



Prisma II XD Platform

System Guide - System Release 2.03

For Your Safety

Explanation of Warning and Caution Icons

Avoid personal injury and product damage! Do not proceed beyond any symbol until you fully understand the indicated conditions.

The following warning and caution icons alert you to important information about the safe operation of this product:



You may find this symbol in the document that accompanies this product. This symbol indicates important operating or maintenance instructions.



You may find this symbol affixed to the product. This symbol indicates a live terminal where a dangerous voltage may be present; the tip of the flash points to the terminal device.



You may find this symbol affixed to the product. This symbol indicates a protective ground terminal.



You may find this symbol affixed to the product. This symbol indicates a chassis terminal (normally used for equipotential bonding).



You may find this symbol affixed to the product. This symbol warns of a potentially hot surface.



You may find this symbol affixed to the product and in this document. This symbol indicates an infrared laser that transmits intensity-modulated light and emits invisible laser radiation or an LED that transmits intensity-modulated light.

Important

Please read this entire guide. If this guide provides installation or operation instructions, give particular attention to all safety statements included in this guide.

Notices

Trademark Acknowledgments

- Cisco, the Cisco logo, Cisco Systems, the Cisco Systems logo, Scientific Atlanta, Prisma, Prisma II, and SciCare are trademarks or registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.
- *All other trademarks mentioned in this document are property of their respective owners.*

Publication Disclaimer

Cisco Systems, Inc. assumes no responsibility for errors or omissions that may appear in this publication. We reserve the right to change this publication at any time without notice. This document is not to be construed as conferring by implication, estoppel, or otherwise any license or right under any copyright or patent, whether or not the use of any information in this document employs an invention claimed in any existing or later issued patent.

Copyright

© 2008 Cisco Systems, Inc. All rights reserved. Printed in the United States of America.

Information in this publication is subject to change without notice. No part of this publication may be reproduced or transmitted in any form, by photocopy, microfilm, xerography, or any other means, or incorporated into any information retrieval system, electronic or mechanical, for any purpose, without the express permission of Cisco Systems, Inc.

Contents

Product Notices	xiii
Important Safety Instructions	xv
Laser Safety	xxv
Warning Labels	xxvii
Chapter 1 Quick Start Guide	1
Step 1: Install the Chassis in a Rack.....	2
To Install the Chassis in a Rack.....	2
Step 2: Make Chassis-to-Chassis ICIM2 Connections.....	3
Chassis-to-Chassis ICIM2 Connections	3
ICIM IN and ICIM OUT Connectors.....	3
To Make ICIM IN and ICIM OUT Cable Connections	3
ICIM IN and ICIM OUT Cables	5
Step 3: Make Electrical Power Connections	6
Electrical Power Connections.....	6
Chassis Wiring and Fusing.....	6
Power Inlet Illustration	9
To Install the Power Cord.....	9
To Install the Power Supply in the Chassis.....	10
To Share Power Between Two Chassis	11
Step 4: Install the ICIM2.....	14
To Install the ICIM2-XD.....	14
Step 5: Set Network Parameters from the Command Line Interface (CLI)	15
Step 6: Connect the ICIM2-XD to the Network	19
To Set Up a Telnet CLI Session	19
Step 7: Install Modules in the Chassis.....	20
To Install the Module	20
Step 8: Set Additional Parameters via CLI (Optional)	22
To Set Additional Users for ICIM2 or ICIM2-XD Access.....	22
Step 9: Set and Verify SNMP Community Strings	23
Step 10: Perform Chassis-to-Chassis ICIM2 Activation (Optional)	25
Step 11: Make Changes to Traps and Enterprise MIBs.....	26
MIB Software	26
Trap Overview	26
Step 12: Make Physical Connections to Modules	28
To Connect Optical Cables	28

To Connect RF Cables	28
Step 13: Verify System Release and Module Firmware Versions	29
Step 14: Install and Use the Firmware Update (SOUP) Utility (Optional)	30
To Install the SOUP on Windows.....	30
To Use the SOUP Utility	30
To Uninstall the SOUP on Windows.....	30

Chapter 2 Introduction 33

Related Publications	35
Prisma II XD Platform	36
XD Platform Components	36
XD Chassis	37
XD Chassis Fan Assembly	37
ICIM2-XD	37
Application Modules.....	37
Prisma II XD Chassis	39
Chassis Features	39
Chassis Configuration.....	41
Typical Chassis Block Diagram	42
Chassis Illustrations.....	42
Chassis Front Panel Features.....	43
Chassis Back Panel Features.....	44
Chassis Midplane.....	44
Fan Assembly	45
Midplane Bus Connectors.....	45
XD Chassis Control Board	45
Chassis Power Supply Architecture.....	47
XD Chassis Fan Assembly	51
Fan Operation.....	51
Fan Assembly Illustration.....	51
AC-to-DC Bulk Power Supply Modules.....	52
Power Sharing	52
Power Supply Configurations.....	52
Electrical Input Voltages	54
Power Inlets	54
AC-to-DC Bulk Power Supply Illustration	55
AC-to-DC Bulk Power Supply Features	55
DC-to-DC Converters.....	56
DC-to-DC Converter Illustration.....	56
Prisma II ICIM2-XD	57
ICIM2-XD Block Diagram.....	57
ICIM2-XD Illustration (Front Panel)	58
ICIM2-XD Front Panel Features.....	58

Chapter 3 Hardware Installation 59

Before You Begin.....	60
Unpacking and Inspecting the Chassis.....	60
Required Equipment and Tools.....	60
Site Requirements	61
Operating Environment.....	61
Chassis Wiring and Fusing.....	61
Rack Location Requirements.....	63
Unused Slots.....	64
Mounting the Chassis in a Rack.....	65
To Install the Chassis in a Rack.....	65
Chassis Dimensions.....	65
Connector Interface Panel.....	67
Connecting the ICIM2 to Additional Chassis	68
To Make ICIM IN and ICIM OUT Cable Connections	68
To Change the Chassis ID Number.....	69
ICIM IN and ICIM OUT Cables.....	70
Chassis-to-Chassis ICIM2 Activation.....	70
External Alarms Connections.....	72
Master-Slave Operation	72
ALARM IN and OUT Connections	72
Master-Slave Illustration.....	73
ALARM IN and OUT Terminal Blocks.....	73
Fan Assembly	74
To Remove the Fan Assembly.....	74
Installing the Power Supply	75
Power Supply Requirements.....	75
Electrical Power Connections.....	76
Chassis Wiring and Fusing.....	76
DC Power Connectors.....	78
Power Inlet Illustration	79
To Install the Power Cord.....	79
To Install the Power Supply in the Chassis.....	80
Power Supply Cooling Fans.....	81
To Install the DC-to-DC Converter	81
To Monitor the Power Supply.....	83
To Enable Power Passing.....	83
Installing the ICIM2-XD.....	85
To Install the ICIM2-XD.....	85
Installing Application Modules	86
To Install the Module	86
To Remove the Module.....	87
Connecting Optical Cables	89
To Connect Optical Cables	89

Connecting RF Cables	90
To Connect RF Cables	90

Chapter 4 Equipment Configuration 91

HyperTerminal Session Setup.....	92
To Set Up a HyperTerminal Serial Port Session	92
CLI Parameters	95
Login.....	95
To Set the Clock.....	96
To Set Additional Users for ICIM2 or ICIM2-XD Access.....	96
To Set and Verify SNMP Community Strings	97
Telnet Session	98
To Set Up a Telnet CLI Session	98
SNMP Parameters.....	100

Chapter 5 ICIM2-XD Operation 101

ICIM Introduction.....	102
Laser Warning.....	102
Overview	102
ICIM2-XD Block Diagram.....	103
ICIM Front Panel.....	104
ICIM2-XD Illustration (Front Panel)	104
ICIM2-XD Front Panel Features.....	104
Operating the ICIM2-XD	105
SNMP Considerations.....	105
Basic SNMP Setup.....	105
Default Community Strings	105
Configuring for Remote Network Access	106
Preliminary Steps for SNMP	106
Setting Trap Receive Parameters	107

Chapter 6 LCI Operation 109

LCI Introduction	110
LCI Function	110
System Requirements	111
Computer Requirements.....	111
Cable Requirements.....	111
Installing LCI.....	112
To Install the LCI Software.....	112
Connecting Your Computer to the Chassis.....	115
To Connect a Computer to the Chassis.....	115
Starting LCI Software	116
To Start LCI Software	116

LCI Module Tree	117
Module Tree.....	117
Accessing the Module Detail Information	118
Module Details Window	118
To Access the Module Details, Double-Click the Chassis.....	119
To Access the Module Details, Right-Click the Chassis	120
To Access the Module Details, Double-Click the Module	121
To Access the Module Details, Right-Click the Module.....	122
Checking the Operating Status	124
To Check the Operating Status using LCI.....	124
Configuring the Module using LCI.....	125
To Set Control Parameters using LCI.....	125
Checking the Module Alarms using LCI.....	127
To Check Alarms using LCI	127
Modifying Module Alarm Limits using LCI.....	129
To Modify Alarm Limits using LCI.....	129
Checking Manufacturing Data using LCI	131
To Check Manufacturing Data using LCI	131

Chapter 7 User Management 133

Introduction.....	134
User Accounts	134
Usernames.....	134
Passwords	135
Security Levels	135
Account Enable or Disable	135
Login Thresholds	135
User Lockout	136
Inactivity Timeout.....	136
Replacing the Default Admin Account.....	137
To Replace the Default Admin Account.....	137
Working With User Accounts	141
To Add a New User.....	141
To Change a User Password	142
To Change a User Security Level.....	143
To Change User Account Status	144
To Unlock User Accounts	145
To Delete a User Account	145
To List All Currently Logged In Users	146
User Lockout.....	148
To View the Current Lockout Interval.....	148
To Specify a New Lockout Interval.....	149
To View Locked-Out Users	150
To View Lockout Time Remaining by User	151
To Unlock a Locked-Out User.....	151

Chapter 8 Event Log 153

Introduction	154
Event Log Fields	154
Event Action IDs	155
Viewing the Event Log	157
To View the Event Log through the CLI	157
To View the Event Log through the Web Interface	158
Clearing the Event Log	159
To Clear the Event Log through the CLI	159
To Clear the Event Log through the Web Interface	159
Setting Event Log Filter Parameters	160
To View Filter Parameters through the CLI	160
To Set Filter Parameters through the CLI	160
To View Filter Parameters through the Web Interface	161
To Set Filter Parameters through the Web Interface	161
Event Log-Related Traps	162
Example: 80% Full Trap	162
Example: 100% Full Trap	163
Downloading and Viewing the Event Log Remotely	164
To Download the Event Log File	164

Chapter 9 SNMP Management 167

Introduction	168
Prisma II Enterprise MIBs	168
ICIM MIB	169
To View the ICIM MIB	169
ICIM MIB Elements	169
Event Log File Management	183
SNTP Time Synchronization	186
Trap Handling	189
Trap Recv Table	190
Trap Logging Auxiliaries	194
Trap Logging Table	194
Module MIB	199
Module MIB Tables	199
Module Table	200
Module Alarm Table	208
Alarm Severity Mappings	213
Current Alarm Table	214
Module Monitor Table	217
Module Control Table	220
Insert Module Table	223
Remove Module Table	223

Remote Reboot of ICIM2 and Modules	226
To Reboot the ICIM2 via SNMP	226
To Reboot a Module via SNMP	226
Prisma II Traps	227
About Traps	227
Trap Receiving Configuration.....	228
To Configure Trap Destination.....	229
Trap Types	230
Enhanced Trap Binding Information	241
Enhanced Trap Alarms	245
Enhanced Trap Events	248
Alarm Threshold Modification	265
System Behavior	267
ICIM2 as Proxy for Module Information.....	267
Delay in the Discovery Process.....	267
Module Removal and Enhanced Traps	267
Frequently Asked Questions.....	268
How do I configure trap destination?.....	268
Why do the same alarm values represent different conditions?.....	268
How do Enhanced Traps differ from other trap types?	269
When do traps associated with module insertion, removal, and alarms occur?.....	269
Where can I find trap definitions?.....	270
What is the Trap Logging Table?.....	270

Chapter 10 Remote Firmware Download Feature 271

Installing the SOUP	272
To Install SOUP on Windows	272
To Uninstall the SOUP on Windows.....	272
Concepts.....	273
The Chassis and the ICIM2.....	273
Release Files.....	273
Active and Inactive Flash.....	273
Concurrency	274
Integration with an NMS (Optional).....	274
Usage	275
Launching Standalone (Windows Only)	275
SOUP Main Screen.....	277
Firmware Upgrade Process	279
FTP Settings	281
SNMP Settings.....	282
FTP Server	283

Firmware Updates	284
------------------------	-----

Chapter 11 Maintenance and Troubleshooting 287

Maintenance.....	289
Maintenance Record	289
Troubleshooting	290
Chassis Troubleshooting.....	290
Alarm Troubleshooting.....	291
Additional Assistance	291
Fan Ok Alarms	292
Fan Alarm Parameters	292
Suggested Actions.....	292
ChasTemp Alarm.....	293
ChasTemp Alarm Parameters.....	293
Suggested Actions.....	293
ConvAIn Alarm.....	294
ConvAIn Alarm Parameters.....	294
Suggested Actions.....	294
ConvA+24 Alarm.....	295
ConvA+24 Alarm Parameters.....	295
Suggested Actions.....	295
To Access the DC-to-DC Converter	295
ConvA+5 Alarm.....	297
ConvA+5 Alarm Parameters.....	297
Suggested Actions.....	297
To Access the DC-to-DC Converter	297
ConvA-5 Alarm.....	299
ConvA-5 Alarm Parameters	299
Suggested Actions.....	299
To Access the DC-to-DC Converter	299
ConvBIn Alarm	301
ConvBIn Alarm Parameters	301
Suggested Actions.....	301
ConvB+24 Alarm.....	302
ConvB+24 Alarm Parameters.....	302
Suggested Actions.....	302
To Access the DC-to-DC Converter	302
ConvB+5 Alarm.....	304
ConvB+5 Alarm Parameters.....	304
Suggested Actions.....	304
To Access the DC-to-DC Converter	304
ConvB-5 Alarm.....	306
ConvB-5 Alarm Parameters.....	306
Suggested Actions.....	306
To Access the DC-to-DC Converter	306

Cleaning Optical Connectors	308
Recommended Equipment	308
Tips for Optimal Fiber-Optic Connector Performance	308
To Clean Optical Connectors	309
Fiber Optic Connector Cleaning Instructions	309
Connecting Optical Cables	312
To Connect Optical Cables	312

Chapter 12 Customer Support Information 313

Obtaining Product Support	314
Support Telephone Numbers	314
Return Product for Repair	316
Obtaining an RMA Number and Shipping Address	316
Completing the Scientific Atlanta Transmission Networks Repair Tag	317
Packing and Shipping the Product	320

Appendix A Prisma II Permitted CLI Commands 323

From CLI	324
From ICIM	325
From */* MODULE	331
From TERMINAL	334

Appendix B Features Available via Remote User Interface 335

Overview	336
ICIM Data	337
Module Data	340
Current Alarms	341
Module Alarms	342
Module Controls	343
Module Monitors	344
System Information	345
User Management	346

Appendix C Module Parameter Descriptions 347

XD Chassis Parameters	348
XD Chassis Configurable Parameters	348
XD Chassis Alarm Data Parameters	348
XD Chassis Operating Status Parameters	349
XD Chassis Manufacturing Data Parameters	349

Contents

Glossary	351
Index	359

Product Notices

System Release

The information in this guide pertains to Prisma II XD Platform System Release 2.03.02 and ICIM2-XD Firmware Release 2.03.01.

Operating Temperature

**CAUTION:**

The warranty may be voided and the equipment damaged if you operate the equipment outside the specified temperature limits (32 to 122°F or 0 to 50°C). Specification temperature limits are measured in the air stream at the fan tray inlet and may be higher than room ambient temperature.

Important Safety Instructions

Read and Retain Instructions

Carefully read all safety and operating instructions before operating this equipment, and retain them for future reference.

Follow Instructions and Heed Warnings

Follow all operating and use instructions. Pay attention to all warnings and cautions in the operating instructions, as well as those that are affixed to this equipment.

Terminology

The terms defined below are used in this document. The definitions given are based on those found in safety standards.

Service Personnel - The term *service personnel* applies to trained and qualified individuals who are allowed to install, replace, or service electrical equipment. The service personnel are expected to use their experience and technical skills to avoid possible injury to themselves and others due to hazards that exist in service and restricted access areas.

User and Operator - The terms *user* and *operator* apply to persons other than service personnel.

Ground(ing) and Earth(ing) - The terms *ground(ing)* and *earth(ing)* are synonymous. This document uses *ground(ing)* for clarity, but it can be interpreted as having the same meaning as *earth(ing)*.

Electric Shock Hazard

This equipment meets applicable safety standards.



WARNING:

To reduce risk of electric shock, perform only the instructions that are included in the operating instructions. Refer all servicing to qualified service personnel only.

Electric shock can cause personal injury or even death. Avoid direct contact with dangerous voltages at all times. The protective ground connection, where provided, is essential to safe operation and must be verified before connecting the power supply.

Know the following safety warnings and guidelines:

- Dangerous Voltages

Important Safety Instructions

- Only qualified service personnel are allowed to perform equipment installation or replacement.
- Only qualified service personnel are allowed to remove chassis covers and access any of the components inside the chassis.
- **Grounding**
 - Prisma II equipment is suitable for installation as part of the common bonding network (CBN).
 - Do not violate the protective grounding by using an extension cable, power cable, or autotransformer without a protective ground conductor.
 - Take care to maintain the protective grounding of this equipment during service or repair and to re-establish the protective grounding before putting this equipment back into operation.

Note: See the Installation section of this document for specific information regarding the AC and DC power, wiring, fusing, and grounding requirements for this product.

Installation Site

When selecting the installation site, comply with the following:

- **Protective Ground** - The protective ground lead of the building's electrical installation should comply with national and local requirements.
- **Environmental Condition** - The installation site should be dry, clean, and ventilated. Do not use this equipment where it could be at risk of contact with water. Ensure that this equipment is operated in an environment that meets the requirements as stated in this equipment's technical specifications, which may be found on this equipment's data sheet.

Installation Requirements



WARNING:

Allow only qualified service personnel to install this equipment. The installation must conform to all local codes and regulations.

Equipment Placement



WARNING:

Avoid personal injury and damage to this equipment. An unstable mounting surface may cause this equipment to fall.

Prisma II equipment is suitable for installation in network telecommunications facilities.

To protect against equipment damage or injury to personnel, comply with the following:

- Install this equipment in a restricted access location.
- Do not install near any heat sources such as radiators, heat registers, stoves, or other equipment (including amplifiers) that produce heat.
- Place this equipment close enough to a DC input voltage source to accommodate the length of this equipment's power cord.
- Route all power cords so that people cannot walk on, place objects on, or lean objects against them. This may pinch or damage the power cords. Pay particular attention to power cords at plugs, outlets, and the points where the power cords exit this equipment.
- Use only with a cart, stand, tripod, bracket, or table specified by the manufacturer, or sold with this equipment.
- Make sure the mounting surface or rack is stable and can support the size and weight of this equipment.
- The mounting surface or rack should be appropriately anchored according to manufacturer's specifications. Ensure this equipment is securely fastened to the mounting surface or rack where necessary to protect against damage due to any disturbance and subsequent fall.

Ventilation

This equipment has openings for ventilation to protect it from overheating. To ensure equipment reliability and safe operation, do not block or cover any of the ventilation openings. Install the equipment in accordance with the manufacturer's instructions.

Rack Mounting Safety Precautions

Mechanical Loading

Make sure that the rack is placed on a stable surface. If the rack has stabilizing devices, install these stabilizing devices before mounting any equipment in the rack.



WARNING:

Avoid personal injury and damage to this equipment. Mounting this equipment in the rack should be such that a hazardous condition is not caused due to uneven mechanical loading.

Important Safety Instructions

Reduced Airflow

When mounting this equipment in the rack, do not obstruct the cooling airflow through the rack. Be sure to mount the blanking plates to cover unused rack space. Additional components such as combiners and net strips should be mounted at the back of the rack, so that the free airflow is not restricted.



CAUTION:

Installation of this equipment in a rack should be such that the amount of airflow required for safe operation of this equipment is not compromised.

Elevated Operating Ambient Temperature

Only install this equipment in a humidity- and temperature-controlled environment that meets the requirements given in this equipment's technical specifications.



CAUTION:

If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient temperature. Therefore, install this equipment in an environment compatible with the manufacturer's maximum rated ambient temperature.

Handling Precautions

When moving a cart that contains this equipment, check for any of the following possible hazards:



WARNING:




Avoid personal injury and damage to this equipment! Move any equipment and cart combination with care. Quick stops, excessive force, and uneven surfaces may cause this equipment and cart to overturn.

- Use caution when moving this equipment/cart combination to avoid injury from tip-over.
- If the cart does not move easily, this condition may indicate obstructions or cables that may need to be disconnected before moving this equipment to another location.
- Avoid quick stops and starts when moving the cart.
- Check for uneven floor surfaces such as cracks or cables and cords.

Grounding

If this equipment is equipped with an external grounding terminal, attach one end of an 18-gauge wire (or larger) to the grounding terminal; then, attach the other end of the wire to a ground, such as a grounded equipment rack.

Equipotential Bonding

If this equipment is equipped with an external chassis terminal marked with the IEC 60417-5020 chassis icon () , the installer should refer to CENELEC standard EN 50083-1 or IEC standard IEC 60728-11 for correct equipotential bonding connection instructions.

Connection to IT Power Systems

This equipment has been tested for IT power systems 240 VAC phase-to-phase.

Connection to -48 V DC/-60 V DC Power Sources

If this equipment is DC-powered, refer to the specific installation instructions in this manual or in companion manuals in this series for information on connecting this equipment to nominal -48 V DC/-60 V DC power sources.

Circuit Overload

Know the effects of circuit overloading before connecting this equipment to the power supply.



CAUTION:

Consider the connection of this equipment to the supply circuit and the effect that overloading of circuits might have on overcurrent protection and supply wiring. Refer to the information on the equipment-rating label when addressing this concern.

General Servicing Precautions



WARNING:

Avoid electric shock! Opening or removing this equipment's cover may expose you to dangerous voltages.



CAUTION:

These servicing precautions are for the guidance of qualified service personnel only. To reduce the risk of electric shock, do not perform any servicing other than that contained in the operating instructions unless you are qualified to do so. Refer all servicing to qualified service personnel.

Be aware of the following general precautions and guidelines:

- **Servicing** - Servicing is required when this equipment has been damaged in any way, such as power supply cord or plug is damaged, liquid has been spilled or objects have fallen into this equipment, this equipment has been exposed to rain or moisture, does not operate normally, or has been dropped.
- **Wristwatch and Jewelry** - For personal safety and to avoid damage of this

Important Safety Instructions

equipment during service and repair, do not wear electrically conducting objects such as a wristwatch or jewelry.

- **Lightning** - Do not work on this equipment, or connect or disconnect cables, during periods of lightning.
- **Labels** - Do not remove any warning labels. Replace damaged or illegible warning labels with new ones.
- **Covers** - Do not open the cover of this equipment and attempt service unless instructed to do so in the instructions. Refer all servicing to qualified service personnel only.
- **Moisture** - Do not allow moisture to enter this equipment.
- **Cleaning** - Use a damp cloth for cleaning.
- **Safety Checks** - After service, assemble this equipment and perform safety checks to ensure it is safe to use before putting it back into operation.

Electrostatic Discharge

Electrostatic discharge (ESD) results from the static electricity buildup on the human body and other objects. This static discharge can degrade components and cause failures.

Take the following precautions against electrostatic discharge:

- Use an anti-static bench mat and a wrist strap or ankle strap designed to safely ground ESD potentials through a resistive element.
- Keep components in their anti-static packaging until installed.
- Avoid touching electronic components when installing a module.

Fuse Replacement

To replace a fuse, comply with the following:

- Disconnect the power before changing fuses.
- Identify and clear the condition that caused the original fuse failure.
- Always use a fuse of the correct type and rating. The correct type and rating are indicated on this equipment.

Batteries

This product may contain batteries. Special instructions apply regarding the safe use and disposal of batteries:

Safety

- Insert batteries correctly. There may be a risk of explosion if the batteries are incorrectly inserted.
- Do not attempt to recharge 'disposable' or 'non-reusable' batteries.
- Please follow instructions provided for charging 'rechargeable' batteries.
- Replace batteries with the same or equivalent type recommended by manufacturer.
- Do not expose batteries to temperatures above 100°C (212°F).

Disposal

- The batteries may contain substances that could be harmful to the environment
- Recycle or dispose of batteries in accordance with the battery manufacturer's instructions and local/national disposal and recycling regulations.



廢電池請回收

- The batteries may contain perchlorate, a known hazardous substance, so special handling and disposal of this product might be necessary. For more information about perchlorate and best management practices for perchlorate-containing substance, see www.dtsc.ca.gov/hazardouswaste/perchlorate.

Modifications

This equipment has been designed and tested to comply with applicable safety, laser safety, and EMC regulations, codes, and standards to ensure safe operation in its intended environment. Refer to this equipment's data sheet for details about regulatory compliance approvals.

Do not make modifications to this equipment. Any changes or modifications could void the user's authority to operate this equipment.

Modifications have the potential to degrade the level of protection built into this equipment, putting people and property at risk of injury or damage. Those persons making any modifications expose themselves to the penalties arising from proven non-compliance with regulatory requirements and to civil litigation for compensation in respect of consequential damages or injury.

Accessories

Use only attachments or accessories specified by the manufacturer.

Electromagnetic Compatibility Regulatory Requirements

This equipment meets applicable electromagnetic compatibility (EMC) regulatory requirements. Refer to this equipment's data sheet for details about regulatory compliance approvals. EMC performance is dependent upon the use of correctly shielded cables of good quality for all external connections, except the power source, when installing this equipment.

- Ensure compliance with cable/connector specifications and associated installation instructions where given elsewhere in this manual.

Otherwise, comply with the following good practices:

- Multi-conductor cables should be of single-braided, shielded type and have conductive connector bodies and backshells with cable clamps that are conductively bonded to the backshell and capable of making 360° connection to the cable shielding. Exceptions from this general rule will be clearly stated in the connector description for the excepted connector in question.
- Ethernet cables should be of single-shielded or double-shielded type.
- Coaxial cables should be of the double-braided shielded type.

EMC Compliance Statements

Where this equipment is subject to USA FCC and/or Industry Canada rules, the following statements apply:

FCC Statement for Class A Equipment

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when this equipment is operated in a commercial environment.

This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case users will be required to correct the interference at their own expense.

Industry Canada - Industrie Canadienne Statement

This apparatus complies with Canadian ICES-003.
Cet appareil est conforme à la norme NMB-003 du Canada.

CENELEC/CISPR Statement with Respect to Class A Information Technology Equipment

This is a Class A equipment. In a domestic environment this equipment may cause radio interference in which case the user may be required to take adequate measures.

Laser Safety

Introduction

This equipment contains an infrared laser that transmits intensity-modulated light and emits invisible radiation.

Warning: Radiation



WARNING:

- Avoid personal injury! Use of controls, adjustments, or procedures other than those specified herein may result in hazardous radiation exposure.
 - Avoid personal injury! The laser light source on this equipment (if a transmitter) or the fiber cables connected to this equipment emit invisible laser radiation. Avoid direct exposure to the laser light source.
 - Avoid personal injury! Viewing the laser output (if a transmitter) or fiber cable with optical instruments (such as eye loupes, magnifiers, or microscopes) may pose an eye hazard.
-
- Do not apply power to this equipment if the fiber is unmated or unterminated.
 - Do not stare into an unmated fiber or at any mirror-like surface that could reflect light emitted from an unterminated fiber.
 - Do not view an activated fiber with optical instruments (e.g., eye loupes, magnifiers, microscopes).
 - Use safety-approved optical fiber cable to maintain compliance with applicable laser safety requirements.

Warning: Fiber Optic Cables



WARNING:

Avoid personal injury! Qualified service personnel may only perform the procedures in this manual. Wear safety glasses and use extreme caution when handling fiber optic cables, particularly during splicing or terminating operations. The thin glass fiber core at the center of the cable is fragile when exposed by the removal of cladding and buffer material. It easily fragments into glass splinters. Using tweezers, place splinters immediately in a sealed waste container and dispose of them safely in accordance with local regulations.

Safe Operation for Software Controlling Optical Transmission Equipment

If this manual discusses software, the software described is used to monitor and/or control ours and other vendors' electrical and optical equipment designed to transmit video, voice, or data signals. Certain safety precautions must be observed when operating equipment of this nature.

For equipment specific safety requirements, refer to the appropriate section of the equipment documentation.

For safe operation of this software, refer to the following warnings.



WARNING:

- Ensure that all optical connections are complete or terminated before using this equipment to remotely control a laser device. An optical or laser device can pose a hazard to remotely located personnel when operated without their knowledge.
- Allow only personnel trained in laser safety to operate this software. Otherwise, injuries to personnel may occur.
- Restrict access of this software to authorized personnel only.
- Install this software in equipment that is located in a restricted access area.

Warning Labels

The following illustrations display the warning labels on this equipment.



TP492

This device has multiple power entry points.
Disconnect the appropriate power connection(s) before servicing. Refer to
Installation / Operator's Guide for power distribution details.

Ce dispositif a les points d'entrée multiples de puissance. Débranchez les
raccordements de puissance appropriés avant l'entretien. Référez-vous au
manual de l'opérateur pour des détails de distribution d'énergie. PN 4023663

T13331

1

Quick Start Guide

Introduction

This chapter provides streamlined step-by-step instructions for installing and configuring the platform hardware and firmware. Later chapters of this guide provide more detailed information on platform design, operation, and maintenance.

In This Chapter

- Step 1: Install the Chassis in a Rack..... 2
- Step 2: Make Chassis-to-Chassis ICIM2 Connections..... 3
- Step 3: Make Electrical Power Connections 6
- Step 4: Install the ICIM2..... 14
- Step 5: Set Network Parameters from the Command Line Interface (CLI) 15
- Step 6: Connect the ICIM2-XD to the Network 19
- Step 7: Install Modules in the Chassis..... 20
- Step 8: Set Additional Parameters via CLI (Optional) 22
- Step 9: Set and Verify SNMP Community Strings 23
- Step 10: Perform Chassis-to-Chassis ICIM2 Activation (Optional) 25
- Step 11: Make Changes to Traps and Enterprise MIBs..... 26
- Step 12: Make Physical Connections to Modules 28
- Step 13: Verify System Release and Module Firmware Versions..... 29
- Step 14: Install and Use the Firmware Update (SOUP) Utility (Optional) 30

Step 1: Install the Chassis in a Rack

To Install the Chassis in a Rack

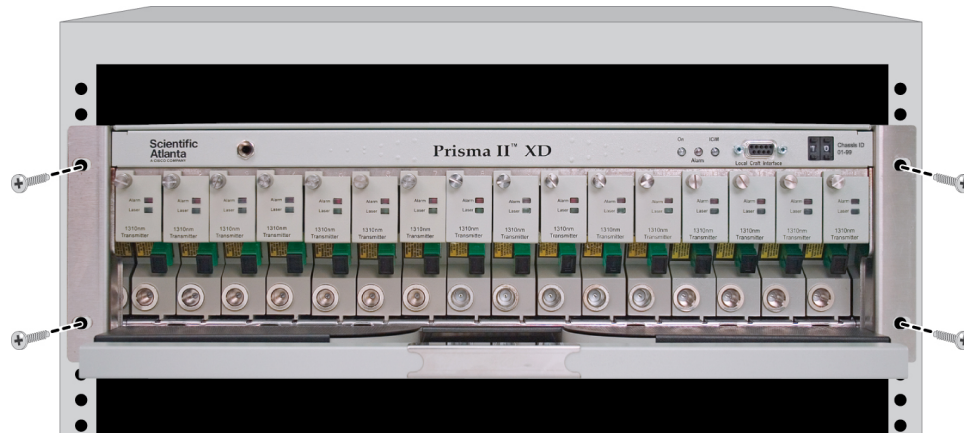


WARNING:

The Prisma II XD Chassis weighs approximately 25 lbs (11.3 kg) empty and 40 lbs (18.1 kg) fully loaded. To avoid personal injury and equipment damage, use safe handling and lifting practices in accordance with your organization's procedures.

Complete the following steps to mount the chassis in a 19-inch rack.

- 1 Use a torque wrench to tighten the bracket mounting screws to 12 to 14 in-lbs (1.36 to 1.58 Nm).
- 2 Position the chassis in the rack with the fan assembly installed, but otherwise empty.
- 3 Insert a mounting screw through each of the four mounting holes on chassis front panel, and then into the rack.



T13303

- 4 Use a medium-sized Phillips-head screwdriver to tighten each mounting screw until it is tight.
- 5 Install additional cable and fiber management hardware as needed and in accordance with local practice.

Step 2: Make Chassis-to-Chassis ICIM2 Connections

Chassis-to-Chassis ICIM2 Connections

This platform allows an ICIM2 or ICIM2-XD located in one chassis to monitor and control application modules located in several other chassis. To establish chassis-to-chassis ICIM2 communication, use the **ICIM IN** and **ICIM OUT** connectors located on the chassis interface panel.

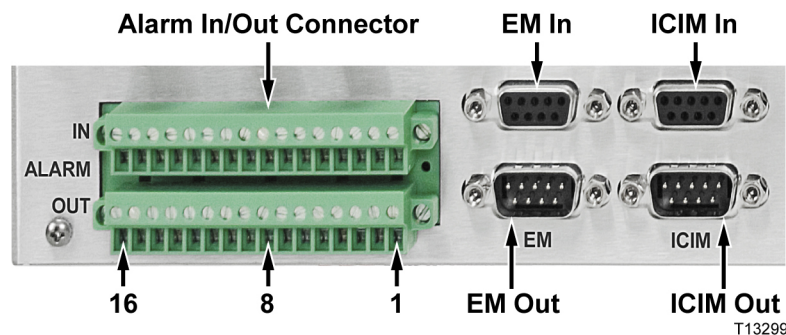
Complete the following steps to establish chassis-to-chassis ICIM2 communication:

- 1 Connect a cable from **ICIM OUT** on the chassis containing the ICIM2 or ICIM2-XD to **ICIM IN** on the second chassis.
- 2 If required, connect a second cable from **ICIM OUT** on the second chassis to **ICIM IN** on the third chassis.
- 3 If required, connect a third cable from **ICIM OUT** on the third chassis to **ICIM IN** on the fourth chassis.

Note: An ICIM2 or ICIM2-XD can control up to 64 application modules in a chassis daisy-chain of no more than 4 chassis.

ICIM IN and ICIM OUT Connectors

Every chassis has a DB9 **ICIM IN** and a DB9 **ICIM OUT** connector for the purpose of chassis-to-chassis ICIM connections. **ICIM IN** is a female connector and **ICIM OUT** is a male connector.

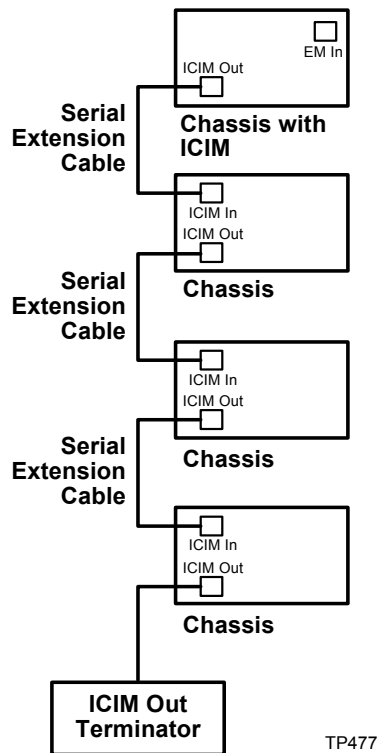


To Make ICIM IN and ICIM OUT Cable Connections

Complete the following steps to make chassis-to-chassis **ICIM IN** and **ICIM OUT** connections.

- 1 Connect the serial extension cable from the **ICIM OUT** of the chassis containing the ICIM2 or ICIM2-XD to the **ICIM IN** connector of the second chassis.

- 2 Change the chassis ID numbers as needed to give each chassis an appropriate unique ID number. See **To Change the Chassis ID Number** below for further details.
- 3 Connect a serial extension cable from the **ICIM OUT** of the second chassis to the **ICIM IN** of the third chassis.
- 4 Continue this daisy-chain connection until all chassis are connected.
- 5 The ICIM OUT port of the last chassis in the daisy-chain must be terminated with an ICIM OUT terminator, part number 4013014, which ships with the ICIM2 or ICIM2-XD.



Note:

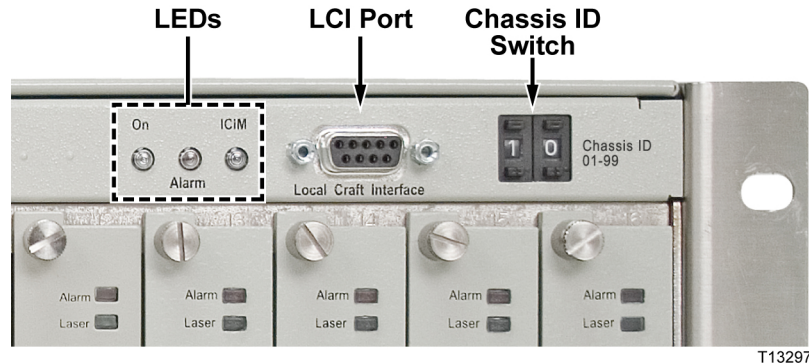
- All chassis connected in this daisy-chain must be powered and have a fan tray or fan assembly installed. For correct operation, proper cooling of the chassis must be maintained over the specified temperature range.
- A single chassis equipped with an ICIM2 or ICIM2-XD must also have its ICIM OUT port terminated with an ICIM OUT terminator, part number 4013014. The ICIM OUT terminator ships with the ICIM2 or ICIM2-XD.

To Change the Chassis ID Number

Complete the following steps to change the chassis ID number.

Step 2: Make Chassis-to-Chassis ICIM2 Connections

- 1 Locate the chassis ID switch at upper right on the front panel of each chassis. The switch can be set to any two-digit value from 00 to 99 (but avoid setting the value to 00, as explained below).



- 2 Use the chassis ID switch to set each chassis ID number to a unique value.

Note:

- The chassis ID number can be changed while the chassis is under power. However, the new ID number will not become effective until chassis power is cycled or the ICIM2-XD is rebooted.
- The chassis numbering scheme used is discretionary, except that each interconnected chassis must have a unique ID number.
- It is important to avoid using chassis ID number 00 in some circumstances, as explained in the following caution.



CAUTION:

Setting the chassis ID to 00 is not recommended as it causes the entity MIB to violate RFC-2737 by creating an invalid object identifier. This may affect operation with some management systems that use the entity MIB. In particular, attempts to access the fans (in virtual slot 0) in chassis 00 will fail if made via serial TNCS (or ROSA-EM) or LCI.

Important: If you change the chassis ID number while the chassis is under power, you must cycle power to the chassis or reboot the ICIM2-XD in order for the new number to take effect.

ICIM IN and ICIM OUT Cables

The cable required for both **ICIM IN** and **ICIM OUT** connections is a shielded 9-wire serial extension cable, DB9 Female to DB9 Male. This cable can be purchased locally or from the factory. The chassis data sheet lists the part number for a 6-foot DB9 Female to DB9 Male serial extension cable. The connectors are a serial 9-pin D-shell (EIA 574/232).

Step 3: Make Electrical Power Connections

Electrical Power Connections

The chassis back panel has an IEC standard AC power inlet and a three-conductor DC power connector for each bulk DC power supply module slot.

- The AC power inlet accepts line voltage at 100 to 240 VAC, 50 or 60 Hz.
- The DC power connector accepts DC input voltage at -40 to -72 VDC (-48 VDC nominal).

The power connectors on the left side of the chassis supply power to the left power supply slot, while those on the right supply power to the right power supply slot. Except for their chassis ground pins, all four power connectors are electrically independent of each other.

Important: Tie the system to earth ground via the ground stud.

Note: For DC power supplies, the return terminal is an "isolated DC return," i.e., it is not connected to the chassis framework.

Chassis Wiring and Fusing

Important: All chassis configurations require an external fuse or circuit breaker (AC and DC current ratings differ; see below) and #16 AWG wiring for both power and grounding.

AC Power Systems

AC power for each AC-to-DC bulk power supply module enters the chassis through a dedicated back-panel IEC power inlet for each power supply module.

Confirm that the IEC power cord or cords supplied with the chassis have the correct plug configuration for the country of use.

The voltage input range for AC systems is 100 to 240 VAC, single phase, 50-60 Hz.

AC input current is 14 A maximum. The chassis should be connected to a single outlet circuit with fuse or circuit breaker overcurrent protection rated 15 A minimum.

Important:

- Use only a grounded electrical outlet when connecting the unit to a power source. If you do not know whether the outlet is grounded, consult with a qualified electrician.
- Maintain reliable earth grounding of rack-mounted equipment. Pay particular attention to supply and ground connections made via power strips or any

method other than direct connection to the branch circuit.

DC Power Systems

External -48 VDC operating power for each DC-to-DC converter (mounted in the chassis just behind the fan assembly) enters the chassis via a dedicated DC power inlet mounted on the chassis back panel.

The voltage input range for DC power systems is -40 VDC to -72 VDC.

Use #16 AWG wire for DC field wiring. The #16 AWG wiring from the external -48 VDC supply is attached to a 3-pin nylon connector which, in turn, plugs into the DC power inlet.

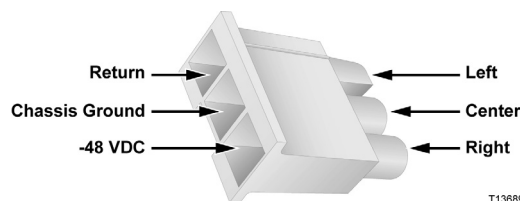
Terminate the chassis side of the cable with a nylon plug of the type supplied with the chassis. Order additional nylon plugs and connector pins from your preferred supplier, as follows:

- Molex #03-12-1036 nylon 3-pin connector
- Molex #18-12-1222 crimp socket contact (3)

Use a Molex Crimp Service Tool #63811-1000 or equivalent to crimp the pins to the cable.

After terminating the cable, twist the conductors loosely (a full turn every few inches is sufficient).

As installed in the DC power connector with the locking tab down, the left pin of the nylon connector is the return, the right pin carries -48 VDC, and the center pin is chassis ground.



Connect the chassis to a reliably grounded DC power source that is electrically isolated from the AC power source.

Important:

- Branch circuit overcurrent protection must be provided by a fuse or circuit breaker with a voltage rating of 72 VDC minimum and a current rating of 18 A maximum.
- The DC field wiring must include a readily accessible disconnect device that is suitably approved and rated.

Earth-Grounding Conditions

The chassis is designed to permit connection of the earthed conductor of the DC supply circuit to chassis ground. Before making this connection, confirm that all of the following conditions are met:

- The chassis is connected directly to the DC supply system earthing electrode conductor or to a bonding jumper from an earthing terminal bar or bus to which the DC supply system earthing electrode conductor is connected.
- The chassis is located in the same immediate area as other equipment connected between the earthed conductor of the same DC supply circuit and earthing conductor, such as in an adjacent cabinet. Also, the point of earthing of the DC system must not be earthed elsewhere.
- The DC power source is located within the same premises as the chassis.
- There are no switching or disconnecting devices in the earthed circuit conductor between the DC source and the point of connection of the earthing electrode conductor.

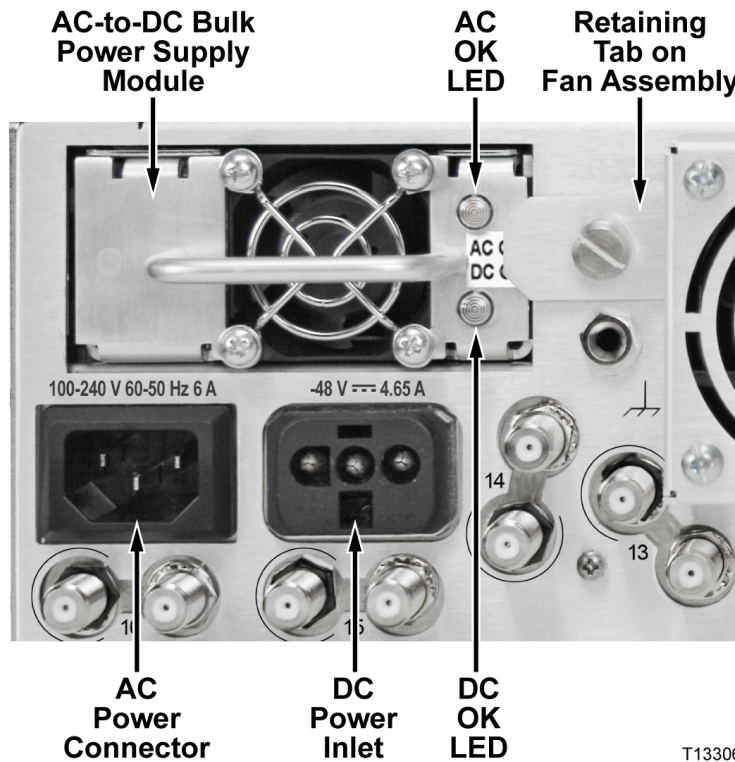
DC Power Passing

An XD chassis with at least one AC-to-DC bulk power supply module installed can serve as an external DC power source for a second XD chassis. Passing DC power from one chassis to another requires a DC power-passing cable made up as described above, but with both ends of the cable terminated by a nylon DC power connector. Two assembled DC power-passing cables are also available from the factory:

- Part number 4011730, 3 m DC power-passing cable
- Part number 4023718, 2 ft DC power-passing cable

Power Inlet Illustration

The following illustration shows locations of the AC and DC power connectors on the chassis back panel.



T13306

To Install the Power Cord

AC Power Cord

Important: The XD chassis is not supplied with an AC power cord. To complete this procedure, you must order the correct power cord for your region. For ordering information, see the *Prisma II XD Platform Data Sheet*, part number 7012804.

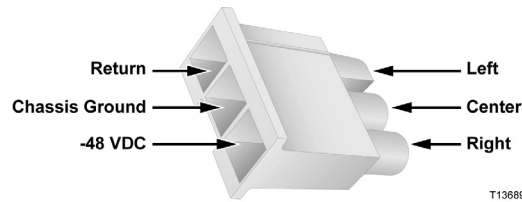
Complete the following steps to install an AC power cord for each bulk power supply module.

- 1 Confirm the location(s) of bulk power supply modules installed in slot A or slot B, or both A and B.
- 2 Insert the IEC plug of each AC power cord into the back-panel IEC power inlet for each installed bulk DC power supply module.
- 3 Attach the plug end of each AC power cord into an AC power receptacle.

DC Power Cord

Complete the following steps to install one or more DC power cords for each unused bulk DC power supply slot as needed.

- 1 Confirm that each unused bulk power supply slot is empty and covered by a blanking panel.
- 2 Locate the DC wire terminal block (white nylon plug) pre-installed in each back-panel DC power connector.
- 3 Remove the terminal block and note the locations of the left, middle, and right terminals as shown below.



- 4 Obtain conductive pins (Molex #18-12-1222) for each DC wire terminal block for each conductor to be used.
- 5 Attach #16 AWG power cable from the fuse panel to the pins and install them in the terminal block as follows:
 - Left terminal: Return conductor
 - Middle terminal: Chassis ground (optional)
 - Right terminal: -48 VDC conductor
- 6 Insert the wire terminal block into the DC power connector until it locks. Tug lightly on the terminal block to confirm that it is locked in position.
- 7 Twist the conductors loosely along the full length of the power cord (a full turn every few inches is sufficient).

To Install the Power Supply in the Chassis

Complete the following steps to install an AC-to-DC bulk power supply module in an available chassis slot.



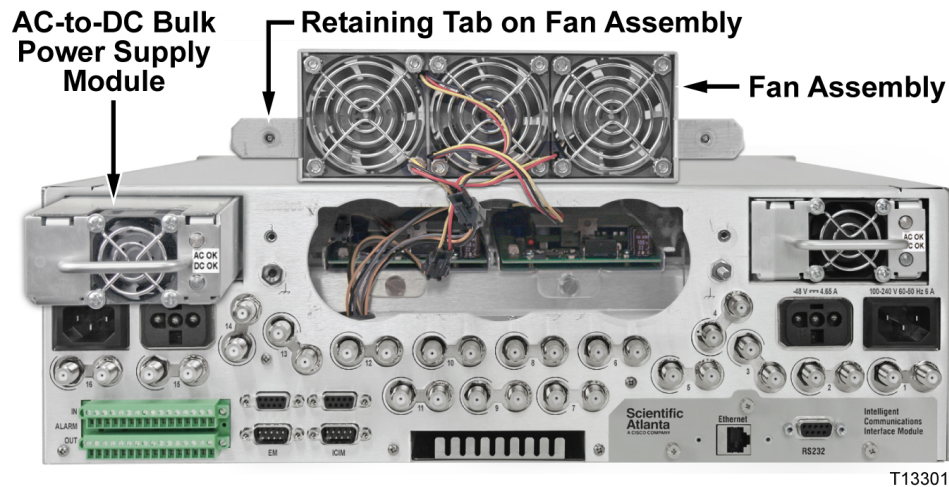
CAUTION:

Always use a screwdriver to loosen or tighten the screws holding the application modules, ICIM2-XD, fan assembly, power supply modules, DC-to-DC converters, or blanking panels in place. Do not attempt to loosen or tighten these screws solely by hand.

- 1 On the chassis back panel, loosen the two screws holding the fan assembly in place. Remove the fan assembly and set it aside temporarily.
- 2 Remove the blanking panel that covers the bulk power supply slot opening.

Step 3: Make Electrical Power Connections

- Pick up the bulk power supply module by its handle and insert the module into the open module slot, as shown in the following illustration.



- Gently slide the power supply module into the chassis until its power connections join connectors on the midplane bus. *Do not force the module into the chassis.* If properly aligned, it should slide in with minimal force.
- If installing a second power supply, repeat the steps above for the second power supply slot, and then continue with step 6.
- Confirm that a DC-to-DC converter assembly is installed inside the chassis next to the new bulk power supply module. This converter will be visible inside the fan opening, mounted horizontally and held in place by a retaining screw.
- Reinstall the fan assembly and tighten the two screws holding it and the power supply module(s) in position.
- Apply power and verify that the green LED on the front panel of each power supply module illuminates, indicating normal operation.
- Confirm that the fan assembly is operational. The fans should be audible once the power supply is operating.

To Share Power Between Two Chassis

You can set up two XD chassis so that the first operates from AC power and supplies -48 VDC to the second. This obviates the need for a second bulk DC power supply module or pair of modules.

The following instructions assume that the first chassis contains two bulk DC power supply modules.

Complete the following steps to configure two XD chassis for power sharing:

- If necessary, disconnect AC power from the supply chassis by unplugging the AC power cords from the AC line.
- Confirm that the second chassis power supply slot(s) are both empty and covered by blank panels.



CAUTION:

To preserve proper airflow within the chassis, all unused slots must be covered by suitable blanking panels, as follows:

- AC-to-DC bulk power supply module blanking panel, part number 4021618
- ICIM2-XD module blanking panel, part number 4021163
- Prisma II XD application module blanking panel, part number 4023066

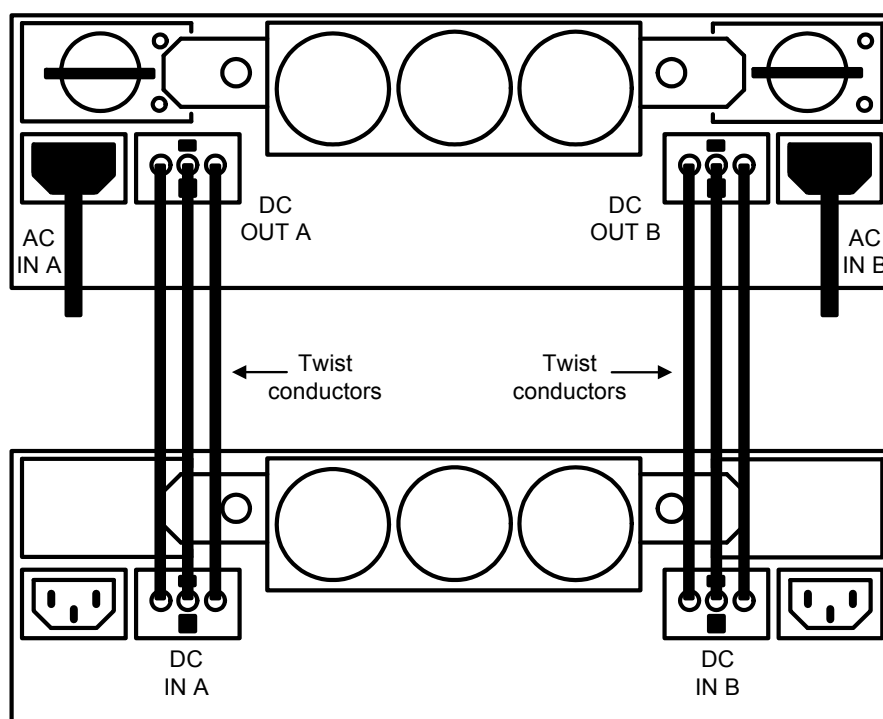
Failure to observe this precaution may result in equipment malfunction or reduced operating life due to overheating.

- 1 Connect a DC power-passing cable from DC power connector A of the first chassis to DC power connector A of the second chassis, as shown below.
- 2 Connect a second DC power-passing cable from DC power connector B of the first chassis to DC power connector B of the second chassis, as shown below.



CAUTION:

When connecting chassis together for power sharing, use either a factory DC power-passing cable, part number 4011730 (3 m) or 4023718 (2 ft), or a custom cable made in accordance with the instructions in this document. Use of other cables for this purpose is not supported.



TP476

Step 3: Make Electrical Power Connections

Note: The steps described above assume that the first chassis contains two AC-to-DC bulk power supply modules. This is the recommended configuration, as it provides redundancy in the event of failure of one bulk power supply module or of one DC-to-DC converter in either or both chassis. Other power configurations are possible. To request further information, see *Customer Support Information* (on page 313).

Step 4: Install the ICIM2

To Install the ICIM2-XD

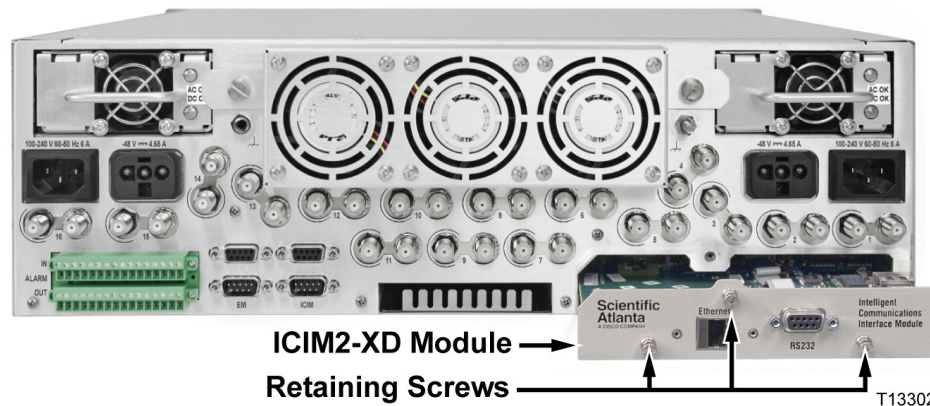
Complete the following steps to install the ICIM2-XD in the chassis.



CAUTION:

Always use a screwdriver to loosen or tighten the screws holding the application modules, ICIM2-XD, fan assembly, power supply modules, DC-to-DC converters, or blanking panels in place. Do not attempt to loosen or tighten these screws solely by hand.

- 1 Remove the blanking panel covering the ICIM slot in the lower right corner of the chassis back panel.
- 2 Hold the ICIM2-XD so that the front panel silkscreen is in correct reading position.
- 3 Align the two ridges on the bottom of the ICIM2-XD with the module guide slots located in the chassis.



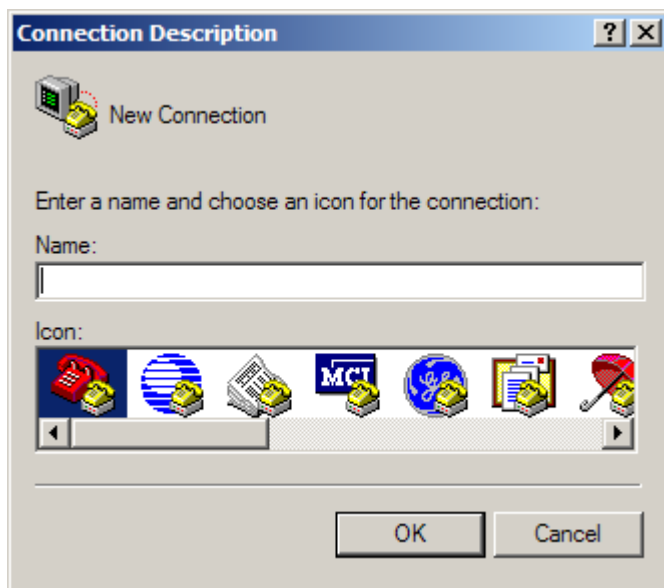
- 4 Gently slide the ICIM2-XD into the chassis until its power and communications connections join connectors on the back plane bus and its front panel rests against the chassis. *Do not force the ICIM2-XD into the chassis.* If properly aligned, it should slide in with minimal force.
- 5 Tighten the retaining screws on either side of the ICIM2-XD to secure it in the chassis. Use a 3/8-in. flat-blade screwdriver to secure. *Do not over-tighten.*

Step 5: Set Network Parameters from the Command Line Interface (CLI)

- 1 Connect one end of a DB-9 to DB-9 straight-through serial cable to an available COM port on the personal computer, and the other end to the ICIM2 front-panel serial port.
- 2 Open a HyperTerminal session on your laptop (or desktop) PC that you will use to connect to the ICIM2. The HyperTerminal program is typically found at:

`Start\All Programs\Accessories\Communication\Hyperterminal`

The new Connection Description dialog box appears.



