
2	Included
1	Included
0	Included

OID Sub Tree:
Type: Included

Date/Time	Source IP	Generic Trap	Specific Trap	Enterprise	Variable Bin...

IONMM > IP tab



□ Auto refresh every 5 seconds.

IPv4

IP Address Mode: Static
IP Address: 192.168.0.61
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.0.1

IPv6

Status: Enabled
Address Duplicated: False
IP Address Mode: DHCPv6
Link Local Address: FE80::2C0:F2FF:FE20:DE75
IP Address: 2001:DB8:2:F101:C33:E563:5590:5BD0
Prefix Length: 64
Gateway Mode: Route Discovery

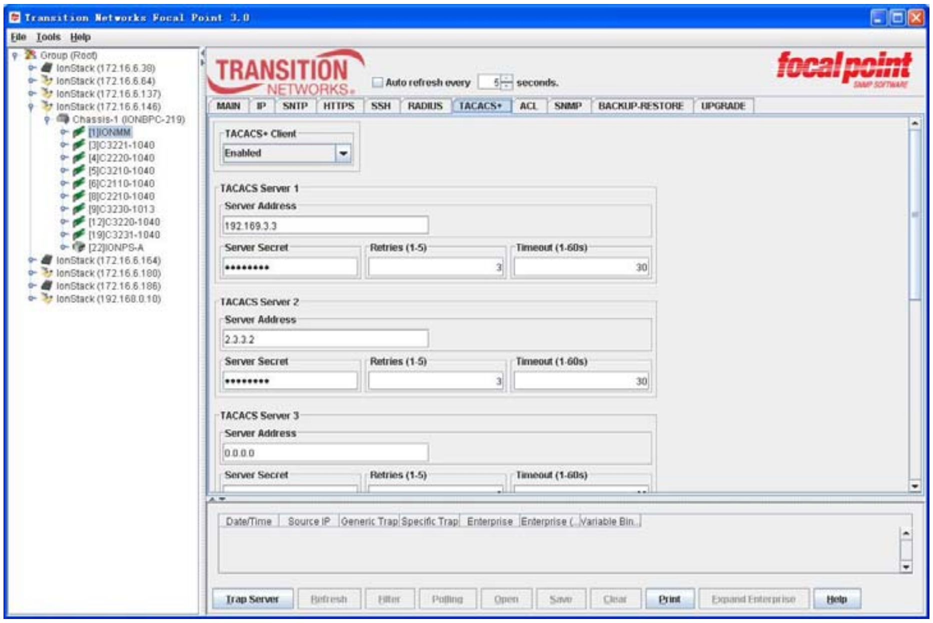
IP Route Table

Destination	Prefix Length	Next Hop	Age (seconds)
2001:DB8:2:F101::1	128	2001:DB8:2:F101::1	234
2001:DB8:2:F101::	64	::	234
FE80::	64	::	234
FF02::1	128	FF02::1	234

DNS Configration

DNS 1: 0.0.0.0
DNS 2: 0.0.0.0
DNS 3: 0.0.0.0

IONMM > TACACS+ tab



□ Auto refresh every 5 seconds.

TACACS+ Client: Enabled

TACACS Server 1

Server Address: 192.169.3.3
Server Secret: ********
Retries (1-5): 3
Timeout (1-60s): 30

TACACS Server 2

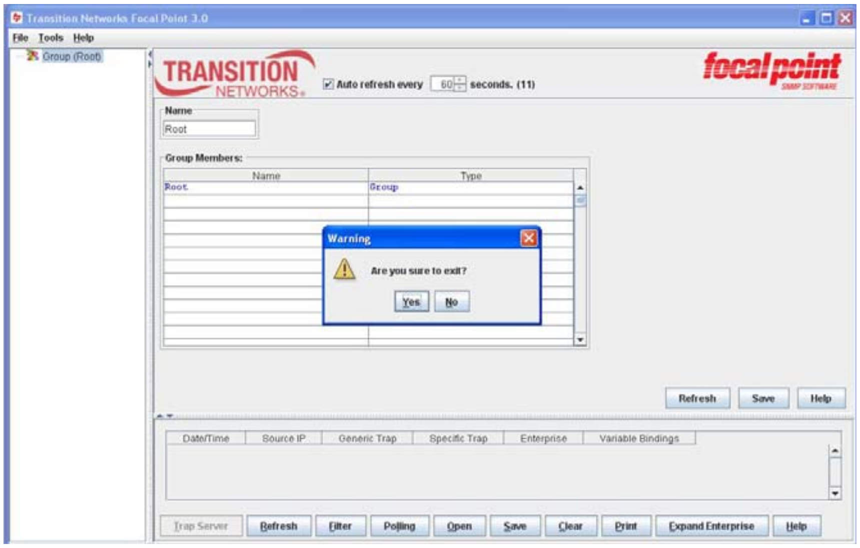
Server Address: 2.3.3.2
Server Secret: ********
Retries (1-5): 3
Timeout (1-60s): 30

TACACS Server 3

Server Address: 0.0.0.0
Server Secret
Retries (1-5)
Timeout (1-60s)

Exit the FP 3.0 Application

1. Select the Focal Point **File** > **Exit** menu path. The message "*Are you sure to exit?*" displays.


Transition Networks Focal Point 3.0
File Tools Help
Group (Root)
TRANSITION NETWORKS
focal point SNMP SOFTWARE
Refresh Save Help
Date/Time Source IP Generic Trap Specific Trap Enterprise Variable Bindings
Trap Server Refresh Filter Polling Open Save Clear Print Expand Enterprise Help

☑ Auto refresh every 60 seconds. (11)

Name: Root

Group Members:

Name	Type
Root	Group

Warning

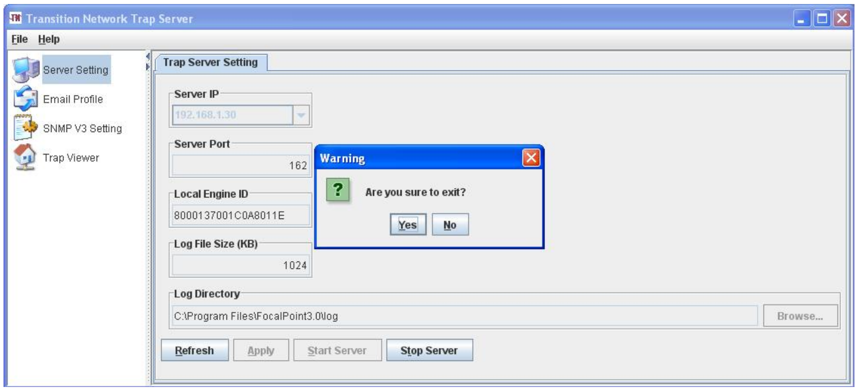
Are you sure to exit?

Yes No

2. Click **Yes** button. The FP 3.0 window closes. If the Trap Server application was previously opened, it remains running.

Exit the Trap Server Application

1. Select the Trap Server **File** > **Exit** menu path. The message "*Are you sure to exit?*" displays.



Server IP: 192.168.1.30

Server Port: 162

Local Engine ID: 8000137001C0A8011E

Log File Size (KB): 1024

Log Directory: C:\Program Files\FocalPoint3.0\log

Warning

Are you sure to exit?

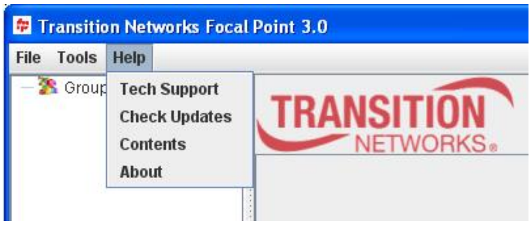
Yes No

2. Click **Yes** button. The FP 3.0 window closes. If the FP 3.0 application was previously opened, it remains running.

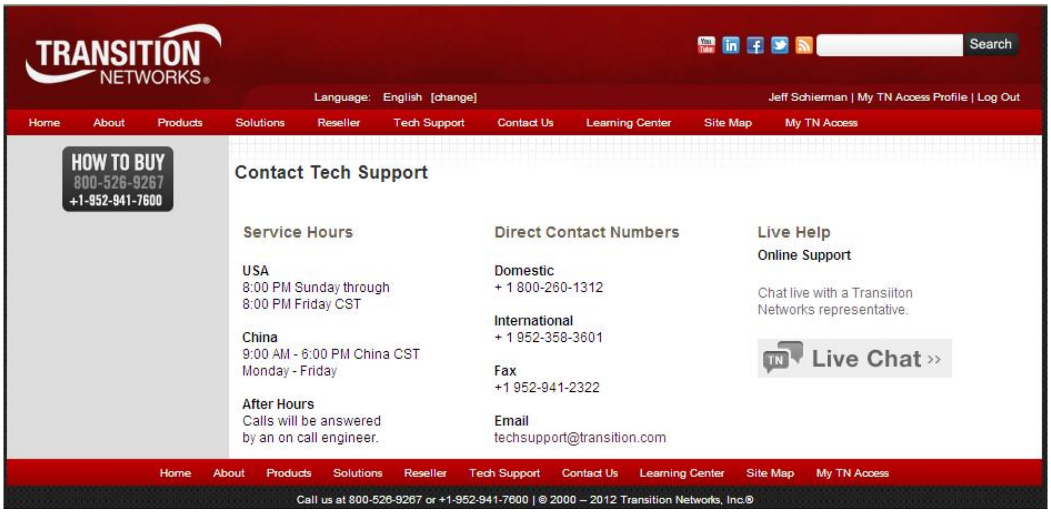
Contact Tech Support

To contact technical support:

1. On the Focal Point main menu, click on **Help** > **Tech Support** to launch Contact Tech support screen.



The Contact Tech support screen is shown below6.


TRANSITION NETWORKS
Search
Language: English [change]
Jeff Schierman | My TN Access Profile | Log Out
Home About Products Solutions Reseller Tech Support Contact Us Learning Center Site Map My TN Access
HOW TO BUY 800-526-9267 +1-952-941-7600

Contact Tech Support

Service Hours

USA
8:00 PM Sunday through
8:00 PM Friday CST

China
9:00 AM - 6:00 PM China CST
Monday - Friday

After Hours
Calls will be answered
by an on call engineer.

Direct Contact Numbers

Domestic
+ 1 800-260-1312

International
+ 1 952-358-3601

Fax
+1 952-941-2322

Email
techsupport@transition.com

Live Help

Online Support

Chat live with a Transiiton Networks representative.

Live Chat ››
Home About Products Solutions Reseller Tech Support Contact Us Learning Center Site Map My TN Access

Call us at 800-526-9267 or +1-952-941-7600 | © 2000 – 2012 Transition Networks, Inc.®

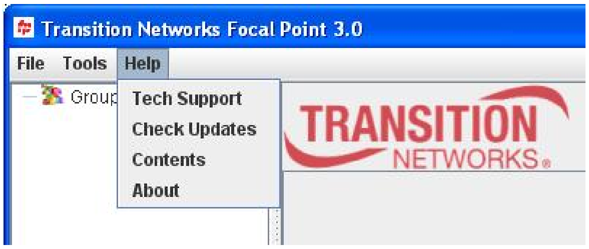
Figure 25: Contact Tech Support Screen

Note: TN NOW Live web chat is available from 6:30 AM to 5:30 PM CST.

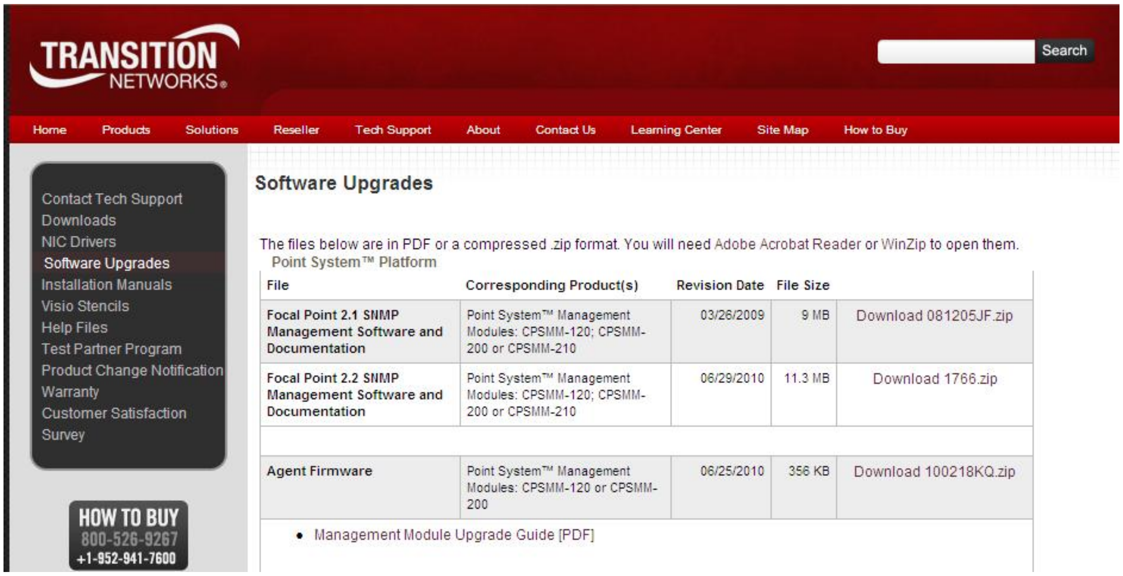
Software Upgrades

To upgrade the Focal Point software:

1. On the Main menu, click on **Help** tab.
2. Click **Check Updates** to launch the TN software upgrade page.



The TN software upgrade page is shown below.



Software Upgrades

The files below are in PDF or a compressed .zip format. You will need Adobe Acrobat Reader or WinZip to open them.

Point System™ Platform

File	Corresponding Product(s)	Revision Date	File Size	
Focal Point 2.1 SNMP Management Software and Documentation	Point System™ Management Modules: CPSMM-120; CPSMM-200 or CPSMM-210	03/26/2009	9 MB	Download 081205JF.zip
Focal Point 2.2 SNMP Management Software and Documentation	Point System™ Management Modules: CPSMM-120; CPSMM-200 or CPSMM-210	06/29/2010	11.3 MB	Download 1766.zip
Agent Firmware	Point System™ Management Modules: CPSMM-120 or CPSMM-200	06/25/2010	356 KB	Download 100218KQ.zip

- Management Module Upgrade Guide [PDF]

Figure 26: TN Software Upgrade Page

This page provides software upgrades and drivers for:

- Agent Firmware
- Side-In Cards
- Management MIBs
- USB Drivers

Chapter 4 - Troubleshooting

Introduction

This chapter provides troubleshooting information to help in resolving problems with Focal Point software, as well as an Uninstall Procedure, MIBs support information, and FocalPoint3.0 Logs.

This chapter also provides information about cable types, cable lengths, and cable specifications. For additional information specific to the ION system, refer to the applicable ION System User Guide manual(s).

Problems and Corrective Actions

The following troubleshooting information is provided to assist the administrator with resolving problems with installing and using Focal Point software. If the information provided does not resolve the problem, contact TN technical support.

Problem: Focal Point software will not load.

Corrective Action:
1. The Java application may not be installed. Type the following command from the command line (UNIX) or the command prompt (Windows): `C:\> java -version` If the response contains the works command not found, the Java application (*JRE2 v1.5.0 or later*) must first be installed. See the Java application instructions for installation advice.
2. The Java application version may be too old for the current Focal Point application. Type the following command from the command line (UNIX) or the command prompt (Windows): `C:\> java -version`
The version displayed must be JRE v1.5.0 or later. If the version is lower, an updated Java application must first be installed. See the Java application instructions for installation advice.
3. Contact TN Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Problem: The Focal Point software loads, but the chassis are not listed.

Corrective Action: **1**. The connection between the PC or Laptop and the SNMP agent might not be made. Confirm that both the PC and Laptop IP addresses, and the SNMP IP address are configured properly. Use the "ping" command to test the IP path to the SNMP agent: `CPSMM100> ping=nnn.nnn.nnn.nnn.` If the response is: `ICMP: ECHO REPLY message received from nnn.nnn.nnn.nnn` then the path is valid. (The "ping" command may also be run from the PC or Laptop to the SNMP agent. The syntax is `ping xxx.xxx.xxx.xxx`)
2. If the path is valid, then the SNMP traffic may be blocked by a router or firewall. Consult your network administrator to determine if this is the case.
3. Make sure the SNMP version selected is correct. See "Discover Transition Agents" on page 38.
4. Contact TN Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Problem: An unknown slide-in card error appears in the chassis view window; however, the Telnet and Web versions function normally.

Corrective Action: **1.** There may be an error in the communication protocol between the hardware (I^2C).
To correct the problem, power the chassis OFF then ON.
2. The "unknown card" may be a new type of slide-in card and, therefore, would not be included in an older revision of the SNMP agent or the Focal Point application. To correct the problem, download and install the newest revision of both SNMP and Focal Point software, or contact Technical Support for assistance.
3. Contact TN Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Problem: The Trap Server does not record traps.

Corrective Action: **1.** Ensure the Trap Server application is running.

- In Windows, if the "TN" icon is displayed in the lower right corner of the monitor, then the Trap Server is running.
- In UNIX, run the "ps" command to list the processes that are currently running. If the process TN Trap Server is listed, then the Trap Server is running.

2. SNMP traps may be blocked by a router or a firewall. Ask your Network administrator if this is the case.
3. The SNMP trap managers may not be configured properly. The result is the SNMP agent does not know the proper IP address. Use the "set" command to configure the trap managers. Enter the following command at the prompt: CPSMM100> set=cpsmm100SNMPTrapMgr.<chassis serial number>.<slot number of the MM>,ip,<new IP Address of PC>
4. Use the "getnext" command to get much of this information and then use the "set=*" command to issue the set request. The following is an example. Enter "super-user mode:"

```
        CPSMM100> su=<private community name> [su] CPSMM>
```

Enter the "getnext" command:

```
        [su] CPSMM100> getnext=cpsmm100snmptrapmgr
```

The response is:

```
        SNMP: GETNEXT [192.251.144.229] id=D2EE6F3F ind=0 cpsmm100snmptrapmgr.1758208.1
        IP Address [4/0x4] 192.251.144.235
```

Enter the set request:

```
        [su] CPSMM100> set=*,ip,172.16.45.105
```

The response is:

```
  SNMP: SET [192.251.144.229] id=D2EE6F3F ind=0 cpsmm100SNMPTrapMgr.1758208.1
  IP Address [4/0x4] 172.16.45.105
```

Save the changes:

```
  [su] CPSMM100> save
```

The response is:

```
  FLASH: Saving configuration, please wait up to one minute...
  Writing Flash (04004500,05E8,00FE0000,00FFFFFE)
  Erasing
  .
  Done Erasing/Verifying
  Writing [000005E8]
  #[0000FFFF]
  Done Writing
  Verifying

        FLASH: Write complete.
```

Problem: The Trap Viewer window exhibits strange resizing behavior.

Corrective Action: **1.** This may be due to Java tool set limitations. To correct this problem, close the Trap Viewer (NOT the Trap *Server*) and re-open the Trap Viewer. This action will not affect the recording of inbound traps.
2. Contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Problem: Can't launch on PC with Windows 7
Application cannot run as a standard user in Windows 7

Meaning: The standard user account type in Windows 7 provides a limited set of permissions needed for most non-administrative application scenarios. Some application tasks are considered administrative tasks that always require administrative privileges. These tasks cannot be accomplished by using a standard user account.

This issue is caused when the User Account Control (UAC) setting is "on". The UAC feature was introduced in Windows Vista as a way to separate regular user's activities from administrative user activities. UAC is a security component that allows an administrator to enter credentials during a non-administrator's user session to perform occasional administrative tasks in Windows 7, Windows Server 2008, Windows Server 2008 R2, Windows Storage Server 2008 R2, Windows Vista.

UAC uses a security infrastructure feature called 'tokens'. A security token is a way to grant an object (a user, process, file, thread, etc.) a specific set of permissions for specific actions. Under UAC, regular users are granted a permission token that lets them do things allowed only to regular users. If the user tries to do something that requires admin privileges, UAC asks for admin credentials. If the credentials are valid, the user is given a security token for just that one action and nothing else.

An admin account running under UAC has two tokens: one for daily regular-user work and one for admin-level privileges. Most programs (e.g., Internet Explorer) are launched under the first token. If you want something run as admin, UAC will poll you for permission first, and then launch the app using the second token. In Windows 7, UAC was changed so that certain signed system binaries (like Control Panel apps) no longer required explicit UAC approval to run. Other system programs (like Internet Explorer) were rewritten to automatically poll the user for admin privileges when doing things like copying files into the Programs directory.

Windows 7 has ten Group Policy settings that can be configured for User Account Control (UAC):

#	MS Group Policy setting	MS Default
1	Admin Approval Mode for the built-in Administrator account	Disabled
2	Allow UI Access apps to prompt for elevation without using secure desktop	Disabled
3	Behavior of elevation prompt for admins in Admin Approval Mode	Prompt for consent for non-Windows binaries
4	Behavior of the elevation prompt for standard users	Prompt for credentials on secure desktop
5	Detect application installations and prompt for elevation	Enabled (home) Disabled (enterprise)
6	Only elevate executables that are signed and validated	Disabled
7	Only elevate UIAccess applications that are installed in secure locations	Enabled
8	Run all administrators in Admin Approval Mode	Enabled
9	Switch to the secure desktop when prompting for elevation	Enabled
10	Virtualize file and registry write failures to per-user locations	Enabled

Corrective Action: Turn UAC Off using the following procedure:
1. Open **User Account Control Settings** by clicking the **Start** button and then clicking **Control Panel**.

2. In the search box, type **uac**, and then click **Change User Account Control setting**s.

3. Turn UAC off. Move the slider to the **Never notify** position, and then click **OK**. If prompted for an administrator password or confirmation, type the password or provide confirmation.

4. Restart your computer to turn off UAC.

To turn UAC on, move the slider to choose when you want to be notified, and then click **OK**.
If prompted for an administrator password or confirmation, type the password or provide confirmation.

See also:
http://msdn.microsoft.com/en-us/library/dd446675(v=ws.10).aspx
http://technet.microsoft.com/en-us/library/dd835564(WS.10).aspx
http://technet.microsoft.com/en-us/library/dd919180(WS.10).aspx

Problem: FP3.0.1/3.0.1_110704 - doesn't work with Java jre1.6.0_26 in Windows XP
Both FP3.0.1 or FP3.0.1_110704(2.2 integrated) don't work with JAVA jre1.6.0_26. FP2.2 works.
FP screen comes up for about 1 second and then closes. Can not launch FP at all with latest java 1.6.0 update 26 in Windows XP 64bit.

Corrective Action: Try replacing the latest Java with old version (i.e., *1.5.0_22* or *jdk1.6.0_18*) and make sure the version is not greater than 1.6.0_18. Go to Focal Point installation home, and switch to sub directory bin, edit the FocalPointApp?.bat, replace the jre path with jre path of the old version in Line 2.

Problem: Can't launch in Windows Vista 64 bit
Meaning: Windows Vista is not a supported OS.

Discovery Result Statuses

Try the following procedures for the possible discovery result statuses. See “Discover Transition Agents” on page 38.

Status Displayed: *Scanning...*
Meaning: Indicate that discovery process is in progress. FP is trying to detect if the destination device can be found.
Recovery: 1. Wait for the status to change. 2. Refer to one of the statuses below.

Status Displayed: *Already existing*
Meaning: Displays if the device has already been discovered and is displayed on the tree view.
Recovery: 1. Verify the IP address of the destination system / device. 2. Verify the destination system / device is the one you want.

Status Displayed: *Not reachable*
Meaning: A network connection can not be made. The ping attempt failed.
Recovery: 1. Verify the IP address of the destination system / device. 2. Make sure the destination is properly configured (to be discoverable). 3. Check the cabling. 4. Retry the operation.

Status Displayed: *Unknown device*
Meaning: The network is reachable, but the destination is not an SNMP agent or not a recognized ION System or Point System device.
Recovery: 1. Verify the IP address of the destination system / device. 2. Make sure the destination is properly configured (to be discoverable). 3. Make sure the SNMP version selected matches the SNMP version required (do this before you select the IP address). See “Accessing a Chassis via Focal Point” on page 22. 4. Retry the operation.

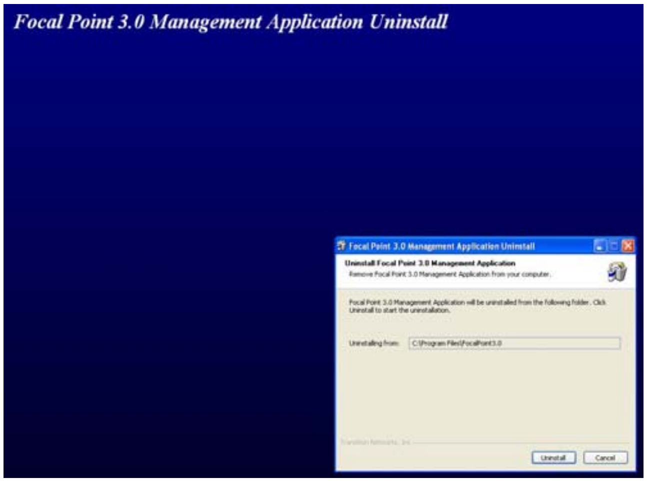
Status Displayed: *Discovered*
Meaning: An ION System or Point System device is found and is added to the tree view.
Recovery: None; the discovery succeeded.

Status Displayed: *Timeout*
Meaning: A timeout occurred to detect the destination.
Recovery: 1. Wait for the timeout period to end. 2. Verify the IP address of the destination system / device. 3. Retry the operation.

Uninstall Procedure

If necessary, use the procedure below to uninstall the existing FP instance. This procedure removes the FP folder from the install location (e.g., *C:\Program Files\FP 3.0*).

1. In Windows Explorer at *C:\Program Files\FocalPoint3.0* double-click the **Uninstall** icon (uninstall). (You can also use the **Start** > **All Programs** > **Transition Networks** > **Uninstall Focal Point 3.0 Management Application** path.)
   The Uninstall FP 3.0 screen displays.

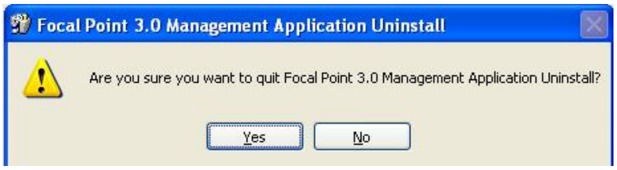

Focal Point 3.0 Management Application Uninstall
Focal Point 3.0 Management Application Uninstall
Uninstall Focal Point 3.0 Management Application
Transition Networks, Inc
Uninstall
Cancel

Remove Focal Point 3.0 Management Application from your computer.

Focal Point 3.0 Management Application will be uninstalled from the following folder. Click Uninstall to start the uninstallation.

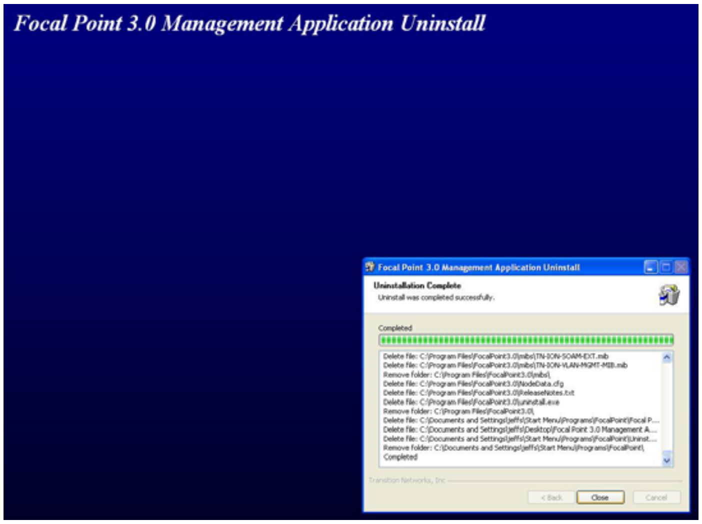
Uninstalling from: C:\Program Files\FocalPoint3.0

2. To quit the uninstall process, press the **Esc** key to display the message "*Are you sure you want to quit ... ?*", and click the **Yes** button to return to normal FP operation.



Are you sure you want to quit Focal Point 3.0 Management Application Uninstall?

To continue the uninstall procedure, click the **Uninstall** button. The uninstall process runs for a short time, and then the "Uninstallation completed" screen displays.


Focal Point 3.0 Management Application Uninstall
Focal Point 3.0 Management Application Uninstall
Uninstallation Complete
Transition Networks, Inc
< Back
Close
Cancel

Uninstall was completed successfully.

Completed

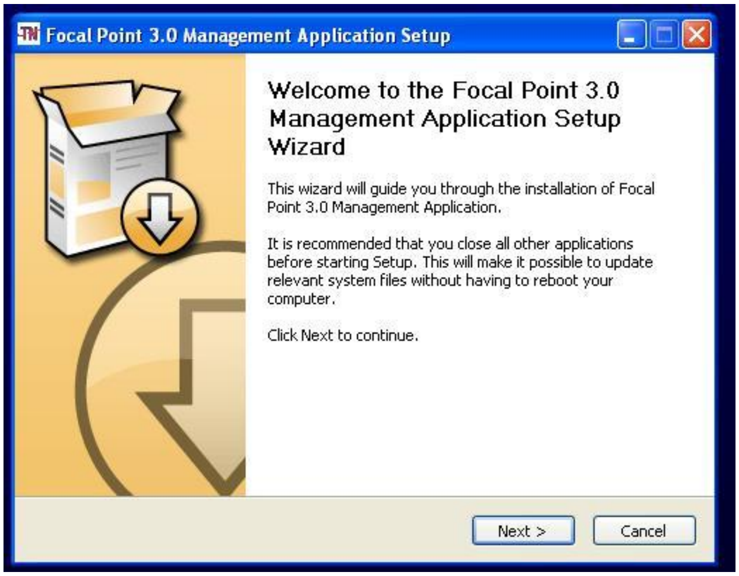
```
Delete file: C:\Program Files\FocalPoint3.0\mibs\TN-ION-SOAM-EXT.mib
Delete file: C:\Program Files\FocalPoint3.0\mibs\TN-ION-VLAN-MGMT-MIB.mib
Remove folder: C:\Program Files\FocalPoint3.0\mibs\
Delete file: C:\Program Files\FocalPoint3.0\NodeData.cfg
Delete file: C:\Program Files\FocalPoint3.0\ReleaseNotes.txt
Delete file: C:\Program Files\FocalPoint3.0\uninstall.exe
Remove folder: C:\Program Files\FocalPoint3.0\
Delete file: C:\Documents and Settings\jeffs\Start Menu\Programs\FocalPoint\Focal P...
Delete file: C:\Documents and Settings\jeffs\Desktop\Focal Point 3.0 Management A...
Delete file: C:\Documents and Settings\jeffs\Start Menu\Programs\FocalPoint\Uninst...
Remove folder: C:\Documents and Settings\jeffs\Start Menu\Programs\FocalPoint\
Completed
```

3. The uninstall procedure is complete. Click the **Close** button. See the "Focal Point Software Installation" section for information on how to re-install FP.

Re-Install Procedure

After performing the Uninstall procedure, use the procedure below to install Focal Point 3.0.

1. If possible, close all other open applications before proceeding. This will avoid having to reboot your computer at the end of this procedure.
2. In Windows Explorer, locate the TN FP 3.0 icon (e.g., at *C:\Program Files\FocalPoint3.0\FP3.0_Alpha_Rev2240*). The initial "*Welcome to the Focal Point 3.0 Management Application Setup Wizard*" screen displays.



Focal Point 3.0 Management Application Setup

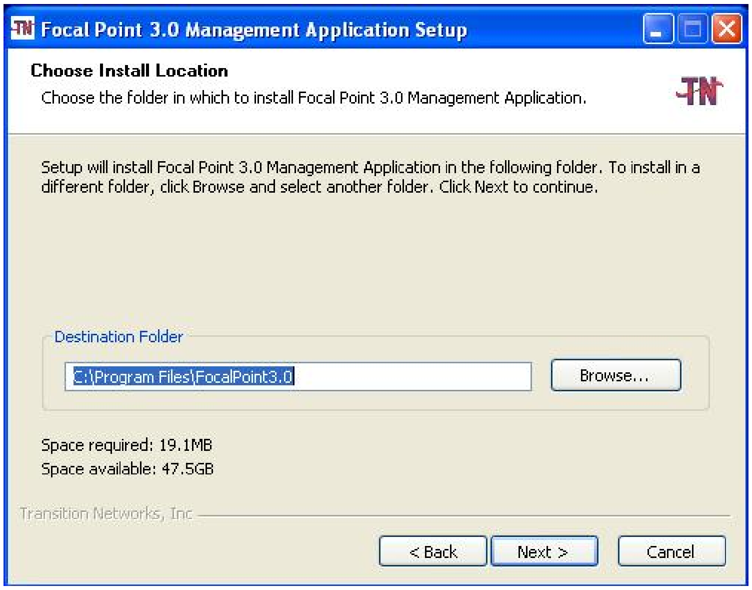
Welcome to the Focal Point 3.0 Management Application Setup Wizard

This wizard will guide you through the installation of Focal Point 3.0 Management Application.

It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.

Click Next to continue.

3. Click the **Next** button. The "*Choose Install Location*" screen displays.



Focal Point 3.0 Management Application Setup

Choose Install Location

Choose the folder in which to install Focal Point 3.0 Management Application.

Setup will install Focal Point 3.0 Management Application in the following folder. To install in a different folder, click Browse and select another folder. Click Next to continue.

Destination Folder: C:\Program Files\FocalPoint3.0

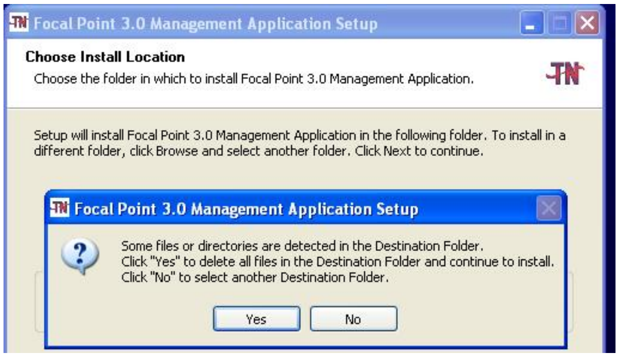
Space required: 19.1MB

Space available: 47.5GB

Transition Networks, Inc

4. To install to the default location (e.g., *C:ProgramFiles\FocalPoint3.0*) click the **Next** button.
   To install to a different location, click Browse and scroll to an existing location or Make a New File, and then click the **Next** button.

5. If the message “*Some files or directories are detected in the Destination Folder.*” displays, select “Yes” to keep just this new version of FP 3.0, or click “No” to keep the old version and this new version. If you select “No” you must select a new Destination Folder location.


Focal Point 3.0 Management Application Setup

Choose Install Location

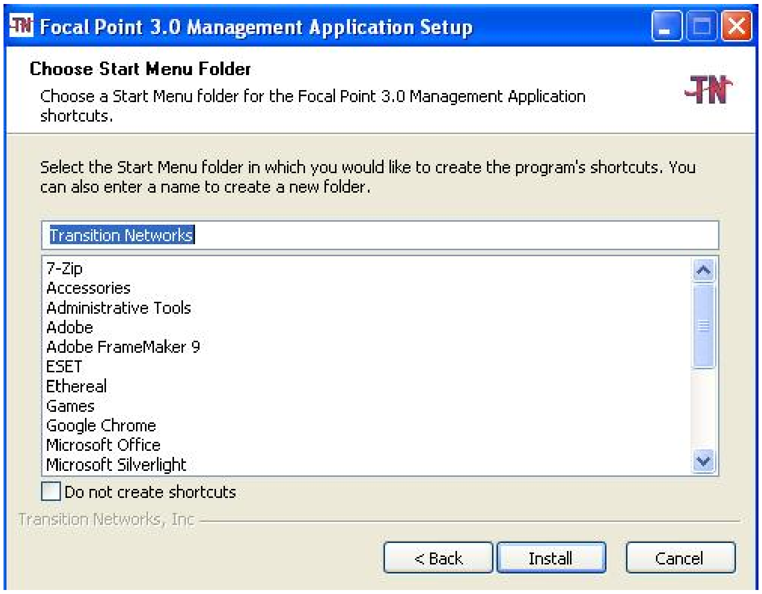
Choose the folder in which to install Focal Point 3.0 Management Application.

Setup will install Focal Point 3.0 Management Application in the following folder. To install in a different folder, click Browse and select another folder. Click Next to continue.

Focal Point 3.0 Management Application Setup

Some files or directories are detected in the Destination Folder.
Click "Yes" to delete all files in the Destination Folder and continue to install.
Click "No" to select another Destination Folder.

The “Choose a Start Menu Folder” screen displays.


Focal Point 3.0 Management Application Setup

Choose Start Menu Folder

Choose a Start Menu folder for the Focal Point 3.0 Management Application shortcuts.

Select the Start Menu folder in which you would like to create the program's shortcuts. You can also enter a name to create a new folder.

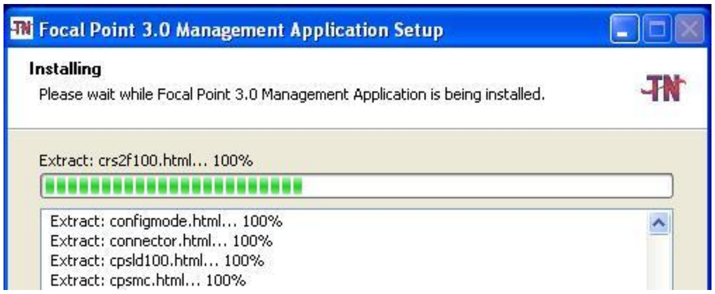
Transition Networks

7-Zip
Accessories
Administrative Tools
Adobe
Adobe FrameMaker 9
ESET
Ethereal
Games
Google Chrome
Microsoft Office
Microsoft Silverlight

□ Do not create shortcuts

Transition Networks, Inc

6. Select an existing shortcut, create a new one, or check the “Do not create shortcuts” checkbox. Click the “Install” button. The message “*Installing - Please wait ...*” displays momentarily.


Focal Point 3.0 Management Application Setup

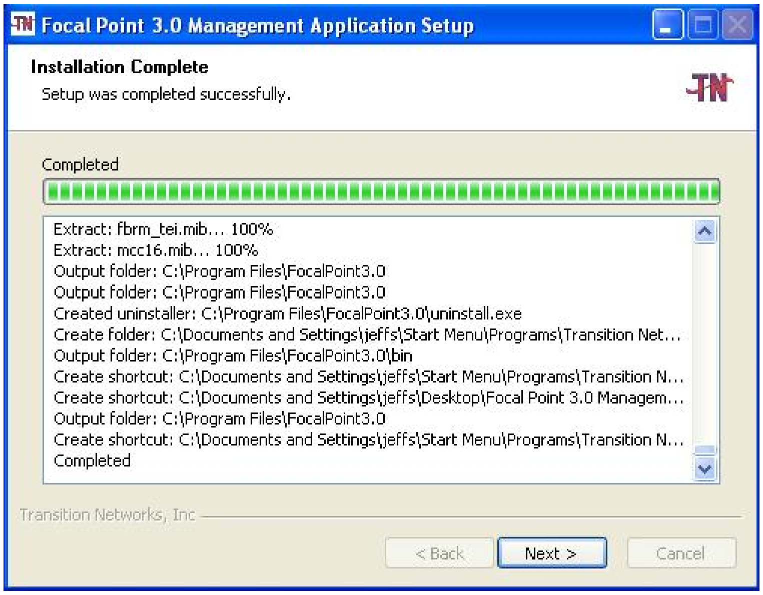
Installing

Please wait while Focal Point 3.0 Management Application is being installed.

Extract: crs2f100.html... 100%

```
Extract: configmode.html... 100%
Extract: connector.html... 100%
Extract: cpsld100.html... 100%
Extract: cpsmc.html... 100%
```

The "*Installation Complete. Setup was completed successfully*." screen displays.



Focal Point 3.0 Management Application Setup

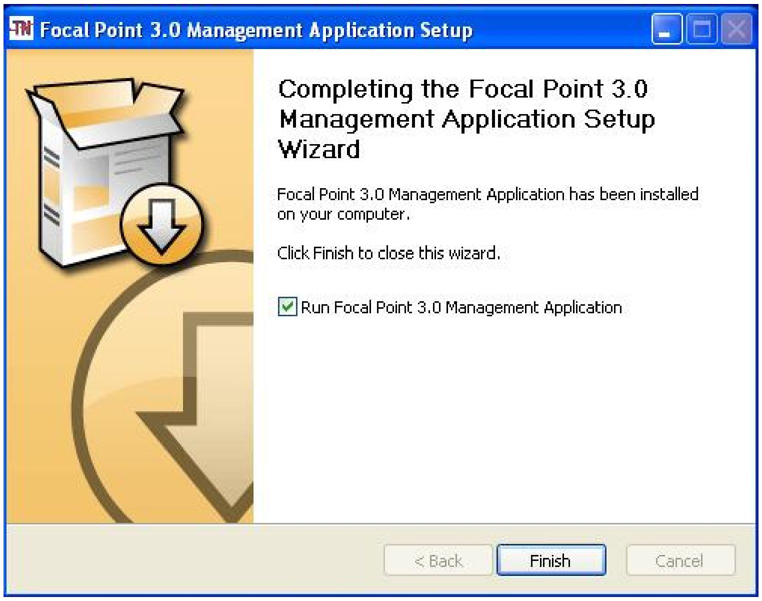
Installation Complete

Setup was completed successfully.

Completed

```
Extract: fbrm_tei.mib... 100%
Extract: mcc16.mib... 100%
Output folder: C:\Program Files\FocalPoint3.0
Output folder: C:\Program Files\FocalPoint3.0
Created uninstaller: C:\Program Files\FocalPoint3.0\uninstall.exe
Create folder: C:\Documents and Settings\jeffs\Start Menu\Programs\Transition Net...
Output folder: C:\Program Files\FocalPoint3.0\bin
Create shortcut: C:\Documents and Settings\jeffs\Start Menu\Programs\Transition N...
Create shortcut: C:\Documents and Settings\jeffs\Desktop\Focal Point 3.0 Managem...
Output folder: C:\Program Files\FocalPoint3.0
Create shortcut: C:\Documents and Settings\jeffs\Start Menu\Programs\Transition N...
Completed
```

7. Click the **Next** button. The "*Completing* ..." screen displays.



Focal Point 3.0 Management Application Setup

Completing the Focal Point 3.0 Management Application Setup Wizard

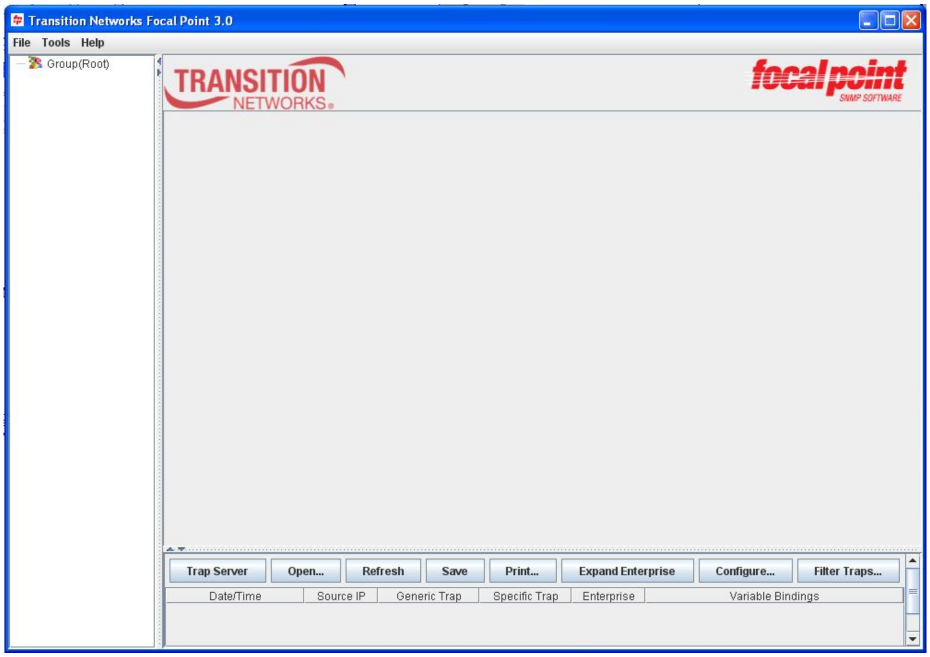
Focal Point 3.0 Management Application has been installed on your computer.

Click Finish to close this wizard.

☑ Run Focal Point 3.0 Management Application

8. If you want to start / run the FP 3.0 application later, uncheck the "*Run Focal Point 3.0 Management Application*" checkbox. Otherwise, click the "**Finish**" button to complete the installation and start the application.

The FP application folder is created (e.g., at *C:\Program Files\FocalPoint3.0*) the FP 3.0 application launches, and the FP 3.0 startup screen displays.



You can either review the "Main Window Pull-down Menu Descriptions" on page 13, or begin using the "Chapter 2 - Focal Point Management Software" as discussed on page 10.

FP 3.0 Traps List

The FP 3.0 traps include:

1. authenticationFailure
2. coldStart
3. dot1agCfmFaultAlarm
4. dot3OamNonThresholdevent
5. dot3OamThresholdevent
6. ionCardStateEvt
7. ionChassisDiscoveredEvt
8. ionChassisRemovedEvt
9. ionDMIRxIntrusionEvt
10. ionDMIRxPowerEvt
11. ionDMITxPowerEvt
12. ionDevSysAclIdsEvt
13. ionDyingGaspEvt
14. ionEntSensorThresholdNotification
15. ionSourceAddrChangeEvt
16. ionProvResultEvt
17. ionSlotStatusChangeEvt
18. ionSoamExtRemoteMepAddTrap
19. ionSoamExtRemoteMepRemoveTrap
20. ionUpgradeEvt
21. linkDown
22. mcc16Error
23. mcc16ErrorClear
24. mcc16PSState
25. newRoot
26. pSCabinetAdded
27. pSDeviceInserted
28. pSDeviceRemoved
29. pSError
30. pSErrorClear
31. pSPowerLost
32. sfbrm100ATUDbFull
33. sfbrm100ATUMemberViolation
34. sfbrm100ATUMissViolation
35. sfbrm100DMILowRxIntrusion
36. sfbrm100DMILowRxPower
37. sfbrm100DMILowTxBias
38. sfbrm100DMILowTxPower
39. sfbrm100DMIOnFiber
40. sfbrm100EEPROMOnFiber
41. sfbrm100LastGasp
42. sfbrm100LinkChanged
43. sfbrm1000AMPeerDyingGasp
44. sfbrm1000AMPeerLinkDown
45. sfbrm1000AMPeerLinkUp
46. sfbrm1000AMRemoteDetected
47. sfbrm1000AMThresholdEvent
48. sfbrm100PeerVersionMismatch
49. sfbrm100VTUMemberViolation
50. sfbrm100 VTUMissViolation
51. tnIntruderDetect

FP 3.0 Rule Conditions on Receipt of ...

The **Trap Server** > **Trap Viewer** > **Traps** tab lets you define trap, notification, and alert details, and displays the status for each defined Rule governing these parameters.

In the **Rule Actions** section check one or more checkboxes for how you want to be notified of the conditions that you have selected (Alert by Audio Beep, Alert by E-mail, Process Group Control String, Alert by Hints).

The Rule Conditions are listed below.

1. authenticationFailure
2. coldStart
3. dot1agCfmFaultAlarm
4. dot3OamNonThresholdevent
5. dot3OamThresholdevent
6. entConfigChange
7. fallingAlarm
8. ifMauJabberTrap
9. ionCardStateEvt
10. ionChassisDiscoveredEvt
11. ionChassisRemovedEvt
12. ionDMIRxIntrusionEvt
13. ionDMIRxPowerEvt
14. ionDMITemperatureEvt
15. ionDMITxBiasEvt
16. ionDMITxPowerEvt
17. ionDevSysAclIdsEvt
18. ionDyingGaspEvt
19. ionEntSensorThresholdNotification
20. ionSourceAddrChangeEvt
21. ionIfTdmAlarmIndicationSignalEvt
22. ionProvResultEvt
23. ionSlotStatusChangeEvt
24. ionSoamExtRemoteMepAddTrap
25. ionSoamExtRemoteMepRemoveTrap
26. ionUpgradeEvt
27. linkDown
28. linkUp
29. lldpRemTablesChange
30. mcc16Error
31. mcc16ErrorClear
32. mcc16PSState
33. newRoot
34. pSCabinetAdded
35. pSCabinetRemoved
36. pSDeviceColdStart
37. pSDeviceInserted
38. pSDeviceRemoved
39. pSError
40. pSErrorClear
41. pSPowerLost
42. risingAlarm
43. rpMauJabberTrap

44. sfbrm100ATUDbFull
45. sfbrm100ATUMemberViolation
46. sfbrm100ATUMissViolation
47. sfbrm100DMILowRxIntrusion
48. sfbrm100DMILowRxPower
49. sfbrm100DMILowTemperature
50. sfbrm100DMILowTxBias
51. sfbrm100DMILowTxPower
52. sfbrm100DMIOnFiber
53. sfbrm100EEPROMOnFiber
54. sfbrm100LastGasp
55. sfbrm100LinkChanged
56. sfbrm1000AMPeerDyingGasp
57. sfbrm1000AMPeerLinkDown
58. sfbrm1000AMPeerLinkUp
59. sfbrm1000AMRemoteDetected
60. sfbrm1000AMThresholdEvent
61. sfbrm100PeerVersionMismatch
62. sfbrm100VTUMemberViolation
63. sfbrm100 VTUMissViolation
64. tnIntruderDetect
65. topologyChange
66. topologyChangeTrap
67. warmStart
68. Other Transition Traps
69. Non Transition traps

FP3.0 MIBs

After successful FP 3.0 installation, the install folder (e.g., *C:\Program Files\FocalPoint3.0\mibs*) contains several MIB files, text files, and a sub-folder. The MIB files can be opened in Notepad, WordPad, MS Word, Open Office, etc.

If you are using the FP3.0 Trap Server to receive traps from Transition Networks devices (ION and Point System), you do not need to deal with MIBs.

If you are using the Trap Server to receive traps from external devices which are not from Transition Networks, you just need to put the related MIB files in a certain directory.

FP 3.0 users should know what MIB files are and what MIB files you must use for a device. The regular MIB definition files end with ".mib" and they are not .xml files; these .mib files comply with RFC 1212 and should be familiar to FP 3.0 users.

The *.xml files are generated and used by the application itself, and users do not need to deal with them.

FP 3.0 Logs

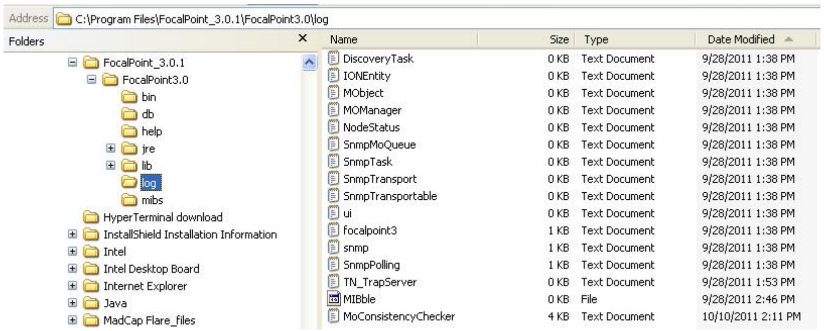
After successful FP 3.0 installation, the install folder (e.g., *C:\Program Files\FocalPoint3.0\log* by default) contains 17 different log files in text format. Most of these log files are used for engineers to collect debug information, and you would only use them at the direction of a TN support specialist. The "TN_TrapServer.log" may be an exception; it can be changed to save to another path and users could import/export it via the Trap Server.

Note that the logs can consume a fairly large amount of disk space over a period of time, and that you can configure both the location and maximum log file size for each type of log file. For information on how to configure log file location and maximum file size, see "Configure Trap Server" on page 32.

Log files are saved in .Zip file format. For example, if the current "TN_TrapServer.log" is full, it will be zipped to a backup file named "TN_TrapServer_1.log.zip" and removed. Then a new empty log file will be generated. Also, if this new file is full again, it will be zipped to another zip file named "TN_TrapServer_2.log.zip".

The set of FP 3.0 logs is listed below.

1. ConfigChanges Log
2. DiscoveryTask Log
3. focalpoint3 Log
4. FPNotePad Log
5. IONEntity Log
6. MObject Log
7. MoConsistencyChecker Log
8. MOManager Log
9. NodeStatus Log
10. snmp Log
11. SnmpMoQueue Log
12. SnmpPolling Log
13. SnmpTask Log
14. SnmpTransport Log
15. SnmpTransportable Log
16. TN_TrapServer Log
17. ui Log



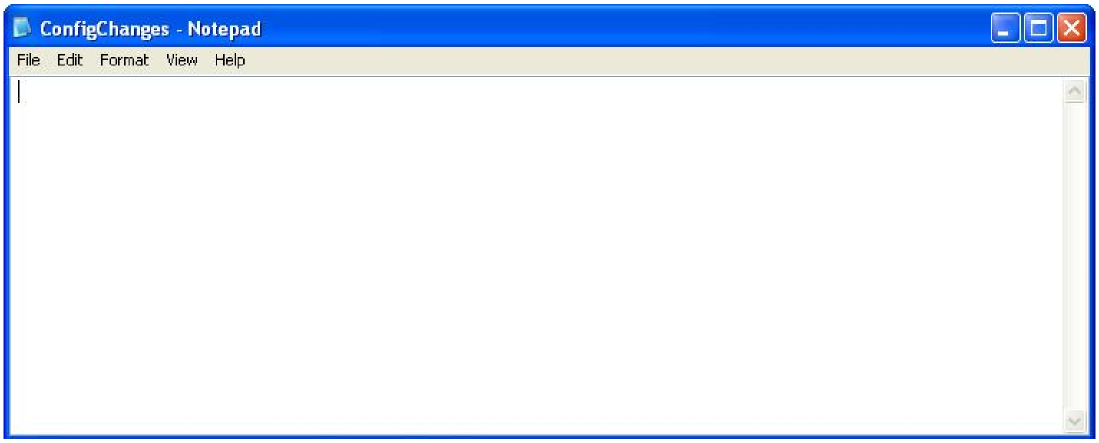
C:\Program Files\FocalPoint_3.0.1\FocalPoint3.0\log

Name	Size	Type	Date Modified
DiscoveryTask	0 KB	Text Document	9/28/2011 1:38 PM
IONEntity	0 KB	Text Document	9/28/2011 1:38 PM
MObject	0 KB	Text Document	9/28/2011 1:38 PM
MOManager	0 KB	Text Document	9/28/2011 1:38 PM
NodeStatus	0 KB	Text Document	9/28/2011 1:38 PM
SnmpMoQueue	0 KB	Text Document	9/28/2011 1:38 PM
SnmpTask	0 KB	Text Document	9/28/2011 1:38 PM
SnmpTransport	0 KB	Text Document	9/28/2011 1:38 PM
SnmpTransportable	0 KB	Text Document	9/28/2011 1:38 PM
ui	0 KB	Text Document	9/28/2011 1:38 PM
focalpoint3	1 KB	Text Document	9/28/2011 1:38 PM
snmp	1 KB	Text Document	9/28/2011 1:38 PM
SnmpPolling	1 KB	Text Document	9/28/2011 1:38 PM
TN_TrapServer	0 KB	Text Document	9/28/2011 1:53 PM
MIBble	0 KB	File	9/28/2011 2:46 PM
MoConsistencyChecker	4 KB	Text Document	10/10/2011 2:11 PM

These FP 3.0 Log files can be opened in Notepad, WordPad, MS Word, Open Office, etc. In many cases you will be asked to copy the log message exactly as it appears in the log, call your TN tech support representative, and provide the log message information. Each of these FP 3.0 log files is described below.

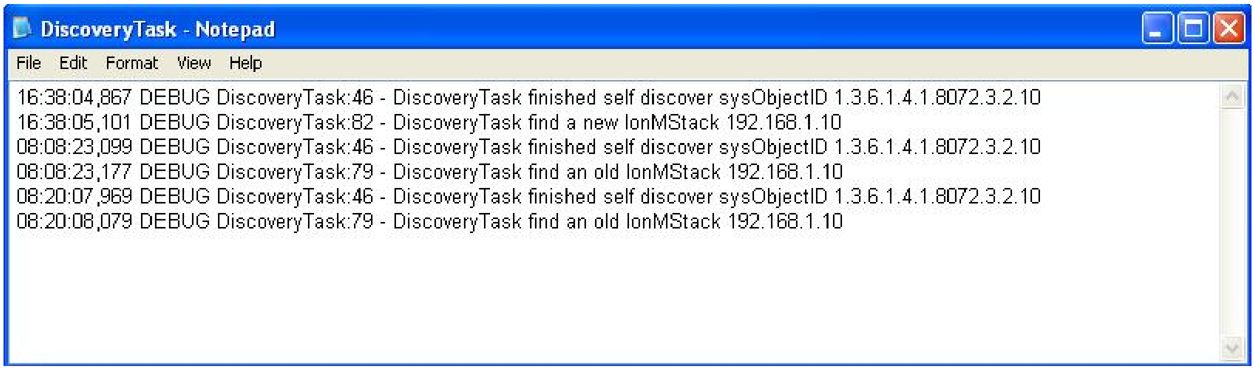
ConfigChanges Log

This log file provides a dated, indexed list of recent changes to the FP configuration. A sample ConfigChanges log in Notepad is shown below.



DiscoveryTask Log

This log file provides a dated, indexed list of discovery tasks performed on the system. A DiscoveryTask log example in Notepad is shown below.



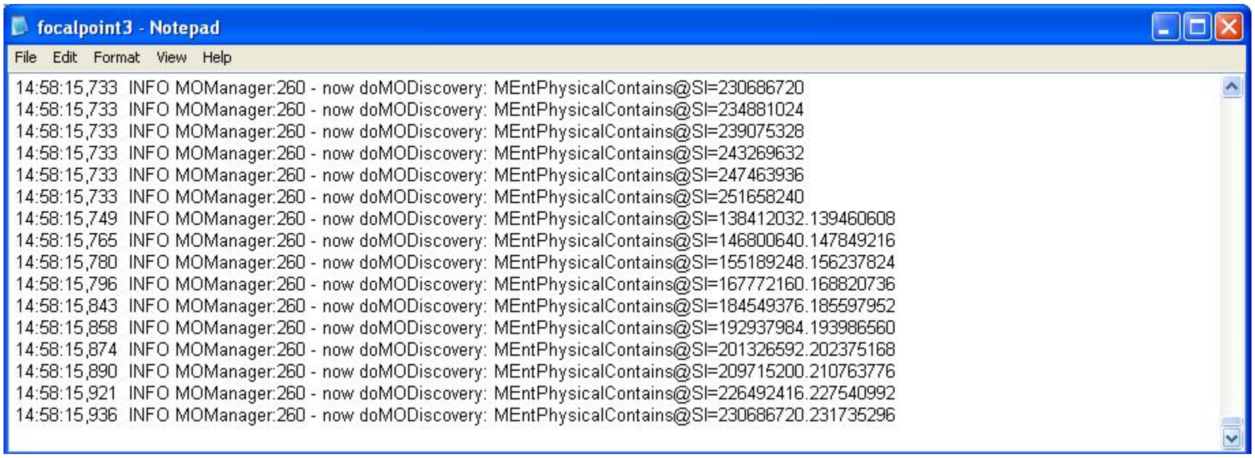
```
16:38:04,867 DEBUG DiscoveryTask:46 - DiscoveryTask finished self discover sysObjectID 1.3.6.1.4.1.8072.3.2.10
16:38:05,101 DEBUG DiscoveryTask:82 - DiscoveryTask find a new IonMStack 192.168.1.10
08:08:23,099 DEBUG DiscoveryTask:46 - DiscoveryTask finished self discover sysObjectID 1.3.6.1.4.1.8072.3.2.10
08:08:23,177 DEBUG DiscoveryTask:79 - DiscoveryTask find an old IonMStack 192.168.1.10
08:20:07,969 DEBUG DiscoveryTask:46 - DiscoveryTask finished self discover sysObjectID 1.3.6.1.4.1.8072.3.2.10
08:20:08,079 DEBUG DiscoveryTask:79 - DiscoveryTask find an old IonMStack 192.168.1.10
```

A DiscoveryTask log example for an ION system is shown below in plain text.

```
11:39:53,074 DEBUG DiscoveryTask:46 - DiscoveryTask finished self discover sysObjectID 1.3.6.1.4.1.8072.3.2.10
11:39:53,309 DEBUG DiscoveryTask:82 - DiscoveryTask find a new IonMStack 192.168.1.10
11:41:15,160 DEBUG DiscoveryTask:46 - DiscoveryTask finished self discover sysObjectID 1.3.6.1.4.1.8072.3.2.10
11:41:15,160 DEBUG DiscoveryTask:79 - DiscoveryTask find an old IonMStack 192.168.1.10
11:46:46,028 DEBUG DiscoveryTask:46 - DiscoveryTask finished self discover sysObjectID 1.3.6.1.4.1.8072.3.2.10
11:46:46,028 DEBUG DiscoveryTask:79 - DiscoveryTask find an old IonMStack 192.168.1.10
13:00:42,194 DEBUG DiscoveryTask:46 - DiscoveryTask finished self discover sysObjectID 1.3.6.1.4.1.8072.3.2.10
13:00:42,194 DEBUG DiscoveryTask:79 - DiscoveryTask find an old IonMStack 192.168.1.10
```

focalpoint3 Log

This log file provides a dated, indexed list of MO (managed objects) discovery tasks performed on the system. A focalpoint3 log example in Notepad is shown below.



```
14:58:15,733  INFO MOManager:260 - now doMODiscovery: MEntPhysicalContains@SI=230686720
14:58:15,733  INFO MOManager:260 - now doMODiscovery: MEntPhysicalContains@SI=234881024
14:58:15,733  INFO MOManager:260 - now doMODiscovery: MEntPhysicalContains@SI=239075328
14:58:15,733  INFO MOManager:260 - now doMODiscovery: MEntPhysicalContains@SI=243269632
14:58:15,733  INFO MOManager:260 - now doMODiscovery: MEntPhysicalContains@SI=247463936
14:58:15,733  INFO MOManager:260 - now doMODiscovery: MEntPhysicalContains@SI=251658240
14:58:15,749  INFO MOManager:260 - now doMODiscovery: MEntPhysicalContains@SI=138412032.139460608
14:58:15,765  INFO MOManager:260 - now doMODiscovery: MEntPhysicalContains@SI=146800640.147849216
14:58:15,780  INFO MOManager:260 - now doMODiscovery: MEntPhysicalContains@SI=155189248.156237824
14:58:15,796  INFO MOManager:260 - now doMODiscovery: MEntPhysicalContains@SI=167772160.168820736
14:58:15,843  INFO MOManager:260 - now doMODiscovery: MEntPhysicalContains@SI=184549376.185597952
14:58:15,858  INFO MOManager:260 - now doMODiscovery: MEntPhysicalContains@SI=192937984.193986560
14:58:15,874  INFO MOManager:260 - now doMODiscovery: MEntPhysicalContains@SI=201326592.202375168
14:58:15,890  INFO MOManager:260 - now doMODiscovery: MEntPhysicalContains@SI=209715200.210763776
14:58:15,921  INFO MOManager:260 - now doMODiscovery: MEntPhysicalContains@SI=226492416.227540992
14:58:15,936  INFO MOManager:260 - now doMODiscovery: MEntPhysicalContains@SI=230686720.231735296
```

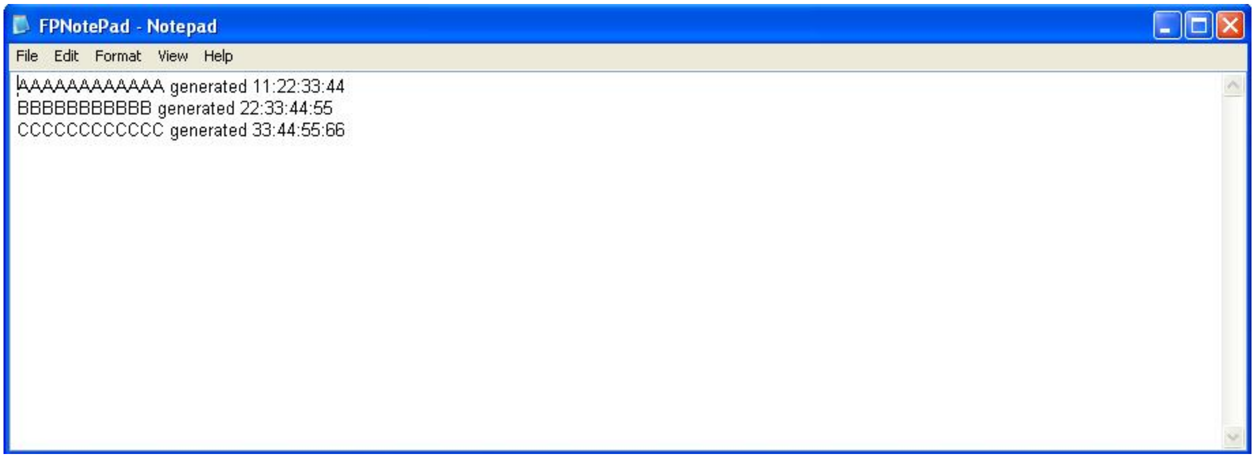
A focalpoint3 Log example for an ION system is shown below in plain text.

```
15:39:41,861  INFO MObject:220 - Add one IonMCard : IonMCard3231 at 177209344
15:39:41,861  WARN SnmpMoQueue:36 - IonMCard3231@SI=177209344 still in discovery, ignore...
15:39:50,064  INFO MOManager:260 - now doMODiscovery: IonMStack@IP=192.168.1.10
15:39:50,064  INFO MOManager:260 - now doMODiscovery: IonMChassis@SI=134217728
15:39:50,064  INFO MOManager:260 - now doMODiscovery: MEntPhysicalContains@SI=1
15:39:50,064  INFO MOManager:260 - now doMODiscovery: MEntPhysicalContains@SI=134217728
15:39:50,080  INFO MOManager:260 - now doMODiscovery: MEntPhysicalContains@SI=134217728.138412032
15:39:50,096  INFO MOManager:260 - now doMODiscovery: MEntPhysicalContains@SI=1.134217728
15:39:50,111  INFO MOManager:260 - now doMODiscovery: MEntPhysicalContains@SI=134217728.142606336
```

FPNotePad Log

This log file contains data from the FP 3 Text Editor application. The files are created from **FP 3.0** > **Tools** > **Text Editor** following a **Save** operation.

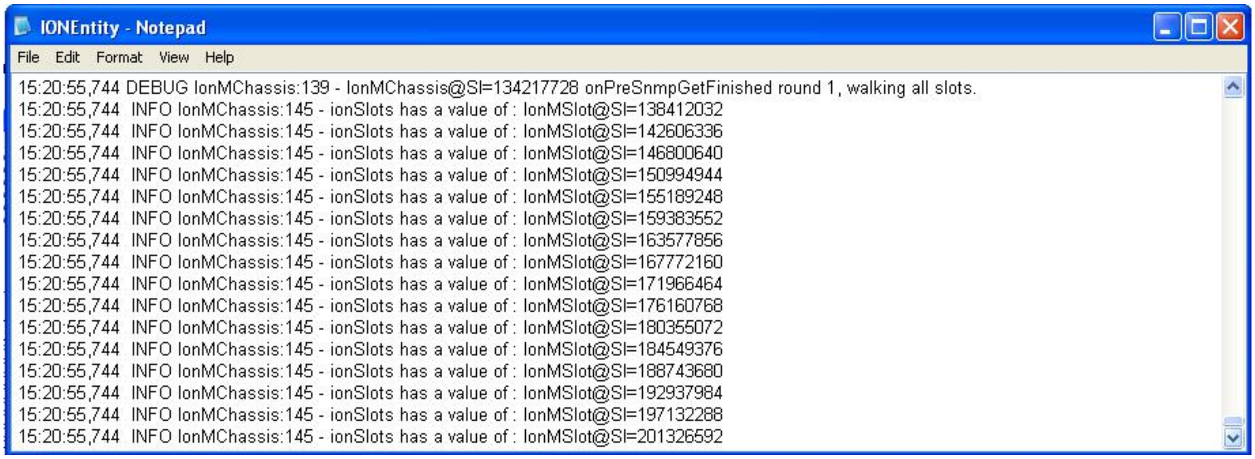
An FPNotePad Log example is shown below.



```
AAAAAAAAAAAA generated 11:22:33:44
BBBBBBBBBBB generated 22:33:44:55
CCCCCCCCCCCC generated 33:44:55:66
```

IONEntity Log

This log file provides a dated, indexed list of managed entities (chassis and slots) for a system. An IONEntity log example in Notepad is shown below.



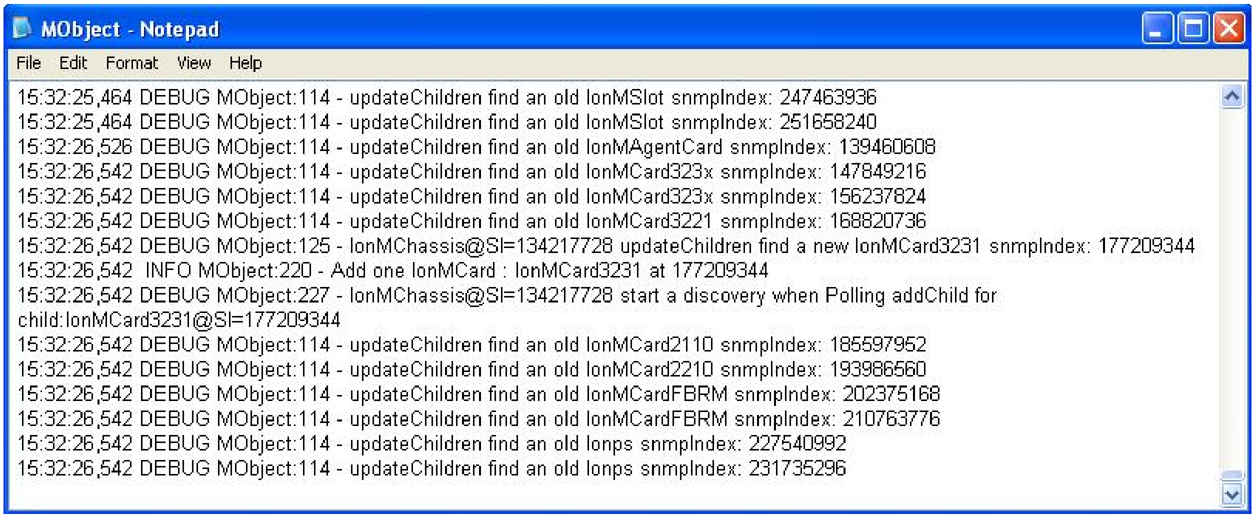
```
15:20:55,744 DEBUG IonMChassis:139 - IonMChassis@SI=134217728 onPreSnmpGetFinished round 1, walking all slots.
15:20:55,744  INFO IonMChassis:145 - ionSlots has a value of : IonMSlot@SI=138412032
15:20:55,744  INFO IonMChassis:145 - ionSlots has a value of : IonMSlot@SI=142606336
15:20:55,744  INFO IonMChassis:145 - ionSlots has a value of : IonMSlot@SI=146800640
15:20:55,744  INFO IonMChassis:145 - ionSlots has a value of : IonMSlot@SI=150994944
15:20:55,744  INFO IonMChassis:145 - ionSlots has a value of : IonMSlot@SI=155189248
15:20:55,744  INFO IonMChassis:145 - ionSlots has a value of : IonMSlot@SI=159383552
15:20:55,744  INFO IonMChassis:145 - ionSlots has a value of : IonMSlot@SI=163577856
15:20:55,744  INFO IonMChassis:145 - ionSlots has a value of : IonMSlot@SI=167772160
15:20:55,744  INFO IonMChassis:145 - ionSlots has a value of : IonMSlot@SI=171966464
15:20:55,744  INFO IonMChassis:145 - ionSlots has a value of : IonMSlot@SI=176160768
15:20:55,744  INFO IonMChassis:145 - ionSlots has a value of : IonMSlot@SI=180355072
15:20:55,744  INFO IonMChassis:145 - ionSlots has a value of : IonMSlot@SI=184549376
15:20:55,744  INFO IonMChassis:145 - ionSlots has a value of : IonMSlot@SI=188743680
15:20:55,744  INFO IonMChassis:145 - ionSlots has a value of : IonMSlot@SI=192937984
15:20:55,744  INFO IonMChassis:145 - ionSlots has a value of : IonMSlot@SI=197132288
15:20:55,744  INFO IonMChassis:145 - ionSlots has a value of : IonMSlot@SI=201326592
```

An IONEntity log example for an ION system is shown below in plain text.

```
15:42:40,974 DEBUG IonMChassis:97 - IonMChassis@SI=134217728onPreSnmpGetFinished
15:42:40,974 DEBUG IonMChassis:139 - IonMChassis@SI=134217728 onPreSnmpGetFinished
round 1, walking all slots.
15:42:40,974  INFO IonMChassis:145 - ionSlots has a value of : IonMSlot@SI=138412032
15:42:40,974  INFO IonMChassis:145 - ionSlots has a value of : IonMSlot@SI=205520896
15:42:41,365 DEBUG IonMChassis:97 - IonMChassis@SI=134217728onPreSnmpGetFinished
15:42:41,365 DEBUG IonMChassis:155 - IonMChassis@SI=134217728 onPreSnmpGetFinished
round 2, discovering all cards.
15:42:50,068 DEBUG IonMStack:90 - IonMStack@IP=192.168.1.10onStartDiscover
15:42:50,068 DEBUG IonMChassis:89 - IonMChassis@SI=134217728onStartDiscover
15:42:50,115 DEBUG IonMStack:98 - IonMStack@IP=192.168.1.10onPreSnmpGetFinished
```

MObject Log

This log file provides a dated, indexed list of managed objects for a system. A MObject log example in Notepad is shown below.