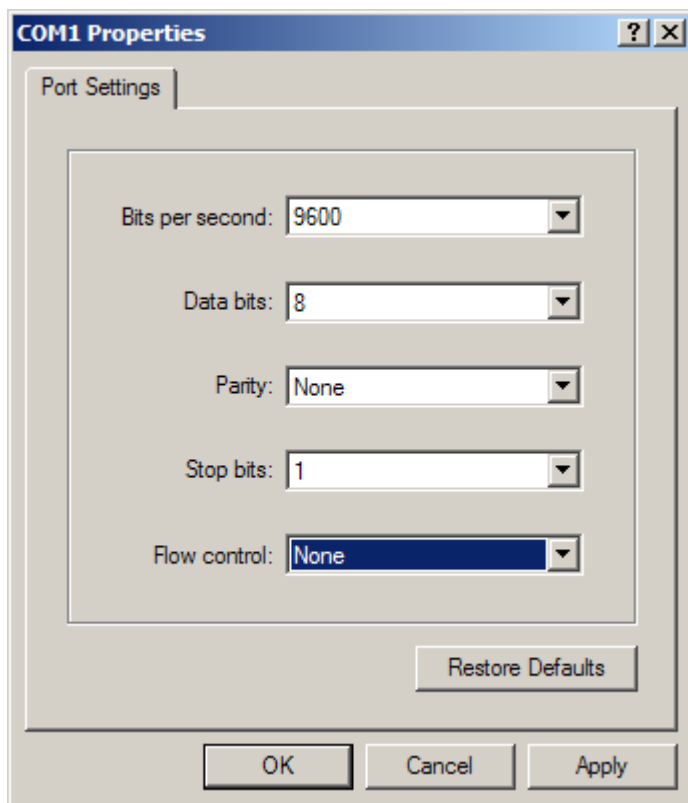
- 3 Type in a name for the connection, select an icon of your choice, and click **OK**. The Connect To dialog box appears.



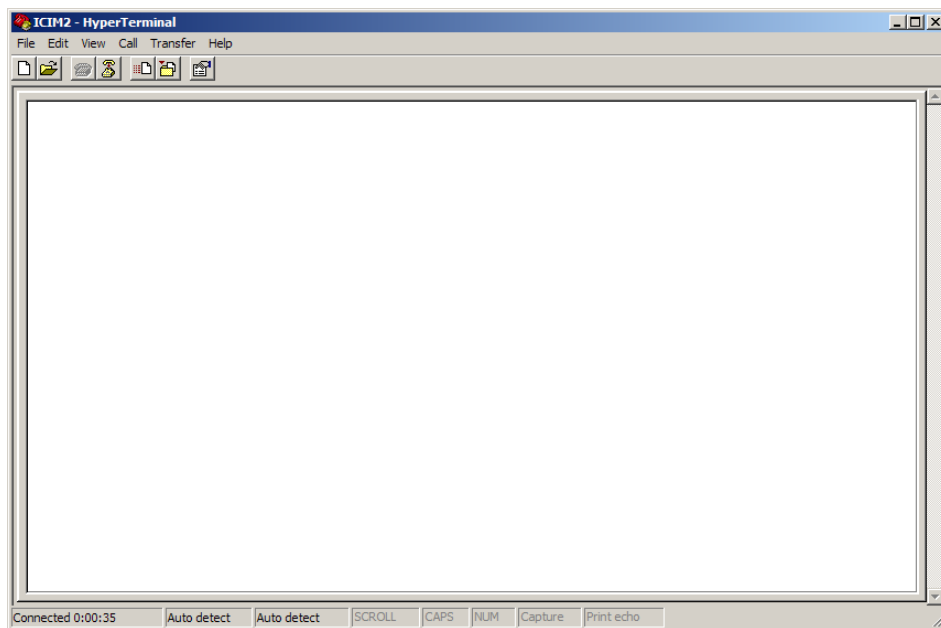
- 4 In the Connect Using field, click the drop-down arrow and select the serial port that you will use for the connection, and then click **OK**. The COM Properties dialog box appears.

Note: For most applications, the serial port is COM1 or COM2.

- 5 Set the following port setting in the COM Properties dialog box.



- 6 Click **OK**. The HyperTerminal main program window appears.



Step 5: Set Network Parameters from the Command Line Interface (CLI)

- 7 On the File menu, click **Save** to save the settings.
- 8 Wait for the ICIM2 boot to finish. Once finished, press **Enter** to display the ICIM2 login prompt:

```
Scientific-Atlanta Intelligent Communications Interface Module (ICIM)
-----
                        W A R N I N G
                        -----

Unauthorized or improper use of this system may result in
administrative disciplinary action and civil or criminal penalties.
By continuing to use this system you indicate your awareness of and
consent to these terms and conditions of use.  LOG OFF IMMEDIATELY
if you do not agree to the conditions stated in this warning.
```

login:

- 9 Log in using the default username **Administrat0r** and the default password **AdminPassw0rd**. Note the 0 (zero) character in each string.

```
Scientific-Atlanta Intelligent Communications Interface Module (ICIM)
login: Administrat0r
Password: AdminPassw0rd
```

Successful login will return the following prompt:

```
login: Administrat0r
Password:
User Administrat0r logged in successfully on 11/13/06 at 15:25:35
Previous successful login was on 11/13/06 at 15:22:16
There were no failed attempts to login with this user id previously
CLI>
```

- 10 Enter the ICIM submenu by typing **icim** at the CLI> prompt.

```
CLI> icim
```

Successful entry into the ICIM menu tree will return the following prompt:

```
ICIM>
```

- 11 Configure the shelf (chassis) IP address, subnet mask, gateway, and clock using the following commands:

```
set ip xxx.xxx.xxx.xxx
set subnet xxx.xxx.xxx.xxx
set gateway xxx.xxx.xxx.xxx
set clock "month/day/year hour:minute:second"
```

Note:

- Be sure to include the quote symbols, e.g., `set clock "3/15/2006 13:09:51"`.
- Clock time is in the 24-hour format.

- 12 To enable these changes, reboot the ICIM2 or ICIM2-XD as follows:

```
ICIM> reboot
```

- 13 After the ICIM2 or ICIM2-XD reboots, repeat the login steps described above to return to the ICIM command prompt. Then use the show command to verify each of the above changes, as follows:

```
show ip
show subnet
show gateway
show clock
```

- 14 Type **logout**, and then press **Enter** to exit the session.

15 Remove the serial cable. It is no longer required.

Important:

- For Telnet operation, the computer you are using must have a network connection through which it can reach the ICIM2 or ICIM2-XD at its IP address.
- No more than four Telnet sessions are allowed at one time.



CAUTION:

Always use the Logout command to close a serial port or Telnet CLI session. Closing a serial port session without issuing the Logout command leaves the session open for a possible future connection. This may allow unauthorized access by a new user if the previous user had a higher authorization privilege level.

Step 6: Connect the ICIM2-XD to the Network

- 1 Using a Category 5 Ethernet (CAT5) cable, connect the front panel Ethernet port of the ICIM2 or ICIM2-XD to your local network.
- 2 Verify connectivity by pinging the ICIM2 or ICIM2-XD IP address. For example:

```
c:\> ping 172.18.50.100
```

Note: The ICIM2 or ICIM2-XD must have an IP address assigned as directed in *Step 5: Set Network Parameters from the Command Line Interface (CLI)* (on page 15). If not completed already, perform this step before continuing with these instructions.
- 3 Follow the steps described in *To Set Up a Telnet CLI Session* (on page 19) to set up a Telnet session with the ICIM2 or ICIM2-XD.

To Set Up a Telnet CLI Session

Complete the following steps to initiate a CLI session with the ICIM2 using Telnet.

Important: The ICIM2 must have an IP address assigned before performing this procedure.

- 1 Open a DOS window on the PC that you will use to connect to the ICIM2.
- 2 At the DOS command prompt, type:

```
telnet <IP address>
```

where **<IP address>** is the IP address of the ICIM2. The session starts and the Telnet login: prompt appears.



- 3 At the login: prompt, type **Administrat0r** (note the zero character in the string), and then press **Enter**.
- 4 At the Password: prompt, type **AdminPassw0rd** (note the zero character in the string), and then press **Enter**. The CLI> command prompt appears.

Step 7: Install Modules in the Chassis

To Install the Module



WARNING:

Avoid damage to your eyes! Do not look into any optical connector while the system is active. Even if the unit is off, there may still be hazardous optical levels present.

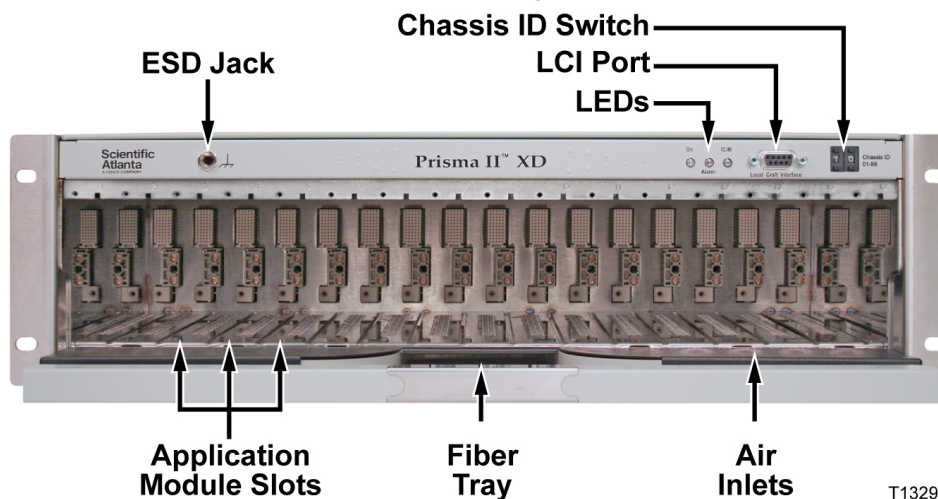
Complete the following steps to install the module in the chassis.



CAUTION:

Always use a screwdriver to loosen or tighten the screws holding the application modules, ICIM2-XD, fan assembly, power supply modules, DC-to-DC converters, or blanking panels in place. Do not attempt to loosen or tighten these screws solely by hand.

- 1 Locate the fiber guides at the bottom of the chassis and the module guide slots inside the chassis as shown in the following illustration.

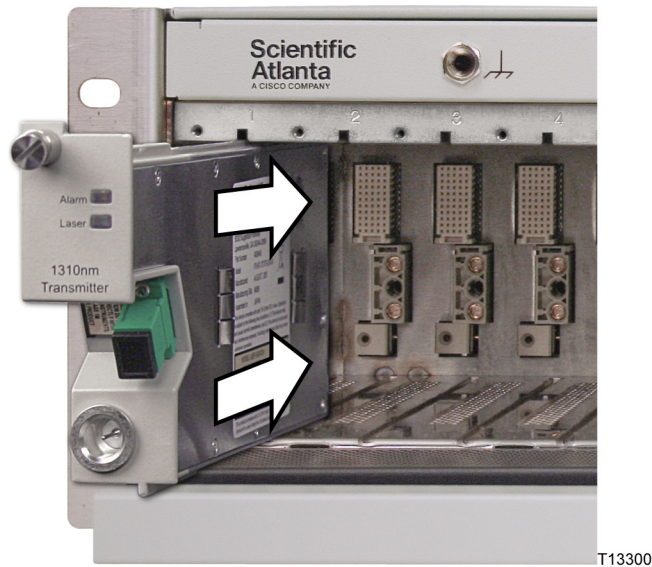


T13295

- 2 Align the ridges on the top and bottom of the module with the module guide slots located on the chassis.

Step 7: Install Modules in the Chassis

- 3 Gently slide the module into the chassis until its power and communications connections join connectors on the midplane bus. *Do not force the module into the chassis.* If properly aligned, it should slide in with minimal force.



- 4 Tighten the screw at the top of the module to secure it in the chassis. Use a 3/8-in. flat-blade screwdriver to secure. *Do not over-tighten.*
- 5 Fill any unused chassis slots with module blanks to help ensure proper cooling air flow.

Step 8: Set Additional Parameters via CLI (Optional)

Additional parameters may be set as needed from the command line interface (CLI) for each application module installed.

Refer to *Prisma II Permitted CLI Commands* (on page 323) and the *Prisma II Platform Remote User Interface Guide, System Release 2.03*, part number 4025477 for information and additional instructions on available commands and using the CLI.

The following CLI commands are pertinent to most installations.

To Set Additional Users for ICIM2 or ICIM2-XD Access

Refer to the *Prisma II Platform Remote User Interface Guide, System Release 2.03*, part number 4025477 for CLI and ICIM Web Interface login settings information.

Note: It is strongly recommended that a new administrator login be created and that the default administrator login be removed.

The table below lists the ICIM mode CLI commands for setting user login parameters.

Commands	Description
ICIM > show user	Shows all users
ICIM > user change password [user name]	Changes user password
ICIM > user add [user name] [access level] enable	Adds a user
ICIM > user delete [user name]	Deletes a user

Note: User names and passwords must be 6 to 14 characters long, and must include at least 1 number.

Step 9: Set and Verify SNMP Community Strings

At the CLI ICIM> command prompt, use the **set** command to change the SNMP Community write, read, and trap strings to corresponding user-defined strings to allow for remote monitoring and control via a network management system (NMS). After entering these commands, use the **info** command to verify the new settings.

The sample dialog below shows how to enter these commands. In the example below:

- myCommWriteString is the user-defined community write string.
- myCommReadString is the user-defined community read string.
- myCommTrapString is the user-defined community trap string.

Refer to *SNMP Management* (on page 167) for SNMP parameter information.

From the CLI command prompt, switch to ICIM command mode and define SNMP Read, Write, and Trap Community strings, as shown below.

```
CLI> icim

ICIM> set commwrite "myCommWriteString"
NOTE: This change will not fully take effect until the ICIM is restarted.
Until that time, some operations will not perform as expected.

SUCCESS!

ICIM> set commread "myCommReadString"
NOTE: This change will not fully take effect until the ICIM is restarted.
Until that time, some operations will not perform as expected.

SUCCESS!

ICIM> set commtrap "myCommTrapString"
NOTE: This change will not fully take effect until the ICIM is restarted.
Until that time, some operations will not perform as expected.

SUCCESS!
```

You can then verify the community string settings, as follows.

```
ICIM> info commread commwrite commtrap

COMMREAD          COMMWRITE          COMMTRAP
myCommReadString  myCommWriteString  myCommTrapString

SUCCESS!

ICIM>
```

Note:

- It is strongly recommended that the ICIM2 or ICIM2-XD be restarted after changing any of the community strings. Otherwise, some operations will continue to work normally, while others will appear to fail.
- It is strongly recommended that new SNMP community strings be created and the default SNMP community strings be removed. Default SNMP community string values are listed below.

SNMP Community String	Default Value
Read Community	public
Write Community	private
Trap Community	SNMP_traps

Step 10: Perform Chassis-to-Chassis ICIM2 Activation (Optional)

Once the chassis are interconnected, the shared ICIM2 or ICIM2-XD should be forced to search for all new modules, rather than be allowed to find them incrementally over the course of a polling cycle.

The recommended method for forcing a search for new modules is to reboot the ICIM2 or ICIM2-XD. This can be accomplished either by physically removing and reinserting the module, or by issuing a reboot command to the ICIM2 or ICIM2-XD via the CLI interface.

To reboot the ICIM2 or ICIM2-XD via CLI, open a console session and type the following commands at the CLI prompt.

```
CLI> icim
ICIM> reboot
```

The response will be:

```
The ICIM2 is about to reboot. This will end all current login and web sessions
Are you sure you want to proceed (Yes/No)> yes
```

```
SUCCESS!
ICIM>
```

```
Scientific-Atlanta Intelligent Communications Interface Module (ICIM)
```

```
-----
W A R N I N G
-----
```

```
Unauthorized or improper use of this system may result in
administrative disciplinary action and civil or criminal penalties.
By continuing to use this system you indicate your awareness of and
consent to these terms and conditions of use. LOG OFF IMMEDIATELY
if you do not agree to the conditions stated in this warning.
```

```
login:
```

Each of the additional modules will then be added to the ICIM2 or ICIM2-XD polling cycle.

Note: Use of the CLI **reboot** command is preferred over the **updateid** command in this case because a reboot will maintain synchronization with the NMS.

Step 11: Make Changes to Traps and Enterprise MIBs

Trap settings and other parameters can be set in one of several ways:

- Using Simple Network Management Protocol (SNMP) commands. Refer to *SNMP Management* (on page 167) for details on accessing the ICIM MIB tables.
- Using the Command Line Interface (CLI) Traps Enable command. Refer to the *Prisma II Platform Remote User Interface Guide, System Release 2.03*, part number 4025477 for details on using the Traps Enable command.
- Using the ICIM Web Interface, which requires no knowledge of SNMP or CLI. For further information, refer to the *Prisma II Platform Remote User Interface Guide, System Release 2.03*, part number 4025477.

Once this is accomplished, changes can be made to the ICIM Trap tables, of which there are 10 entries (one for each destination IP address).

Following are the objects in the p2TrapRecvEntry table that should be set.

MIB Object	Value
p2TrapRecvEnable	1-disabled; 2-enabled
p2TrapRecvAddr	IP address of trap receiver
p2TrapRecvTelcoAlarm	1-disabled; 2-enabled

MIB Software

MIBs associated with the software system release are available and should be compiled in your SNMP tool. They are labeled as follows:

- SCIATL-PRISMAII-ICIM-MIB.mib
- SCIATL-PRISMAII-MODULE-MIB.mib

Trap Overview

The Prisma II system can be configured to provide various alarm and warning conditions to an NMS or system monitor application.

There are nine different trap categories that can be independently enabled to provide the desired level of information on events occurring in a system. These traps can be forwarded to up to 10 different IP addresses. The trap filtering can be configured uniquely for each user.

See *SNMP Management* (on page 167) for trap details.

Step 11: Make Changes to Traps and Enterprise MIBs

Note: All trap types (module insertion, alarm events, etc.) are reported through the Enhanced Alarm trap. Therefore, only the Enhanced Alarm traps are enabled by default, and this is the recommended configuration.

Step 12: Make Physical Connections to Modules

Once all configuration changes are complete, you are ready to make fiber-optic and RF cable connections for each module as appropriate.

To Connect Optical Cables



CAUTION:

High power density exists on fiber when optical power is present. To avoid microscopic damage to fiber mating surfaces, turn off optical power or reduce power below 15 dBm before making or breaking optical connections.

Complete the following steps for each optical cable connection to be made and on every module to be installed.

- 1 Clean the end of the fiber to be connected as described in *Cleaning Optical Connectors* (on page 308).
- 2 Connect the optical cable to the module connector.
- 3 Route the cable to the appropriate destination.
- 4 Clean the remaining cable end, and then connect the cable to the mating module connector.

Note: Remember to observe minimum bend radius and other accepted handling practices when working with fiber-optic cables.

- 5 After cable installation is complete, return the module control settings to their original states.

To Connect RF Cables

Complete the following steps for each RF cable connection to be made.

- 1 Connect the RF cable to the appropriate back-panel module connector.
- 2 Route the cable to the appropriate destination.

Step 13: Verify System Release and Module Firmware Versions

To check the current firmware revision levels in all modules in the ICIM2 or ICIM2-XD domain, enter the following CLI command at the ICIM> prompt:

```
ICIM> show domain
```

A column labeled ACTIVEREV in the response lists the active firmware revision numbers for each module in the domain. Each module firmware revision should be compatible with the revision number of the system release firmware. For information on module and system release firmware compatibility, contact your customer serviced representative.

If any modules report a firmware version that is not compatible with the system release firmware, use the procedures described in the next step to update the module firmware.

Step 14: Install and Use the Firmware Update (SOUP) Utility (Optional)

The Prisma II Software Upgrade Program (SOUP) is a user-friendly utility that allows users to perform firmware upgrades on Prisma II modules. The SOUP utility simplifies the firmware upgrade process by providing a graphical user interface (GUI) that is easy to use and requires little training.

When connected to a chassis, the SOUP utility shows the user the current versions of firmware on all modules and allows the user to download and activate other versions from system release files. The SOUP works together with the ICIM2 or ICIM2-XD to send the binary image files and appropriate commands to the modules to upgrade their firmware. As the modules are being upgraded, the SOUP displays relevant progress information to the user.

To Install the SOUP on Windows

Complete the following steps to install the Prisma II SOUP on Windows.

- 1 Download the Prisma II SOUP installation file to your Windows desktop.
- 2 Double-click the Prisma II SOUP installation icon to start the installation.
- 3 Follow the instructions of the installation wizard.

After the installation is complete, you will have an icon on the desktop to launch the SOUPLauncher application. There will also be a program group called Prisma II SOUP on your Start button menu.

To Use the SOUP Utility

After the SOUP utility is launched through SOUPLauncher, it attempts to connect to the ICIM and retrieve information about all the modules it manages. After retrieving the module information, the SOUP connects to the FTP server holding the system release files and retrieves the firmware versions available for each module. This information is then displayed to the user in the application main screen.

For additional details on using SOUP, see *Remote Firmware Download Feature* (on page 271).

To Uninstall the SOUP on Windows

Complete the following steps to remove the Prisma II SOUP from your computer.

- 1 Open the **Control Panel** from the Windows Start menu.
- 2 From the Control Panel, open the **Add or Remove Programs** application.

Step 14: Install and Use the Firmware Update (SOUP) Utility (Optional)

- 3 Find and choose the **Prisma II SOUP** entry in the list of installed programs. If the entry is not present, the program is not installed on the computer or was not installed properly.
- 4 Click the **Change/Remove** button.
- 5 Follow the instructions of the uninstall wizard.

2

Introduction

Overview

This guide describes the Prisma II™ Extreme Density (XD) Platform. This platform consists of the Prisma II XD Chassis and its power supplies, fan assembly, application modules, and control systems.

Purpose

This guide provides information and instructions for implementing the Prisma II XD Chassis, internal components, and external control systems.

Who Should Use This Document

This document is intended for authorized service personnel who have experience working with similar equipment. The service personnel should have appropriate background and knowledge to complete the procedures described in this document.

Qualified Personnel



WARNING:

Allow only qualified and skilled personnel to install, operate, maintain, and service this product. Otherwise, personal injury or equipment damage may occur.

Only appropriately qualified and skilled personnel should attempt to install, operate, maintain, and service this product.

Scope

This guide discusses the following topics.

- The Prisma II XD Platform and its components
- Installation procedures
- Equipment configuration
- Operation of the ICIM2-XD control module
- Local Command Interface (LCI) operation
- User management
- Event log management
- SNMP management
- Remote software download (SOUP)
- Chassis maintenance and troubleshooting
- CLI command reference
- Features available via remote user interface
- Descriptions of module parameters

Document Version

This is the first release of this guide (Rev A).

In This Chapter

■ Related Publications	35
■ Prisma II XD Platform	36
■ Prisma II XD Chassis	39
■ XD Chassis Fan Assembly	51
■ AC-to-DC Bulk Power Supply Modules	52
■ DC-to-DC Converters	56
■ Prisma II ICIM2-XD	57

Related Publications

You may find the following publications useful as you implement the procedures in this document.

- *Prisma II Platform Remote User Interface Guide, System Release 2.03*, part number 4025477
- *Prisma II™ High Density Dual Reverse Receiver Installation and Operation Guide*, part number 4015908
- *Prisma II™ 1550 nm High Density QAM Transmitter Installation and Operation Guide*, part number 4019959
- *Prisma II™ High Density Forward Receiver Installation and Operation Guide*, part number 4020002
- *Prisma II™ 1310 nm High Density Transmitter Installation and Operation Guide*, part number 4009700
- *Prisma II™ Multi-Wavelength High Density Transmitter Installation and Operation Guide*, part number 4023013

Prisma II XD Platform

The Prisma II XD Platform is a configurable and expandable system for providing transmit and receive functions to fiber-optic communications networks.



T13294

The Prisma II XD Platform can be configured for use in a variety of service provider environments. Key features of the Prisma II XD Platform are:

- High module density
- Broad operating temperature range
- Rapid installation and setup
- Support for local and remote system monitoring and control

XD Platform Components

The Prisma II XD Platform consists of the following products.

- Prisma II XD Chassis
- Prisma II XD fan assembly
- Prisma II XD AC-to-DC bulk power supply modules (one or two)
- Prisma II ICIM2-XD Intelligent Communications Interface Module
- Prisma II High-Density Platform application modules
- Prisma II XD Chassis application module blanking panels

Note: The ICIM2-XD can control up to 64 application modules in a daisy-chain configuration of up to four full chassis.

XD Chassis

The chassis houses all other system components. A midplane bus system inside the chassis distributes electrical power to all installed modules. The midplane bus system also transports communication and control signals between installed application modules and the ICIM2-XD.

XD Chassis Fan Assembly

The chassis uses a negative pressure fan system to pull cooling air from the ambient environment. Three fans are housed in a field-replaceable assembly attached at the back of the chassis.

The fan assembly can be removed for inspection and maintenance, to provide access to the DC-to-DC converters inside the chassis, or to remove either of the AC-to-DC bulk power supply modules.

ICIM2-XD

The Prisma II Intelligent Communications Interface Module 2 for the XD platform (ICIM2-XD) provides users with access to application module configuration settings, status monitoring, and alarm monitoring.

The ICIM2-XD is logically identical to the ICIM2 module designed to fit the Prisma II Platform chassis. However, the ICIM2-XD is physically smaller than the ICIM2 and lacks a front-panel keypad or liquid-crystal display. Because of these physical differences, the ICIM2-XD can only be installed in an XD chassis and an ICIM2 can only be installed in a Prisma II chassis.

Note: When a Prisma II chassis and a Prisma II XD chassis are part of a daisy-chain connection of two or more chassis, a single ICIM2 or ICIM2-XD can and must be used to control both chassis.

Application Modules

Prisma II XD application modules perform a prescribed set of independent transmit or receive functions. These modules install from the front of the chassis, are hot-swappable, and have plug-and-play capability.

All XD application modules share a common half-height, high-density form factor. The following application modules are currently available:

- Prisma II 1310 nm High Density Transmitter
- Prisma II 1550 nm High Density QAM Transmitter
- Prisma II High Density Forward Receiver
- Prisma II High Density Dual Reverse Receiver

Chapter 2 Introduction

■ Prisma II Multi-Wavelength High Density Transmitter

Additional applications may become available in the future. For further information, contact Scientific Atlanta using the information provided in *Customer Support Information* (on page 313).

Detailed information about each application module is provided in the installation and operation guide for that module. For document ordering information, see *Related Publications* (on page 35).

Prisma II XD Chassis

The XD chassis houses the fan assembly, one or two AC-to-DC bulk power supply modules, a chassis control board (CCB), two internal DC-to-DC converter assemblies, the ICIM2-XD, and up to 16 high-density application modules.

Through an internal midplane bus, the chassis provides modules with electrical power, a shared serial bus, a high-speed data bus for the ICIM2-XD, and connections to two back-panel RF connections per application module. The midplane interface is designed so that application modules can be replaced even when the system is under power and fully operational.

Ports on the front and back of the chassis support external communication with the ICIM via the midplane bus. This communication enables system management via local craft interface (LCI), command line interface (CLI), hypertext transfer protocol (HTTP), or Simple Network Management Protocol (SNMP) commands.

A fiber tray built into the chassis provides strain relief and facilitates front-to-back routing for optical cables connected to the application modules.

Chassis Features

The chassis has several noteworthy operational features, including hot-swap, resource sharing, redundancy, and Prisma II Platform compatibility. These are described in more detail below.

Hot-Swap (Application Modules and ICIM2-XD)

The chassis and its application modules embody several design features that help to ensure a smooth and non-destructive module hot-swap.

- The ICIM2-XD and chassis control board have circuits that limit inrush current to no more than 120% of the maximum allowed for each power bus.
- Each module contains bus isolation and power management circuits to ensure a gentle power ramp-up. This reduces the possibility of arcing and voltage spikes.
- The system software notifies the ICIM2-XD of a hot-swap as soon as it occurs, rather than when the ICIM2-XD polls for information. This results in faster status updates.
- The connector pins on each module are staged, so that the first connection made on insertion and the last connection broken on removal is ground, followed by power, and finally, the signal pins.



CAUTION:

For a chassis under power, field replacement of the fans, AC-to-DC bulk power supply modules, or DC-to-DC converter assemblies must be completed in two minutes or less to prevent possible chassis overheating due to temporary removal of the fan assembly.



CAUTION:

- Before removing an AC-to-DC bulk power supply module from the chassis, disable AC input power to the module by disconnecting the associated AC power cord.
- Before removing a DC-to-DC converter assembly from the chassis, disable DC input power to the converter assembly by disconnecting the associated AC power cord (if AC operated) or DC power-passing cable (if DC operated).
- Do not disable power to both sides of the chassis at the same time when such action may cause a loss of service.

Resource Sharing

The AC-to-DC bulk power supply modules and the ICIM2-XD control module are resources that can be shared by multiple chassis.

An AC-to-DC bulk power supply module installed in one chassis can provide operating power for a second chassis by connecting a DC power-passing cable between the two chassis. Power sharing saves cost and improves polling cycle times by reducing the number of intelligent modules and their associated polling overhead.

The ICIM2-XD in one chassis can be used to control modules installed in up to three additional chassis (four chassis total) through a series daisy-chain connection from the ICIM OUT port of the first chassis to the ICIM IN port of the second, and so on.

Redundancy

Terminal blocks on the back panel of the chassis provide ALARM IN and ALARM OUT control lines for each of the 16 application module slots (32 alarm signal lines total). The alarm outputs are brought HIGH (+5 VDC) by hardware or software during module removal or other fault condition. The alarm signal lines allow for external configuration of redundancy options, including the option to locate master and slave modules in separate chassis.

Prisma II Platform Compatibility

Prisma II Platform chassis can be used together with Prisma II XD Platform chassis in the same daisy-chain network. Because they are logically identical, either an ICIM2 or an ICIM2-XD can be used to control the chassis and modules in this network. Only one control module (ICIM2 or ICIM2-XD) is permitted per daisy-chain.

Chassis Configuration

The chassis has front slots that support up to 16 Prisma II XD half-height, high-density application modules. Two slots on the chassis back panel accept up to two AC-to-DC bulk power supply modules. A third slot on the back holds the ICIM2-XD control module.

Chassis and Slot Numbering

For management purposes, every chassis in an ICIM2 domain is assigned a unique chassis number. The chassis has a switch on the front panel that permits selection of a chassis ID number from 00 through 99.

Note: It is important to avoid using chassis ID number 00 in some circumstances, as explained in the following caution.



CAUTION:

Setting the chassis ID to 00 is not recommended as it causes the entity MIB to violate RFC-2737 by creating an invalid object identifier. This may affect operation with some management systems that use the entity MIB. In particular, attempts to access the fans (in virtual slot 0) in chassis 00 will fail if made via serial TNCS (or ROSA-EM) or LCI.

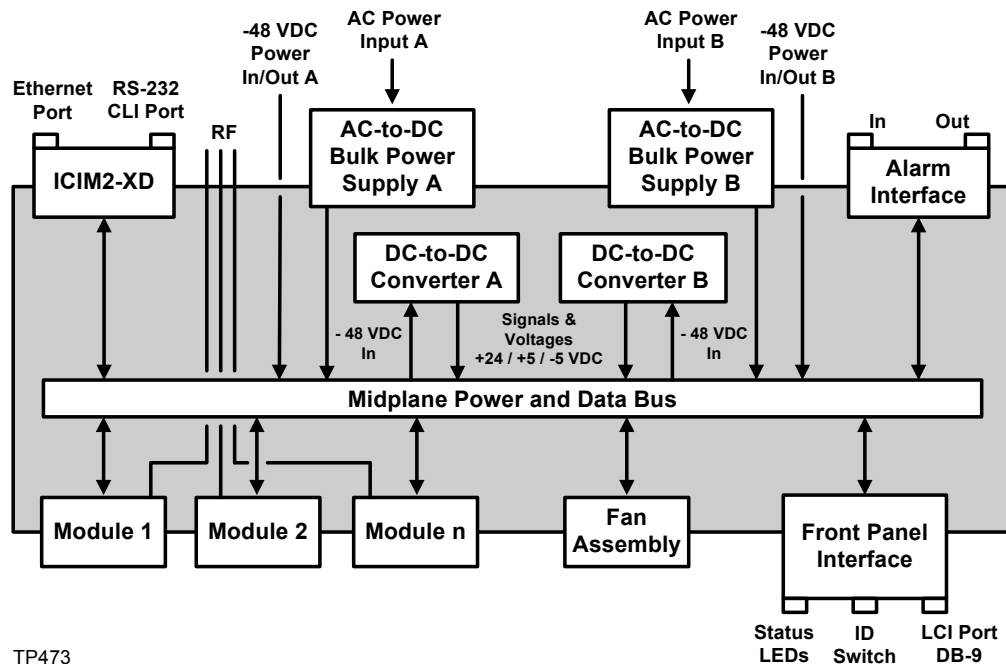
Each application module installed in the chassis is identified by a unique slot number from 1 to 16. Together with the chassis numbers, these slot numbers enable network management software to address each application module individually.

Note: The fan assembly and ICIM2-XD module installed in the chassis back panel have the following virtual slot number assignments.

Module	Virtual Slot
Fan assembly	00
ICIM2-XD control module	17

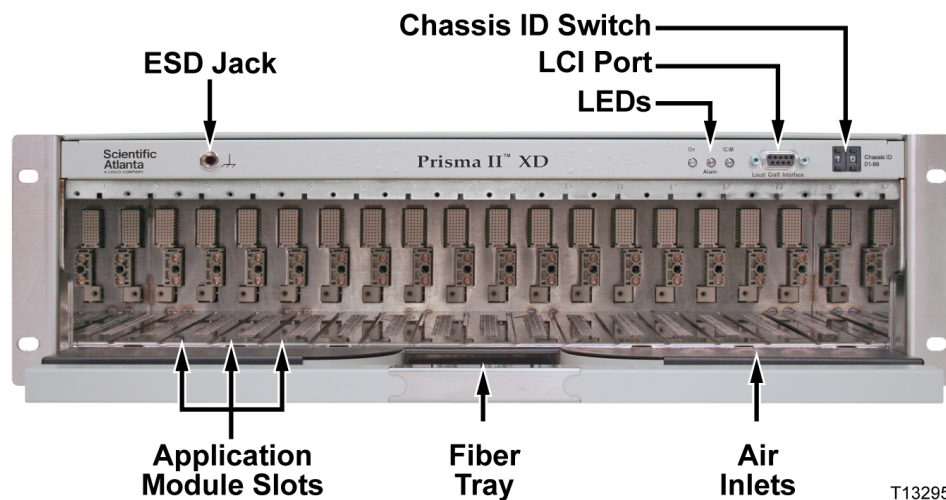
Typical Chassis Block Diagram

The block diagram below shows a typical Prisma II XD Chassis configuration with two power supplies, an ICIM2-XD, and several application modules installed.

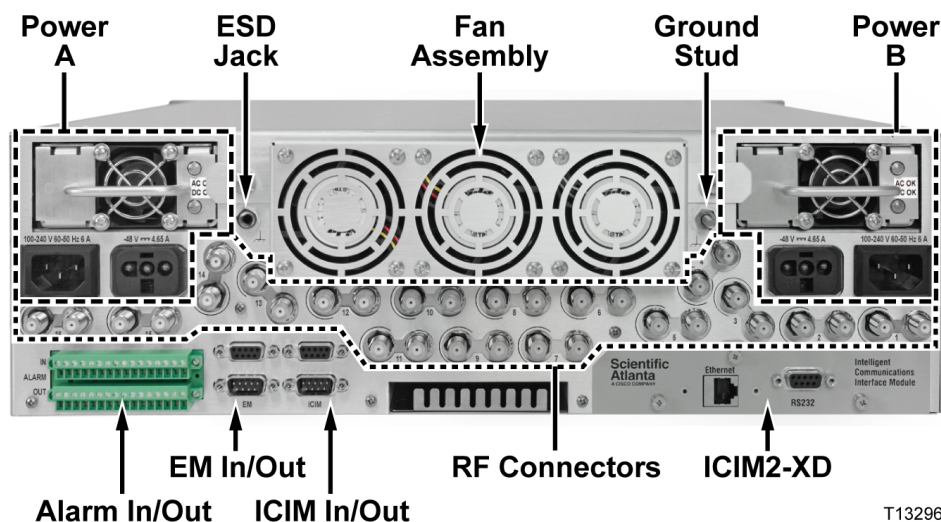


Chassis Illustrations

The following illustration shows the front of the chassis as it appears when filled with application modules. The LED indicators, chassis ID switch, and LCI port are visible across the top panel.



The following illustration shows the back of the chassis as it appears with both power supplies and the ICIM2-XD installed. The fans, I/O connectors, RF connectors, and power inlets are located as indicated on the back of the chassis.



Chassis Front Panel Features

Part	Function
ESD Jack	ESD (electrostatic discharge) jack, to be used before touching any modules.
ON LED (green)	Indicates the presence of +5 VDC on the chassis midplane bus. Flashes to indicate active ICIM2-XD communication via the LCI port. At power-up, flashes to indicate failure of chassis self-test.
ALARM LED (red)	Indicates a fault condition in one or more installed application modules. Glow steadily to indicate a critical fault condition. Flashes to indicate a non-critical fault condition. At power-up, flashes to indicate failure of chassis self-test.
ICIM LED (green)	Illuminates to indicate that an ICIM2-XD is installed.
Chassis ID Switch	Located at the top right of the front panel, allows the operator to assign an identification number, known as the Shelf number, to every chassis for addressing by an ICIM2 or ICIM2-XD through CLI or SNMP commands. Note: Every chassis connected to an particular ICIM2 or ICIM2-XD must have a unique chassis ID number.

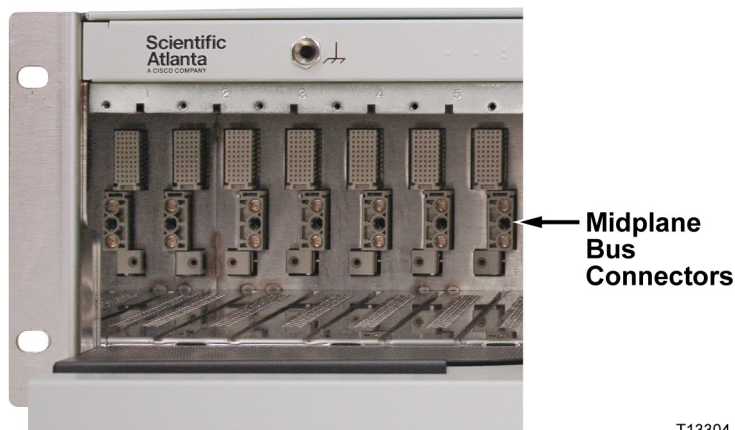
Chassis Back Panel Features

Part	Function
ESD Jack	ESD (electrostatic discharge) jack, to be used prior to touching any modules.
ALARMS IN/ALARMS OUT	Allows for an ALARM OUT connection and an ALARM IN connection for each module slot in the chassis.
EM IN/EM OUT	An RS-485 bus that enables serial communication with the ICIM2-XD using Transmission Network Control System (TNCS) or another element management system.
ICIM IN/ICIM OUT	A dedicated bus that enables serial communication between the ICIM2-XD and modules in other chassis for control and monitoring purposes.
Power Supply Inlets	<p>One or two AC-to-DC bulk power supply modules can be installed in the chassis. Utility AC power enters via a standard IEC power connector.</p> <p>A DC power connector for each bulk power supply slot provides -48 VDC output when using one chassis to power a second through a power-chain connection. Or, if the associated bulk power supply slot is not populated, this DC power connector serves as a -48 VDC input for DC operation.</p>
Ground Studs	Ground studs.
RF Connectors	A pair of RF connectors for each application module slot (1-16) support up to two independent RF ports per module.

Chassis Midplane

The chassis midplane provides bus connections for distribution of power and communication signals. The midplane also connects two RF ports on the module back panel to each of the 16 application module slots.

The chassis midplane layout is shown below.



T13304

Fan Assembly

The fan assembly is installed in the back of the chassis at the factory. It is held in place by two screws, one on either side of the assembly. The assembly can be removed as a unit for periodic maintenance or inspection. Tools are needed to remove or install the fan assembly.

The fan assembly must be removed to install or remove either of the AC-to-DC bulk power supply modules, or to gain access to the DC-to-DC converter assemblies mounted in the chassis just behind the fans.

Important: Do not operate the chassis for more than two minutes without the fan assembly installed. For safe operation, proper cooling of the chassis must be maintained over the specified temperature range.



CAUTION:

- Before removing an AC-to-DC bulk power supply module from the chassis, disable AC input power to the module by disconnecting the associated AC power cord.
- Before removing a DC-to-DC converter assembly from the chassis, disable DC input power to the converter assembly by disconnecting the associated AC power cord (if AC operated) or DC power-passing cable (if DC operated).
- Do not disable power to both sides of the chassis at the same time when such action may cause a loss of service.

Midplane Bus Connectors

The connectors on the chassis midplane bus accommodate electrical power, digital signals, and analog signals for each module. All connectors are self-guiding and allow a blind-mate connection.

XD Chassis Control Board

The chassis has an internal chassis control board that provides the following functions:

- Fan monitoring and control
- AC-to-DC bulk power supply monitoring
- DC-to-DC converter monitoring
- Chassis temperature monitoring
- LED control
- Alarm signaling

Each of these functions is described in greater detail below.

Fan Monitoring and Control

The chassis control board monitors and controls all fans used for chassis air circulation. It reports an alarm (Fan1_Ok, Fan2_Ok, Fan3_Ok) if any of the three fans in the fan assembly is disconnected, broken, or jammed. It monitors internal chassis temperature (ChasTemp), disables all three fans if the temperature falls below 0°C, and enables all three fans if the temperature rises above 10°C.

AC-to-DC Bulk Power Supply Monitoring

The chassis control board monitors the following AC-to-DC bulk power supply conditions:

- AC-to-DC bulk power supply module A installed (PSA Inst)
- AC-to-DC bulk power supply module B installed (PSB Inst)

PSA Inst and PSB Inst monitor for two conditions at their respective power supply slots. First, they check whether an AC-to-DC bulk power supply module is installed. If the power supply module is installed, they then check for the presence of AC input power to that slot. The absence of AC input power to a populated power supply slot will trigger an alarm condition.

This alarm behavior can be temporarily muted for slot A (AlmMuteA) or slot B (AlmMuteB) to prevent alarms from occurring during servicing. For example, muting can be used to prevent an alarm when temporarily removing AC input power to a populated power supply slot during field replacement of a DC-to-DC converter.

DC-to-DC Converter Monitoring

The chassis control board monitors the following DC-to-DC converter module conditions:

- DC-to-DC converter A -48 VDC input (ConvAIn)
- DC-to-DC converter B -48 VDC input (ConvBIn)
- DC-to-DC Converter A +24 VDC output (ConvA+24)
- DC-to-DC Converter B +24 VDC output (ConvB+24)
- DC-to-DC Converter A +5 VDC output (ConvA+5)
- DC-to-DC Converter B +5 VDC output (ConvB+5)
- DC-to-DC Converter A -5 VDC output (ConvA-5)
- DC-to-DC Converter B -5 VDC output (ConvB-5)

Chassis Temperature Monitoring

The chassis control board monitors the internal temperature of the chassis and reports an alarm if the temperature (ChasTemp) falls outside normal limits.

LED Control

The chassis control board controls three front-panel LED indicators:

- The On LED lights to indicate that the midplane bus has all required DC operating voltage.
- The Alarm LED blinks to indicate a minor alarm, and glows steady to signal a major alarm.
- The ICIM LED lights to indicate that an ICIM2-XD module is installed in the chassis.

Alarm Signaling

The chassis control board has alarm-out contacts to control an external alarming device triggered by an event. It can also read an input alarm from an external source. These two lines are routed to ALARM IN and ALARM OUT connectors on the back of the chassis.

Fuse Protection

The chassis control board is protected by a fuse to reduce the chance of losing the entire chassis in the event of a component failure on the board. This fuse is soldered in place, and is not intended to be replaced in the field.

Chassis Power Supply Architecture

The chassis can operate from utility AC power or from external -48 VDC power.

For AC operation, one or two AC-to-DC bulk power supply modules are installed in the chassis. Each of these modules supplies -48 VDC power to one of two DC-to-DC converter assemblies inside the chassis. The DC-to-DC converter assemblies, in turn, generate the midplane bus working voltages at +24, +5, and -5 VDC.

A single AC-to-DC bulk power supply module is sufficient to operate two fully populated chassis. Installing a second AC-to-DC bulk power supply in one chassis adds redundancy in the event of a power supply module failure.

For DC operation, one or both AC-to-DC bulk power supply modules are removed, and power for one or both internal DC-to-DC converter assemblies is supplied from a battery room, another XD chassis, or some other external -48 VDC power source. External DC power enters the chassis via a DC power connector associated with each power supply module slot.

The DC power connector can serve one of two functions, depending on the power supply configuration:

- When the associated AC-to-DC bulk power supply slot is empty, its DC power connector acts as an inlet for external -48 VDC.
- When the associated AC-to-DC bulk power supply slot is populated, its DC

power connector acts as an outlet for -48 VDC from the bulk power supply module.

This functionality enables two chassis to be interconnected via their DC power connectors so that the power supply module(s) in one chassis provide operating power for the second chassis.



CAUTION:

A single DC power connector cannot act as in input and an output connector at the same time. Before applying external DC power, confirm that the AC-to-DC bulk power supply slot associated with the DC power connector is empty and covered by a blanking panel.



CAUTION:

To preserve proper airflow within the chassis, all unused slots must be covered by suitable blanking panels, as follows:

- AC-to-DC bulk power supply module blanking panel, part number 4021618
- ICIM2-XD module blanking panel, part number 4021163
- Prisma II XD application module blanking panel, part number 4023066

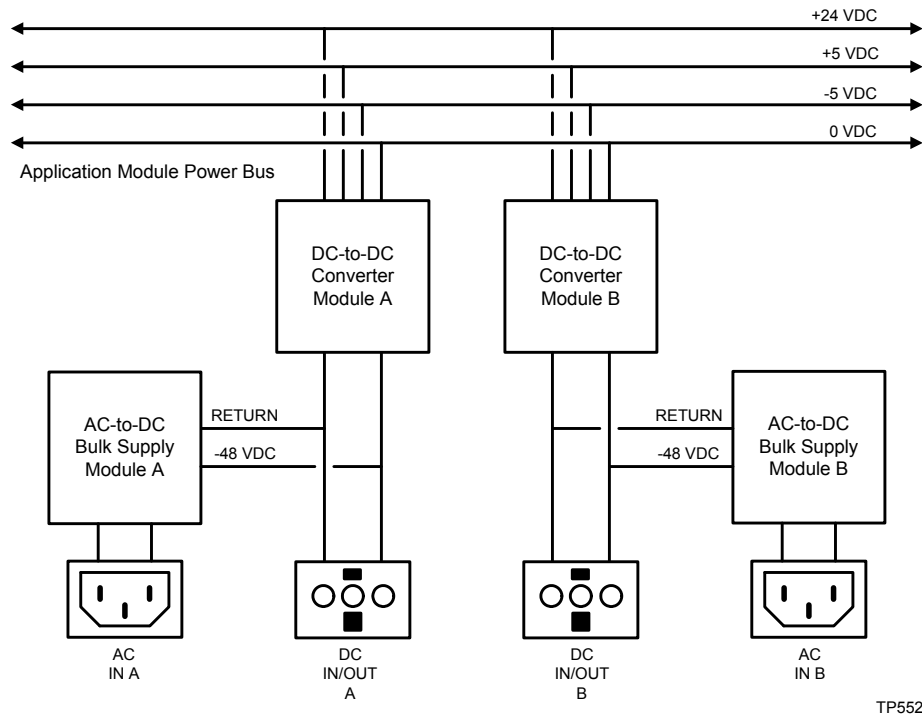
Failure to observe this precaution may result in equipment malfunction or reduced operating life due to overheating.



CAUTION:

When connecting chassis together for power sharing, use either a factory DC power-passing cable, part number 4011730 (3 m) or 4023718 (2 ft), or a custom cable made in accordance with the instructions in this document. Use of other cables for this purpose is not supported.

The following diagram shows the general power supply architecture for a single Prisma II XD Platform chassis.



As shown above, each AC-to-DC bulk power supply module feeds a separate, dedicated DC-to-DC converter assembly. The chassis ships with two DC-to-DC converters installed, but without either AC-to-DC bulk power supply module installed.

Each DC-to-DC converter can power a full chassis on its own. The use of dual independent converters, together with dual AC-to-DC bulk power supplies, allows for full power supply redundancy.

Power Sharing

Routing of -48 VDC power from an AC powered chassis to a second chassis is achieved by connecting a DC power-passing cable between the DC power connectors of the two chassis. Two such cables are currently available from the factory:

- Part number 4011730, 3 m DC power passing cable
- Part number 4023718, 2 ft DC power passing cable



CAUTION:

When connecting chassis together for power sharing, use either a factory DC power-passing cable, part number 4011730 (3 m) or 4023718 (2 ft), or a custom cable made in accordance with the instructions in this document. Use of other cables for this purpose is not supported.



WARNING:

Any external power supply must provide proper electrical components to power the chassis or risk serious equipment damage or personal injury.

XD Chassis Fan Assembly

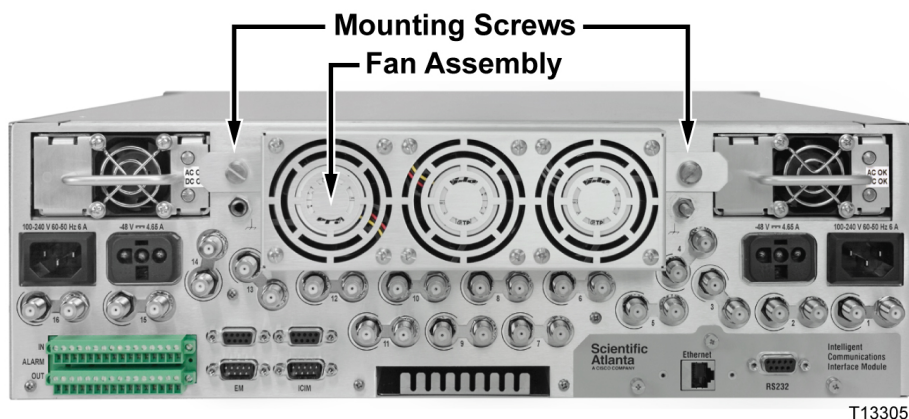
The fan assembly cools the chassis and its application modules. The fan assembly also contains the sensor circuits that provide temperature and power supply status information to monitoring devices.

Fan Operation

Cooling air is allowed to enter the front of the chassis through perforated panels on either side of the fiber tray. The fans draw air through these panels, up through the cooling fins of the application modules, across the inside top of the enclosure, and out the back of the chassis.

Note: The AC-to-DC bulk power supply modules contain their own smaller fans for cooling the power supply circuits. These fans work independently of the chassis fan assembly.

Fan Assembly Illustration



AC-to-DC Bulk Power Supply Modules

The chassis AC-to-DC bulk power supply modules convert incoming AC utility power to -48 VDC. This DC voltage feeds a separate DC-to-DC converter for each bulk power supply module inside the chassis to produce +24, +5, and -5 VDC chassis working voltages. These voltages are made available to the ICIM2-XD and all application modules via the chassis midplane bus.

Two dedicated slots for AC-to-DC bulk power supply modules are located in the back of the chassis. The use of two power supply systems allows for redundant power feeds. The AC-to-DC bulk power supply modules are held in place by tabs on either side of the fan assembly. Installation or removal of a bulk power supply module or its associated DC-to-DC converter requires temporary removal of the fan assembly.



CAUTION:

For a chassis under power, field replacement of the fans, AC-to-DC bulk power supply modules, or DC-to-DC converter assemblies must be completed in two minutes or less to prevent possible chassis overheating due to temporary removal of the fan assembly.

Power Sharing

The -48 VDC output from an AC-to-DC bulk power supply module in one XD chassis can be passed to a second XD chassis. A DC-to-DC converter in the second chassis then uses the external -48 VDC to provide local working voltages to the chassis midplane bus. This bulk power-sharing scheme avoids the need to purchase a new set of bulk power supply modules when adding a chassis.

If two AC-to-DC bulk power supplies are installed in one XD chassis, the DC output from each bulk supply can be passed to the corresponding DC input of a second chassis. This scheme provides redundant power for both chassis: if one bulk DC power supply should fail, the remaining power supply takes the full load for both chassis.

Power Supply Configurations

A Prisma II XD Chassis can operate with one or two AC-to-DC bulk power supply modules installed, or with no bulk power supplies installed if external -48 VDC is applied to the chassis at one or both back-panel DC power connectors. The chassis thus supports a wide range of power supply configurations, subject to two requirements:

- If an AC-to-DC bulk power supply slot is populated, its corresponding DC power connector cannot be used as a power inlet.
- If an AC-to-DC bulk power supply slot is empty, its corresponding DC power

connector cannot be used as a power outlet.

Not all of the possible power supply configurations satisfy both of these requirements. The following table lists all possible configurations and identifies those which are valid.

Power Supply A	Power Supply B	External -48 VDC A	External -48 VDC B	Configuration Status
-	-	-	Applied	Valid
-	-	Applied	-	Valid
-	-	Applied	Applied	Valid
-	Installed	-	-	Valid
-	Installed	-	Applied	-
-	Installed	Applied	-	Valid
-	Installed	Applied	Applied	-
Installed	-	-	-	Valid
Installed	-	-	Applied	Valid
Installed	-	Applied	-	-
Installed	-	Applied	Applied	-
Installed	Installed	-	-	Valid
Installed	Installed	-	Applied	-
Installed	Installed	Applied	-	-
Installed	Installed	Applied	Applied	-

Important: Only the power supply configurations identified as valid above are supported. Other configurations may produce unexpected results, and therefore are not supported.

DC-to-DC Converter Alarms

Two alarm parameters, ConvAIn (converter A input) and ConvBIn (converter B input), are designed to alert the operator in the event of a loss of DC input power to the chassis. Each alarm activates if the associated AC-to-DC bulk power supply slot is empty and there is no DC power at the associated DC power connector.

Important:

- If both sides of the chassis lose DC power, no converter alarms are (or can be) generated.
- Chassis configurations in which an AC-to-DC bulk power supply slot is empty but intentionally not supplied with external DC power will generate a converter alarm unless the muted using the AlmMuteA or AlmMuteB control parameters.

Electrical Input Voltages

- AC-to-DC bulk power supply modules accept AC input in the range of 100 to 240 VAC.
- DC-to-DC converter assemblies accept DC input in the range of -40 to -72 VDC and deliver +24, +5, and -5 VDC output to the chassis midplane.

Power Inlets

Two sets of power inlets are available on the chassis back panel to match the electrical power source available at different installation sites.

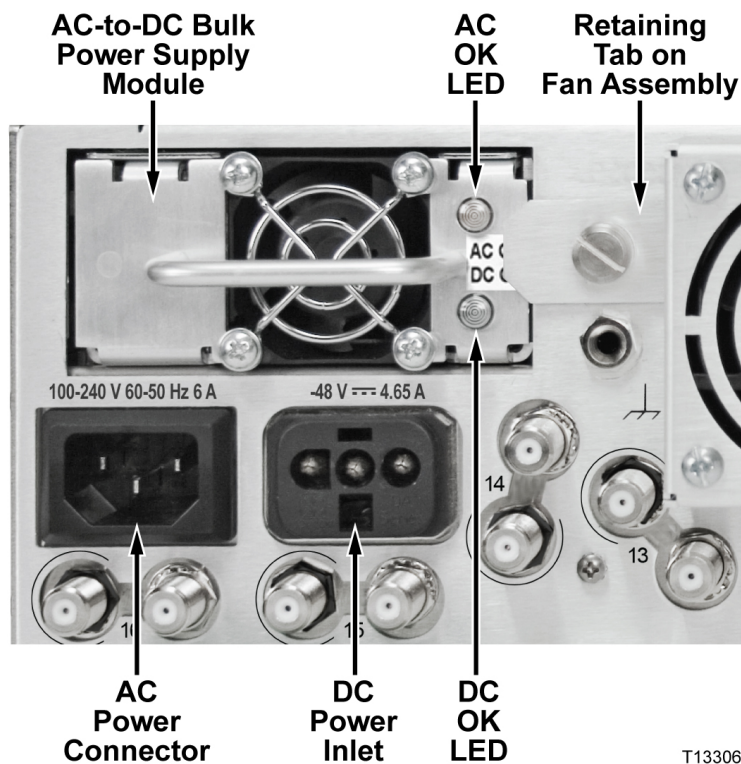
- The DC power inlets accept a nominal -48 VDC input (-40 to -72 VDC). When not used as an input, these connectors can be used to route -48 VDC out for use by other chassis.
- The AC power inlets accept local utility power (100 to 240 VAC, 50 or 60 Hz) via standard IEC power inlets.

The DC power inlets are provided with locking three-wire terminal blocks, which come pre-inserted in the DC power inlets.

Important: Use an equipotential bonding conductor to make a connection from the chassis ground stud to a reliable earthing mechanism at the installation site. For additional information, refer to EN 50083-1/A1:1977.

Note: The chassis ships with the CCB, fan assembly, and DC-to-DC converter assemblies and with no AC-to-DC bulk power supplies installed. The chassis can be ordered with or without an ICIM2-XD installed. See the *Prisma II XD Platform Data Sheet*, part number 7012804 for ordering information.

AC-to-DC Bulk Power Supply Illustration



AC-to-DC Bulk Power Supply Features

Part	Function
AC OK LED	Amber ON - AC OK Amber OFF - No AC
DC OK LED	Green ON - DC OK Green OFF - No DC
Internal fan	Locally controlled by the power supply thermostat

DC-to-DC Converters

All XD chassis ship with two DC-to-DC converter assemblies installed. Both converters are mounted inside the chassis just behind the fan assembly. Each DC-to-DC converter uses the -48 VDC output from its corresponding bulk power supply module to develop +24, +5, and -5 VDC chassis working voltages.

Each DC-to-DC converter has a red LED mounted on its PC board. This LED glows if a fault occurs in the converter while it is under power.

Inspection of the status LEDs and removal and replacement of the DC-to-DC converters requires removal of the fan assembly.



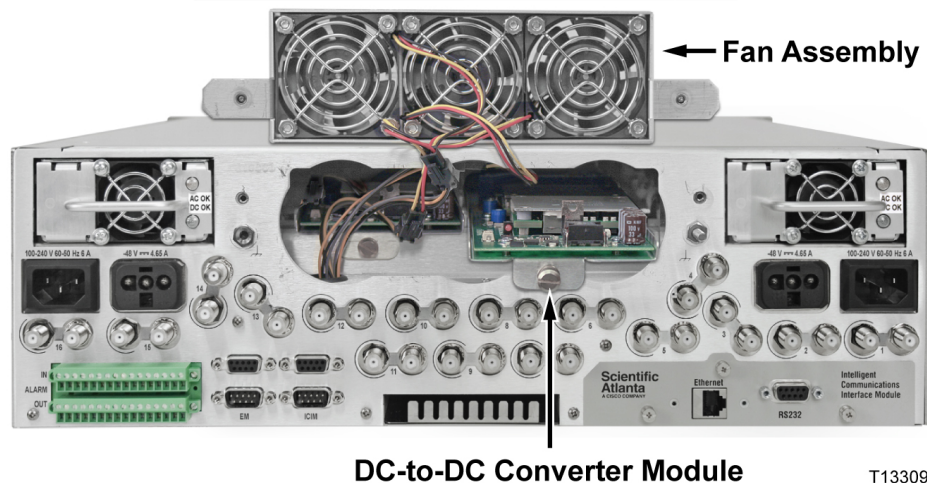
CAUTION:

For a chassis under power, field replacement of the fans, AC-to-DC bulk power supply modules, or DC-to-DC converter assemblies must be completed in two minutes or less to prevent possible chassis overheating due to temporary removal of the fan assembly.