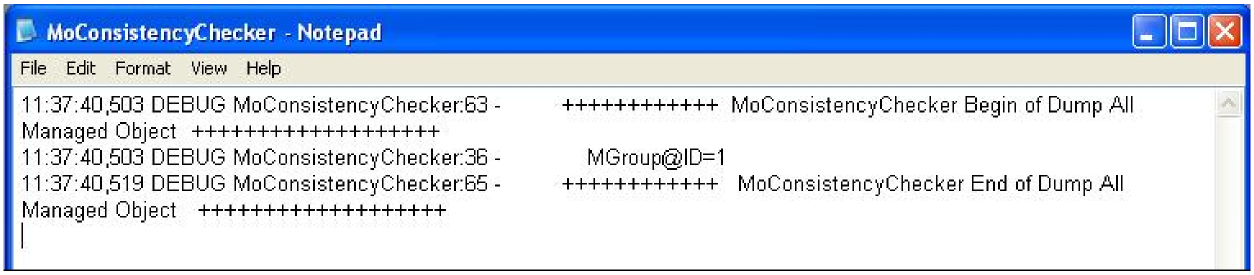
```
15:32:25,464 DEBUG MObject:114 - updateChildren find an old IonMSlot snmpIndex: 247463936
15:32:25,464 DEBUG MObject:114 - updateChildren find an old IonMSlot snmpIndex: 251658240
15:32:26,526 DEBUG MObject:114 - updateChildren find an old IonMAgentCard snmpIndex: 139460608
15:32:26,542 DEBUG MObject:114 - updateChildren find an old IonMCard323x snmpIndex: 147849216
15:32:26,542 DEBUG MObject:114 - updateChildren find an old IonMCard323x snmpIndex: 156237824
15:32:26,542 DEBUG MObject:114 - updateChildren find an old IonMCard3221 snmpIndex: 168820736
15:32:26,542 DEBUG MObject:125 - IonMChassis@SI=134217728 updateChildren find a new IonMCard3231 snmpIndex: 177209344
15:32:26,542  INFO MObject:220 - Add one IonMCard : IonMCard3231 at 177209344
15:32:26,542 DEBUG MObject:227 - IonMChassis@SI=134217728 start a discovery when Polling addChild for
child:IonMCard3231@SI=177209344
15:32:26,542 DEBUG MObject:114 - updateChildren find an old IonMCard2110 snmpIndex: 185597952
15:32:26,542 DEBUG MObject:114 - updateChildren find an old IonMCard2210 snmpIndex: 193986560
15:32:26,542 DEBUG MObject:114 - updateChildren find an old IonMCardFBRM snmpIndex: 202375168
15:32:26,542 DEBUG MObject:114 - updateChildren find an old IonMCardFBRM snmpIndex: 210763776
15:32:26,542 DEBUG MObject:114 - updateChildren find an old Ionps snmpIndex: 227540992
15:32:26,542 DEBUG MObject:114 - updateChildren find an old Ionps snmpIndex: 231735296
```

A MObject log example for an ION system is shown below in plain text.

```
15:44:21,913 DEBUG MObject:125 - IonMChassis@SI=134217728 updateChildren find a new IonMCard3231
snmpIndex: 177209344
15:44:21,913  INFO MObject:220 - Add one IonMCard : IonMCard3231 at 177209344
15:44:21,913 DEBUG MObject:227 - IonMChassis@SI=134217728 start a discovery when Polling addChild for
child:IonMCard3231@SI=177209344
15:44:21,913 DEBUG MObject:114 - updateChildren find an old IonMCard2110 snmpIndex: 185597952
15:44:21,913 DEBUG MObject:114 - updateChildren find an old IonMCard2210 snmpIndex: 193986560
15:44:21,913 DEBUG MObject:114 - updateChildren find an old IonMCardFBRM snmpIndex: 202375168
15:44:21,913 DEBUG MObject:114 - updateChildren find an old IonMCardFBRM snmpIndex: 210763776
15:44:21,913 DEBUG MObject:114 - updateChildren find an old Ionps snmpIndex: 227540992
15:44:21,913 DEBUG MObject:114 - updateChildren find an old Ionps snmpIndex: 231735296
15:44:30,117 DEBUG MObject:114 - updateChildren find an old IonMChassis snmpIndex: 134217728
15:44:30,570 DEBUG MObject:114 - updateChildren find an old IonMSlot snmpIndex: 138412032
15:44:30,570 DEBUG MObject:114 - updateChildren find an old IonMSlot snmpIndex: 142606336
15:44:30,570 DEBUG MObject:114 - updateChildren find an old IonMSlot snmpIndex: 146800640
15:44:31,757 DEBUG MObject:114 - updateChildren find an old IonMAgentCard snmpIndex: 139460608
15:44:31,757 DEBUG MObject:114 - updateChildren find an old IonMCard323x snmpIndex: 147849216
15:44:31,757 DEBUG MObject:114 - updateChildren find an old IonMCard323x snmpIndex: 156237824
15:44:31,757 DEBUG MObject:114 - updateChildren find an old IonMCard3221 snmpIndex: 168820736
15:44:31,757 DEBUG MObject:114 - updateChildren find an old IonMCard2110 snmpIndex: 185597952
15:44:31,757 DEBUG MObject:114 - updateChildren find an old IonMCard2210 snmpIndex: 193986560
15:44:31,757 DEBUG MObject:114 - updateChildren find an old IonMCardFBRM snmpIndex: 202375168
```

MoConsistencyChecker Log

This log file provides a dated, indexed list of managed object parameters for a system. A MoConsistencyChecker log example in Notepad is shown below.



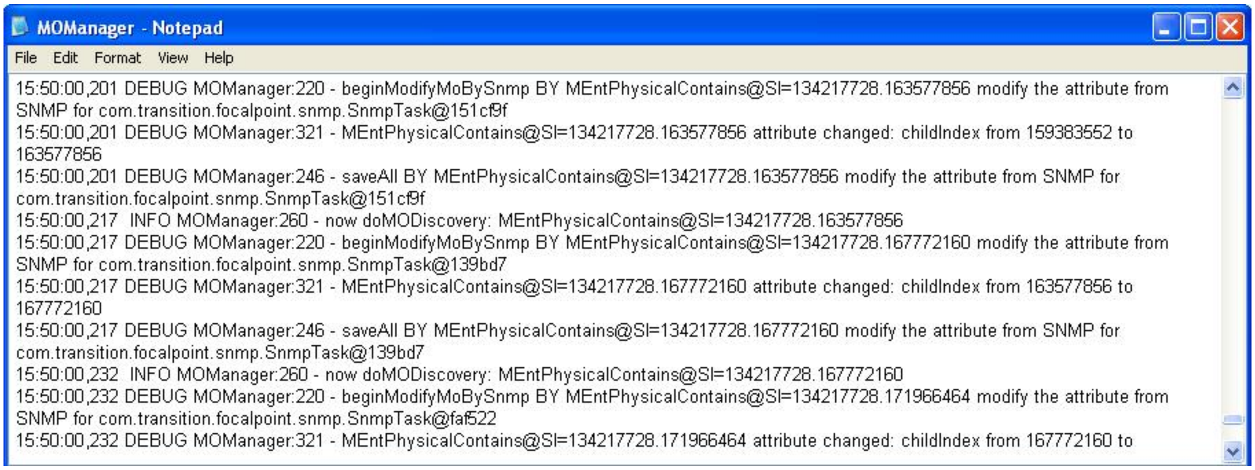
```
11:37:40,503 DEBUG MoConsistencyChecker:63 -    ++++++++++++ MoConsistencyChecker Begin of Dump All
Managed Object ++++++++++++++++++++
11:37:40,503 DEBUG MoConsistencyChecker:36 -      MGroup@ID=1
11:37:40,519 DEBUG MoConsistencyChecker:65 -    ++++++++++++  MoConsistencyChecker End of Dump All
Managed Object  ++++++++++++++++++++
```

A MoConsistencyChecker log example for an ION system is shown below in plain text.

```
08:17:04,513  WARN MoConsistencyChecker:53 - MIfTDRTest@SI=147849728 has null value of ResultValid
08:17:04,513 DEBUG MoConsistencyChecker:36 -                MIfMACSecurity@SI=147849728
08:17:04,513 DEBUG MoConsistencyChecker:36 -                MIfPriority@SI=147849728
08:17:04,513 DEBUG MoConsistencyChecker:36 -                MIfVLAN@SI=147849728
08:17:04,513 DEBUG MoConsistencyChecker:36 -                MIfVLANTagMgmt@SI=147849728
08:17:04,513 DEBUG MoConsistencyChecker:36 -                MDot3PauseEntry@SI=147849728
08:17:04,513 DEBUG MoConsistencyChecker:36 -                MionLOAMIfMgmtEntry@SI=147849728
08:17:04,513 DEBUG MoConsistencyChecker:36 -                MDot3OamStatsEntry@SI=147849728
08:17:04,513 DEBUG MoConsistencyChecker:36 -                MDot3OamEntry@SI=147849728
08:17:04,513 DEBUG MoConsistencyChecker:36 -                MDot3OamPeerEntry@SI=147849728
08:17:04,528 DEBUG MoConsistencyChecker:36 -                MDot3OamLoopbackEntry@SI=147849728
08:17:04,528 DEBUG MoConsistencyChecker:36 -                MDot3OamEventConfigEntry@SI=147849728
08:17:04,528 DEBUG MoConsistencyChecker:36 -                MDot3OamEventLogEntry@SI=147849728.1
08:17:04,528 DEBUG MoConsistencyChecker:36 -                MDot3OamEventLogEntry@SI=147849728.2
08:17:04,528 DEBUG MoConsistencyChecker:36 -                MIonIfTNDPEntity@SI=147849728
08:17:04,528 DEBUG MoConsistencyChecker:36 -                  MifMauAutoNegEntry@ID=2901
08:17:04,528 DEBUG MoConsistencyChecker:36 -                  MInterface@SI=147849728
08:17:04,528 DEBUG MoConsistencyChecker:36 -                  MEthInterface@SI=147849728
08:17:04,528 DEBUG MoConsistencyChecker:36 -                  MDMInfo@SI=147849728
08:17:04,528 DEBUG MoConsistencyChecker:36 -                  MIfFwdPortList@SI=147849728
08:17:04,528 DEBUG MoConsistencyChecker:36 -                  MIfPriorityRemap@SI=147849728.0
08:17:04,528 DEBUG MoConsistencyChecker:36 -                    MIfX@SI=147849728
08:17:04,528 DEBUG MoConsistencyChecker:36 -                    MRmonEtherStats@SI=147849728
08:17:04,528 DEBUG MoConsistencyChecker:36 -                    MDot3StatsEntry@SI=147849728
08:17:04,528 DEBUG MoConsistencyChecker:36 -                      MEntityPhysical@SI=147849728
08:17:04,544 DEBUG MoConsistencyChecker:36 -                  MIfFwdPortList@SI=147849472
08:17:04,544 DEBUG MoConsistencyChecker:36 -                  MIfTDRResult@SI=147849472.1
08:17:04,544 DEBUG MoConsistencyChecker:36 -                  MIfTDRResult@SI=147849472.2
08:17:04,544 DEBUG MoConsistencyChecker:36 -                  MIfTDRResult@SI=147849472.3
08:17:04,544 DEBUG MoConsistencyChecker:36 -                  MIfTDRResult@SI=147849472.4
08:17:04,544 DEBUG MoConsistencyChecker:36 -                  MIfPriorityRemap@SI=147849472.0
08:17:04,544 DEBUG MoConsistencyChecker:36 -                  MDot3ControlEntry@SI=147849472
08:17:04,544 DEBUG MoConsistencyChecker:36 -                    MIfX@SI=147849472
08:17:04,544 DEBUG MoConsistencyChecker:36 -                    MRmonEtherStats@SI=147849472
08:17:04,544 DEBUG MoConsistencyChecker:36 -                    MDot3StatsEntry@SI=147849472
08:17:04,544 DEBUG MoConsistencyChecker:36 -                      MEntityPhysical@SI=147849472
08:17:04,544 DEBUG MoConsistencyChecker:36 -                MEntityPhysical@SI=147849216
08:17:04,544 DEBUG MoConsistencyChecker:36 -      IonMChassisSlot@SI=134217728.1
08:17:04,560 DEBUG MoConsistencyChecker:36 -      IonMChassisSlot@SI=134217728.2
08:17:04,560 DEBUG MoConsistencyChecker:36 -      IonMChassisSlot@SI=134217728.24
08:17:04,560 DEBUG MoConsistencyChecker:36 -        MEntityPhysical@SI=134217728
08:17:04,560 DEBUG MoConsistencyChecker:36 -      MEntityPhysical@SI=1
08:17:04,560 DEBUG MoConsistencyChecker:65 -  ++++++++++++  MoConsistencyChecker End of Dump All Managed
Object  ++++++++++++++++++++
```

MOManager Log

This log file provides a dated, indexed list of managed objects' status for a system. A MOManager log example in Notepad is shown below.



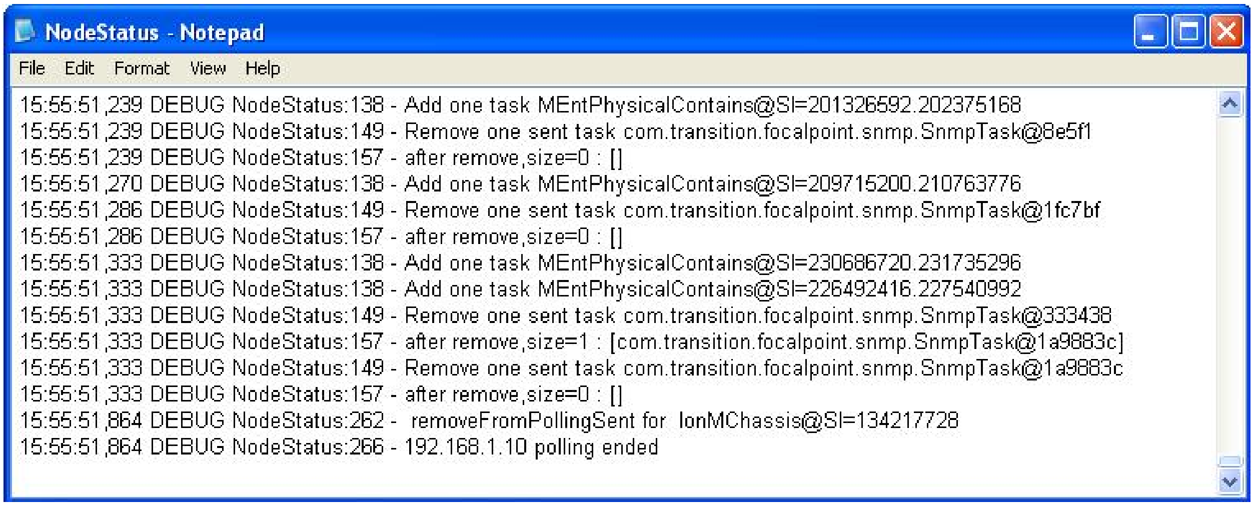
```
15:50:00,201 DEBUG MOManager:220 - beginModifyMoBySnmp BY MEntPhysicalContains@SI=134217728.163577856 modify the attribute from
SNMP for com.transition.focalpoint.snmp.SnmpTask@151cf9f
15:50:00,201 DEBUG MOManager:321 - MEntPhysicalContains@SI=134217728.163577856 attribute changed: childIndex from 159383552 to
163577856
15:50:00,201 DEBUG MOManager:246 - saveAll BY MEntPhysicalContains@SI=134217728.163577856 modify the attribute from SNMP for
com.transition.focalpoint.snmp.SnmpTask@151cf9f
15:50:00,217  INFO MOManager:260 - now doMODiscovery: MEntPhysicalContains@SI=134217728.163577856
15:50:00,217 DEBUG MOManager:220 - beginModifyMoBySnmp BY MEntPhysicalContains@SI=134217728.167772160 modify the attribute from
SNMP for com.transition.focalpoint.snmp.SnmpTask@139bd7
15:50:00,217 DEBUG MOManager:321 - MEntPhysicalContains@SI=134217728.167772160 attribute changed: childIndex from 163577856 to
167772160
15:50:00,217 DEBUG MOManager:246 - saveAll BY MEntPhysicalContains@SI=134217728.167772160 modify the attribute from SNMP for
com.transition.focalpoint.snmp.SnmpTask@139bd7
15:50:00,232  INFO MOManager:260 - now doMODiscovery: MEntPhysicalContains@SI=134217728.167772160
15:50:00,232 DEBUG MOManager:220 - beginModifyMoBySnmp BY MEntPhysicalContains@SI=134217728.171966464 modify the attribute from
SNMP for com.transition.focalpoint.snmp.SnmpTask@faf522
15:50:00,232 DEBUG MOManager:321 - MEntPhysicalContains@SI=134217728.171966464 attribute changed: childIndex from 167772160 to
```

A MOManager log example for an ION system is shown below in plain text.

```
15:39:15,356 DEBUG MOManager:321 - MEntPhysicalContains@SI=134217728.230686720 attribute changed: childIndex
from 226492416 to 230686720
15:39:15,356 DEBUG MOManager:246 - saveAll BY MEntPhysicalContains@SI=134217728.230686720 modify the attribute
from SNMP for com.transition.focalpoint.snmp.SnmpTask@afe203
15:39:15,356  INFO MOManager:260 - now doMODiscovery: MEntPhysicalContains@SI=134217728.230686720
15:39:15,371 DEBUG MOManager:220 - beginModifyMoBySnmp BY MEntPhysicalContains@SI=134217728.234881024
modify the attribute from SNMP for com.transition.focalpoint.snmp.SnmpTask@b23610
15:39:15,371 DEBUG MOManager:321 - MEntPhysicalContains@SI=134217728.234881024 attribute changed: childIndex
from 230686720 to 234881024
15:39:15,371 DEBUG MOManager:246 - saveAll BY MEntPhysicalContains@SI=134217728.234881024 modify the attribute
from SNMP for com.transition.focalpoint.snmp.SnmpTask@b23610
15:39:15,371  INFO MOManager:260 - now doMODiscovery: MEntPhysicalContains@SI=134217728.234881024
15:39:15,387 DEBUG MOManager:220 - beginModifyMoBySnmp BY MEntPhysicalContains@SI=134217728.239075328
modify the attribute from SNMP for com.transition.focalpoint.snmp.SnmpTask@16ff53f
15:39:15,387 DEBUG MOManager:321 - MEntPhysicalContains@SI=134217728.239075328 attribute changed: childIndex
from 234881024 to 239075328
```

NodeStatus Log

This log file provides a dated, indexed list of added and removed tasks for a system. A NodeStatus log example in Notepad is shown below.



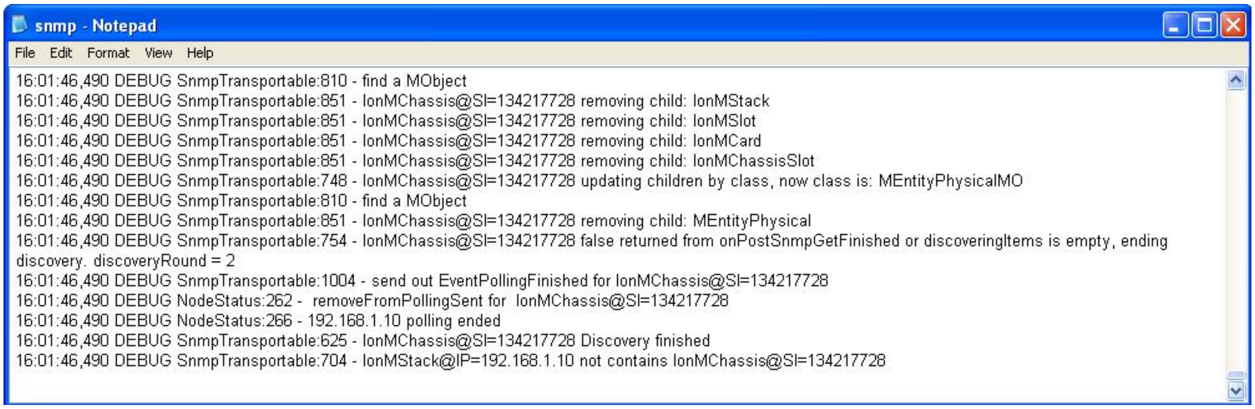
```
15:55:51,239 DEBUG NodeStatus:138 - Add one task MEntPhysicalContains@SI=201326592.202375168
15:55:51,239 DEBUG NodeStatus:149 - Remove one sent task com.transition.focalpoint.snmp.SnmpTask@8e5f1
15:55:51,239 DEBUG NodeStatus:157 - after remove,size=0 : []
15:55:51,270 DEBUG NodeStatus:138 - Add one task MEntPhysicalContains@SI=209715200.210763776
15:55:51,286 DEBUG NodeStatus:149 - Remove one sent task com.transition.focalpoint.snmp.SnmpTask@1fc7bf
15:55:51,286 DEBUG NodeStatus:157 - after remove,size=0 : []
15:55:51,333 DEBUG NodeStatus:138 - Add one task MEntPhysicalContains@SI=230686720.231735296
15:55:51,333 DEBUG NodeStatus:138 - Add one task MEntPhysicalContains@SI=226492416.227540992
15:55:51,333 DEBUG NodeStatus:149 - Remove one sent task com.transition.focalpoint.snmp.SnmpTask@333438
15:55:51,333 DEBUG NodeStatus:157 - after remove,size=1 : [com.transition.focalpoint.snmp.SnmpTask@1a9883c]
15:55:51,333 DEBUG NodeStatus:149 - Remove one sent task com.transition.focalpoint.snmp.SnmpTask@1a9883c
15:55:51,333 DEBUG NodeStatus:157 - after remove,size=0 : []
15:55:51,864 DEBUG NodeStatus:262 -  removeFromPollingSent for  IonMChassis@SI=134217728
15:55:51,864 DEBUG NodeStatus:266 - 192.168.1.10 polling ended
```

A NodeStatus log example for an ION system is shown below in plain text.

```
15:42:55,405 DEBUG NodeStatus:149 - Remove one sent task com.transition.focalpoint.snmp.SnmpTask@1dbac25
15:42:55,405 DEBUG NodeStatus:157 - after remove,size=0 : []
15:42:55,421 DEBUG NodeStatus:138 - Add one task MEntPhysicalContains@SI=134217728.247463936
15:42:55,421 DEBUG NodeStatus:149 - Remove one sent task com.transition.focalpoint.snmp.SnmpTask@c173f8
15:42:55,421 DEBUG NodeStatus:157 - after remove,size=0 : []
15:42:55,437 DEBUG NodeStatus:138 - Add one task MEntPhysicalContains@SI=134217728.251658240
15:42:55,437 DEBUG NodeStatus:149 - Remove one sent task com.transition.focalpoint.snmp.SnmpTask@14282a4
15:42:55,437 DEBUG NodeStatus:157 - after remove,size=0 : []
15:42:55,468 DEBUG NodeStatus:138 - Add one task MEntPhysicalContains@SI=138412032
15:42:55,468 DEBUG NodeStatus:138 - Add one task MEntPhysicalContains@SI=142606336
15:42:55,468 DEBUG NodeStatus:138 - Add one task MEntPhysicalContains@SI=146800640
15:42:55,468 DEBUG NodeStatus:138 - Add one task MEntPhysicalContains@SI=150994944
15:42:55,468 DEBUG NodeStatus:138 - Add one task MEntPhysicalContains@SI=155189248
15:42:55,468 DEBUG NodeStatus:138 - Add one task MEntPhysicalContains@SI=159383552
15:42:55,468 DEBUG NodeStatus:138 - Add one task MEntPhysicalContains@SI=163577856
15:42:55,468 DEBUG NodeStatus:138 - Add one task MEntPhysicalContains@SI=167772160
15:42:55,468 DEBUG NodeStatus:138 - Add one task MEntPhysicalContains@SI=171966464
```

snmp Log

This log file provides a dated, indexed list of SNMP actions / status for a system. An snmp log example in Notepad is shown below.



```
16:01:46,490 DEBUG SnmpTransportable:810 - find a MObject
16:01:46,490 DEBUG SnmpTransportable:851 - IonMChassis@SI=134217728 removing child: IonMStack
16:01:46,490 DEBUG SnmpTransportable:851 - IonMChassis@SI=134217728 removing child: IonMSlot
16:01:46,490 DEBUG SnmpTransportable:851 - IonMChassis@SI=134217728 removing child: IonMCard
16:01:46,490 DEBUG SnmpTransportable:851 - IonMChassis@SI=134217728 removing child: IonMChassisSlot
16:01:46,490 DEBUG SnmpTransportable:748 - IonMChassis@SI=134217728 updating children by class, now class is: MEntityPhysicalMO
16:01:46,490 DEBUG SnmpTransportable:810 - find a MObject
16:01:46,490 DEBUG SnmpTransportable:851 - IonMChassis@SI=134217728 removing child: MEntityPhysical
16:01:46,490 DEBUG SnmpTransportable:754 - IonMChassis@SI=134217728 false returned from onPostSnmpGetFinished or discoveringItems is empty, ending
discovery. discoveryRound = 2
16:01:46,490 DEBUG SnmpTransportable:1004 - send out EventPollingFinished for IonMChassis@SI=134217728
16:01:46,490 DEBUG NodeStatus:262 -  removeFromPollingSent for  IonMChassis@SI=134217728
16:01:46,490 DEBUG NodeStatus:266 - 192.168.1.10 polling ended
16:01:46,490 DEBUG SnmpTransportable:625 - IonMChassis@SI=134217728 Discovery finished
16:01:46,490 DEBUG SnmpTransportable:704 - IonMStack@IP=192.168.1.10 not contains IonMChassis@SI=134217728
```

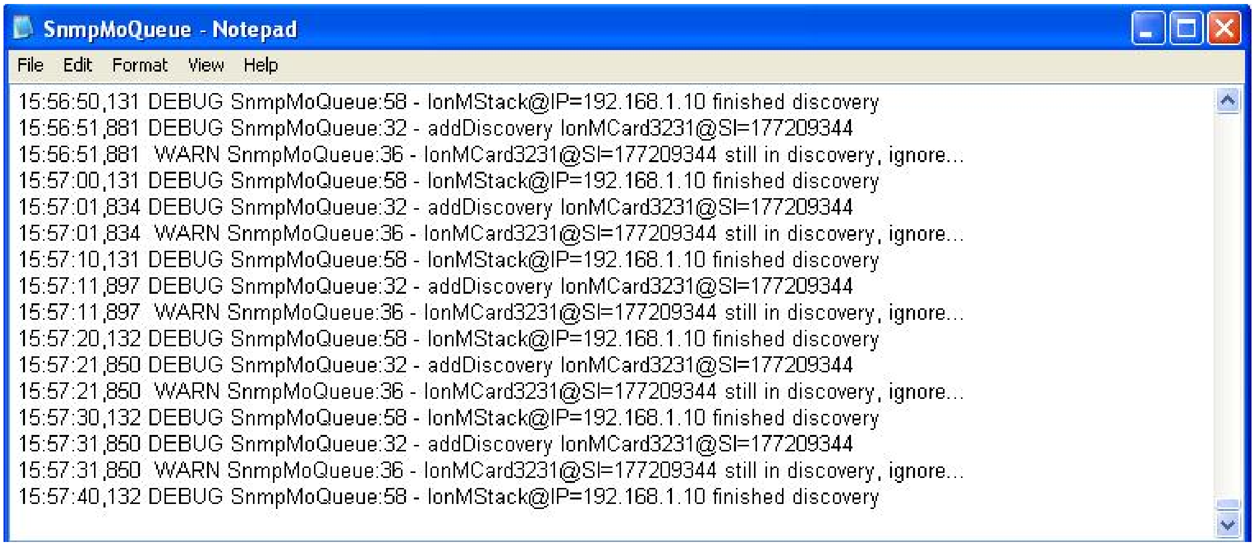
An snmp log example for an ION system is shown below in plain text.

```
14:02:51,703 DEBUG SnmpTransportable:810 - find a MObject
14:02:51,703 DEBUG SnmpTransportable:851 - IonMChassis@SI=134217728 removing child: IonMStack
14:02:51,703 DEBUG SnmpTransportable:851 - IonMChassis@SI=134217728 removing child: IonMSlot
14:02:51,703 DEBUG SnmpTransportable:851 - IonMChassis@SI=134217728 removing child: IonMCard
14:02:51,703 DEBUG SnmpMoQueue:32 - addDiscovery IonMCard3231@SI=177209344
14:02:51,703  WARN SnmpMoQueue:36 - IonMCard3231@SI=177209344 still in discovery, ignore...
14:02:51,703 DEBUG SnmpTransportable:545 - addToDiscoveryPool Mo: IonMCard3231@SI=177209344
14:02:51,718 DEBUG SnmpTransportable:851 - IonMChassis@SI=134217728 removing child: IonMChassisSlot
14:02:51,718 DEBUG SnmpTransportable:748 - IonMChassis@SI=134217728 updating children by class, now class is:
MEntityPhysicalMO
14:02:51,718 DEBUG SnmpTransportable:810 - find a MObject
14:02:51,718 DEBUG SnmpTransportable:851 - IonMChassis@SI=134217728 removing child: MEntityPhysical
14:02:51,718 DEBUG SnmpTransportable:754 - IonMChassis@SI=134217728 false returned from onPostSnmpGetFinished or
discoveringItems is empty, ending discovery. discoveryRound = 2
14:02:51,718 DEBUG SnmpTransportable:1004 - send out EventPollingFinished for IonMChassis@SI=134217728
14:02:51,718 DEBUG NodeStatus:262 -  removeFromPollingSent for  IonMChassis@SI=134217728
14:02:51,718 DEBUG NodeStatus:266 - 192.168.1.10 polling ended
14:02:51,718 DEBUG SnmpTransportable:625 - IonMChassis@SI=134217728 Discovery finished
14:02:51,718 DEBUG SnmpTransportable:704 - IonMStack@IP=192.168.1.10 not contains IonMChassis@SI=134217728
```

SnmpMoQueue Log

This log file provides a dated, indexed list of managed object queue actions/ status for a system.

An snmp log example in Notepad is shown below.



```
15:56:50,131 DEBUG SnmpMoQueue:58 - IonMStack@IP=192.168.1.10 finished discovery
15:56:51,881 DEBUG SnmpMoQueue:32 - addDiscovery IonMCard3231@SI=177209344
15:56:51,881  WARN SnmpMoQueue:36 - IonMCard3231@SI=177209344 still in discovery, ignore...
15:57:00,131 DEBUG SnmpMoQueue:58 - IonMStack@IP=192.168.1.10 finished discovery
15:57:01,834 DEBUG SnmpMoQueue:32 - addDiscovery IonMCard3231@SI=177209344
15:57:01,834  WARN SnmpMoQueue:36 - IonMCard3231@SI=177209344 still in discovery, ignore...
15:57:10,131 DEBUG SnmpMoQueue:58 - IonMStack@IP=192.168.1.10 finished discovery
15:57:11,897 DEBUG SnmpMoQueue:32 - addDiscovery IonMCard3231@SI=177209344
15:57:11,897  WARN SnmpMoQueue:36 - IonMCard3231@SI=177209344 still in discovery, ignore...
15:57:20,132 DEBUG SnmpMoQueue:58 - IonMStack@IP=192.168.1.10 finished discovery
15:57:21,850 DEBUG SnmpMoQueue:32 - addDiscovery IonMCard3231@SI=177209344
15:57:21,850  WARN SnmpMoQueue:36 - IonMCard3231@SI=177209344 still in discovery, ignore...
15:57:30,132 DEBUG SnmpMoQueue:58 - IonMStack@IP=192.168.1.10 finished discovery
15:57:31,850 DEBUG SnmpMoQueue:32 - addDiscovery IonMCard3231@SI=177209344
15:57:31,850  WARN SnmpMoQueue:36 - IonMCard3231@SI=177209344 still in discovery, ignore...
15:57:40,132 DEBUG SnmpMoQueue:58 - IonMStack@IP=192.168.1.10 finished discovery
```

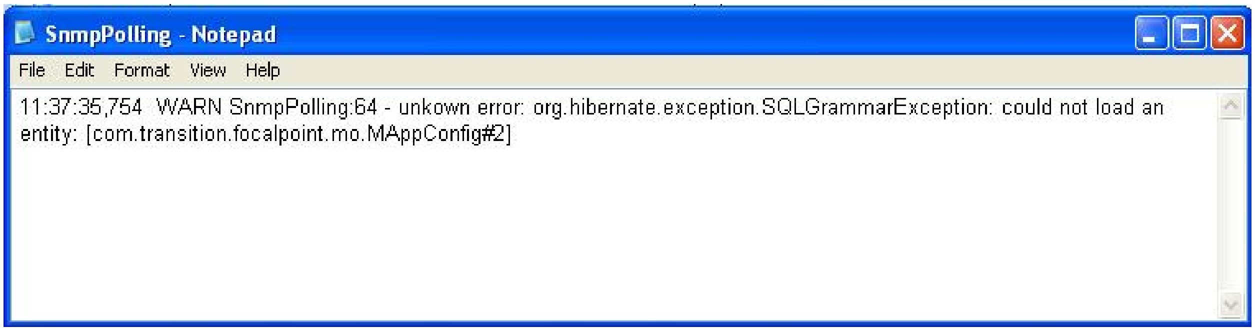
An SnmpMoQueue log example for an ION system is shown below in plain text.

```
16:38:05,101 DEBUG SnmpMoQueue:32 - addDiscovery IonMStack@IP=192.168.1.10
16:38:05,101 DEBUG SnmpMoQueue:45 - scheduleDiscovery IonMStack@IP=192.168.1.10
16:38:10,335 DEBUG SnmpMoQueue:58 - IonMStack@IP=192.168.1.10 finished discovery
16:38:10,335 DEBUG SnmpMoQueue:64 - Finished all discovery...
16:38:16,648 DEBUG SnmpMoQueue:58 - IonMStack@IP=192.168.1.10 finished discovery
16:38:16,648 DEBUG SnmpMoQueue:64 - Finished all discovery...
16:38:17,086 DEBUG SnmpMoQueue:58 - IonMStack@IP=192.168.1.10 finished discovery
16:38:17,086 DEBUG SnmpMoQueue:64 - Finished all discovery...
16:38:31,742 DEBUG SnmpMoQueue:58 - IonMStack@IP=192.168.1.10 finished discovery
16:38:31,742 DEBUG SnmpMoQueue:64 - Finished all discovery...
16:38:36,649 DEBUG SnmpMoQueue:58 - IonMStack@IP=192.168.1.10 finished discovery
16:38:36,649 DEBUG SnmpMoQueue:64 - Finished all discovery...
16:38:56,727 DEBUG SnmpMoQueue:58 - IonMStack@IP=192.168.1.10 finished discovery
16:38:56,727 DEBUG SnmpMoQueue:64 - Finished all discovery...
16:39:16,665 DEBUG SnmpMoQueue:58 - IonMStack@IP=192.168.1.10 finished discovery
16:39:16,665 DEBUG SnmpMoQueue:64 - Finished all discovery...
```

SnmpPolling Log

This log file provides a dated, indexed list of known and unknown error messages / descriptions for a system.

An SnmpPolling log example in Notepad is shown below.



```
11:37:35,754  WARN SnmpPolling:64 - unkown error: org.hibernate.exception.SQLGrammarException: could not load an
entity: [com.transition.focalpoint.mo.MAppConfig#2]
```

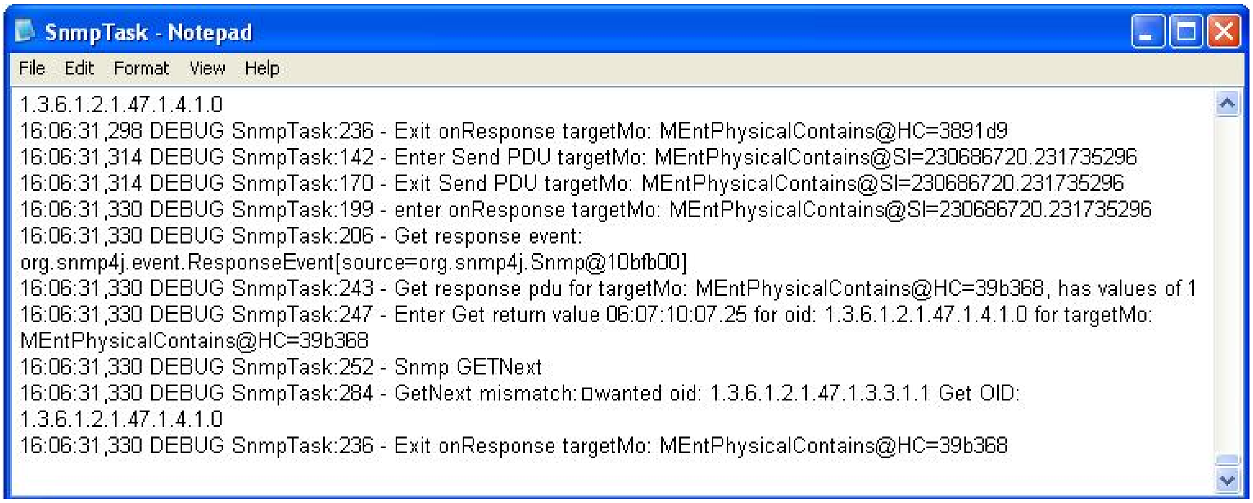
An SnmpPolling log example for an ION system is shown below in plain text.

```
15:27:48,926  WARN SnmpPolling:64 - unkown error: org.hibernate.exception.SQLGrammarException: could not load an
entity: [com.transition.focalpoint.mo.MAppConfig#2]
```

SnmpTask Log

This log file provides a dated, indexed list of SNMP task actions / descriptions for a system.

An SnmpTask log example in Notepad is shown below.



```
1.3.6.1.2.1.47.1.4.1.0
16:06:31,298 DEBUG SnmpTask:236 - Exit onResponse targetMo: MEntPhysicalContains@HC=3891d9
16:06:31,314 DEBUG SnmpTask:142 - Enter Send PDU targetMo: MEntPhysicalContains@SI=230686720.231735296
16:06:31,314 DEBUG SnmpTask:170 - Exit Send PDU targetMo: MEntPhysicalContains@SI=230686720.231735296
16:06:31,330 DEBUG SnmpTask:199 - enter onResponse targetMo: MEntPhysicalContains@SI=230686720.231735296
16:06:31,330 DEBUG SnmpTask:206 - Get response event:
org.snmp4j.event.ResponseEvent[source=org.snmp4j.Snmp@10bfb00]
16:06:31,330 DEBUG SnmpTask:243 - Get response pdu for targetMo: MEntPhysicalContains@HC=39b368, has values of 1
16:06:31,330 DEBUG SnmpTask:247 - Enter Get return value 06:07:10:07.25 for oid: 1.3.6.1.2.1.47.1.4.1.0 for targetMo:
MEntPhysicalContains@HC=39b368
16:06:31,330 DEBUG SnmpTask:252 - Snmp GETNext
16:06:31,330 DEBUG SnmpTask:284 - GetNext mismatch:□wanted oid: 1.3.6.1.2.1.47.1.3.3.1.1 Get OID:
1.3.6.1.2.1.47.1.4.1.0
16:06:31,330 DEBUG SnmpTask:236 - Exit onResponse targetMo: MEntPhysicalContains@HC=39b368
```

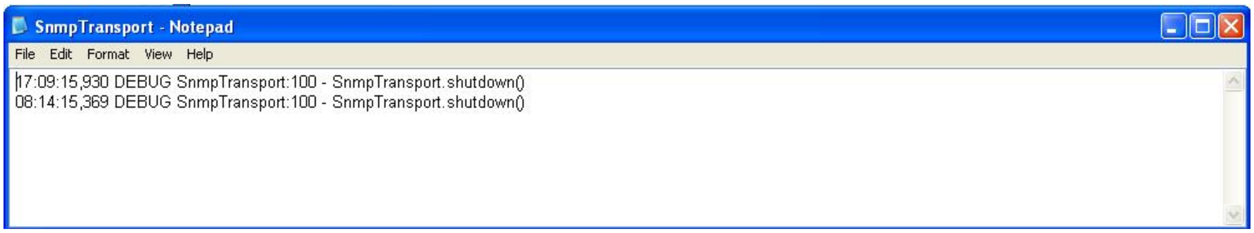
An SnmpTask log example for an ION system is shown below in plain text.

```
16:12:35,690 DEBUG SnmpTask:199 - enter onResponse targetMo: MEntPhysicalContains@SI=247463936
16:12:35,690 DEBUG SnmpTask:206 - Get response event:
org.snmp4j.event.ResponseEvent[source=org.snmp4j.Snmp@ee75b7]
16:12:35,690 DEBUG SnmpTask:243 - Get response pdu for targetMo: MEntPhysicalContains@HC=a705d3, has values of 1
16:12:35,690 DEBUG SnmpTask:247 - Enter Get return value 12:07:15:34.25 for oid: 1.3.6.1.2.1.47.1.4.1.0 for targetMo:
MEntPhysicalContains@HC=a705d3
16:12:35,690 DEBUG SnmpTask:252 - Snmp GETNext
16:12:35,690 DEBUG SnmpTask:284 - GetNext mismatch:
wanted oid: 1.3.6.1.2.1.47.1.3.3.1.1 Get OID: 1.3.6.1.2.1.47.1.4.1.0
16:12:35,690 DEBUG SnmpTask:236 - Exit onResponse targetMo: MEntPhysicalContains@HC=a705d3
16:12:35,690 DEBUG SnmpTask:142 - Enter Send PDU targetMo: MEntPhysicalContains@SI=146800640.147849216
16:12:35,690 DEBUG SnmpTask:170 - Exit Send PDU targetMo: MEntPhysicalContains@SI=146800640.147849216
16:12:35,690 DEBUG SnmpTask:199 - enter onResponse targetMo: MEntPhysicalContains@SI=251658240
16:12:35,690 DEBUG SnmpTask:206 - Get response event:
org.snmp4j.event.ResponseEvent[source=org.snmp4j.Snmp@ee75b7]
16:12:35,690 DEBUG SnmpTask:243 - Get response pdu for targetMo: MEntPhysicalContains@HC=16f9d87, has values of 1
16:12:35,690 DEBUG SnmpTask:142 - Enter Send PDU targetMo: MEntPhysicalContains@SI=155189248.156237824
16:12:35,690 DEBUG SnmpTask:247 - Enter Get return value 12:07:15:34.25 for oid: 1.3.6.1.2.1.47.1.4.1.0 for targetMo:
MEntPhysicalContains@HC=16f9d87
16:12:35,690 DEBUG SnmpTask:252 - Snmp GETNext
16:12:35,690 DEBUG SnmpTask:284 - GetNext mismatch:
wanted oid: 1.3.6.1.2.1.47.1.3.3.1.1 Get OID: 1.3.6.1.2.1.47.1.4.1.0
```

SnmpTransport Log

This log file provides a dated, indexed list of SNMP transport actions for a system.

An SnmpTransport log example in Notepad is shown below.



```
17:09:15,930 DEBUG SnmpTransport:100 - SnmpTransport.shutdown()
08:14:15,369 DEBUG SnmpTransport:100 - SnmpTransport.shutdown()
```

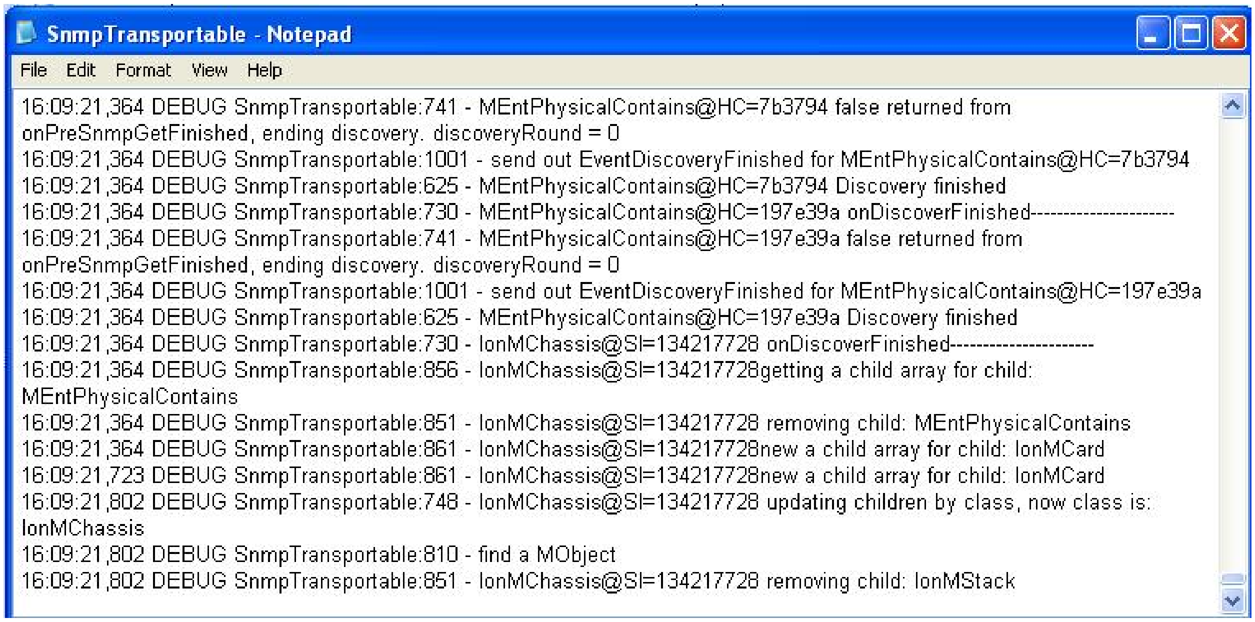
An SnmpTransport log example for an ION system is shown below in plain text.

```
17:09:15,930 DEBUG SnmpTransport:100 - SnmpTransport.shutdown()
08:14:15,369 DEBUG SnmpTransport:100 - SnmpTransport.shutdown()
```

SnmpTransportable Log

This log file provides a dated, indexed list of SNMP debug messages for a system.

An SnmpTransportable log example in Notepad is shown below.



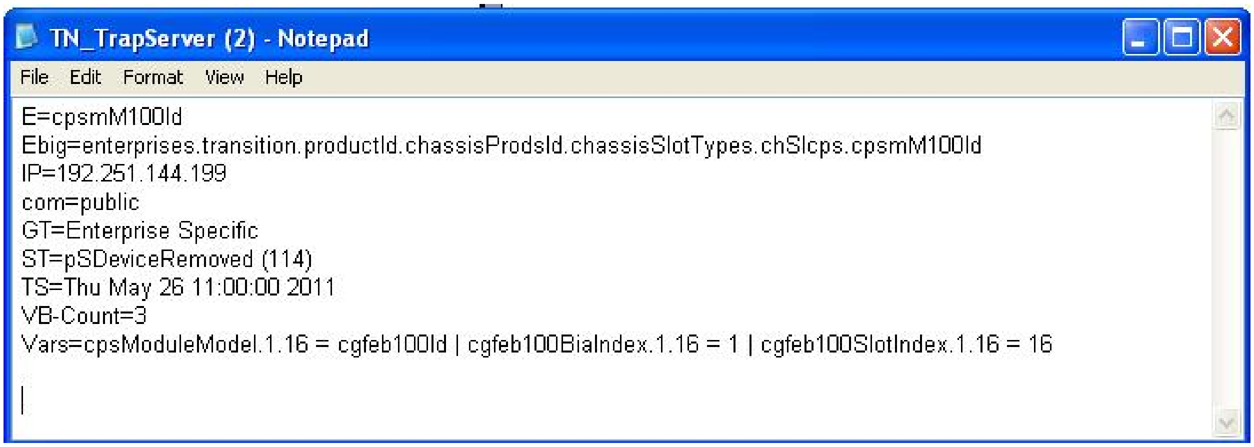
```
16:09:21,364 DEBUG SnmpTransportable:741 - MEntPhysicalContains@HC=7b3794 false returned from
onPreSnmpGetFinished, ending discovery. discoveryRound = 0
16:09:21,364 DEBUG SnmpTransportable:1001 - send out EventDiscoveryFinished for MEntPhysicalContains@HC=7b3794
16:09:21,364 DEBUG SnmpTransportable:625 - MEntPhysicalContains@HC=7b3794 Discovery finished
16:09:21,364 DEBUG SnmpTransportable:730 - MEntPhysicalContains@HC=197e39a onDiscoverFinished---------------------
16:09:21,364 DEBUG SnmpTransportable:741 - MEntPhysicalContains@HC=197e39a false returned from
onPreSnmpGetFinished, ending discovery. discoveryRound = 0
16:09:21,364 DEBUG SnmpTransportable:1001 - send out EventDiscoveryFinished for MEntPhysicalContains@HC=197e39a
16:09:21,364 DEBUG SnmpTransportable:625 - MEntPhysicalContains@HC=197e39a Discovery finished
16:09:21,364 DEBUG SnmpTransportable:730 - IonMChassis@SI=134217728 onDiscoverFinished---------------------
16:09:21,364 DEBUG SnmpTransportable:856 - IonMChassis@SI=134217728getting a child array for child:
MEntPhysicalContains
16:09:21,364 DEBUG SnmpTransportable:851 - IonMChassis@SI=134217728 removing child: MEntPhysicalContains
16:09:21,364 DEBUG SnmpTransportable:861 - IonMChassis@SI=134217728new a child array for child: IonMCard
16:09:21,723 DEBUG SnmpTransportable:861 - IonMChassis@SI=134217728new a child array for child: IonMCard
16:09:21,802 DEBUG SnmpTransportable:748 - IonMChassis@SI=134217728 updating children by class, now class is:
IonMChassis
16:09:21,802 DEBUG SnmpTransportable:810 - find a MObject
16:09:21,802 DEBUG SnmpTransportable:851 - IonMChassis@SI=134217728 removing child: IonMStack
```

An SnmpTransportable log example for an ION system is shown below in plain text.

```
16:12:15,549 DEBUG SnmpTransportable:387 - ------------------------------MEntPhysicalContains@SI=146800640.147849216
onStartDiscover---------------------------
16:12:15,549 DEBUG SnmpTransportable:347 - Exit addToSnmpTaskMEntPhysicalContains
16:12:15,549 DEBUG SnmpTransportable:387 - ------------------------------MEntPhysicalContains@SI=138412032.139460608
onStartDiscover---------------------------
16:12:15,549 DEBUG SnmpTransportable:347 - Exit addToSnmpTaskMEntPhysicalContains
16:12:15,564 DEBUG SnmpTransportable:686 - IonMChassis@SI=134217728 has a new child of
MEntPhysicalContains@SI=155189248.156237824
16:12:15,564 DEBUG SnmpTransportable:730 - MEntPhysicalContains@SI=155189248.156237824 onDiscoverFinished---------
-------------
16:12:15,564 DEBUG SnmpTransportable:741 - MEntPhysicalContains@SI=155189248.156237824 false returned from
onPreSnmpGetFinished, ending discovery. discoveryRound = 0
16:12:15,564 DEBUG SnmpTransportable:1001 - send out EventDiscoveryFinished for
MEntPhysicalContains@SI=155189248.156237824
16:12:15,564 DEBUG SnmpTransportable:625 - MEntPhysicalContains@SI=155189248.156237824 Discovery finished
16:12:15,564 DEBUG SnmpTransportable:730 - MEntPhysicalContains@HC=11611c6 onDiscoverFinished----------------------
16:12:15,564 DEBUG SnmpTransportable:741 - MEntPhysicalContains@HC=11611c6 false returned from
onPreSnmpGetFinished, ending discovery. discoveryRound = 0
```

TN_TrapServer Log

This log file provides descriptive text for a single trap. A TN_TrapServer log example in Notepad is shown below, with one PS trap.



```
E=cpsmM100Id
Ebig=enterprises.transition.productId.chassisProdsId.chassisSlotTypes.chSlcps.cpsmM100Id
IP=192.251.144.199
com=public
GT=Enterprise Specific
ST=pSDeviceRemoved (114)
TS=Thu May 26 11:00:00 2011
VB-Count=3
Vars=cpsModuleModel.1.16 = cgfeb100Id | cgfeb100BiaIndex.1.16 = 1 | cgfeb100SlotIndex.1.16 = 16
```

A TN_TrapServer log example for an ION system is shown below in plain text.

```
E=cpsmM100Id
Ebig=enterprises.transition.productId.chassisProdsId.chassisSlotTypes.chSlcps.cpsmM100Id
IP=192.251.144.199
com=public
GT=Enterprise Specific
ST=pSDeviceRemoved (114)
TS=Thu May 26 11:00:00 2011
VB-Count=3
Vars=cpsModuleModel.1.16 = cgfeb100Id | cgfeb100BiaIndex.1.16 = 1 | cgfeb100SlotIndex.1.16 = 16
```

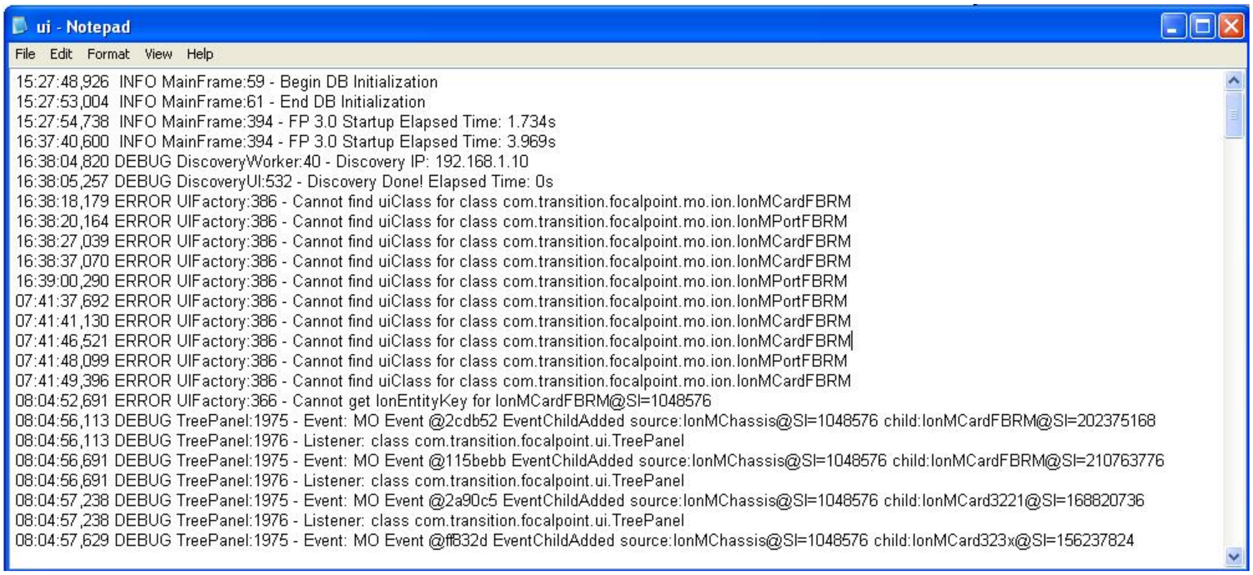
The log parameters are explained below.

Category	Meaning	Example
E=	Endian	cpsmM100Id
Ebig=	bigEndian	enterprises.transition.productId.chassisProdsId.chassisSlotTypes.chSlcps.cpsmM100Id
IP=	IP address	192.251.144.199
com=	public	
GT=	Generic Trap	Enterprise Specific
ST=	Specific Trap	pSDeviceRemoved (114)
TS=	Timestamp – the log date that the file was recorded	Thu May 26 11:00:00 2011
VB-Count=	The number of Varbinds (Variable bindings)	3
Vars=	Varbinds (Variable bindings) - the variable number of values that are included in an SNMP packet. Each varbind has an OID, type, and value (the value for/from that Object ID).	cpsModuleModel.1.16 = cgfeb100Id | cgfeb100BiaIndex.1.16 = 1 | cgfeb100SlotIndex.1.16 = 16

ui Log

This log file provides a dated, indexed list of debug exceptions for a system.

A ui log example in Notepad is shown below.



```
15:27:48,926  INFO MainFrame:59 - Begin DB Initialization
15:27:53,004  INFO MainFrame:61 - End DB Initialization
15:27:54,738  INFO MainFrame:394 - FP 3.0 Startup Elapsed Time: 1.734s
16:37:40,600  INFO MainFrame:394 - FP 3.0 Startup Elapsed Time: 3.969s
16:38:04,820 DEBUG DiscoveryWorker:40 - Discovery IP: 192.168.1.10
16:38:05,257 DEBUG DiscoveryUI:532 - Discovery Done! Elapsed Time: 0s
16:38:18,179 ERROR UIFactory:386 - Cannot find uiClass for class com.transition.focalpoint.mo.ion.IonMCardFBRM
16:38:20,164 ERROR UIFactory:386 - Cannot find uiClass for class com.transition.focalpoint.mo.ion.IonMPortFBRM
16:38:27,039 ERROR UIFactory:386 - Cannot find uiClass for class com.transition.focalpoint.mo.ion.IonMCardFBRM
16:38:37,070 ERROR UIFactory:386 - Cannot find uiClass for class com.transition.focalpoint.mo.ion.IonMCardFBRM
16:39:00,290 ERROR UIFactory:386 - Cannot find uiClass for class com.transition.focalpoint.mo.ion.IonMPortFBRM
07:41:37,692 ERROR UIFactory:386 - Cannot find uiClass for class com.transition.focalpoint.mo.ion.IonMPortFBRM
07:41:41,130 ERROR UIFactory:386 - Cannot find uiClass for class com.transition.focalpoint.mo.ion.IonMCardFBRM
07:41:46,521 ERROR UIFactory:386 - Cannot find uiClass for class com.transition.focalpoint.mo.ion.IonMCardFBRM
07:41:48,099 ERROR UIFactory:386 - Cannot find uiClass for class com.transition.focalpoint.mo.ion.IonMPortFBRM
07:41:49,396 ERROR UIFactory:386 - Cannot find uiClass for class com.transition.focalpoint.mo.ion.IonMCardFBRM
08:04:52,691 ERROR UIFactory:366 - Cannot get IonEntityKey for IonMCardFBRM@SI=1048576
08:04:56,113 DEBUG TreePanel:1975 - Event: MO Event @2cdb52 EventChildAdded source:IonMChassis@SI=1048576 child:IonMCardFBRM@SI=202375168
08:04:56,113 DEBUG TreePanel:1976 - Listener: class com.transition.focalpoint.ui.TreePanel
08:04:56,691 DEBUG TreePanel:1975 - Event: MO Event @115bebb EventChildAdded source:IonMChassis@SI=1048576 child:IonMCardFBRM@SI=210763776
08:04:56,691 DEBUG TreePanel:1976 - Listener: class com.transition.focalpoint.ui.TreePanel
08:04:57,238 DEBUG TreePanel:1975 - Event: MO Event @2a90c5 EventChildAdded source:IonMChassis@SI=1048576 child:IonMCard3221@SI=168820736
08:04:57,238 DEBUG TreePanel:1976 - Listener: class com.transition.focalpoint.ui.TreePanel
08:04:57,629 DEBUG TreePanel:1975 - Event: MO Event @ff832d EventChildAdded source:IonMChassis@SI=1048576 child:IonMCard323x@SI=156237824
```

A ui log example for an ION system is shown below in plain text.

```
13:21:48,640 DEBUG TreePanel:1718 - insertNodesByMos, mo is: IonMCard3231@SI=177209344parentNode is:
IonMChassis@SI=134217728
13:21:48,640 ERROR UIFactory:572 - Cannot find constructor for class com.transition.focalpoint.ui.ion.card.button.IonCardC2x2xBtn
java.lang.reflect.InvocationTargetException
        at sun.reflect.NativeConstructorAccessorImpl.newInstance0(Native Method)
        at sun.reflect.NativeConstructorAccessorImpl.newInstance(Unknown Source)
        at sun.reflect.DelegatingConstructorAccessorImpl.newInstance(Unknown Source)
        at java.lang.reflect.Constructor.newInstance(Unknown Source)
        at com.transition.focalpoint.ui.UIFactory.createIonCardBtn(UIFactory.java:567)
        at com.transition.focalpoint.ui.ion.IonChasUI.updateCardBtn(IonChasUI.java:199)
        at com.transition.focalpoint.ui.ion.IonChasUI.<init>(IonChasUI.java:70)
        at sun.reflect.NativeConstructorAccessorImpl.newInstance0(Native Method)
        at sun.reflect.NativeConstructorAccessorImpl.newInstance(Unknown Source)
        at sun.reflect.DelegatingConstructorAccessorImpl.newInstance(Unknown Source)
        at java.lang.reflect.Constructor.newInstance(Unknown Source)
        at com.transition.focalpoint.ui.UIFactory.createIonEntityUI(UIFactory.java:378)
        at com.transition.focalpoint.ui.DetailPanel.showIonEntityUI(DetailPanel.java:299)
        at com.transition.focalpoint.ui.PanelManager.showIonEntity(PanelManager.java:113)
        at com.transition.focalpoint.ui.TreePanel.showNode(TreePanel.java:543)
        at com.transition.focalpoint.ui.TreePanel.access$1500(TreePanel.java:88)
        at java.awt.LightweightDispatcher.retargetMouseEvent(Unknown Source)
        at java.awt.LightweightDispatcher.processMouseEvent(Unknown Source)
        at java.awt.Window.dispatchEventImpl(Unknown Source)
        at java.awt.Component.dispatchEvent(Unknown Source)
        at java.awt.EventQueue.dispatchEvent(Unknown Source)
Caused by: java.lang.NullPointerException
        at com.transition.focalpoint.ui.ion.card.button.IonCardC2x2xBtn.initButton(IonCardC2x2xBtn.java:77)
        at com.transition.focalpoint.ui.ion.card.button.IonCardC2x2xBtn.<init>(IonCardC2x2xBtn.java:65)
        ... 56 more
13:22:21,859 DEBUG TreePanel:1975 - Event: MO Event @906429 EventChildRemoved source:IonMChassis@SI=134217728
child:IonMCard3231@SI=177209344
13:22:21,859 DEBUG TreePanel:1976 - Listener: class com.transition.focalpoint.ui.TreePanel
```

Chapter 5 - Contact & Warranty Information

Introduction

This chapter explains how to contact Transition Networks via phone, fax, email, and direct mail. It also explains what the warranty covers, who to contact to return product, and how and where to return the product.

Contact Us

Technical Support

Technical support is available 24-hours a day at:

United States:	1-800-260-1312
International:	00-1-952-941-7600

Web-based training

Transition Networks provides 12-16 seminars per month via live web-based training.

Log onto www.transition.com and click the Learning Center link at the top of the page.

E-Mail

Ask a question anytime by sending an e-mail message to our technical support staff: techsupport@transition.com

Address

Transition Networks
10900 Red Circle Drive
Minnetonka, MN 55343, U.S.A.
Telephone: 952-941-7600
Toll free U.S.A & Canada: 800-526-9267
Fax: 952-941-2322

Warranty

Limited lifetime warranty

Effective for products shipped May 1, 1999 and after. Every Transition Networks labeled product purchased after May 1, 1999 will be free from defects in material and workmanship for its lifetime. This warranty covers the original user only and is not transferable.

What the warranty does not cover

This warranty does not cover damage from accident, acts of God, neglect, contamination, misuse or abnormal conditions of operation or handling, including over-voltage failures caused by use outside of the specified ratings of the product, or normal wear and tear of its mechanical components. If the user is unsure about the proper means of installing or using the equipment, contact Transition Networks' free technical support services.

Establishing original ownership

To establish original ownership and provide date of purchase, please complete and return the registration card accompanying the product or register the product on-line on our product registration page.

Transition Networks will, at its option:

- Repair the defective product to functional specifications at no charge
- Replace the product with an equivalent functional product
- Refund the purchase price of a defective product

Who to contact for returns

To return a defective product for warranty coverage, contact Transition Networks' technical support department for a return authorization number. Transition's technical support department can be reached through any of the following means:

Service Hours

Mon thru Fri 7 AM - 6 PM CST:

Contact Tech Support via telephone at 800-260-1312 or 952-941-7600 or
Fax 952-941-2322

Email techsupport@transition.com

Live web chat: Transition Now

Any Other Time

Voice Mail 800-260-1312 x 579 or 952-941-7600 x 579

How and where to send the returns

Send the defective product postage and insurance prepaid to the following address:

Transition Networks, Inc.
10900 Red Circle Drive
Minnetonka, MN 55343 USA
Attn: RETURNS DEPT: CRA/RMA # ___________

Failure to properly protect the product during shipping may void this warranty. The return authorization number must be written on the outside of the carton to ensure its acceptance. We cannot accept delivery of any equipment that is sent to us without a CRA or RMA number.

CRA's are valid for 60 days from the date of issuance. An invoice will be generated for payment on any unit(s) not returned within 60 days.

Upon completion of a demo/ evaluation test period, units must be returned or purchased within 30 days. An invoice will be generated for payment on any unit(s) not returned within 30 days after the demo/ evaluation period has expired.

The customer must pay for the non-compliant product(s) return transportation costs to Transition Networks for evaluation of said product(s) for repair or replacement. Transition Networks will pay for the shipping of the repaired or replaced in-warranty product(s) back to the customer (any and all customs charges, tariffs, or/and taxes are the customer's responsibility).

Before making any non-warranty repair, Transition Networks requires a $200.00 charge plus actual shipping costs to and from the customer. If the repair is greater than $200.00, an estimate is issued to the customer for authorization of repair. If no authorization is obtained, or the product is deemed 'not repairable', Transition Networks will retain the $200.00 service charge and return the product to the customer not repaired. Non-warranted products that are repaired by Transition Networks for a fee will carry a 180-day limited warranty. All warranty claims are subject to the restrictions and conventions set forth by this document.

Transition Networks reserves the right to charge for all testing and shipping incurred, if after testing, a return is classified as "No Problem Found."

THIS WARRANTY IS YOUR ONLY REMEDY. NO OTHER WARRANTIES, SUCH AS FITNESS FOR A PARTICULAR PURPOSE, ARE EXPRESSED OR IMPLIED. TRANSITION NETWORKS IS NOT LIABLE FOR ANY SPECIAL, INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES OR LOSSES, INCLUDING LOSS OF DATA, ARISING FROM ANY CAUSE OR THEORY. AUTHORIZED RESELLERS ARE NOT AUTHORIZED TO EXTEND ANY DIFFERENT WARRANTY ON TRANSITION NETWORKS'S BEHALF.

Customer pays non-compliant return costs

The customer must pay for the non-compliant product(s) return transportation costs to Transition Networks for evaluation of said product(s) for repair or replacement. Transition Networks will pay for the shipping of the repaired or replaced in-warranty product(s) back to the customer *(any and all customs charges, tariffs, or/and taxes are the customer's responsibility).*

Non-warranty repair costs

Before making any non-warranty repair, Transition Networks requires a $200.00 charge plus actual shipping costs to and from the customer. If the repair is greater than $200.00, an estimate is issued to the customer for authorization of the repair. If no authorization is obtained, or the product is deemed not repairable, Transition Networks will retain the $200.00 service charge and return the product to the customer not repaired.

Repaired non-warranty products

Non-warranted products that are repaired by Transition Networks for a fee will carry a 180-day limited warranty. All warranty claims are subject to the restrictions and conventions set forth by this document.

Transition Networks reserves the right to charge for all testing and shipping incurred, if after testing, a return is classified as "No Problem Found."

This warranty is your only remedy

This warranty is your only remedy. No other warranties, such as fitness for a particular purpose, are expressed or implied. Transition Networks is not liable for any special, indirect, incidental or consequential damages or losses, including loss of data, arising from any cause or theory. Authorized resellers cannot extend any different warranty on behalf of transition networks.

Appendix A: Messages & Responses

This Appendix lists the messages that can be displayed at the GUI (graphical user interface) and the CLI (command-line interface) and provides recommended recovery procedures where applicable.

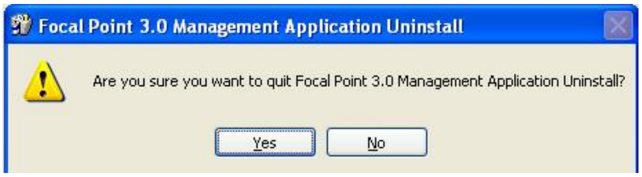
ION System and PS CLI Commands

See the applicable *System CLI Reference* manual for the full set of ION CLI commands and messages.

FP 3.0 Messages and Descriptions

This section lists the messages that can be displayed at the GUI (graphical user interface). Each item in the list includes an explanation of the probable cause/source of the message and suggested corrective actions in response to the message.

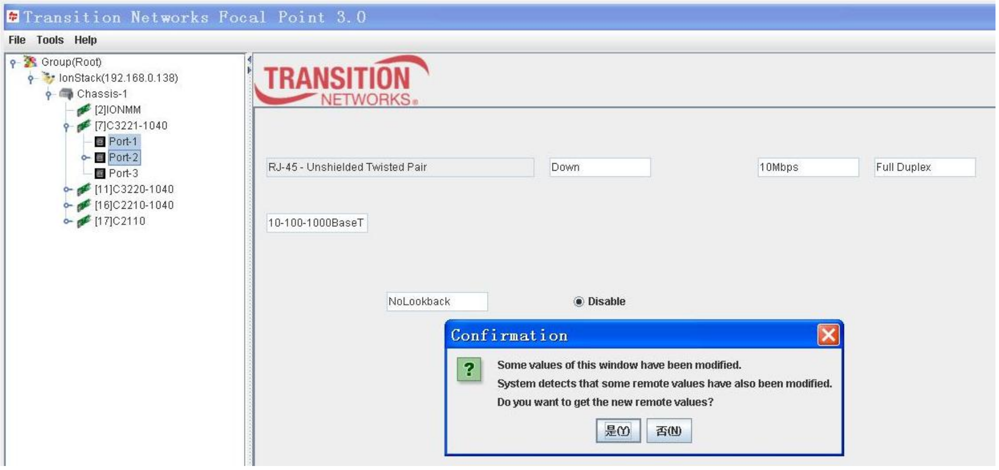
Are you sure you want to quit Focal Point 3.0 Management Application Uninstall?



Are you sure you want to quit Focal Point 3.0 Management Application Uninstall?

You started to uninstall the FP 3.0 Management application. **1)** If you are sure you want to finish the FP 3.0 uninstall, click **OK**. Otherwise, click **No** to quit the FP 3.0 uninstall process. **2)** Refer to the "Uninstall Procedure" on page 50 for more details. **3)** If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Confirmation - Some values of this window have been modified.
System detects that some remote values have also been modified.
Do you want to get remote values now?



RJ-45 - Unshielded Twisted Pair | Down | 10Mbps | Full Duplex

10-100-1000BaseT

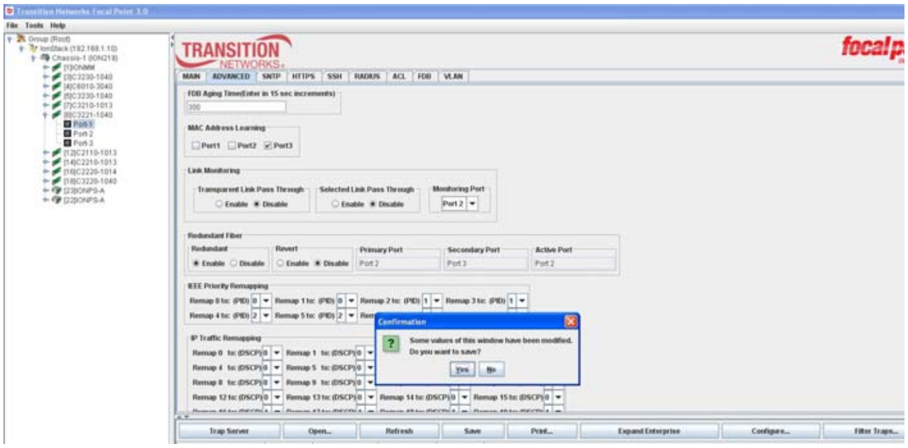
NoLookback ● Disable

Some values of this window have been modified.
System detects that some remote values have also been modified.
Do you want to get the new remote values?