Note:

- Do not operate the chassis with the fan assembly removed for more than two minutes. Otherwise, overheating may result.
- DC-to-DC converters can be replaced in the field but they are not hot-swappable. Before replacing a converter, disconnect its -48 VDC power supply, and do not restore DC power until the converter has been fully installed in the chassis.
- The chassis can remain operational during the converter replacement as long as the second DC-to-DC converter is operating.

DC-to-DC Converter Illustration



Prisma II ICIM2-XD

The ICIM2-XD provides an interface to Prisma II High Density application modules. It supports communication with the application modules via command line interface (CLI), Simple Network Management Protocol (SNMP), or through a user-friendly ICIM Web Interface.

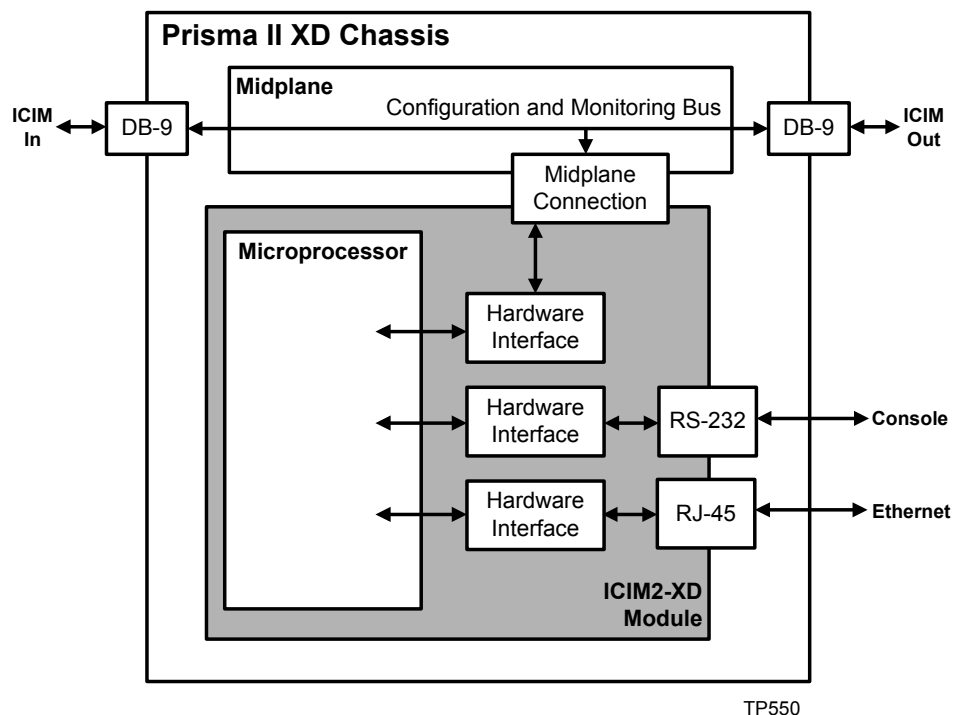
The ICIM2-XD can control up to 64 application modules through a daisy-chain connection of up to four chassis.

Important:

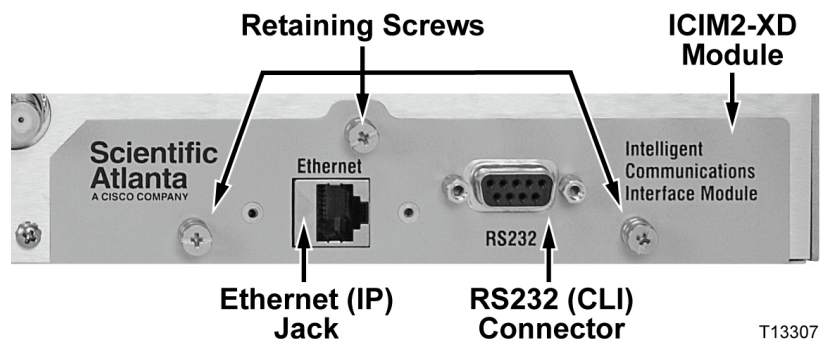
- All chassis connected in a daisy-chain must be powered and have their own fan assembly installed.
- All chassis connected in this daisy-chain must have a unique chassis identification (ID) number.
- To ensure communications with all application modules, only one ICIM2-XD may be installed per daisy-chain configuration.

ICIM2-XD Block Diagram

The main components and functions of the ICIM2-XD are illustrated in the block diagram below.



ICIM2-XD Illustration (Front Panel)



ICIM2-XD Front Panel Features

Part	Function
Ethernet connector	Directly connects the ICIM2-XD to an IP network. The front-panel Ethernet port is suitable for connection to intra-building wiring, non-exposed wiring or cabling only.
RS232 connector	Used to connect a co-located PC to the Prisma II Enhanced system for local console port CLI communication and setup.

3

Hardware Installation

Introduction

This chapter describes site requirements, equipment, tools needed, and instructions for installation of the chassis and its application modules.

In This Chapter

■ Before You Begin.....	60
■ Site Requirements	61
■ Mounting the Chassis in a Rack.....	65
■ Connector Interface Panel.....	67
■ Connecting the ICIM2 to Additional Chassis	68
■ External Alarms Connections	72
■ Fan Assembly	74
■ Installing the Power Supply	75
■ Installing the ICIM2-XD.....	85
■ Installing Application Modules	86
■ Connecting Optical Cables	89
■ Connecting RF Cables	90

Before You Begin

The chassis back panel provides all RF ports, I/O connectors, power inlets and connectors, and ground connections.

ESD jacks are provided on the front and back panels for use when installing or removing application modules, cabling, the fan assembly, AC-to-DC bulk power supplies, DC-to-DC converters, or the ICIM2-XD.

Unpacking and Inspecting the Chassis

As you unpack the chassis, inspect it for shipping damage. If you find any damage, contact Customer Service. Refer to *Customer Support Information* (on page 313) for information on contacting Customer Service. Record the chassis serial number and date of installation for future reference.

Required Equipment and Tools

Before you begin, gather the equipment and tools listed in the following table.

You need . . .	To . . .
a medium-sized Phillips-head or flat-blade screwdriver	tighten the screws that secure the chassis to the equipment rack.
a medium-sized flat-blade screwdriver	tighten and loosen the screws that secure the application modules to the chassis front pane and the fan assembly to the chassis back panel.
a small Phillips-head or flat-blade screwdriver	tighten the screws that secure the ICIM2-XD module to the chassis back panel.
application module extraction tool, part number 4022921 (supplied with XD chassis)	remove application modules from the chassis as needed.

Note: Always use a tool when loosening or tightening the screws that hold the application modules to the chassis front panel.

Site Requirements

This section describes environmental, physical, and wiring requirements to be met prior to equipment installation. Before you begin, make certain that your installation site meets the requirements discussed in this section.

Operating Environment



CAUTION:

Avoid damage to this product! Operating this product outside the specified operating temperature limits voids the warranty.

Follow these recommendations to maintain an acceptable operating temperature for the equipment.

- Operating temperature at the air inlet must be between 0°C and 50°C (32°F and 122°F).
- Keep cooling vents clear and free of obstructions.
- Provide ventilation as needed using one or more of the following methods.
 - Air-deflecting baffles
 - Forced-air ventilation
 - Air outlets above enclosures, either alone or in combination

Note: Refer to module data sheets and product guides for product-specific module temperature specifications.

Chassis Wiring and Fusing

Important: All chassis configurations require an external fuse or circuit breaker (AC and DC current ratings differ; see below) and #16 AWG wiring for both power and grounding.

AC Power Systems

AC power for each AC-to-DC bulk power supply module enters the chassis through a dedicated back-panel IEC power inlet for each power supply module.

Confirm that the IEC power cord or cords supplied with the chassis have the correct plug configuration for the country of use.

The voltage input range for AC systems is 100 to 240 VAC, single phase, 50-60 Hz.

AC input current is 14 A maximum. The chassis should be connected to a single outlet circuit with fuse or circuit breaker overcurrent protection rated 15 A minimum.

Important:

- Use only a grounded electrical outlet when connecting the unit to a power source. If you do not know whether the outlet is grounded, consult with a qualified electrician.
- Maintain reliable earth grounding of rack-mounted equipment. Pay particular attention to supply and ground connections made via power strips or any method other than direct connection to the branch circuit.

DC Power Systems

External -48 VDC operating power for each DC-to-DC converter (mounted in the chassis just behind the fan assembly) enters the chassis via a dedicated DC power inlet mounted on the chassis back panel.

The voltage input range for DC power systems is -40 VDC to -72 VDC.

Use #16 AWG wire for DC field wiring. The #16 AWG wiring from the external -48 VDC supply is attached to a 3-pin nylon connector which, in turn, plugs into the DC power inlet.

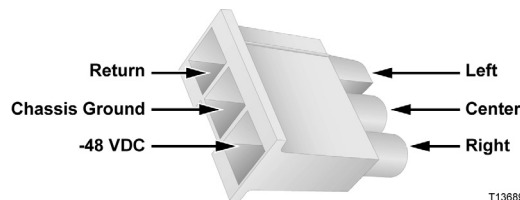
Terminate the chassis side of the cable with a nylon plug of the type supplied with the chassis. Order additional nylon plugs and connector pins from your preferred supplier, as follows:

- Molex #03-12-1036 nylon 3-pin connector
- Molex #18-12-1222 crimp socket contact (3)

Use a Molex Crimp Service Tool #63811-1000 or equivalent to crimp the pins to the cable.

After terminating the cable, twist the conductors loosely (a full turn every few inches is sufficient).

As installed in the DC power connector with the locking tab down, the left pin of the nylon connector is the return, the right pin carries -48 VDC, and the center pin is chassis ground.



Connect the chassis to a reliably grounded DC power source that is electrically isolated from the AC power source.

Important:

- Branch circuit overcurrent protection must be provided by a fuse or circuit breaker with a voltage rating of 72 VDC minimum and a current rating of 18 A

maximum.

- The DC field wiring must include a readily accessible disconnect device that is suitably approved and rated.

Earth-Grounding Conditions

The chassis is designed to permit connection of the earthed conductor of the DC supply circuit to chassis ground. Before making this connection, confirm that all of the following conditions are met:

- The chassis is connected directly to the DC supply system earthing electrode conductor or to a bonding jumper from an earthing terminal bar or bus to which the DC supply system earthing electrode conductor is connected.
- The chassis is located in the same immediate area as other equipment connected between the earthed conductor of the same DC supply circuit and earthing conductor, such as in an adjacent cabinet. Also, the point of earthing of the DC system must not be earthed elsewhere.
- The DC power source is located within the same premises as the chassis.
- There are no switching or disconnecting devices in the earthed circuit conductor between the DC source and the point of connection of the earthing electrode conductor.

DC Power Passing

An XD chassis with at least one AC-to-DC bulk power supply module installed can serve as an external DC power source for a second XD chassis. Passing DC power from one chassis to another requires a DC power-passing cable made up as described above, but with both ends of the cable terminated by a nylon DC power connector. Two assembled DC power-passing cables are also available from the factory:

- Part number 4011730, 3 m DC power-passing cable
- Part number 4023718, 2 ft DC power-passing cable

Rack Location Requirements

Follow these recommendations when installing the chassis in a rack.

- Locate the rack away from strong RF radiation and line transients that can damage the equipment.
- Locate the rack in an area that permits access to connectors on the front and rear of the chassis as needed.

Unused Slots

Important: All unused slots in the chassis must be filled with blanking panels. Application module blanking panels, part number 4023066, are available from the factory. Replacement AC-to-DC bulk power supply blanking panels (part number 4021618) and ICIM2-XD blanking panels (part number 4021163) are also available, if needed.

Mounting the Chassis in a Rack

To Install the Chassis in a Rack

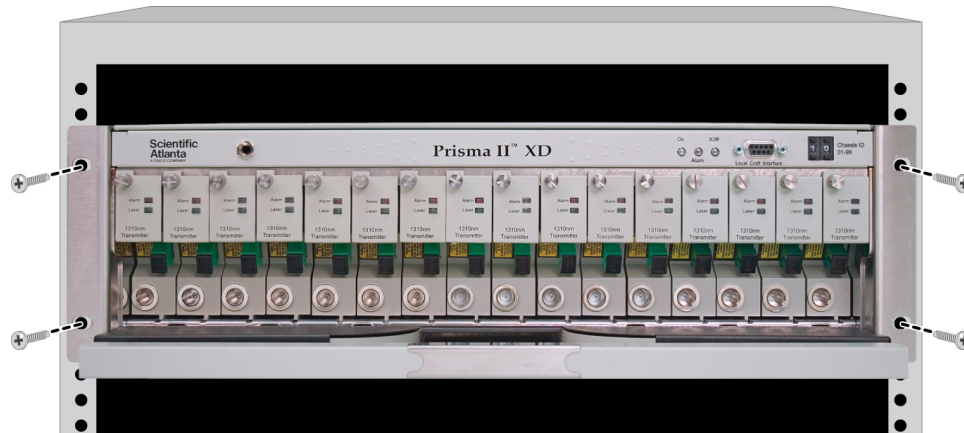


WARNING:

The Prisma II XD Chassis weighs approximately 25 lbs (11.3 kg) empty and 40 lbs (18.1 kg) fully loaded. To avoid personal injury and equipment damage, use safe handling and lifting practices in accordance with your organization's procedures.

Complete the following steps to mount the chassis in a 19-inch rack.

- 1 Use a torque wrench to tighten the bracket mounting screws to 12 to 14 in-lbs (1.36 to 1.58 Nm).
- 2 Position the chassis in the rack with the fan assembly installed, but otherwise empty.
- 3 Insert a mounting screw through each of the four mounting holes on chassis front panel, and then into the rack.



T13303

- 4 Use a medium-sized Phillips-head screwdriver to tighten each mounting screw until it is tight.
- 5 Install additional cable and fiber management hardware as needed and in accordance with local practice.

Chassis Dimensions

Use the dimensions given below to determine clearance requirements for installing the chassis in the rack.

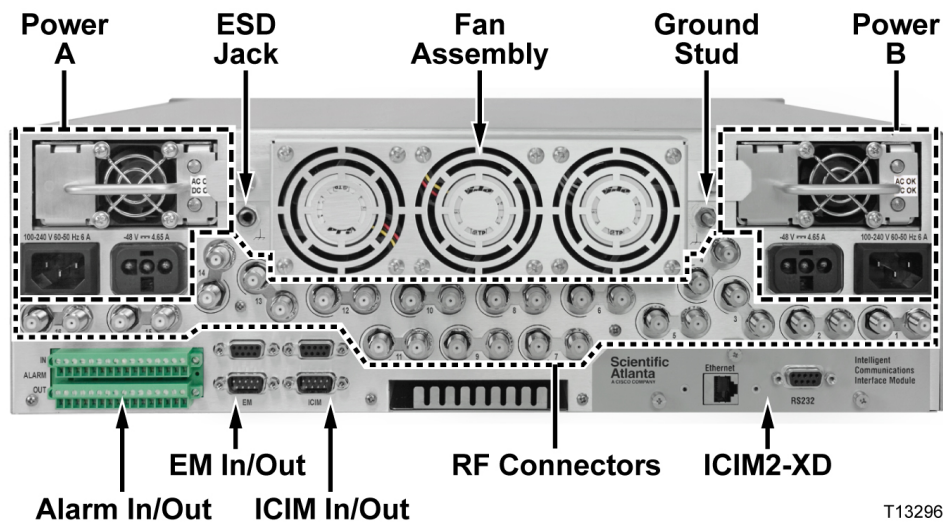
Dimension	English	Metric
Height	5.25 in.	13.3 cm
Width	17.5 in.	44.5 cm

Chapter 3 Hardware Installation

Depth	22 in.	55.9 cm
-------	--------	---------

Connector Interface Panel

All electrical and non-optical interface connections are made at the chassis back panel.



Connecting the ICIM2 to Additional Chassis

This platform allows an ICIM2 or ICIM2-XD located in one chassis to monitor and control application modules located in several other chassis. To establish chassis-to-chassis ICIM2 communication, use the **ICIM IN** and **ICIM OUT** connectors located on the chassis interface panel.

Complete the following steps to establish chassis-to-chassis ICIM2 communication:

- 1 Connect a cable from ICIM OUT on the chassis containing the ICIM2 or ICIM2-XD to ICIM IN on the second chassis.
- 2 If required, connect a second cable from ICIM OUT on the second chassis to ICIM IN on the third chassis.
- 3 If required, connect a third cable from ICIM OUT on the third chassis to ICIM IN on the fourth chassis.

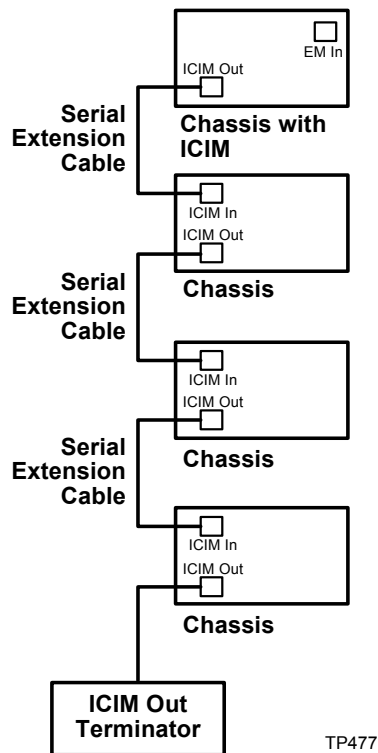
Note: An ICIM2 or ICIM2-XD can control up to 64 application modules in a chassis daisy-chain of no more than 4 chassis.

To Make ICIM IN and ICIM OUT Cable Connections

Complete the following steps to make chassis-to-chassis **ICIM IN** and **ICIM OUT** connections.

- 1 Connect the serial extension cable from the **ICIM OUT** of the chassis containing the ICIM2 or ICIM2-XD to the **ICIM IN** connector of the second chassis.
- 2 Change the chassis ID numbers as needed to give each chassis an appropriate unique ID number. See **To Change the Chassis ID Number** below for further details.
- 3 Connect a serial extension cable from the **ICIM OUT** of the second chassis to the **ICIM IN** of the third chassis.
- 4 Continue this daisy-chain connection until all chassis are connected.

- 5 The ICIM OUT port of the last chassis in the daisy-chain must be terminated with an ICIM OUT terminator, part number 4013014, which ships with the ICIM2 or ICIM2-XD.



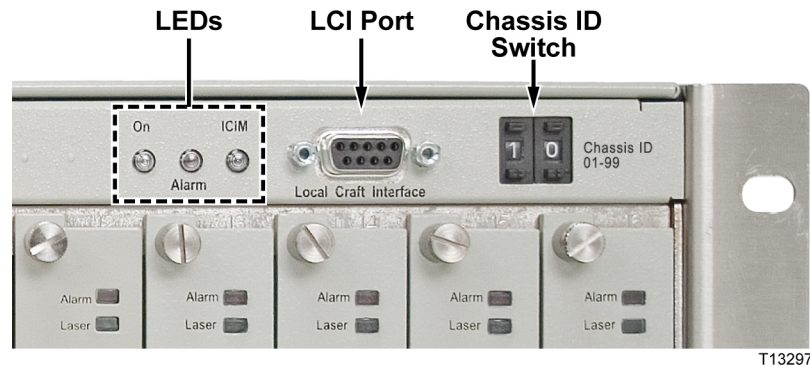
Note:

- All chassis connected in this daisy-chain must be powered and have a fan tray or fan assembly installed. For correct operation, proper cooling of the chassis must be maintained over the specified temperature range.
- A single chassis equipped with an ICIM2 or ICIM2-XD must also have its ICIM OUT port terminated with an ICIM OUT terminator, part number 4013014. The ICIM OUT terminator ships with the ICIM2 or ICIM2-XD.

To Change the Chassis ID Number

Complete the following steps to change the chassis ID number.

- 1 Locate the chassis ID switch at upper right on the front panel of each chassis. The switch can be set to any two-digit value from 00 to 99 (but avoid setting the value to 00, as explained below).



- 2 Use the chassis ID switch to set each chassis ID number to a unique value.

Note:

- The chassis ID number can be changed while the chassis is under power. However, the new ID number will not become effective until chassis power is cycled or the ICIM2-XD is rebooted.
- The chassis numbering scheme used is discretionary, except that each interconnected chassis must have a unique ID number.
- It is important to avoid using chassis ID number 00 in some circumstances, as explained in the following caution.



CAUTION:

Setting the chassis ID to 00 is not recommended as it causes the entity MIB to violate RFC-2737 by creating an invalid object identifier. This may affect operation with some management systems that use the entity MIB. In particular, attempts to access the fans (in virtual slot 0) in chassis 00 will fail if made via serial TNCS (or ROSA-EM) or LCI.

Important: If you change the chassis ID number while the chassis is under power, you must cycle power to the chassis or reboot the ICIM2-XD in order for the new number to take effect.

ICIM IN and ICIM OUT Cables

The cable required for both **ICIM IN** and **ICIM OUT** connections is a shielded 9-wire serial extension cable, DB9 Female to DB9 Male. This cable can be purchased locally or from the factory. The chassis data sheet lists the part number for a 6-foot DB9 Female to DB9 Male serial extension cable. The connectors are a serial 9-pin D-shell (EIA 574/232).

Chassis-to-Chassis ICIM2 Activation

Once the chassis are interconnected, the shared ICIM2 or ICIM2-XD should be forced to search for all new modules, rather than be allowed to find them incrementally over the course of a polling cycle.

The recommended method for forcing a search for new modules is to reboot the ICIM2 or ICIM2-XD. This can be accomplished either by physically removing and reinserting the ICIM2 or by issuing a **reboot** command to the ICIM2 via the CLI interface.

To reboot the ICIM2 or ICIM2-XD via CLI, open a console or Telnet session and type the following commands at the CLI prompt.

```
CLI> icim  
ICIM> reboot
```

The response will be:

```
The ICIM2 is about to reboot. This will end all current login and web sessions  
Are you sure you want to proceed (Yes/No)> yes
```

```
SUCCESS!  
ICIM>
```

```
Scientific-Atlanta Intelligent Communications Interface Module (ICIM)
```

```
-----  
W A R N I N G  
-----
```

```
Unauthorized or improper use of this system may result in  
administrative disciplinary action and civil or criminal penalties.  
By continuing to use this system you indicate your awareness of and  
consent to these terms and conditions of use. LOG OFF IMMEDIATELY  
if you do not agree to the conditions stated in this warning.
```

```
login:
```

Each of the additional modules will then be added to the ICIM2 or ICIM2-XD polling cycle.

Note: Use of the CLI **reboot** command is preferred over the **updateid** command in this case because a reboot will maintain synchronization with the element management system.

External Alarms Connections

This platform supports hardware redundancy through external alarm connections provided on each chassis. This feature can be used to set up a "master-slave" relationship between a primary set of modules in one chassis and a backup set of similar modules located in a separate chassis.

Master-Slave Operation

All Prisma II modules ship from the factory configured for independent operation, referred to as Single mode. For redundant operation, these modules can be reconfigured to operate in Master mode or Slave mode through the command line interface (CLI) or ICIM Web Interface.

The chassis allows for local hard-wired redundancy by using the ALARM IN and ALARM OUT connectors on the connector interface panel. With these connectors, a Master-Slave pair of modules can be configured so that if the Master fails, the Slave takes over.

ALARM IN and OUT Connections

The chassis provides two sets of connections for external alarms to and from each module slot. These alarm connections are provided via a pair of connectors labeled ALARM IN and ALARM OUT on the chassis back panel.

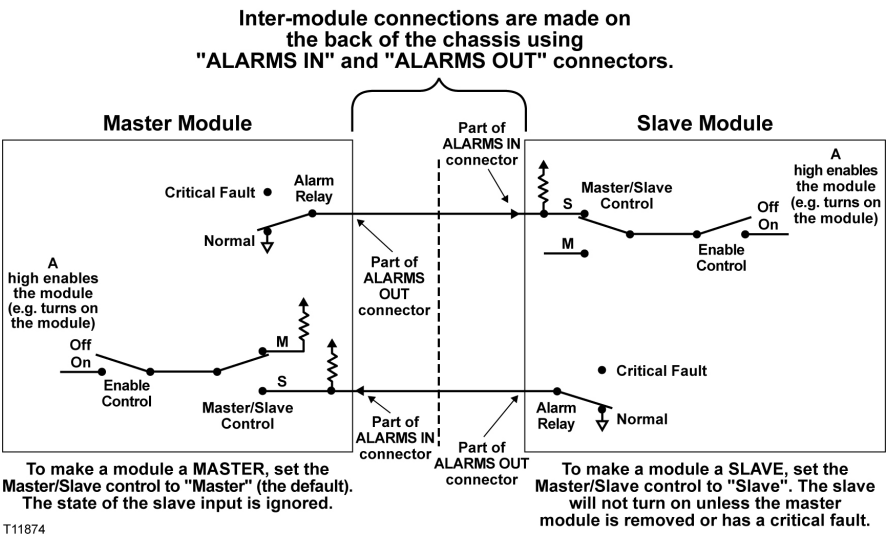
When a critical alarm occurs in a master module, the master turns off and the slave (redundant module) is enabled. To make this happen, the pin representing the master module slot in the ALARM OUT connector must be wired to the pin representing the slave module slot in the ALARM IN connector.

Master and slave modules can be installed either in the same chassis or in different chassis, as long as the modules are correctly configured and interconnected.

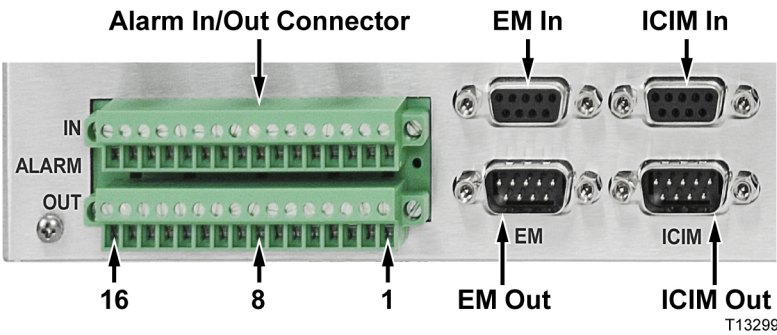
Note:

- After setting up the modules, it is important to ensure that they are not moved to different slots. Otherwise, the ALARM IN and OUT connections will have to be rearranged.
- A module cannot act as both a master and a slave. Accordingly, any module configured as a master ignores its own ALARM IN contacts.
- To verify proper wiring and redundant configuration, unplug the master device and confirm that the slave module turns on as a result.

Master-Slave Illustration



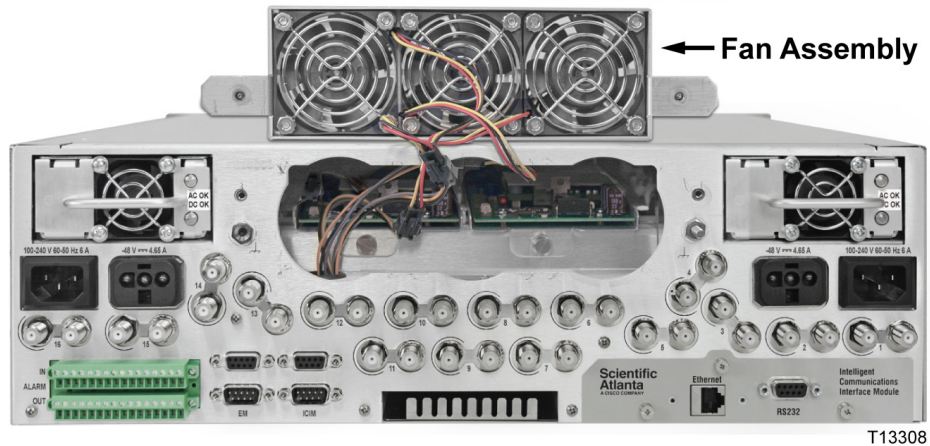
ALARM IN and OUT Terminal Blocks



Fan Assembly

To Remove the Fan Assembly

The fan assembly is installed at the factory. It can be removed for maintenance or inspection or to access the DC-to-DC converter assemblies by loosening the two screws located on either side of the assembly, as shown below.



Important: Do not operate any chassis without the fans installed. For correct operation, proper cooling of the chassis must be maintained over the specified temperature range.



CAUTION:

Always use a screwdriver to loosen or tighten the screws holding the application modules, ICIM2-XD, fan assembly, power supply modules, DC-to-DC converters, or blanking panels in place. Do not attempt to loosen or tighten these screws solely by hand.



CAUTION:

For a chassis under power, field replacement of the fans, AC-to-DC bulk power supply modules, or DC-to-DC converter assemblies must be completed in two minutes or less to prevent possible chassis overheating due to temporary removal of the fan assembly.

Installing the Power Supply

Power Supply Requirements

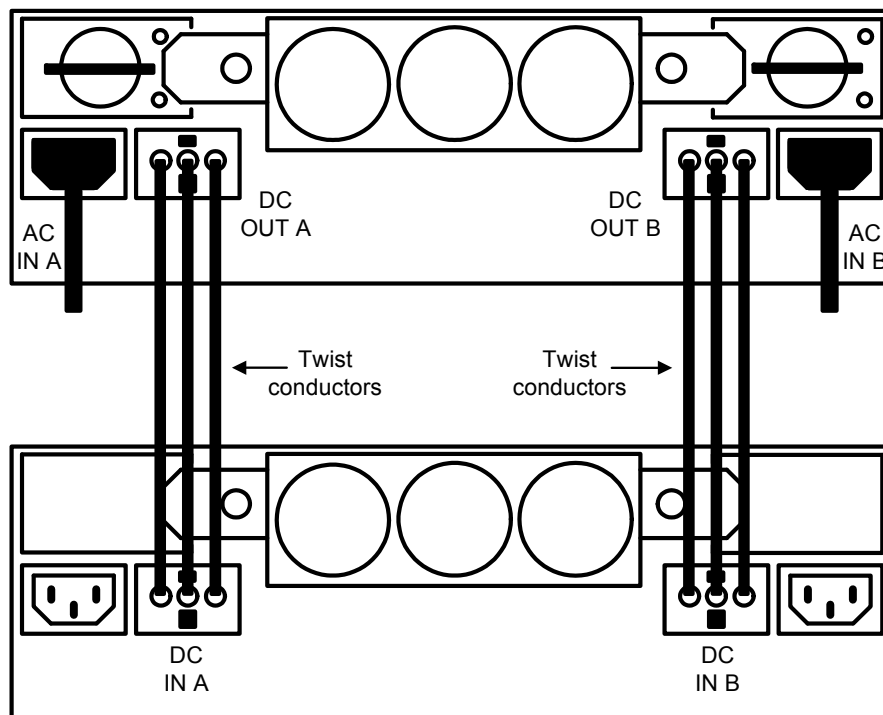
The chassis accepts one or two AC-to-DC bulk power supply modules. These modules fit in dedicated slots on either side of the chassis back panel.

AC-to-DC bulk power supplies convert incoming utility AC power (100 to 240 VAC, 50 or 60 Hz) to -48 VDC for use by DC-to-DC converters inside the chassis. The internal DC-to-DC converters in turn generate the chassis midplane bus working voltages at +24, +5, and -5 VDC.

Power Sharing

Two Prisma II XD Chassis can operate from a single AC-to-DC bulk power supply module or from a pair of bulk power supply modules. A power-chain connection is used to route -48 VDC from a chassis with one or both bulk power supply modules installed to a second chassis whose corresponding bulk power supply module slots are empty and have blanking panels installed.

The following illustration shows the recommended cabling for power sharing between an exclusively AC powered chassis (top) and an exclusively DC powered chassis (bottom).



TP476

Electrical Power Connections

The chassis back panel has an IEC standard AC power inlet and a three-conductor DC power connector for each bulk DC power supply module slot.

- The AC power inlet accepts line voltage at 100 to 240 VAC, 50 or 60 Hz.
- The DC power connector accepts DC input voltage at -40 to -72 VDC (-48 VDC nominal).

The power connectors on the left side of the chassis supply power to the left power supply slot, while those on the right supply power to the right power supply slot. Except for their chassis ground pins, all four power connectors are electrically independent of each other.

Important: Tie the system to earth ground via the ground stud.

Note: For DC power supplies, the return terminal is an "isolated DC return," i.e., it is not connected to the chassis framework.

Chassis Wiring and Fusing

Important: All chassis configurations require an external fuse or circuit breaker (AC and DC current ratings differ; see below) and #16 AWG wiring for both power and grounding.

AC Power Systems

AC power for each AC-to-DC bulk power supply module enters the chassis through a dedicated back-panel IEC power inlet for each power supply module.

Confirm that the IEC power cord or cords supplied with the chassis have the correct plug configuration for the country of use.

The voltage input range for AC systems is 100 to 240 VAC, single phase, 50-60 Hz.

AC input current is 14 A maximum. The chassis should be connected to a single outlet circuit with fuse or circuit breaker overcurrent protection rated 15 A minimum.

Important:

- Use only a grounded electrical outlet when connecting the unit to a power source. If you do not know whether the outlet is grounded, consult with a qualified electrician.
- Maintain reliable earth grounding of rack-mounted equipment. Pay particular attention to supply and ground connections made via power strips or any method other than direct connection to the branch circuit.

DC Power Systems

External -48 VDC operating power for each DC-to-DC converter (mounted in the chassis just behind the fan assembly) enters the chassis via a dedicated DC power inlet mounted on the chassis back panel.

The voltage input range for DC power systems is -40 VDC to -72 VDC.

Use #16 AWG wire for DC field wiring. The #16 AWG wiring from the external -48 VDC supply is attached to a 3-pin nylon connector which, in turn, plugs into the DC power inlet.

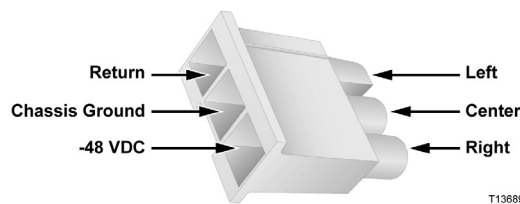
Terminate the chassis side of the cable with a nylon plug of the type supplied with the chassis. Order additional nylon plugs and connector pins from your preferred supplier, as follows:

- Molex #03-12-1036 nylon 3-pin connector
- Molex #18-12-1222 crimp socket contact (3)

Use a Molex Crimp Service Tool #63811-1000 or equivalent to crimp the pins to the cable.

After terminating the cable, twist the conductors loosely (a full turn every few inches is sufficient).

As installed in the DC power connector with the locking tab down, the left pin of the nylon connector is the return, the right pin carries -48 VDC, and the center pin is chassis ground.



Connect the chassis to a reliably grounded DC power source that is electrically isolated from the AC power source.

Important:

- Branch circuit overcurrent protection must be provided by a fuse or circuit breaker with a voltage rating of 72 VDC minimum and a current rating of 18 A maximum.
- The DC field wiring must include a readily accessible disconnect device that is suitably approved and rated.

Earth-Grounding Conditions

The chassis is designed to permit connection of the earthed conductor of the DC supply circuit to chassis ground. Before making this connection, confirm that all of the following conditions are met:

- The chassis is connected directly to the DC supply system earthing electrode conductor or to a bonding jumper from an earthing terminal bar or bus to which the DC supply system earthing electrode conductor is connected.
- The chassis is located in the same immediate area as other equipment connected between the earthed conductor of the same DC supply circuit and earthing conductor, such as in an adjacent cabinet. Also, the point of earthing of the DC system must not be earthed elsewhere.
- The DC power source is located within the same premises as the chassis.
- There are no switching or disconnecting devices in the earthed circuit conductor between the DC source and the point of connection of the earthing electrode conductor.

DC Power Passing

An XD chassis with at least one AC-to-DC bulk power supply module installed can serve as an external DC power source for a second XD chassis. Passing DC power from one chassis to another requires a DC power-passing cable made up as described above, but with both ends of the cable terminated by a nylon DC power connector. Two assembled DC power-passing cables are also available from the factory:

- Part number 4011730, 3 m DC power-passing cable
- Part number 4023718, 2 ft DC power-passing cable

DC Power Connectors

The chassis back panel provides a separate DC power connector for each AC-to-DC bulk power supply slot. The chassis ships with a white nylon plug installed in each DC power connector. These white nylon plugs have no pins installed, and serve mainly to guard against potential improper use of the DC power connector.



CAUTION:

A single DC power connector cannot act as in input and an output connector at the same time. Before applying external DC power, confirm that the AC-to-DC bulk power supply slot associated with the DC power connector is empty and covered by a blanking panel.

Each DC power connector on the chassis back panel can serve as either a DC power inlet or a DC power outlet, but not both, as follows:

- With no AC-to-DC bulk power supply module installed, the corresponding DC power connector can serve as an inlet for -48 VDC supplied by a battery room, a second XD chassis, or another external DC power source. In this configuration, however, the same DC power connector cannot be used as a -48 VDC output.
- With an AC-to-DC bulk power supply module installed, the corresponding DC power connector can serve as an outlet for -48 VDC to power a second XD

chassis. In this configuration, however, the same DC power connector cannot be used as a DC power inlet.

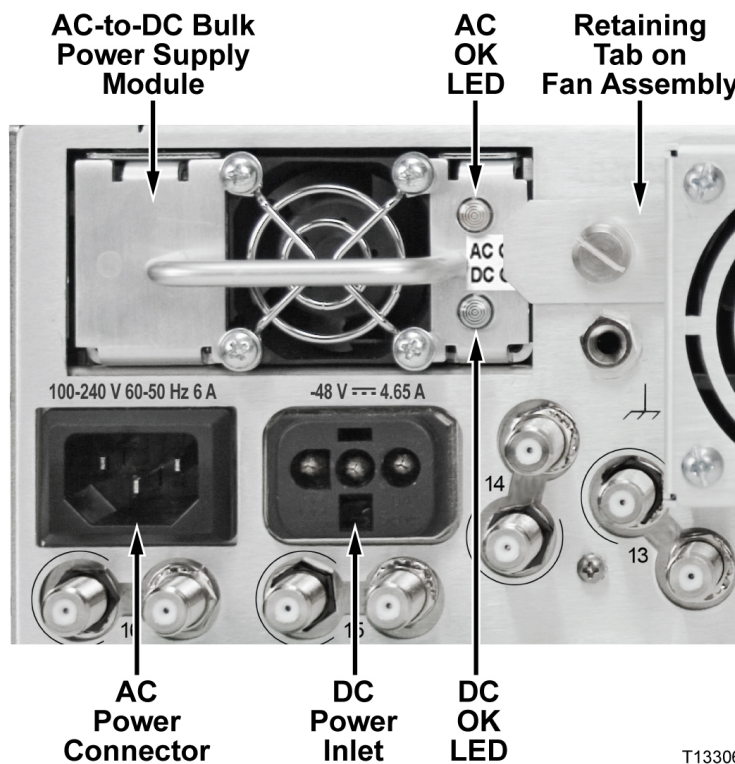


CAUTION:

When connecting chassis together for power sharing, use either a factory DC power-passing cable, part number 4011730 (3 m) or 4023718 (2 ft), or a custom cable made in accordance with the instructions in this document. Use of other cables for this purpose is not supported.

Power Inlet Illustration

The following illustration shows locations of the AC and DC power connectors on the chassis back panel.



T13306

To Install the Power Cord

AC Power Cord

Important: The XD chassis is not supplied with an AC power cord. To complete this procedure, you must order the correct power cord for your region. For ordering information, see the *Prisma II XD Platform Data Sheet*, part number 7012804.

Complete the following steps to install an AC power cord for each bulk power supply module.

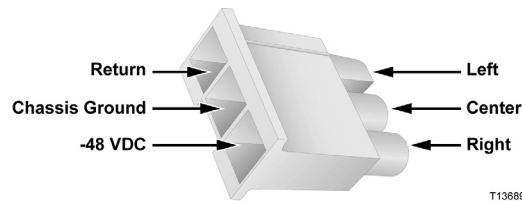
- 1 Confirm the location(s) of bulk power supply modules installed in slot A or slot B, or both A and B.

- 2 Insert the IEC plug of each AC power cord into the back-panel IEC power inlet for each installed bulk DC power supply module.
- 3 Attach the plug end of each AC power cord into an AC power receptacle.

DC Power Cord

Complete the following steps to install one or more DC power cords for each unused bulk DC power supply slot as needed.

- 1 Confirm that each unused bulk power supply slot is empty and covered by a blanking panel.
- 2 Locate the DC wire terminal block (white nylon plug) pre-installed in each back-panel DC power connector.
- 3 Remove the terminal block and note the locations of the left, middle, and right terminals as shown below.



- 4 Obtain conductive pins (Molex #18-12-1222) for each DC wire terminal block for each conductor to be used.
- 5 Attach #16 AWG power cable from the fuse panel to the pins and install them in the terminal block as follows:
 - Left terminal: Return conductor
 - Middle terminal: Chassis ground (optional)
 - Right terminal: -48 VDC conductor
- 6 Insert the wire terminal block into the DC power connector until it locks. Tug lightly on the terminal block to confirm that it is locked in position.
- 7 Twist the conductors loosely along the full length of the power cord (a full turn every few inches is sufficient).

To Install the Power Supply in the Chassis

Complete the following steps to install an AC-to-DC bulk power supply module in an available chassis slot.

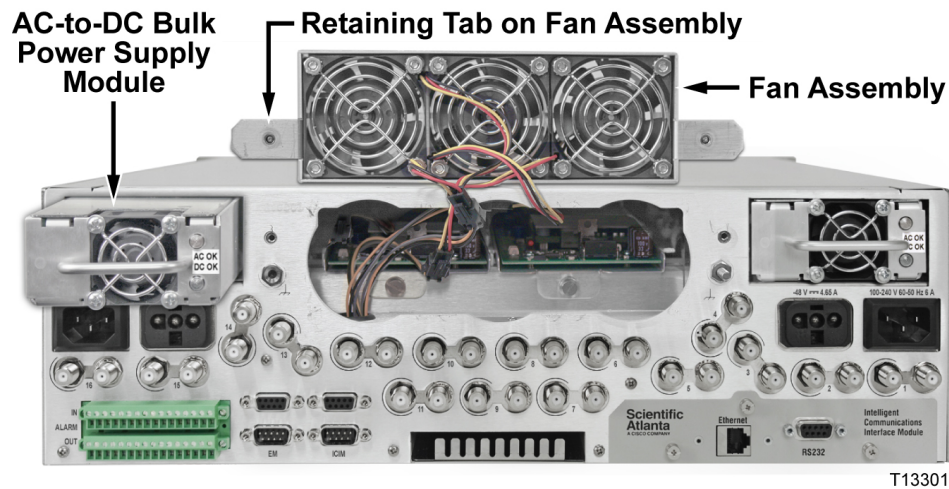


CAUTION:

Always use a screwdriver to loosen or tighten the screws holding the application modules, ICIM2-XD, fan assembly, power supply modules, DC-to-DC converters, or blanking panels in place. Do not attempt to loosen or tighten these screws solely by hand.

- 1 On the chassis back panel, loosen the two screws holding the fan assembly in place. Remove the fan assembly and set it aside temporarily.

- 2 Remove the blanking panel that covers the bulk power supply slot opening.
- 3 Pick up the bulk power supply module by its handle and insert the module into the open module slot, as shown in the following illustration.



- 4 Gently slide the power supply module into the chassis until its power connections join connectors on the midplane bus. *Do not force the module into the chassis.* If properly aligned, it should slide in with minimal force.
- 5 If installing a second power supply, repeat the steps above for the second power supply slot, and then continue with step 6.
- 6 Confirm that a DC-to-DC converter assembly is installed inside the chassis next to the new bulk power supply module. This converter will be visible inside the fan opening, mounted horizontally and held in place by a retaining screw.
- 7 Reinstall the fan assembly and tighten the two screws holding it and the power supply module(s) in position.
- 8 Apply power and verify that the green LED on the front panel of each power supply module illuminates, indicating normal operation.
- 9 Confirm that the fan assembly is operational. The fans should be audible once the power supply is operating.

Power Supply Cooling Fans

Each power supply module has internal fans that provide airflow for cooling.

To Install the DC-to-DC Converter

Complete the following steps as needed to install a DC-to-DC converter assembly in the chassis.

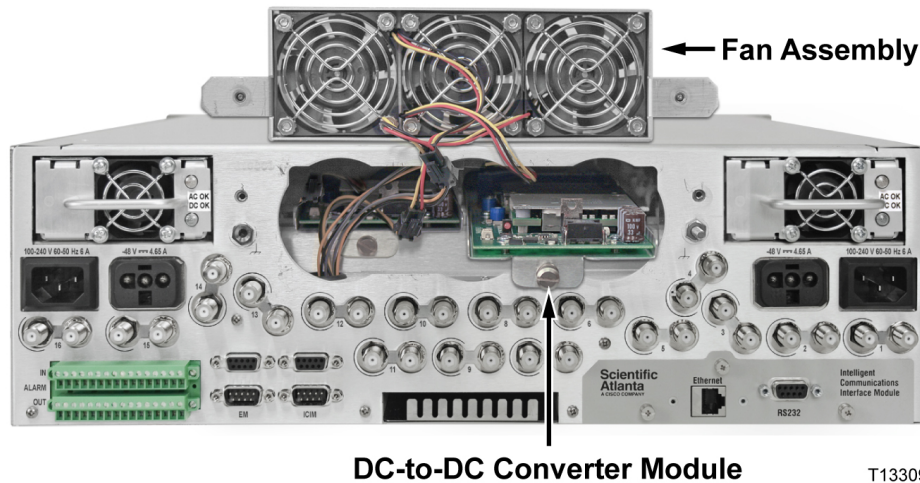


CAUTION:

Always use a screwdriver to loosen or tighten the screws holding the application modules, ICIM2-XD, fan assembly, power supply modules, DC-to-DC converters, or blanking panels in place. Do not attempt to loosen or tighten these screws solely by hand.

- 1 If necessary, loosen the two screws holding the fan assembly in place, remove the fan assembly, and set it aside temporarily.
- 2 Locate the appropriate position for the DC-to-DC converter assembly on top of the horizontal shelf just inside the fan assembly opening.

Note: There are two positions for DC-to-DC converter assemblies, one for each possible AC-to-DC bulk power supply module installed.



- 3 Gently slide the DC-to-DC converter assembly into the chassis until its power connections join connectors on the midplane bus. *Do not force the converter into the chassis.* If properly aligned, it should slide in with minimal force.
- 4 If installing a second DC-to-DC converter, repeat the steps above for the second converter, and then continue with step 5.
- 5 Briefly apply power and verify that the red LED on the DC-to-DC converter board(s) remains unlit, indicating normal operation.



CAUTION:

For a chassis under power, field replacement of the fans, AC-to-DC bulk power supply modules, or DC-to-DC converter assemblies must be completed in two minutes or less to prevent possible chassis overheating due to temporary removal of the fan assembly.

- 6 Reinstall the fan assembly and tighten the two screws holding it and the power supply module(s) in position.
- 7 Confirm that the fan assembly is operational. The fans should be audible once the power supply is operating.

To Monitor the Power Supply

The AC-to-DC bulk power supplies and DC-to-DC converters may be monitored remotely via the ICIM2-XD using CLI or SNMP commands. Use any of the following methods to monitor power supply operational and alarm status.

- LEDs on each bulk power supply indicate its operational and alarm status. The ON LED monitors electrical power into the module, and the ALARM LED monitors alarms in module temperature or module failure.
- Command Line Interface (CLI) commands may be used to obtain power supply or other module status information either through an attached personal computer or over a network.
- Simple Network Management Protocol (SNMP) commands also may be used to obtain power supply or other module status information remotely.

For information on power supply monitoring using CLI commands or the ICIM Web Interface, refer to the *Prisma II Platform Remote User Interface Guide, System Release 2.03*, part number 4025477. For information on power supply monitoring using SNMP commands, refer to *SNMP Management* (on page 167).

To Enable Power Passing

Complete the following steps to enable power passing between two Prisma II XD Platform chassis.

- 1 On the chassis supplying power, identify an available DC power connector whose corresponding AC-to-DC bulk power supply slot is populated.
- 2 On the chassis receiving power, identify an available DC power connector whose corresponding AC-to-DC bulk power supply slot empty and covered by a blanking panel.
- 3 Install a DC power-passing cable (described below) between the two DC power connectors just identified.

DC Power-passing Cable

Two assembled DC power-passing cables are currently available from the factory:

- Part number 4011730, 3 m DC power passing cable
- Part number 4023718, 2 ft DC power passing cable

DC power-passing cables can also be made up in custom lengths to suit the needs of specific installations. The cable used to pass DC power from one chassis to another must have the following characteristics:

- Return (left) conductor - #16 AWG insulated stranded wire
- -48 VDC (right) conductor - #16 AWG insulated stranded wire
- Ground (center) conductor - #16 AWG insulated stranded wire

Chapter 3 Hardware Installation

- Conductors twisted together loosely (a full turn every few inches is sufficient)
- Both ends terminated by white nylon connectors of the type supplied with the chassis

Installing the ICIM2-XD

Note: To ensure communications with all application modules, install the ICIM2-XD in the dedicated slot on the back of the chassis. Install only one ICIM2 or ICIM2-XD per daisy-chain configuration.

To Install the ICIM2-XD

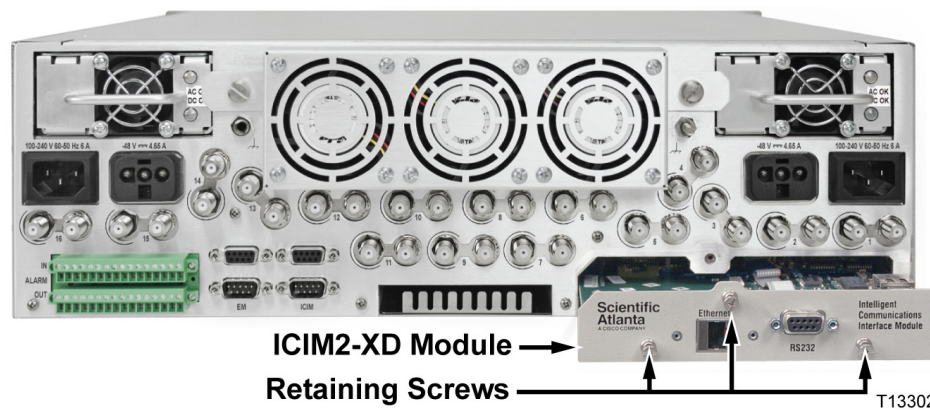
Complete the following steps to install the ICIM2-XD in the chassis.



CAUTION:

Always use a screwdriver to loosen or tighten the screws holding the application modules, ICIM2-XD, fan assembly, power supply modules, DC-to-DC converters, or blanking panels in place. Do not attempt to loosen or tighten these screws solely by hand.

- 1 Remove the blanking panel covering the ICIM slot in the lower right corner of the chassis back panel.
- 2 Hold the ICIM2-XD so that the front panel silkscreen is in correct reading position.
- 3 Align the two ridges on the bottom of the ICIM2-XD with the module guide slots located in the chassis.



- 4 Gently slide the ICIM2-XD into the chassis until its power and communications connections join connectors on the back plane bus and its front panel rests against the chassis. *Do not force the ICIM2-XD into the chassis.* If properly aligned, it should slide in with minimal force.
- 5 Tighten the retaining screws on either side of the ICIM2-XD to secure it in the chassis. Use a 3/8-in. flat-blade screwdriver to secure. *Do not over-tighten.*

Installing Application Modules

All XD application modules are hot-swappable and plug-and-play. This means that they can be installed or replaced without removing power from the chassis, and without affecting the operation of other modules installed in the chassis.

Important:

- The following procedure assumes that the chassis is mounted in a rack.
- When an application module is inserted into the chassis, one or more alarms may be generated momentarily while the module powers up. This will be briefly indicated on the module LED and may also generate an alarm in the event log. This is normal and does not indicate a module problem.

To Install the Module



WARNING:

Avoid damage to your eyes! Do not look into any optical connector while the system is active. Even if the unit is off, there may still be hazardous optical levels present.

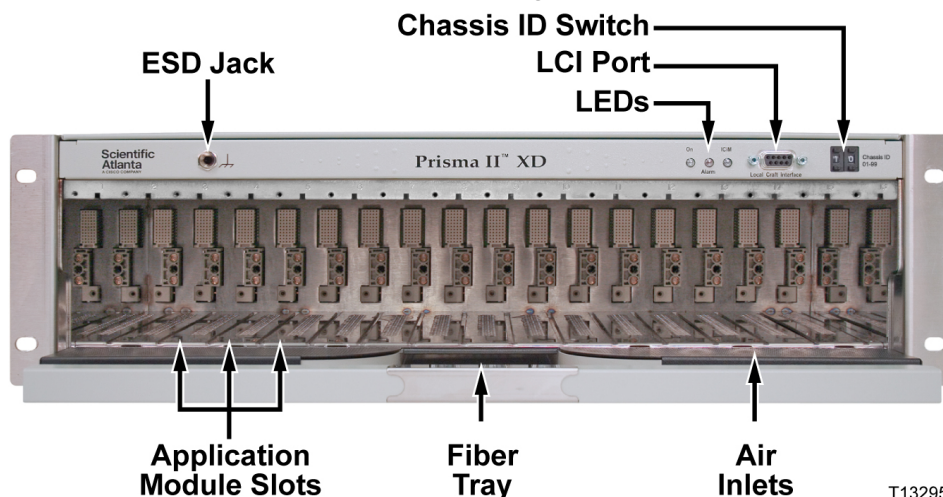
Complete the following steps to install the module in the chassis.



CAUTION:

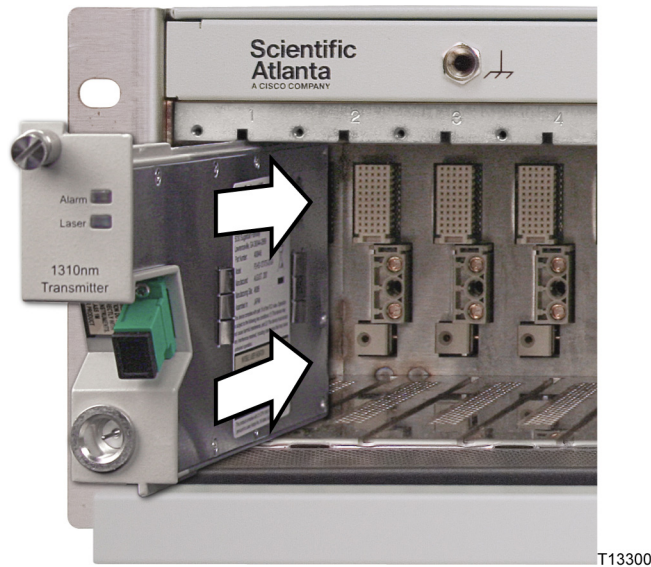
Always use a screwdriver to loosen or tighten the screws holding the application modules, ICIM2-XD, fan assembly, power supply modules, DC-to-DC converters, or blanking panels in place. Do not attempt to loosen or tighten these screws solely by hand.

- 1 Locate the fiber guides at the bottom of the chassis and the module guide slots inside the chassis as shown in the following illustration.



- 2 Align the ridges on the top and bottom of the module with the module guide slots located on the chassis.

- 3 Gently slide the module into the chassis until its power and communications connections join connectors on the midplane bus. *Do not force the module into the chassis.* If properly aligned, it should slide in with minimal force.



- 4 Tighten the screw at the top of the module to secure it in the chassis. Use a 3/8-in. flat-blade screwdriver to secure. *Do not over-tighten.*
- 5 Fill any unused chassis slots with module blanks to help ensure proper cooling air flow.

To Remove the Module



WARNING:

Avoid damage to your eyes! Do not look into any optical connector while the system is active. Even if the unit is off, there may still be hazardous optical levels present.

Complete the following steps to remove the module from the chassis.



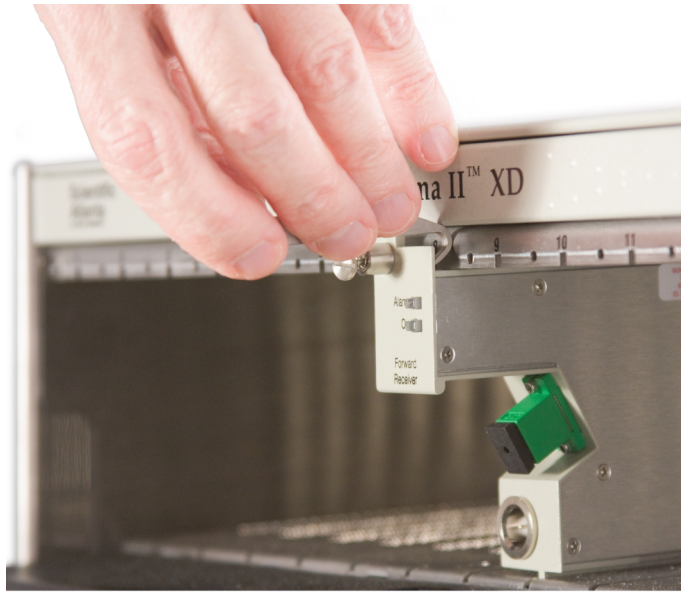
CAUTION:

Always use a screwdriver to loosen or tighten the screws holding the application modules, ICIM2-XD, fan assembly, power supply modules, DC-to-DC converters, or blanking panels in place. Do not attempt to loosen or tighten these screws solely by hand.

- 1 Loosen the screw at the top of the module to be removed using a 3/8-in. flat-blade screwdriver.
Important: Make sure that the screw is completely loose before performing the next step.
- 2 Locate the module extraction tool, part number 4022921, which was supplied with the chassis.

Chapter 3 Hardware Installation

- 3 Insert the hooked end of the tool behind the upper right corner of the module front panel. Rotate the tool upward as shown below to pry the module away from the chassis mounting flange.



T13427

- 4 Using your fingers, gently slide the module completely out of the chassis slot.
- 5 If necessary, fill the empty chassis slot with a module blanking panel to help ensure proper cooling air flow.