The Local port page which connects the remote device is not shown correctly after FP 3.0 has been running so many hours. For example, after FP3.0 has been running 24 hours, the C3221-1040 Port 2 MAIN tab displays incorrectly with the error message.

1) Click the **Yes** button to clear the confirmation message and start the rediscover process.
2) Delete this stack: the IONMM is re-discovered, and the C3221-1040 Port 2 MAIN page will recover.
3) If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Confirmation - Some values of this window have been modified.
Do you want to save?



FDB Aging Time(Enter in 15 sec increments): 300

MAC Address Learning: □ Port1 □ Port2 ☑ Port3

Link Monitoring
Transparent Link Pass Through: ○ Enable ● Disable
Selected Link Pass Through: ○ Enable ● Disable
Monitoring Port: Port 2

Redundant Fiber
Redundant: ● Enable ○ Disable
Revert: ○ Enable ● Disable
Primary Port: Port 2
Secondary Port: Port 3
Active Port: Port 2

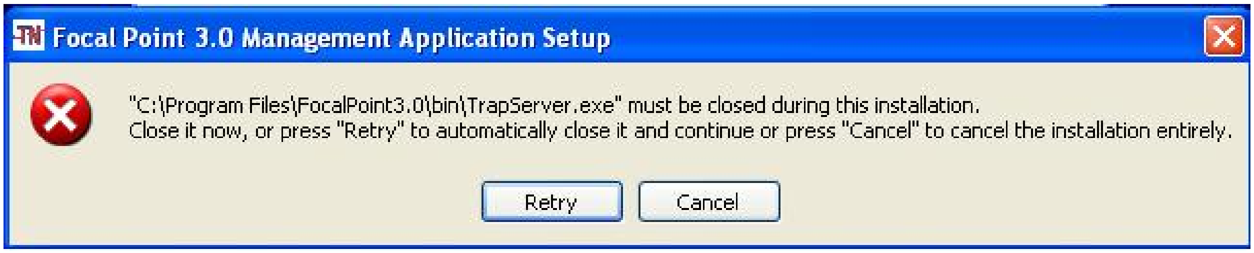
IEEE Priority Remapping
Remap 0 to: (PID) 0 Remap 1 to: (PID) 0 Remap 2 to: (PID) 1 Remap 3 to: (PID) 1
Remap 4 to: (PID) 2 Remap 5 to: (PID) 2

IP Traffic Remapping
Remap 0 to: (DSCP) 0 Remap 1 to: (DSCP) 0
Remap 4 to: (DSCP) 0 Remap 5 to: (DSCP) 0
Remap 8 to: (DSCP) 0 Remap 9 to: (DSCP) 0
Remap 12 to: (DSCP) 0 Remap 13 to: (DSCP) 0 Remap 14 to: (DSCP) 0 Remap 15 to: (DSCP) 0

Confirmation
Some values of this window have been modified.
Do you want to save?
Yes No

Confirmation message only. You made some changes and the clicked another device or port location.
1) Either click the **Yes** button to clear the confirmation message and save the changes, or click the No button to continue without saving the changes that you just made.
2) If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

“C:\Program Files\FocalPoint3.0\binb\TrapServer.exe” must be closed during this installation.
Close it now, or press “Retry” to automatically close it and continue or press “Cancel” to cancel the installation entirely.

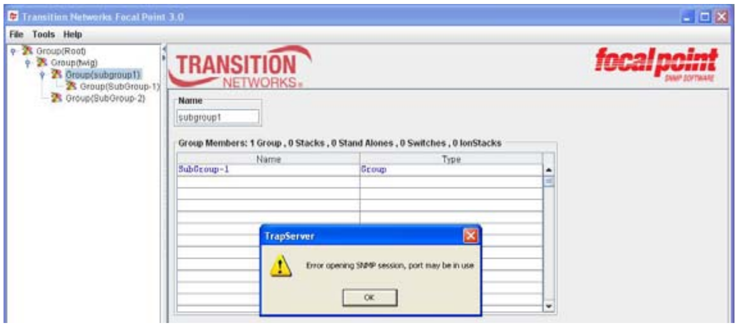

Focal Point 3.0 Management Application Setup

"C:\Program Files\FocalPoint3.0\bin\TrapServer.exe" must be closed during this installation.
Close it now, or press "Retry" to automatically close it and continue or press "Cancel" to cancel the installation entirely.

During FP 3.0 installation, you had a Focal Point 3 application open, which is causing problems with the FP 3.0 install process.

1) Close any running FP 3. 0 application (e.g., TrapServer), or click the **Retry** button to have the FP 3.0 install close the running program for you.
2) to cancel the FP 3.0 install process click the **Cancel** button.
3) If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Error opening SNMP session, port may be in use



Name: subgroup1

Group Members: 1 Group , 0 Stacks , 0 Stand Alones , 0 Switches , 0 IonStacks

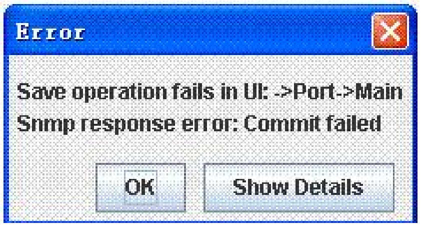
Name	Type
SubGroup-1	Group

Error opening SNMP session, port may be in use

You tried to open the Trap Server application, but another instance of the application may already be open.

1) Click **OK** to clear the TrapServer Error dialog box.
2) Close any previous version of the Trap Server application.
3) Try a different port number.
4) If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

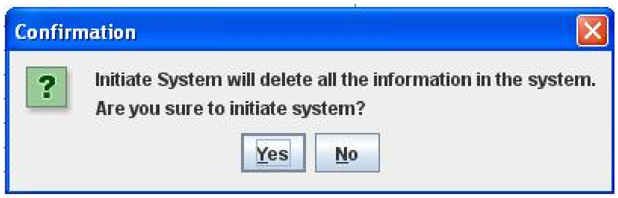
Error - Save operation fails in UI: ->Port->Main Snmp response error: Commit failed



Save operation fails in UI: ->Port->Main
Snmp response error: Commit failed

You tried to Set Port Admin mode from 1000BaseX to 100BaseFX, but the attempt failed.
1) Click the **Show Details** button and look for failure reasons.
2) Click the **OK** button to clear the message.
3) Check the related section of the documentation / helps and retry the operation.
4) Verify that this device supports the attempted operation. If not, switch to a device that does.
5) If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Initiate System will delete all the information in the system. Are you sure to initiate system?

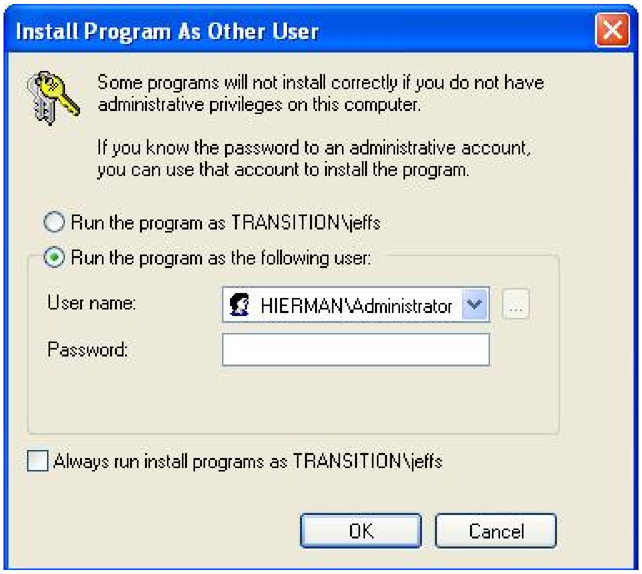

Confirmation

Initiate System will delete all the information in the system.
Are you sure to initiate system?

At the **Tools** dropdown, you selected **Initiate System**.

1) At this confirmation message, either click the **Yes** button to continue the Initiate System process (which deletes all system data) or click the **No** button to end the Initiate System process.
2) If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Install Program as Other User


Install Program As Other User

Some programs will not install correctly if you do not have administrative privileges on this computer.

If you know the password to an administrative account, you can use that account to install the program.

○ Run the program as TRANSITION\jeffs

● Run the program as the following user:

User name: HIERMAN\Administrator

Password:

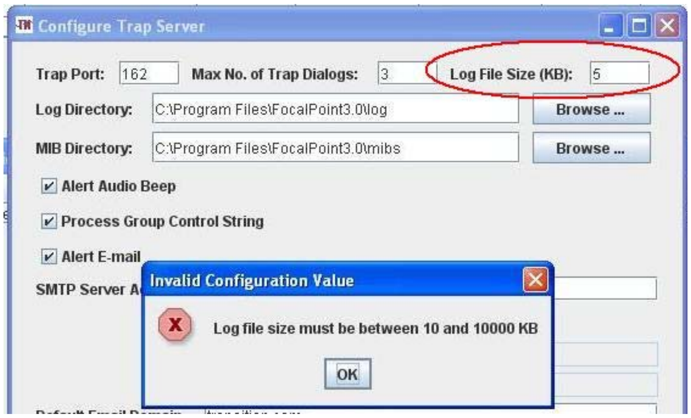
□ Always run install programs as TRANSITION\jeffs

Install message advising of admin privilege issues.

1) Select one of the Run radio button options: either:
  a) the "***Run the program as XXXXXX\user***" radio button if you do not have admin privileges or do not know the password to the admin account.

or:
  b) the "***Run the program as the following user:" xxxxxx\Administrator"*** radio button if you have admin privileges. Enter the password to the admin account.
2) Click the **OK** button.
3) Continue the install process.
4) If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Invalid Configuration File
Log file size must be between 10 and 10000 KB



Configure Trap Server

Trap Port: 162 Max No. of Trap Dialogs: 3 Log File Size (KB): 5

Log Directory: C:\Program Files\FocalPoint3.0\log

MIB Directory: C:\Program Files\FocalPoint3.0\mibs

☑ Alert Audio Beep

☑ Process Group Control String

☑ Alert E-mail

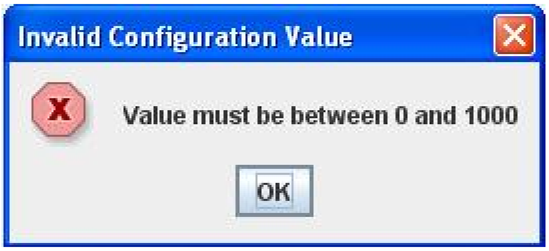
Invalid Configuration Value

Log file size must be between 10 and 10000 KB

At **Configure Traps Server**, you selected a **Log File Size** outside the valid range of 1-10,000 KB.

1) Click the **OK** button to clear the error message.
2) Enter a valid **Log File Polling Interval** in the range of 1 KB to 10,000 KB (10 Mb).
3) If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Invalid Configuration File
Value must be between 0 and 1000



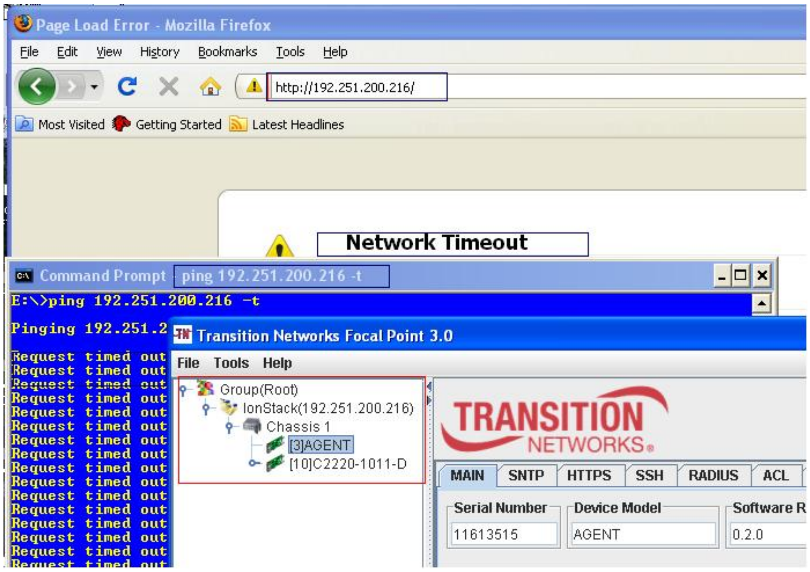
Invalid Configuration Value

Value must be between 0 and 1000

At **Configure Traps Viewer**, you selected a **Log File Polling Interval** outside the valid range of 1-1000.

1) Click the **OK** button to clear the error message.
2) Enter a valid **Log File Polling Interval** in the range of 1-1000.
3) If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Network Timeout


Page Load Error - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://192.251.200.216/
Most Visited Getting Started Latest Headlines
Network Timeout
Command Prompt ping 192.251.200.216 -t
Transition Networks Focal Point 3.0
File Tools Help
Group(Root)
IonStack(192.251.200.216)
Chassis 1
[3]AGENT
[10]C2220-1011-D
TRANSITION NETWORKS
MAIN SNTP HTTPS SSH RADIUS ACL

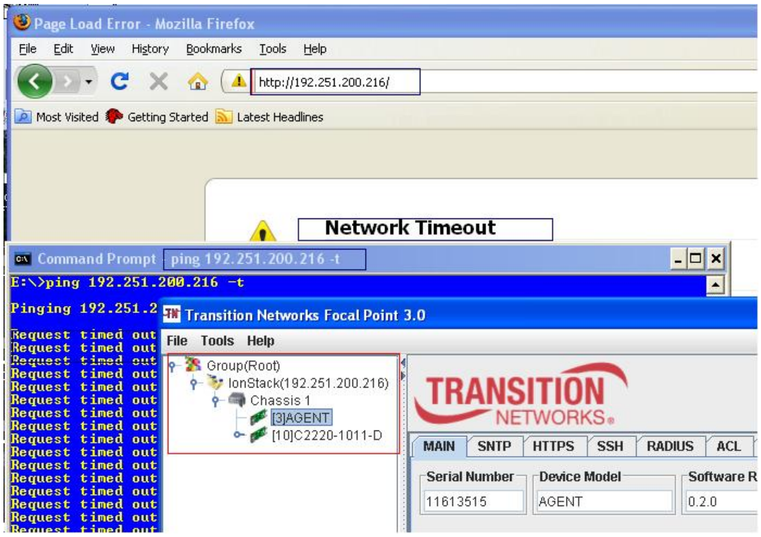
```
E:\>ping 192.251.200.216 -t

Pinging 192.251.2
Request timed out
Request timed out
Request timed out
Request timed out
Request timed out
Request timed out
Request timed out
Request timed out
Request timed out
Request timed out
Request timed out
Request timed out
Request timed out
Request timed out
Request timed out
Request timed out
```

Serial Number: 11613515
Device Model: AGENT
Software R: 0.2.0

The attempted operation (e.g., ping) could not be completed and the web browser network timeout occurred.
1) Refresh the browser screen.
2) Verify the procedure in the related section of the manual or helps.
3) Try the operation again.
4) If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Ping request timed out


Page Load Error - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://192.251.200.216/
Most Visited Getting Started Latest Headlines
Network Timeout
Command Prompt ping 192.251.200.216 -t
Transition Networks Focal Point 3.0
File Tools Help
Group(Root)
IonStack(192.251.200.216)
Chassis 1
[3]AGENT
[10]C2220-1011-D
TRANSITION NETWORKS
MAIN SNTP HTTPS SSH RADIUS ACL

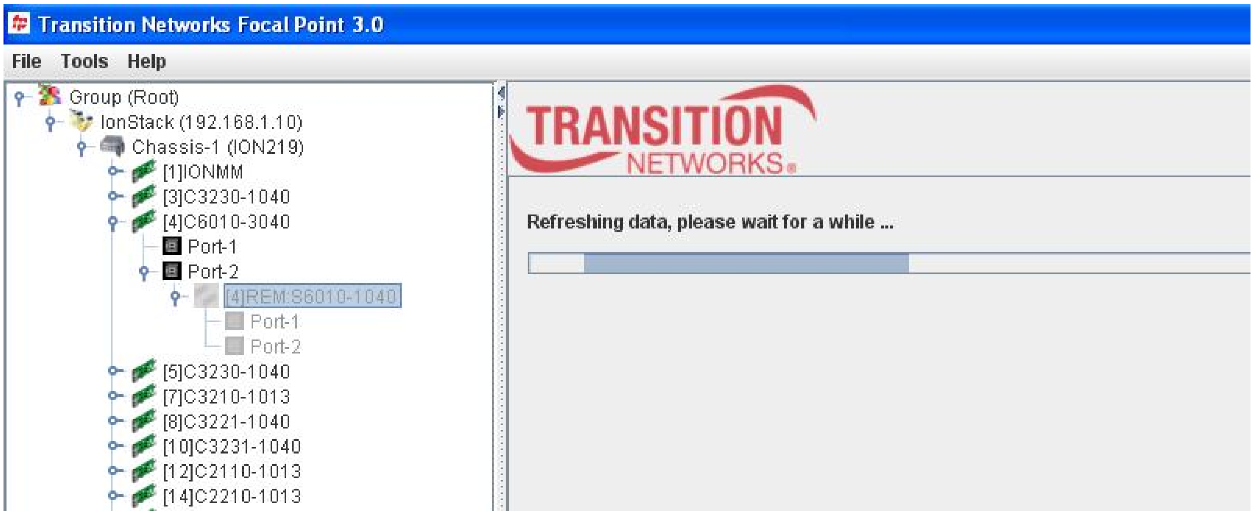
```
E:\>ping 192.251.200.216 -t

Pinging 192.251.2
Request timed out
Request timed out
Request timed out
Request timed out
Request timed out
Request timed out
Request timed out
Request timed out
Request timed out
Request timed out
Request timed out
Request timed out
Request timed out
Request timed out
Request timed out
Request timed out
```

Serial Number: 11613515
Device Model: AGENT
Software R: 0.2.0

The attempted ping operation could not be completed in the time allotted, and a web browser timeout occurred.
1) Refresh the browser screen.
2) Verify the procedure in the related section of the manual or helps.
3) Try the operation again.
4) If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Refreshing data, please wait for a while ...

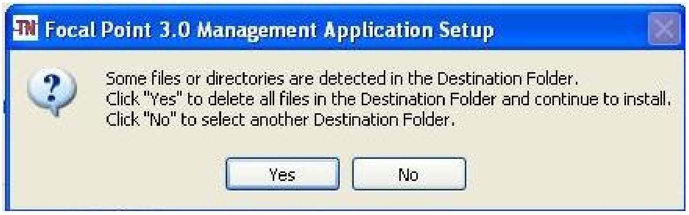


Refreshing data, please wait for a while ...

You clicked on a chassis device, but it was not immediately recognized / discovered.

1) Wait a few seconds for the message to clear and the slot view to re-display.
2) Unplug and re-plug the card in the ION chassis.
3) Cycle power to the device.
4) If a remote device, click the **Refresh** button at the bottom of the local (chassis) device's **MAIN** tab.
5) Check the device's DIP switch settings and jumper settings (e.g., the Hardware/Software Mode jumper on the x6010).
6) Contract and then expand the Group (Root) tree node.
7) Try an alternate connection method (e.g., ION CLI, ION System web interface, or Telnet).
8) Try a different device / port for the intended operation.
9) If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

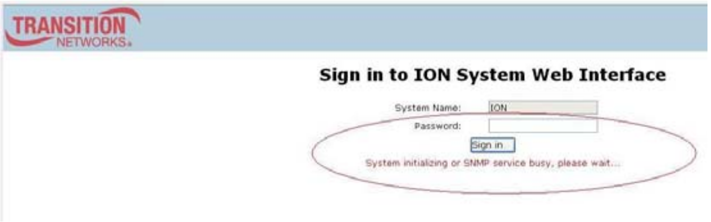
Some files or directories are detected in the Destination Folder.



Some files or directories are detected in the Destination Folder.
Click "Yes" to delete all files in the Destination Folder and continue to install.
Click "No" to select another Destination Folder.

The FP 3.0 Management Application Setup Wizard detected one or more FP directories or files, indicating a previous FP install.
1) Determine if you want to keep the old FP version. If you want to remove all of the existing FP files, click the **Yes** button; if you want to keep the old FP version, click the **No** button.
2) Continue with the "Re-Install Procedure" on page 63.
3) If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

System initializing or SNMP service busy, please wait...



Sign in to ION System Web Interface

System Name: ION

Password:

Sign in

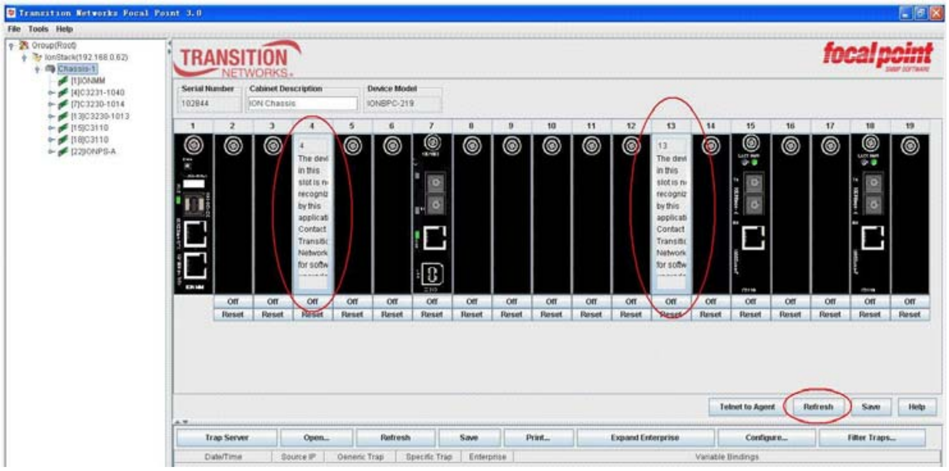
System initializing or SNMP service busy, please wait...

Meaning: The system password was accepted, but the system message displays at the '**Sign in to ION System Web Interface**' screen.

Recovery: Sign in using the correct password. The default password is *private*. Note that the password is case sensitive.

1. Make sure the keyboard's "Caps Lock" is off.
2. Wait one to several minutes (how long depends on the population of the chassis) for the password to be accepted and the login to proceed.
3. Verify the SNMP configuration.
4. Remove the ION Stack from Focal Point and then add it back.
5. Close and then re-open the Focal Point 3.0 application.
6. If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

The device in this slot is not recognized by his application.



Transition Networks Focal Point 3.0

Group(Root)
IonStack(192.168.0.62)
Chassis-1
[1]IONMM
[4]C3231-1040
[7]C3230-1014
[13]C3230-1013
[15]C3110
[18]C3110
[22]IONPS-A

Serial Number: 102844

Cabinet Description: ION Chassis

Device Model: IONBPC-219

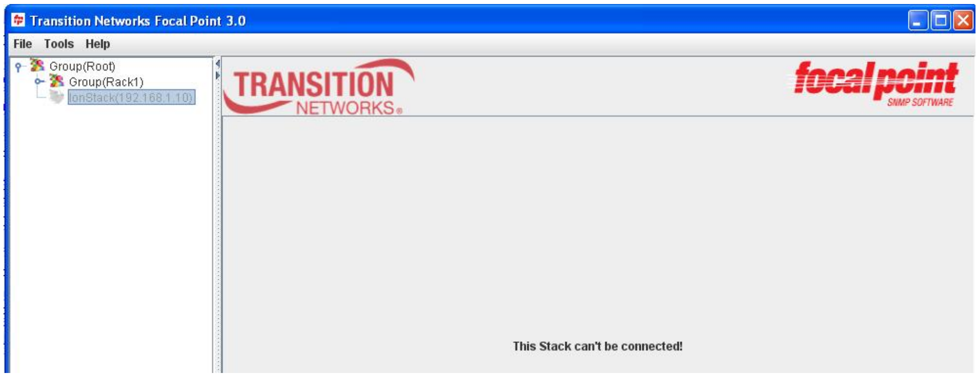
4 The devi in this slot is n recogniz by this applicati Contact Transitic Network for softw

13 The devi in this slot is n recogniz by this applicati Contact Transiti Network for softw

You tried to access a chassis device that is not working or is not yet discovered.

1) Wait a few seconds for the message to clear and the slot view to re-display.
2) Click the **Reset** button below the particular slot.
3) Contract and then expand the stack /chassis tree view.
4) Select **Tools** > **Discover Transition Agents ...**, enter an IP address or range, and then click the **Start** button to re-try the discovery process.
5) If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

This Stack can't be connected!



This Stack can't be connected!

You tried to select a Group or Stack that is not connected / discovered, or you tried to expand the stack, but the stack entry grayed out and the message displayed.

1) Wait a few seconds for the message to clear and the chassis view to re-display.

2) Click the **Refresh** button to try to clear the message.

3) Select another Group from the Stack.

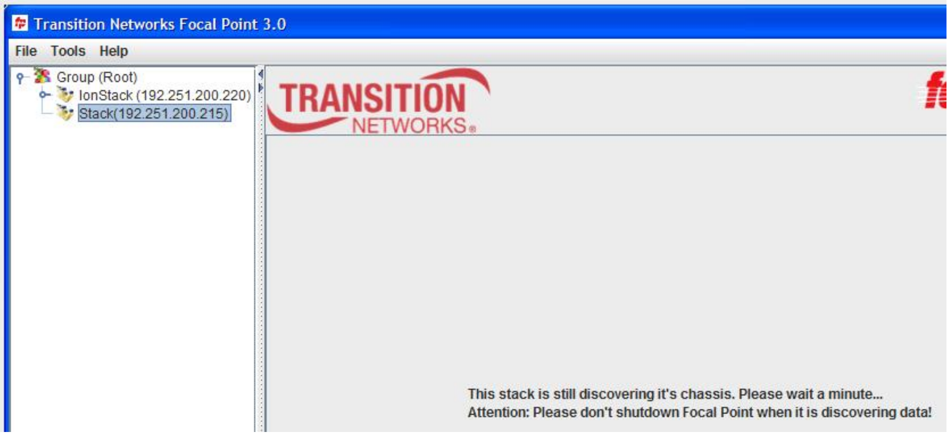
4) Contract and then expand the stack /chassis tree view.

5) Click the **Reset** button below the particular slot.

6) Select **Tools** > **Discover Transition Agents ...**, enter an IP address or range, and then click the **Start** button to re-try the discovery process.

7) If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

This stack is still discovering its chassis. Please wait a minute...
Attention: Please don't shutdown Focal Point when it is discovering data.



This stack is still discovering it's chassis. Please wait a minute...
Attention: Please don't shutdown Focal Point when it is discovering data!

You selected SNMPv1 under **Discovering Transition Agents** > **Config** button before you started to discover Point System chassis (**Tools** > **Discover Transition Agents ...**). The system hung while discovering the PS chassis.

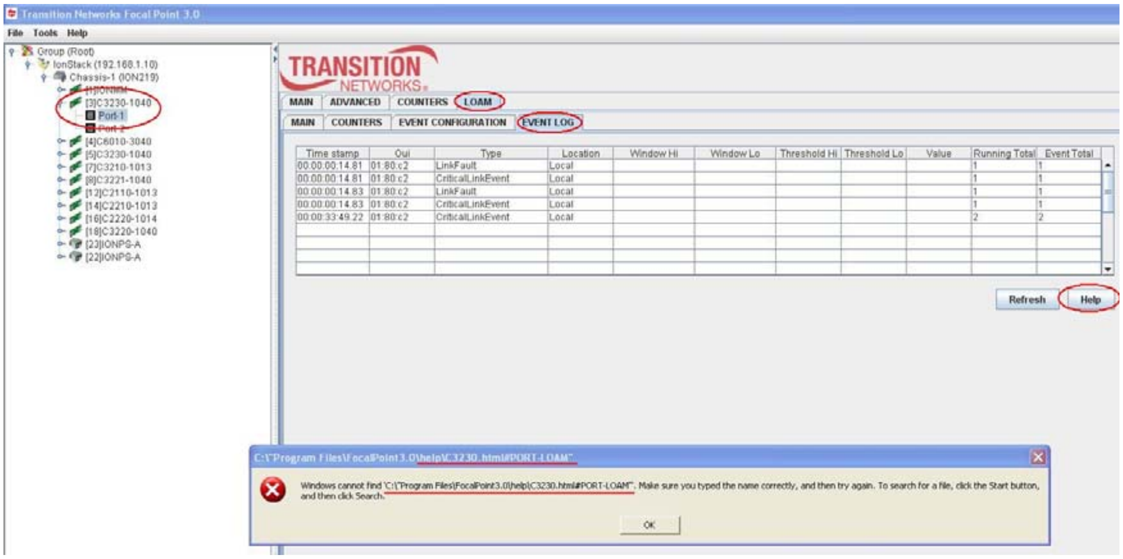
1) Wait 2-3 minutes.

2) Manually collapse and expend the Group (Root) tree.

3) Try selecting SNMPv2 and try the discovery process again.

4) If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Windows cannot find – *'drive\"path\filename"*



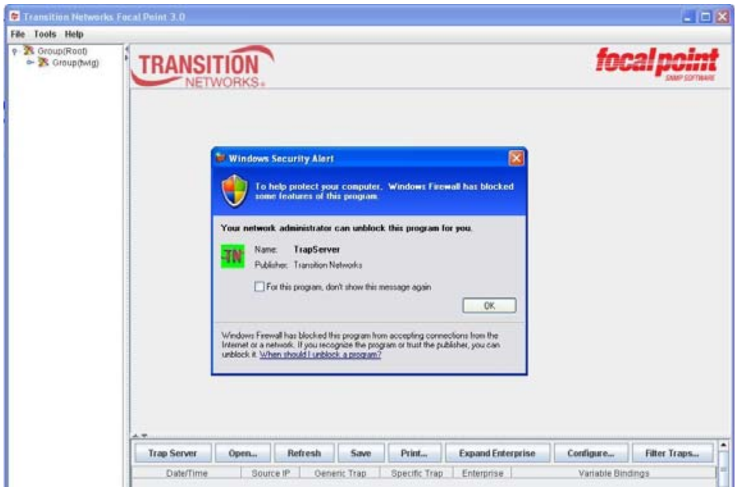
Time stamp	Oui	Type	Location	Window Hi	Window Lo	Threshold Hi	Threshold Lo	Value	Running Total	Event Total
00:00:00:14.81	01:80:c2	LinkFault	Local						1	1
00:00:00:14.81	01:80:c2	CriticalLinkEvent	Local						1	1
00:00:00:14.83	01:80:c2	LinkFault	Local						1	1
00:00:00:14.83	01:80:c2	CriticalLinkEvent	Local						1	1
00:00:33:49.22	01:80:c2	CriticalLinkEvent	Local						2	2

C:\"Program Files\FocalPoint3.0\help\C3230.html#PORT-LOAM"

Windows cannot find 'C:\"Program Files\FocalPoint3.0\help\C3230.html#PORT-LOAM"'. Make sure you typed the name correctly, and then try again. To search for a file, click the Start button, and then click Search.

For example, you clicked the **Help** button, but the required file does not exist, or is not located where expected.
1) Click the **OK** button to clear the message.
2) Verify that the default install location was used, and that the listed file/location exists.
3) Retry the operation.
4) If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

Windows Security Alert – To help protect your computer, Windows Firewall has blocked some features of this program for you.



To help protect your computer, Windows Firewall has blocked some features of this program.

Your network administrator can unblock this program for you.

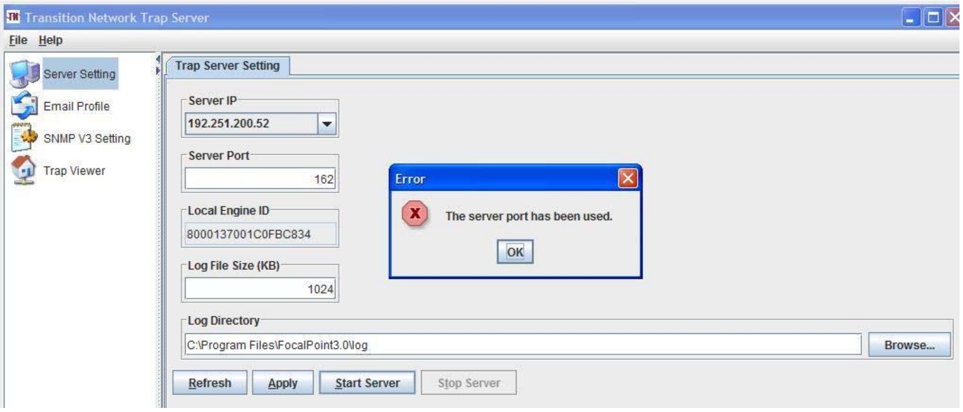
Name: TrapServer
Publisher: Transition Networks

☐ For this program, don't show this message again

Windows Firewall has blocked this program from accepting connections from the Internet or a network. If you recognize the program or trust the publisher, you can unblock it. When should I unblock a program?

1) Check your Windows Firewall settings.
2) Check the "For this program, don't show this message again" checkbox.
3) Click the **OK** button to clear the Windows Security Alert message and continue operation.
4) If the problem persists, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.

The server port has been used.



Server IP: 192.251.200.52
Server Port: 162
Local Engine ID: 8000137001C0FBC834
Log File Size (KB): 1024
Log Directory: C:\Program Files\FocalPoint3.0\log

The server port has been used.

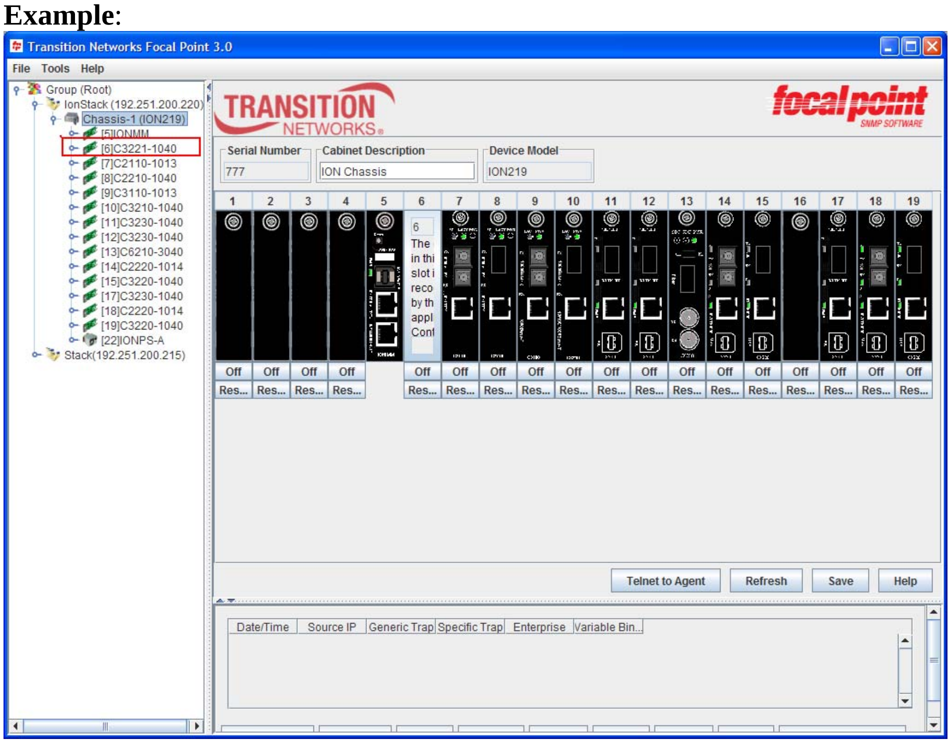
At **Trap Server** > **Server Setting** in the **Server Port** field you entered a port number that is not currently available.

1) Click the **OK** button to clear the error message.
2) Enter an available (unused) port number.
3) Continue operation.

The card in this slot is not recognized by the application.

Description: Power off 2 cards slot 6_C3221 and slot 7_C2110. Then power on both slots 6 & 7. No longer recognize the card C3221 in slot 6 after power on/off test.