Connecting Optical Cables

Important:

- Make all connections with the optical power off. This will reduce the risk of damage to fiber-optic connectors.
- Clean the optical connectors as needed before making optical connections. See *Cleaning Optical Connectors* (on page 308) for instructions.

Note: Observe laser safety precautions. Refer to *Laser Safety* (on page xxv) for further information.

To Connect Optical Cables



CAUTION:

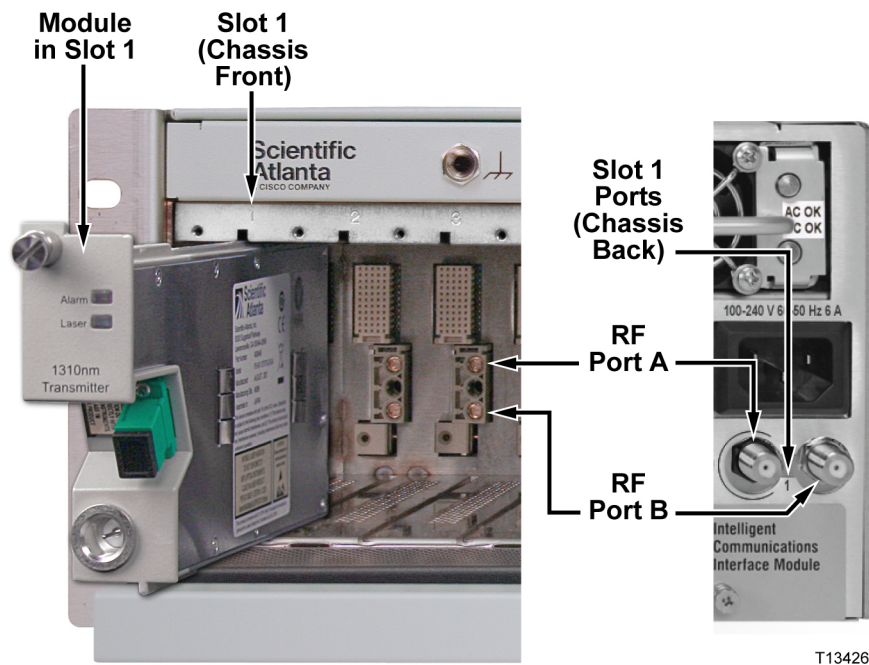
High power density exists on fiber when optical power is present. To avoid microscopic damage to fiber mating surfaces, turn off optical power or reduce power below 15 dBm before making or breaking optical connections.

Complete the following steps for each optical cable connection to be made and on every module to be installed.

- 1 Clean the end of the fiber to be connected as described in *Cleaning Optical Connectors* (on page 308).
- 2 Connect the optical cable to the module connector.
- 3 Route the cable to the appropriate destination.
- 4 Clean the remaining cable end, and then connect the cable to the mating module connector.
Note: Remember to observe minimum bend radius and other accepted handling practices when working with fiber-optic cables.
- 5 After cable installation is complete, return the module control settings to their original states.

Connecting RF Cables

The chassis back panel has two RF connectors, A and B, for each application module slot. Each pair of RF connectors is numbered (1-16) to show its corresponding slot number. RF port A, leftmost in each pair, is marked by a black semicircle or nut at the base of the connector. RF port A provides connection to the upper of two independent RF channels on the chassis midplane, while RF port B provides connection to the lower RF channel.



Note: The application module installed in each chassis slot determines whether and how the two RF channels are used. See the appropriate application module documentation for further information.

To Connect RF Cables

Complete the following steps for each RF cable connection to be made.

- 1 Connect the RF cable to the appropriate back-panel module connector.
- 2 Route the cable to the appropriate destination.

4

Equipment Configuration

Introduction

This chapter provides instructions for configuring the chassis and application modules for remote management.

There are several different ways to configure the equipment. This chapter presents one approach for configuration.

Refer to *Prisma II Permitted CLI Commands* (on page 323) for a complete list of CLI commands.

For further information on configuration using the CLI or ICIM Web Interface, see the *Prisma II Platform Remote User Interface Guide, System Release 2.03*, part number 4025477.

In This Chapter

■ HyperTerminal Session Setup.....	92
■ CLI Parameters.....	95
■ Telnet Session	98
■ SNMP Parameters.....	100

HyperTerminal Session Setup

HyperTerminal is a terminal emulation program that is included with the Microsoft Windows operating system.

The following equipment is required to perform this procedure.

- A personal computer (preferably a laptop computer for a local connection)
- A terminal emulation program such as Windows HyperTerminal or a remote terminal emulation program such as Telnet
- A DB-9 to DB-9 straight-through serial cable

You can use HyperTerminal to initiate a direct-connect communications session with an ICIM2 through its front-panel serial port.

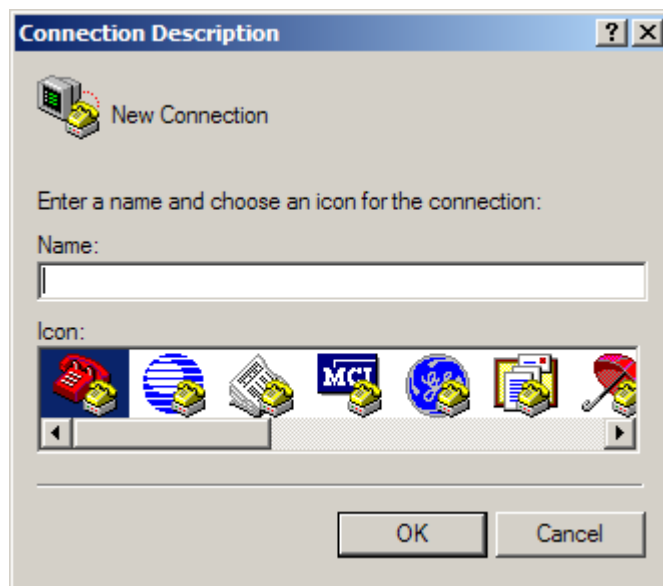
To Set Up a HyperTerminal Serial Port Session

Complete the following steps to set up the HyperTerminal emulation program.

- 1 Connect one end of a DB-9 to DB-9 straight-through serial cable to an available COM port on the personal computer, and the other end to the ICIM2 or ICIM2-XD front-panel serial port.
- 2 Open a HyperTerminal session on your laptop (or desktop) PC that you will use to connect to the ICIM2 or ICIM2-XD. The HyperTerminal program is typically found at:

`Start\All Programs\Accessories\Communication\Hyperterminal`

The new Connection Description dialog box appears.



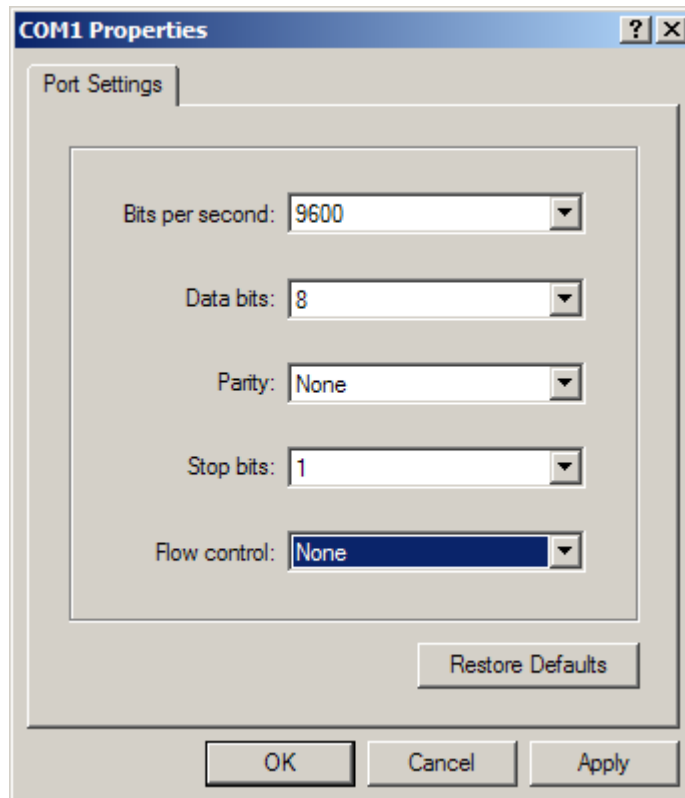
- 3 Type in a name for the connection, select an icon of your choice, and click **OK**. The Connect To dialog box appears.



- 4 In the Connect Using field, click the drop-down arrow and select the serial port that you will use for the connection, and then click **OK**. The COM Properties dialog box appears.

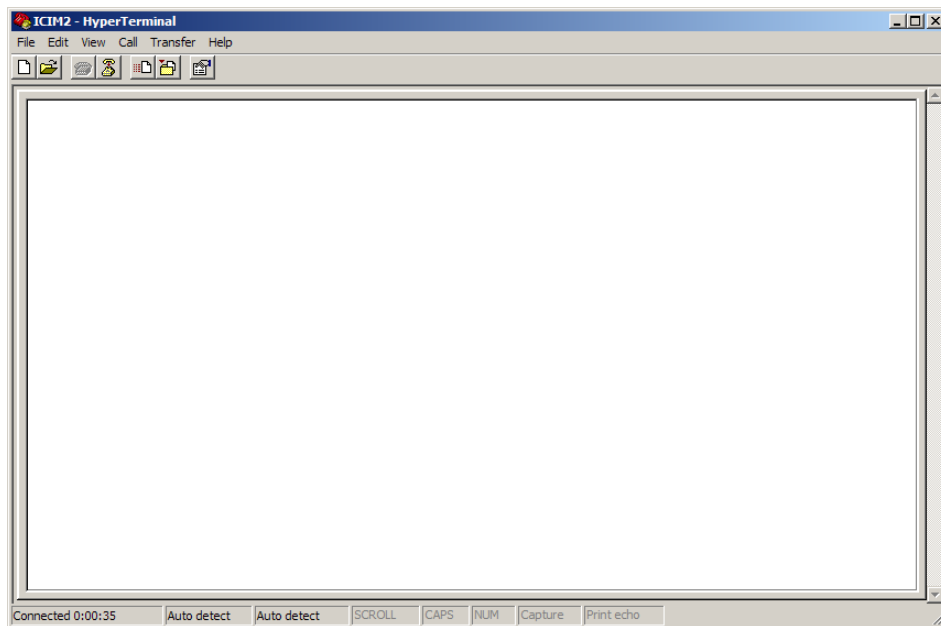
Note: For most applications, the serial port is COM1 or COM2.

- 5 Set the following port setting in the COM Properties dialog box.



Chapter 4 Equipment Configuration

- 6 Click **OK**. The HyperTerminal main program window appears.



- 7 On the File menu, click **Save** to save the settings.

CLI Parameters

Additional parameters may be set as needed from the command line interface (CLI) for each application module installed.

Refer to *Prisma II Permitted CLI Commands* (on page 323) and the *Prisma II Platform Remote User Interface Guide, System Release 2.03*, part number 4025477 for information and additional instructions on available commands and using the CLI.

Following are examples of parameters available through the CLI.

Login

- 1 Log in using the default username **Administrat0r** and the default password **AdminPassw0rd**. Note the 0 (zero) character in each string.

```
Scientific-Atlanta Intelligent Communications Interface Module (ICIM)
login: Administrat0r
Password: AdminPassw0rd
```

Successful login will return the following prompt:

```
login: Administrat0r
Password:
User Administrat0r logged in successfully on 11/13/06 at 15:25:35
Previous successful login was on 11/13/06 at 15:22:16
There were no failed attempts to login with this user id previously
CLI>
```

- 2 Enter the ICIM submenu by typing **icim** at the CLI> prompt.

```
CLI> icim
```

Successful entry into the ICIM menu tree will return the following prompt:

```
ICIM>
```

- 3 Configure the shelf (chassis) IP address, subnet mask, gateway, and clock using the following commands:

```
set ip xxx.xxx.xxx.xxx
set subnet xxx.xxx.xxx.xxx
set gateway xxx.xxx.xxx.xxx
set clock "month/day/year hour:minute:second"
```

Note:

- Be sure to include the quote symbols, e.g., `set clock "3/15/2006 13:09:51"`.
- Clock time is in the 24-hour format.

- 4 To enable these changes, reboot the ICIM2 or ICIM2-XD as follows:

```
ICIM> reboot
```

- 5 After the ICIM2 or ICIM2-XD reboots, repeat the login steps described above to return to the ICIM command prompt. Then use the show command to verify each of the above changes, as follows:

```
show ip
show subnet
show gateway
```

```
show clock
```

- 6 Type **logout**, and then press **Enter** to exit the session.
- 7 Remove the serial cable. It is no longer required.

Important:

- For Telnet operation, the computer you are using must have a network connection through which it can reach the ICIM2 or ICIM2-XD at its IP address.
- No more than four Telnet sessions are allowed at one time.



CAUTION:

Always use the Logout command to close a serial port or Telnet CLI session. Closing a serial port session without issuing the Logout command leaves the session open for a possible future connection. This may allow unauthorized access by a new user if the previous user had a higher authorization privilege level.

To Set the Clock

From the CLI command prompt, switch to ICIM command mode and set the date and time for the ICIM2, as shown below.

```
CLI> icim
ICIM> set clock "10/10/2005 15:50:00"
MM-DD-YYYY HH:mm:ss
10-10-2005 15:50:00
Mon, 10 Oct 2005 15:50:00 EST
SUCCESS!
```

To Set Additional Users for ICIM2 or ICIM2-XD Access

Refer to the *Prisma II Platform Remote User Interface Guide, System Release 2.03*, part number 4025477 for CLI and ICIM Web Interface login settings information.

Note: It is strongly recommended that a new administrator login be created and that the default administrator login be removed.

The table below lists the ICIM mode CLI commands for setting user login parameters.

Commands	Description
ICIM > show user	Shows all users
ICIM > user change password [user name]	Changes user password
ICIM > user add [user name] [access level] enable	Adds a user
ICIM > user delete [user name]	Deletes a user

Note: User names and passwords must be 6 to 14 characters long, and must include at least 1 number.

To Set and Verify SNMP Community Strings

From the CLI command prompt, switch to ICIM command mode and define SNMP Read, Write, and Trap Community strings, as shown below.

```
CLI> icim

ICIM> set commwrite "myCommWriteString"
NOTE: This change will not fully take effect until the ICIM is restarted.
Until that time, some operations will not perform as expected.

SUCCESS!

ICIM> set commread "myCommReadString"
NOTE: This change will not fully take effect until the ICIM is restarted.
Until that time, some operations will not perform as expected.

SUCCESS!

ICIM> set commtrap "myCommTrapString"
NOTE: This change will not fully take effect until the ICIM is restarted.
Until that time, some operations will not perform as expected.

SUCCESS!
```

You can then verify the community string settings, as follows.

```
ICIM> info commread commwrite commtrap

COMMREAD          COMMWRITE          COMMTRAP

myCommReadString  myCommWriteString  myCommTrapString

SUCCESS!

ICIM>
```

Note:

- It is strongly recommended that the ICIM2 or ICIM2-XD be restarted after changing any of the community strings. Otherwise, some operations will continue to work normally, while others will appear to fail.
- It is strongly recommended that new SNMP community strings be created and the default SNMP community strings be removed. Default SNMP community string values are listed below.

SNMP Community String	Default Value
Read Community	public
Write Community	private
Trap Community	SNMP_traps

Telnet Session

Telnet is a remote terminal emulation program included with the Microsoft Windows operating system. In the absence of a network management system, you can use Telnet to initiate a remote communications session with an ICIM2 or ICIM2-XD and configure the equipment in the domain using CLI commands.

Important:

- For Telnet operation, the computer you are using must have a network connection through which it can reach the ICIM2 or ICIM2-XD at its IP address.
- No more than four Telnet sessions are allowed at one time.



CAUTION:

Always use the Logout command to close a serial port or Telnet CLI session. Closing a serial port session without issuing the Logout command leaves the session open for a possible future connection. This may allow unauthorized access by a new user if the previous user had a higher authorization privilege level.

To Set Up a Telnet CLI Session

Complete the following steps to initiate a CLI session with the ICIM2 using Telnet.

Important: The ICIM2 must have an IP address assigned before performing this procedure.

- 1 Open a DOS window on the PC that you will use to connect to the ICIM2.
- 2 At the DOS command prompt, type:

```
telnet <IP address>
```

where <IP address> is the IP address of the ICIM2. The session starts and the Telnet login: prompt appears.

```

C:\ Telnet 172.24.28.151
Scientific-Atlanta Intelligent Communications Interface Module (ICIM)

-----
                W A R N I N G
-----

Unauthorized or improper use of this system may result in
administrative disciplinary action and civil or criminal penalties.
By continuing to use this system you indicate your awareness of and
consent to these terms and conditions of use.  LOG OFF IMMEDIATELY
if you do not agree to the conditions stated in this warning.

login: Administrat0r
Password:
User Administrat0r logged in successfully on 12/05/06 at 09:08:13
Previous successful login was on 12/05/06 at 08:51:47
There were no failed attempts to login with this user id previously
CLI> _
  
```

- 3 At the login: prompt, type **Administrat0r** (note the zero character in the string), and then press **Enter**.
- 4 At the Password: prompt, type **AdminPassw0rd** (note the zero character in the string), and then press **Enter**. The CLI> command prompt appears.

SNMP Parameters

Trap settings and other parameters can be set in one of several ways:

- Using Simple Network Management Protocol (SNMP) commands. Refer to *SNMP Management* (on page 167) for details on accessing the ICIM MIB tables.
- Using the Command Line Interface (CLI) Traps Enable command. Refer to the *Prisma II Platform Remote User Interface Guide, System Release 2.03*, part number 4025477 for details on using the Traps Enable command.
- Using the ICIM Web Interface, which requires no knowledge of SNMP or CLI. For further information, refer to the *Prisma II Platform Remote User Interface Guide, System Release 2.03*, part number 4025477.

Once this is accomplished, changes can be made to the ICIM Trap tables, of which there are 10 entries (one for each destination IP address).

Following are the objects in the p2TrapRecvEntry table that should be set.

MIB Object	Value
p2TrapRecvEnable	1-disabled; 2-enabled
p2TrapRecvAddr	IP address of trap receiver
p2TrapRecvTelcoAlarm	1-disabled; 2-enabled

5

ICIM2-XD Operation

Introduction

This chapter describes the ICIM2-XD software interface for platform configuration, monitoring, and control.

Unlike the ICIM2 in the Prisma II Platform chassis, the ICIM2-XD has no front-panel LCD and keypad interface. For information on using this interface, see **ICIM2 Operation** in the *Prisma II Platform System Guide, System Release 2.03*, part number 4025478.

For detailed information on system parameters specific to the Prisma II XD chassis, see *Module Parameter Descriptions* (on page 347).

In This Chapter

■ ICIM Introduction.....	102
■ ICIM Front Panel.....	104
■ Operating the ICIM2-XD	105
■ Setting Trap Receive Parameters	107

ICIM Introduction

Laser Warning



WARNING:

- Avoid personal injury! Use of controls, adjustments, or procedures other than those specified herein may result in hazardous radiation exposure.
 - Avoid personal injury! The laser light source on this equipment (if a transmitter) or the fiber cables connected to this equipment emit invisible laser radiation. Avoid direct exposure to the laser light source.
 - Avoid personal injury! Viewing the laser output (if a transmitter) or fiber cable with optical instruments (such as eye loupes, magnifiers, or microscopes) may pose an eye hazard.
- Do not apply power to this equipment if the fiber is unmated or unterminated.
 - Do not stare into an unmated fiber or at any mirror-like surface that could reflect light emitted from an unterminated fiber.
 - Do not view an activated fiber with optical instruments (e.g., eye loupes, magnifiers, microscopes).
 - Use safety-approved optical fiber cable to maintain compliance with applicable laser safety requirements.
 - Even if the unit is off, there may still be hazardous optical levels present.

Overview

The ICIM2-XD serves as the interface between the user and the application modules installed in a chassis or daisy chain. It also serves as the interface between each application module in the chassis or daisy chain and the Transmission Network Control System (TNCS).

The ICIM2-XD supports configuration and status monitoring for up to 64 modules located in 4 Prisma II XD chassis.

Unlike the ICIM2 control module found in the Prisma II Platform chassis, the ICIM2-XD is mounted in the back of the chassis and has no LCD or keypad interface. In all other respects, the ICIM2-XD operates identically to the ICIM2. It features easy-to-use software that is navigated remotely via CLI, SNMP, or the ICIM Web Interface.

Important:

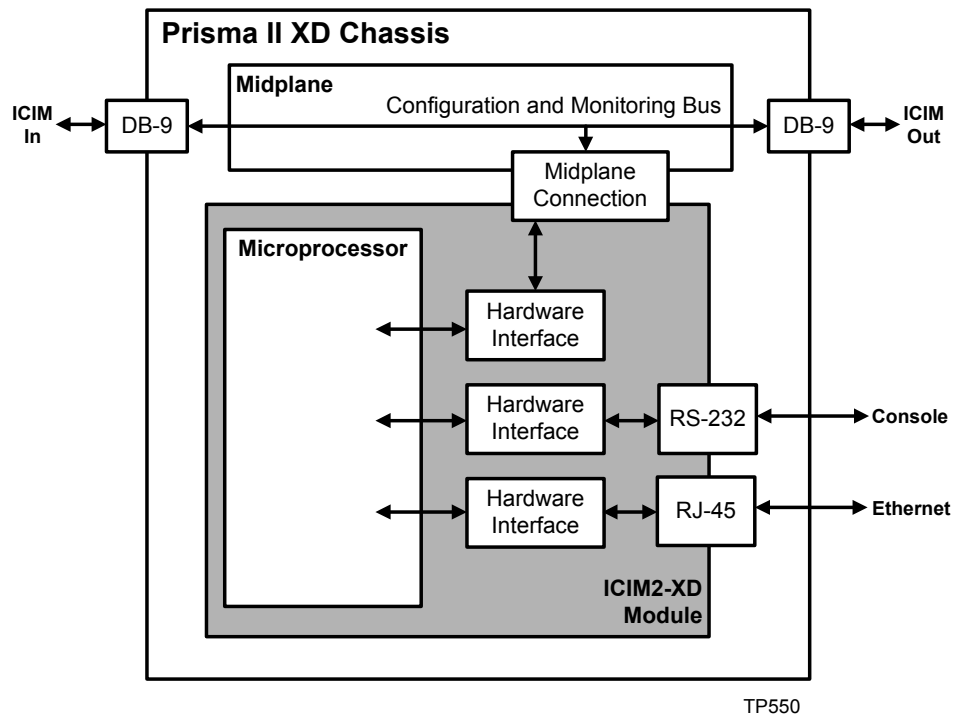
- There can be only one ICIM2 or ICIM2-XD per daisy-chain connection of Prisma II or Prisma II XD chassis (or combination of both).
- All chassis connected in a daisy chain must have a unique chassis identification

(ID) number.

- The last chassis in a daisy chain must have a terminator installed in the ICIM OUT connector. Otherwise, faulty communication with the ICIM2 or ICIM2-XD may occur.

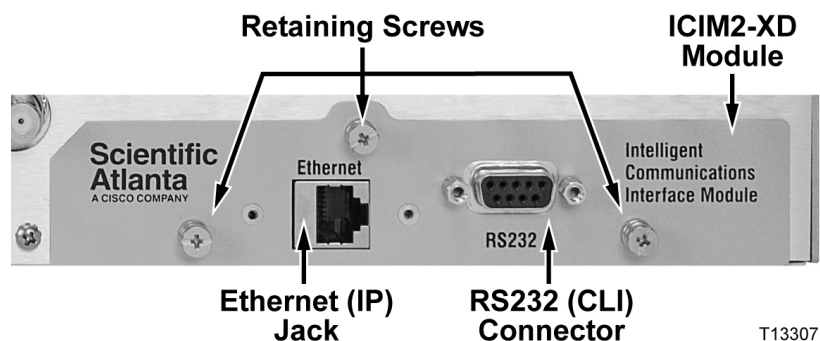
ICIM2-XD Block Diagram

The main components and functions of the ICIM2-XD are illustrated in the block diagram below.



ICIM Front Panel

ICIM2-XD Illustration (Front Panel)



ICIM2-XD Front Panel Features

Part	Function
Ethernet connector	Directly connects the ICIM2-XD to an IP network. The front-panel Ethernet port is suitable for connection to intra-building wiring, non-exposed wiring or cabling only.
RS232 connector	Used to connect a PC to the Prisma II system for local console port CLI communication and setup.

Operating the ICIM2-XD

Once the platform is installed, it runs without the aid of an operator. If alarms are generated or your system configuration changes, you can use the ICIM2-XD to make any adjustments needed beyond the initial setup.

Note: For details on chassis-related system parameters, see *Module Parameter Descriptions* (on page 347). Parameters for application modules are described in separate user documents for each module. See *Related Publications* (on page 35).

SNMP Considerations

The following items should be considered when implementing SNMP.

- The SNMP connection is made through the Ethernet port on the front of the ICIM2-XD. (Use 10baseT cable with an RJ-45 connector.) To meet GR1089-CORE requirements, shielded cable must be used with both ends grounded.
- The network management system (NMS) must be installed behind a firewall to prevent any ill-intentioned persons with an SNMP manager from accessing and tampering with the ICIM2-XD.
- When the ICIM2-XD has to handle excessive SNMP traffic, it will respond slowly to both SNMP control and front panel input. If this occurs, reduce the update rate of the SNMP manager.

Basic SNMP Setup

Refer to your SNMP manager documentation or MIB information for instructions on implementing SNMP. Before you can use and reconfigure SNMP services, you need to know the community strings in your network and the IP addresses or computer names for SNMP management hosts to which traps are sent.

Default Community Strings

The community string provides primitive security and context checking for both agents and managers that request and initiate trap operations. An agent does not accept a request from a manager outside the community. Community strings that the ICIM2-XD expects are as follows:

SNMP Community String	Default Value
Read Community	public
Write Community	private
Trap Community	SNMP_traps

Configuring for Remote Network Access

You can access the ICIM2-XD through the CLI to configure for remote monitoring and control by an SNMP network management system (NMS). This configuration involves entering the appropriate IP address, IP subnet, and gateway IP as described in *Equipment Configuration* (on page 91). For additional information on SNMP, see *SNMP Management* (on page 167).

Preliminary Steps for SNMP

Take the following initial steps when implementing SNMP.

- Confirm that the NMS is installed behind a firewall to prevent access to and tampering with the ICIM2-XD by unauthorized persons with an SNMP manager.
- Make the SNMP connection through the Ethernet port on the front of the ICIM2-XD. Use a 10BaseT cable with an RJ-45 connector.
- Monitor the ICIM2-XD response time for possible slow response to both SNMP control and front-panel input, especially during periods of heavy network traffic. If required, reduce the update rate of the SNMP manager.

Setting Trap Receive Parameters

You can use the ICIM Web Interface to specify up to 10 IP addresses to which proprietary traps will be sent. You can also specify the events that will result in a trap being sent to the network management systems at these IP addresses. For details, see the *Prisma II Platform Remote User Interface Guide, System Release 2.03*, part number 4025477.

Note: The Cold Start trap will always be sent to all network management systems.

6

LCI Operation

Introduction

This chapter provides installation and operating instructions for Local Craft Interface (LCI). This information is useful if you are using LCI to configure, operate, or monitor a module.

In This Chapter

■ LCI Introduction	110
■ System Requirements	111
■ Installing LCI.....	112
■ Connecting Your Computer to the Chassis.....	115
■ Starting LCI Software	116
■ LCI Module Tree	117
■ Accessing the Module Detail Information	118
■ Checking the Operating Status	124
■ Configuring the Module using LCI.....	125
■ Checking the Module Alarms using LCI.....	127
■ Modifying Module Alarm Limits using LCI.....	129
■ Checking Manufacturing Data using LCI.....	131

LCI Introduction

LCI Function

Local Craft Interface (LCI) is software that functions as a user interface to the Prisma II XD Platform. LCI is installed on a laptop or desktop PC, which is then connected to the chassis via the LCI port. You can use LCI to configure, operate, and monitor the modules in the chassis to which the PC is connected.

System Requirements

You will need the following computer software and hardware to run LCI.

Computer Requirements

- Pentium II 300 MHz processor or equivalent
- 128 MB RAM
- 10 MB available hard drive space
- CD-ROM Drive
- Windows 95 or later operating system software

Cable Requirements

The required cable is a standard “off the shelf” serial extension cable, DB9 Female to DB9 Male. This cable can be purchased locally or ordered from the factory as part number 180143. The connectors are a serial 9-pin D-shell (EIA 574/232).

Installing LCI

This section describes the procedure for installing your LCI software. The installation steps shown here pertain to LCI release 2.3. You can check for the most recent release of LCI by visiting the following web site:

www.scientificatlanta.com/tncs/upgrades/upgrades.htm

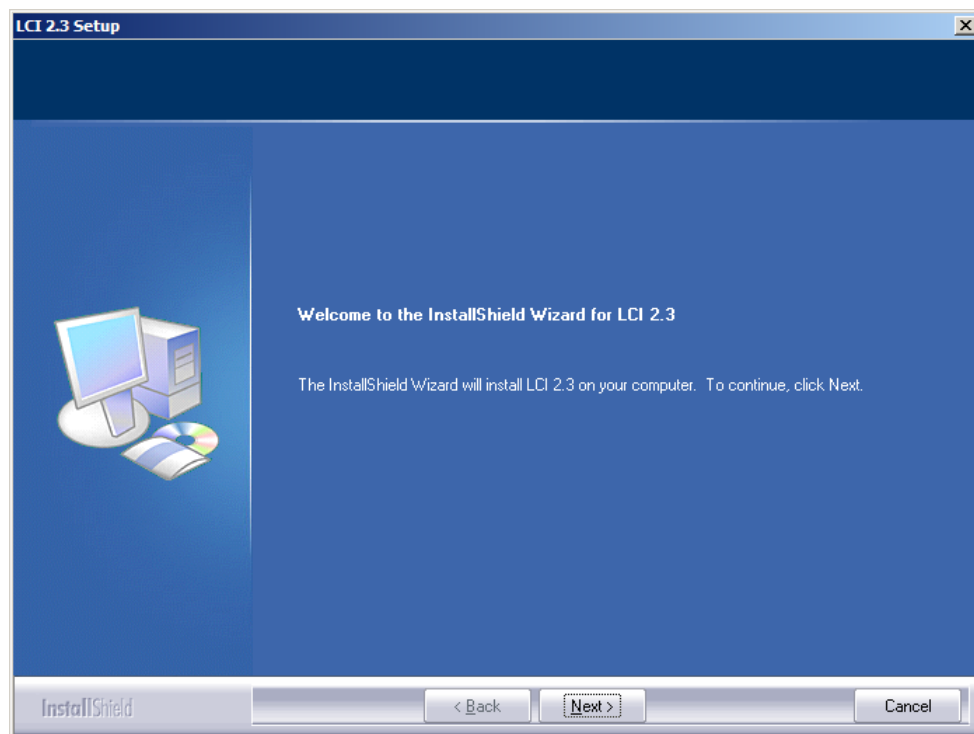
To Install the LCI Software

Complete the following steps to install the LCI software.

- 1 Close all programs that are running on your computer.
- 2 Insert the LCI CD-ROM into your CD-ROM drive.

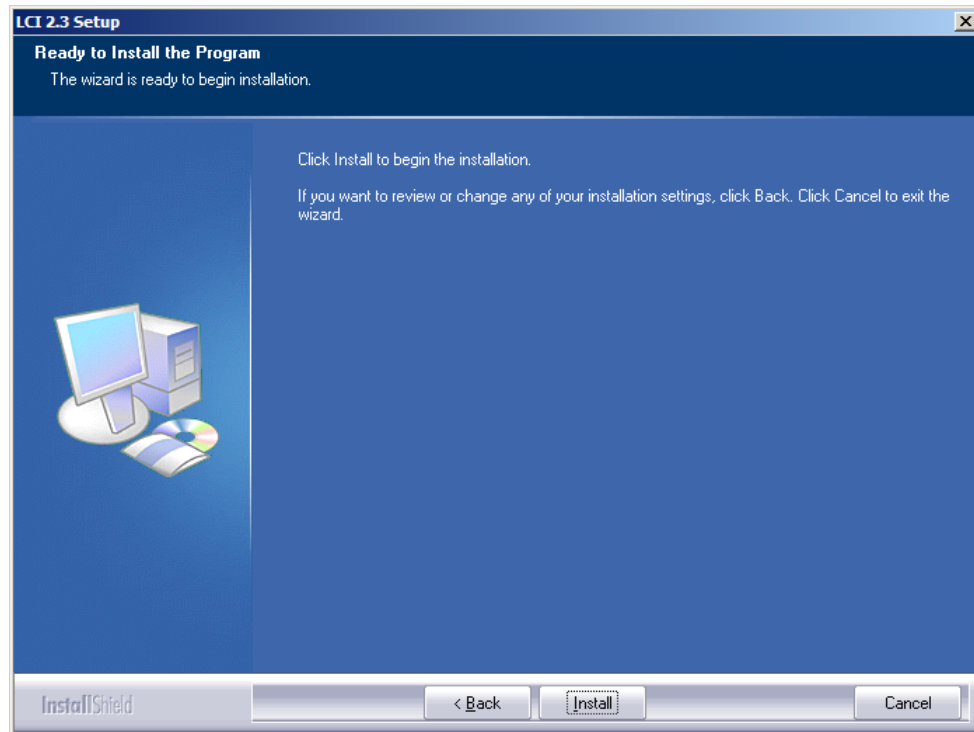
Results:

- The LCI software installation program starts automatically. If the installation program does not start automatically, open Windows Explorer and double-click the file **setup.exe** on the LCI CD-ROM.
- The Welcome screen appears as shown in the following illustration.



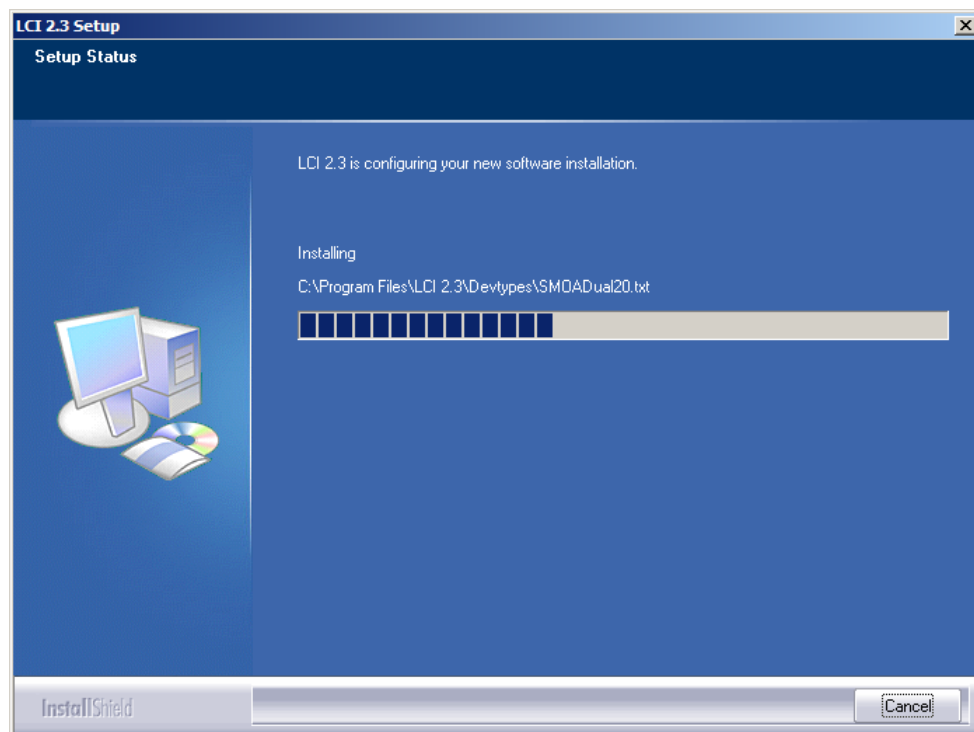
- 3 Click **Next** to continue with the installation process.

Result: The Ready to Install the Program screen appears as shown in the following illustration.

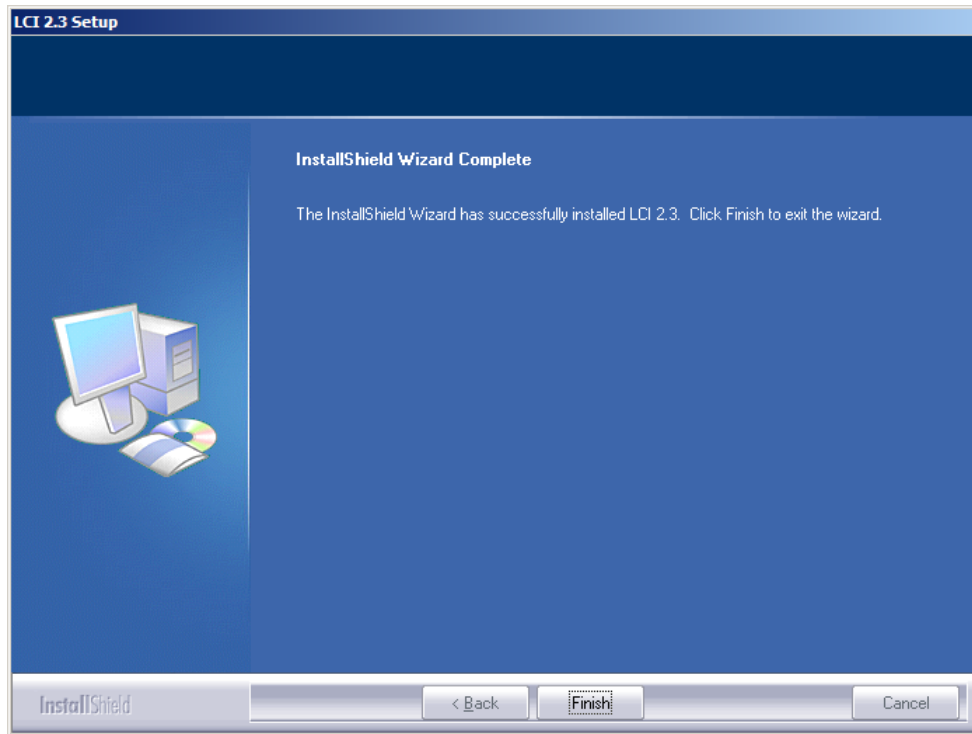


- 4 Click **Install** to begin installation.

Result: After a moment, the **Setup Status** screen appears displaying a progress indicator, as shown in the following illustration.



- 5 When finished, the Installation Wizard Complete screen appears, as shown in the following illustration.



- 6 Click **Finish** to exit the Install wizard.

Result: An LCI shortcut is placed on your Windows desktop, as shown in the following illustration.



The LCI software is now ready to use.

Connecting Your Computer to the Chassis

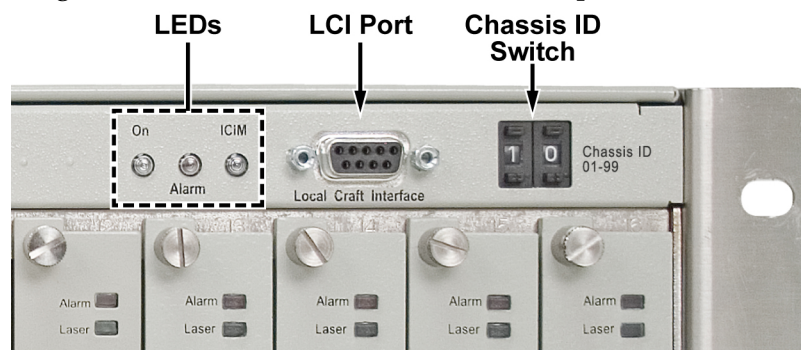
Before you start LCI, you must first connect your computer to the chassis that contains the module(s) you want to check.

Important:

- LCI only communicates with modules installed in the chassis to which your computer is connected. To check other modules, you must connect your computer to the chassis in which they are installed.
- If LCI does not communicate with a module in the chassis to which your computer is connected, it may be necessary to update the LCI application.

To Connect a Computer to the Chassis

- 1 Plug one end of a 9-pin serial extension cable into your computer.
- 2 Plug the other end of the cable into the LCI port, labeled **Local Craft Interface**.



T13297

Starting LCI Software

When LCI is started, it polls the module(s) located in the chassis to which your computer is attached. For each module it finds, LCI does the following:

- Represents the module in the module tree of the main LCI window
- Makes the polling information available so you can check and configure various parameters

Important: Your computer must be connected to the chassis before you start LCI. For instructions, refer to *Connecting Your Computer to the Chassis* (on page 115).

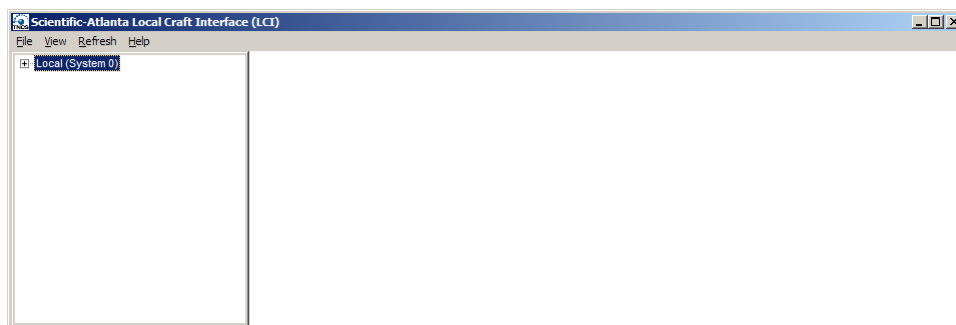
To Start LCI Software

To start the software, double-click the LCI icon on your Windows desktop.



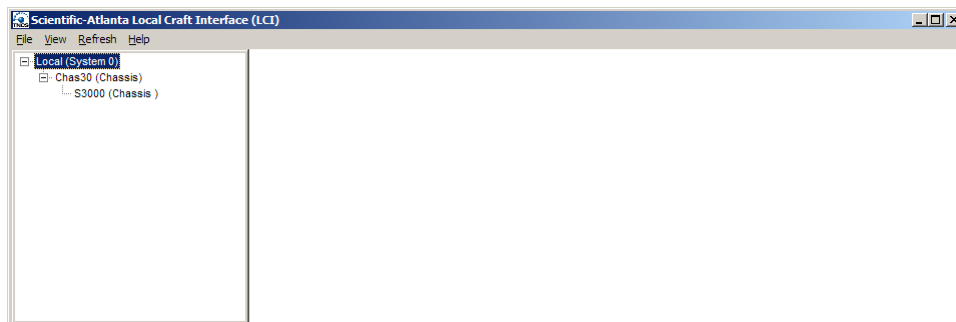
Results:

- LCI polls the modules in the chassis.
- The main LCI window appears.



LCI Module Tree

The LCI main window contains a tree that represents your system in a hierarchical manner.



Module Tree

The module tree shown above represents a computer connected to a chassis that contains no application modules. The following table describes the three tree levels in the hierarchy.

Module Tree Level	Description
Local (System 0)	Computer being used
Chassxx (Chassis)	Chassis to which the computer is connected
Sxxxx (Module name)	<p>Module(s) located within the chassis. Each module is of the format <i>chassis slot location (module name)</i>.</p> <p>Example: In the module tree shown above, S3000 (Chassis) represents a power supply located in slot 0 of chassis 30.</p> <p>Note: If this chassis had application modules installed, they would be listed together with the power supply with designations S30xx, where xx would indicate the slot number.</p>

Accessing the Module Detail Information

The Module Details window displays information about module parameters, alarms, and status. You can access this window from the module tree using any of these methods:

- Double-click the chassis and select the module in the graphic that appears.
- Right-click the chassis and select **Open** from the menu that appears.
- Double-click the module.
- Right-click the module and select **Details** from the menu that appears.

Although you can use the method most convenient for you, the procedures throughout this chapter are described using the right-click module technique.

Note: Two items that may appear in the Module Details window are mode-specific. Manual Alarm status only appears in the Controls section when Master mode is selected. Relay status only appears in the Status section when Slave mode is selected.

Module Details Window

0 Chas30.53000 p2xdchas Chassis

Prisma II XD-Chassis

Parameters

	Present Value	Present Status	Nominal Value	Minor-Alarm Low-Limit	Minor-Alarm High-Limit	Major-Alarm Low-Limit	Major-Alarm High-Limit	
Chassis Temperature	26.5	Normal	25	-35	60	.40	65	deg-C
+24V Converter A	0.0	Normal	24.7	18.4	25.9	18.0	26.1	V
+5V Converter A	0.0	Normal	5.4	3.7	5.9	3.6	6.1	V
-5V Converter A	0.0	Normal	-5.4	-5.5	-4.6	-5.6	-4.5	V
+24V Converter B	24.0	Normal	24.7	18.4	25.9	18.0	26.1	V
+5V Converter B	5.1	Normal	5.4	3.7	5.9	3.6	6.1	V
-5V Converter B	-5.3	Normal	-5.4	-5.5	-4.6	-5.6	-4.5	V

Alarms

Summary Status	Normal	Mute Converter A Alarm	On
Communication Status	Normal	Mute Converter B Alarm	Off
Fan 1 Status	Normal		
Fan 2 Status	Normal		
Fan 3 Status	Normal		
Converter A Input Status	Normal		
Converter B Input Status	Normal		

Controls

Properties

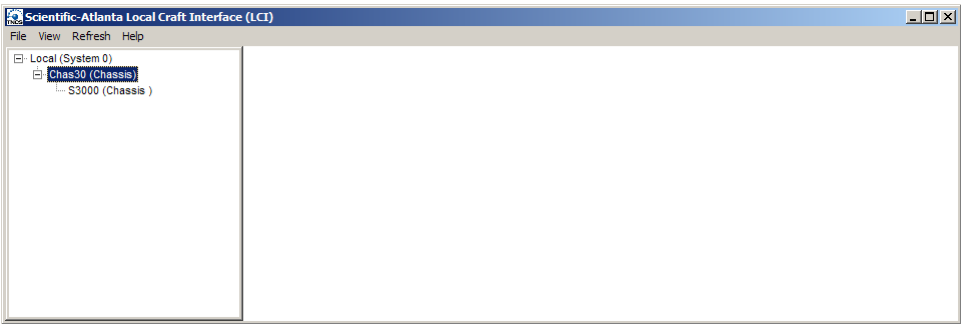
Devtype	Revision	1.06
Name	S3000	
Graphic		
Service Name		
Symbol		
Device Location		
Alias		
Notify Set A		
Notify Set B		
M&C-Scan	On-Scan	
Maintenance Mode	Normal	
Poll Counter	384	
Script		
Comm Alarm Threshold	1	
Comm Quality		%
Address	3000	
Port	COM1	
Generic Name	Chassis	
Description	Prisma II XD-Chassis	
Software Revision	1.01.05	
Script Version	N/A	
Serial Number	*ABCDEF	G
Time Of Service	228	Hrs
Day Code	M07	
Module Type	5020	

Status

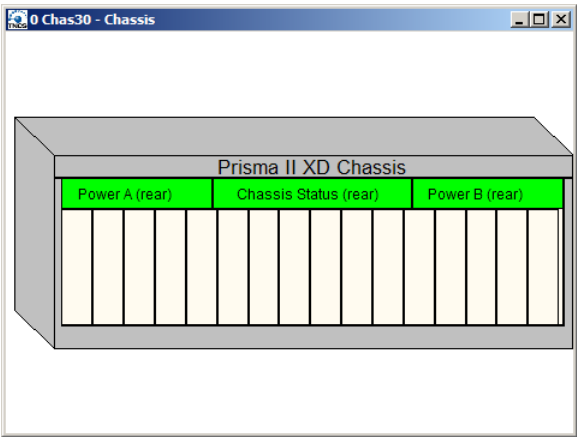
PS A Installed	Yes	
PS B Installed	Yes	
Converter A Installed	Yes	
Converter B Installed	No	
+24V Chassis	24.6	VDC
+5V Chassis	5.1	VDC
-5V Chassis	-4.4	VDC

To Access the Module Details, Double-Click the Chassis

- 1 Double-click the chassis.

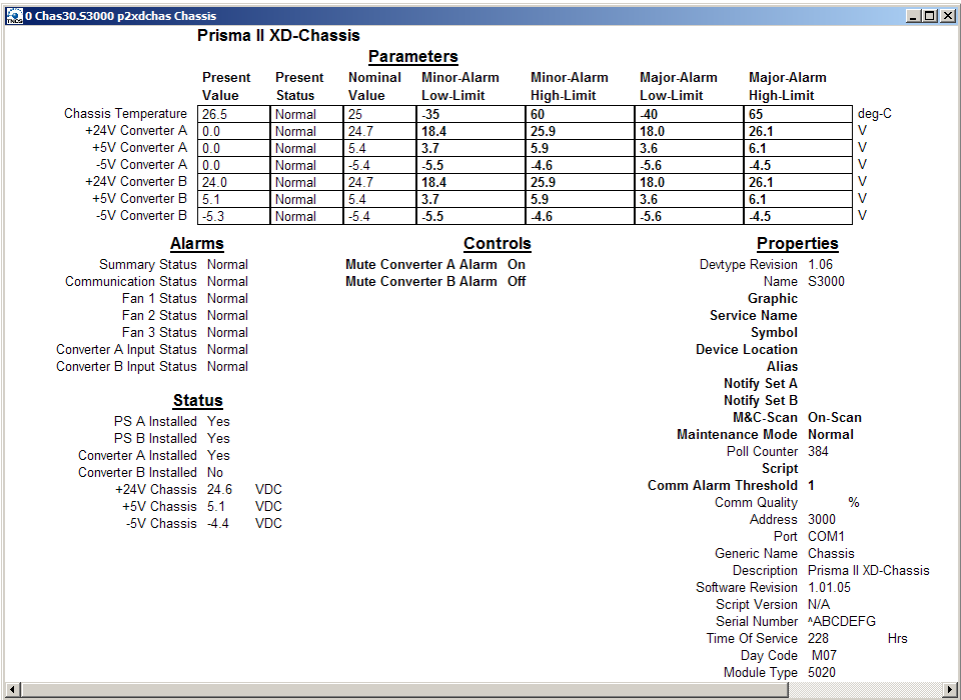


Result: A graphic representation of the chassis appears.



- 2 Double-click the module whose information you want to view or configure.

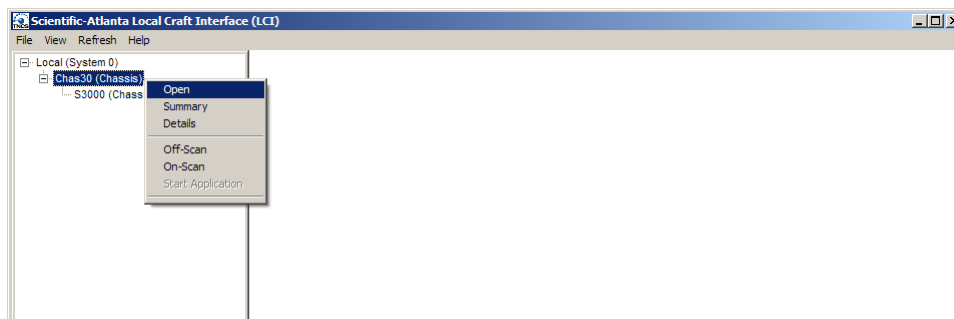
Result: The Module Details window appears.



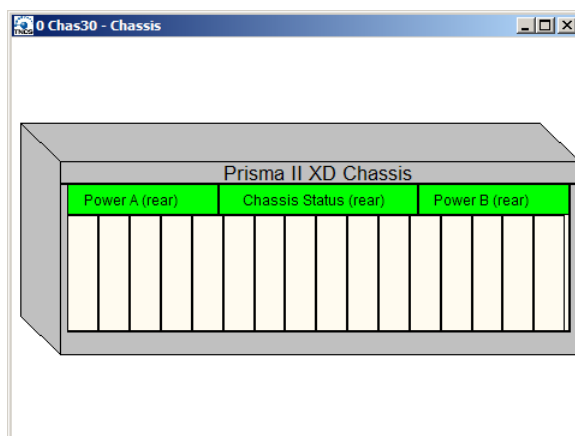
- 3 Proceed with viewing or configuring information.

To Access the Module Details, Right-Click the Chassis

- 1 Right-click the chassis, and then click **Open**.

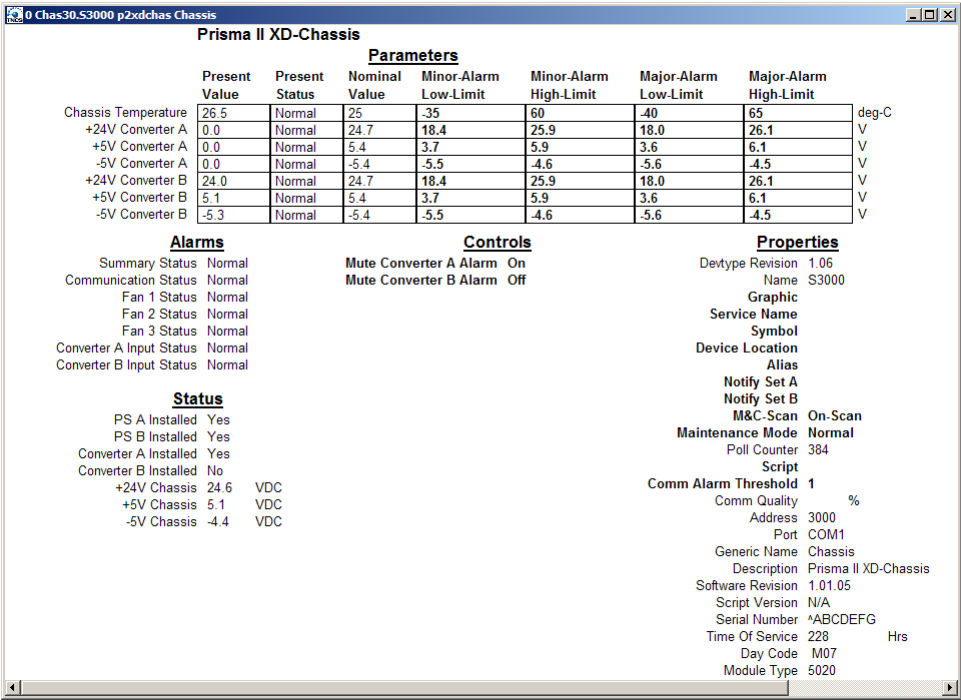


Result: A graphic representation of the chassis appears.



- 2 Double-click the module whose information you want to view or configure.

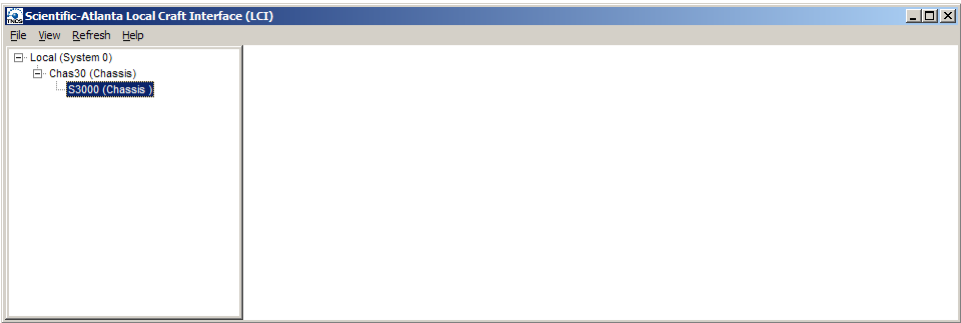
Result: The Module Details window appears.



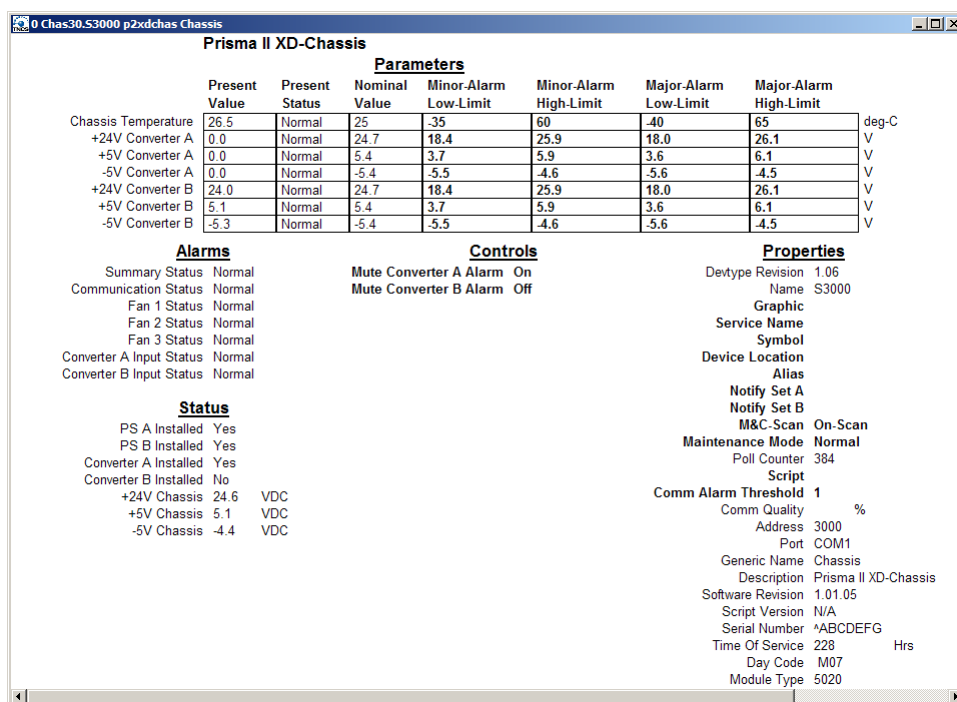
3 Proceed with viewing or configuring information.

To Access the Module Details, Double-Click the Module

1 Double-click the module.



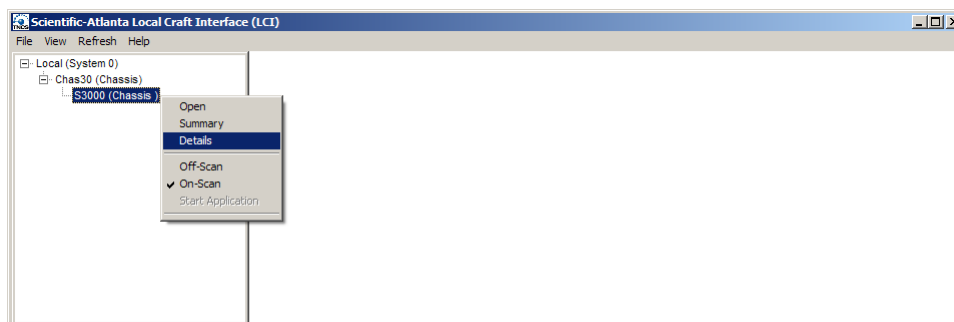
Result: The Module Details window appears.