Example:



Group (Root)
IonStack (192.251.200.220)
Chassis-1 (ION219)
[5]IONMM
[6]C3221-1040
[7]C2110-1013
[8]C2210-1040
[9]C3110-1013
[10]C3210-1040
[11]C3230-1040
[12]C3230-1040
[13]C6210-3040
[14]C2220-1014
[15]C3220-1040
[17]C3230-1040
[18]C2220-1014
[19]C3220-1040
[22]IONPS-A
Stack(192.251.200.215)

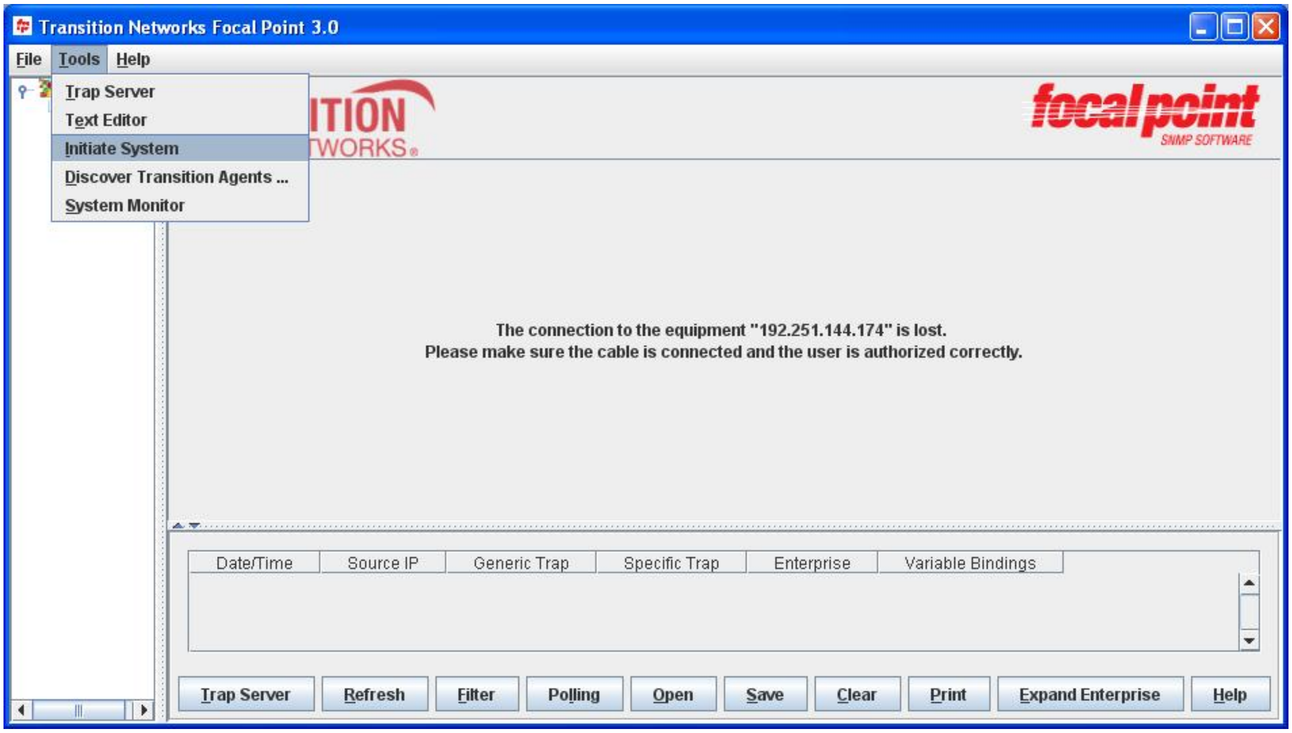
Serial Number: 777
Cabinet Description: ION Chassis
Device Model: ION219

6
The
in thi
slot i
reco
by th
appl
Cont

Recovery:

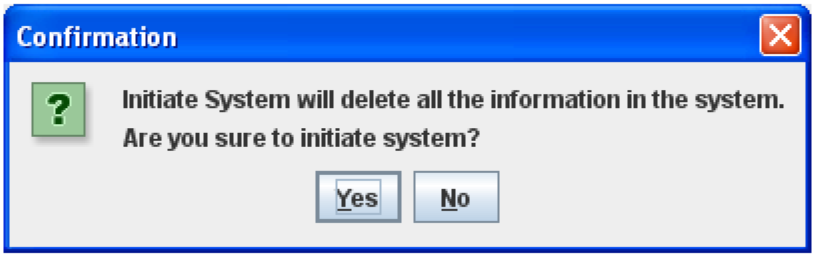
1. Make sure you have the latest firmware for all cards. Upgrade to a more current version if available.
2. Continue operation.
3. If the problem persists, contact Technical Support.

Message: **The connection to the equipment "x.x.x.x" is lost. Please make sure the cable is connected and the user is authorized correctly.**



The connection to the equipment "192.251.144.174" is lost.
Please make sure the cable is connected and the user is authorized correctly.

Meaning: A connection problem occurred.
Recovery:
1. Make sure the cable is properly connected.
2. Make sure the user is authorized correctly.
3. Use the **Tools** > **Initiate System** menu path. A confirmation message displays.



Initiate System will delete all the information in the system.
Are you sure to initiate system?

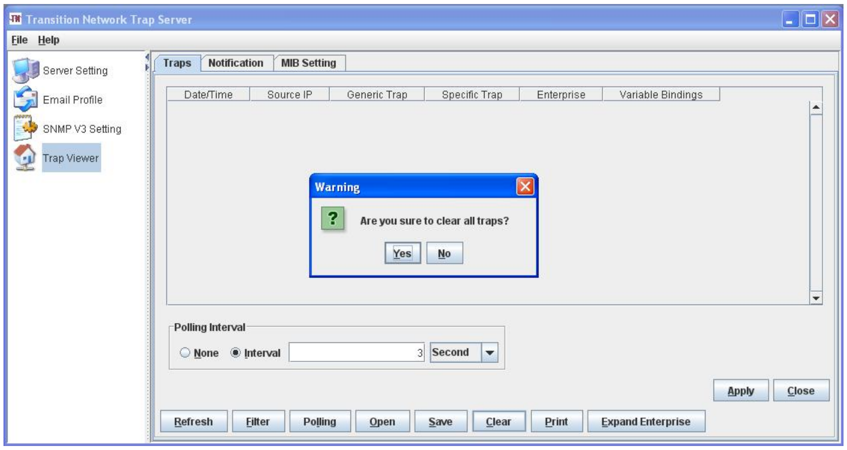
4. Click **Yes**. The message clears.
5. Perform the **Tools** > **Discover Transition Agents ...** menu path again.

Trap Server Messages

This section lists the messages that can be displayed using the FP3.0 Trap Server application.

Message: **Are you sure to clear all traps?**

Meaning: At **Trap Server** > **Trap Viewer** > **Traps**, you clicked the **Clear** button.



Date/Time	Source IP	Generic Trap	Specific Trap	Enterprise	Variable Bindings

Warning

Are you sure to clear all traps?

Yes No

Polling Interval

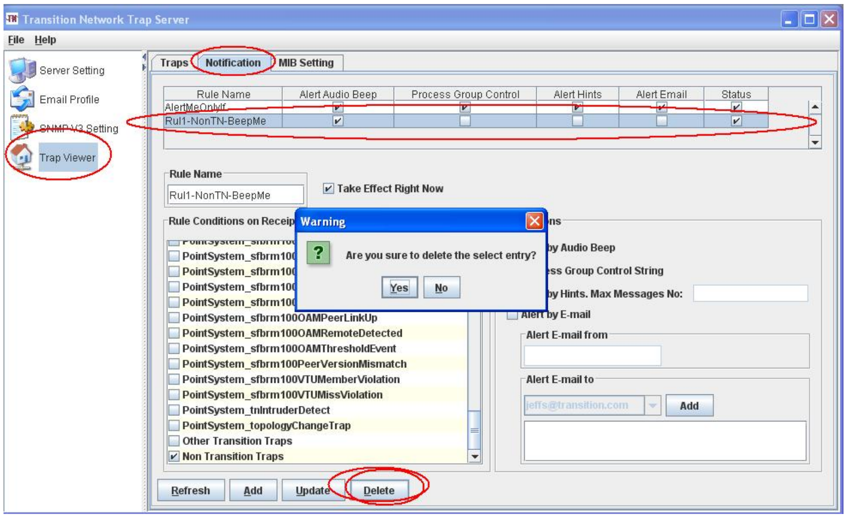
○ None ● Interval 3 Second

Recovery:

1. If you are sure you want to clear the traps, click the **Yes** button. Otherwise click **No**.
2. See "Configure Notification" on page 48 for more information.

Message: **Are you sure to clear the selected entry?**

Meaning: At **Trap Server** > **Trap Viewer** > **Notification**, you clicked the **Delete** button.



Rule Name	Alert Audio Beep	Process Group Control	Alert Hints	Alert Email	Status
AlertMeOnlyIf	☑	☑	☑	☑	☑
Rul1-NonTN-BeepMe	☑	□	□	□	☑

Rule Name: Rul1-NonTN-BeepMe

☑ Take Effect Right Now

Rule Conditions on Receip

□ PointSystem_sfbrm10
□ PointSystem_sfbrm10
□ PointSystem_sfbrm10
□ PointSystem_sfbrm10
□ PointSystem_sfbrm10
□ PointSystem_sfbrm100OAMPeerLinkUp
□ PointSystem_sfbrm100OAMRemoteDetected
□ PointSystem_sfbrm100OAMThresholdEvent
□ PointSystem_sfbrm100PeerVersionMismatch
□ PointSystem_sfbrm100VTUMemberViolation
□ PointSystem_sfbrm100VTUMissViolation
□ PointSystem_tnIntruderDetect
□ PointSystem_topologyChangeTrap
□ Other Transition Traps
☑ Non Transition Traps

Warning

Are you sure to delete the select entry?

Yes No

ns

by Audio Beep

ss Group Control String

by Hints. Max Messages No:

□ Alert by E-mail

Alert E-mail from

Alert E-mail to: jeffs@transition.com Add

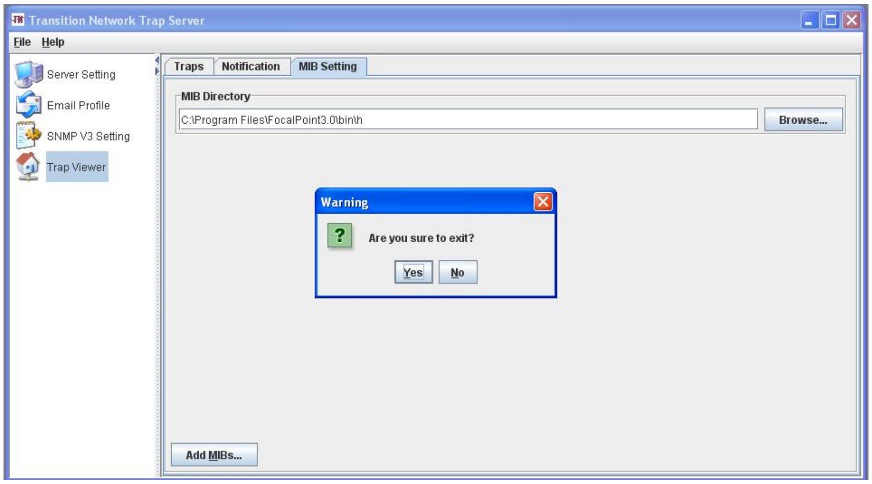
Recovery:

1. If you are sure you want to delete this entry, click the **Yes** button. Otherwise click **No**.

2. See "Configure Notification" on page 52.

Message: **Are you sure to exit?**

Meaning: At the **Trap Server** > **Trap Viewer** > **MIB Setting** tab, you clicked the **File** > **Exit** path.



C:\Program Files\FocalPoint3.0\bin\h

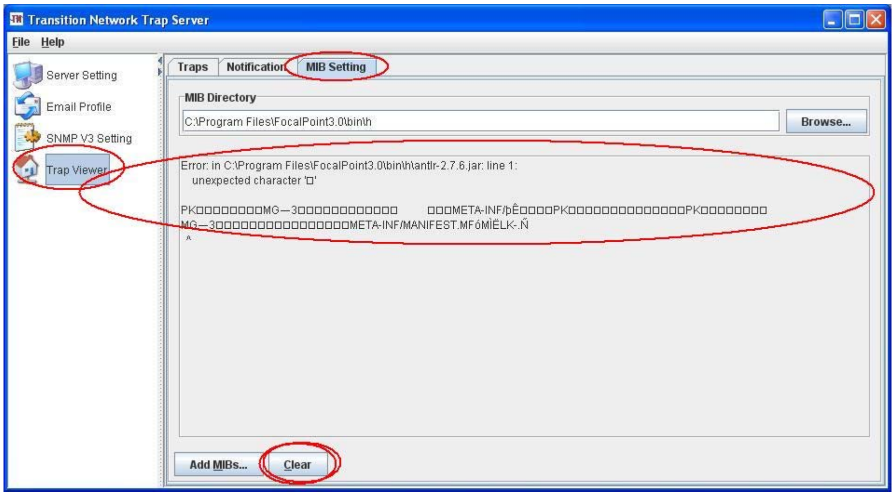
Are you sure to exit?

Recovery:

1. If you are sure you want to exit, click the **Yes** button. Otherwise click **No**.
2. See Configure MIB Setting on page 19.

Message: **Error in C:\Program Files\FocalPoint3.\xxxx0 - unexpected character "y'**

Meaning: At **Trap Server** > **Trap Viewer** > **MIB Setting** tab, you selected a MIB Directory and clicked "**Add MIBs...**", but the entry failed.



C:\Program Files\FocalPoint3.0\bin\h

```
Error: in C:\Program Files\FocalPoint3.0\bin\h\antlr-2.7.6.jar: line 1:
   unexpected character '□'

PK□□□□□□□□□MG—3□□□□□□□□□□□□□       □□□META-INF/þÊ□□□□PK□□□□□□□□□□□□□□□PK□□□□□□□□□
MG—3□□□□□□□□□□□□□□□□□□META-INF/MANIFEST.MFóMÌËLK-.Ñ
 ^
```

Recovery:

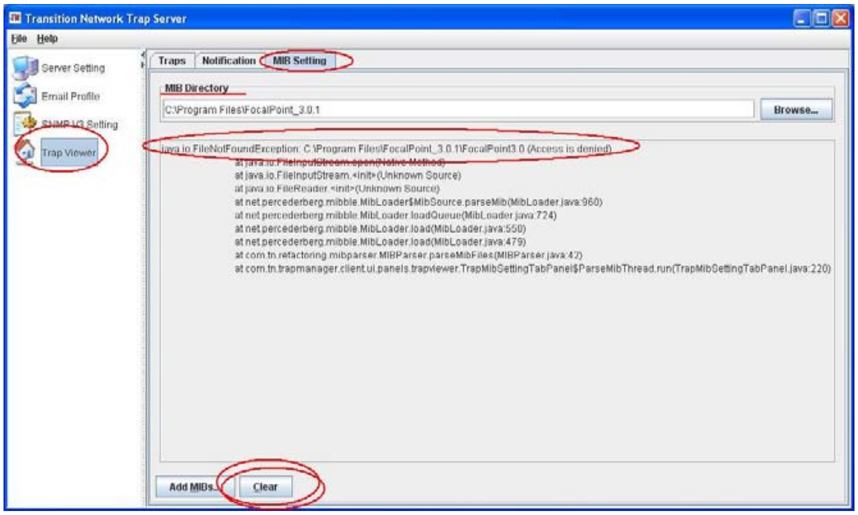
1. Click the **Clear** button to clear the Error message.
2. Browse to and select an existing, valid MIB.
3. Click the **Add MIBs...** button
4. See Configure MIB Setting on page 19.

Message: **File Not Found Exception - Trap Viewer - MIB Setting tab**

java.io.FileNotFoundException: C:\Program Files\FocalPoint_3.0.1\FocalPoint3.0 (Access is Denied)

Meaning: At **Trap Server** > **Trap Viewer** > **MIB Setting** tab, you selected a MIB Directory and clicked "**Add MIBs...**", but the entry failed.

Example:



MIB Directory: C:\Program Files\FocalPoint_3.0.1

```
java.io.FileNotFoundException: C:\Program Files\FocalPoint_3.0.1\FocalPoint3.0 (Access is denied)
        at java.io.FileInputStream.open(Native Method)
        at java.io.FileInputStream.<init>(Unknown Source)
        at java.io.FileReader.<init>(Unknown Source)
        at net.percederberg.mibble.MibLoader$MibSource.parseMib(MibLoader.java:960)
        at net.percederberg.mibble.MibLoader.loadQueue(MibLoader.java:724)
        at net.percederberg.mibble.MibLoader.load(MibLoader.java:550)
        at net.percederberg.mibble.MibLoader.load(MibLoader.java:479)
        at com.tn.refactoring.mibparser.MIBParser.parseMibFiles(MIBParser.java:42)
        at com.tn.trapmanager.client.ui.panels.trapviewer.TrapMibSettingTabPanel$ParseMibThread.run(TrapMibSettingTabPanel.java:220)
```

Recovery:

1. Click the **Clear** button to clear the Error message.

2. Browse to and select an existing, valid MIB.

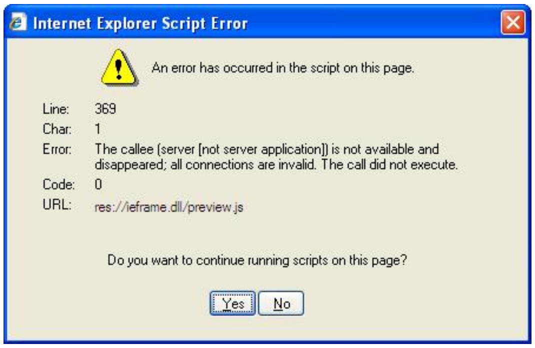
3. Click the **Add MIBs...** button

4. See 'Configure MIB Setting' on page 19.

Message: **Internet Explorer Script Error - An error occurred in the script on this page.**

Meaning: A web browser detected an error on a particular web page.

Example:



An error has occurred in the script on this page.

Line: 369
Char: 1
Error: The callee (server [not server application]) is not available and disappeared; all connections are invalid. The call did not execute.
Code: 0
URL: res://ieframe.dll/preview.js

Do you want to continue running scripts on this page?

Recovery:

1. To continue running the script, click **Yes**; to stop, click **No**.

2. Verify the FP 3.0 operation; see the related section of this document.

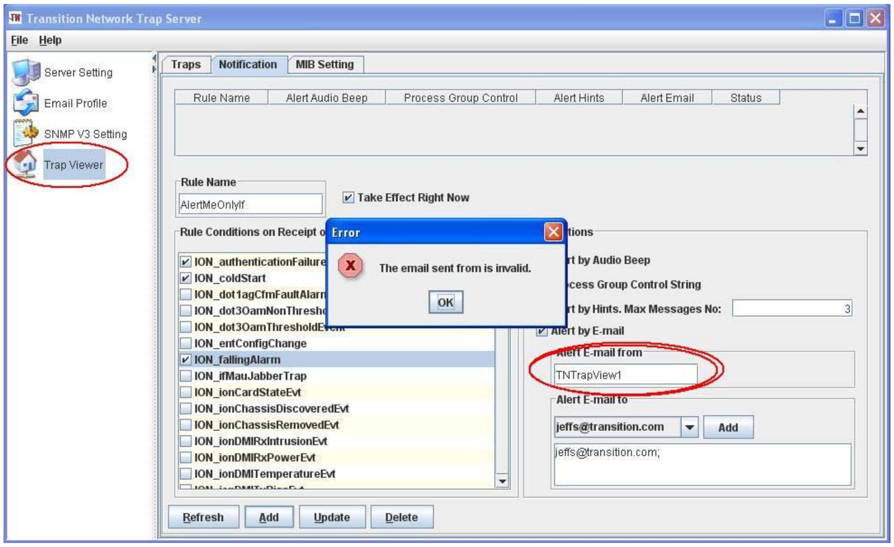
3. Check the OS and web browser vendor's website (e.g., for Windows: http://support.microsoft.com/kb/308260),
for Firefox: http://support.mozilla.com/en-US/kb/Warning%20Unresponsive%20script,
for Chrome http://www.google.com/chrome/intl/en/webmasters-faq.html)

4. If the problem recurs, note the FP3.0 page and contact TN support.

Message: **Error - The email sent from is invalid**

Meaning: At **Trap Server** > **Trap Viewer** > **Notification** tab, you entered an invalid email address.

Example:



Error

The email sent from is invalid.

OK

Rule Name: AlertMeOnlyIf

☑ Take Effect Right Now

Alert by Hints. Max Messages No: 3

☑ Alert by E-mail

Alert E-mail from: TNTrapView1

Alert E-mail to: jeffs@transition.com

jeffs@transition.com;

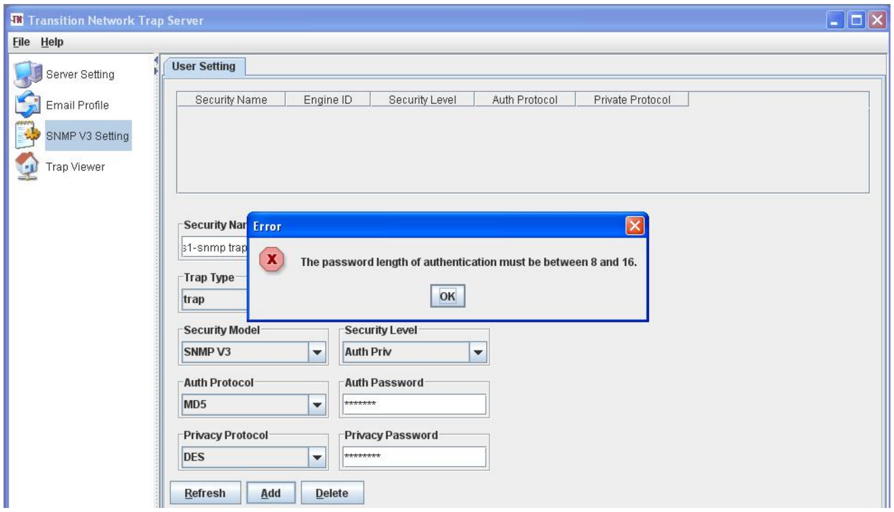
Recovery:

1. Click the **OK** button to clear the Error message.
2. Enter a valid email address in the format **xxxx@yyyy.zz**z.
3. See "Configure Notification" on page 52 for more information.

Message: **The password length of authentication must be between 8 and 16.**

Meaning: You entered too many or too few password characters.

Example:



Error

The password length of authentication must be between 8 and 16.

OK

Security Name: s1-snmp trap

Trap Type: trap

Security Model: SNMP V3

Security Level: Auth Priv

Auth Protocol: MD5

Auth Password: *******

Privacy Protocol: DES

Privacy Password: ********

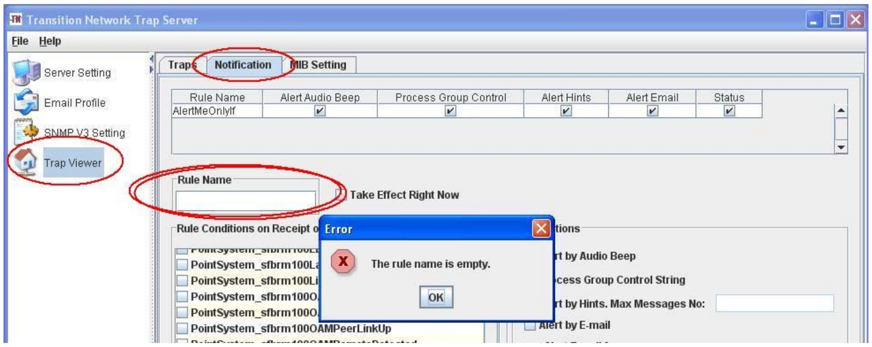
Recovery:

1. Click the **OK** button to clear the Error message.
2. Enter a valid password of 8-16 characters.
3. See "Configure Notification" on page 52 for more information.

Message: **Error - The rule name is empty.**

Meaning: At **Trap Server** > **Trap Viewer** > **Notification** tab, you did not enter a **Rule Name**.

Example:



Rule Name	Alert Audio Beep	Process Group Control	Alert Hints	Alert Email	Status
AlertMeOnlyIf	☑	☑	☑	☑	☑

□ PointSystem_sfbrm100La
□ PointSystem_sfbrm100Li
□ PointSystem_sfbrm1000
□ PointSystem_sfbrm1000
□ PointSystem_sfbrm100OAMPeerLinkUp

Error

The rule name is empty.

Recovery:

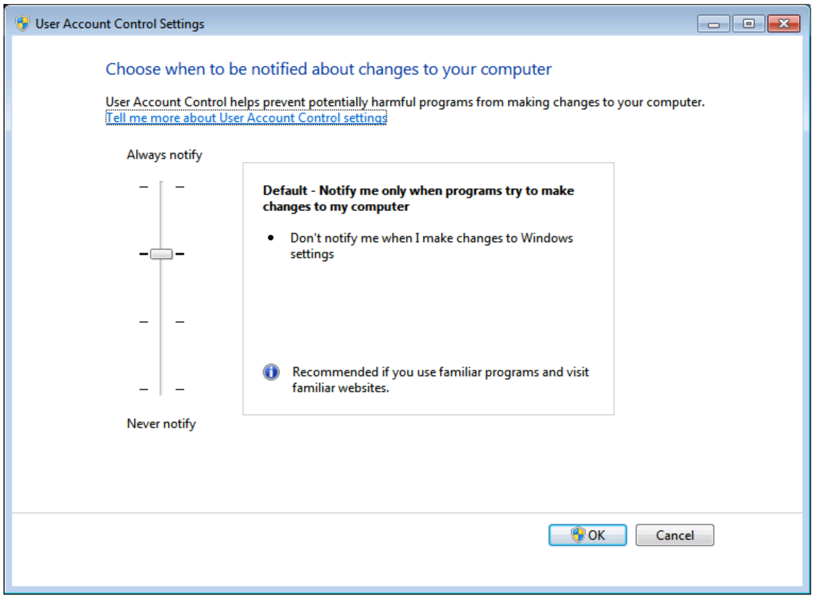
1. Click the **OK** button to clear the Error message.

2. Enter a valid Rule Name. See "Configure Notification" on page 52.

Message: **Do you want to allow this following program to make changes to this computer?**

Meaning: **User Account Control Settings ON**

Example:



Choose when to be notified about changes to your computer

User Account Control helps prevent potentially harmful programs from making changes to your computer.
Tell me more about User Account Control settings

Default - Notify me only when programs try to make changes to my computer

- Don't notify me when I make changes to Windows settings

Recommended if you use familiar programs and visit familiar websites.

Recovery:

In Microsoft Windows 7, turn off UAC (User Account Control), or from Windows **Task Manager** > **Processes Properties** > **Compatibility**, set the check mark on privilege level to run this program as an Administrator. With this modification, now the window pops up to confirm "*do you want to allow this following program to make changes to this computer*" every time launching FP. Click "**OK**", and then FP will launch without issue.

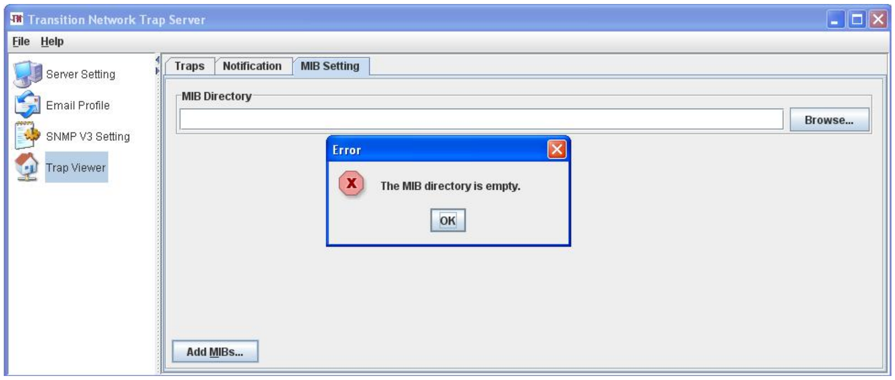
To turn off UAC in MS Vista:

1. Click **Start**, and then click **Control** Panel.
2. In Control Panel, click **User Accounts**.
3. In the User Accounts window, click **User Accounts**.
4. In the User Accounts tasks window, click **Turn User Account Contro**l on or off.
5. If UAC is currently configured in Admin Approval Mode, the UAC message appears. Click **Continue**.

6. Clear the Use User Account Control (UAC) to help protect your computer check box, and then click **OK**.
7. Click **Restart Now** to apply the change right away, or click **Restart Later** and close the User Accounts tasks window.

Message: **The MIB directory is empty.**

Meaning: At **Trap Server** > **Trap Viewer** > **MIB Setting** you clicked the **Add MIBS ...** button without a MIB selected from the **MIB Directory** field.



The MIB directory is empty.

Recovery:

1. Click the **OK** button to clear the Error dialog.

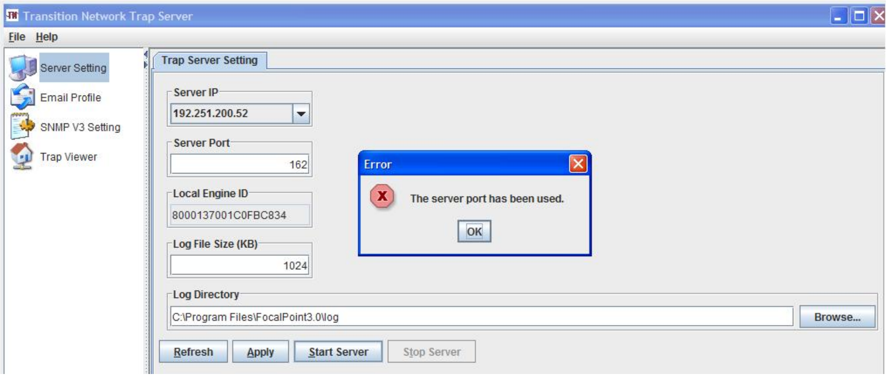
2. Browse to and select a valid MIB (e.g., with a .bin file extension).

3. Click the **Add MIBS ...** button.

4. See 'Configure MIB Setting' on page 19.

Message: **The server port has been used.**

Meaning: If a UDP port has been occupied by another OS process, SNMP can not set up a UDP socket on that port to receive traps.



Server IP: 192.251.200.52

Server Port: 162

Local Engine ID: 8000137001C0FBC834

Log File Size (KB): 1024

Log Directory: C:\Program Files\FocalPoint3.0\log

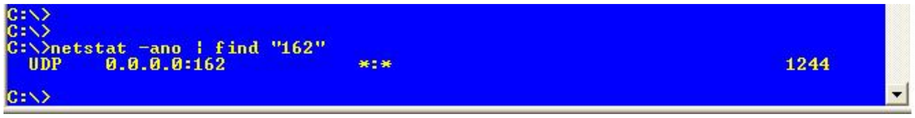
The server port has been used.

Recovery:

1. Click the **OK** button to clear the Error dialog.

2. Either stop the process or use another "free" port.

3. To check if a port has been used by a process, try the command **netstat -ano | find "162"** (where 162 is the port you are checking). For example:



```
C:\>
C:\>
C:\>netstat -ano | find "162"
  UDP    0.0.0.0:162            *:*                                    1244

C:\>
```

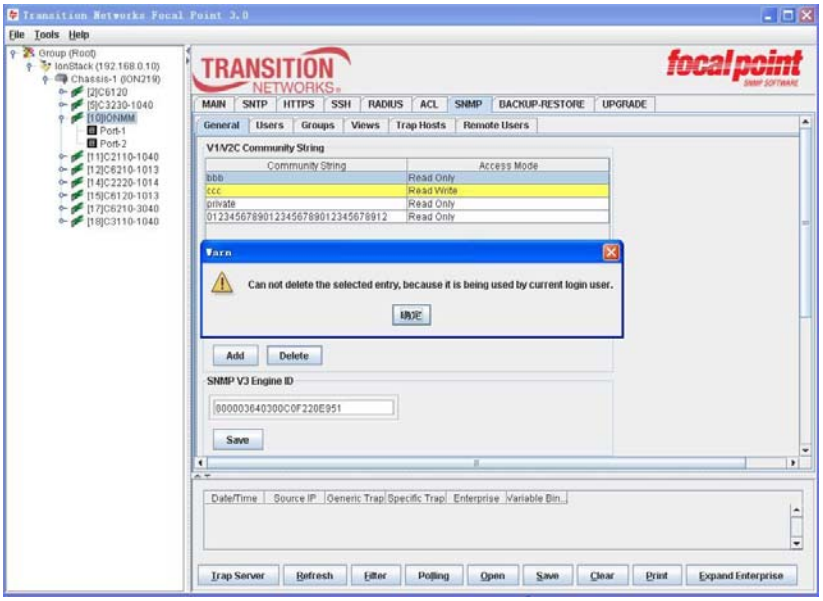
4. See "1. Trap Server Setup' on page 42.

Message: **Can not delete the selected entry, because it is being used by current login user.**

Message: **The connection to the equipment "192.168.0.10" is lost. Please make sure the cable is connected and the user is authorized correctly.**

Meaning: You started to delete the current SNMP login community string; if you delete it, FP3.0 will lose connection. Deleting the current login community string in FP is not allowed.

Example: Message - **IONMM** > **SNMP** - *Can not delete the selected entry, because it is being used by current login user*.


Transition Networks Focal Point 3.0
File Tools Help
Group (Root)
IonStack (192.168.0.10)
Chassis-1 (ION219)
[2]C6120
[5]C3230-1040
[10]IONMM
Port-1
Port-2
[11]C2110-1040
[12]C6210-1013
[14]C2220-1014
[15]C6120-1013
[17]C6210-3040
[18]C3110-1040
TRANSITION NETWORKS
focal point SNMP SOFTWARE
MAIN SNTP HTTPS SSH RADIUS ACL SNMP BACKUP-RESTORE UPGRADE
General Users Groups Views Trap Hosts Remote Users
Add Delete
Save
Date/Time Source IP Generic Trap Specific Trap Enterprise Variable Bin...
Trap Server Refresh Filter Polling Open Save Clear Print Expand Enterprise

V1/V2C Community String

Community String	Access Mode
bbb	Read Only
ccc	Read Write
private	Read Only
01234567890123456789012345678912	Read Only

Warn

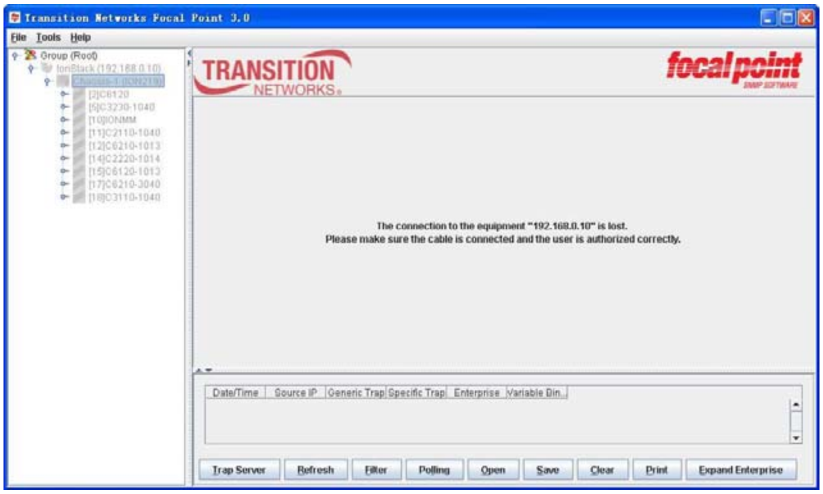
Can not delete the selected entry, because it is being used by current login user.

确定

SNMP V3 Engine ID: 800003640300C0F220E951

Meaning: If the login user is removed from another place, e.g. the Web interface, the left tree nodes will display gray and the right panel will display the message but nothing else.

Example: Message - Point System - *The connection to the equipment "192.168.0.10" is lost. Please make sure the cable is connected and the user is authorized correctly***.**


Transition Networks Focal Point 3.0
File Tools Help
Group (Root)
IonStack (192.168.0.10)
Chassis-1 (ION219)
[2]C6120
[5]C3230-1040
[10]IONMM
[11]C2110-1040
[12]C6210-1013
[14]C2220-1014
[15]C6120-1013
[17]C6210-3040
[18]C3110-1040
TRANSITION NETWORKS
focal point SNMP SOFTWARE
Date/Time Source IP Generic Trap Specific Trap Enterprise Variable Bin...
Trap Server Refresh Filter Polling Open Save Clear Print Expand Enterprise

The connection to the equipment "192.168.0.10" is lost.
Please make sure the cable is connected and the user is authorized correctly.