- 2 Proceed with viewing or configuring information.

To Access the Module Details, Right-Click the Module

- 1 Right-click the module, and then click **Details**.

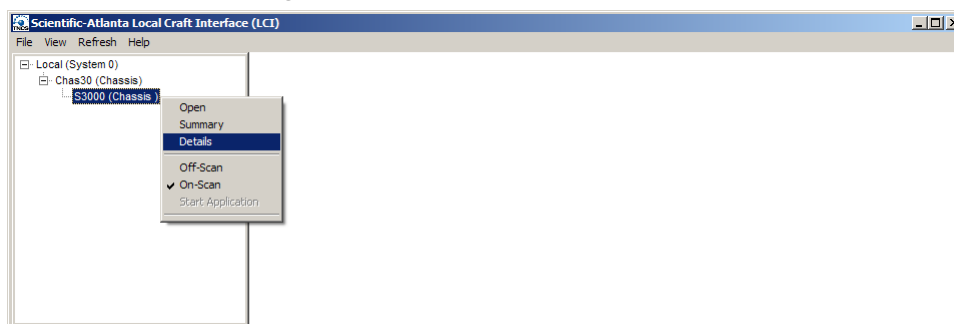


Checking the Operating Status

To Check the Operating Status using LCI

Using the LCI, you can check the status of all operating parameters of this module.

- 1 In the module tree, right-click the module, and then click **Details**.



Result: The Module Details window appears. The monitored parameters are displayed under **Parameters** and **Status**.

Prisma II XD-Chassis

	Present Value	Present Status	Nominal Value	Minor-Alarm Low-Limit	Minor-Alarm High-Limit	Major-Alarm Low-Limit	Major-Alarm High-Limit	
Chassis Temperature	26.5	Normal	25	-35	60	-40	65	deg-C
+24V Converter A	0.0	Normal	24.7	18.4	25.9	18.0	26.1	V
+5V Converter A	0.0	Normal	5.4	3.7	5.9	3.6	6.1	V
-5V Converter A	0.0	Normal	-5.4	-5.5	-4.6	-5.6	-4.5	V
+24V Converter B	24.0	Normal	24.7	18.4	25.9	18.0	26.1	V
+5V Converter B	5.1	Normal	5.4	3.7	5.9	3.6	6.1	V
-5V Converter B	-5.3	Normal	-5.4	-5.5	-4.6	-5.6	-4.5	V

Alarms

Summary Status Normal

Communication Status Normal

Fan 1 Status Normal

Fan 2 Status Normal

Fan 3 Status Normal

Converter A Input Status Normal

Converter B Input Status Normal

Status

PS A Installed Yes

PS B Installed Yes

Converter A Installed Yes

Converter B Installed No

+24V Chassis 24.6 VDC

+5V Chassis 5.1 VDC

-5V Chassis -4.4 VDC

Controls

Mute Converter A Alarm On

Mute Converter B Alarm Off

Properties

Devtype Revision 1.06

Name S3000

Graphic

Service Name

Symbol

Device Location

Alias

Notify Set A

Notify Set B

M&C-Scan On-Scan

Maintenance Mode Normal

Poll Counter 384

Script

Comm Alarm Threshold 1

Comm Quality %

Address 3000

Port COM1

Generic Name Chassis

Description Prisma II XD-Chassis

Software Revision 1.01.05

Script Version N/A

Serial Number *ABCDEFG

Time Of Service 228 Hrs

Day Code M07

Module Type 5020

- 2 Check the operating parameters.

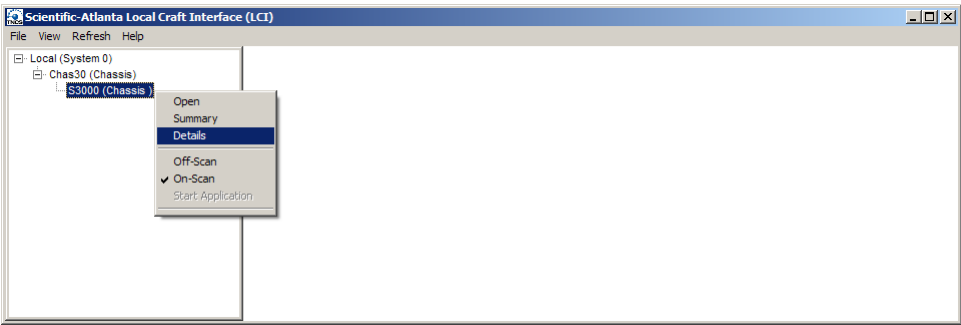
Note: For details on chassis-related system parameters, see *Module Parameter Descriptions* (on page 347). Parameters for application modules are described in separate user documents for each module. See *Related Publications* (on page 35).

Configuring the Module using LCI

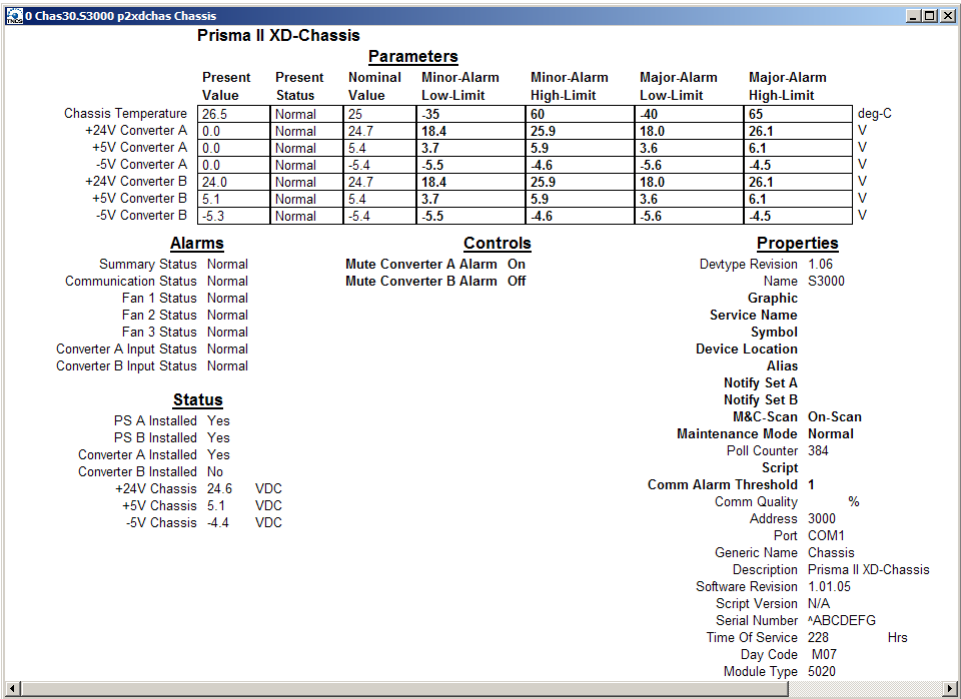
To Set Control Parameters using LCI

Using LCI, you can configure the parameters of this module.

- 1 In the module tree, right-click the module, and then click **Details**.

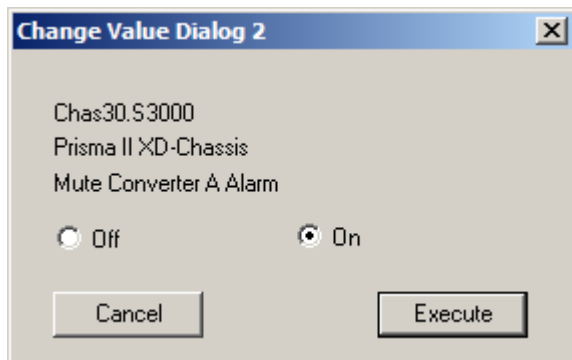


Result: The Module Details window appears.



- 2 Under **Controls**, double-click the parameter you want to configure.

Result: The Change Value dialog box appears. This example shows the dialog box for the Mute Converter A Alarm parameter.



- 3 Depending on the parameter you chose, select or type a new value.
- 4 Click **Execute**.

Result: The new value appears next to the parameter.

Note: For details on chassis-related system parameters, see *Module Parameter Descriptions* (on page 347). Parameters for application modules are described in separate user documents for each module. See *Related Publications* (on page 35).

Checking the Module Alarms using LCI

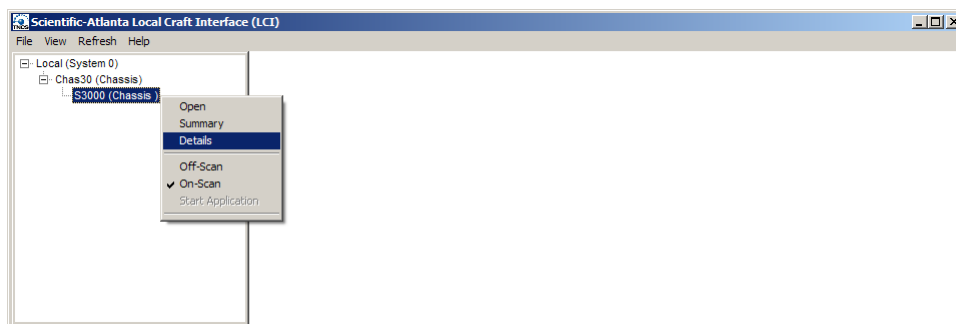
Using LCI, you can check the alarm status of various parameters. Alarms that you can check are listed below.

Alarms limits fall into one of the following categories.


- Major low
- Minor low
- Minor high
- Major high

To Check Alarms using LCI

Right-click the module, and then click **Details**.



Result: The Module Details window appears. The alarms are shown under **Parameters and Alarms**.


0 Chas30.53000 p2XDchas Chassis

Prisma II XD-Chassis

Parameters

	Present Value	Present Status	Nominal Value	Minor-Alarm Low-Limit	Minor-Alarm High-Limit	Major-Alarm Low-Limit	Major-Alarm High-Limit	
Chassis Temperature	26.5	Normal	25	-35	60	-40	65	deg-C
+24V Converter A	0.0	Normal	24.7	18.4	25.9	18.0	26.1	V
+5V Converter A	0.0	Normal	5.4	3.7	5.9	3.6	6.1	V
-5V Converter A	0.0	Normal	-5.4	-5.5	-4.6	-5.6	-4.5	V
+24V Converter B	24.0	Normal	24.7	18.4	25.9	18.0	26.1	V
+5V Converter B	5.1	Normal	5.4	3.7	5.9	3.6	6.1	V
-5V Converter B	-5.3	Normal	-5.4	-5.5	-4.6	-5.6	-4.5	V

Alarms

Summary Status

Normal

Communication Status

Normal

Fan 1 Status

Normal

Fan 2 Status

Normal

Fan 3 Status

Normal

Converter A Input Status

Normal

Converter B Input Status

Normal

Controls

Mute Converter A Alarm

On

Mute Converter B Alarm

Off

Properties

Devtype Revision

1.06

Name

S3000

Graphic

Service Name

Symbol

Device Location

Alias

Notify Set A

Notify Set B

M&C-Scan

On-Scan

Maintenance Mode

Normal

Poll Counter

384

Script

Comm Alarm Threshold

1

Comm Quality

%

Address

3000

Port

COM1

Generic Name

Chassis

Description

Prisma II XD-Chassis

Software Revision

1.01.05

Script Version

N/A

Serial Number

*ABCDEFG

Time Of Service

228 Hrs

Day Code

M07

Module Type

5020

Status

PS A Installed

Yes

PS B Installed

Yes

Converter A Installed

Yes

Converter B Installed

No

+24V Chassis

24.6 VDC

+5V Chassis

5.1 VDC

-5V Chassis

-4.4 VDC

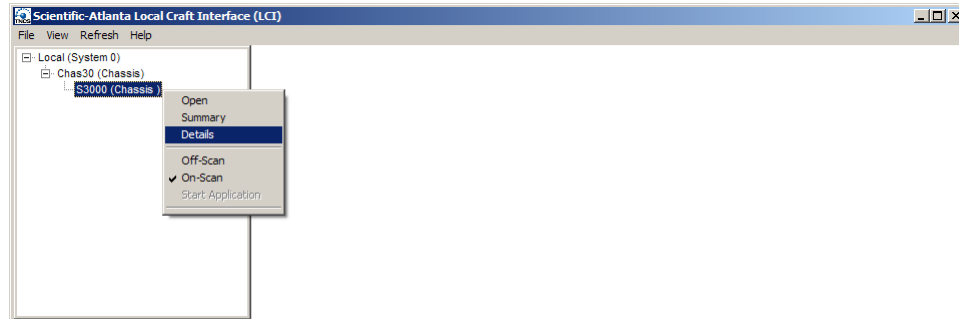
Note: For details on chassis-related system parameters, see *Module Parameter Descriptions* (on page 347). Parameters for application modules are described in separate user documents for each module. See *Related Publications* (on page 35).

Modifying Module Alarm Limits using LCI

To Modify Alarm Limits using LCI

Using LCI, you can modify alarm limits for several parameters. Parameters whose alarm limits you can change are listed below.

- 1 In the module tree, right-click the module, and then click **Details**.



Result: The Module Details window appears. The alarm limits are shown under **Parameters**.

The screenshot shows the 'Prisma II XD-Chassis' Module Details window. It contains four main sections: Parameters, Alarms, Controls, and Properties.

Parameters

	Present Value	Present Status	Nominal Value	Minor-Alarm Low-Limit	Minor-Alarm High-Limit	Major-Alarm Low-Limit	Major-Alarm High-Limit	
Chassis Temperature	26.5	Normal	25	-35	60	-40	65	deg-C
+24V Converter A	0.0	Normal	24.7	18.4	25.9	18.0	26.1	V
+5V Converter A	0.0	Normal	5.4	3.7	5.9	3.6	6.1	V
-5V Converter A	0.0	Normal	-5.4	-5.5	-4.6	-5.6	-4.5	V
+24V Converter B	24.0	Normal	24.7	18.4	25.9	18.0	26.1	V
+5V Converter B	5.1	Normal	5.4	3.7	5.9	3.6	6.1	V
-5V Converter B	-5.3	Normal	-5.4	-5.5	-4.6	-5.6	-4.5	V

Alarms

Summary Status	Normal
Communication Status	Normal
Fan 1 Status	Normal
Fan 2 Status	Normal
Fan 3 Status	Normal
Converter A Input Status	Normal
Converter B Input Status	Normal

Controls

Mute Converter A Alarm	On
Mute Converter B Alarm	Off

Properties

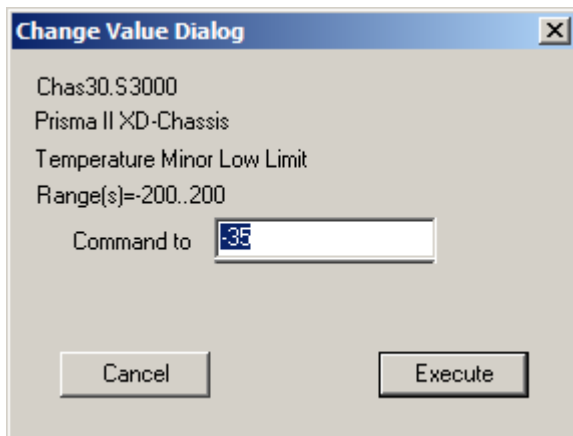
Devtype Revision	1.06
Name	S3000
Graphic	
Service Name	
Symbol	
Device Location	
Alias	
Notify Set A	
Notify Set B	
M&C-Scan	On-Scan
Maintenance Mode	Normal
Poll Counter	384
Script	
Comm Alarm Threshold	1
Comm Quality	%
Address	3000
Port	COM1
Generic Name	Chassis
Description	Prisma II XD-Chassis
Software Revision	1.01.05
Script Version	N/A
Serial Number	^ABCDEFG
Time Of Service	228 Hrs
Day Code	M07
Module Type	5020

Status

PS A Installed	Yes
PS B Installed	Yes
Converter A Installed	Yes
Converter B Installed	No
+24V Chassis	24.6 VDC
+5V Chassis	5.1 VDC
-5V Chassis	-4.4 VDC

- 2 Double-click the limit you want to change.

Result: The Change Value dialog box appears. This example shows the dialog box for the chassis temperature Minor Low limit parameter.



- 3 In the **Command to** box, type the value to use for the limit.
- 4 Click **Execute**.

Result: The new value appears in the alarm limit column.

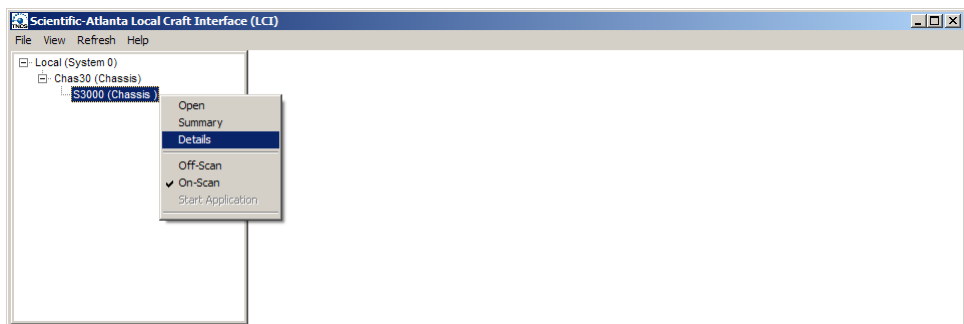
Note: For details on chassis-related system parameters, see *Module Parameter Descriptions* (on page 347). Parameters for application modules are described in separate user documents for each module. See *Related Publications* (on page 35).

Checking Manufacturing Data using LCI

To Check Manufacturing Data using LCI

Using LCI, you can check the manufacturing data of the module.

- 1 In the module tree, right-click the module, and then click **Details**.



Result: The Module Details window appears. The manufacturing data is displayed under **Properties**.

Prisma II XD-Chassis

	Present Value	Present Status	Nominal Value	Minor-Alarm Low-Limit	Minor-Alarm High-Limit	Major-Alarm Low-Limit	Major-Alarm High-Limit	
Chassis Temperature	26.5	Normal	25	-35	60	-40	65	deg-C
+24V Converter A	0.0	Normal	24.7	18.4	25.9	18.0	26.1	V
+5V Converter A	0.0	Normal	5.4	3.7	5.9	3.6	6.1	V
-5V Converter A	0.0	Normal	-5.4	-5.5	-4.6	-5.6	-4.5	V
+24V Converter B	24.0	Normal	24.7	18.4	25.9	18.0	26.1	V
+5V Converter B	5.1	Normal	5.4	3.7	5.9	3.6	6.1	V
-5V Converter B	-5.3	Normal	-5.4	-5.5	-4.6	-5.6	-4.5	V

Alarms

Summary Status Normal

Communication Status Normal

Fan 1 Status Normal

Fan 2 Status Normal

Fan 3 Status Normal

Converter A Input Status Normal

Converter B Input Status Normal

Status

PS A Installed Yes

PS B Installed Yes

Converter A Installed Yes

Converter B Installed No

+24V Chassis 24.6 VDC

+5V Chassis 5.1 VDC

-5V Chassis -4.4 VDC

Controls

Mute Converter A Alarm On

Mute Converter B Alarm Off

Properties

Devtype Revision 1.06

Name S3000

Graphic

Service Name

Symbol

Device Location

Alias

Notify Set A

Notify Set B

M&C-Scan On-Scan

Maintenance Mode Normal

Poll Counter 384

Script

Comm Alarm Threshold 1

Comm Quality %

Address 3000

Port COM1

Generic Name Chassis

Description Prisma II XD-Chassis

Software Revision 1.01.05

Script Version N/A

Serial Number *ABCDEFG

Time Of Service 228 Hrs

Day Code M07

Module Type 5020

- 2 Proceed with viewing the manufacturing data.

Note: For details on chassis-related system parameters, see *Module Parameter Descriptions* (on page 347). Parameters for application modules are described in separate user documents for each module. See *Related Publications* (on page 35).

7

User Management

Introduction

This chapter explains the procedures for adding and removing ICIM2 or ICIM2-XD users and for changing user access and authorization levels.

In This Chapter

- Introduction..... 134
- Replacing the Default Admin Account..... 137
- Working With User Accounts 141
- User Lockout 148

Introduction

The ICIM2 and ICIM2-XD support up to 16 user accounts. This chapter describes user accounts in detail, and explains how the system administrator (a user with Admin level security access) may set up and edit user accounts through the CLI or Web Interface. Additionally, this chapter includes a table listing access levels and corresponding resources, identifying the activities available to users with specific privileges.

User Accounts

Each user account is set up with a username and password. To initiate an account, the system administrator first chooses the access level and the status. Accounts to be activated immediately are given the status of **enable**, while those whose activation should be delayed are given the status of **disable**. The system administrator may also adjust the (single) inactivity timeout as well as the limit of failed log-in attempts for the ICIM2.

When a user logs onto the ICIM2 or ICIM2-XD via the CLI or Web Interface, the username and password are checked for authentication. A check is also performed to ensure that the user account is enabled. Users with disabled accounts are not permitted access to the ICIM2 or ICIM2-XD.

Additionally, security levels are compared to ensure that the user is authorized to access only the options appropriate to their access level. Another check verifies that the user has not reached the login failure limit as defined by the system administrator and saved in the ICIM2 or ICIM2-XD. A trap is sent if a user reaches the failed login attempts limit, and the user is prevented from making further log-in attempts for a designated lockout time period.

Usernames

Usernames, also known as login IDs, are formed from the alphanumeric characters A through Z (uppercase), a through z (lowercase), and the numbers 0 through 9. Special characters are not supported in login IDs. Usernames must have at least 6 characters, cannot exceed 14 characters, and must contain at least one alphabetic character and one numeric character. The username cannot be changed once it is created. If entered incorrectly, the system administrator must delete the user account and create a new account using the correct username, password, status, and access level.

Passwords

Passwords are formed from the alphanumeric characters A through Z (uppercase), a through z (lowercase), the numbers 0 through 9, and may include other printable keyboard characters. Control characters are not supported. Passwords must have at least 6 characters, cannot exceed 14 characters, and must contain at least one alphabetic character and one numeric character. Additionally, the password may not include or consist solely of the username (login ID). For security reasons, passwords are not echoed when adding, changing, or entering them at login. If you forget your password, contact the system administrator, as only he or she is able to change it. Users with Admin level privileges can change the password for any user.

Security Levels

User account security levels define the privileges available to users at that level. Choices are Read-Only, Read-Write, and Admin. The system administrator must have Admin privileges in order to add, change, or delete user accounts, or to modify system settings for the ICIM2 or ICIM2-XD and the modules in its domain.

Users who do not need to modify module alarm thresholds, controls, or CLLI codes should be assigned Read-Only privileges. Users who need to regulate module information or change CLLI codes need Read-Write privileges.

See *Features Available via Remote User Interface* (on page 335) for details regarding features available through the remote interface and user access levels required to view or edit data elements.

Account Enable or Disable

Each account is assigned a status of enable or disable. If an account is enabled, it may be used right away. If disabled, the account may not be accessed until the system administrator has activated it. The disabled account status is useful for employees who are temporarily unavailable because they have not started work yet or are on vacation.

Each time someone attempts to log onto a disabled account, a trap is sent alerting management to the event. The attempt is also logged in the event log.

Note: If you discover that your account is disabled, see your system administrator.

Login Thresholds

The login threshold defines the number of failed login attempts that must occur before a maximum threshold trap is sent. Admin level users may adjust the login threshold for the ICIM2 or ICIM2-XD. This threshold is the same for all users on a particular ICIM2 or ICIM2-XD. The default is 5 times, and the range is from 0 to 15. Login failure threshold checking may be disabled by setting the threshold to 0. A failed login attempt trap is sent for every failed login attempt.

User Lockout

Beginning with System Release 2.02, User Lockout may be enabled to prevent users who exceed the maximum failed login attempts threshold from logging in for a designated lockout interval (60 minutes by default). Locked-out users may try to log in again after the user lockout period expires or after an administrator removes the lockout. For further details, see *User Lockout* (on page 148).

Inactivity Timeout

The inactivity timeout is the number of minutes that a user account must be idle following login before it is automatically logged out by the ICIM2 or ICIM2-XD. The timeout value is the same number of minutes for all users on a particular ICIM2 or ICIM2-XD. The default is 10 minutes, but this value may be set anywhere from 1 to 60 minutes by a user with Admin privileges. The inactivity timeout cannot be disabled.

Replacing the Default Admin Account

All ICIM2 and ICIM2-XD units ship from the factory with a single default Admin level account. This account is assigned the username `Administrat0r` and the password `AdminPassw0rd`.

For security reasons, it is strongly recommended that the system administrator add a new Admin user level as the first step after starting up the ICIM2 or ICIM2-XD. After this new Admin level user is added, the default Admin user account may be deleted.

Important:

Before deleting the default Admin user account, be sure that you have created a new Admin account and noted its login defaults for future reference. Failure to remember the new username and password may result in being locked out of the ICIM2 or ICIM2-XD permanently. You cannot revert to the default Admin username and password once they are deleted.

To Replace the Default Admin Account

Complete the following steps to replace the default Admin account.

From the CLI

- 1 Log on to the ICIM2 or ICIM2-XD using the default username and password.

The sample dialog below shows the addition of a new user account **newAdmin1** with password **enterpassword1**.

```
CLI> icim
ICIM> user add newAdmin1 admin enable
Please enter the password: enterpassword1
Please reenter the password: enterpassword1
```

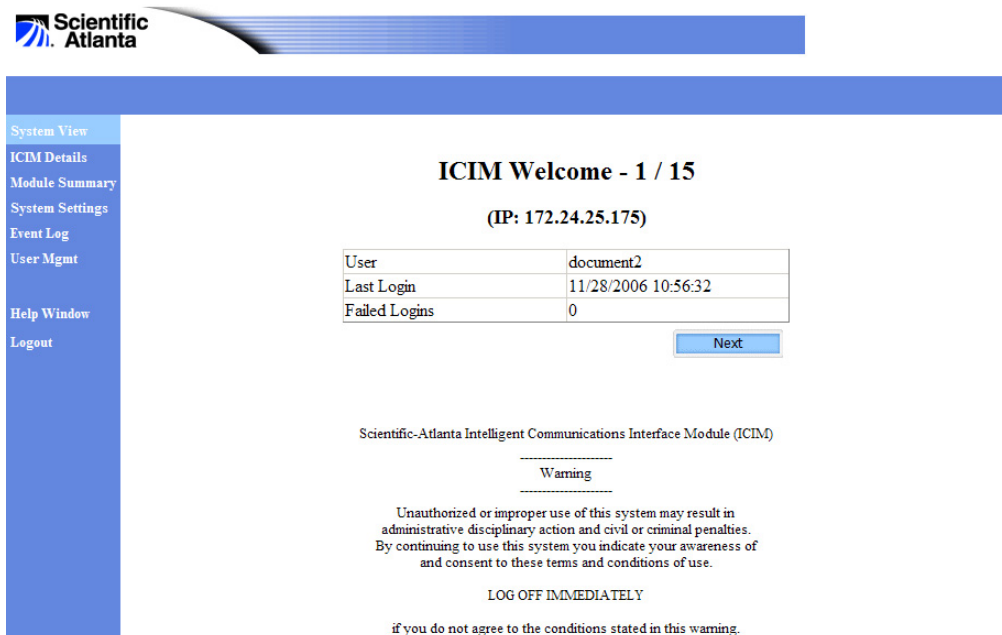
Note: Passwords are not echoed to the terminal as they are entered.

- 2 Type **show user**, and then confirm that the new user appears in the resulting list of user names.
- 3 Log out of the ICIM2 or ICIM2-XD.
- 4 Log back onto the ICIM2 or ICIM2-XD using the new Admin account username and password.
- 5 At the ICIM prompt, type **user delete Administrat0r**. The following message appears:


```
You are about to delete user 'Administrat0r' from the authorization table.
```
- 6 To confirm, type **yes**, and then press **Enter**.
- 7 Type **show user**, and then confirm that the user `Administrat0r` no longer appears in the resulting list of user names.

From the Web Interface

- 1 Log onto the ICIM2 or ICIM2-XD using the default username and password.



Scientific Atlanta

ICIM Welcome - 1 / 15
(IP: 172.24.25.175)

User	document2
Last Login	11/28/2006 10:56:32
Failed Logins	0

[Next](#)

Scientific-Atlanta Intelligent Communications Interface Module (ICIM)

Warning

Unauthorized or improper use of this system may result in administrative disciplinary action and civil or criminal penalties. By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use.

LOG OFF IMMEDIATELY

if you do not agree to the conditions stated in this warning.

TP396

- 2 Click **User Mgmt** in the menu in the left pane. The User Management table appears as shown below.

User Management
(Max 16 Users)

Number	User ID	Security	Status	Last Login	Failed Logins	Locked		
1	Administrat0r	Admin	Enabled	03/08/07 11:11:32	0	No	Edit	Delete
2	document2	Read-Only	Enabled	<None>	0	No	Edit	Delete
3	icim22	Read-Only	Enabled	<None>	0	No	Edit	Delete
4	newUser5	Read-Only	Enabled	<None>	0	No	Edit	Delete

[New User](#)

TP387

- Click the **New User** button beneath the User Management table. The New User Information screen appears as shown below.

TP397

- Enter the User ID and Password in the fields provided, and then enter the password again in the Confirm Password field.
Note: The password information you enter is not displayed.
- Select the appropriate Security Level and Status from the drop-down menus.
- Click the **Save** button to save your settings.
- Log out of the ICIM2 or ICIM2-XD.
- Log back onto the ICIM2 or ICIM2-XD using the new Admin account name and password. For example:
newAdmin1
enterpassword1
- Click **User Mgmt** in the menu in the left pane.
- When the User Management Table appears, move the mouse to the delete button next to the row with the default Admin account username Administrat0r.

User Management

(Max 16 Users)

Number	User ID	Security	Status	Last Login	Failed Logins	Locked		
1	Administrat0r	Admin	Enabled	03/08/07 11:11:32	0	No	Edit	Delete
2	document2	Read-Only	Enabled	<None>	0	No	Edit	Delete
3	icim22	Read-Only	Enabled	<None>	0	No	Edit	Delete
4	newUser5	Read-Only	Enabled	<None>	0	No	Edit	Delete
5	newAdmin1	Admin	Enabled	<None>	0	No	Edit	Delete

[New User](#)

TP388

- Click the **delete** button to remove the default Admin account.

Important:

- Keep track of the Administrator username and password. There is no way to retrieve the default username and password once they are deleted.
- Use the new Administrator account whenever performing system administrator tasks.

Working With User Accounts

The system administrator may perform any of these functions related to user accounts:

- Add new user accounts to give new users access to the ICIM2 or ICIM2-XD via the CLI and Web Interface.
- Change the password, security access level, or status (enabled or disabled) for a user account.
- Unlock user accounts that have become locked due to excessive failed login attempts.
- Delete user accounts that were entered in error or are no longer needed.
- View a list of currently logged in users.

This section describes the steps for each of these procedures.

To Add a New User

When setting up a new account, the system administrator first determines the appropriate user access level for the account. The administrator then determines whether the account will come up in a disabled or enabled state.

Complete the following steps to add a new user.

From the CLI

- 1 Log on to the ICIM2 or ICIM2-XD using an account with Admin privileges.
- 2 Enter ICIM mode.
- 3 Add the user at the ICIM prompt. For example:

```
ICIM> user add newUser1 read enable
Please enter the password: userpassword1
Please reenter the password: userpassword1
```

Note: Passwords are not echoed to the terminal as they are entered.

- 4 Type **show user**, and then confirm that the new user appears in the resulting list of usernames.

```
ICIM> show user
```

LOGIN IDENTIFIER	ACCESS LEVEL	STATUS	LAST LOGIN	FAILED	LOCKED
sysAdmin	ADMIN	Enabled	11/21/06 15:02:47	0	No
icim22	ADMIN	Enabled	11/07/06 10:05:46	0	No
newAdmin1	ADMIN	Enabled	11/21/06 15:06:11	0	No
newUser1	READ	Enabled	00/00/00 00:00:00	0	No

From the Web Interface

- 1 Log on to the ICIM2 or ICIM2-XD using an account with Admin privileges.

- 2 Click **User Mgmt** in the menu in the left pane.
- 3 When the User Management table appears, click the **New User** button beneath the table. A New User Information form appears.

New User Information

User ID	<input type="text" value="newUser1"/>
Password	<input type="password"/>
Confirm Password	<input type="password"/>
Security Level	<input type="text" value="Read-Only"/>
Status	<input type="text" value="Enabled"/>

TP398

- 4 Enter the required user account information in the form:
 - username (e.g., newUser1)
 - password (e.g., userpassword1)
 - confirm password (e.g., userpassword1)

Note: Usernames and passwords must contain 6 to 14 characters and include at least 1 alphabetic character and at least 1 number.
- 5 Choose the appropriate access level (Read-Only, Read-Write, or Admin) from the drop-down menu.
- 6 Choose the appropriate account status (enable or disable) from the drop-down menu.
- 7 Click the **Save** button to keep the changes, and then click **OK** on the confirmation dialog to confirm the change.
- 8 Verify that the new account appears on the User Management table with the correct information.

To Change a User Password

Complete the following steps to change a user password.

From the CLI

- 1 Log on to the ICIM2 or ICIM2-XD using an account with Admin privileges.
- 2 Enter ICIM mode.
- 3 Add the user at the ICIM prompt. For example:

```
ICIM> user change password newUser1
Please enter the password: changepassword2
Please reenter the password: changepassword2
```

Note: Passwords are not echoed to the terminal as they are entered.

From the Web Interface

- 1 Log on to the ICIM2 or ICIM2-XD using an account with Admin privileges.
- 2 Click **User Mgmt** in the menu in the left pane.
- 3 When the User Management table appears, click the **Edit** button on the row next to the account with the password to be changed.
- 4 When the edit window appears, verify that you are changing the correct account.

User Information (User=newUser1)

Password	<input type="text"/>	
Confirm Password	<input type="text"/>	<input type="button" value="Cancel"/> <input type="button" value="Save"/>

Security Level	<input type="text" value="Read-Only"/>	<input type="button" value="Cancel"/> <input type="button" value="Save"/>
----------------	--	---

Status	<input type="text" value="Enabled"/>	<input type="button" value="Cancel"/> <input type="button" value="Save"/>
--------	--------------------------------------	---

Unlock User	<input type="button" value="Save"/>
-------------	-------------------------------------

TP389

- 5 Type the new password in the password box (e.g., changepassword2).
- 6 Confirm the password in the confirmation box (e.g., changepassword2).
Note: Passwords are not echoed to the terminal as they are entered.
- 7 Click the **Save** button near the Confirm Password field.
- 8 When the OK to Save dialog box appears, choose **Save**.
- 9 Confirm that the user appears on the User Management table.

To Change a User Security Level

Complete the following steps to change a user security level.

From the CLI

- 1 Log on to the ICIM2 or ICIM2-XD using an account with Admin privileges.
- 2 Enter ICIM mode.
- 3 Edit the user information at the ICIM prompt. For example:
`ICIM> user change access_rights newUser1 readwrite`
- 4 Type **show user**, and then confirm that the change appears in the Access Level column of the User Management table.

```
ICIM> show user
LOGIN IDENTIFIER  ACCESS LEVEL  STATUS  LAST LOGIN          FAILED  LOCKED
sysAdmin          ADMIN         Enabled  11/21/06 15:02:47  0      No
```

Chapter 7 User Management

icim22	ADMIN	Enabled	11/07/06 10:05:46	0	No
newAdmin1	ADMIN	Enabled	11/21/06 15:06:11	0	No
newUser1	READWRITE	Enabled	00/00/00 00:00:00	0	No

From the Web Interface

- 1 Log on to the ICIM2 or ICIM2-XD using an account with Admin privileges.
- 2 Click **User Mgmt** in the menu in the left pane. The User Management table appears.
- 3 Click the **Edit** link on the row next to the account with the Security Level to be changed.
- 4 In the edit window, verify that you are changing the correct account.

User Information (User=newUser1)

TP390

- 5 Choose the appropriate Security Level from the drop-down menu.
- 6 Click the **Save** button on the Security Level row.
- 7 When the OK to Save dialog box appears, choose **Save**.
- 8 Confirm that the User Management table reflects the new security level.

To Change User Account Status

Complete the following steps to change (enable or disable) user account status.

From the CLI

- 1 Log on to the ICIM2 or ICIM2-XD using an account with Admin privileges.
- 2 Enter ICIM mode.
- 3 Edit the user information at the ICIM prompt. For example:

```
ICIM> user change account_status newUser1 disable
```
- 4 Type **show user**, and then confirm that the change appears in the Status column of the User Management table.

```
ICIM> show user
```

LOGIN IDENTIFIER	ACCESS LEVEL	STATUS	LAST LOGIN	FAILED	LOCKED
sysAdmin	ADMIN	Enabled	11/21/06 15:02:47	0	No
icim22	ADMIN	Enabled	11/07/06 10:05:46	0	No
newAdmin1	ADMIN	Enabled	11/21/06 15:06:11	0	No
newUser1	READ	Disabled	<None>	0	No

From the Web Interface

- 1 Log on to the ICIM2 or ICIM2-XD using an account with Admin privileges.
- 2 Click **User Mgmt** in the menu in the left pane. The User Management table appears.
- 3 Click the **Edit** link on the row next to the account with the status to be changed.
- 4 In the edit window, verify that you are changing the correct account.

User Information (User=newUser1)

Password
 Confirm Password
Cancel Save

Security Level Read-Write
Cancel Save

Status Enabled
Cancel Save

Unlock User Save

TP391

- 5 Choose the appropriate Status from the drop-down menu.
- 6 Click the **Save** button on the Status row.
- 7 When the OK to Save dialog box appears, choose **Save**.
- 8 Confirm that the User Management table reflects the new status.

To Unlock User Accounts

Users who reach a specified maximum number of failed ICIM2 or ICIM2-XD login attempts may have their user accounts locked. These users will be unable to log in until a predetermined lockout interval expires, or until a system administrator unlocks the account. For complete instructions on working with the User Lockout feature and unlocking user accounts, see *User Lockout* (on page 148).

To Delete a User Account

Complete the following steps to delete a user account.

From the CLI

- 1 Log on to the ICIM2 or ICIM2-XD using an account with Admin privileges.
- 2 Enter ICIM mode.
- 3 Add the user at the ICIM prompt. For example:

```
ICIM> user delete newUser1
```
- 4 Type **show user**, and then confirm that the account is no longer listed in the resulting User Management table.

```
ICIM> show user
LOGIN IDENTIFIER  ACCESS LEVEL  STATUS  LAST LOGIN  FAILED  LOCKED
sysAdmin          ADMIN         Enabled  11/21/06  15:02:47   0       No
icim22            ADMIN         Enabled  11/07/06  10:05:46   0       No
newAdmin1         ADMIN         Enabled  11/21/06  15:06:11   0       No
```

From the Web Interface

- 1 Log on to the ICIM2 or ICIM2-XD using an account with Admin privileges.
- 2 Click **User Mgmt** in the menu in the left pane. The User Management table appears.

User Management

(Max 16 Users)

Number	User ID	Security	Status	Last Login	Failed Logins	Locked		
1	Administrat0r	Admin	Enabled	03/08/07 11:11:32	0	No	Edit	Delete
2	document2	Read-Only	Enabled	<None>	0	No	Edit	Delete
3	icim22	Read-Only	Enabled	<None>	0	No	Edit	Delete
4	newUser5	Read-Only	Enabled	<None>	0	No	Edit	Delete
5	newAdmin1	Admin	Enabled	<None>	0	No	Edit	Delete

[New User](#)

TP392

- 3 Click the **Delete** button next to the row with the username for the account to remove.
- 4 In the confirmation box, verify that you are deleting the account that you intend to remove.
- 5 Verify that the account is not listed on the User Management Table.

Note: After an account is deleted, there is no more information concerning it except what has already been logged in the event log file.

To List All Currently Logged In Users

Complete the following steps to list all current ICIM2 or ICIM2-XD users.

From the CLI

- 1 Navigate to the ICIM prompt.
- 2 Type **who**, and then press **Enter** to display a list of current users.

```

ICIM> who
LOGIN IDENTIFIER      IP ADDRESS      TYPE      LOGIN TIME
icim22                172.9.9.12      CLI       11/21/06 15:08:10
newAdmin1             172.8.8.12      WEB       11/21/06 14:18:34

```

From the Web Interface

- 1 Click the **User Mgmt** menu option on the left pane.
- 2 View the Currently Logged In table in the lower section of the page.

Currently Logged In

User ID	Session Type	Source IP	Login Date / Time
document2	WEB	172.18.1.7	11/28/06 16:13:45

TP399

User Lockout

The User Lockout feature imposes a temporary lockout on ICIM2 or ICIM2-XD users who reach the maximum number of failed login attempts. Users who are locked out will not be able to log in to the ICIM2 or ICIM2-XD until the lockout interval expires, even if they try to log in using the correct login information.

By default, User Lockout is enabled with a lockout interval of 60 minutes. Admin users can select any lockout interval from 1 to 60 minutes, or can set the interval to 0 to disable User Lockout. All changes made to the lockout interval are recorded in the event log.

Admin users have commands available for checking the lockout time remaining by user and for unlocking a locked user account before the lockout interval expires. Admin users and users with unknown user names are not subject to lockouts. Lockout data is stored in volatile memory, so if the ICIM2 or ICIM2-XD reboots, this data is lost and all users are unlocked.

This section describes the following User Lockout actions available to Admin users:

- View the current lockout interval
- Specify a new lockout interval
- View locked-out users
- View lockout time remaining by user
- Unlock a locked-out user

Admin users can perform all of these actions through CLI commands, and can view the current lockout interval, specify a new interval, and view locked-out users through the ICIM Web Interface.

To View the Current Lockout Interval

Complete the following steps to view the current status of the User Lockout feature.

From the CLI

- 1 Log on to the ICIM2 or ICIM2-XD using an account with Admin privileges.
- 2 Enter ICIM command mode.
- 3 Type **show lockout**, and then press **Enter**. The system displays the current user lockout interval, as shown in the example below.

```
ICIM> show lockout
LOCKOUT
60
SUCCESS!
ICIM>
```

The number following LOCKOUT is the current length of the lockout interval in minutes. An interval of 0 means that user lockout is disabled.

Note: You can use **info lockout** instead of **show lockout**; the two commands have identical functions.

From the Web Interface

- 1 Log on to the ICIM2-XD using an account with Admin privileges.
- 2 Click **System Settings** in the menu in the left pane. The System Settings table appears as shown in the example below.

System Settings

Login Settings

Max Login Attempts	5	attempts	1-15 attempts, 0 disables the limit.
Inactivity Timeout	60	minutes	1-60 minutes
Lockout Interval	60	minutes	1-60 minutes, 0 disables the lockout feature

TP393

- 3 Note the value in the Lockout Interval field. This number indicates the current length of the lockout interval in minutes. A value of 0 means that User Lockout is disabled.

To Specify a New Lockout Interval

Complete the following steps to either disable User Lockout or to enable this feature and specify a new lockout interval.

From the CLI

- 1 Log on to the ICIM2 or ICIM2-XD using an account with Admin privileges.
- 2 Enter ICIM mode.
- 3 Type **set lockout x**, where **x** is a whole number from 0 to 60, and then press **Enter**. The system acknowledges your entry, as shown in the example below.

```
ICIM> set lockout 30
SUCCESS!
ICIM>
```

Note:

- Setting the lockout interval to 0 disables user lockout.
- Never change the User Lockout interval while a user is locked, as this may result in an unexpected actual lockout interval for the user.

From the Web Interface

- 1 Log on to the ICIM2-XD using an account with Admin privileges.
- 2 Click **System Settings** in the menu in the left pane.

- When the System Settings table appears, click in the **Lockout Interval** field and type the desired lockout value in the space provided.

System Settings

Login Settings

Max Login Attempts	5	attempts	1-15 attempts, 0 disables the limit.
Inactivity Timeout	60	minutes	1-60 minutes
Lockout Interval	60	minutes	1-60 minutes, 0 disables the lockout feature

TP394

- Click **Apply** to save your changes, or click **Cancel** to abort.

To View Locked-Out Users

Complete the following steps to view a list of all users and their current lockout status.

From the CLI

- Log on to the ICIM2 or ICIM2-XD using an account with Admin privileges.
- Enter ICIM mode.
- Type **show user**, and then press **Enter**. The system displays a list of all users, as shown in the example below.

```
ICIM> show user
```

LOGIN IDENTIFIER	ACCESS LEVEL	STATUS	LAST LOGIN	FAILED	LOCKED
Administrat0r	ADMIN	Enabled	03/08/07 11:11:32	0	No
document2	READ	Enabled	<None>	0	Yes
icim22	READ	Enabled	<None>	0	No
newUser5	READ	Enabled	<None>	0	No

- Check the values in the LOCKED column. Any users with YES in this column, such as document2 in the example above, are currently locked out.

Note: When a user account becomes locked, the Failed count (number of failed login attempts) is returned to zero.

From the Web Interface

- Log on to the ICIM2 or ICIM2-XD using an account with Admin privileges.

- Click **User Mgmt** in the menu in the left pane. The User Management table appears as shown in the example below.

User Management

(Max 16 Users)

Number	User ID	Security	Status	Last Login	Failed Logins	Locked		
1	Administrat0r	Admin	Enabled	03/08/07 11:11:32	0	No	Edit	Delete
2	document2	Read-Only	Enabled	<None>	0	Yes	Edit	Delete
3	icim22	Read-Only	Enabled	<None>	0	No	Edit	Delete
4	newUser5	Read-Only	Enabled	<None>	0	No	Edit	Delete

[New User](#)

TP395

- Note the value in the LOCKED column. Any users with YES in this column, such as firstUser2 in the example above, are currently locked out.

To View Lockout Time Remaining by User

Note: This feature is available only to Admin users and is accessible only through CLI.

Complete the following steps to view the lockout time remaining for all currently locked out users.

From the CLI

- Log on to the ICIM2 or ICIM2-XD using an account with Admin privileges.
- Enter ICIM mode.
- At the ICIM prompt, type **show lockedusers**, and then press **Enter**. A listing of all currently locked out users and their remaining lockout time appears, as shown in the example below.

```
ICIM> show lockedusers
LOCKED USER      MINUTES UNTIL UNLOCK
firstUser2        12
SUCCESS!
ICIM>
```

Note: If no users are currently locked out, the word (none) will appear in the list.

To Unlock a Locked-Out User

Note: This feature is available only to Admin users and is accessible only through the CLI.

Complete the following steps to unlock a user account that has been locked due to excessive incorrect login attempts.

From the CLI

- Log on to the ICIM2 or ICIM2-XD using an account with Admin privileges.

Chapter 7 User Management

- 2 Navigate to the ICIM prompt.
- 3 Type **user unlock <username>**, where **<username>** is the name of the user to be unlocked, and then press **Enter**.

```
ICIM> user unlock firstUser2
SUCCESS!
ICIM>
```

The user account is now unlocked, and the user will be able to attempt to log in again.

Alternative Methods

There are two other ways to unlock a user account that has been locked out:

- Cycle power to the ICIM2 or ICIM2-XD off and then on again. Because lockout information is stored in volatile memory, cycling power to the ICIM2 or ICIM2-XD returns all users to default unlocked status.
- In the Web Interface, use the Unlock User feature in the Edit User window under User Management. For details, see **To Change User Account Status** in *Working with User Accounts* (on page 141).

Note: Never change the User Lockout interval while a user is locked, as this may result in an unexpected actual lockout interval for the user.

8

Event Log

The ICIM2 and ICIM2-XD use an event log to record certain events in the Prisma II system. This chapter describes the structure of the event log and identifies actions that it may record. Instructions are provided for viewing the log via the CLI or ICIM Web Interface, and for maintaining the event log via CLI commands.

In This Chapter

- Introduction..... 154
- Viewing the Event Log..... 157
- Clearing the Event Log 159
- Setting Event Log Filter Parameters..... 160
- Event Log-Related Traps 162
- Downloading and Viewing the Event Log Remotely..... 164

Introduction

The ICIM2 and ICIM2-XD maintain a log of significant events in the Prisma II system due to user activity unrelated to the network management system (NMS). The log can be viewed by Admin level users through the CLI or ICIM Web Interface. It can also be downloaded to an FTP server for offline viewing.

Certain types of events can be selected for exclusion from the log. Additionally, changes made through the MIB, usually by the NMS, are not part of the event log.

The event log holds up to 5,000 events. If a new event is logged when the log is already full, the oldest event is removed and the new event is added. To minimize log wrapping, several traps are sent to indicate that the log is nearing capacity, and one trap is sent to indicate that the log is full.

It is up to the NMS user or administrator to empty the log each time it nears capacity. To empty the event log, the NMS typically will first upload the log file from the ICIM2 or ICIM2-XD to an FTP server, and then clear the log file for new events.

Event Log Fields

Each event in the event log contains the following six fields.

Date and Time (Timestamp)

This field records the date and time that the event was logged.

User Name (User ID)

This field records the name of the user whose actions caused the event. Some events, such as inserting or removing a module, will not contain a user name.

User Access Rights (Security Level)

This field records the access rights of the user whose actions caused the event. Possible values of this field will be:

- Admin
- Read-Only
- ReadWrite
- Unknown (e.g., if there is no user name)

Event Category

This field records the category of the event. Possible values of this field will be:

- Security

- Administration
- System
- Hardware
- Provision

Event Action ID

This field records the action ID of the event. Possible values are detailed later.

Event Description

This field contains text describing the event in more detail. For example, if a module is inserted, the description would list the chassis and slot numbers for the insertion.

Event Action IDs

Each event that may appear in the event log is identified by a unique character string called an event action ID. The table below lists the action IDs for these events and identifies their respective event categories.

Note: Action IDs may be displayed differently depending on whether the log is viewed through the CLI or the ICIM Web Interface.

Event Action ID	Event Category
LOGIN_SUCCESS	SECURITY
LOGIN_FAILED	SECURITY
LOG_OFF	SECURITY
SESSION_TIMEOUT	SECURITY
LOGIN_THRSHLD_RCHD	SECURITY
IPSEC_ENABLED	SECURITY
IPSEC_DISABLED	SECURITY
IKE_PEER_ADD	SECURITY
IKE_PEER_REMOVE	SECURITY
USER_ACCT_LOCKOUT	SECURITY
CHG_LOGIN_THRESHOLD	ADMINISTRATION
CHG_TRAP_DESTINATION	ADMINISTRATION
CHG_INACTIVITY_TIMER	ADMINISTRATION
CHG_USER	ADMINISTRATION
GET_USER	ADMINISTRATION
CHG_LOG_OPTION	ADMINISTRATION

Event Action ID	Event Category
SET_CLOCK	ADMINISTRATION
CHG_SNTP	ADMINISTRATION
CHG_LOCKOUT_INTERVAL	ADMINISTRATION
LOG_NEAR_FULL	SYSTEM
LOG_FULL	SYSTEM
DOWNLOAD_START	SYSTEM
DOWNLOAD_COMPLETE	SYSTEM
REBOOT	SYSTEM
SYSTEM_ERROR	SYSTEM
WATCHDOG_CPU_OVERLOAD	SYSTEM
WATCHDOG_REBOOT	SYSTEM
EVENTLOG_FORMAT	SYSTEM
SELFTTEST_FAILED	SYSTEM
SNTP_FAILED	SYSTEM
MODULE_INSERT	HARDWARE
MODULE_REMOVE	HARDWARE
CHG_SERVICE_MODE	PROVISION
SET_CLLI	PROVISION
SET_COMMREAD	PROVISION
SET_COMMWRITE	PROVISION
SET_COMMTRAP	PROVISION
SET_GATEWAY	PROVISION
SET_IP	PROVISION
SET_SUBNET	PROVISION
SET_UPDATEID	PROVISION
SET_MODULE_CTRL	PROVISION
SET_ALARM_PARAM	PROVISION
ADD_ROUTE	PROVISION
DELETE_ROUTE	PROVISION

Viewing the Event Log

The event log may be viewed in either of two ways: through the CLI or via the ICIM Web Interface. This section describes both methods.

To View the Event Log through the CLI

Two CLI commands are available for viewing the event log.

- The **icim show eventlog** displays an abbreviated version of the event log. Only the Date and Time, User Name, and Description fields are included, so most log entries will fit on a single line on the terminal screen.
- The **icim show eventlogall** command displays all log fields: Date and Time, User Name, User Access Rights, Event Category, Action ID, and Description. Some fields use abbreviations to maintain a display that is readable on a terminal.

Examples of each command are shown below.

Abbreviated Event Log

To view an abbreviated version of the event log, use the **icim show eventlog** command, as shown in the following example.

```
CLI> icim show eventlog
11/17/06 09:24:17 Administrat0r Set ICIM CLLI to ICIM2_CLLI
11/17/06 09:23:33 Administrat0r Log Off
11/17/06 09:22:57 Module inserted (1/12)
11/17/06 09:22:55 Module inserted (1/9)
11/17/06 09:22:32 Administrat0r Login successful
5 log messages displayed

SUCCESS!
CLI>
```

Note: The example above also illustrates that no user name is shown for module insertion events.

Full Event Log

To view a full version of the event log that includes all fields, use the **icim show eventlogall** command, as shown in the following example.

```
CLI> icim show eventlogall
11/17/06 09:24:17 Administrat0r AD PR SET_CLLI Set ICIM CLLI t
o ICIM2_CLLI
11/17/06 09:23:33 Administrat0r AD SE LOG_OFF Log Off
11/17/06 09:22:57 HW MODULE_INSERT Module inserted
(1/12)
11/17/06 09:22:55 HW MODULE_INSERT Module inserted
(1/9)
11/17/06 09:22:32 Administrat0r AD SE LOGIN_SUCCESS Login successfu
l
5 log messages displayed

SUCCESS!
CLI>
```

Chapter 8 Event Log

As shown in the example above, the full view of the event log provides more detail, but may be more difficult to read because the log entries typically do not fit on a single line.

To shorten the entries and help improve readability, abbreviated values are used in the User Access Rights and Event Category columns. The User Access Rights column will contain one of the following abbreviated values:

- AD (Admin)
- RW (ReadWrite)
- RO (Read-Only)

Note: If the user name is blank (as in the Module Insert event), the User Access Rights field will also be blank.

Similarly, the Event Category column will contain one of the following values:

- SE (Security)
- AD (Administration)
- SY (System)
- HW (Hardware)
- PR (Provisioning)

To View the Event Log through the Web Interface

After logging in, select **Event Log** from the menu in the left column. The Event Log table appears, resembling the example below.

Event Log					
Clear Event Log					
<<Previous [1] Next>>			Page 1 of 1		
Timestamp	Action	User ID	Description	Sec Level	Category
11/17/06 09:24:17	Set CLI	Administrat0r	Set ICIM CLI to ICIM2_CLI	Admin	Provision
11/17/06 09:23:33	Log Off	Administrat0r	Log Off	Admin	Security
11/17/06 09:22:57	Module Insert		Module inserted (1/12)	Unknown	Hardware
11/17/06 09:22:55	Module Insert		Module inserted (1/9)	Unknown	Hardware
11/17/06 09:22:32	Login Success	Administrat0r	Login successful	Admin	Security

The log will be displayed one page at a time, with up to 25 logs per page. Use the **Previous** and **Next** links to scroll through any additional pages.

Clearing the Event Log

To prevent event wrapping when the log gets full, the log must be periodically cleared of events. Typically, the log is downloaded to an FTP server before it is cleared from ICIM2 or ICIM2-XD memory.

The event log may be cleared through the CLI or the ICIM Web Interface. This section describes both methods.

To Clear the Event Log through the CLI

To clear the log, use the **icim eventlogclear** command. This will clear the entire log. You will be prompted for confirmation before the log is cleared, as shown in the example below.

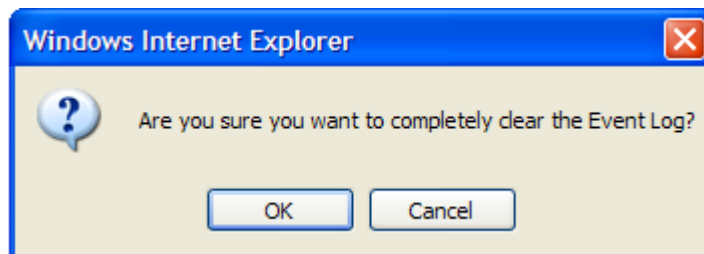
```
CLI> icim eventlogclear

You are about to remove 6 entries from the system log.
Are you sure you want to proceed (Yes/No)? yes

SUCCESS!
CLI>
```

To Clear the Event Log through the Web Interface

With the event log displayed in the Web window, click the **Clear Event Log** button. You will be asked to confirm the operation.



Click **OK** to continue.

Setting Event Log Filter Parameters

Associated with the event log are filter parameters that determine whether certain types of events are included in or excluded from the log.

Events are included or excluded according to event category. Each event belongs to one of the following event categories:

- Administration
- Hardware
- Provisioning
- Security
- System

Administration and Security events are always included in the event log. System, Hardware, and Provisioning events may be included in or excluded from the event log by changing filter parameters. Changes to event log filter parameters only affect the logging of future events. Events that are already part of the log file will remain in the log file, regardless of subsequent filter parameter changes.

Event log filter parameters may be viewed and set through the CLI or the ICIM Web Interface. This section describes both methods.

To View Filter Parameters through the CLI

To view the current filter parameter settings, use the **icim show eventlogfilter** command, as shown in the following example.

```
CLI> icim show eventlogfilter

Event Log Settings:

Provisioning Events: on
Hardware Events: on
System Events: on

(a value of "on" means to log events of that category)

SUCCESS!
CLI>
```

To Set Filter Parameters through the CLI

To change filter parameters through the CLI, use the following command:

icim eventlogfilter <category> <setting>

The possible values for <category> and <setting> are listed below along with their resulting effects on the filter settings.

<category>	<setting>	Result
hardware	on	Includes hardware events in the event log.
hardware	off	Excludes hardware events from the event log.
provisioning	on	Includes provisioning events in the event log.
provisioning	off	Excludes provisioning events from the event log.
system	on	Includes system events in the event log.
system	off	Excludes system events from the event log.

The example below turns off logging of hardware events, and then shows the filter parameters settings.

```
CLI> icim eventlogfilter hardware off
SUCCESS!
CLI> icim show eventlogfilter

Event Log Settings:

  Provisioning Events: on
  Hardware Events: off
  System Events: on

  (a value of "on" means to log events of that category)

SUCCESS!
CLI>
```

To View Filter Parameters through the Web Interface

To view the current filter parameter settings, log in to the Web Interface and then select the **System Settings** page from the left menu. The second group of items on this page shows the event log settings.

To Set Filter Parameters through the Web Interface

To change the current filter parameter settings, use the check boxes in the Event Log Settings group on the System Settings page.

Event Log Settings

<input checked="" type="checkbox"/> Log Provisioning events
<input checked="" type="checkbox"/> Log Hardware events
<input checked="" type="checkbox"/> Log System events

Check the box beside each event category to be included in the log, and clear the box beside each category to be excluded. When finished, click the **Apply** button to save your changes, or click **Cancel** to abort.

Event Log-Related Traps

To alert the NMS of possible lost event log entries due to wrapping, the ICIM2 sends several traps as the log nears capacity. A trap is sent when the log is 80%, 85%, 90%, 95%, and 100% full. This means that five traps total are sent if the NMS takes no action to clear the log. Once the log reaches 100% full and begins wrapping, no more log-full traps are sent.

The traps are of the TelcoAlarm variety, and contain all the varbinds defined as part of that trap type. All traps except the 100% full trap specify **LogMemHalfFull** as the p2TrapLogLabel varbind, although the p2TrapLogDescr varbind specifies the percentage. The 100% full trap specifies **LogMemoryFull** as the p2TrapLogLabel varbind.

Examples of the 80% full trap and the 100% full trap are provided below.

Example: 80% Full Trap

```
Specific: 9
Message reception date: 9/13/2006
Message reception time: 2:27:25.066 PM
Time stamp: 0 days 00h:11m:20s.13th
Message type: Trap (v1)
Protocol version: SNMPv1
Transport: IP/UDP
Agent
  Address: 172.24.28.193
  Port: 1035
Manager
  Address: 172.18.9.66
  Port: 162
Community: prismatrap
SNMPv1 agent address: 172.24.28.193
Enterprise: p2trapEvents
Bindings (15)
  Binding #1: p2TrapLogSequence *** (int32) 12
  Binding #2: p2TrapLogSeverity *** (int32) warning(3)
  Binding #3: p2TrapLogState *** (int32) event(3)
  Binding #4: p2TrapLogLabel *** (octets) LogMemHalfFull
  Binding #5: p2IcimStatusMsg.0 *** (int32) 0
  Binding #6: p2TrapLogText *** (octets) ICIM2
  Binding #7: p2ChassisID.2.15 *** (int32) 2
  Binding #8: p2SlotID.2.15 *** (int32) 15
  Binding #9: p2ModuleCLLlcode.2.15 *** (octets) 1.2.243
  Binding #10: p2ModuleCLEIcode.2.15 *** (octets) (zero-length)
  Binding #11: p2TrapLogTime *** (octets) 2006-9-13,1:51:39.42
  Binding #12: p2TrapLogDateTime *** (octets) Wed, 13 Sep 2006 01:51:39 EST
  Binding #13: p2TrapLogValue *** (octets) N/A
  Binding #14: p2TrapLogUnit *** (octets) N/A
  Binding #15: p2TrapLogDescr *** (octets) Log memory is %80 full
```

Example: 100% Full Trap

```

Specific: 9
Message reception date: 9/13/2006
Message reception time: 2:44:27.081 PM
Time stamp: 0 days 00h:28m:22s.13th
Message type: Trap (v1)
Protocol version: SNMPv1
Transport: IP/UDP
Agent
  Address: 172.24.28.193
  Port: 1039
Manager
  Address: 172.18.9.66
  Port: 162
Community: prismatrap
SNMPv1 agent address: 172.24.28.193
Enterprise: p2trapEvents
Bindings (15)
  Binding #1: p2TrapLogSequence *** (int32) 16
  Binding #2: p2TrapLogSeverity *** (int32) warning(3)
  Binding #3: p2TrapLogState *** (int32) event(3)
  Binding #4: p2TrapLogLabel *** (octets) LogMemoryFull
  Binding #5: p2IcimStatusMsg.0 *** (int32) 0
  Binding #6: p2TrapLogText *** (octets) ICIM2
  Binding #7: p2chassisID.2.15 *** (int32) 2
  Binding #8: p2slotID.2.15 *** (int32) 15
  Binding #9: p2moduleCLLlcode.2.15 *** (octets) 1.2.243
  Binding #10: p2moduleCLEIcode.2.15 *** (octets) (zero-length)
  Binding #11: p2TrapLogTime *** (octets) 2006-9-13,2:8:41.45
  Binding #12: p2TrapLogDateTime *** (octets) Wed, 13 Sep 2006 02:08:41 EST
  Binding #13: p2TrapLogValue *** (octets) N/A
  Binding #14: p2TrapLogUnit *** (octets) N/A
  Binding #15: p2TrapLogDescr *** (octets) Log memory is %100 full

```

Downloading and Viewing the Event Log Remotely

The event log can be downloaded from the ICIM2 or ICIM2-XD to an FTP server at any time. It is recommended that the file be downloaded before it reaches capacity to avoid losing the oldest events in the log as new events are added.

Transfer of the event log file is initiated using SNMP via the `prismallFileMgmtGroup` MIB. For additional information, see *Event Log File Management* (on page 183).

To Download the Event Log File

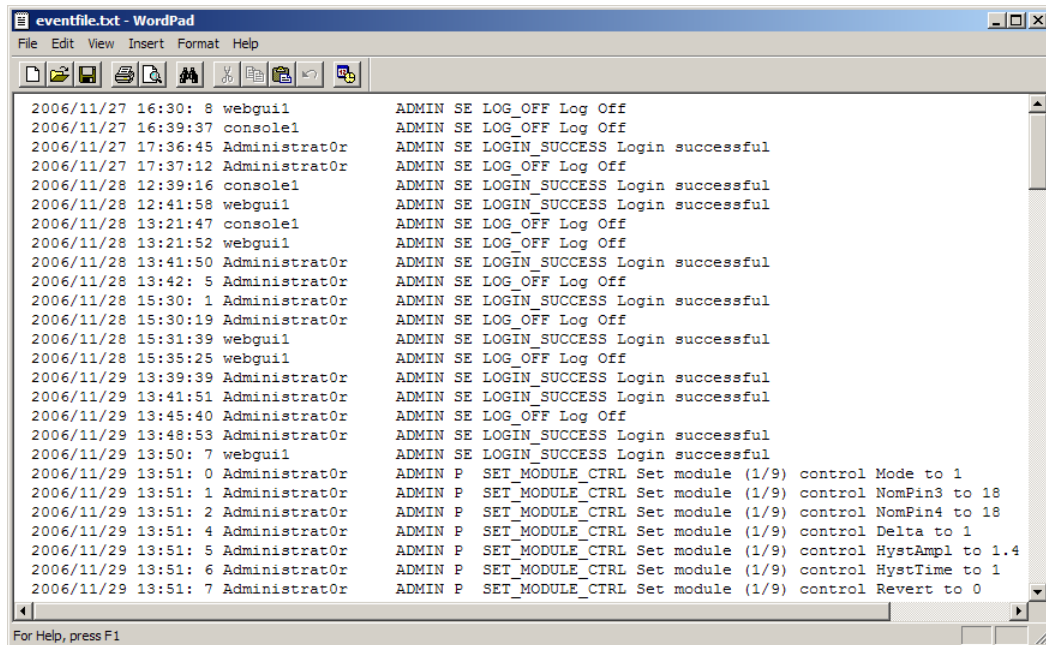
Complete the following steps in SNMP to initiate the event log file download.

- 1 Set `p2icimFileMgmtUsername` to the FTP user name.
- 2 Set `p2icimFileMgmtPassword` to the FTP password.
- 3 Set `p2icimFileMgmtIpAdress` to the IP address of the FTP server.
- 4 Set `p2icimFileMgmtFilePath` to the path of the destination file on the FTP server.
- 5 Set `p2icimFileMgmtFileName` to the destination file name on the FTP server.
- 6 Set `p2icimFileMgmtCmd` to **upload(1)**.
- 7 Set `p2icimFileMgmtAction` to **execute(2)**.

In response to these commands, the ICIM2 or ICIM2-XD will log into the FTP server and transfer the event log file.

The event log file is a text file with space-separated columns, formatted in a manner almost identical to the response to the **icim show eventlogall** command from the CLI. Most recent events appear at the bottom of the file, and there is no file header.

A sample portion of the event log file as downloaded from the ICIM2 or ICIM2-XD to an FTP server is shown below.



```

eventfile.txt - WordPad
File Edit View Insert Format Help

2006/11/27 16:30: 8 webgui1      ADMIN SE LOG_OFF Log Off
2006/11/27 16:39:37 console1    ADMIN SE LOG_OFF Log Off
2006/11/27 17:36:45 Administrat0r ADMIN SE LOGIN_SUCCESS Login successful
2006/11/27 17:37:12 Administrat0r ADMIN SE LOG_OFF Log Off
2006/11/28 12:39:16 console1    ADMIN SE LOGIN_SUCCESS Login successful
2006/11/28 12:41:58 webgui1      ADMIN SE LOGIN_SUCCESS Login successful
2006/11/28 13:21:47 console1    ADMIN SE LOG_OFF Log Off
2006/11/28 13:21:52 webgui1      ADMIN SE LOG_OFF Log Off
2006/11/28 13:41:50 Administrat0r ADMIN SE LOGIN_SUCCESS Login successful
2006/11/28 13:42: 5 Administrat0r ADMIN SE LOG_OFF Log Off
2006/11/28 15:30: 1 Administrat0r ADMIN SE LOGIN_SUCCESS Login successful
2006/11/28 15:30:19 Administrat0r ADMIN SE LOG_OFF Log Off
2006/11/28 15:31:39 webgui1      ADMIN SE LOGIN_SUCCESS Login successful
2006/11/28 15:35:25 webgui1      ADMIN SE LOG_OFF Log Off
2006/11/29 13:39:39 Administrat0r ADMIN SE LOGIN_SUCCESS Login successful
2006/11/29 13:41:51 Administrat0r ADMIN SE LOGIN_SUCCESS Login successful
2006/11/29 13:45:40 Administrat0r ADMIN SE LOG_OFF Log Off
2006/11/29 13:48:53 Administrat0r ADMIN SE LOGIN_SUCCESS Login successful
2006/11/29 13:50: 7 webgui1      ADMIN SE LOGIN_SUCCESS Login successful
2006/11/29 13:51: 0 Administrat0r ADMIN P SET_MODULE_CTRL Set module (1/9) control Mode to 1
2006/11/29 13:51: 1 Administrat0r ADMIN P SET_MODULE_CTRL Set module (1/9) control NomPin3 to 18
2006/11/29 13:51: 2 Administrat0r ADMIN P SET_MODULE_CTRL Set module (1/9) control NomPin4 to 18
2006/11/29 13:51: 4 Administrat0r ADMIN P SET_MODULE_CTRL Set module (1/9) control Delta to 1
2006/11/29 13:51: 5 Administrat0r ADMIN P SET_MODULE_CTRL Set module (1/9) control HystAmpl to 1.4
2006/11/29 13:51: 6 Administrat0r ADMIN P SET_MODULE_CTRL Set module (1/9) control HystTime to 1
2006/11/29 13:51: 7 Administrat0r ADMIN P SET_MODULE_CTRL Set module (1/9) control Revert to 0

For Help, press F1

```

In this example:

- The date-time format is yyyy/mm/dd hh:mm:ss, and seconds are shown without leading zeros.
- Event categories are abbreviated, with Security shown as SE and Provisioning shown as P.

9

SNMP Management

Introduction

This chapter provides information about using Simple Network Management Protocol (SNMP) commands for remote system monitoring and control. The ICIM2 and ICIM2-XD recognize SNMP v1 and v2c commands, but only sends SNMP v1 traps to ensure backward compatibility.

For details on chassis-related system parameters, see *Module Parameter Descriptions* (on page 347). Parameters for application modules are described in separate user documents for each module. See *Related Publications* (on page 35).

In This Chapter

■ Introduction.....	168
■ ICIM MIB	169
■ Module MIB.....	199
■ Remote Reboot of ICIM2 and Modules	226
■ Prisma II Traps	227
■ Alarm Threshold Modification	265
■ System Behavior.....	267
■ Frequently Asked Questions.....	268

Introduction

Simple network management protocol (SNMP) is an ISO standard communication protocol often used by network and element management systems to monitor network devices for alarms and other significant conditions.

SNMP accesses information about network devices through management information base (MIB) objects. MIBs are hierarchical tree-structured descriptions used to define database elements. SNMP is used to manage individual data elements and the values assigned to MIB objects.

SNMP addresses a single MIB object using a numeric string called an object identifier (OID). The OID defines a branching path through the hierarchy to the location of the object. In addition to the OID, a MIB object is known by its object descriptor, a text string intended to be more meaningful to a human operator. The OID and object descriptor are unique to each MIB object.

Also defined for each MIB object is the access that SNMP can afford to the object data value. For example, if a MIB object has read-write access, SNMP can be used to both get (retrieve) and set (define or change) the value of the object. If an object is read-only, SNMP can be used to get the object value, but not to change it.

Prisma II Enterprise MIBs

The Prisma II Enterprise management information bases (MIBs) allow easy access to ICIM2, trap, and module information via SNMP. There are two proprietary MIBs for management and event notification:

- SCIATL-PRISMAII-ICIM-MIB contains a scalar list of values used to control Prisma II ICIM management functions. Included are two trap tables, one for trap configuration and the other for trap logging.

Current version: 200702222200Z

- SCIATL-PRISMAII-MODULE-MIB contains a series of tables for managing Prisma II application modules.

Current version: 200702062209Z

These MIBs are based on the original ICIM MIBs, PRISMAII-ICIMR13-MIB and PRISMAII-MODULER13-MIB, which are now considered obsolete.

Details of the elements of the ICIM MIB and MODULE MIB are provided in the sections below.

ICIM MIB

MIB objects for the ICIM2 and ICIM2-XD fall into several categories. Information includes the state of the ICIM2 or ICIM2-XD in reference to network settings, FTP, download control, and manufacturing data. Each of the ICIM2 or ICIM2-XD object identifiers appears below with a description and other pertinent information concerning the element.

To View the ICIM MIB

To view the Prisma II ICIM MIB, be sure to compile and load both proprietary MIBs, SCIATL-PRISMAII-ICIM-MIB and SCIATL-PRISMAII-MODULE-MIB, in your MIB browser.

The ICIM2 or ICIM2-XD object identifier (OID) is 1.3.6.1.4.1.1429.1.6.2.2.13.100. This is the dot version of the full path that expands to:

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).scientificatlanta(1429).saTerr(1).saTerrOptical(6).saTerrOpticalPrismaII(2).saPrismaIIrev2(2).saPrismaIIlicim(13).prismaIIlicim(100).

ICIM MIB Elements

The ICIM MIB contains the following elements, which are discussed in detail in this section.

ICIM MIB Element	Example Value
p2icimChassisID	6
p2icimSlotID	15
p2icimSMCAAddress	615
p2icimType	5011
p2icimManufactureData	ICIM2
p2icimSerialNumber	AADORSF
p2icimHardwareRevision	BdRev87A
p2icimSoftwareRevision	2.00.08
p2icimSoftwareDate	11032006
p2icimTimeOfService	219
p2icimMACAddr	00:14:FF:FF:FF:61
p2icimIPAddr	172.24.24.24
p2icimSubnetMask	255.255.255.0

ICIM MIB Element	Example Value
p2icimGatewayAddr	172.24.24.254
p2PreviousIP	174.24.24.23
p2icimUpdateChassisIDs	0
p2icimAttnStatus	High (1)
p2icimDomainSize	6
p2icimNextImage	currentActive (1)
p2icimActiveCodeRevision	2.00.08
p2icimInactiveCodeRevision	N/ A
p2icimBootCodeRevision	2.00.03
p2icimFtpServerAddr	172.24.13.12
p2icimFtpUsername	Set
p2icimFtpPassword	Set
p2icimDownLdDir	(zero-length)
p2icimDownLdFilename	ICIM2_2_00_08_app.BIN
p2icimDownLdCmd	Cancel (4)
p2icimDownLdState	Idle (1)
p2icimDownLdTarget	100
p2icimDownLdResult	No-result-available (9999)
p2icimDownLdSignature	1146728270
p2icimDownLdSemaphore	1146720732
p2icimDownLdUser	0
p2icimCLLlcode	SCIATL01
p2icimCLElcode	VLLUAA4DAA
p2icimSelfTest	ICIM2 Self-Test Passed
p2icimStatusMsg	6 Nov 03 2006 05:50:03 AM Broadcast reboot command successful
p2icimDownLdProg	0
p2icimClock	2006-12-15 11:38:57
p2icimTimeZone	EDT
p2icimDateTime	Fri, 15 Dec 2006 11:32:57 EST
p2icimNotify	0
p2icimStatusMsgClearKey	2

p2icimChassisID

The number that appears in the chassis ID switch on the front panel of the chassis in which the ICIM2 or ICIM2-XD is installed indicates the value for the chassis ID. Valid chassis ID values are 00 to 99 inclusive. However, the use of 00 as the chassis ID value is not recommended in some circumstances, as the following caution explains.

**CAUTION:**

Setting the chassis ID to 00 is not recommended as it causes the entity MIB to violate RFC-2737 by creating an invalid object identifier. This may affect operation with some management systems that use the entity MIB. In particular, attempts to access the fans (in virtual slot 0) in chassis 00 will fail if made via serial TNCS (or ROSA-EM) or LCI.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.100.1

p2icimSlotID

The value in this object identifies the slot number in which the ICIM2 or ICIM2-XD is installed, and is always 15.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.100.2

p2icimSMCAAddress

The value in this object is the chassis number times 100 plus the ICIM2 or ICIM2-XD slot number. Leading zeros may be cropped. Thus, for chassis 20, the p2icimSMCAAddress will be 2015.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.100.3

p2icimType

The value in this object is used to uniquely identify the ICIM2 or ICIM2-XD model. In other contexts, this may be referred to as the Devtype.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.100.4

p2icimManufactureData

This object holds a string of up to 30 characters that describes the ICIM2 or ICIM2-XD in words. For the ICIM2, the string is ICIM2.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.100.5

p2icimSerialNumber

This object holds the serial number assigned to this unit during the manufacturing process.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.100.6

p2icimHardwareRevision

The value in this object is the hardware revision of this ICIM2 or ICIM2-XD, e.g., BdRev87A.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.100.7

p2icimSoftwareRevision

This object is no longer used, but kept in place for backward compatibility. Active, inactive, and boot code revisions display through p2icimActiveCodeRevision, p2icimInactiveCodeRevision, and p2icimBootCodeRevision (described below).

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.100.8

p2icimSoftwareDate

The value in this object represents the date that the firmware was built, e.g., 01202007 (Jan. 20, 2007).

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.100.9

p2icimTimeOfService

This object shows the number of hours that this ICIM2 or ICIM2-XD has been in service, which may be any number of hours starting from 0.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.100.10

p2icimMACAddr

This object holds the physical MAC address assigned to this ICIM2 or ICIM2-XD, in the form 00:11:22:33:44:55.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.100.12

p2icimIPAddr

This object holds the network IP address assigned to this ICIM2 or ICIM2-XD.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.100.13

p2icimSubnetMask

This object holds the network subnet mask used to reach this ICIM2 or ICIM2-XD.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.100.14

p2icimGatewayAddr

This object represents the network gateway address used by this ICIM2 or ICIM2-XD.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.100.15

p2PreviousIP

This object returns the value 0.0.0.0 until the IP address of the ICIM2 or ICIM2-XD is changed for the first time. After that, it holds the previous IP address.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.100.16

p2icimUpdateChassisIDs

Setting the value of this object to 1 updates every module in this ICIM2 or ICIM2-XD domain with its chassis ID and slot number. As a result, each module sends all of its information to the ICIM2 or ICIM2-XD. It takes time for the ICIM2 or ICIM2-XD to update the database with the new data. A get on this object always returns the value 0.

Access: read-write

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.100.19

p2icimAttnStatus

This object will normally display high (1) unless one of the modules pulls the attention line low (2). In that case, the ICIM2 or ICIM2-XD will service the request from the module, and when complete, will return the attention line to high (1).

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.100.20

p2icimDomainSize

This object shows the number of modules managed by this ICIM2 or ICIM2-XD.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.100.21

p2icimNextImage

The value in this object indicates which image will be active following the next ICIM2 or ICIM2-XD reboot. Values may be current active image (1) or current inactive image (2).

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.100.22

p2icimActiveCodeRevision

This object displays the active firmware image revision for the ICIM2 or ICIM2-XD.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.100.23

This object is used to determine the active software version. The ICIM2 and ICIM2-XD can store two flash images, one in the Active area and the other in the Inactive area. The SOUP program is used to download code to the two flash areas and switch between them.

p2icimInactiveCodeRevision

This object displays the inactive firmware image revision for the ICIM2 or ICIM2-XD.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.100.24

This object is used to determine the inactive software version. The ICIM2 and ICIM2-XD can store two flash images, one in the Active area and the other in the Inactive area. The SOUP program is used to download code to the two flash areas and switch between them.

p2icimBootCodeRevision

This object displays the current boot image revision for the ICIM2 or ICIM2-XD.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.100.25

p2icimFtpServerAddr**WARNING:**

This object is for use by the SOUP firmware download utility only. It is not intended for use by system operators.

Use this object to set the remote FTP server IP address for the download in the form 172.18.1.11. When the ICIM2 or ICIM2-XD receives a request to start the file transfer process via p2icimDownLdCmd, this string will be accessed for the remote IP address.

Access: read-write

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.100.26

p2icimFtpUsername**WARNING:**

This object is for use by the SOUP firmware download utility only. It is not intended for use by system operators.

Use this object to set the remote username for the FTP server. If the object does not contain a value, a get will display "Not set." For security reasons, if the username is entered and a get operation is requested, "Set" will display rather than the actual entry.

The p2icimFtpUsername may contain up to 31 characters. When the ICIM2 or ICIM2-XD receives a request to start the file transfer process via p2icimDownLdCmd, this string will be accessed for the remote username.

Access: read-write

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.100.27

p2icimFtpPassword**WARNING:**

This object is for use by the SOUP firmware download utility only. It is not intended for use by system operators.

Use this object to set the remote password for the FTP server. If the object does not contain a value, a get operation will display "Not set." For security reasons, if the password is entered and a get operation is requested, "Set" will display rather than the actual entry.

The p2icimFtpPassword may contain up to 31 characters. When the ICIM2 or ICIM2-XD receives a request to start the file transfer process via p2icimDownLdCmd, this string will be accessed for the remote password when the ICIM2 or ICIM2-XD logs into the FTP server.

Access: read-write

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.100.28

p2icimDownLdDir**WARNING:**

This object is for use by the SOUP firmware download utility only. It is not intended for use by system operators.

Use this object to set the remote directory path (excluding filename) on the FTP server where the download file exists. The p2icimDownLdDir may contain up to 127 printable characters. When the ICIM2 or ICIM2-XD receives a request to start the file transfer process via p2icimDownLdCmd, this string will be accessed for the remote path (without the filename).

Access: read-write

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.100.29

p2icimDownLdFilename**WARNING:**

This object is for use by the SOUP firmware download utility only. It is not intended for use by system operators.

Use this object to set the remote filename of the release file on the FTP server where the download file exists. The p2icimDownLdFilename may contain up to 31 printable characters. When the ICIM2 or ICIM2-XD receives a request to start the file transfer process via p2icimDownLdCmd, this string will be accessed for the remote filename.

Access: read-write

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.100.30

p2icimDownLdCmd**WARNING:**

This object is for use by the SOUP firmware download utility only. It is not intended for use by system operators.

This object is used to set commands for execution by the SOUP download utility.

The table below lists all valid commands.

Command	Function
ftp-begin (1)	Ftps the file using the parameters outlined above (p2icimFtpServerAddr, p2icimFtpUsername, p2icimFtpPassword, p2icimDownLdDir, p2icimDownLdFilename) to the target indicated in p2icimDownLdTarget.
download-boot-begin (2)	Downloads the boot image from RAM to flash or from RAM to a module.
download-appl-begin (3)	Downloads an application image from RAM to flash or from RAM to a module.

Command	Function
cancel (4)	Ends the current operation. This is the initialized state of this OID.
download-exit (5)	Exits the download.
version-switch (6)	Changes the pointer for the current inactive image to become the current active image following the next reboot.
soft-reboot (7)	Initiates a firmware reboot.
hard-reboot (8)	Initiates a hardware reboot.
enable-reboot (9)	Allows the next reboot command to take effect on the ICIM2, ICIM2-XD, or module indicated in the p2icimDownLdTarget.
disable-reboot (10)	Disallows the next reboot command to take effect on the ICIM2, ICIM2-XD, or module indicated in the p2icimDownLdTarget.
download-cancel (11)	Cancels the download.
inactive (12)	Used by the ICIM2 or ICIM2-XD firmware exclusively during the download.
invalidate-image (13)	Instructs the ICIM2 or ICIM2-XD to erase its inactive image, which is done to prevent use of an application image that may be incompatible with the boot image.

Access: read-write

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.100.31

p2icimDownLdState

This object displays the state machine value to indicate FTP download progress. The values for the download state are set by the download software, and may be one of the following:

Value	Meaning
idle (1)	Indicates the idle state, which is also the initialized state.
ftp-in-progress (2)	Indicates that an image is being transferred to the ICIM2 or ICIM2-XD.
download-in-progress (3)	Indicates that an image is being written to flash or transferred to a module.
version-switch-in-progress (4)	Indicates that the NextImage pointer is being toggled in the ICIM2 or ICIM2-XD or a module from currentActive to currentInactive, or vice versa.
reboot-in-progress (5)	Indicates that an entity (ICIM2, ICIM2-XD, or module) is being rebooted.

Value	Meaning
reboot-enable-in-progress (6)	Indicates that an entity is being flagged for reboot.

Note: If the file being transferred is small, these states may change too quickly to be seen individually.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.100.32

p2icimDownLdTarget



WARNING:

This object is for use by the SOUP firmware download utility only. It is not intended for use by system operators.

This object identifies the ICIM2 or ICIM2-XD or module chassis and slot to upgrade with the release image, in the form of 0015 for chassis 00, slot 15. This may be the broadcast address of 9999. The target must be set before a file may be downloaded.

Access: read-write

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.100.33

p2icimDownLdResult

Perform a get on this object to display the result of the download as one of 47 result codes. The result codes are self-explanatory, e.g., ftp-success(200).

P2icimDownLdResult is only valid when the download state is idle.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.100.34

p2icimDownLdSignature

This object is used by the element management system when launching the SOUP utility for the download. Performing a get on this object returns a value generated by the ICIM2 or ICIM2-XD clock. The value of the signature is not necessarily positive. See *Remote Firmware Download Feature* (on page 271) for details.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.100.35

p2icimDownLdSemaphore



WARNING:

This object is for use by the SOUP firmware download utility only. It is not intended for use by system operators.

This object is used together with p2icimDownLdUser exclusively by the SOUP utility to prevent multiple sessions of the SOUP from accessing the ICIM2 or ICIM2-XD simultaneously. Performing a get on this object returns either 0 or a value generated by the ICIM2 or ICIM2-XD clock. The value of the semaphore is not necessarily positive. See *Remote Firmware Download Feature* (on page 271) for details.

Access: read-write

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.100.36

p2icimDownLdUser



WARNING:

This object is for use by the SOUP firmware download utility only. It is not intended for use by system operators.

This object is used together with p2icimDownLdSemaphore exclusively by the SOUP utility to prevent multiple sessions of the SOUP from accessing the ICIM2 or ICIM2-XD simultaneously. Performing a get on this object when it is not in use returns the value 0. See *Remote Firmware Download Feature* (on page 271) for details.

Access: read-write

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.100.37

p2icimCLLlcode

Use this object to set the Common Language Locator ID (CLLI) code for the ICIM2 or ICIM2-XD. The maximum length of this string is 20 alphanumeric characters.

Access: read-write

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.100.38

p2icimCLElcode

Use this object to view the Common Language Equipment ID (CLEI) code that is written to the ICIM2 or ICIM2-XD as part of the manufacturing process. The maximum length of this string is 20 alphanumeric characters. An example of a CLEI code is VLL4AALDAA.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.100.39

p2icimSelfTest

Use this object to display the results of the basic functional self-test that the ICIM2 or ICIM2-XD performs at boot-up. If the ICIM2 or ICIM2-XD passed the self-test, performing a get on this object returns the message "ICIM Self-Test Passed." If the ICIM2 or ICIM2-XD encountered one or more problems, a get on this object returns the message "ICIM Self-Test failed - Error Code" followed by a decimal representation of the hexadecimal code of the failure(s).

ICIM Test Failed	Hexadecimal Code	Decimal Value
SDRAM	0x01000001	16777217
Boot Flash	0x01000002	16777218
Application Flash	0x01000004	16777220
EEPROM	0x01000008	16777224
Real Time Clock	0x01000010	16777232
Real Time Clock Battery	0x01000020	16777248

If the ICIM2 or ICIM2-XD encounters more than one problem, the error code returned is the *sum* of the individual error codes. For example:

- If the Real Time Clock Battery failed the self-test, the error code would be 16777248 decimal or 1000020 hex.
- If the Real Time Clock Battery and the Real Time Clock both failed the self-test, the error code would be $((16 + 32) + 16777216 =) 16777264$ decimal or $((10 + 20) + 1000000 =) 1000030$ hex.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.100.40

p2icimStatusMsg

Use this object to display the most recent status or error message saved in the ICIM2 or ICIM2-XD. An example of an informational message is:

```
6 Jan 18 2006 01:12:35 PM Broadcast reboot command successful
```

In this message:

- 6 is the level, meaning notice.
- Jan. 18 2006 is the date.
- 01:12:35 PM is the time.
- "Broadcast reboot command successful" is the message text.

The importance level of a message may be one of the following: emergency (1), alert (2), critical (3), error (4), warning (5), notice (6), or general system (7).

Note: To clear p2icimStatusMsg, set p2icimStatusMsgClearKey to 1. Otherwise, the current status message will persist until replaced by a message having an equal or greater urgency level.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.100.41

p2icimDownLdProg



WARNING:

Accessing this object while the SOUP firmware download utility is running may interfere with the progress of the download.

Perform a get on this object to display the current download progress percentage when a new image is being transferred from RAM to flash or from RAM to a module. The SOUP utility also displays download progress to the user through a colored progress bar.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.100.42

p2icimClock

Perform a get on this object to return the ICIM2 or ICIM2-XD date and time in the format: 2006-1-18,9:14:8. To change the ICIM2 or ICIM2-XD clock, set this object in the format MM/DD/YY HH:MM:SS, for example: 03/02/07 08:01:01. Note that leading zeros are important.

Access: read-write

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.100.43

p2icimTimeZone

To add the time zone to the ICIM2 or ICIM2-XD, set p2icimTimeZone to one of the valid USA time zones using the following abbreviations:

Abbreviation	Time Zone
EST	Eastern Standard Time
EDT	Eastern Daylight Time
CST	Central Standard Time
CDT	Central Daylight Time
MST	Mountain Standard Time
MDT	Mountain Daylight Time
PST	Pacific Standard Time
PDT	Pacific Daylight Time

Abbreviation	Time Zone
AST	Alaska Standard Time
ADT	Alaska Daylight Time
HST	Hawaii-Aleutian Standard Time
HDT	Hawaii-Aleutian Daylight Time

Note: If a time zone is not entered, the default time zone "EST" appears.

Access: read-write

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.100.44

p2icimDateTime

This object displays the day of the week, date, time, and time zone in the format "Thu, 04 May 2006 22:43:11 EDT."

Note: If a time zone is not entered in p2icimTimeZone, the default time zone EST (Eastern Standard Time) appears.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.100.45

p2icimNotify

This object tracks the number of times that an ICIM MIB or Module MIB object is set through the CLI or Web Interface. The value in this object is an integer that starts at 1 when the ICIM2 or ICIM2-XD boots up, and increments each time an ICIM MIB or Module MIB object is set through the CLI or Web Interface.

If p2icimNotify reaches its maximum value of 2,147,483,647 (hexadecimal 7FFFFFFF), any further changes cause the value to return to 1 and increment again from that point. Thus, once incremented, the value of p2icimNotify only returns to 0 if the ICIM2 or ICIM2-XD is reset.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.100.46

p2icimStatusMsgClearKey

This object lets you control whether status messages are cleared or kept by assigning one of two possible values:

Value	Function
1	Clear status messages
2	Keep status messages

Setting the value of this object to 2 lets the user exit the object gracefully, without error messages or other impact. This setting also allows the status message to persist unless replaced by a message of the same or greater urgency level. A get on this object always returns the value 2.

Access: read-write

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.100.47

Event Log File Management

The Prisma II File Management Group (prismaIIFileMgmtGroup) is a subset of ICIM MIB objects that allows the user to transfer an event log file from the ICIM2 or ICIM2-XD to a remote computer or workstation. These objects also let users evaluate the progress of the file transfer, as well as to clear the event log, which is recommended following an event log file transfer.

The prismaIIFileMgmtGroup object identifier (OID) is 1.3.6.1.4.1.1429.1.6.2.2.13.101. This is the dot version of the full path that expands to:

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).scientificatlanta(1429).saTerr(1).saTerrOptical(6).saTerrOpticalPrismaII(2).saPrismaIIrev2(2).saPrismaIIlicim(13).prismaIIFileMgmtGroup(101).

Step-by-step procedures for transferring and clearing the event log are provided below following individual prismaIIFileMgmtGroup object descriptions.

p2icimFileMgmtCmd

This object selects the type of activity to perform: uploadLog (1) or clearLog (2). To transfer the event log to a remote PC or workstation, set p2icimFileMgmtCmd to 1. To clear all entries from the event log on the ICIM2 or ICIM2-XD and reformat it to restart logging, set p2icimFileMgmtCmd to 2.

Note: p2icimFileMgmtCmd must be set before p2icimFileMgmtAction is set (see below) in order to perform a successful event log transfer or clear action.

Access: read-write

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.101.1

p2icimFileMgmtAction

This object executes the event log transfer or clear action as defined by p2icimFileMgmtCmd. When p2icimFileMgmtAction is set to execute (2), the file transfer begins or the event log is cleared. Other valid values for p2icimFileMgmtAction are idle (1) and abort (3).

Note: For a successful transfer or clear action to occur, p2icimFileMgmtCmd and all other related prismaIIFileMgmtGroup MIB objects must be set before setting p2icimFileMgmtAction to execute (2). To abort an upload, set p2icimFileMgmtAction to abort (3).

Access: read-write

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.101.2

p2icimFileMgmtIpAdress

This object holds the destination FTP server IP address, in the format 172.240.250.1, of the remote PC or workstation to which the event log will be transferred. For file transfers, this object must be set before the command is executed.

Access: read-write

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.101.3

p2icimFileMgmtUsername

This object holds the FTP username for the file transfer process. The username may be up to 31 characters. Before a username is entered, a get on p2icimFileMgmtUsername returns "Not set." After a username is entered, a get on this object returns "Set." The object does not return the username itself for security reasons. For file transfers, this object must be set before the command is executed.

Access: read-write

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.101.4

p2icimFileMgmtPassword

This object holds the FTP password for the file transfer process. The password may be up to 31 characters. Before a password is entered, a get on p2icimFileMgmtPassword returns "Not set." After a password is entered, a get on this object returns "Set." The object does not return the password itself for security reasons. For file transfers, this object must be set before the command is executed.

Access: read-write

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.101.5

p2icimFileMgmtFilePath

This object holds the full path (minus the filename) where the event log should be stored on the remote PC or workstation. The path may be up to 127 characters, and may be of zero length. For file transfers, this object must be set before the command is executed. A path of zero length implies the FTP server directory on the remote machine.

Access: read-write

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.101.6

p2icimFileMgmtFileName

This object holds the name of the event log file following upload to the remote system. The filename may be up to 31 characters in length, including an optional file extension; for example, event1024.log. For file transfers, this object must be set before the command is executed.

Access: read-write

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.101.7

p2icimFileMgmtXferSize

This object holds the size in bytes of the file to be transferred from the ICIM2 or ICIM2-XD. This information is supplied by the underlying file transfer program, and may be used together with p2icimFileMgmtXferBytes to calculate the progress of the file transfer process (see below).

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.101.8

p2icimFileMgmtXferBytes

This object holds the number of bytes of the file that have been transferred so far. This information is supplied by the underlying file transfer program, and may be used together with p2icimFileMgmtXferSize to calculate the progress of the file transfer process (see below).

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.101.9

p2icimFileMgmtResult

This object holds a value representing the progress or result of the file transfer, which is provided by the underlying file transfer program. The possible values for p2icimFileMgmtResult are listed below.

- unknown (1)
- idle (2)
- active (3)
- complete (4)
- failed (5)
- aborting (6)
- aborted (7)

Note: If no files have been transferred, the value displays as idle (2).

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.101.10

To Transfer an Event Log File

Complete the following steps to execute an event log file transfer.

- 1 Set the following MIB objects in the file management group:
 - p2icimFileMgmtUsername - file transfer FTP username
 - p2icimFileMgmtPassword - file transfer FTP password
 - p2icimFileMgmtIpAddress - destination IP address
 - p2icimFileMgmtFilePath - destination path omitting file name
 - p2icimFileMgmtFileName - destination file name only
- 2 Set p2icimFileMgmtCmd to upload (1).
- 3 Set p2icimFileMgmtAction to execute (2).

The event log file immediately starts to transfer via FTP (File Transfer Protocol) to the designated remote IP address. This implies that an active FTP server is running on the remote machine.

To Calculate File Transfer Progress

Complete the following steps to calculate progress at any point during the file transfer process.

- 1 Get the current values of p2icimFileMgmtXferSize and p2icimFileMgmtXferBytes.
- 2 Divide the value of p2icimFileMgmtXferBytes by the value of p2icimFileMgmtXferSize.
- 3 Multiply by 100. The result is the percentage of the file size transferred so far.

To Clear the Event Log File

Complete the following steps to clear the event log.

- 1 Set p2icimFileMgmtCmd to clearEventlog (2).
- 2 Set p2icimFileMgmtAction to execute (2).

After clearing the event log, logging will restart with the formatting of a new event log and a single entry in the log noting the clear action.

SNTP Time Synchronization

Synchronized Network Time Protocol (SNTP) enables the ICIM2 or ICIM2-XD to synchronize its real-time clock (RTC) with a Network Time Protocol (NTP) server. SNTP time synchronization is disabled by default, and must be enabled using SNMP or CLI commands.

SNTP time synchronization works in either of two modes: unicast or broadcast. In unicast mode, the ICIM2 or ICIM2-XD requests the time from an NTP server at regular intervals. In broadcast mode, the ICIM2 or ICIM2-XD receives the time from a designated NTP server at regular intervals. This section describes the MIB objects used to select unicast vs. broadcast mode and related SNTP operating parameters.

Important:

- SNTP and network management system (NMS) time synchronization are mutually incompatible. Before enabling the SNTP feature on the ICIM2 or ICIM2-XD, be sure to disable NMS time synchronization, and vice versa.
- The NTP server delivers the time in Coordinated Universal Time (UTC), which the ICIM2 or ICIM2-XD converts to local time. Be sure to set the time zone on the ICIM2 or ICIM2-XD; otherwise, the ICIM2 or ICIM2-XD uses the default Eastern Standard Time (EST) to calculate local time.
- In order for SNTP clock updates to work properly, the time zone must be set correctly before enabling SNTP time synchronization in the ICIM2 or ICIM2-XD.
- Before changing other SNTP settings, the SNTP state must be set to disabled (2). After changing these settings, be sure to reset the SNTP state to enabled (1) to activate the ICIM2 or ICIM2-XD SNTP task with the new parameters.

The SNTP Client group is a subset of ICIM MIB objects that allows the user to configure appropriate SNTP parameters. The SNTP Client group object identifier is 1.3.6.1.4.1.1429.1.6.2.2.13.102. This is the dot version of the full path that expands to:

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).scientificatlanta(1429).saTerr(1).saTerrOptical(6).saTerrOpticalPrismaII(2).saPrismaIIrev2(2).saPrismaIIlicim(13).prismaIISNTPClient(102).

SNTP Configuration Procedure

To request synchronization with the NTP server, you will complete the following steps:

- 1 Be sure that the SNTP state is disabled (2).
- 2 Set p2icimSNTPmode to unicast (1) or broadcast (2) (the default) as appropriate.
- 3 Set p2icimSNTPtimeout to a suitable value from 5 (the default) to 60 seconds.
- 4 Set p2icimSNTPIPaddress to the IP address of the designated NTP server.
- 5 Set p2icimSNTPinterval to a suitable value from 1 (the default) to 168 hours.
- 6 Set the SNTP state to enabled (1) to activate SNTP settings.

The parameters for requesting SNTP time synchronization are further described below. All parameters are stored in non-volatile memory, so they do not need to be reset following ICIM2 or ICIM2-XD reboots.

Note: The same sequence of steps can be performed using CLI commands, as described in the *Prisma II Platform Remote User Interface Guide, System Release 2.03*, part number 4025477.

p2icimSNTPmode

This object selects the mode for SNTP operation: unicast (1) or broadcast (2). The default is broadcast (2). To have the ICIM2 or ICIM2-XD request time from the NTP server, set p2icimSNTPmode to unicast (1). To have the ICIM2 or ICIM2-XD wait to receive time from the NTP server, set p2icimSNTPmode to broadcast (2).

Note: Before changing this setting, be sure that p2icimSNTPstate is set to disabled (2). Then, set p2icimSNTPstate to enabled (1) to activate SNTP settings.

Access: read-write

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.102.1

p2icimSNTPtimeout

This object specifies the timeout interval for unicast mode. This is the time period that the ICIM2 or ICIM2-XD waits for a response from the NTP server after requesting the time. The timeout interval is expressed in seconds as a whole-number value in the range 5 to 60. The default is 5 seconds.

The timeout interval for broadcast mode is fixed at 20 minutes. This is the time period that the ICIM2 or ICIM2-XD listens for an NTP broadcast after each user-defined interval.

Note: Before changing this setting, be sure that p2icimSNTPstate is set to disabled (2). Then, set p2icimSNTPstate to enabled (1) to activate SNTP settings.

Access: read-write

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.102.2

p2icimSNTPIPAddress

This object holds the IP address of the designated NTP server. The address must be in the format ###.###.###.###, for example, 123.3.23.12.

Note: Before changing this setting, be sure that p2icimSNTPstate is set to disabled (2). Then, set p2icimSNTPstate to enabled (1) to activate SNTP settings.

Access: read-write

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.102.3

p2icimSNTPinterval

This object sets the time interval between consecutive synchronization requests in either unicast (requesting time) or broadcast mode (waiting to receive time).

For example, if p2icimSNTPinterval is set to 24 hours:

- The ICIM2 or ICIM2-XD in unicast mode will request the time from the NTP server. When the ICIM2 or ICIM2-XD gets the time and synchronizes its real-time clock, it will wait 24 hours before requesting the time again.

- The ICIM2 or ICIM2-XD in broadcast mode will listen for an NTP broadcast for up to 20 minutes. When it receives the time and synchronizes the real-time clock, it will wait 24 hours before listening for another NTP broadcast.

This polling interval is expressed in hours as a whole-number value in the range 1 to 168 (1 week). The default is 1 hour.

Note: Before changing this setting, be sure that p2icimSNTPstate is set to disabled (2). Then, set p2icimSNTPstate to enabled (1) to activate SNTP settings.

Access: read-write

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.102.4

p2icimSNTPstate

This object defines the current state of the SNTP client as either enabled (1) or disabled (2). The default is disabled (2). Be sure to disable the SNTP client before changing any other SNTP settings, and to enable the SNTP client when ready to activate SNTP settings.

Access: read-write

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.102.5

p2icimSNTPlastUpdate

This object holds the time stamp indicating the last time the ICIM2 or ICIM2-XD was synchronized with the NTP server, in the format yyyy-mm-dd, hh:mm:ss.0. For example, 2007-2-6,13:48:16.0.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.102.6

Trap Handling

The Prisma II Trap Handling Group (prismaIItrap) is a subset of ICIM MIB objects that allows users to configure trap receiver properties. These objects also let users review the history of traps generated by the ICIM2 or ICIM2-XD.

The prismaIItrap object identifier (OID) is 1.3.6.1.4.1.1429.1.6.2.2.13.200. This is the dot version of the full path that expands to:

iso(1).org(3).dod(6).internet(1).private(4).enterprise(1).scientificatlanta(1429).saTerr(1).saTerrOptical(6).saTerrOpticalPrismaII(2).saPrismaIIrev2(2).saPrismaII(13).PrismaIItrap(200).

Trap Recv Table

Through setting the objects in the Trap Recv table, you enable traps to be sent to the IP addresses of up to 10 different receivers or targets. The index into the table represents one of 10 rows, designated 0 to 9.

To Receive Traps

Complete the following steps to receive traps.

- 1 Set p2TrapRecvEnable to enabled (2).
- 2 Set the IP address, in the format 172.18.2.24, of the remote entity to receive traps.
- 3 Set p2TrapRecvTelcoAlarm to enabled (2).

Instance	p2TrapRecvIndex[IDX]	p2TrapRecvEnable	p2TrapRecvAddr	p2TrapRecvIPC	ommand	p2TrapRecvSelfTest	p2TrapRecvTelcoAlarm
0	0	enabled(2)	172.18.50.42	enabled(2)		disabled(1)	enabled(2)
1	1	enabled(2)	172.18.50.3	enabled(2)		disabled(1)	enabled(2)
2	2	enabled(2)	172.18.50.6	enabled(2)		disabled(1)	enabled(2)
3	3	disabled(1)	0.0.0.0	disabled(1)		disabled(1)	enabled(2)
4	4	disabled(1)	0.0.0.0	disabled(1)		disabled(1)	enabled(2)
5	5	disabled(1)	0.0.0.0	disabled(1)		disabled(1)	enabled(2)
6	6	disabled(1)	0.0.0.0	disabled(1)		disabled(1)	enabled(2)
7	7	disabled(1)	0.0.0.0	disabled(1)		disabled(1)	enabled(2)
8	8	disabled(1)	0.0.0.0	disabled(1)		disabled(1)	enabled(2)
9	9	disabled(1)	0.0.0.0	disabled(1)		disabled(1)	enabled(2)

TP490

Note: All trap settings are documented for completeness. Information contained in this trap is expanded upon in the Enhanced trap. Where practical, we recommend using the Enhanced trap as it is more useful. Enabling this trap and the Enhanced trap together will cause two traps to be sent for each triggering event. For more information, see *Prisma II Traps* (on page 227).

Specific OIDs for the Trap Recv Table (1.3.6.1.4.1.1429.1.6.2.2.13.200.8) follow.

p2TrapRecvIndex

This object holds the index into a row of the p2TrapRecvEntry table. It has an integer value from 0 to 9.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.200.8.1.1

p2TrapRecvEnable

The value in this object enables or disables the complete row. If disabled (1), even though there may be a valid remote IP address saved in the row and traps may be enabled (2) in the row, traps will not be sent to this IP address. To enable the row, set p2TrapRecvEnable to enabled (2).

Access: read-write

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.200.8.1.2

p2TrapRecvAddr

To change this object from its initialized state, enter a valid IP address in the format 172.24.18.2, indicating the PC or workstation to which traps will be sent.

Access: read-write

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.200.8.1.3

p2TrapRecvIPChange

To receive a trap when the IP address of the ICIM2 or ICIM2-XD is changed, set p2TrapRecvIpChange to enabled (2). Disabled (1) is the default.

Note: All trap settings are documented for completeness. Information contained in this trap is expanded upon in the Enhanced trap. Where practical, we recommend using the Enhanced trap as it is more useful. Enabling this trap and the Enhanced trap together will cause two traps to be sent for each triggering event. For more information, see *Prisma II Traps* (on page 227).

Access: read-write

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.200.8.1.4

p2TrapRecvModuleInsert

To receive a trap when a module is inserted into any chassis managed by this ICIM2 or ICIM2-XD, set p2TrapRecvModuleInsert to enabled (2). Disabled (1) is the default.

Note: All trap settings are documented for completeness. Information contained in this trap is expanded upon in the Enhanced trap. Where practical, we recommend using the Enhanced trap as it is more useful. Enabling this trap and the Enhanced trap together will cause two traps to be sent for each triggering event. For more information, see *Prisma II Traps* (on page 227).

Access: read-write

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.200.8.1.5

p2TrapRecvModuleRemove

To receive a trap when a module is removed from any chassis managed by this ICIM2 or ICIM2-XD, set p2TrapRecvModuleRemove to enabled (2). Disabled (1) is the default.

Note: All trap settings are documented for completeness. Information contained in this trap is expanded upon in the Enhanced trap. Where practical, we recommend using the Enhanced trap as it is more useful. Enabling this trap and the Enhanced trap together will cause two traps to be sent for each triggering event. For more information, see *Prisma II Traps* (on page 227).

Access: read-write

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.200.8.1.6

p2TrapRecvMinorAlarm

Set this object to enable or disable sending traps to the SNMP manager when a minor alarm in a module changes state. The user may choose to receive minor alarm traps never (1), only when cleared (2), only when set (3), or "always," i.e., when set or cleared (4).

This trap is edge triggered, meaning that it is sent if there is a change in a monitored value that causes it to go into or out of a state of minor alarm. If p2TrapRecvEnable is set to disabled (1), traps will not be sent.

Note: All trap settings are documented for completeness. Information contained in this trap is expanded upon in the Enhanced trap. Where practical, we recommend using the Enhanced trap as it is more useful. Enabling this trap and the Enhanced trap together will cause two traps to be sent for each triggering event. For more information, see *Prisma II Traps* (on page 227).

Access: read-write

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.200.8.1.7

p2TrapRecvMajorAlarm

Set this object to enable or disable sending traps to the SNMP manager when a major alarm in a module changes state. The user may choose to receive minor alarm traps never (1), only when cleared (2), only when set (3), or "always," i.e., when set or cleared (4).

This trap is edge triggered, meaning that it is sent if there is a change in a monitored value that causes it to go into or out of a state of major alarm. If p2TrapRecvEnable is set to disabled (1), traps will not be sent.

Note: All trap settings are documented for completeness. Information contained in this trap is expanded upon in the Enhanced trap. Where practical, we recommend using the Enhanced trap as it is more useful. Enabling this trap and the Enhanced trap together will cause two traps to be sent for each triggering event. For more information, see *Prisma II Traps* (on page 227).

Access: read-write

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.200.8.1.8

p2TrapRecvDwnLdComplete

Set this object to enable (2) or disable (1) sending traps following a download to the ICIM2, ICIM2-XD, or module. Disabled (1) is the default.

Note: All trap settings are documented for completeness. Information contained in this trap is expanded upon in the Enhanced trap. Where practical, we recommend using the Enhanced trap as it is more useful. Enabling this trap and the Enhanced trap together will cause two traps to be sent for each triggering event. For more information, see *Prisma II Traps* (on page 227).

Access: read-write

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.200.8.1.9

p2TrapRecvRebootCommand

Set this object to enable (2) or disable (1) sending traps following a reboot command to the ICIM2 and/or module(s). Disabled (1) is the default.

If the reboot command is broadcast to all modules and the ICIM2 or ICIM2-XD, only one broadcast reboot trap will be generated.

Note: All trap settings are documented for completeness. Information contained in this trap is expanded upon in the Enhanced trap. Where practical, we recommend using the Enhanced trap as it is more useful. Enabling this trap and the Enhanced trap together will cause two traps to be sent for each triggering event. For more information, see *Prisma II Traps* (on page 227).

Access: read-write

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.200.8.1.10

p2TrapRecvSelfTest

Set this object to enable (2) or disable (1) sending traps following an ICIM2, ICIM2-XD, or module self-test failure. Disabled (1) is the default.

Specific self-test error code values are enumerated under **p2icimSelfTest** and **p2moduleSelfTest**.

Note: All trap settings are documented for completeness. Information contained in this trap is expanded upon in the Enhanced trap. Where practical, we recommend using the Enhanced trap as it is more useful. Enabling this trap and the Enhanced trap together will cause two traps to be sent for each triggering event. For more information, see *Prisma II Traps* (on page 227).

Access: read-write

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.200.8.1.11

p2TrapRecvTelcoAlarm

Set this object to enable (2) or disable (1) sending traps following an ICIM2, ICIM2-XD, or module alarm or event. Disabled (1) is the default, but enabled (2) is the normal operating setting to receive traps.

The Enhanced traps generate the most information concerning the condition causing the alarm or event. Bindings for the Enhanced traps are detailed in *Enhanced Trap Binding Information* (on page 241).

Access: read-write

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.200.8.1.12

Note: All trap settings are documented for completeness. Information contained in this trap is expanded upon in the Enhanced trap. Where practical, we recommend using the Enhanced trap as it is more useful. Enabling this trap and the Enhanced trap together will cause two traps to be sent for each triggering event. For more information, see *Prisma II Traps* (on page 227).

Trap Logging Auxiliaries

p2TrapLastSequenceNumber

To observe the most current sequence number used by the Enhanced traps, perform a get operation on this object. If no traps have been sent, the p2TrapLastSequenceNumber is 0. Valid sequence numbers are 1 through 2,147,483,647. The sequence number resets to 0 at startup or ICIM2 or ICIM2-XD reboot, or if the p2TrapLogEntry table is cleared with the p2TrapLogClearKey. The first trap sent after the sequence number resets will have the sequence number 1. If incremented past 2,147,483,647, the sequence number wraps to 1 again.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.200.1

p2TrapLogClearKey

To clear the p2TrapLogEntry table, set p2TrapLogClearKey to clear (1). The next Enhanced trap generated will start with sequence number 1, and be copied to the Trap Log table to start populating it again. To continue to send traps without restarting the sequencing, and continue to save them in the trap log table without first clearing it, set p2TrapLogClearKey to keep (2). This OID will return Keep Logging (2) when a get operation is performed.

Access: read-write

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.200.2

Trap Logging Table

The Trap Logging table serves as an aid to tracking by keeping a copy of up to 1,000 traps. When this table becomes full, it makes space for new trap records by deleting the oldest trap records from the table.

To activate trap logging, you configure and enable at least one row in p2TrapRecvTable. If p2TrapRecvTelcoAlarm is also enabled (2), traps are logged automatically. The trap sequence number serves as the index into the Trap Logging table.

A disruption in the network connectivity of the ICIM2 or ICIM2-XD does not mean that a trap is lost. A copy of each Enhanced trap generated is saved in the Trap Logging table, and can be retrieved using the trap sequence number.

Elements of the Trap Logging table line up with trap bindings. For more information regarding the bindings, see *Enhanced Trap Binding Information* (on page 241).

The figure below shows how the Trap Logging table might appear when displayed in a MIB browser.

Instance	p2TrapLogSequenceID	p2TrapLogSeverity	p2TrapLogState	p2TrapLogLabel	p2TrapLogOID	p2TrapLogText	p2TrapLogChassisID	p2TrapLogSlotID	p2TrapLogCLLcode	p2TrapLogCLEIcode	p2T
1	1	minor(2)	alarm(1)	InRF	p2almIndex.1.2.3	Module=HDTx, Model=1020	1	2	N/A	N/A	200
2	2	minor(2)	alarm(1)	InRF	p2almIndex.1.3.3	Module=HDTx, Model=1020	1	3	N/A	N/A	200
3	3	minor(2)	alarm(1)	InRF	p2almIndex.1.4.3	Module=HDTx, Model=1020	1	4	N/A	N/A	200
4	4	major(1)	alarm(1)	InRF	p2almIndex.1.5.3	Module=HDTx, Model=1032	1	5	N/A	N/A	200
5	5	minor(2)	alarm(1)	InRF	p2almIndex.1.7.3	Module=HDTx, Model=1032	1	7	N/A	N/A	200
6	6	minor(2)	alarm(1)	InRF	p2almIndex.1.8.3	Module=HDTx, Model=1032	1	8	N/A	N/A	200
7	7	minor(2)	alarm(1)	InRF	p2almIndex.1.9.3	Module=HDTx, Model=1032	1	9	N/A	N/A	200
8	8	minor(2)	alarm(1)	InRF	p2almIndex.1.10.3	Module=HDTx, Model=1032	1	10	N/A	N/A	200
9	9	minor(2)	alarm(1)	InRF	p2almIndex.1.11.3	Module=HDTx, Model=1032	1	11	N/A	N/A	200
10	10	minor(2)	alarm(1)	InRF	p2almIndex.1.12.3	Module=HDTx, Model=1032	1	12	N/A	N/A	200
11	11	minor(2)	alarm(1)	InRF	p2almIndex.1.13.3	Module=HDTx, Model=1032	1	13	N/A	N/A	200
12	12	minor(2)	alarm(1)	InRF	p2almIndex.1.14.3	Module=HDTx, Model=1032	1	14	N/A	N/A	200
13	13	minor(2)	alarm(1)	InRF	p2almIndex.1.16.3	Module=HDTx, Model=1032	1	16	N/A	N/A	200
14	14	major(1)	alarm(1)	InPwr	p2almIndex.2.1.1	Module=P2-HD-RXF, Model=2015	2	1	N/A	N/A	200
15	15	major(1)	alarm(1)	Alarm	p2almIndex.2.1.4	Module=P2-HD-RXF, Model=2015	2	1	N/A	N/A	200
16	16	major(1)	alarm(1)	InPwr	p2almIndex.2.2.1	Module=P2-HD-RXF, Model=2015	2	2	N/A	N/A	200
17	17	major(1)	alarm(1)	InPwr	p2almIndex.2.2.1	Module=P2-HD-RXF, Model=2015	2	2	N/A	N/A	200

LogText	p2TrapLogChassisID	p2TrapLogSlotID	p2TrapLogCLLcode	p2TrapLogCLEIcode	p2TrapLogTime	p2TrapLogDateTime	p2TrapLogValue	p2TrapLogUnit	p2TrapLogDescr
HDTx, Model=1020	1	2	N/A	N/A	2007-11-27:10:8:42.75	Tue, 27 Nov 2007 10:08:42 EST	-13.2618	dB	InRF exceeded minor threshold
HDTx, Model=1020	1	3	N/A	N/A	2007-11-27:10:8:44.50	Tue, 27 Nov 2007 10:08:44 EST	-13.8482	dB	InRF exceeded minor threshold
HDTx, Model=1020	1	4	N/A	N/A	2007-11-27:10:8:45.05	Tue, 27 Nov 2007 10:08:45 EST	-12.9882	dB	InRF exceeded minor threshold
HDTx, Model=1032	1	5	N/A	N/A	2007-11-27:10:8:47.20	Tue, 27 Nov 2007 10:08:47 EST	-50	dB	RF input exceeds major threshold
HDTx, Model=1032	1	7	N/A	N/A	2007-11-27:10:8:49.78	Tue, 27 Nov 2007 10:08:49 EST	-50	dB	RF input exceeds minor threshold
HDTx, Model=1032	1	8	N/A	N/A	2007-11-27:10:8:51.10	Tue, 27 Nov 2007 10:08:51 EST	-50	dB	RF input exceeds minor threshold
HDTx, Model=1032	1	9	N/A	N/A	2007-11-27:10:8:52.41	Tue, 27 Nov 2007 10:08:52 EST	-50	dB	RF input exceeds minor threshold
HDTx, Model=1032	1	10	N/A	N/A	2007-11-27:10:8:53.70	Tue, 27 Nov 2007 10:08:53 EST	-50	dB	RF input exceeds minor threshold
HDTx, Model=1032	1	11	N/A	N/A	2007-11-27:10:8:55.1	Tue, 27 Nov 2007 10:08:55 EST	-50	dB	RF input exceeds minor threshold
HDTx, Model=1032	1	12	N/A	N/A	2007-11-27:10:8:56.33	Tue, 27 Nov 2007 10:08:56 EST	-50	dB	RF input exceeds minor threshold
HDTx, Model=1032	1	13	N/A	N/A	2007-11-27:10:8:57.65	Tue, 27 Nov 2007 10:08:57 EST	-50	dB	RF input exceeds minor threshold
HDTx, Model=1032	1	14	N/A	N/A	2007-11-27:10:8:58.96	Tue, 27 Nov 2007 10:08:58 EST	-50	dB	RF input exceeds minor threshold
HDTx, Model=1032	1	16	N/A	N/A	2007-11-27:10:9:1.56	Tue, 27 Nov 2007 10:09:01 EST	-50	dB	RF input exceeds minor threshold
P2-HD-RXF, Model=2015	2	1	N/A	N/A	2007-11-27:10:9:4.75	Tue, 27 Nov 2007 10:09:04 EST	-21.2668	dBm	InPwr exceeded major threshold
P2-HD-RXF, Model=2015	2	1	N/A	N/A	2007-11-27:10:9:4.76	Tue, 27 Nov 2007 10:09:04 EST	N/A	N/A	Alarm exceeded major threshold
P2-HD-RXF, Model=2015	2	2	N/A	N/A	2007-11-27:10:9:6.30	Tue, 27 Nov 2007 10:09:06 EST	-21.3549	dBm	InPwr exceeded major threshold

TP489

The table below shows sample entries for each element of the Trap Logging table. The elements themselves are described in this section.