Recovery:

1. Select another entry or select another function.
2. Make sure the cable is connected and the user is authorized correctly.
3. Try the **Tools** > **Initiate System** menu path to clear the error condition and retry the operation.
4. If possible, log out the current login user.
5. See "1. Trap Server Setup' on page 42.

Problem: **Your attempt to add a new SNMP local user failed.** A new SNMP local user only can be created by cloning the FP login user, and setting its security level to be equal or lower than the login user's level.

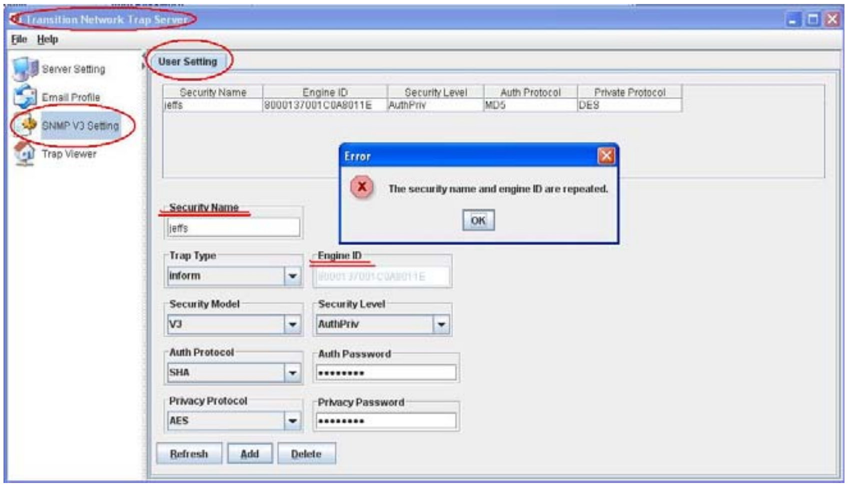
Recovery:

1. Make sure the new SNMP local user being created is properly configured. Refer to 'SNMP V3 User Settings' on page 45.
2. Verify the ION system or Point System SNMP configuration settings. Refer to the related manual for additional information.

Message: **The security name and engine ID are repeated**

Meaning: At **Trap Server** > **SNMP V3 Setting** > **User Setting** you tried to add a new user setting with a Security Name and Engine ID that match an existing user.

Example:



Security Name	Engine ID	Security Level	Auth Protocol	Private Protocol
jeffs	8000137001C0A8011E	AuthPriv	MD5	DES

The security name and engine ID are repeated.

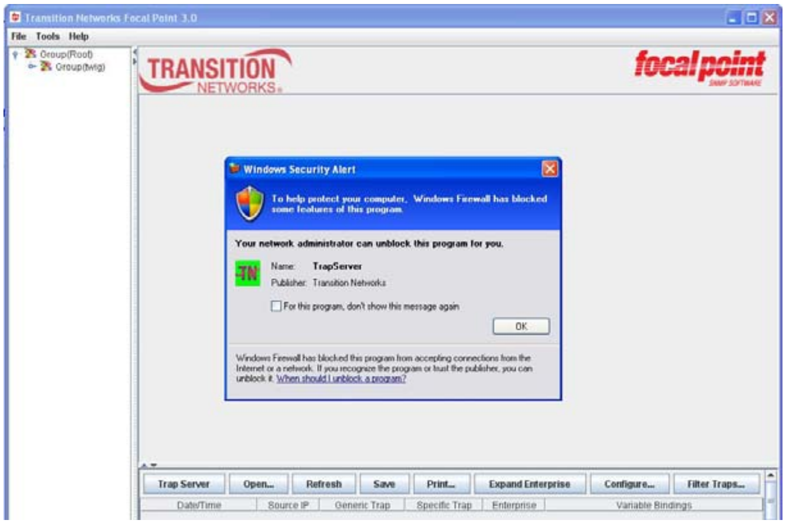
Security Name: jeffs
Trap Type: inform
Engine ID: 8000137001C0A8011E
Security Model: V3
Security Level: AuthPriv
Auth Protocol: SHA
Auth Password: ********
Privacy Protocol: AES
Privacy Password: ********

Recovery:

1. Click the **OK** button to clear the Error message.
2. Enter a unique Security Name and Engine ID.
3. Click the **Add** button.
4. See 'SNMP V3 User Settings' on page 45.

Message: **Windows Security Alert**

Meaning: Windows Firewall has blocked some features of this program



Windows Security Alert

To help protect your computer, Windows Firewall has blocked some features of this program.

Your network administrator can unblock this program for you.

Name: TrapServer
Publisher: Transition Networks

□ For this program, don't show this message again

Windows Firewall has blocked this program from accepting connections from the Internet or a network. If you recognize the program or trust the publisher, you can unblock it. When should I unblock a program?

Recovery:

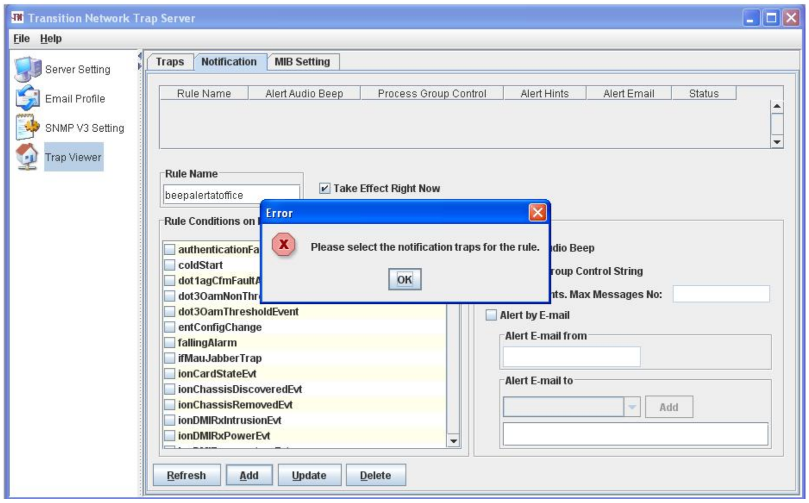
1. This can be resolved in either of two ways:

a) Select **Start** -> **Control Panel** -> **Security Center**. Then click on the "**Windows Firewall**" option, click on "**Recommendations**", and, then check the "**I have a firewall solution that I'll monitor myself**" checkbox. Verify that this is what you really want to do and the Windows Security Alert message will not display again. **<u>or</u>**:

b) If you still want to have the Windows firewall running even though it's redundant, just set it to "loose monitoring" for some additional system security.

Message: **Please select the notification traps for the rule.**

Meaning: At the **Trap Server** > **Trap Viewer** > **Notification** tab menu path you clicked the **Add** button to create a Rule without first selecting one or more Rule Conditions.



Error

Please select the notification traps for the rule.

Rule Name: beepalertatoffice

☑ Take Effect Right Now

Recovery:

1. Click the **OK** button to clear the Error message.

2. Select one or more Rule Conditions in the **Rule Conditions on Receipt of ...** section.

3. Click the **Add** button.

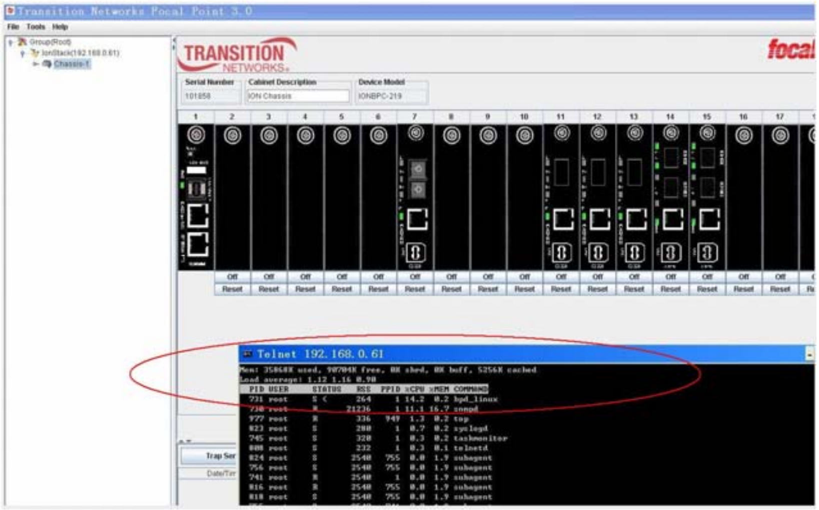
4. See 'Configure Notifications' on page 52.

Problem: **CPU Utilization High**

IONMM card %CPU up to 98%

Meaning: Focal Point, used as an SNMP manager connecting with the IONMM, will consume resources on agent side.
The more Focal Point clients connected, the more resources are consumed. If you unplug one/more card(s) from the chassis or cut off the remote card from local one after rebooting it, any snmp get/get-next/get-bulk operations will issue high CPU utilization on agent side.

Example:



Serial Number: 101858
Cabinet Description: ION Chassis
Device Model: IONBPC-219

```
Mem: 35868K used, 90704K free, 0K shrd, 0K buff, 5256K cached
Load average: 1.12 1.16 0.90
  PID USER     STATUS   RSS  PPID %CPU %MEM COMMAND
  731 root     S <      264     1 14.2  0.2 bpd_linux
  730 root     R      21236     1 11.1 16.7 snmpd
  977 root     R        336   949  1.3  0.2 top
  823 root     S        280     1  0.7  0.2 syslogd
  745 root     S        320     1  0.3  0.2 taskmonitor
  808 root     S        232     1  0.3  0.1 telnetd
  824 root     S       2540   755  0.0  1.9 subagent
  756 root     S       2540   755  0.0  1.9 subagent
  741 root     R       2540     1  0.0  1.9 subagent
  816 root     R       2540   755  0.0  1.9 subagent
  818 root     S       2540   755  0.0  1.9 subagent
```

Recovery:

1. The issue is fixed after an IONMM firmware upgrade to revision 1.1.0 or higher.
2. See “Upgrade” on page 33.

Problem: **System can't send trap or inform after IONMM reboot**

Meaning: After IONMM reboot finished, system can't send trap or inform; you have to remove the current trap host and re-add it from FP, after this trap/inform can be sent normally.

Recovery:

1. The issue is fixed after an IONMM firmware upgrade to revision 1.1.0 or higher.
2. See “Upgrade” on page 33.

SMTP Server Status Codes

SMTP success conditions are indicated by the **Authentication Succeeded** response to the AUTH command to indicate that the authentication was successful.

The following error codes indicate SMTP failure conditions (i.e., these enhanced status codes are returned if the authentication is unsuccessful).

Message: **A password transition is needed**
Meaning: This response to the AUTH command indicates that the user needs to transition to the selected authentication mechanism. This is typically done by authenticating once using the Plain authentication mechanism.
Recovery:
1. Verify the operation.
2. See 'SMTP Server Setting' on page 44.

Message: **Temporary authentication failure**
Meaning: This response to the AUTH command indicates that the authentication failed due to a temporary server failure. The client will notify the user of server failure.
Recovery:
1. Verify the operation.
2. See 'SMTP Server Setting' on page 44.

Message: **Authentication mechanism is too weak**
Meaning: This response to the AUTH command indicates that the selected authentication mechanism is weaker than server policy permits for that user.
Recovery:
1. Verify the operation.
2. See 'SMTP Server Setting' on page 44.

Message: **Authentication credentials invalid**
Meaning: This response to the AUTH command indicates that the authentication failed due to invalid or insufficient authentication credentials.
Recovery:
1. Verify the operation.
2. See 'SMTP Server Setting' on page 44.

Message: **Authentication Exchange line is too long**
Meaning: This response to the AUTH command indicates that the authentication failed due to the client sending a Base-64 response that is longer than the maximum buffer size available for the currently selected SASL mechanism.
Recovery:
1. Verify the operation.
2. See 'SMTP Server Setting' on page 44.

Message: **Authentication required**
Meaning: This response is returned when server policy requires authentication in order to perform the requested action and authentication is not currently in force.
Recovery:
1. Verify the operation.
2. See 'SMTP Server Setting' on page 44.

Appendix B: SNMP Primer

This document contains descriptions of SNMP concepts that explain the behind the scenes workings of SNMP Agents and Applications. For most users, the amount of effort required to understand these arcane details will outweigh the benefits. The fact of the matter is that SNMP is anything but "Simple." Fortunately, these details are masked by Network Management Station software such as Transition Networks' Focal Point and Embedded Web Server. If this document is insufficient to allow you to understand SNMP to your satisfaction, then you should either read "Understanding SNMP MIBs" by David Perkins and Evan McGinnis (Prentice Hall), or just relax and allow Focal Point or the Web interface to take care of things for you.

Basic SNMP Concepts and Terms

As new terms are introduced, they will be displayed in **bold** font. Pay special attention to these terms, because after their introduction, it will be assumed that you understand them.

The primary purpose of SNMP is to allow the network administrator to monitor and configure devices on the network, remotely via the network. These configuration and monitoring capabilities are collectively referred to as **Management**.

The network-attached computer that resides within a manageable device and performs management functions is called the SNMP **Agent**.

A computer that is used by the network administrator to work with various Agents around the network is known as a **Network Management Station** or **NMS**. High-level Management software (like Focal Point) that runs on a NMS is referred to as a **Management Application**. Usually, a single NMS will manage multiple Agents.

Designers of network equipment decide which features of their products will be accessible via SNMP, and then create hardware and software to support this management. The collection of the descriptions of all of these features is called a **Management Information Base** or **MIB**, and a description of an individual manageable feature in the MIB is referred to as a **MIB Variable**.

In order for the NMS to be able to carry on meaningful conversations with the Agent, the NMS must have a description of all of the manageable features the Agent knows about. To this end, each type of agent has an associated document called a **MIB Module**, which contains these descriptions. MIB Module files are loaded into the NMS. The primary purpose of the MIB Module is to provide documentation of the name and description of each and every manageable feature a particular type of Agent knows about. Of course, some Management Applications (like Transition Networks' Focal Point) are provided with a large amount of custom information (in addition to the MIB Module document) so that they can provide advanced features such as graphical representation of the equipment.

Note that strictly speaking, the MIB is nothing but a set of ideas. However, since the MIB Module is the most tangible representation of the MIB, the terms "MIB" and "MIB Module" are used interchangeably by many.

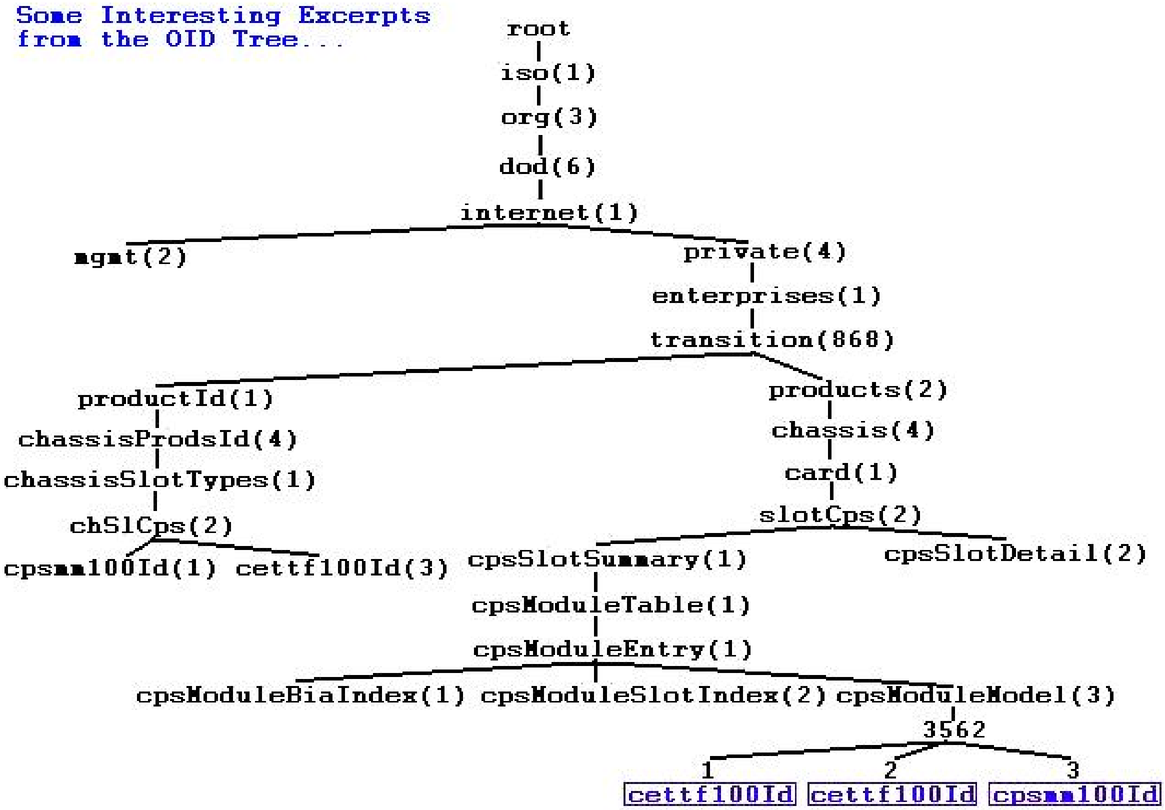
To prevent naming conflicts and provide organization, all of the manageable features of all products from all vendors are arranged into one enormous tree structure referred to as the **MIB Tree** or "**The MIB**," which is managed by the Internet Assigned Numbers Authority (IANA). Each vendor of SNMP equipment has an exclusive section of The MIB Tree that they control.

Each branch of the MIB Tree has a number and a name, and the complete path from the top of the tree down to the point of interest forms the name of that point. A name created in this way is known as an **Object ID** or **OID**.

Nodes near the top of the MIB Tree have names that *extremely* general in nature. (You have to move all the way down to the fourth level before you get to "Internet"!) The names get more and more specific as you move down, until you reach the bottom, where each node represents a particular feature on a specific piece of installed hardware known to a particular Agent.

A sample OID

The remainder of this document uses examples from the Transition Networks Point System product to illustrate SNMP concepts that are applicable to all SNMP compliant products.



This figure shows just a few of the thousands of items (i.e. Variables) in the MIB Tree. We will now take a close look at one of them, called `cpsModuleModel`. `cpsModuleModel` is the MIB Variable that allows us to ask the Point System Agent what type of device is in a particular slot in a particular cabinet.

Looking at this example, it becomes evident that some portions of the MIB Tree are fixed, and others are dynamic. In our example, the path through the tree from the root (at the top) down to `cpsModuleModel` never changes because (to that point) it is a generic reference to a Manageable Feature possessed by every example of the product. This unchanging portion of the tree is clearly insufficient, since a specific user can install one or more cabinets in a Point System stack, and each cabinet can have from 2 to 19 slots - and we need to be able to talk *specifically* about each of those slots. To make the leap from 'generic references to features' to 'specific pieces of installed equipment,' we need a dynamic section on our tree. This dynamic section, which appears at the bottom of the tree, is built by the Agent in response to the hardware it sees. In this example, we have a single cabinet with a serial number of 3562, and the first three slots of this cabinet are shown.

If we wanted to know what type of card was installed in the second slot of our cabinet, what OID would the NMS need to ask for? To find the answer, trace from the top of the tree down to the item we want, recording all of the names/numbers as we go:

```
   iso(1).org(3).dod(6).internet(1).private(4).transition(868).products(2).chassis(4).
card(1).slotCps(2).cpsSlotSummary(1).cpsModuleTable(1).cpsModuleEntry(1).cpsModuleMode
l(3).3562.3
or
   1.3.6.1.4.868.2.4.1.2.1.1.1.3.3562.3
```

In day-to-day practice, these long-form OIDs are rarely seen. It is far more common to start from the lowest "fixed" branch of the MIB Tree like so:

```
 cpsModuleModel.3562.3
```

This is theoretically ambiguous since there is nothing to stop two different vendors from each having MIB variables called `cpsModuleModel`, but in actual practice problems due to conflicts are very rare, primarily because the OIDs are shortened only for use by people. Behind the scenes, the Agents and Management Applications continue to use the long form OIDs.

MIB Table Indices

Indices are the means through which the "dynamic" portion of the MIB tree mentioned above are constructed.

The definition for each variable in a MIB Module contains both a description of the "fixed" portion of that variable's OID and (where applicable) a list of indices that make up the dynamic portion of the OID. To form a complete OID, we take the "fixed" portion of the OID and append the index values. This forms a complete OID that (assuming that it exists) has a data value associated with it.

So, for example, the variable `cpsModuleModel` has a "fixed" OID of

```
 1.3.6.1.4.1.868.2.4.1.2.1.1.1.3
```

If we ask the Agent about this OID, the Agent will return an error, because the OID is ambiguous; `cpsModuleModel` is used to tell us the model of a device in a particular slot in a particular cabinet, but we haven't yet specified which cabinet or which slot. The MIB Module definition for `cpsModuleModel` contains two indices to help us out of this predicament: **BIA** and **slot**. To form a complete OID about which the Agent is able to answer questions, we append a value for BIA and a value for slot. Assuming that our cabinet serial number and slot are the same as in the previous example, we get the following OID:

```
 1.3.6.1.4.1.868.2.4.1.2.1.1.1.3.3562.3
```

which is usually expressed this way:

```
 cpsModuleModel.3562.3
```

The fixed portion of the OID represents everything about the object's location in the tree that is known to the vendor at the time of manufacture. The dynamic portion of the OID represents that portion of the object's location in the MIB tree which cannot be determined until the equipment is installed and initialized.

What if there aren't any indices?

MIB Variables that occur only once in the entire Agent (rather than being repeated for each of several devices) have no indices. When the definition of a MIB Variable does not contain any indices, the placeholder value "`.0`" is used to indicate this. For example, it is neither necessary nor permissible to specify a cabinet or slot when asking about the Group Control String. There is one Group Control String for the entire system, and its complete OID is:

```
 cpsGroupCtrl.0
```

or

```
 1.3.6.1.4.1.868.2.4.2.2.3.1.0
```

The "`.0`" at the end says "no indices are required."

Values

The Value of a MIB Variable can take on many forms. Strings and integers are very common, but the most common type is an enumeration.

The values of normal integers don't have any particular meaning beyond perhaps a count of some sort. '3' just means that there are three of something. An enumeration is a special integer that doesn't count anything. Instead, each integer value corresponds to some particular meaning which is reflected in a label that is associated with that integer value.

For example, the MIB variable `cettf100FiberLink` indicates the link status of the fiber port on the device, and it has an enumerated value of either 1 for `linkUp` or 2 for `linkDown`.

The combination of a complete OID and the value and data type associated with that OID is called a **Variable Binding**. For example:

`cettf100FiberLink.3562.3` is an `integer` with a value of `linkDown(2)`

If an OID does not have any data associated with it (this is fairly common), it is impossible to create a variable binding for that OID. For example, the OID '`1.3.6.1.4.1.868.2.4.1.2.1.1.1.3`' (from our MIB Table Indices example above) cannot be bound because it is incomplete.

Notation

There are many situations in SNMP where a numeric value has a text label associated with it in the MIB Module file. When such a values is written about or displayed, it is common to list both, with the text label followed by the numeric value in parenthesis. This notation is used both for values of MIB variables and for branches of the MIB Tree.

Several examples can be found in this document. Our sample OID contains "`cpsModuleModel(3)`" and many other label/numeric pairs. In this case, the "`3`" refers to the 3rd branch of the OID tree from the above level, and "`cpsModuleModel`" is the text label assigned to this branch in the MIB Module file.

The above 'Values' example contains `linkDown(2)`. This is a value of "`2`" which has a text label of "`linkDown`".

SNMP Operations

In SNMPv1, there are four types of transactions that can occur between the Agent and the NMS:

- **Get**
  The Get operation is performed by NMS when it wants to retrieve management information contained in an Agent. To use this request, the Agent must know exactly what it is looking for. In the Get Request, the NMS provides a complete OID to the Agent. Unless there is an error, the Response from the Agent contains a variable binding containing the same OID and the data associated with it. If the OID does not exist or does not have any data associated with it, the operation fails.

- **Getnext**
  Like a Get, this is a request by an NMS to retrieve management information contained in an Agent. The difference is that the NMS doesn't need to know the complete OID to make the request. This is useful in stepping through dynamic lists of MIB variables (which cannot be not fully specified in the MIB Module), like the list of cabinets in a Point System stack. In the Getnext request, the NMS provides either a complete OID or a fragment of an OID. Unless there is an error, the Response from the Agent is a binding containing the OID and Data of the item immediately to the right of the specified OID in the tree. The Agent will move up or down the tree as required to find the next OID that can be bound.

The Getnext operation can be used repeatedly to retrieve all of the information in the portion of the MIB Tree that the agent knows about. This is known as a **MIB Walk**.

- **Set**
  A Set operation is used by an NMS to tell the Agent to change a piece of management information contained in that Agent. In the Set Request, the NMS provides a complete variable binding to the Agent, expecting the Agent to write the provided data into the data area associated with the provided OID. If the OID does not exist, does not have any writable data associated with it, or for any reason cannot accept the provided data, the operation fails.

- **Trap**
  A trap is a one way notification from the Agent to the NMS, when some urgent condition occurs, such as the failure of a communications channel. It is the only operation that is initiated by the Agent rather than the NMS.

Summary

- The term **Management** refers to the ability to monitor and configure equipment remotely via the network.
- The computing entity within the managed equipment that performs management functions is called the **Agent**.
- Each piece of equipment has a vendor-defined list of manageable features. This list is called a **MIB**, or Management Information Base.
- **Object ID**s are names used to refer to particular items of interest within an SNMP agent. Usually, these items are individual pieces of management data. All OIDs have a fixed portion, and some also have a dynamic portion.
- The MIB Module document is a human and machine readable description of a MIB. Equipped with this document (at a minimum), a network management application can be used to manage a device.
- The four basic SNMPv1 operations **GET**, **GETNEXT**, **SET**, and **TRAP** are used to exchange information between an Agent and a network management application.

SNMP Versions Supported

Simple Network Management Protocol (SNMP) is a network management protocol that provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.

FP3.0 supports three security models: SNMPv1, SNMPv2c, and SBNMv3.

SNMPv1 (SNMP version 1) is the original Internet-standard Network Management Framework, as described in IETF RFCs 1155, 1157, and 1212.

SNMPv2c (Community-based SNMP version 2) is a SNMP Framework which supplements the SNMPv2 Framework, as described in RFC 1901. It adds the SNMPv2c message format, which is similar to the SNMPv1 message format. The second version of SNMP, it supports centralized and distributed network management strategies, and includes improvements in the Structure of Management Information (SMI), protocol operations, management architecture, and security.

Both versions (SNMPv1 and SNMPv2) of the Internet Standard Management SNMP Framework share the same basic structure and components, and all versions follow the same architecture. The SNMP framework consists of 1) a data definition language, 2) definitions of management information (the Management Information Base, or MIB), 3) a protocol definition, and 4) security and administration.

SNMPv3 (Simple Network Management Protocol Version 3) is an interoperable standards-based protocol for network management. SNMPv3 provides secure access to devices by a combination of authenticating and encrypting packets over the network. Although SNMPv3 makes no changes to the protocol aside from the addition of cryptographic security, its developers have managed to make things look much different by introducing new textual conventions, concepts, and terminology.

SNMPv3 provides important security features: 1) Confidentiality - Encryption of packets to prevent snooping by an unauthorized source. 2) Integrity - Message integrity to ensure that a packet has not been tampered with in transit including an optional packet replay protection mechanism. 3) Authentication - to verify that the message is from a valid source.

SNMP Version v1, v2c, v3 Considerations

1. SNMPv3 provides secure access to the ION system by a combination of authenticating and encrypting packets over the network. With the SNMPv3 feature, users can enable SNMPv1/v2c or SNMPv3 access to ION system as follows:

SNMP Access	How To Configure	Description
SNMP v1/v2c only	• Add SNMPv1/v2c community strings. • Remove all SNMPv3 users.	Only allow SNMPv1/v2c access to ION system though community strings.
SNMPv3 only	• Remove all SNMPv1/v2c community strings. • Add SNMPv3 users, assign the users to groups, enable the groups to have access to views, add views to have access to MIBs.	Only allow SNMPv3 access to ION system though SNMPv3 users.
SNMPv1/v2c/v3	• Add SNMPv1/v2c community strings • Add SNMPv3 users, assign the users to groups, enable the groups to have access to views, add views to have access to MIBs.	Allow SNMPv1/v2 access to ION system though community strings. Also allow SNMPv3 access to ION system though SNMPv3 users.

2. You can configure the SNMPv1/v2c write community string and read only community string. SNMPv1 and v2c share the same community strings.

3. You can set the local SNMPv3 engine ID in the **SNMP** > **GENERAL** tab. An SNMPv3 engine is an independent SNMP agent that resides on the IONMM. This engine protects against message replay, delay, and redirection. The engine ID is also used in combination with user passwords to generate the security keys for authenticating and encrypting SNMPv3 packets.

   A local engine ID is automatically generated that is unique to the IONMM. The input engine ID is referred to as the default engine ID. If the local engine ID is deleted or changed, all SNMP users are cleared, and you must reconfigure all existing users.

   A new engine ID can be specified by entering 9 to 64 hexadecimal characters. An engineID can not be empty. At default the SNMPv3 engine ID string of an IONMM is “80 00 03 64 03 00 c0 f2 xx xx xx” (“03 64” is the enterprise number of Transition Networks; “00 c0 f2 xx xx xx” is the MAC address of an ION device). In other words, the default IONMM SNMPv3 engine ID string is: *the MAC address of the IONMM* **+** ’*Transition Network*s’.

   The engine ID is specified by hexadecimal characters. Each two input characters correspond to one octet character. For engine ID “80 00 03 64 03 00 c0 f2 00 01 02”, the first two characters ’80’ correspond to the first octet character ‘\128’ with ASCII value of 128 (8*16 + 0 = 128).
   The second two characters “00” correspond to the second octet character ‘\0’ with ASCII value of 0 (0*16 + 0 = 0).

SNMP v3 Concepts and Terms

Simple Network Management Protocol Version 3 (SNMPv3) is an interoperable standards-based protocol for network management. SNMPv3 provides secure access to devices by a combination of authenticating and encrypting packets over the network. Although SNMPv3 makes no changes to the protocol aside from the addition of cryptographic security, its developers have managed to make things look much different by introducing new textual conventions, concepts, and terminology.

SNMPv3 primarily added security and remote configuration enhancements to SNMP. Security has been the biggest weakness of SNMP since the beginning. Authentication in SNMP Versions 1 and 2 amounts to nothing more than a password (community string) sent in clear text between a manager and agent. Each SNMPv3 message contains security parameters which are encoded as an octet string. The meaning of these security parameters depends on the security model being used.

SNMPv3 provides important security features:

Confidentiality - Encryption of packets to prevent snooping by an unauthorized source.

Integrity - Message integrity to ensure that a packet has not been tampered with in transit including an optional packet replay protection mechanism.

Authentication - to verify that the message is from a valid source.

SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and the group in which the user resides. A security level is the permitted level of security within a security model. A combined security model / security level determines which security mechanism is used when handling an SNMP packet. Three security models are available: SNMPv1, v2c, and v3. The table below shows the combinations of security models / levels.

SNMPv3 Private MIB Levels / Auth / Encryption

Model	Level	Authentication	Encryption	Results
v1	noAuthNoPriv	Community String	None	Uses a community string match for authentication.
v2c	noAuthNoPriv	Community String	None	Uses a community string match for authentication.
v3	noAuthNoPriv	Username	None	Uses a username match for authentication.
v3	authNoPriv	MD5 or SHA	None	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms.
v3	authPriv	MD5 or SHA	DES/AES	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides DES/AES encryption in addition to authentication based on the DES/AES standard.

SNMPv3 Summary and Key Features

SNMPv3 includes the following key features:

- SNMPv3 EngineID
- SNMPv3 USM
- SNMP VACM
- SNMP Trap/Inform (v1/v2c/v3 trap, v2c/v3 inform)

SNMPv3 Services Provided

The SNMPv3 function supports these services:

- SNMP v3 user management, authentication and encryption.
- SNMP VACM management.
- SNMP v1/v2c/v3 selection.
- SNMP notification (v1/v2c/v3 trap, v2c/v3 inform) functionality.

SNMPv3 features can be configured via the Web interface, CLI, Telnet, or SSH. The SNMPv3 configuration can be backed up and restored. These services are further detailed below.

SNMPv3 Services

No.	Function	Description	Reference
1	SNMP v3 USM	SNMP v3 User-based Security Model.	RFC 3414
2	SNMP VACM	SNMP View-based Access Control Model.	RFC 3415
3	SNMP v1/v2c/v3 version selection	SNMP v1/v2c/v3 version selection	Private MIB
4	SNMP v1/v2c/v3 Trap	SNMP v1/v2c/v3 Trap functionality	Private MIB
5	SNMP v1/v2c/v3 Inform	SNMP v1/v2c/v3 Inform functionality	Private MIB
6	Web for SNMP v3	Configure SNMP v3 via Web	None
7	CLI for SNMP v3	Configure SNMP v3 via CLI	None
8	Backup/Restore for SNMP v3	Backup/Restore SNMP v3 configuration.	None

SNMP v3 EngineID Concept

An SNMP engine provides services for sending and receiving messages, authenticating and encrypting messages, and controlling access to managed objects. There is a one-to-one association between an SNMP engine and the SNMP entity which contains it. The SNMP v3 engine contains:

- a Dispatcher
- a Message Processing Subsystem
- a Security Subsystem, and
- an Access Control Subsystem.

Within an administrative domain, an snmpEngineID is the unique and unambiguous identifier of an SNMP engine. Since there is a one-to-one association between SNMP engines and SNMP entities, it also uniquely and unambiguously identifies the SNMP entity within that administrative domain. Note that it is possible for SNMP entities in different administrative domains to have the same value for snmpEngineID. Federation of administrative domains may necessitate assignment of new values.

The User-based Security Model requires a discovery process to obtain enough information about other SNMP engines in order to communicate with them. Discovery requires a non-authoritative SNMP engine to learn the authoritative SNMP engine's snmpEngineID value before starting communication.

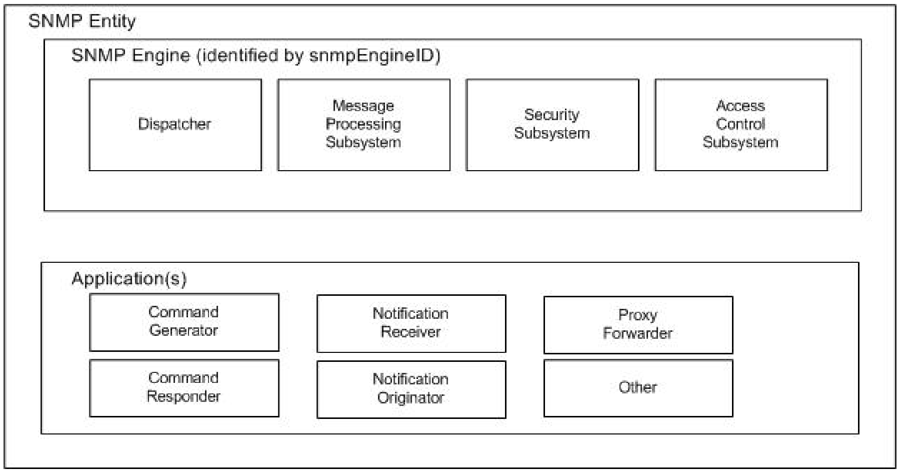


Figure 27. SNMP v3 Entity / Engine / Applications

Local engineID:

- The engineID for the local SNMP engine.
- The engineID for the SNMP engine residing in the managed IONMM or standalone S2x2x/S3x2x/S3240.

Remote engineID:

- The engineID for a remote SNMP engine.
- In the ION system, the remote engineID is only used to configure the engineID of the remote SNMPv3 inform receipt server.

RFC standard: RFC 3411.

SNMPv3 EngineID MIBs

<u>Public MIB for enginID</u>: snmpEngine

- OID is 1.3.6.1.6.3.10.2.1
- For local engineID
- Read-only

<u>Private MIB for local enginID</u>:

- OID is 1.3.6.1.4.1.868.2.5.3.1.1.14.3.1
- Read-write
- Used to modify the local engineID.
- When modifying the local engineID, all the local SNMPv3 USM users will be deleted.