Trap Log Element	Entry 10	Entry 14
p2TrapLogSequence	10	14
p2TrapLogSeverity	minor (2)	major (1)
p2TrapLogState	alarm (1)	alarm (1)
p2TrapLogLabel	InRF	InPwr
p2TrapLogOID	p2almIndex.1.12.3	p2almIndex.2.1.1
p2TrapLogText	Module=HDTx, Model=1032	Module=P2-HD-RXF, Model= 2015
p2TrapLogChassisID	1	2
p2TrapLogSlotID	12	1
p2TrapLogCLLcode	N/A	N/A
p2TrapLogCLEIcode	N/A	N/A
p2TrapLogTime	2007-11-27, 10:8:56.33	2007-11-27, 10:9:4.75
p2TrapLogDateTime	Tue, 27 Nov 2007 10:08:56 EST	Tue, 27 Nov 2007 10:09:04 EST
p2TrapLogValue	-50	-21.2668
p2TrapLogUnit	dB	dBm
p2TrapLogDescr	RF input exceeds minor threshold	InPwr exceeds major threshold

Specific OIDs for the Trap Log Table (1.3.6.1.4.1.1429.1.6.2.2.13.200.20) follow.

p2TrapLogSequence

This object holds a unique number assigned to each trap as it is generated. This serves as an index into the Trap Logging table.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.200.20.1.1

p2TrapLogSeverity

This object holds the severity value, which assists in assigning priority to trap generating conditions. Severity may be major (1), minor (2), or warning (3).

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.200.20.1.2

p2TrapLogState

This object holds the state value which, together with severity, quickly gives a view into the current condition of the ICIM2, ICIM2-XD, or application module. State may be alarm (1), clear (2), or event (3).

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.200.20.1.3

p2TrapLogLabel

This object holds the trap log label. For an alarm or clear trap, the label must be the same as the p2almLabel assigned to the condition which caused the trap; for example, ChasTemp. For events, the value of this object indicates the type of event that occurred and caused the trap to be sent, and may be one of the following:

- DownloadComplete (reserved for future use)
- RebootCommand
- SelfTest
- AuthentictnFailed
- AdminChange
- LogMemHalfFull
- LogMemoryFull
- LoginThreshold
- SNTP (reserved for future use)
- UpdateChassisID

■ UserLockout

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.200.20.1.4

p2TrapLogOID

This object holds details regarding the condition that generated the trap. For an alarm or clear trap, this may be the third index into the Module Alarm table. For the download or reboot, this may be the p2icimStatusMessage. However, only the most recent status message is retained by the ICIM2 or ICIM2-XD. If a message from another event overwrites the status message, additional information may no longer be available at the OID specified for the particular trap. If an event is logged, details about the event may be saved in the event log.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.200.20.1.5

p2TrapLogText

This object holds a string that further describes the entity or condition responsible for trap generation. This usually is a concatenation of the module name and model number, although it may include the self-test failure code.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.200.20.1.6

p2TrapLogChassisID

The value in this object identifies the chassis in which the ICIM2, ICIM2-XD, or application module resides at the time of trap generation.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.200.20.1.7

p2TrapLogSlotID

This object holds the slot number in which the ICIM2, ICIM2-XD, or application module resides at the time of trap generation.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.200.20.1.8

p2TrapLogCLLlcode

This object is reserved for future use.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.200.20.1.9

p2TrapLogCLEIcode

This object is reserved for future use.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.200.20.1.10

p2TrapLogTime

This object holds a date and time stamp indicating when the trap was generated.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.200.20.1.11

p2TrapLogDateTime

This object displays the full local time in the format: Tue, 27 Nov 2007 10:08:56 EST. The local time zone must be entered in p2icimTimeZone or the default time zone, EST, will always show.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.200.20.1.12

p2TrapLogValue

This object holds the most recent monitored value associated with the object in alarm or clear state.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.200.20.1.13

p2TrapLogUnit

The value in this object indicates the unit of measure for the value in p2TrapLogValue.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.200.20.1.14

p2TrapLogDescr

This object holds a verbose description of the alarm.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.200.20.1.15

Module MIB

The module MIB consists of several tables indexed by the chassis and slot numbers of the modules managed by the ICIM2 or ICIM2-XD. A third index into a table may be necessary at times to create a unique instance, as further explained in *Module Alarm Table* (on page 208).

Module MIB Tables

The module MIB includes the following tables:

- p2moduleTable
- p2moduleAlarmTable
- p2moduleCurrentAlarmTable
- p2moduleMonitorTable
- p2moduleControlTable
- p2InsertModuleTable
- p2RemoveModuleTable

The contents of each module MIB table are described below.

Table Name	Table Contents
Module Table	Basic manufacturing features and firmware download data for each module.
Module Alarm Table	Status of each module with regard to alarm thresholds and nominal values. See <i>Module Alarm Table</i> (on page 208) for further information.
Module Current Alarm Table	Records the module elements in major or minor alarm at a given time.
Module Monitor Table	Contains monitored module values.
Module Control Table	Contains module controls that may be adjusted.
Insert Module Table	Chassis and slot number of each module inserted after the ICIM2 or ICIM2-XD initially polls the chassis.
Remove Module Table	Chassis number, slot number, and other information on each module removed from a chassis controlled by this ICIM2 or ICIM2-XD.

p2moduleNumber

This object shows the total number of active modules that have data in the Module table.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.1

Module Table

The Module table contains information regarding each of the modules managed by the ICIM2 or ICIM2-XD. It is indexed by the chassis and slot number where the module currently resides.

The p2moduleTable OID is: 1.3.6.1.4.1.1429.1.6.2.2.13.300.2.

Rows in the table are accessed via p2moduleEntry.

The p2moduleEntry OID is: 1.3.6.1.4.1.1429.1.6.2.2.13.300.2.1.

The figure below shows how the Module table might appear when displayed in a MIB browser.

Instance	p2chassisID	p2slotID	p2smcAddress	p2moduleType	p2nextImage	p2activeCodeRevision	p2inactiveCodeRevision	p2moduleDownloadable	p2moduleSelfTest	p2fantrayPS
1.0	1	0	100	5020	currentActi...	1.01.04	91.01.04	yes(1)	Passed	no(2)
1.1	1	1	101	1020	not-applica...	N/A	N/A	no(2)	N/A	not-applicable(3)
1.15	1	15	115	1032	not-applica...	N/A	N/A	no(2)	N/A	not-applicable(3)
2.0	2	0	200	5020	currentActi...	1.01.04	91.01.04	yes(1)	Passed	no(2)
2.3	2	3	203	2015	currentActi...	1.01.11	91.01.11	yes(1)	Passed	not-applicable(3)
2.12	2	12	212	2015	currentActi...	1.01.11	91.01.11	yes(1)	Passed	not-applicable(3)
3.0	3	0	300	5020	currentActi...	1.01.04	91.01.04	yes(1)	Passed	no(2)
3.2	3	2	302	2014	currentActi...	1.01.09	91.01.09	yes(1)	Passed	not-applicable(3)
3.6	3	6	306	2011	currentActi...	1.01.08	91.01.08	yes(1)	Passed	not-applicable(3)
3.11	3	11	311	2014	currentActi...	1.01.09	91.01.09	yes(1)	Passed	not-applicable(3)
3.16	3	16	316	2011	currentActi...	1.01.08	91.01.08	yes(1)	Passed	not-applicable(3)
98.0	98	0	9800	5020	currentActi...	1.01.04	91.01.04	yes(1)	Passed	no(2)
98.4	98	4	9804	1020	not-applica...	N/A	N/A	no(2)	N/A	not-applicable(3)
98.5	98	5	9805	1020	not-applica...	N/A	N/A	no(2)	N/A	not-applicable(3)
98.9	98	9	9809	1020	not-applica...	N/A	N/A	no(2)	N/A	not-applicable(3)
98.10	98	10	9810	1020	not-applica...	N/A	N/A	no(2)	N/A	not-applicable(3)
98.11	98	11	9811	1020	not-applica...	N/A	N/A	no(2)	N/A	not-applicable(3)
98.13	98	13	9813	1020	not-applica...	N/A	N/A	no(2)	N/A	not-applicable(3)
98.14	98	14	9814	1020	not-applica...	N/A	N/A	no(2)	N/A	not-applicable(3)
98.15	98	15	9815	1020	not-applica...	N/A	N/A	no(2)	N/A	not-applicable(3)

The table below shows sample entries for each element of the Module table. The elements themselves are described in this section.

Module Table	First Module Entry	Second Module Entry
p2chassisID	1	1
p2slotID	0	1
p2smcAddress	100	101
p2moduleType	5020	1020
p2moduleName	XD-Chassis	HDTx
p2manufactureData		3dBm TxTS 1310 nm
p2dateCode	M07	H07
p2serialNumber	^ABCDEFGF	^MMAAFEFJ
p2coreCodeRevision	CF_CCB3	155
p2scriptRevision	N/A	1

Module Table	First Module Entry	Second Module Entry
p2timeOfService	744	1633
p2numOfMonitoredVars	14	7
p2numOfAnalogControls	0	1
p2numOfDigitalControls	2	5
p2numOfControls	2	6
p2numOfAlarms	12	7
p2NextImage	currentActive (1)	not-applicable (3)
p2activeCodeRevision	1.01.04	N/A
p2inactiveCodeRevision	91.01.04	N/A
p2bootCodeRevision	0.00.03	N/A
p2moduleCLLcode	N/A	N/A
p2moduleCLEIcode	N/A	N/A
p2moduleDownloadable	yes (1)	no (0)
p2moduleSelfTest	Passed	N/A
p2FantrayPSsplit	no (2)	not-applicable (3)

p2chassisID

This object identifies the chassis number in which the module is installed. The value in this object provides one index into the Module table.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.2.1.1

p2slotID

This object identifies the slot number in which the module is currently installed. The value in this object provides one index into the Module table.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.2.1.2

p2smcAddress

This object reports the module status monitoring and control (SMC) address, which is the chassis number times 100, plus the slot number of this module. For example, a module in chassis 1 slot 1 would have a p2smcAddress of 101.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.2.1.3

p2moduleType

This object holds a number assigned during the manufacturing process to uniquely identify this type of module. This is also referred to as the **devtype** or TNCS type number.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.2.1.4

p2moduleName

This object holds the name assigned to modules of this particular type.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.2.1.5

p2manufactureData

This object holds a string of manufacturing data, which can be up to 30 characters in length.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.2.1.6

p2dateCode

This object holds the date code, which is a string consisting of three characters. A letter specifies the month, and a two-digit number specifies the year this module was manufactured and tested. The following letters are used to specify the month:

Letter	Month
A	January
B	February
C	March
D	April
E	May
F	June
G	July
H	August
J	September
K	October
L	November
M	December

Example: M07 = December 2007

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.2.1.7

p2serialNumber

The value in this object designates the module serial number.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.2.1.8

p2coreCodeRevision

The value in this object is CF_CCB3 for downloadable CCBs designed to interface with the ICIM2 or ICIM2-XD.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.2.1.9

p2scriptRevision

This object is deprecated in the downloadable modules, which do not use scripts. It is retained for compatibility with previous versions of the modules, which still use scripts.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.2.1.10

p2timeOfService

This object reports the number of hours this module has been in service. The value is updated every hour for the first 120 hours, and every 12 hours up to 120,000.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.2.1.11

p2numOfMonitoredVars

The value in this object represents the total number of monitored variables for this module.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.2.1.12

p2numOfAnalogControls

The value in this object represents the total number of analog variables for this module.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.2.1.13

p2numOfDigitalControls

The value in this object represents the total number of digital and state controls for this module.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.2.1.14

p2numOfControls

The value in this object represents the total number of control variables for this module.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.2.1.15

p2numOfAlarms

The value in this object represents the total number of alarm variables for this module.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.2.1.16

p2NextImage

The value in this object represents the firmware image to be active following the module reboot. Options are currentActive (1), currentInactive (2), or not applicable (3).

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.2.1.17

p2activeCodeRevision

The value in this object represents the version of the firmware active for this module.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.2.1.18

p2inactiveCodeRevision

This object is reserved for future use.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.2.1.19

p2bootCodeRevision

The value in this object represents the current boot image revision for the module.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.2.1.20

p2moduleCLLlcode

This object is reserved for future use.

Access: read-write

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.2.1.21

p2moduleCLElcode

This object is reserved for future use.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.2.1.22

p2moduleDownloadable

The value in this object indicates whether the module supports firmware downloads. The value may be either yes (1) or no (2).

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.2.1.23

p2moduleSelfTest

This object displays the results of the basic functional self-test that the module performs at boot-up or when inserted into a chassis slot. If the module passed the self-test, performing a get on this object returns the message "Self-Test Passed." If the module encounters one or more problems, the message "Self-Test failed - Error Code" is returned followed by a decimal representation of the hexadecimal code of the failure(s).

Self-Test Error Codes: Prisma II Platform

The following error codes are used for the Prisma II Fan Tray, Pre-Amplifier, Post-Amplifier, and Optical Switch modules.

Modules Test Failed	Hexadecimal Code	Decimal Value
Flash bank 1 CRC	0x2000001	33554433
Flash bank 2 CRC	0x2000002	33554434
ColdFire RAM	0x2000004	33554436

Flash bank 0 CRC	0x2000008	33554440
EEPROM read	0x2000010	33554448
EEPROM write	0x2000020	33554464
EEPROM write-protect	0x2000040	33554496
SPI BUS	0x2000080	33554560
Local Craft Interface port	0x2000100	33554688
ICIM 485 port	0x2000200	33554944
Local Debug port	0x2000400	33555456
CAN BUS	0x2000800	33556480
Analog to Digital	0x2001000	33558528
Digital to Analog	0x2002000	33562624
IO	0x2004000	33570816
Power Supply	0x2008000	33587200

Self-Test Error Codes: Prisma II XD Platform

The following error codes are used for the Prisma II XD client control board, fan assembly, AC-to-DC bulk power supplies, DC-to-DC converters, ICIM2 or ICIM2-XD, and installed application modules.

Modules Test Failed	Hexadecimal Code	Decimal Value
Flash bank 1 CRC	0x2000001	33554433
Flash bank 2 CRC	0x2000002	33554434
ColdFire RAM	0x2000004	33554436
Flash bank 0 CRC	0x2000008	33554440
EEPROM read	0x2000010	33554448
EEPROM write	0x2000020	33554464
EEPROM write-protect	0x2000040	33554496
SPI BUS	0x2000080	33554560
Local Craft Interface port	0x2000100	33554688
ICIM2 485 port	0x2000200	33554944
Local Debug port	0x2000400	33555456
CAN BUS	0x2000800	33556480
Analog to Digital	0x2001000	33558528
Digital to Analog	0x2002000	33562624
IO	0x2004000	33570816

Power Supply	0x2008000	33587200
--------------	-----------	----------

If self-test discovers more than one problem, the error code returned is the *sum* of the individual error codes. For example:

- If the power supply on a pre-amplifier failed, the error code displayed would be 33587200 in decimal (2008000 hex).
- If the power supply and the write to the EEPROM failed on a post-amplifier module self-test, the error code would be $((32768 + 32) + 33554432 =) 33587232$ decimal or $((8000 + 20) + 2000000 =) 2008020$ hex.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.2.1.24

p2FantrayPSsplit

Note: This object pertains to the Prisma II Platform chassis only.

The value in this object tells the NMS how to interpret alarms that originate from a fan tray, power supply, or application module. This information is important in establishing the actual origin of fan tray and power supply alarms for troubleshooting purposes.

The fan tray manages alarms for the fan tray as well as for the power supply modules in slot 1 and slot 3. The ICIM2 with Release 1.00 firmware associates fan tray, power supply 1, and power supply 3 alarms with a single logical chassis slot location (slot 3). The NMS must then remap the alarms to physical chassis slot locations in order to indicate the actual origin of the alarm.

In a chassis with an ICIM2 at Release 2.00 or later and a fan tray at Release 1.01 or later firmware, these alarms are reported as originating from their respective physical chassis slot locations. This makes it unnecessary for the NMS to remap fan tray and power supply alarms to chassis slot locations.

However, due to the potential mix of 1.00 and 1.01 fan trays in the field, the NMS must be told when to remap alarms to physical slot locations for a particular chassis. The p2FantrayPSsplit element performs this function. It has three possible values:

Value	Meaning
Yes (1)	This module is a newer fan tray (DevType 5012) or power supply (DevType 5013) with split data. Therefore, the data is only for the particular module (fan tray or power supply) you are viewing. The NMS does not need to perform slot remapping.
No (2)	This module is an older fan tray-power supply combination (DevType 5010) with unsplit data. Therefore, the data needs to be separated into fan tray, power supply 1, and power supply 3. The NMS needs to perform slot remapping.
Not Applicable (3)	This module is neither a power supply nor a fan tray module.

The default value of 3 (not applicable) tells the NMS that the module in alarm is neither the fan tray nor a power supply, making the issue moot. A value of 1 (Yes) means that the alarms are split by module, so alarm remapping is not needed. A value of 2 (No) means that the alarms are not split, so remapping is required.

Access: read-write

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.2.1.25

Module Alarm Table

Currently, the alarms in the Module Alarm table and the corresponding traps generated by the alarm (or clear) condition are reported as Major or Minor with respect to severity level. See *Alarm Severity Mappings* (on page 213) for details concerning the alarm severity mappings.

The p2moduleAlarmTable OID is: 1.3.6.1.4.1.1429.1.6.2.2.13.300.5.

Note:

- Alarm thresholds can only be adjusted for type 1, 2 and 7 alarms. (See the **p2almType** below.) The type of alarm is shown in the p2almType field. The p2almLimitAdjust field will be set to "enabled" if the limits can be adjusted, or to "disabled" if they cannot be adjusted.
- The ICIM2 or ICIM2-XD shows the alarm thresholds for all alarm types as read-writable, whether they can be adjusted or not. However, an error will result if the user attempts to change an alarm threshold with non-adjustable limits.

p2module Alarm Table	Entry 1	Entry 2	Entry 3	Entry 4	Entry 5
Instance	6.0.1	6.0.2	6.1.1	6.1.2	6.1.3
index *	1	2	1	2	3
label	FansOk	ChasTemp	Ps1PwrIn	Ps1+24	Ps1+5VDC
Value	1 (fault)	2 (ok)	0 (ok)	2 (ok)	2 (ok)
Type	5	2	5	2	2
Nominal	1	25	1	24.7	5.4
Hysteresis	na	1	na	0.1	0.1
Major Low	na	-40	na	18	3.6
Minor Low	na	-35	na	18.4	3.7
Minor High	na	60	na	25.9	5.9
Major High	na	65	na	26.1	6.1
Limit Adjust	disabled (2)	enabled (1)	disabled (2)	enabled (1)	enabled (1)
Limit Range Lo	na	-32768	na	-3276.8	-3276.8

p2module Alarm Table	Entry 1	Entry 2	Entry 3	Entry 4	Entry 5
Limit Range Hi	na	32767	na	3276.7	3276.7

* The index value for the alarm is actually the third digit of the instance value. The alarm label will always have the same index value for that module. The index value is not a running index for the entire Module Alarm table.

p2almIndex

This object holds one of the indices into the alarm table. Indices include chassis and slot, as well as p2almIndex per alarm type for the module, which form the unique instance into the Module Alarm table.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.5.1.1

p2almLabel

This object holds a string of eight characters or less that describes an alarm characteristic of a module type.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.5.1.2

p2almValue

This object holds the alarm value, which may be a Boolean or Non-Boolean value as appropriate to the alarm type. The table below shows how the meanings of different alarm values vary depending on their class or enumeration (Non-Boolean vs. Boolean).

Class/Enumeration	0	1	2	3	4
Non-Boolean (p2almType 1, 2, 3, 4, 7, 8 - see table under palmType)	Major low	Minor low	OK	Minor high	Major high
Boolean (p2almType 5 or 6)	OK	Fault	na	na	na

Important: Certain alarm values can have very different meanings depending on the type of alarm. For example, for Boolean alarm types (p2almType = 5 or 6), p2almValue = 0 indicates that there is no fault (OK). However, for Non-Boolean alarm types (p2almType = 1, 2, 3, 4, 7, or 8), p2almValue = 0 indicates a major low alarm. See also **p2almType** below for more on alarm types.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.5.1.3

p2almType

This object holds the alarm type. The alarm type is a number from 1 to 8 that identifies three key characteristics of the alarm:

- **Class** - whether the alarm value is Boolean or Non-Boolean. This affects the way that the alarm values are interpreted.
- **Impact** - whether the alarm thresholds are fixed by the module or can be changed by the user. A module alarm is controlled by the module. If a monitored value violates an alarm threshold set by a module, the module may shut down. User alarm thresholds may be configured by the user. However, these alarms will not cause modules to shut down.
- **Threshold Implementation** - whether the threshold for the alarm is an absolute value, or is relative to one or more other control parameters.

The table below identifies the class, impact, and threshold implementation for each possible value of p2almType. Alarm types with user-adjustable thresholds are indicated with an asterisk (*) in the table and paragraphs below.

p2almType	Class	Impact	Threshold Implementation
1 *	Non-Boolean	User	Relative
2 *	Non-Boolean	User	Absolute
3	Non-Boolean	Module	Relative
4	Non-Boolean	Module	Absolute
5	Boolean	User	na
6	Boolean	Module	na
7 *	Non-Boolean	User	Absolute
8	Non-Boolean	Module	Absolute

* Only these alarm thresholds may be changed by a user.

More on Alarm Types

A Major alarm for module alarm types 3, 4, and 6 below may shut down the module or an important feature of it, such as the laser, if a major threshold is violated. User alarms of type 1, 2, 5, and 7 will not shut down the module if a Major threshold (low or high) is exceeded.

- 1 The relative user alarm. The alarm thresholds are interpreted as a positive or negative value relative to the nominal value of the alarmed variable. The alarm thresholds can be adjusted by the operator, but this will not shut down the module.
- 2 The absolute user alarm. The alarm thresholds are interpreted as absolute values of the alarmed variable. The alarm thresholds can be adjusted by the operator, but this will not shut down the module.

- 3 The relative module alarm. The interpretation of thresholds is like type 1, but a Major Alarm will set the module in the safe state. The alarm thresholds are not user-adjustable.
- 4 The absolute module alarm. The interpretation of thresholds is like type 2, but a Major Alarm will set the module in the safe state. The alarm thresholds are not user-adjustable.
- 5 User Boolean alarm. The state 0 means no alarm (OK). The nominal set to 1 (see **p2almNominal** below) means that input signal of 1 causes an alarm. If nominal is 0, input value of 0 causes alarm. This alarm does not set the unit to the safe state. The alarm thresholds are not user-adjustable.
- 6 Module Boolean alarm. The state 0 means no alarm (OK). The nominal set to 1 (see **p2almNominal** below) means that input signal of 1 causes an alarm. If nominal is 0, input value of 0 causes alarm. This alarm will set the unit to the safe state. The alarm thresholds are not user-adjustable.
- 7 The user alarm with complete inhibit. Same as type 2 except that inhibiting this alarm will always put it in the no alarm state. It will not set anything to the safe state, set the alarm LED or relay or pull the attention line low. The alarm thresholds can be adjusted by the operator, but this will not shut down the module.
- 8 The Module alarm with complete inhibit. Same as type 7 except that the limits are not user adjustable. Unlike other module alarms it will not set anything to the safe set when an alarm is triggered. The alarm thresholds are not user-adjustable.

Important: The alarm type and alarm value are inseparably linked, in that the value may only be understood with respect to the type of alarm. (See also **p2almValue** above.)

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.5.1.4

p2almNominal

This object holds the alarm nominal value. To view the current value for a particular module and element, see the Module Monitor table.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.5.1.5

p2almHysteresis

This object defines the hysteresis value for the alarm. The hysteresis value determines how far from the alarm threshold a parameter must change before an alarm condition will clear. The purpose of hysteresis is to prevent the rapid setting and clearing of alarms that otherwise would occur when a parameter makes small fluctuations about the alarm threshold value.

For example, assume that the Minor High limit for chassis temperature is set to 45°C, and the hysteresis value for this alarm parameter is 1°C. When the chassis temperature rises above 45°C, the Minor High alarm occurs. In order for the alarm to clear, the temperature must fall below 44°C, which is the alarm threshold value of 45 minus the hysteresis value of 1.

Likewise, if the chassis temperature had a Minor Low alarm threshold of -20°C and a hysteresis value of 1°C, a Minor Low alarm would occur if the temperature fell below -20°C, but would not clear until the temperature rose above -19°C.

See **Note** at the end of this section for additional information.

Access: read-write

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.5.1.8

p2almMajorLowLimit

This object holds the Major Low alarm threshold value. See **Note** at the end of this section for additional information.

Access: read-write

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.5.1.9

p2almMinorLowLimit

This object holds the Minor Low alarm threshold value. See **Note** at the end of this section for additional information.

Access: read-write

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.5.1.10

p2almMinorHighLimit

This object holds the Minor High alarm threshold value. See **Note** at the end of this section for additional information.

Access: read-write

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.5.1.11

p2almMajorHighLimit

This object holds the Major High alarm threshold value. See **Note** at the end of this section for additional information.

Access: read-write

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.5.1.12

p2almLimitAdjust

The value in this object indicates whether an alarm has adjustable threshold values. It will be set to enabled (1) if adjustable, disabled (2) if non-adjustable. See **Note** at the end of this section for additional information.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.5.1.13

p2almLimitRangeLo

The value in this object is the lower limit for an adjustable alarm threshold.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.5.1.14

p2almLimitRangeHi

The value in this object is the upper limit for an adjustable alarm threshold.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.5.1.15

Note: Alarm thresholds can only be adjusted for type 1, 2 and 7 alarms. The type of alarm is shown in the p2almType field. The p2almLimitAdjust field will be set to "enabled" if the limits can be adjusted, or to "disabled" if they cannot be adjusted.

The ICIM2 or ICIM2-XD treats all modules the same in that the alarm thresholds will be shown as read-writable for all alarm types, whether they can be adjusted or not. An error will result if the user attempts to change an alarm threshold with non-adjustable limits.

Alarm Severity Mappings

All Prisma II and Prisma II XD chassis alarms report to Major or Minor severity levels, as shown in the following tables.

Note: For additional information on alarms, alarm types, and alarm values, see *Module Alarm Table* (on page 208).

Prisma II Chassis - Fan Tray and Power Supplies

Alarm Type	Severity Level
FansOk	Minor
ChasTemp	Major/Minor per threshold settings
Ps1PwrIn	Major
Ps1+24	Major/Minor per threshold settings

Alarm Type	Severity Level
Ps1+5VDC	Major/Minor per threshold settings
Ps1-5VDC	Major/Minor per threshold settings
Ps3PwrIn	Major
Ps3+24	Major/Minor per threshold settings
Ps3+5VDC	Major/Minor per threshold settings
Ps3-5VDC	Major/Minor per threshold settings

Prisma II XD Chassis - Fan Assembly and Power Supplies

Alarm Type	Severity Level
Fan 1_Ok	Major
Fan 2_Ok	Major
Fan 3_Ok	Major
ChasTemp	Major/Minor per threshold settings
ConvAIn	Major
ConvA+24	Major/Minor per threshold settings
ConvA+5	Major/Minor per threshold settings
ConvA-5	Major/Minor per threshold settings
ConvBIn	Major
ConvB+24	Major/Minor per threshold settings
ConvB+5	Major/Minor per threshold settings
ConvB-5	Major/Minor per threshold settings

Current Alarm Table

The Current Alarm table displays the module elements currently in alarm. This table is highly dynamic, and updates with each poll of a module, if needed.

When a module element first goes into alarm, an entry is made in the Current Alarm table and the date and time are recorded. If the alarm changes from Major to Minor or vice versa, the change is acknowledged and the time stamp is adjusted.

If an alarm clears, the entry is removed from the Current Alarm table. If a module is removed from the ICIM2 or ICIM2-XD domain, all of its corresponding alarms are removed from the table.

The indices are chassis, slot, and index, the same as the index into the p2moduleAlarm table associated with this alarmed item.

p2moduleCurrentAlarmTable OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.8

p2moduleCurrentAlarmEntry OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.8.1

The figure below shows how the Current Alarm table might appear when displayed in a MIB browser.

Instance	p2curAlmIndex(IDX)	p2curAlmSeverity	p2curAlmLabel	p2curAlmDescr	p2curAlmTime
1.2.3	3	minor(2)	InRF	Module=HDTx, Model=1020	Wed, 02 Nov 2005 11:55:39 EST
1.3.3	3	minor(2)	InRF	Module=HDTx, Model=1020	Wed, 02 Nov 2005 11:55:40 EST
1.4.3	3	minor(2)	InRF	Module=HDTx, Model=1020	Wed, 02 Nov 2005 11:55:42 EST
1.5.3	3	major(1)	InRF	Module=HDTx, Model=1032	Wed, 02 Nov 2005 11:55:43 EST
1.7.3	3	minor(2)	InRF	Module=HDTx, Model=1032	Wed, 02 Nov 2005 11:55:46 EST
1.8.3	3	minor(2)	InRF	Module=HDTx, Model=1032	Wed, 02 Nov 2005 11:55:47 EST
1.9.3	3	minor(2)	InRF	Module=HDTx, Model=1032	Wed, 02 Nov 2005 11:55:48 EST
1.10.3	3	minor(2)	InRF	Module=HDTx, Model=1032	Wed, 02 Nov 2005 11:55:50 EST
1.11.3	3	minor(2)	InRF	Module=HDTx, Model=1032	Wed, 02 Nov 2005 11:55:51 EST
1.12.3	3	minor(2)	InRF	Module=HDTx, Model=1032	Wed, 02 Nov 2005 11:55:52 EST
1.13.3	3	minor(2)	InRF	Module=HDTx, Model=1032	Wed, 02 Nov 2005 11:55:53 EST
1.14.3	3	minor(2)	InRF	Module=HDTx, Model=1032	Wed, 02 Nov 2005 11:55:55 EST
1.16.3	3	minor(2)	InRF	Module=HDTx, Model=1032	Wed, 02 Nov 2005 11:55:57 EST
2.1.1	1	major(1)	InPwr	Module=P2-HD-RxF, Model=2015	Wed, 02 Nov 2005 11:56:01 EST
2.1.4	4	major(1)	Alarm	Module=P2-HD-RxF, Model=2015	Wed, 02 Nov 2005 11:56:01 EST
2.2.1	1	major(1)	InPwr	Module=P2-HD-RxF, Model=2015	Wed, 02 Nov 2005 11:56:02 EST
2.4.1	1	major(1)	InPwr	Module=P2-HD-RxF, Model=2015	Wed, 02 Nov 2005 11:56:05 EST
2.5.1	1	major(1)	InPwr	Module=P2-HD-RxF, Model=2015	Wed, 02 Nov 2005 11:56:07 EST
2.6.1	1	major(1)	InPwr	Module=P2-HD-RxF, Model=2015	Wed, 02 Nov 2005 11:56:08 EST
2.7.1	1	major(1)	InPwr	Module=P2-HD-RxF, Model=2015	Wed, 02 Nov 2005 11:56:10 EST
2.8.1	1	major(1)	InPwr	Module=P2-HD-RxF, Model=2015	Wed, 02 Nov 2005 11:56:11 EST
2.9.1	1	major(1)	InPwr	Module=P2-HD-RxF, Model=2015	Wed, 02 Nov 2005 11:56:13 EST
2.10.1	1	major(1)	InPwr	Module=P2-HD-RxF, Model=2015	Wed, 02 Nov 2005 11:56:14 EST

TP485

The table below shows sample entries for each element of the Current Alarm table. The elements themselves are described in this section.

Instance	p2curAlmIndex *	p2curAlmSeverity	p2curAlmLabel	p2curAlmDescr	p2curAlmTime
1.2.3	3	minor (2)	InRF	Module=HDTx, Model=1032	Wed, 02 Nov 2005 11:55:39 EST
1.3.3	3	minor (2)	InRF	Module=HDTx, Model=1032	Wed, 02 Nov 2005 11:55:40 EST
1.4.3	3	minor (2)	InRF	Module=HDTx, Model=1032	Wed, 02 Nov 2005 11:55:42 EST
1.5.3	3	major (1)	InRF	Module=HDTx, Model=1032	Wed, 02 Nov 2005 11:55:43 EST
1.7.3	3	minor (2)	InRF	Module=HDTx, Model=1032	Wed, 02 Nov 2005 11:55:46 EST
1.8.3	3	minor (2)	InRF	Module=HDTx, Model=1032	Wed, 02 Nov 2005 11:55:47 EST
1.9.3	3	minor (2)	InRF	Module=HDTx, Model=1032	Wed, 02 Nov 2005 11:55:48 EST
1.10.3	3	minor (2)	InRF	Module=HDTx, Model=1032	Wed, 02 Nov 2005 11:55:50 EST
1.11.3	3	minor (2)	InRF	Module=HDTx, Model=1032	Wed, 02 Nov 2005 11:55:51 EST
1.12.3	3	minor (2)	InRF	Module=HDTx, Model=1032	Wed, 02 Nov 2005 11:55:52 EST
1.13.3	3	minor (2)	InRF	Module=HDTx, Model=1032	Wed, 02 Nov 2005 11:55:53 EST

Instance	p2curAlm Index *	p2curAlm Severity	p2curAlm Label	p2curAlmDescr	p2curAlmTime
1.14.3	3	minor (2)	InRF	Module=HDTx, Model=1032	Wed, 02 Nov 2005 11:55:55 EST
1.16.3	3	minor (2)	InRF	Module=HDTx, Model=1032	Wed, 02 Nov 2005 11:56:57 EST
2.1.1	1	minor (2)	InPwr	Module=P2-HD- RXF, Model=2015	Wed, 02 Nov 2005 11:56:01 EST

* The index value for the alarm is actually the third digit of the instance value. The alarm label will always have the same index value for that module. The index value is not a running index for the entire Current Alarm table.

p2curAlmIndex

The value in this object is the index into the p2moduleAlarm table for this object in alarm. It is one of three indices into the Current Alarm table, along with p2chassisID and p2slotID.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.8.1.1

p2curAlmSeverity

The value in this object represents the current level of severity for the alarm shows here. The alarm may be Major (1) or Minor (2).

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.8.1.2

p2curAlmLabel

The value in this object represents the label assigned to the alarm, which corresponds to the p2almLabel.

Example: Fan1_Ok

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.8.1.3

p2curAlmDescr

This object holds the alarm description, which is a concatenation of the module name and the model number in text form. It is exactly the same as p2TrapLogText, sent by the Enhanced traps and logged in the Trap Log table.

Example: Module=HDTx, Model=1032

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.8.1.4

p2curAlmTime

This object shows the time that the alarm was first recorded in the Current Alarm table, or the time that the severity level last changed from Major to Minor or vice versa.

Format Example: Wed, 02 Nov 2005 11:56:50 EST

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.8.1.5

Module Monitor Table

The Module Monitor table shows the actual values of module elements. Values may only be updated via a module in response to requests from the ICIM2 or ICIM2-XD.

As with the Module Control table and the Module Alarm table, the Module Monitor table is indexed by the chassis and slot number of a particular module. The third index into the table is represented by the p2monitor Index value.

The OID of p2moduleMonitorTable is: 1.3.6.1.4.1.1429.1.6.2.2.13.300.7.

Rows may be accessed via p2moduleMonitorEntry OID:

1.3.6.1.4.1.1429.1.6.2.2.13.300.7.1.

The figure below shows how the Current Monitor table might appear when displayed in a MIB browser.

Instance	p2monitorIndex(IDX)	p2monitorLabel	p2monitorValue	p2monitorUnit	p2monitorType	p2monitorStateNames
1.0.1	1	ConvA+24	24.1499	V	F	N/A
1.0.2	2	ConvA+5	5.28269	V	F	N/A
1.0.3	3	ConvA-5	-5.26423	V	F	N/A
1.0.4	4	ConvB+24	24.0095	V	F	N/A
1.0.5	5	ConvB+5	5.27484	V	F	N/A
1.0.6	6	ConvB-5	-5.2905	V	F	N/A
1.0.7	7	PSA_Inst	1	N/A	S	(0) No, (1) Yes
1.0.8	8	PSB_Inst	1	N/A	S	(0) No, (1) Yes
1.0.9	9	ConvAlns	1	N/A	S	(0) No, (1) Yes
1.0.10	10	ConvBlns	1	N/A	S	(0) No, (1) Yes
1.0.11	11	Chas+24V	24.1177	V	F	N/A
1.0.12	12	Chas+5V	5.0277	V	F	N/A
1.0.13	13	Chas-5V	-4.93157	V	F	N/A
1.0.14	14	ChasTemp	26.75	degC	F	N/A
1.1.1	1	OutPwr	2.97	dBm	F	N/A
1.1.2	2	LasBias	72	mA	F	N/A
1.1.3	3	InRF	2.18	dB	F	N/A
1.1.4	4	ModTemp	31.28	degC	F	N/A
1.1.5	5	TecCur	29.4	mA	F	N/A
1.1.6	6	LasTemp	36.2	degC	F	N/A
1.1.7	7	LasRF	1.91	dB	F	N/A
1.2.1	1	OutPwr	3.2	dBm	F	N/A
1.2.2	2	LasBias	45.0147	mA	F	N/A

The table below shows sample entries for each element of the Current Alarm table. The elements themselves are described in this section.

Instance	Index *	Label	Value	Unit	Type	StateName
1.0.1	1	Conv+24	24.1499	V	F	N/A

Instance	Index *	Label	Value	Unit	Type	StateName
1.0.2	2	ConvA+5	5.28269	V	F	N/A
1.0.3	3	ConvA-5	-5.26423	V	F	N/A
1.0.4	4	ConvB+24	24.0095	V	F	N/A
1.0.5	5	ConvB+5	5.27484	V	F	N/A
1.0.6	6	ConvB-5	-5.2905	N/A	F	N/A
1.0.7	7	PSA_Inst	1	N/A	S	(0) No, (1) Yes
1.0.8	8	PSB_Inst	1	N/A	S	(0) No, (1) Yes
1.0.9	9	ConvAIns	1	N/A	S	(0) No, (1) Yes
1.0.10	10	ConvBIns	1	N/A	S	(0) No, (1) Yes
1.0.11	11	Chas+24V	24.1177	V	F	N/A
1.0.12	12	Chas+5V	5.0277	V	F	N/A
1.0.13	13	Chas-5V	-4.93157	V	F	N/A
1.0.14	14	ChasTemp	26.75	degC	F	N/A
1.1.1	1	OutPwr	2.97	dBm	F	N/A
1.1.2	2	LasBias	72	mA	F	N/A

* The index value for the alarm is actually the third digit of the instance value. The monitor label will always have the same index value for that module. The index value is not a running index for the entire Module Monitor table.

p2monitorIndex

The value in this object is the third index into the Module Monitor table.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.7.1.1

p2monitorLabel

This object holds a short description, eight characters or less, of the monitored variable found in the string associated with p2monitorLabel.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.7.1.2

p2monitorValue

This object holds the monitor value, which is the actual value given by a module for the monitored variable.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.7.1.3

p2monitorUnit

This object indicates the units assigned to the value appearing in p2monitorValue. The table below summarizes the common units used by monitored values and controls.

Unit	Meaning
A	amperes
dB	decibels (10log10)
dBm	decibels relative to 1 mW (0.0 dBm is 1.0 mW)
degC	degrees in Centigrade
hrs	hours
Inst	installed
mA	milliamperes
%	percentage
sec	seconds

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.7.1.4

p2monitorType

This object indicates the monitor data type, represented with one of the following letters:

Unit	Meaning
F	floating point value
D	digital, integer value
B	Boolean, 0 or 1
L	long, a floating point value converted to 8 ASCII Hex digits
S	state with enumerated list of state names (up to 8 characters each)

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.7.1.5

p2monitorStateNames

If the element is a state variable, this object lists all the state names for the element.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.7.1.6

Module Control Table

The Module Control table contains control information for every module in the ICIM2 or ICIM2-XD domain that has control variables.

Like the Alarm table and Monitor table, the Control table has three indices:

- Chassis number
- Slot number
- Individual index, which varies per module by control type

Collectively, these indices make up the instance into the table.

p2ModuleControlTable OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.6

p2ModuleControlEntry OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.6.1

The figure below shows how the Module Control table might appear when displayed in a MIB browser.

Insta...	p2cntrlIndex(IDX)	p2cntrlLabel	p2cntrlValue	p2cntrlUnit	p2cntrlType	p2cntrlRangeLo	p2cntrlRangeHi	p2cntrlRangeStep	p2cntrlStateNames
1.0.1	1	AlmMuteA	0	N/A	S	0	1	1	(0) Off, (1) On
1.0.2	2	AlmMuteB	0	N/A	S	0	1	1	(0) Off, (1) On
1.1.1	1	Enable	1	N/A	B	0	1	1	N/A
1.1.2	2	CwMode	0	N/A	B	0	1	1	N/A
1.1.3	3	LoRFInh	0	N/A	B	0	1	1	N/A
1.1.4	4	Master	1	N/A	S	0	1	1	(0) Slave, (1) Master
1.1.5	5	RFDriVe	0	dB	F	-1.5	1.5	0.5	N/A
1.1.6	6	AGC	0	N/A	B	0	1	1	N/A
1.2.1	1	Enable	1	N/A	B	0	1	1	N/A
1.2.2	2	CwMode	0	N/A	B	0	1	1	N/A
1.2.3	3	LoRFInh	0	N/A	B	0	1	1	N/A
1.2.4	4	Master	1	N/A	S	0	1	1	(0) Slave, (1) Master
1.2.5	5	RFDriVe	0	dB	F	-5	5	0.5	N/A
1.2.6	6	AGC	0	N/A	B	0	1	1	N/A
1.3.1	1	Enable	1	N/A	B	0	1	1	N/A
1.3.2	2	CwMode	0	N/A	B	0	1	1	N/A
1.3.3	3	LoRFInh	0	N/A	B	0	1	1	N/A
1.3.4	4	Master	1	N/A	S	0	1	1	(0) Slave, (1) Master
1.3.5	5	RFDriVe	0	dB	F	-5	5	0.5	N/A
1.3.6	6	AGC	0	N/A	B	0	1	1	N/A
1.4.1	1	Enable	1	N/A	B	0	1	1	N/A
1.4.2	2	CwMode	0	N/A	B	0	1	1	N/A
1.4.3	3	LoRFInh	0	N/A	B	0	1	1	N/A
1.4.4	4	Master	1	N/A	S	0	1	1	(0) Slave, (1) Master

TP484

The table below shows sample entries for each element of the Module Control table. The elements themselves are described in this section.

Instance	Index *	Label	Value	Unit	Type	Range Low	Range High	Range Step	StateNames
1.0.1	1	AlmMuteA	0	N/A	S	0	1	1	(0) Off, (1) On
1.0.2	2	AlmMuteB	0	N/A	S	0	1	1	(0) Off, (1) On
1.1.1	1	Enable	1	N/A	B	0	1	1	N/A
1.1.2	2	CwMode	0	N/A	B	0	1	1	N/A
1.1.3	3	LoRFInh	0	N/A	B	0	1	1	N/A
1.1.4	4	Master	1	N/A	S	0	1	1	(0) Slave, (1) Master

Instance	Index *	Label	Value	Unit	Type	Range Low	Range High	Range Step	StateNames
1.1.5	5	RFDriVe	0	dB	F	-1.5	1.5	0.5	N/A
1.1.6	6	AGC	0	N/A	B	0	1	1	N/A
1.2.1	1	Enable	1	N/A	B	0	1	1	N/A
1.2.2	2	CwMode	0	N/A	B	0	1	1	N/A

* The index value for the alarm is actually the third digit of the instance value. The alarm label will always have the same index value for that module. The index value is not a running index for the entire Module Control table.

p2cntrlIndex

The value in this object is one index into the Module Control table is the p2cntrlIndex. It is the third index; chassis and slot are the first and second indices to this table.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.6.1.1

p2cntrlLabel

This object holds a short description of the control, represented as a string of not more than eight characters. The description varies by module and its controls.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.6.1.2

p2cntrlValue

The value in this object may be changed by the user to control an aspect of the module.

Access: read-write

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.6.1.3

p2cntrlUnit

This object indicates the units assigned to the values appearing in p2cntrlValue. The table below summarizes the common units used by monitored values and controls.

Unit	Meaning
A	amperes
dB	decibels (10log10)
dBm	decibels relative to 1 mW (0.0 dBm is 1.0 mW)
degC	degrees in Centigrade
hrs	hours

Unit	Meaning
Inst	installed
mA	milliamperes
%	percentage
sec	seconds

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.6.1.4

p2cntrlType

The value in this object represents the data type of the control variable:

Unit	Meaning
F	floating point value
D	digital, integer value
B	Boolean, 0 or 1
S	state with enumerated list of state names (up to 8 characters each)

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.6.1.5

p2cntrlRangeLo

The value in this object is the lower limit for the control.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.6.1.6

p2cntrlRangeHi

The value in this object is the upper limit for the control.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.6.1.7

p2cntrlRangeStep

The value in this object is the range step (smallest allowable increment) for the control.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.6.1.8

p2cntrlStateNames

If the control is a state variable, this object will list the state names for the control.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.6.1.9

Insert Module Table

If a module is inserted into the chassis following the initial polling of the ICIM2 or ICIM2-XD, the module chassis and slot appear in the Insert Module table. The table is indexed sequentially by occurrence.

p2InsertModuleTable OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.3

p2InsertModuleEntry OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.3.1

p2InsertModuleIndex

The value in this object is the index into the Insert Module table, which is sequential with respect to time.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.3.1.1

p2InsertModuleChassisID

The value in this object represents the number of the chassis in which the module is installed.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.3.1.2

p2InsertModuleSlotID

The value in this object represents the number of the slot in which the module is installed.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.3.1.3

Remove Module Table

If a module is removed from a slot, some data concerning the module appears in the Remove Module table. Information captured in this table allows managers to determine if the removed module was replaced by a module of the same type. This table is indexed sequentially based on occurrence.

As with other tables for the module, the rows in this table may be accessed via the `p2RemoveModuleEntry`.

`p2RemoveModuleTable` OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.4

`p2IRemoveModuleEntry` OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.4.1

p2RemoveModuleIndex

The value in this object represents the index into the Remove Module table, which is sequential with respect to time.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.4.1.1

p2RemoveModuleChassisID

The value in this object represents the number of the chassis in which the module had been installed.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.4.1.2

p2RemoveModuleSlotID

The value in this object represents the number of the slot in which the module had been installed.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.4.1.3

p2RemoveModuleName

The value in this object represents the name assigned to this module type during the manufacturing process.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.4.1.4

p2RemoveModuleType

The value in this object represents the number assigned during the manufacturing process to uniquely identify this type of module. This is also referred to as the Devtype or TNCS type number.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.4.1.5

p2RemoveModuleSerialNum

The value in this object designates the serial number of the removed module.

Access: read-only

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.300.4.1.6

Remote Reboot of ICIM2 and Modules

You can boot the ICIM2, ICIM2-XD, and associated application modules remotely using a series of SNMP commands. The modules may be rebooted using a hard reboot (service interrupting) or a soft reboot (non-service interrupting). The ICIM2 or ICIM2-XD always performs a hard reboot (non-service interrupting) in response to either a soft reboot or hard reboot command.

To Reboot the ICIM2 via SNMP

Complete the following steps to reset the ICIM2 or ICIM2-XD via SNMP.

- 1 Set p2icimDownLdTgt to "ccss," where **cc** is the chassis number and **ss** is the slot number.
- 2 Set p2icimDownLdCmd to "9" (reboot enable).
- 3 Set p2icimDownLdCmd to "7" or "8" (7 for soft reboot, 8 for hard reboot).

Note:

- For the ICIM2 or ICIM2-XD, the soft reboot and the hard reboot is the same.
- An ICIM2 or ICIM2-XD reboot clears the module database in the ICIM2 or ICIM2-XD and requires rediscovery of the domain to update the module status. Discovery times may be as long as five minutes, depending on the system size and configuration.

To Reboot a Module via SNMP

Complete the following steps to reset an application module via SNMP.

- 1 Set p2icimDownLdTgt to "ccss," where **cc** is the chassis number and **ss** is the slot number.
- 2 Set p2icimDownLdCmd to "9" (reboot enable).
- 3 Set p2icimDownLdCmd to "7" or "8" (7 for soft reboot, 8 for hard reboot).

Note: A module soft reboot will not interrupt service to the end customer, but a hard reboot may cause a brief disruption of service.

Prisma II Traps

This section describes trap destination configuration and provides details on trap types, conditions causing traps, and trap logging.

About Traps

The Prisma II system can be configured to provide various alarm and warning conditions, called *traps*, to an element management system or system monitor application. Up to eight different traps can be enabled independently to provide information on events occurring in a system:

- IP Change
- Module Insertion
- Module Removal
- Alarm Event
- Download Complete
- Self-Test
- Reboot
- Enhanced Alarm

These traps can be sent to up to ten different IP addresses, or "users." Trap filtering can be configured independently for each user.

Each trap is accompanied by one or more *bindings*, which are parameters representing the physical or logical objects associated with the trap.

The following table briefly describes each of the traps listed above and identifies its associated bindings.

Trap	Description	Binding
IP Change Trap	An informational event indicating when the ICIM2 or ICIM2-XD IP address has been changed.	1. Previous IP address
Module Insertion Trap	An informational event indicating that a module has been inserted into a chassis.	1. Chassis ID 2. Slot ID
Module Removal Trap	An informational event indicating that a module has been removed from a chassis.	1. Chassis ID 2. Slot ID

Trap	Description	Binding
Alarm Event Trap	An informational event indicating that an alarm has changed state on a module.	1. Chassis ID 2. Slot ID 3. Alarm Table Index 4. Alarm Label (Description)
Download Complete Trap	An informational event indicating that new application software has been downloaded to a module.	1. Chassis ID 2. Slot ID
Reboot Command Trap	An informational event indicating that a module has been commanded to reboot (hard or soft).	1. Chassis ID 2. Slot ID
Self-Test Trap	An alarm indicating that a module has failed its power-on self test.	1. Chassis ID 2. Slot ID
Enhanced Alarm Trap	An event indicating that an alarm has changed state or an event has occurred with a module. This trap includes additional bindings to indicate CLLI and CLEI codes for telecommunications equipment.	1. Trap Sequence Number 2. Severity 3. State 4. Description 5. OID 6. Module Name and type 7. Chassis ID 8. Slot ID 9. CLLI code 10. CLEI code 11. TimeStamp 12. Date Time Zone 13. Value 14. Unit 15. Description

Note: All trap types (module insertion, alarm events, etc.) are reported through the Enhanced Alarm trap. By default, only the Enhanced Alarm traps are enabled.

Trap Receiving Configuration

Trap receiving is configured in the p2TrapRecvTable.

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.200.8

A sample view of this table is provided below.

Object	RX Trap	RX Trap	RX Trap	RX Trap	Example (same as RX Trap #3)					
p2TrapRecvIndex	0	1	2	3	4	5	6	7	8	9
p2TrapRecvEnable	enabled (2)	disabled (1)	disabled (1)	disabled (1)	1	1	1	1	1	1
p2TrapRecvAddr	172.24.28.66	172.24.28.94	0.0.0.0	0.0.0.0	0	0	0	0	0	0
p2TrapRecvIPChange	disabled (1)	disabled (1)	disabled (1)	disabled (1)	1	1	1	1	1	1
p2TrapRecvModuleInsert	disabled (1)	disabled (1)	disabled (1)	disabled (1)	1	1	1	1	1	1
p2TrapRecvModuleRemove	disabled (1)	disabled (1)	disabled (1)	disabled (1)	1	1	1	1	1	1
p2TrapRecvMinorAlarm	never (1)	never (1)	never (1)	never (1)	1	1	1	1	1	1
p2TrapRecvMajorAlarm	never (1)	never (1)	never (1)	never (1)	1	1	1	1	1	1
p2TrapRecvDwnLdComplete	disabled (1)	disabled (1)	disabled (1)	disabled (1)	1	1	1	1	1	1
p2TrapRecvRebootCommand	disabled (1)	disabled (1)	disabled (1)	disabled (1)	1	1	1	1	1	1
p2TrapRecvSelfTest	disabled (1)	disabled (1)	disabled (1)	disabled (1)	1	1	1	1	1	1
p2TrapRecvTelcoAlarm	enabled (2)	enabled (2)	enabled (2)	enabled (2)	2	2	2	2	2	2

As shown in the table, the traps can be filtered for each of the 10 trap receiving addresses. It is important to note that if p2TrapRecvEnable is set to "disabled," no enterprise specific traps will be sent to that IP address even if the individual filters are enabled.

The recommended (and default) trap configuration is to only enable p2TrapRecvTelcoAlarm traps. The other traps are also reported through this trap type. Enabling p2TrapRecvTelcoAlarms along with other trap types will result in duplicate traps for a single alarm event. The trap type filtering remains in place in order to support legacy systems.

To Configure Trap Destination

By setting the objects in the Trap Recv table, you can enable traps to be sent to up to 10 different IP addresses. The index into the table represents one of 10 rows, designated 0 to 9.

Complete the following steps to receive traps.

- 1 Set p2TrapRecvEnable to enabled (2), which allows traps to be sent to the IP address on the same row.
- 2 Set the IP address of the remote entity to receive traps. Use the format 172.18.2.24.
- 3 Set p2TrapRecvTelcoAlarm to enabled (2).

The table below shows how these settings might appear in a MIB browser after enabling IP address 192.0.2.102 to receive Enhanced traps only.

Instance	p2TrapRecvIndex[IDX]	p2TrapRecvEnable	p2TrapRecvAddr	p2TrapRecvIPC	ommand	p2TrapRecvSelfTest	p2TrapRecvTelcoAlarm
0	0	enabled(2)	172.18.50.42	enabled(2)		disabled(1)	enabled(2)
1	1	enabled(2)	172.18.50.3	enabled(2)		disabled(1)	enabled(2)
2	2	enabled(2)	172.18.50.6	enabled(2)		disabled(1)	enabled(2)
3	3	disabled(1)	0.0.0.0	disabled(1)		disabled(1)	enabled(2)
4	4	disabled(1)	0.0.0.0	disabled(1)		disabled(1)	enabled(2)
5	5	disabled(1)	0.0.0.0	disabled(1)		disabled(1)	enabled(2)
6	6	disabled(1)	0.0.0.0	disabled(1)		disabled(1)	enabled(2)
7	7	disabled(1)	0.0.0.0	disabled(1)		disabled(1)	enabled(2)
8	8	disabled(1)	0.0.0.0	disabled(1)		disabled(1)	enabled(2)
9	9	disabled(1)	0.0.0.0	disabled(1)		disabled(1)	enabled(2)

TP490

Note: All trap settings are documented for completeness only. Information contained in other proprietary traps is expanded upon in the Enhanced traps. We do not recommend using the older (legacy) traps, as the new Enhanced Trap is more useful. Enabling other traps together with the Enhanced Trap will cause two traps to be sent for each event. For more information, see *Trap Recv Table* (on page 190).

Trap Types

As indicated in the p2TrapRecvTable, there are several types of proprietary traps. All proprietary traps are documented for completeness only. Information contained in other traps is expanded upon in the Enhanced trap. In general, it is best to avoid using older traps as the new Enhanced trap is more useful. Enabling other traps together with the Enhanced trap will cause two traps to be sent for each of these events. For more information, see *Trap Recv Table* (on page 190).

Most traps have two sections: the header and the bindings. The headers are essentially the same from one trap to another. The table shown below describes each data element contained in the trap header. The first field, indicated by the label "Specific:" is important as it identifies which trap has been received.

Trap Header

The table below explains and provides an example of each trap header label.

Label	Example	Description
Specific	8	Type of trap sent (8 = SelfTest).
Message reception date	1/18/2006	Date trap received remotely.
Message reception time	11:31:24.550 AM	Time trap received remotely.
Time stamp	3 days 00h:02m:04s.00th	ICIM2 or ICIM2-XD up time since last reboot.
Message type	Trap (v1)	Trap via SNMP version 1.
Protocol version	SNMPv1	SNMP version 1.

Label	Example	Description
Transport	IP/UDP	Transport protocol used.
Agent		
Address	172.24.28.168	IP address of the ICIM2 or ICIM2-XD.
Port	162	ICIM2 or ICIM2-XD port.
Manager		
Address	172.18.43.3	Remote IP address.
Port	162	Remote port.
Community	prismatrap	SNMP trap community.
SNMPv1 agent address	172.24.28.168	IP address of the ICIM2 or ICIM2-XD.
Enterprise	p2trapEvents	MIB associated with overall trap generation.
Bindings (2)	2	Number of bindings to follow.