<u>Private MIB for remote enginID</u>:

- OID is 1.3.6.1.4.1.868.2.5.3.1.1.14.4.1
- Read-write
- The combination of *ionDevSysSnmpTrapManagerAddrTDomain* and *ionDevSysSnmpTrapManagerAddrTAddress* must be unique.
- The engineID in this table must be unique (it can <u>not</u> be the same as the local engineID).
- Used to add/delete remote engineIDs.
- When deleting a remote engineID, all the SNMPv3 USM users belonging to the SNMP engine will be deleted.

You must add a remote engine before you can add remote users for this engine.

SNMPv3 USM (User-Based Security Model)

The ION SNMP v3 implementation uses the traditional concept of a user (identified by a *userName*) with associated security information. This is a key SNMPv3 security feature implemented per RFC 3414.

SNMP v3 USM Service: USM provides the following security service:

- Data Integrity is the provision of the property that data has not been altered or destroyed in an unauthorized manner, nor have data sequences been altered to an extent greater than can occur non-maliciously.
- Data Origin Authentication is the provision of the property that the claimed identity of the user on whose behalf received data was originated is corroborated.
- Data Confidentiality is the provision of the property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
- Message timeliness and limited replay protection is the provision of the property that a message whose generation time is outside of a specified time window is not accepted. Note that message reordering is not dealt with and can occur in normal conditions too.

SNMP v3USM User: Management operations using this Security Model make use of a defined set of user identities. For any user on whose behalf management operations are authorized at a particular SNMP engine, that SNMP engine must have knowledge of that user. An SNMP engine that wishes to communicate with another SNMP engine must also have knowledge of a user known to that engine, including knowledge of the applicable attributes of that user.

SNMPv3 USM User and SNMP Engine

- A USM user must belong to a SNMP engine.
- You must add a remote engine before you can add remote users for this engine.
- If a user belongs to the local SNMP engine, it is called a local USM user.
- If a user belongs to a remote SNMP engine, it is called a remote USM user.
- If an engineID of a SNMP engine is changed or deleted, its USM users are deleted.

SNMPv3 USM MIB

Public MIB for USM: usmUser

- OID is 1.3.6.1.6.3.15.1.2
- Used to add/modify/delete USM users
- Store information for both local USM users and remote USM users

SNMPv3 VACM (View-based Access Control Model)

The View-based Access Control Model defines a set of services that an application (such as a Command Responder or a Notification Originator application) can use for checking access rights.

Access Control occurs (either implicitly or explicitly) in an SNMP entity when processing SNMP retrieval or modification request messages from an SNMP entity.

Access Control also occurs in an SNMP entity when an SNMP notification message is generated (by a Notification Originator application).

VACM includes these elements:

- Groups
- SecurityLevel
- Contexts
- MIB Views and View Families
- Access Policy

SNMPv3 USM – VACM MIBs

Public MIB for VACM: snmpVacmMIB

- OID is 1.3.6.1.6.3.16
- Used to manage VACM configurations including the mapping from user to groups, groups access, view table.
- RFC 3415

SNMP v3 Default Values

snmpVacmMIB (RFC 3415)	vacmContextTable	The table of locally available contexts.
	vacmSecurityToGroup Table	Mapping USM user or v1/v2c community string to Group.
	vacmAccess Table	Group access right to View
	vacmViewSpinLock	Lock for creating and modifying Views.
	vacmViewTree Family Table	View to OID tree management table.

SNMPv3 VACM – Groups

A Group is a set of zero or more <*securityModel*, *securityName*> tuples on whose behalf SNMP management objects can be accessed. A Group defines the access rights afforded to all securityNames which belong to that group. The combination of a *securityModel* and a securityName maps to at most one Group. A Group is identified by a *groupName*.

The Access Control module assumes that the *securityName* has already been authenticated as needed and provides no further authentication of its own.

The View-based Access Control Model uses the *securityModel* and the *securityName* as inputs to the Access Control module when called to check for access rights. It determines the *groupName* as a function of *securityModel* and *securityName*.

Note that when the security model is v1 or v2c, the groups "public" and "private" can not be removed, but when the security model is v3 the groups "public" and "private" can be removed.

SNMPv3 VACM – Views

Views are used to restrict the access rights of some groups to only a subset of the management information in the management domain.

A view subtree is the set of all MIB object instances which have a common ASN.1 OBJECT IDENTIFIER prefix to their names.

A family of view subtrees is a pairing of an OBJECT IDENTIFIER value (called the family name) with a bit string value (called the family mask). The family mask indicates which sub-identifiers of the associated family name are significant to the family's definition.

SNMPv3 Traps and Informs

A Trap is an SNMP message sent from one application to another (which is typically on a remote host). Their purpose is merely to notify the other application that something has happened, has been noticed, etc. The big problem with Traps is that they're unacknowledged, so you don't actually know if the remote application received your -important message. The trap is available for SNMP v1, v2c and v3.

An Inform is an acknowledged Trap. When the remote application receives an inform it sends back an acknowledgement message. Inform is available for SNMP v2c and v3. For SNMP v3, an inform must be sent to a specific remote USM user resided in the inform receiver.

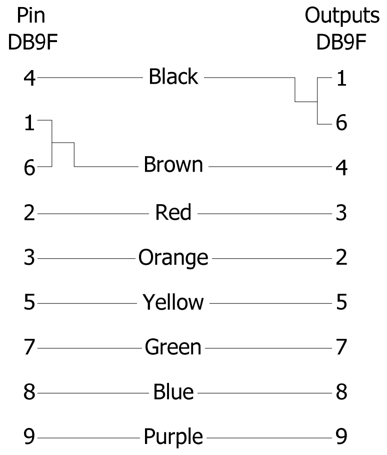
Appendix C - Cable & Connector Specifications

Cable Specifications

Null Modem Cable: Use the Null Modem cable for connecting a terminal or terminal emulator to the DB-9 of the management module to access the CLI. The table below shows the pin assignments for the DB9 cable.

Function	Mnemonic	Pin
Carrier Detect	CD	1
Receive Data	RXD	2
Transmit Data	TXD	3
Data Terminal Ready	DTR	4
Signal Ground	GND	5
Data Set Ready	DSR	6
Request To Send	RTS	7
Clear To Send	CTS	8

9-Pin RS232 Null Modem Cable:



RJ-45 cable (Category 5):
Gauge: 24 to 22 AWG
Attenuation: 22.0 dB/100m @ 100 MHz
Max. Cable Distance: 100 meters

- Straight-Through or Crossover cable can be used.
- Shielded Twisted-Pair (STP) or Unshielded Twisted-Pair (UTP) can be used.
- All pin pairs (1&2, 3&6, 4&5, 7&8) are active in a Gigabit Ethernet network.
- Use only dedicated wire pairs for active pins (e.g., blue/white & white/blue, orange/white & white/orange, etc.)
- DO NOT use flat or silver satin wire.

Point System Connector Types

The types of connectors that can be built into a Point System converter are listed below. No type of converter uses all of these connector types. Some converters return 16 bit connector style values that contain additional information on the connector in the upper byte. In these cases, the lower byte is one of the values below.

Point System Connector Types

Value	Connector Description
rj-45 (10)	RJ-45, unshielded twisted pair
stmm (11)	ST fiber, multimode
stsm (12)	ST fiber, singlemode
scmm (13)	SC fiber, multimode
scsm (14)	SC fiber, singlemode
scsmlh (15)	SC fiber, singlemode, long haul
scsmelh (16)	SC fiber, singlemode, extra long haul
scsmlhlw (17)	SC fiber, long haul, long wavelength
mtrjmm (18)	MT-RJ multimode fiber
lc (19)	LC fiber, singlemode
bnc (20)	BNC coax
stsmlh (21)	ST Singlemode Long Haul
stsmelh (22)	ST Singlemode Extra Long Haul
scmm1300 (23)	SC Multimode 1300nm
stmm1300 (24)	ST Multimode 1300nm
mtrjsm (25)	MTRJ singlemode fiber
serial26 (26)	Universal 26-pin Serial Interface Connector
stmmlh (27)	ST Multimode Long Haul
scsmsh (28)	SC Singlemode Short Haul
scsimplex (29)	SC Simplex
bncdual (30)	Dual BNC coax connectors
db9rsxxx (31)	DB9 for RS232 and RS485
termblock (32)	Terminal Block for RS485
rj11 (33)	RJ-11, unshielded twisted pair
sc40km (34)	SC fiber, 1550nm 40km
sc125km (35)	SC fiber, 1 x 9, 125km Gigabit
din6 (38)	DIN 6-Pin for RS232
cmm(39)	LC Multimode Fiber
sfp(40)	SFP Small Form Factor Pluggable
sfmmlh(42)	Single-Fiber Multimode
scmmlh(43)	SC Multimode (long haul)
lcmmlh(44)	LC Singlemode (long haul)
xfp(47)	XFP 10 Gigabit
sfpPlus(48)	SFP+ 10 Gigabit

Appendix D - ION System and PointSystem / FocalPoint 3.0 Restrictions

Introduction

The ION System (Chassis III) and Point System (Chassis II) operate differently under FocalPoint 3.0 (FP3.0) software.

This section presents a series of known issues and descriptions, and possible workarounds for the supported FP3.0 environments.

Environments

1. ION Chassis and ION cards with FP3.0 software
2. ION Chassis and Point System cards with FP3.0 software
3. Point Systems chassis and PS cards with FP3.0 software

Point System Issues, Descriptions, and Workarounds

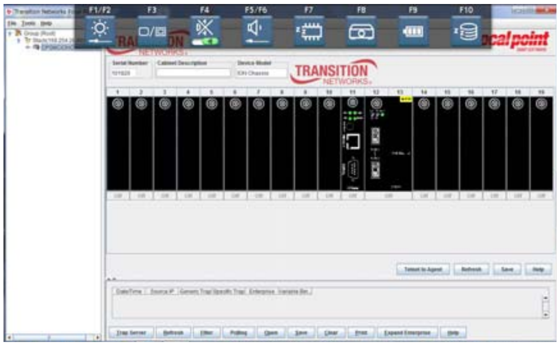
See below for specific Point System issues, descriptions, and suggested workarounds.

Issue: Must have At Least 1 PS Card if Running CPSMM120 Management Card

Description: If you install a PS Management card with no other PS cards, the system is inoperable.
Workaround: Install and run the PS Management card with other PS cards.

Issue: Can not turn off PS Card's Power in ION Chassis / IONADP with FP3.0

Description: FP3.0 and Agent II can not change the power in a ION Chassis running Point System cards (e.g., with the CPSMM-120 used in the ION chassis). When you view the ION Chassis and Point System cards in FP3.0, the power option is grayed out. You can not click the power button below the card and power off the card. You can not turn on/off each Point System module connected by an IONADP to an ION Chassis under Focal Point 3.0. The Off switches are grayed out / not functional.



Workaround: Use another means to power off the card.

ION System Issues, Descriptions, and Workarounds

See below for specific ION system issues, descriptions, and suggested workarounds.

Issue: Can not run more than One Instance of FP Concurrently

Description: Connecting more than one Focal Point system to one IONMM or standalone converter card will make the IONMM or standalone inoperable.
Workaround: Run just one instance of FP at a time.

Issue: The "unknown" value in Line Build Out is modified to "".

Description: FP_Compatability_C6x10: please unite some parameters of C6x10 in FP for "Software Revision 1.2.1".
Workaround: Be aware of the LBO change.

Issue: The "Refresh" button inside the loopback frame is ignored in FP.

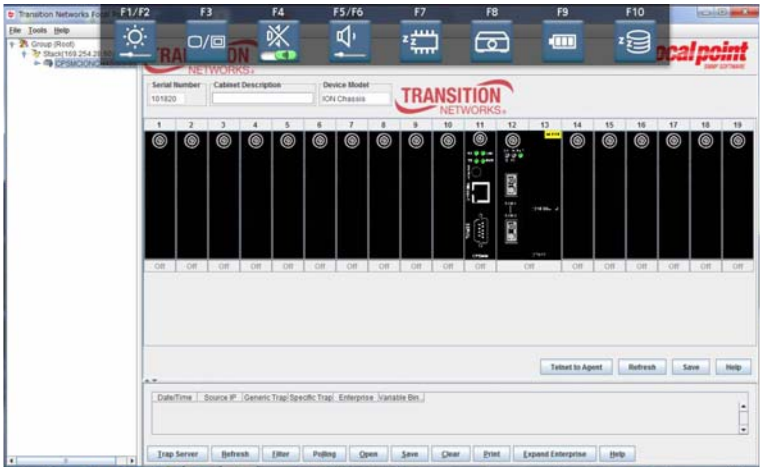
Description: FP_Compatability_C6x10: please unite some parameters of C6x10 in FP for "Software Revision 1.2.1". All refresh functions are based on the one **Refresh** button in the tab (refer to #3090).
Workaround: Avoid using the "Refresh" button inside the loopback frame when using FocalPoint v 1.2.1 with the C6x10 NIDs.

Issue: ION SNMP v3 user can view all of the OIDs

When you login to FP with a SNMP v3 user, view OID is "1.3.6", and verify if this user can only access this view defined OIDs, the view OIDs limitation don't work effectively, no matter the OIDs are what, this user can still access all of the OIDs.
Description: The problem is that FP cannot “hide” the GUI components for the unauthorized OIDs; the unauthorized values are impossible to be displayed in these components, because they cannot read from or write to the devices.
Workaround: Be aware of the issue with SNMP v3 users logging in to FP.

Issue: Can not turn off PS Card’s Power in ION Chassis / IONADP with FP3.0

Description: FP3.0 and Agent II can not change the power in a ION Chassis running Point System cards (e.g., with the CPSMM-120 used in the ION chassis). When you view the ION Chassis and Point System cards in FP3.0, the power option is grayed out.   You can not click the power button below the card and power off the card.
You can not turn on/off each Point System module connected by an IONADP to an ION Chassis under Focal Point 3.0. The Off switches are grayed out / not functional.



Serial Number: 101820
Cabinet Description:
Device Model: ION Chassis

Workaround: Use another means to power off the card.

Issue: SNMP User Level Restrictions

Description: ION system restrictions in FP when using SNMP user level management:
Low revision ION system SNMP can’t create high revision SNMP user.
Workaround: Restrict in FP interface to disable SNMPv1/v2 user can clone SNMPv3 user.

Description: Lower level ION system SNMPv3 user (NoAuthNoPriv) can not clone a higher level SNMPv3 user (AuthPriv).
Workaround: Check user level in FP interface before sending the SNMP requirement.

Issue: SNMP User Level Restrictions

Description: ION system restrictions in FP when Power Supply input = 0V, FP should display a warning (gray).
Workaround: Check power supply levels.

Glossary

This section describes many of the terms and mnemonics used in this manual. Note that the use of or description of a term does not in any way imply support of that feature or of any related function(s).

AES

(Advanced Encryption Standard) A privacy protocol; one of two encryption algorithms used for ION system data privacy. AES is a symmetric-key encryption standard adopted by the U.S. government. The standard comprises three block ciphers, AES-128, AES-192 and AES-256, adopted from a larger collection originally published as Rijndael. Each cipher has a 128-bit block size, with key sizes of 128, 192 and 256 bits, respectively. AES ciphers were analyzed extensively and are now used worldwide (as was its predecessor, DES). AES was announced by NIST as U.S. FIPS PUB 197 (FIPS 197) in 2001 after a 5-year standardization process. AES was implemented as a Federal government standard in 2002 after approval by the U.S. Secretary of Commerce. AES is available in many different encryption packages. See also “DES”.

Agent

In SNMP, a software module that performs the network management functions requested by network management stations.

Authentication

The process of ensuring message integrity and protection against message replays. Authentication includes both data integrity and data origin authentication.

Authenticated SMTP Server

A computer used for or dedicated to SMTP server functions that provides user authentication. See also “SMTP server”.

Authoritative SNMP engine

SNMPv3 introduced the concept of an authoritative SNMP engine that lets you create authorized users for specific SNMPv3 agents. One of the SNMP copies involved in network communication designated as the allowed SNMP engine to protect against message replay, delay, and redirection. The security keys used for authenticating and encrypting SNMPv3 packets are generated as a function of the authoritative SNMP engine's engine ID and user passwords. When an SNMP message expects a response (e.g., get exact, get next, set request), the receiver of these messages is authoritative. When an SNMP message does not expect a response, the sender is authoritative.
See also “SNMP engine”.

BPC

(Back Plane Controller) the ION chassis component that provides communication between the SIC cards and the IONMM. The BPC is an active device with a microprocessor and management software used to interconnect IONMM and SIC cards via the Ethernet management plane. The BPC has knowledge of the cards that are present in the system, and is responsible for managing the Ethernet switch that interconnects all the chassis slots.

BPDU

(Bridge Protocol Data Unit) Data messages that are exchanged across the switches within an extended LAN that uses a spanning tree protocol topology. BPDU packets contain information on ports, addresses, priorities and costs and ensure that the data ends up where it was intended to go.

Bridge

A device that connects one local area network (LAN) to another LAN.

ciphertext

Ciphertext is encrypted text. Plaintext is what you have before encryption, and ciphertext is the encrypted result.

Community

In SNMP, a relationship between an agent and a set of SNMP managers that defines security characteristics. "Community" is a local concept, defined at the agent. The agent establishes on community for each required combination of authentication, access control, etc. Each community is given a unique name within the agent, and the management stations within that community must employ that community name in all 'get' and 'set' operations.

Two levels of ION system access privileges are password protected:

- Read access (Read ONLY) - a Community Name with a particular set of privileges to monitor the network without the right to change any of its configuration.
- Read/Write (Read and make changes) - a Community Name with an extended set of privileges to monitor the network as well as actively change any of its configuration.

Community string

A string that is used as the name of the community; acts as a password by controlling access to the SNMP community. A text string used to authenticate messages between a management station and an SNMP v1/v2c engine.

DES

(Data Encryption Standard) A privacy protocol; one of two encryption algorithms used for ION system data privacy. DES is a block cipher that uses shared secret encryption. It was selected by the National Bureau of Standards as an official FIPS standard for the US in 1976 and has since enjoyed widespread use internationally. DES is based on a symmetric-key algorithm that uses a 56-bit key. Despite criticism, DES was approved as a federal standard in 1976, and published in1977 as FIPS PUB 46, authorized for use on all unclassified data. DES was confirmed as the standard in 1983, 1988 (revised as FIPS-46-1), 1993 (FIPS-46-2), and in 1999 (FIPS-46-3, as "Triple DES"). See also “AES”.

Discovering / Discovery

Discovery allows a Service OAM capable NID to learn sufficient information (e.g. MAC addresses etc.) regarding other SOAM capable NIDs so that OAM frames can be exchanged with those discovered NIDs.

EGP

(Exterior Gateway Protocol) is a protocol for exchanging routing information between two neighbor gateway hosts (each with its own router) in a network of autonomous systems. EGP is commonly used between hosts on the Internet to exchange routing table information. The routing table contains a list of known routers, the addresses they can reach, and a cost metric associated with the path to each router so that the best available route is chosen. Each router polls its neighbor at intervals between 120 to 480 seconds and the neighbor responds by sending its complete routing table. EGP-2 is the latest version of EGP. A more recent exterior gateway protocol, the Border Gateway Protocol (BGP), provides additional capabilities.

Encryption

A method of hiding data from an unauthorized user by scrambling the contents of an SNMP packet. See also “DES” and “AES”.

Engine ID

In SNMP v3, each agent has an engine ID that uniquely identifies the agent in the device. The engine ID can be set by the network administrator and is unique to that internal network (or it may be pre-configured by the device manufacturer). Each packet contains two engine IDs. One is used to identify security information (e.g., user name, key location). The second one specifies where the packet payload is coming from and going to. SNMPv1 and v2c did not use the engine ID concept; they relied instead on the IP address or the domain name of the device. However, IP addresses may be changed and the Domain Name System may be down. Also, IP addresses and domain names may be known outside the organization, which can cause security vulnerabilities. A single device can have multiple engine IDs, with each Engine ID associated with one of the SNMP agents in the device.

Group Views

The ION system supports three SNMP v3 Views: notifview, readview, and writeview.

ICIF

(Interconnection of Cabinets) Multiple Point System cabinets can be managed by a single Base Management Module if the Inter-Cabinet Interface (ICIF) ports of the Management Modules in all of the cabinets are connected with straight-through RJ-45 cables.

Informs

One of two types of SNMP notifications that can be sent. See also "traps".

An SNMP notification can be sent as a ‘trap’ or an ‘inform’. Traps are less reliable since the trap receiver does not send acknowledgments when it receives traps. The trap sender cannot determine if the traps were received. However, an SNMP entity that receives an inform request acknowledges the message with an SNMP response PDU. If the sender never receives the response, the inform request can be sent again, making informs more likely to reach their intended destination. However, informs use more agent and network resources. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received, otherwise the request times out. Also, a trap is sent only once, while an inform may be retried several times.

The ION SNMPv3 feature provides users SNMP v1/v2c/v3 access to manage the ION system through the IONMM. Any ION defined traps can be sent to the configured trap servers in v1 or v2c or v3 format through the IONMM. If the IONMM sends out v2c/v3 informs, the trap servers will send responses.

MD5

(Message-Digest algorithm 5) An authentication protocol; one of two cryptography methods used for ION system user authentication. MD5 is a widely used cryptographic hash function with a 128-bit hash value. Specified in RFC 1321, MD5 is used in a wide range of security applications, and is also commonly used to check file integrity. However, it has been shown that MD5 is not collision resistant; as such, MD5 is not suitable for applications like SSL certificates or digital signatures that rely on this property. MD5 was designed by Ron Rivest in 1991 to replace the earlier hash function MD4. See also “SHA”.

MIB

(Management Information Base) The set of variables that are used to monitor and control a managed device.
A formal description of a set of network objects that can be managed using the Simple Network Management Protocol (SNMP). The format of the MIB is defined as part of the SNMP.

MIBs stems from the OSI/ISO Network management model and are a type of database used to manage the devices in a communications network. A MIB comprises a collection of objects in a (virtual) database used to manage entities (such as routers and switches) in a network. Objects in the MIB are defined using a subset of Abstract Syntax Notation One (ASN.1) called "Structure of Management Information Version 2 (SMIv2)" RFC 2578. The database is hierarchical (tree-structured) and entries are addressed through object identifiers. IETF RFCs discuss MIBs, notably RFC 1155, "Structure and Identification of Management Information for TCP/IP based internets", RFC 1213, "Management Information Base for Network Management of TCP/IP-based internets", and RFC 1157, "A Simple Network Management Protocol".

MIB Module

Strictly speaking, a MIB is just a set of ideas; however, since the MIB Module is the most tangible representation of the MIB, the terms "MIB" and "MIB Module" are used interchangeably by many. To prevent naming conflicts and provide organization, all of the manageable features of all products from all vendors are arranged into one enormous tree structure referred to as the MIB Tree or "The MIB," which is managed by the Internet Assigned Numbers Authority (IANA). Each vendor of SNMP equipment has an exclusive section of The MIB Tree that they control.

MIB object identifier

See “OID”.

MIB variable

See “OID”.

MIB walk

Performing an "SNMP MIB walk" discovers MIBs and OIDs on devices, and determines which MIBs and OIDs are supported on a particular device.

Some MIB applications can produce a complete listing of the supported MIBs and OIDs and report the current setting for each OID. They can also recognize MIBs from various vendors (private MIBs) and public MIB sources, and walk the SNMP tree for a target device and pull the value of each OID in the supported MIBs, to find out which MIBs and OIDs are supported on a particular device. Most commercial MIB browser tools can perform an "SNMP MIB walk".

MO

(Managed Object, or “Object”) the term 'managed object' can have multiple meanings:

1. In SNMP, a data variable that represents some resource or other aspect of a managed device.

2. In telecom management, a resource within the telecommunications environment that can be managed via the OAMP application protocols.

3. In networking, an abstract representation of network resources that are managed. The 'MIB' is the database that stores all managed objects. A managed object is 'dynamic' and it communicates with other managed network recourses. A managed object may represent a physical entity, a network service, or an abstraction of a resource that exists independently of its use in management.

4. The OOP programming language model is organized around "objects" rather than "actions" and data rather than logic.

NID

(Network Interface Device) A device that serves as the demarcation point between the carrier's local loop and the customer's premises wiring. In telecommunications, a NID is a device that serves as the demarcation point between

the carrier's local loop and the customer's premises wiring. In fiber-to-the-premises systems, the signal is transmitted to the customer premises using fiber optic technologies.
In general terms, a NID may also be called a Network Interface Unit (NIU), Telephone Network Interface (TNI), Slide-in-card (SIC), or a slide-in-module.

NMS

(Network Management Station) A high-end workstation that, like the Managed Device, is also connected to the network. A station on the network that executes network management applications that monitor and control network elements such as hosts, gateways and terminal servers. See also “SNMP”.

Notification

An SNMP trap or inform message. See also "traps" and "informs". SNMP notifications can be sent as traps or informs. Traps are less reliable since the receiver does not send an acknowledgment when it receives a trap (the sender cannot tell if the traps were received). However, an SNMP entity that receives an inform request acknowledges the message with an SNMP response PDU. If the sender never receives the response, the inform request can be sent again (making informs more likely to reach their intended destination). On the other hand, informs use more agent and network resources. While a trap is discarded as soon as it is sent, an inform request is held in memory until a either response is received or the request times out. Note also that traps are sent only once, while an inform may be resent several times. These inform retries increase traffic and contribute to a higher overhead on the network.

Notifview

An SNMP v3 string of up to 64 characters that is the name of the view that enables you to specify a notify, inform, or trap. The default notifview is 'nothing' (i.e., the null OID). If a view is specified, any notifications in that view that are generated are sent to all users associated with the group (provided an SNMP server host configuration has been created for the user).

Notify view

A view name (not to exceed 64 characters) for each group that defines the list of notifications that can be sent to each user in the group.

Object

See “Managed object”.

OID

(Object Identifier) Known as a “MIB object identifier” or “MIB variable” in the SNMP network management protocol, an OID is a number assigned to devices in a network for identification purposes. Each branch of the MIB

Tree has a number and a name, and the complete path from the top of the tree down to the point of interest forms the name of that point. A name created in this way is known as an Object ID or OID.

In SNMP, an Object Identifier points to a particular parameter in the SNMP agent.

PDU

(Protocol Data Unit) information delivered as a unit between network peer entities; may contain data, address information, or control information.

plaintext

Ciphertext is encrypted text. Plaintext is what you have before encryption, and ciphertext is the encrypted result.

Port-based Authentication

802.1X allows each user's access to the LAN to be conditioned on who the user is, not which Ethernet receptacle the user happens to plug into. (Standard: IEEE 802.1X.)

Privacy

An encrypted state of the contents of an SNMP packet where they are prevented from being disclosed on a network. Encryption is performed with algorithms called DES or AES.

RADIUS

(Remote Authentication Dial In User Service) a networking protocol that provides centralized authentication, authorization, and accounting management for computers to connect and use a network service.

Read view

An SNMP View name (not to exceed 64 characters) for each group that defines the list of object identifiers (OIDs) that are accessible for reading by users belonging to the SNMP Group.

Readview

A string of up to 64 characters that is the name of the view that enables you only to view the contents of the agent. The default readview is assumed to be every object belonging to the Internet (1.3.6.1) OID space, unless you use the read option to override this state.

Security model

The security strategy used by the SNMP agent. Currently, ION supports three security models: SNMPv1, SNMPv2c, and SNMPv3.

Security model

The security strategy used by the SNMP agent. Currently, FP supports three security models: SNMPv1, SNMPv2c, and SNMPv3.

SHA

(Secure Hash Algorithm) An authentication protocol; one of two cryptography methods used for ION system user authentication. SHA-1 is a cryptographic hash function designed by the National Security Agency (NSA) and published by the NIST as a U.S. FIPS standard. SHA-1 is part of many widely accepted security applications and protocols (e.g., TLS, SSL, PGP, SSH, S/MIME, and IPSec). See also “MD5”.

SMI

(Structure of Management Information) one of two parts of the Managed Object Bas for TCP/IP protocol networks (along with SNMP). The SMI defines the general framework within which an SNMP MIB can be defined. An SMI identifies the data types that can be used in the MIB, how objects within the MIB are named and specified, and guidelines for extending the MIB.(The SMI, however, does not define any actual MIB objects.) See also “SNMP SMI”.

SMTP server

A computer used for or dedicated to SMTP server functions; may or may not use authentication. See also “Authenticated SMTP Server”.

SNMP

(Simple Network Management Protocol) A request-response protocol that defines network communication between a Managed Device and a Network Management Station (NMS). A set of protocols for managing complex IP networks. (Standard: RFC 1157.) A protocol for network management that provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security. Various SNMP versions exist.

SNMP Community String

An Octet String that may contain a string used to add security to SNMP devices.

SNMP engine

SNMPv3 introduced the concept of an authoritative SNMP engine that lets you create authorized users for specific SNMPv3 agents. A copy of SNMP can reside either on the local or remote device. See also “Engine ID”, “Authoritative SNMP engine”.

SNMP Group

A collection of SNMP users that belongs to a common SNMP list that defines an access policy, in which OIDs are both read-accessible and write-accessible. Users belonging to a particular SNMP Group inherit all of the attributes defined by the group.

SNMP Message

A sequence representing the entire SNMP message, which consists of the SNMP version, Community String, and SNMP PDU.

SNMP PDU

An SNMP PDU contains the body of an SNMP message. There are several types of PDUs (e.g., GetRequest, GetResponse, and SetRequest).

SNMP SMI

(SNMP Structure of Management Information) a collection of managed objects, residing in a virtual information store. The SMI is divided into three parts: module definitions, object definitions, and, notification definitions. There are two types of SMI: SMIv1 and SMIv2. For additional information see IETF RFC 1155 v1 and RFC 2578 v2.

SNMP User

The person for which an SNMP management operation is performed. For informs, the user is a person on a remote SNMP engine who receives the informs.

SNMP View

A mapping between SNMP objects and the access rights available for those objects. An object can have different access rights in each view. Access rights indicate whether the object is accessible by either a community string or a user.

SNMP Version

An integer that identifies the version of SNMP (e.g., SNMPv1 = 0).

SNMPv1

(SNMP version 1) the original Internet-standard Network Management Framework, as described in RFCs 1155, 1157, and 1212.

SNMPv2

(SNMP version 2) the SNMPv2 Framework as derived from the SNMPv1 Framework. SNMP v2 is described in STD 58, RFCs 2578, 2579, 2580, and RFCs 1905-1907. SNMPv2 has no message definition.

SNMPv2c

(Community-based SNMP version 2) an experimental SNMP Framework which supplements the SNMPv2 Framework, as described in RFC 1901. It adds the SNMPv2c message format, which is similar to the SNMPv1 message format. The second version of SNMP, it supports centralized and distributed network management strategies, and includes improvements in the Structure of Management Information (SMI), protocol operations, management architecture, and security.

SNMPv3

(SNMP version 3) an extensible SNMP Framework which supplements the SNMPv2 Framework by supporting a new SNMP message format, Security for Messages, Access Control, and Remote configuration of SNMP parameters. The SNMPv3 protocol adds encryption and authentication mechanisms into the SNMP protocol for a secure management protocol where SNMP agents can not be accessed by unauthorized parties.

SNMP View

A mapping between SNMP objects and the access rights available for those objects. An object can have different access rights in each view. Access rights indicate whether the object is accessible by either a community string or a user.

Trap

In SNMP, a trap is a type of PDU used to report an alert or other asynchronous event about a managed subsystem.

Also, a place in a program for handling unexpected or unallowable conditions - for example, by sending an error message to a log or to a program user. If a return code from another program was being checked by a calling program, a return code value that was unexpected and unplanned for could cause a branch to a trap that recorded the situation, and take other appropriate action.

An ION system trap is a one-way notification (e.g., from the IONMM to the NMS) that alerts the administrator about instances of MIB-defined asynchronous events on the managed device. It is the only operation that is initiated by the IONMM rather than the NMS. For a management system to understand a trap sent to it by the IONMM, the NMS must know what the object identifier (OID) defines. Therefore, it must have the MIB for that trap loaded. This provides the correct OID information so that the NMS can understand the traps sent to it.

Traps

One of two types of SNMP notifications that can be sent. An unsolicited message sent by an agent to a NMS to notify it of some unusual event. See also "informs".

USM

(User-Based Security Model) The SNMPv3 USM lets you implement authentication and privacy in SNMP communication between agents and managers. For example, IETF RFC 2574 defines the User-based Security Model (USM) for SNMPv3. Contrast with “VACM”.

VACM

(View-Based Access Control Model) a new security feature defined by SNMPv3. Like User-based Security Model (USM) it authenticates, encrypts, and decrypts SNMPv3 packets, as specified in RFC 2575. An SNMP entity’s Access Control subsystem checks if a specific type of access to a specific managed object is allowed. Access control occurs in the agent when processing SNMP retrieval or modification request messages from a manager, and when a notification message is sent to the manager. VACM concepts are based the problems with SNMPv1 and SNMPv2c community strings. A community string identifies the requesting entity, the location of the requesting entity, and determines access control information and MIB view information. A single community string variable provides low flexibility and functionality. VACM builds on the community string concept with a stricter, and more dynamic, more easily administered access control model. Contrast with “USM”.

Varbind

In SNMP, a sequence of two fields, an Object ID and the value for/from that Object ID. The term ‘Varbinds’ is short for Variable bindings. It’s the variable number of values that are included in an SNMP packet. Each varbind is made of an OID, type, and value.

Well Known Ethernet Multicast Addresses

Some common Ethernet multicast MAC addresses are shown below with their related Field Type and typical usage.

Ethernet Multicast Address	Usage
01-00-0C-CC-CC-CC	CDP (Cisco Discovery Protocol), VTP (VLAN Trunking Protocol)
01-00-0C-CC-CC-CD	Cisco Shared Spanning Tree Protocol Address
01-80-C2-00-00-00	Spanning Tree Protocol (for bridges) (IEEE 802.1D)
01-80-C2-00-00-01	Ethernet OAM Protocol (IEEE 802.3ah)
01-80-C2-00-00-02	IEEE Std 802.3 Slow Protocols multicast address
01-80-C2-00-00-03	IEEE Std 802.1X PAE address
01-80-C2-00-00-04	IEEE MAC-specific control protocols
01-80-C2-00-00-08	Spanning Tree Protocol (for provider bridges) (IEEE 802.1AD)
01-00-5E-xx-xx-xx	IPv4 Multicast (RFC 1112)
33-33-xx-xx-xx-xx	IPv6 Multicast (RFC 2464)

Well Known Ports

The set of all available port numbers are divided into three ranges: Well Known Ports, Registered Ports, and Dynamic and/or Private Ports. The Well Known Ports are those from 0 through 1023. The Registered Ports are those from 1024 through 49151. Registered ports require IANA registration. The Dynamic and/or Private Ports are those from 49152 through 65535. Port 443 is reserved for the HTTPS, port 179 for the BGP Border Gateway Protocol, and port 161 for SNMP.

To see all the used and listening ports on your computer, use the **netstat** (or similar) command line command. For further port assignment information, see IETF RFC 1700.

Port Number	Description
20	FTP
22	SSH Remote Login Protocol
23	Telnet
25	Simple Mail Transfer Protocol (SMTP)
53	Domain Name System (DNS)
69	Trivial File Transfer Protocol (TFTP)
80	HTTP
143	Interim Mail Access Protocol (IMAP)
161	SNMP /TCP
161	SNMP /UDP
161	SNMPTRAP /TCP
162	SNMPTRAP /UDP
179	Border Gateway Protocol (BGP)
190	Gateway Access Control Protocol (GACP)
389	Lightweight Directory Access Protocol (LDAP)
443	HTTPS
546	DHCP Client
547	DHCP Server

Write View

A view name (up to 64 characters) for each SNMP group that defines the list of object identifiers (OIDs) that are able to be created or modified by users of the group.

Writeview

A string of up to 64 characters that is the name of the view that lets you enter data and configure the contents of the agent. The default writeview is 'nothing' (i.e., the null OID). You must configure write access.

XML

(Extensible Markup Language) is a simple, very flexible text format. XML was derived from SGML (ISO 8879). XML was originally designed for large-scale electronic publishing; XML also plays an important and growing role in the exchange of a wide variety of data on the Web and elsewhere.

Index

Transition Networks
10900 Red Circle Drive
Minnetonka, MN 55343 USA
Tel: 952- 941-7600 or 1-800-526-9267
Fax: 952-941-2322

Printed in the U.S.A.

Focal Point™ 3.0 Management Application for the ION System and Point System
User Guide, 33293 Rev E