The number following the word Specific indicates the type of trap sent. The possible values and meanings of this number are as follows:

Unit	Meaning
2	Insert Module
3	Remove Module
4	Alarm (Major or Minor, Alarm or Clear)
5	IP Change Event
6	Download Complete (reserved for future use)
7	Reboot Command
8	SelfTest Failure
9	Telco Alarm

At least one binding follows the header. The Enhanced traps include 15 bindings carrying information regarding the entity that caused the trap to be sent. For more information on Enhanced traps, see *Enhanced Trap Binding Information* (on page 241).

Other proprietary traps send very basic data, such as the chassis and slot of the ICIM2, ICIM2-XD, or application module.

Trap Binding Example

The table below explains and provides an example of trap bindings.

Binding	MIB Name (Examples)	Explanation
1: ChassisID	p2chassisID	Chassis where the ICIM2, ICIM2-XD, or application module is installed.
2: SlotID	p2slotID	Slot where the ICIM2, ICIM2-XD, or application module is installed.
3: Self-Test data	p2moduleSelfTest	SelfTest Failed - Error code value.

IP Change Trap (Specific: 5)

This trap is sent when an ICIM2 or ICIM2-XD IP address is changed through the CLI. If p2TrapRecvIPChange is set to enabled (2), a trap containing the previous IP will be sent. The new IP address will take effect on the next ICIM2 or ICIM2-XD reboot.

Note: Documentation on this trap is included for completeness. All information in this trap is contained in and expanded upon in the Enhanced trap. We recommend using the Enhanced trap instead of this trap, as the Enhanced trap is more useful. Enabling this trap together with the Enhanced trap will cause two traps to be sent for each triggering event.

Specific: 5 appears in the heading to indicate that this is an IP Change trap. The table below describes the binding.

Binding	MIB Name (Examples)	Explanation
1: PreviousIP	p2PreviousIP	The IP address previously given to the ICIM2 or ICIM2-XD before a new IP address was assigned. The new IP address takes effect upon the next ICIM2 or ICIM2-XD reboot.

IP Change Trap Example

```
Specific: 5
Message reception date: 1/31/2006
Message reception time: 1:19:58.793 PM
Time stamp: 3 days 00h:25m:57s.00th
Message type: Trap (v1)
Protocol version: SNMPv1
Transport: IP/UDP
Agent
  Address: 172.24.28.168
  Port: 1051
Manager
  Address: 172.18.4.23
  Port: 162
Community: prismatrap
SNMPv1 agent address: 172.24.28.168
Enterprise: p2trapEvents
Bindings (1)
  Binding #1: p2PreviousIP.0 (ipaddr) 172.24.28.168
```

Module Insert Trap (Specific: 2)

This trap is sent as soon as the ICIM2 or ICIM2-XD discovers that a module has been inserted. If p2TrapRecvModuleInsert is enabled (2), a trap containing the chassis and slot of the new module is sent. A number appears in the heading indicating that this is a module insert trap.

Note: Documentation on this trap is included for completeness. All information in this trap is contained in and expanded upon in the Enhanced trap. We recommend using the Enhanced trap instead of this trap, as the Enhanced trap is more useful. Enabling this trap together with the Enhanced trap will cause two traps to be sent for each triggering event.

Specific: 2 appears in the heading to indicate that this is an InsertRemove trap. The table below describes the bindings.

Binding	MIB Name (Examples)	Explanation
1: ChassisID	p2InsertModuleChassisID	Chassis where the module is installed.
2: SlotID	p2InsertModuleSlotID	Slot where the module is installed.

Module Insert Trap Example

```
Specific: 2
Message reception date: 1/31/2006
Message reception time: 1:24:47.626 PM
Time stamp: 3 days 00h:30m:46s.00th
Message type: Trap (v1)
Protocol version: SNMPv1
Transport: IP/UDP
Agent
  Address: 172.24.28.168
  Port: 1055
Manager
  Address: 172.18.4.28
  Port: 162
Community: prismatrap
SNMPv1 agent address: 172.24.28.168
Enterprise: p2trapEvents
Bindings (2)
  Binding #1: p2InsertModuleChassisID.1 (int32) 2
  Binding #2: p2InsertModuleSlotID.1 (int32) 13
```

Module Remove Trap (Specific: 3)

This trap is sent when the ICIM2 or ICIM2-XD discovers that a module has been removed from the chassis. If p2TrapReceiveModuleRemove is enabled (2), a trap with the chassis and slot where the removed module had been installed will be sent.

Note: Documentation on this trap is included for completeness. All information in this trap is contained in and expanded upon in the Enhanced trap. We recommend using the Enhanced trap instead of this trap, as the Enhanced trap is more useful. Enabling this trap together with the Enhanced trap will cause two traps to be sent for each triggering event.

Specific: 3 appears in the heading to indicate that this is a ModuleRemove trap. The table below describes the bindings.

Binding	MIB Name (Examples)	Explanation
1: ChassisID	p2RemoveModuleChassisID	Chassis where the module was formerly installed.
2: SlotID	p2RemoveModuleSlotID	Slot where the module was formerly installed.

Module Remove Trap Example

```

Specific: 3
  Message reception date: 1/31/2006
  Message reception time: 1:27:35.778 PM
  Time stamp: 3 days 00h:33m:35s.00th
  Message type: Trap (v1)
  Protocol version: SNMPv1
  Transport: IP/UDP
  Agent
    Address: 172.24.28.168
    Port: 1060
  Manager
    Address: 172.18.4.23
    Port: 162
  Community: prismatrap
  SNMPv1 agent address: 172.24.28.168
  Enterprise: p2trapEvents
  Bindings (2)
    Binding #1: p2RemoveModuleChassisID.1 (int32) 2
    Binding #2: p2RemoveModuleSlotID.1 (int32) 11

```

Alarm Traps (Specific: 4)

Alarm traps are edge triggered, meaning that whenever an alarm changes state, a trap is sent. An alarm changes state when a monitored value exceeds a limit set by an alarm threshold, or when a monitored Boolean parameter value changes from OK to Fault. Both of these events will generate alarms.

Alarms may trigger Major or Minor alarm traps, depending on the type of alarm limit that was exceeded. A Major alarm trap is sent when the monitored value exceeds the Major High or a Major Low alarm threshold. A Minor alarm trap is sent when the monitored value exceeds the Minor High or Minor Low alarm threshold.

Major and Minor alarm traps affect the ICIM2 or ICIM2-XD polling cycle in different ways, as follows:

- If an alarm is Minor, the module in alarm sends a trap to the ICIM2 or ICIM2-XD after the next polling interval. Minor alarm handling is integral to the polling process, and does not disrupt the normal polling cycle.
- If an alarm is Major, the module in alarm brings the ICIM2 or ICIM2-XD Attention line low to request immediate service. In response, the ICIM2 or ICIM2-XD first identifies the module requesting attention, and then polls the module to obtain the alarm information. After handling the Major alarm, the ICIM2 or ICIM2-XD resets the polling process, so that it resumes at the beginning of the cycle, rather than at the point in the cycle at which it was interrupted.

To configure alarm traps in the p2TrapRecvTable, select values for p2TrapRecvMajorAlarm or p2TrapRecvMinorAlarm. If traps are to be sent when monitored values exceed their Major Low or Major High threshold values, configure p2TrapRecvMajorAlarm. If traps are to be sent when monitored values exceed their Minor Low or Minor High threshold values, set values in p2TrapRecvMinorAlarm.

Note: A monitor value stated in a trap binding is a snapshot in time, and so may not indicate a value consistent with an alarm condition. If in doubt, verify the actual monitor value using the appropriate equipment interfaces.

The user may configure alarm trap behavior by selecting one of four options:

- Never (1), meaning that traps of this type should never be sent
- Clear (2), meaning that traps should be sent only when alarms are cleared
- Set (3), meaning that traps should be sent only when alarms are set
- Always (4), meaning that traps should be sent when alarms are set or cleared

Note: Documentation on this trap is included for completeness. All information in this trap is contained in and expanded upon in the Enhanced trap. We recommend using the Enhanced trap instead of this trap, as the Enhanced trap is more useful. Enabling this trap together with the Enhanced trap will cause two traps to be sent for each triggering event.

Specific: 4 appears in the heading to indicate an Alarm trap. (Specific: 4 as a value indicates a major alarm or clear, or a minor alarm or clear condition.) The table below describes the bindings.

Binding	MIB Name (Examples)	Explanation
1: ChassisID	p2chassisID	Chassis where the module is installed.
2: SlotID	p2slotID	Slot where the module is installed.
3: Index	p2almIndex	The index into the alarm table where more information may be found.
4: Label	p2almLabel	Label for the element that is in the state of alarm, e.g., ConvA+24.

Alarm Trap Example

```

Specific: 4
  Message reception date: 1/31/2006
  Message reception time: 1:31:58.829 PM
  Time stamp: 3 days 00h:37m:58s.00th
  Message type: Trap (v1)
  Protocol version: SNMPv1
  Transport: IP/UDP
  Agent
    Address: 172.24.28.168
    Port: 1074
  Manager
    Address: 172.18.4.23
    Port: 162
  Community: prismatrap
  SNMPv1 agent address: 172.24.28.168
  Enterprise: p2trapEvents
  Bindings (4)
    Binding #1: p2chassisID.2.3 (int32) 2
    Binding #2: p2slotID.2.3 (int32) 3
    Binding #3: p2almIndex.2.3.4 (int32) 4
    Binding #4: p2almLabel.2.3.4 (octets) Psl+24

```

Download Complete Trap (Specific: 6)

When a download to the ICIM2, ICIM2-XD, or application module completes, a trap is sent. To enable this trap type, set p2TrapRecvDwnLdComplete to enabled (2).

Note: Documentation on this trap is included for completeness. All information in this trap is contained in and expanded upon in the Enhanced trap. We recommend using the Enhanced trap instead of this trap, as the Enhanced trap is more useful. Enabling this trap together with the Enhanced trap will cause two traps to be sent for each triggering event.

Specific: 6 appears in the heading to indicate a RebootCommand trap. The table below describes the bindings.

Binding	MIB Name (Examples)	Explanation
1: ChassisID	p2chassisID	Chassis where the ICIM2, ICIM2-XD, or application module is installed.
2: SlotID	p2slotID	Slot where the ICIM2, ICIM2-XD, or application module is installed.

Download Complete Trap Example

```

Specific: 6
  Message reception date: 1/31/2006
  Message reception time: 1:45:19.299 PM
  Time stamp: 3 days 00h:51m:21s.00th
  Message type: Trap (v1)
  Protocol version: SNMPv1
  Transport: IP/UDP
  Agent
    Address: 172.24.28.168
    Port: 1141
  Manager
    Address: 172.18.4.23
    Port: 162
  Community: prismatrap
  SNMPv1 agent address: 172.24.28.168
  Enterprise: p2trapEvents
  Bindings (2)
    Binding #1: p2chassisID.2 (int32) 2
    Binding #2: p2slotID.2 (int32) 3

```

Reboot Command Trap (Specific: 7)

When the ICIM2, ICIM2-XD, or application module receives the command to reboot, a trap is generated. If this reboot command is generated via the SOUP application, a broadcast reboot is sent out. In this case, only one trap may be generated for the ICIM2 or ICIM2-XD and all modules under its management. To configure the reboot command trap to be sent, set p2TrapRecvRebootCommand to enabled (2).

Note: Documentation on this trap is included for completeness. All information in this trap is contained in and expanded upon in the Enhanced trap. We recommend using the Enhanced trap instead of this trap, as the Enhanced trap is more useful. Enabling this trap together with the Enhanced trap will cause two traps to be sent for each triggering event.

Specific: 7 appears in the heading to indicate a RebootCommand trap. The table below describes the bindings.

Binding	MIB Name (Examples)	Explanation
1: ChassisID	p2chassisID	Chassis where the ICIM2, ICIM2-XD, or application module is installed.
2: SlotID	p2slotID	Slot where the ICIM2, ICIM2-XD, or application module is installed.

The example below shows the bindings for a broadcast RebootCommand trap. Chassis 99 and slot 99 indicate that the reboot command was broadcast to all modules.

Reboot Command Trap Example

```

Specific: 7
  Message reception date: 1/31/2006
  Message reception time: 1:47:14.920 PM
  Time stamp: 3 days 00h:53m:16s.00th
  Message type: Trap (v1)
  Protocol version: SNMPv1
  Transport: IP/UDP
  Agent
    Address: 172.24.28.168
    Port: 1145
  Manager
    Address: 172.18.4.23
    Port: 162
  Community: prismatrap
  SNMPv1 agent address: 172.24.28.168
  Enterprise: p2trapEvents
  Bindings (2)
    Binding #1: p2chassisID.99 (int32) 99
    Binding #2: p2slotID.99 (int32) 99

```

Self-Test Trap (Specific: 8)

This trap is sent if the ICIM2, ICIM2-XD, or application module fails the self-test. The trap contains an error code, which is module specific. See the sections on p2icimSelfTest in *ICIM MIB* (on page 169) and p2moduleSelfTest in *Module MIB* (on page 199) for further discussion of the error codes. To receive the SelfTest traps, set p2TrapRecvSelfTest to enabled (2).

Note: Documentation on this trap is included for completeness. All information in this trap is contained in and expanded upon in the Enhanced trap. We recommend using the Enhanced trap instead of this trap, as the Enhanced trap is more useful. Enabling this trap together with the Enhanced trap will cause two traps to be sent for each triggering event.

Specific: 8 appears in the heading to indicate a SelfTest trap. The table below describes the bindings.

Binding	MIB Name (Examples)	Explanation
1: ChassisID	p2chassisID	Chassis where ICIM2, ICIM2-XD, or application module is installed.
2: SlotID	p2slotID	Slot where the ICIM2, ICIM2-XD, or application module is installed.
3: Self-Test data	p2moduleSelfTest	SelfTest Failed - Error Code value.

Self-Test Trap Example

```

Specific: 8
Message reception date: 1/31/2006
Message reception time: 2:22:20.190 PM
Time stamp: 3 days 00h:00m:20s.00th
Message type: Trap (v1)
Protocol version: SNMPv1
Transport: IP/UDP
Agent
  Address: 172.24.28.168
  Port: 1025
Manager
  Address: 172.18.4.23
  Port: 162
Community: prismatrap
SNMPv1 agent address: 172.24.28.168
Enterprise: p2trapEvents
Bindings (3)
  Binding #1: p2chassisID.2 (int32) 2
  Binding #2: p2slotID.2 (int32) 15
  Binding #3: p2moduleSelfTest.2.15 (octets) SelfTest Failed - Error Code 32.

```

Enhanced Traps (Specific: 9)

The Enhanced traps summarize information for all trap types, with additional data, exclusive of all other traps. Also, if an alarm exists upon startup or module insertion, Enhanced traps will be sent. To configure the Enhanced traps, set p2TrapRecvTelcoAlarm to enabled (2).

Specific: 9 appears in the heading to indicate an Enhanced trap. The table below describes the bindings.

Example of Bindings

Trap Binding	MIB Name (Examples)	Explanation
1 Sequence	p2TrapLogSequence	Tracking number from 1 to 2,147,483,647.
2 Severity	p2TrapLogSeverity	Trap severity level - major (1), minor (2), warning (3).
3 State	p2TrapLogState	State - alarm (1), clear (2), event (3).
4 Label	p2TrapLogLabel or p2almLabel.1.3.4	Event Name or Alarm Label.
5 OID	p2almIndex.1.3 or p2icimStatusMsg	More data regarding the alarm or event is found at this OID.
6 Text	p2TrapLogText	Module name and model number of ICIM2 or ICIM2-XD.
7 ChassisID	p2icimChassisID	Chassis where the ICIM2, ICIM2-XD, or application module is installed.
8 SlotID	p2icimSlotID	Slot where the ICIM2, ICIM2-XD, or application module is installed.
9 CLLIcode	p2icimCLLIcode	Reserved for future use.
10 CLEIcode	p2icimCLEIcode	Reserved for future use.

Trap Binding	MIB Name (Examples)	Explanation
11 Time	p2TrapLogTime	Time trap generated in the format: YYYY-MM-DD, HH:MM:SS.ss
12 DateTime	p2TrapLogDateTime	Date and time generated in the format: DOW, DD MM YYYY HH:MM:SS ZZZ
13 Value	p2TrapLogValue	Monitored value of the object in alarm.
14 Units	p2TrapLogUnit	Monitored units of the value in alarm.
15 Description	p2TrapLogDesc	Verbose description of the alarm or event.

Example

```

Binding #1: p2TrapLogSequence *** (int32) 6
Binding #2: p2TrapLogSeverity *** (int32) major(1)
Binding #3: p2TrapLogState *** (int32) alarm(1)
Binding #4: p2almLabel.0.11.2 *** (octets) OutPwrA
Binding #5: p2almIndex.0.11 *** (int32) 2
Binding #6: p2TrapLogText *** (octets)
  Module=1550nm Post-Amp FTTP,Model=3031
Binding #7: p2chassisID.0.11 *** (int32) 0
Binding #8: p2slotID.0.11 *** (int32) 11
Binding #9: p2moduleCLLIcode.0.11 *** (octets) SCIATL01
Binding #10: p2moduleCLEIcode.0.11 *** (octets) PostAmpCLEI
Binding #11: p2TrapLogTime *** (octets) 2006-8-22,15:45:38.11
Binding #12: p2TrapLogDateTime *** (octets) Tue, 22 Aug 2006 15:45:38 EST
Binding #13: p2TrapLogValue *** (octets) -50
Binding #14: p2TrapLogUnit *** (octets) dBm
Binding #15: p2TrapLogDescr *** (octets)
  Optical output power of bank A exceeds major threshold (1550nm)

```

Trap Generation

Proprietary traps are generated as described above for edge triggered alarms or clear alarms (meaning a change in state of an alarm), as well as for any of the following events:

- Changing the IP address of an ICIM2 or ICIM2-XD
- Inserting or removing a module
- Successful completion of a download
- Reboot of ICIM2, ICIM2-XD, or application module
- Failure of an ICIM2, ICIM2-XD, or application module self-test

Additionally, the Enhanced traps are generated if an alarm condition exists in one of the modules upon startup or module insertion.

Trap Logging

When an Enhanced trap is sent, a copy is also kept in the Trap Logging table. Each trap has a unique sequence number which may be used as the index into the Trap Logging table. All bindings captured in the Enhanced traps are also logged, and may be accessed in the event of network failures between the SNMP manager and the ICIM2 or ICIM2-XD. The log retains up to 1,000 most recent Enhanced traps.

The figure below shows how the Trap Logging table might appear when displayed in a MIB browser.

Instance	p2TrapLogSequenceID	p2TrapLogSeverity	p2TrapLogState	p2TrapLogLabel	p2TrapLogOID	p2TrapLogText	p2TrapLogChassisID	p2TrapLogSlotID	p2TrapLogCLLcode	p2TrapLogCLEcode	p2TrapLogDescr
1	1	minor(2)	alarm(1)	IrRF	p2almindex.1.2.3	Module=HDTx, Model=1020	1	2	N/A	N/A	200
2	2	minor(2)	alarm(1)	IrRF	p2almindex.1.3.3	Module=HDTx, Model=1020	1	3	N/A	N/A	200
3	3	minor(2)	alarm(1)	IrRF	p2almindex.1.4.3	Module=HDTx, Model=1020	1	4	N/A	N/A	200
4	4	major(1)	alarm(1)	IrRF	p2almindex.1.5.3	Module=HDTx, Model=1032	1	5	N/A	N/A	200
5	5	minor(2)	alarm(1)	IrRF	p2almindex.1.7.3	Module=HDTx, Model=1032	1	7	N/A	N/A	200
6	6	minor(2)	alarm(1)	IrRF	p2almindex.1.8.3	Module=HDTx, Model=1032	1	8	N/A	N/A	200
7	7	minor(2)	alarm(1)	IrRF	p2almindex.1.9.3	Module=HDTx, Model=1032	1	9	N/A	N/A	200
8	8	minor(2)	alarm(1)	IrRF	p2almindex.1.10.3	Module=HDTx, Model=1032	1	10	N/A	N/A	200
9	9	minor(2)	alarm(1)	IrRF	p2almindex.1.11.3	Module=HDTx, Model=1032	1	11	N/A	N/A	200
10	10	minor(2)	alarm(1)	IrRF	p2almindex.1.12.3	Module=HDTx, Model=1032	1	12	N/A	N/A	200
11	11	minor(2)	alarm(1)	IrRF	p2almindex.1.13.3	Module=HDTx, Model=1032	1	13	N/A	N/A	200
12	12	minor(2)	alarm(1)	IrRF	p2almindex.1.14.3	Module=HDTx, Model=1032	1	14	N/A	N/A	200
13	13	minor(2)	alarm(1)	IrRF	p2almindex.1.16.3	Module=HDTx, Model=1032	1	16	N/A	N/A	200
14	14	major(1)	alarm(1)	IrPwr	p2almindex.2.1.1	Module=P2HD-RxF, Model=2015	2	1	N/A	N/A	200
15	15	major(1)	alarm(1)	Alarm	p2almindex.2.1.4	Module=P2HD-RxF, Model=2015	2	1	N/A	N/A	200
16	16	major(1)	alarm(1)	IrPwr	p2almindex.2.2.1	Module=P2HD-RxF, Model=2015	2	2	N/A	N/A	200
17	17	major(1)	alarm(1)	Alarm	p2almindex.2.4.1	Module=P2HD-RxF, Model=2015	2	4	N/A	N/A	200
LogText	p2TrapLogChassisID	p2TrapLogSlotID	p2TrapLogCLLcode	p2TrapLogCLEcode	p2TrapLogTime	p2TrapLogDate	p2TrapLogValue	p2TrapLog	p2TrapLogDescr		
HDTx, Model=1020	1	2	N/A	N/A	2007-11-27:10:8:42.75	Tue, 27 Nov 2007 10:08:42 EST	-13.2618	dB	IrRF exceeded minor threshold		
HDTx, Model=1020	1	3	N/A	N/A	2007-11-27:10:8:44.50	Tue, 27 Nov 2007 10:08:44 EST	-13.8482	dB	IrRF exceeded minor threshold		
HDTx, Model=1020	1	4	N/A	N/A	2007-11-27:10:8:45.05	Tue, 27 Nov 2007 10:08:45 EST	-12.9802	dB	IrRF exceeded minor threshold		
HDTx, Model=1032	1	5	N/A	N/A	2007-11-27:10:8:47.20	Tue, 27 Nov 2007 10:08:47 EST	-50	dB	RF input exceeds major threshold		
HDTx, Model=1032	1	7	N/A	N/A	2007-11-27:10:8:49.78	Tue, 27 Nov 2007 10:08:49 EST	-50	dB	RF input exceeds minor threshold		
HDTx, Model=1032	1	8	N/A	N/A	2007-11-27:10:8:51.10	Tue, 27 Nov 2007 10:08:51 EST	-50	dB	RF input exceeds minor threshold		
HDTx, Model=1032	1	9	N/A	N/A	2007-11-27:10:8:52.41	Tue, 27 Nov 2007 10:08:52 EST	-50	dB	RF input exceeds minor threshold		
HDTx, Model=1032	1	10	N/A	N/A	2007-11-27:10:8:53.70	Tue, 27 Nov 2007 10:08:53 EST	-50	dB	RF input exceeds minor threshold		
HDTx, Model=1032	1	11	N/A	N/A	2007-11-27:10:8:55.1	Tue, 27 Nov 2007 10:08:55 EST	-50	dB	RF input exceeds minor threshold		
HDTx, Model=1032	1	12	N/A	N/A	2007-11-27:10:8:56.33	Tue, 27 Nov 2007 10:08:56 EST	-50	dB	RF input exceeds minor threshold		
HDTx, Model=1032	1	13	N/A	N/A	2007-11-27:10:8:57.05	Tue, 27 Nov 2007 10:08:57 EST	-50	dB	RF input exceeds minor threshold		
HDTx, Model=1032	1	14	N/A	N/A	2007-11-27:10:8:58.56	Tue, 27 Nov 2007 10:08:58 EST	-50	dB	RF input exceeds minor threshold		
HDTx, Model=1032	1	16	N/A	N/A	2007-11-27:10:9:1.56	Tue, 27 Nov 2007 10:09:01 EST	-50	dB	RF input exceeds minor threshold		
P2HD-RxF, Model=2015	2	1	N/A	N/A	2007-11-27:10:9:4.75	Tue, 27 Nov 2007 10:09:04 EST	-21.2668	dBm	IrPwr exceeded major threshold		
P2HD-RxF, Model=2015	2	1	N/A	N/A	2007-11-27:10:9:4.76	Tue, 27 Nov 2007 10:09:04 EST	N/A	N/A	Alarm exceeded major threshold		
P2HD-RxF, Model=2015	2	2	N/A	N/A	2007-11-27:10:9:6.30	Tue, 27 Nov 2007 10:09:06 EST	-21.3549	dBm	IrPwr exceeded major threshold		

TP489

Note: At least one row in p2TrapRecvTable must be configured and enabled and p2TrapRecvTelcoAlarm enabled (2) for logging of traps to occur automatically. For details, see *To Configure Trap Destination* (on page 229).

Enhanced Trap Binding Information

The Enhanced trap type was originally added to support the Telco requirement to include a trap sequence number (p2TrapLogSequence) binding. In addition, the Enhanced trap type includes other bindings to convey complete alarm information.

Important: The default and recommended configuration is to enable only the Enhanced trap type. Enabling Enhanced alarm traps and other trap types at the same time may result in duplicate traps being sent to the element management system. These other trap types remain to allow backward compatibility with previously deployed systems.

The table below provides a descriptive listing of the Enhanced trap bindings.

Trap Binding	Description
1 p2TrapLogSequence	A unique number assigned to each trap as it is generated. Serves as an index into the Trap Logging table.
2 p2TrapLogSeverity	The number assigned as a guide to prioritizing trap generating conditions. Severity may be major (1), minor (2), or warning (3).
3 p2TrapLogState	State, along with severity, quickly gives a view into the current state of an entity. State may be alarm (1), clear (2), or event (3).

Trap Binding	Description
4 p2almLabel p2TrapLogLabel	For an alarm or clear trap, the label is the same as the p2almLabel assigned to the condition that caused the trap, e.g. ChasTemp. For events, the type of event that sent the trap is identified as DownloadComplete, RebootCommand, SelfTest, AuthentictnFailed, AdminChange, LogMenuHalfFull, LogMenuFull, LoginThreshold, SNTP, UpdateChassisIDs, or UserLockout.
5 p2almIndex p2InsertModuleEntry p2icimStatusMsg p2RemoveModuleEntry p2ModuleSelfTest p2icimSelfTest p2icimIPAddr	More information regarding the trap may be found at the OID specified in this element. For an alarm or clear trap, this may be the third index into the Module Alarm table. For the download, reboot, or self-test event, this may be the p2icimStatusMessage. However, only the most recent status message is retained by the ICIM2 or ICIM2-XD. If a message generated by another even overwrites the status message, additional information may no longer be available at the OID specified for the particular trap. If an event is logged, event details may be saved in the event log.
6 p2TrapLogText	Display string which further describes the entity or condition responsible for trap generation. This usually is a concatenation of the module name and module number, although it may include the self-test failure code.
7 p2icimChassisID p2chassis	Chassis in which the ICIM2, ICIM2-XD, or application module resides at the time of trap generation.
8 p2icimSlotID p2slotID	Slot number in which the ICIM2, ICIM2-XD, or application module resides at the time of trap generation.
9 p2icimCLLlcode	Reserved for future use.
10 p2icimCLElcode	Reserved for future use.
11 p2TrapLogTime	Date and time stamp indicating when the trap was generated.
12 p2TrapLogDateTime	Full local time displayed in the format: DOW, DD MMM YYYY HH:MM:SS ZZZ Note: The local time zone must be entered in p2icimTimeZone or the default time zone, EST, will show.
13 p2TrapLogValue	Monitored value of the object in alarm.
14 p2TrapLogUnit	Monitored units of the value in alarm.
15 p2TrapLogDescr	Verbose description of the alarm or event.

Trap Sequence Numbering

To observe the most current sequence number used by the Enhanced traps, perform a get operation on this OID. If no traps have been sent, the p2TrapLastSequenceNumber is 0. Valid sequence numbers are 1 through 2,147,483,647. The sequence number resets to 1 with the first trap sent after the ICIM2 or ICIM2-XD boots up, or the p2TrapLogEntry table is cleared with the p2TrapLogClearKey, or with the trap following sequence number 2,147,483,647.

OID: 1.3.6.1.4.1.1429.1.6.2.2.13.200.1

Enhanced Trap Binding Categories

Each trap has a heading and bindings. Generally, Enhanced trap bindings fall into the categories below. However, examples of specific traps follow this general explanation.

Enhanced Trap Header Example

Labels	Example	Explanation
Specific	9	Type of trap sent (9 = Enhanced).
Message reception date	1/18/2006	Date trap was received remotely.
Message reception time	11:31:24.550 AM	Time trap was received remotely.
Time stamp	3 days 00h:02m:04s.00th	ICIM2 or ICIM2-XD up time since last reboot.
Message type	Trap (v1)	Trap via SNMP version 1.
Protocol version	SNMPv1	SNMP version 1.
Transport	IP/UDP	Transport protocol used.
Agent		
Address	172.1.1.2	IP address of the ICIM2 or ICIM2-XD.
Port	1037	ICIM2 or ICIM2-XD port.
Manager		
Address	172.2.2.3	Remote IP address.
Port	162	Remote port.
Community	prismatrap	SNMP trap community.
SNMPv1 agent address	172.1.1.2	IP address of the ICIM2 or ICIM2-XD.
Enterprise	p2trapEvents	MIB associated with overall trap generation.
Bindings (15)	15	Number of bindings to follow.

In the heading of a trap, the type of trap is indicated after the first word Specific. Values following the Specific stand for:

- 2 Insert Module
- 3 Remove Module
- 4 Alarm (Major or Minor, Alarm or Clear)
- 5 Ip Change Event
- 6 Download Complete (reserved for future use)
- 7 Reboot Command
- 8 SelfTest Failure
- 9 Enhanced Alarm

Important: The default and recommended configuration is to enable only the Enhanced trap type. Enabling Enhanced alarm traps and other trap types at the same time may result in duplicate traps being sent to the element management system. These other trap types remain to allow backward compatibility with previously deployed systems.

Enhanced Trap Bindings Example

Trap Binding	MIB Name (Examples)	Explanation
1 Sequence	p2TrapLogSequence	Tracking number from 1 to 2,147,483,647.
2 Severity	p2TrapLogSeverity	Trap severity level - major (1), minor (2), warning (3).
3 State	p2TrapLogState	State - alarm (1), clear (2), event (3).
4 Label	p2TrapLogLabel or p2almLabel.1.3.4	Event Name or Alarm Label.
5 OID	p2almIndex.1.3 or p2icimStatusMsg	More data regarding the alarm or event is found at this OID.
6 Text	p2TrapLogText	Module name and model number of ICIM2 or ICIM2-XD.
7 ChassisID	p2icimChassisID	Chassis where the ICIM2, ICIM2-XD, or application module is installed.
8 SlotID	p2icimSlotID	Slot where the ICIM2, ICIM2-XD, or application module is installed.
9 CLLIcode	p2icimCLLIcode	Reserved for future use.
10 CLEIcode	p2icimCLEIcode	Reserved for future use.

Trap Binding		MIB Name (Examples)	Explanation
11	Time	p2TrapLogTime	Time trap generated in the format: YYYY-MM-DD,HH:MM:SS.ss
12	DateTime	p2TrapLogDateTime	Date and Time generated in the format: DOW, DD MMM YYYY HH:MM:SS ZZZ
13	Value	p2TrapLogValue	Value of the element in alarm.
14	Units	p2TrapLogUnit	Units in which the value is described.
15	Description	p2TrapLogDescr	Verbose description of the alarm or event.

Enhanced Trap Alarms

The current system release supports Enhanced trap alarms that alert the element management system to the following alarm types:

- Alarm Major
- Alarm Major Clear
- Alarm Minor
- Alarm Minor Clear

This section provides examples of each of these alarm types.

Alarm Major

```
Specific: 9
Message reception date: 12/17/2007
Message reception time: 5:36:49 PM
Time stamp: 4 days 02h:04m:34s.68th
Message type: Trap (v1)
Protocol version: SNMPv1
Transport: IP/UDP
Agent
  Address: 192.168.1.149
  Port: 1182
Manager
  Address: 192.168.1.7
  Port: 162
Community: prismatrap
SNMPv1 agent address: 192.168.1.149
Enterprise: p2trapEvents
Bindings (15)
  Binding #1: p2TrapLogSequence *** (int32) 81
  Binding #2: p2TrapLogSeverity *** (int32) major(1)
  Binding #3: p2TrapLogState *** (int32) alarm(1)
  Binding #4: p2almLabel.99.0.2 *** (octets) Fan2_Ok
  Binding #5: p2almIndex.99.0 *** (int32) 2
  Binding #6: p2TrapLogText *** (octets) Module=XD-Chassis, Model=5020
  Binding #7: p2chassisID.99.0 *** (int32) 99
  Binding #8: p2slotID.99.0 *** (int32) 0
  Binding #9: p2moduleCLLICODE.99.0 *** (octets) Grayson
  Binding #10: p2moduleCLEICODE.99.0 *** (octets) N/A
  Binding #11: p2TrapLogTime *** (octets) 2007-12-17,17:36:55.80
  Binding #12: p2TrapLogDateTime *** (octets) Mon, 17 Dec 2007 17:36:55 EST
  Binding #13: p2TrapLogValue *** (octets) N/A
  Binding #14: p2TrapLogUnit *** (octets) N/A
  Binding #15: p2TrapLogDescr *** (octets) Fan2_Ok exceeded major threshold
```

Alarm Major Clear

```
Specific: 9
Message reception date: 12/17/2007
Message reception time: 5:37:46 PM
Time stamp: 4 days 02h:05m:31s.68th
Message type: Trap (v1)
Protocol version: SNMPv1
Transport: IP/UDP
Agent
  Address: 192.168.1.149
  Port: 1184
Manager
  Address: 192.168.1.7
  Port: 162
Community: prismatrap
SNMPv1 agent address: 192.168.1.149
Enterprise: p2trapEvents
Bindings (15)
  Binding #1: p2TrapLogSequence *** (int32) 82
  Binding #2: p2TrapLogSeverity *** (int32) major(1)
  Binding #3: p2TrapLogState *** (int32) clear(2)
  Binding #4: p2almLabel.99.0.2 *** (octets) Fan2_Ok
  Binding #5: p2almIndex.99.0 *** (int32) 2
  Binding #6: p2TrapLogText *** (octets) Module=XD-Chassis, Model=5020
  Binding #7: p2chassisID.99.0 *** (int32) 99
  Binding #8: p2slotID.99.0 *** (int32) 0
  Binding #9: p2moduleCLLICODE.99.0 *** (octets) Grayson
  Binding #10: p2moduleCLEICODE.99.0 *** (octets) N/A
  Binding #11: p2TrapLogTime *** (octets) 2007-12-17,17:37:52.80
  Binding #12: p2TrapLogDateTime *** (octets) Mon, 17 Dec 2007 17:37:52 EST
  Binding #13: p2TrapLogValue *** (octets) N/A
  Binding #14: p2TrapLogUnit *** (octets) N/A
  Binding #15: p2TrapLogDescr *** (octets) Fan2_Ok within major threshold
```


Alarm Minor

```

Specific: 9
Message reception date: 12/17/2007
Message reception time: 5:34:38 PM
Time stamp: 4 days 02h:02m:23s.50th
Message type: Trap (v1)
Protocol version: SNMPv1
Transport: IP/UDP
Agent
  Address: 192.168.1.149
  Port: 1178
Manager
  Address: 192.168.1.7
  Port: 162
Community: prismatrap
SNMPv1 agent address: 192.168.1.149
Enterprise: p2trapEvents
Bindings (15)
  Binding #1: p2TrapLogSequence *** (int32) 79
  Binding #2: p2TrapLogSeverity *** (int32) minor(2)
  Binding #3: p2TrapLogState *** (int32) alarm(1)
  Binding #4: p2almLabel.99.0.4 *** (octets) ChasTemp
  Binding #5: p2almIndex.99.0 *** (int32) 4
  Binding #6: p2TrapLogText *** (octets) Module=XD-Chassis, Model=5020
  Binding #7: p2chassisID.99.0 *** (int32) 99
  Binding #8: p2slotID.99.0 *** (int32) 0
  Binding #9: p2moduleCLLICODE.0.0 *** (octets) Grayson
  Binding #10: p2moduleCLEICODE.0.0 *** (octets) N/A
  Binding #11: p2TrapLogTime *** (octets) 2007-12-17,17:34:44.62
  Binding #12: p2TrapLogDateTime *** (octets) Mon, 17 Dec 2007 17:34:44 EST
  Binding #13: p2TrapLogValue *** (octets) 28.75
  Binding #14: p2TrapLogUnit *** (octets) degC
  Binding #15: p2TrapLogDescr *** (octets) ChasTemp exceeded minor threshold

```

Alarm Minor Clear

```

Specific: 9
Message reception date: 12/17/2007
Message reception time: 5:35:46 PM
Time stamp: 4 days 02h:03m:31s.50th
Message type: Trap (v1)
Protocol version: SNMPv1
Transport: IP/UDP
Agent
  Address: 192.168.1.149
  Port: 1180
Manager
  Address: 192.168.1.7
  Port: 162
Community: prismatrap
SNMPv1 agent address: 192.168.1.149
Enterprise: p2trapEvents
Bindings (15)
  Binding #1: p2TrapLogSequence *** (int32) 80
  Binding #2: p2TrapLogSeverity *** (int32) minor(2)
  Binding #3: p2TrapLogState *** (int32) clear(2)
  Binding #4: p2almLabel.99.0.4 *** (octets) ChasTemp
  Binding #5: p2almIndex.99.0 *** (int32) 4
  Binding #6: p2TrapLogText *** (octets) Module=XD-Chassis, Model=5020
  Binding #7: p2chassisID.99.0 *** (int32) 99
  Binding #8: p2slotID.99.0 *** (int32) 0
  Binding #9: p2moduleCLLICODE.99.0 *** (octets) Grayson
  Binding #10: p2moduleCLEICODE.99.0 *** (octets) N/A
  Binding #11: p2TrapLogTime *** (octets) 2007-12-17,17:35:52.62
  Binding #12: p2TrapLogDateTime *** (octets) Mon, 17 Dec 2007 17:35:52 EST
  Binding #13: p2TrapLogValue *** (octets) 25.75
  Binding #14: p2TrapLogUnit *** (octets) degC
  Binding #15: p2TrapLogDescr *** (octets) ChasTemp within minor threshold

```

Enhanced Trap Events

The current system release supports Enhanced traps that alert management to certain events related to user login, changes to system settings, event log memory usage, SNMP failures, and user lockout activity.

All event traps display binding 2 (severity) as warning (3) and binding 3 (state) as event (3).

Binding 4 (label) may be an alarm label, or may include any of the following event types:

- Admin Change
- Authentication Failed
- Download Complete (reserved for future use)
- IP Change
- Login Threshold
- Log (Event Log)
- Module Insert
- Module Remove
- Reboot
- SelfTest
- SNMP (reserved for future use)
- Update Chassis IDs
- User Lockout

For example:

```
Binding #2: p2TrapLogSeverity *** (int32) warning(3)
Binding #3: p2TrapLogState *** (int32) event(3)
Binding #4: p2TrapLogLabel *** (octets) AdminChange
```

This section describes the events that cause each of these traps to be sent and gives examples of each trap where appropriate.

AdminChange

An AdminChange trap is sent when an Admin user performs one of the following actions.

- Add a user
- Change a password
- Change access level

- Enable or disable the status of a user
- Delete a user
- Fail to add a user because the list of users is full (16)
- Change the inactivity timeout
- Change the login thresholds
- Change the User Lockout interval setting

Chapter 9 SNMP Management

Admin Change Example - Add New User

```
Specific: 9
Message reception date: 10/30/2006
Message reception time: 1:46:53.476 PM
Time stamp: 2 days 22h:12m:43s.91th
Message type: Trap (v1)
Protocol version: SNMPv1
Transport: IP/UDP
Agent
  Address: 172.24.25.175
  Port: 1055
Manager
  Address: 172.18.10.23
  Port: 162
Community: prismatrap
SNMPv1 agent address: 172.24.25.175
Enterprise: p2trapEvents
Bindings (15)
  Binding #1: p2TrapLogSequence *** (int32) 22
  Binding #2: p2TrapLogSeverity *** (int32) warning(3)
  Binding #3: p2TrapLogState *** (int32) event(3)
  Binding #4: p2TrapLogLabel *** (octets) AdminChange
  Binding #5: p2icimStatusMsg.0 *** (int32) 0
  Binding #6: p2TrapLogText *** (octets) ICIM2
  Binding #7: p2chassisID.1.15 *** (int32) 1
  Binding #8: p2slotID.1.15 *** (int32) 15
  Binding #9: p2moduleCLLlcode.1.15 *** (octets) Engineering Lab
  Binding #10: p2moduleCLEIcode.1.15 *** (octets) ICIMCLEI75
  Binding #11: p2TrapLogTime *** (octets) 2006-10-30,13:46:35.19
  Binding #12: p2TrapLogDateTime *** (octets) Mon, 30 Oct 2006 13:46:35 EST
  Binding #13: p2TrapLogValue *** (octets) N/A
  Binding #14: p2TrapLogUnit *** (octets) N/A
  Binding #15: p2TrapLogDescr *** (octets) Add user ReadWrite3
```

Admin Change Example - Change ICIM2 or ICIM2-XD Setting (Inactivity Timer)

```
Specific: 9
Message reception date: 10/30/2006
Message reception time: 1:25:26.078 PM
Time stamp: 2 days 21h:51m:16s.53th
Message type: Trap (v1)
Protocol version: SNMPv1
Transport: IP/UDP
Agent
  Address: 172.24.25.175
  Port: 1054
Manager
  Address: 172.18.10.23
  Port: 162
Community: prismatrap
SNMPv1 agent address: 172.24.25.175
Enterprise: p2trapEvents
Bindings (15)
  Binding #1: p2TrapLogSequence *** (int32) 21
  Binding #2: p2TrapLogSeverity *** (int32) warning(3)
  Binding #3: p2TrapLogState *** (int32) event(3)
  Binding #4: p2TrapLogLabel *** (octets) AdminChange
  Binding #5: p2icimStatusMsg.0 *** (int32) 0
  Binding #6: p2TrapLogText *** (octets) ICIM2
  Binding #7: p2chassisID.1.15 *** (int32) 1
  Binding #8: p2slotID.1.15 *** (int32) 15
  Binding #9: p2moduleCLLlcode.1.15 *** (octets) Engineering Lab
  Binding #10: p2moduleCLEIcode.1.15 *** (octets) ICIMCLEI75
  Binding #11: p2TrapLogTime *** (octets) 2006-10-30,13:25:7.77
  Binding #12: p2TrapLogDateTime *** (octets) Mon, 30 Oct 2006 13:25:07 EST
  Binding #13: p2TrapLogValue *** (octets) N/A
  Binding #14: p2TrapLogUnit *** (octets) N/A
  Binding #15: p2TrapLogDescr *** (octets) Change inactivity timer setting
    to: 10 minutes
```

Admin Change Example - Change ICIM2 or ICIM2-XD Setting (Login Threshold)

```

Specific: 9
Message reception date: 10/30/2006
Message reception time: 1:19:04.310 PM
Time stamp: 2 days 21h:44m:54s.78th
Message type: Trap (v1)
Protocol version: SNMPv1
Transport: IP/UDP
Agent
  Address: 172.24.25.175
  Port: 1049
Manager
  Address: 172.18.10.23
  Port: 162
Community: prismatrap
SNMPv1 agent address: 172.24.25.175
Enterprise: p2trapEvents
Bindings (15)
  Binding #1: p2TrapLogSequence *** (int32) 16
  Binding #2: p2TrapLogSeverity *** (int32) warning(3)
  Binding #3: p2TrapLogState *** (int32) event(3)
  Binding #4: p2TrapLogLabel *** (octets) AdminChange
  Binding #5: p2IcimStatusMsg.0 *** (int32) 0
  Binding #6: p2TrapLogText *** (octets) ICIM2
  Binding #7: p2chassisID.1.15 *** (int32) 1
  Binding #8: p2slotID.1.15 *** (int32) 15
  Binding #9: p2moduleCLLlcode.1.15 *** (octets) Engineering Lab
  Binding #10: p2moduleCLEIcode.1.15 *** (octets) ICIMCLEI75
  Binding #11: p2TrapLogTime *** (octets) 2006-10-30,13:18:46.0
  Binding #12: p2TrapLogDateTime *** (octets) Mon, 30 Oct 2006 13:18:46 EST
  Binding #13: p2TrapLogValue *** (octets) N/A
  Binding #14: p2TrapLogUnit *** (octets) N/A
  Binding #15: p2TrapLogDescr *** (octets) Change login threshold setting
                to: 5 minutes

```

Admin Change Example - Change User Password

```

Specific: 9
Message reception date: 10/30/2006
Message reception time: 1:48:37.618 PM
Time stamp: 2 days 22h:14m:28s.06th
Message type: Trap (v1)
Protocol version: SNMPv1
Transport: IP/UDP
Agent
  Address: 172.24.25.175
  Port: 1056
Manager
  Address: 172.18.10.23
  Port: 162
Community: prismatrap
SNMPv1 agent address: 172.24.25.175
Enterprise: p2trapEvents
Bindings (15)
  Binding #1: p2TrapLogSequence *** (int32) 23
  Binding #2: p2TrapLogSeverity *** (int32) warning(3)
  Binding #3: p2TrapLogState *** (int32) event(3)
  Binding #4: p2TrapLogLabel *** (octets) AdminChange
  Binding #5: p2IcimStatusMsg.0 *** (int32) 0
  Binding #6: p2TrapLogText *** (octets) ICIM2
  Binding #7: p2chassisID.1.15 *** (int32) 1
  Binding #8: p2slotID.1.15 *** (int32) 15
  Binding #9: p2moduleCLLlcode.1.15 *** (octets) Engineering Lab
  Binding #10: p2moduleCLEIcode.1.15 *** (octets) ICIMCLEI75
  Binding #11: p2TrapLogTime *** (octets) 2006-10-30,13:48:19.34
  Binding #12: p2TrapLogDateTime *** (octets) Mon, 30 Oct 2006 13:48:19 EST
  Binding #13: p2TrapLogValue *** (octets) N/A
  Binding #14: p2TrapLogUnit *** (octets) N/A
  Binding #15: p2TrapLogDescr *** (octets) Changed user password for
                ReadWrite3

```

Admin Change Example - Delete User

```
Specific: 9
Message reception date: 10/30/2006
Message reception time: 1:50:06.243 PM
Time stamp: 2 days 22h:15m:56s.68th
Message type: Trap (v1)
Protocol version: SNMPv1
Transport: IP/UDP
Agent
  Address: 172.24.25.175
  Port: 1057
Manager
  Address: 172.18.10.23
  Port: 162
Community: prismatrap
SNMPv1 agent address: 172.24.25.175
Enterprise: p2trapEvents
Bindings (15)
  Binding #1: p2TrapLogSequence *** (int32) 24
  Binding #2: p2TrapLogSeverity *** (int32) warning(3)
  Binding #3: p2TrapLogState *** (int32) event(3)
  Binding #4: p2TrapLogLabel *** (octets) AdminChange
  Binding #5: p2IcimStatusMsg.0 *** (int32) 0
  Binding #6: p2TrapLogText *** (octets) ICIM2
  Binding #7: p2chassisID.1.15 *** (int32) 1
  Binding #8: p2slotID.1.15 *** (int32) 15
  Binding #9: p2moduleCLLIcode.1.15 *** (octets) Engineering Lab
  Binding #10: p2moduleCLEIcode.1.15 *** (octets) ICIMCLEI75
  Binding #11: p2TrapLogTime *** (octets) 2006-10-30,13:49:47.97
  Binding #12: p2TrapLogDateTime *** (octets) Mon, 30 Oct 2006 13:49:47 EST
  Binding #13: p2TrapLogValue *** (octets) N/A
  Binding #14: p2TrapLogUnit *** (octets) N/A
  Binding #15: p2TrapLogDescr *** (octets) Delete user ReadWrite3
```

AuthentictnFailed

An AuthentictnFailed trap is sent when a user login (authentication) fails due to one of the following causes:

- The user ID is disabled.
- The password is not correct.
- The user ID is not correct or is not found.
- There are too many users logged into the ICIM2 or ICIM2-XD at the current time.
- The list of valid users could not be retrieved from the EEPROM.

Authentication Failed - Password incorrect

```

Specific: 9
Message reception date: 10/30/2006
Message reception time: 1:15:21.261 PM
Time stamp: 2 days 21h:41m:11s.73th
Message type: Trap (v1)
Protocol version: SNMPv1
Transport: IP/UDP
Agent
  Address: 172.24.25.175
  Port: 1048
Manager
  Address: 172.18.10.23
  Port: 162
Community: prismatrap
SNMPv1 agent address: 172.24.25.175
Enterprise: p2trapEvents
Bindings (15)
  Binding #1: p2TrapLogSequence *** (int32) 15
  Binding #2: p2TrapLogSeverity *** (int32) warning(3)
  Binding #3: p2TrapLogState *** (int32) event(3)
  Binding #4: p2TrapLogLabel *** (octets) AuthentictnFailed
  Binding #5: p2icimStatusMsg.0 *** (int32) 0
  Binding #6: p2TrapLogText *** (octets) ICIM2
  Binding #7: p2chassisID.1.15 *** (int32) 1
  Binding #8: p2slotID.1.15 *** (int32) 15
  Binding #9: p2moduleCLLlcode.1.15 *** (octets) Engineering Lab
  Binding #10: p2moduleCLEIcode.1.15 *** (octets) ICIMCLEI75
  Binding #11: p2TrapLogTime *** (octets) 2006-10-30,13:15:2.94
  Binding #12: p2TrapLogDateTime *** (octets) Mon, 30 Oct 2006 13:15:02 EST
  Binding #13: p2TrapLogValue *** (octets) N/A
  Binding #14: p2TrapLogUnit *** (octets) N/A
  Binding #15: p2TrapLogDescr *** (octets) Password failed: Administrat0r

```

Authentication Failed - User ID Disabled

```

Specific: 9
Message reception date: 10/30/2006
Message reception time: 4:31:48.399 PM
Time stamp: 0 days 00h:06m:26s.51th
Message type: Trap (v1)
Protocol version: SNMPv1
Transport: IP/UDP
Agent
  Address: 172.24.28.151
  Port: 1047
Manager
  Address: 172.18.10.23
  Port: 162
Community: prismatrap
SNMPv1 agent address: 172.24.28.151
Enterprise: p2trapEvents
Bindings (15)
  Binding #1: p2TrapLogSequence *** (int32) 24
  Binding #2: p2TrapLogSeverity *** (int32) warning(3)
  Binding #3: p2TrapLogState *** (int32) event(3)
  Binding #4: p2TrapLogLabel *** (octets) AuthentictnFailed
  Binding #5: p2icimStatusMsg.0 *** (int32) 0
  Binding #6: p2TrapLogText *** (octets) ICIM2
  Binding #7: p2chassisID.3.15 *** (int32) 3
  Binding #8: p2slotID.3.15 *** (int32) 15
  Binding #9: p2moduleCLLlcode.3.15 *** (octets) icimCLLlcode7
  Binding #10: p2moduleCLEIcode.3.15 *** (octets) (zero-length)
  Binding #11: p2TrapLogTime *** (octets) 2006-10-30,16:33:14.89
  Binding #12: p2TrapLogDateTime *** (octets) Mon, 30 Oct 2006 16:33:14 EST
  Binding #13: p2TrapLogValue *** (octets) N/A
  Binding #14: p2TrapLogUnit *** (octets) N/A
  Binding #15: p2TrapLogDescr *** (octets) Try to login to a disabled account:
    bogusUser2

```

Download Complete

This trap is reserved for future use.

IP Change

An IPChange trap is sent as notification that the IP address of the ICIM2 or ICIM2-XD has been changed.

IP Change Example - ICIM2 or ICIM2-XD IP Change

```
Specific: 9
Message reception date: 8/25/2006
Message reception time: 10:03:30.896 AM
Time stamp: 0 days 00h:15m:19s.00th
Message type: Trap (v1)
Protocol version: SNMPv1
Transport: IP/UDP
Agent
  Address: 172.2.5.168
  Port: 1030
Manager
  Address: 172.24.3.151
  Port: 162
Community: prismatrap
SNMPv1 agent address: 172.2.5.168
Enterprise: p2trapEvents
Bindings (15)
  Binding #1: p2TrapLogSequence *** (int32) 7
  Binding #2: p2TrapLogSeverity *** (int32) warning(3)
  Binding #3: p2TrapLogState *** (int32) event(3)
  Binding #4: p2TrapLogLabel *** (octets) IPchange
  Binding #5: p2IcimIPAddr *** (int32) 0
  Binding #6: p2TrapLogText *** (octets) ICIM IP address changed --
    172.24.28.151.
  Binding #7: p2IcimChassisID *** (int32) 0
  Binding #8: p2IcimSlotID *** (int32) 15
  Binding #9: p2IcimCLLicode *** (octets) SCIATL01
  Binding #10: p2IcimCLEIcode *** (octets) VLLUAA4DAA
  Binding #11: p2TrapLogTime *** (octets) 2006-8-25,10:5:8.42
  Binding #12: p2TrapLogDateTime *** (octets) Fri, 25 Aug 2006 10:05:08 EDT
  Binding #13: p2TrapLogValue *** (octets) N/A
  Binding #14: p2TrapLogUnit *** (octets) N/A
  Binding #15: p2TrapLogDescr *** (octets) ICIM IP Address has been changed
```

LoginThreshold

The LoginThreshold trap is sent when a user reaches the number of failed login attempts via the CLI or Web Interface as allowed by the login threshold.

Log Threshold Example - Too Many Failed Login Attempts

```

Specific: 9
  Message reception date: 10/30/2006
  Message reception time: 1:19:29.216 PM
  Time stamp: 2 days 21h:45m:19s.70th
  Message type: Trap (v1)
  Protocol version: SNMPv1
  Transport: IP/UDP
  Agent
    Address: 172.24.25.175
    Port: 1052
  Manager
    Address: 172.18.10.23
    Port: 162
  Community: prismatrap
  SNMPv1 agent address: 172.24.25.175
  Enterprise: p2trapEvents
  Bindings (15)
    Binding #1: p2TrapLogSequence *** (int32) 19
    Binding #2: p2TrapLogSeverity *** (int32) warning(3)
    Binding #3: p2TrapLogState *** (int32) event(3)
    Binding #4: p2TrapLogLabel *** (octets) LoginThreshold
    Binding #5: p2IcimStatusMsg.0 *** (int32) 0
    Binding #6: p2TrapLogText *** (octets) ICIM2
    Binding #7: p2chassisID.1.15 *** (int32) 1
    Binding #8: p2slotID.1.15 *** (int32) 15
    Binding #9: p2moduleCLLIcode.1.15 *** (octets) Engineering Lab
    Binding #10: p2moduleCLEIcode.1.15 *** (octets) ICIMCLEI75
    Binding #11: p2TrapLogTime *** (octets) 2006-10-30,13:19:10.91
    Binding #12: p2TrapLogDateTime *** (octets) Mon, 30 Oct 2006 13:19:10 EST
    Binding #13: p2TrapLogValue *** (octets) N/A
    Binding #14: p2TrapLogUnit *** (octets) N/A
    Binding #15: p2TrapLogDescr *** (octets) Maximum failed session login
                  attempts reached

```

Log Memory Traps

The event log traps LogMemHalfFull or LogMemoryFull are sent when the event log is nearing capacity. Traps are sent at each of the following intervals.

- 80% full
- 85% full
- 90% full
- 95% full
- 100% full

When all 5,000 entries in the event log table are filled, the LogMemoryFull trap is sent. New entries then replace the oldest entries as the information wraps. No additional LogMemoryFull traps are sent.

LogMemHalfFull Example

```
Specific: 9
Message reception date: 9/13/2006
Message reception time: 2:27:25.066 PM
Time stamp: 0 days 00h:11m:20s.13th
Message type: Trap (v1)
Protocol version: SNMPv1
Transport: IP/UDP
Agent
  Address: 172.24.28.193
  Port: 1035
Manager
  Address: 172.18.9.66
  Port: 162
Community: prismatrap
SNMPv1 agent address: 172.24.28.193
Enterprise: p2trapEvents
Bindings (15)
  Binding #1: p2TrapLogSequence *** (int32) 12
  Binding #2: p2TrapLogSeverity *** (int32) warning(3)
  Binding #3: p2TrapLogState *** (int32) event(3)
  Binding #4: p2TrapLogLabel *** (octets) LogMemHalfFull
  Binding #5: p2IcimStatusMsg.0 *** (int32) 0
  Binding #6: p2TrapLogText *** (octets) ICIM2
  Binding #7: p2chassisID.2.15 *** (int32) 2
  Binding #8: p2slotID.2.15 *** (int32) 15
  Binding #9: p2moduleCLLlcode.2.15 *** (octets) 1.2.243
  Binding #10: p2moduleCLEIcode.2.15 *** (octets) (zero-length)
  Binding #11: p2TrapLogTime *** (octets) 2006-9-13,1:51:39.42
  Binding #12: p2TrapLogDateTime *** (octets) Wed, 13 Sep 2006 01:51:39 EST
  Binding #13: p2TrapLogValue *** (octets) N/A
  Binding #14: p2TrapLogUnit *** (octets) N/A
  Binding #15: p2TrapLogDescr *** (octets) Log memory is %80 full
```

LogMemoryFull Example

```
Specific: 9
Message reception date: 9/13/2006
Message reception time: 2:44:27.081 PM
Time stamp: 0 days 00h:28m:22s.13th
Message type: Trap (v1)
Protocol version: SNMPv1
Transport: IP/UDP
Agent
  Address: 172.24.28.193
  Port: 1039
Manager
  Address: 172.18.9.66
  Port: 162
Community: prismatrap
SNMPv1 agent address: 172.24.28.193
Enterprise: p2trapEvents
Bindings (15)
  Binding #1: p2TrapLogSequence *** (int32) 16
  Binding #2: p2TrapLogSeverity *** (int32) warning(3)
  Binding #3: p2TrapLogState *** (int32) event(3)
  Binding #4: p2TrapLogLabel *** (octets) LogMemoryFull
  Binding #5: p2IcimStatusMsg.0 *** (int32) 0
  Binding #6: p2TrapLogText *** (octets) ICIM2
  Binding #7: p2chassisID.2.15 *** (int32) 2
  Binding #8: p2slotID.2.15 *** (int32) 15
  Binding #9: p2moduleCLLlcode.2.15 *** (octets) 1.2.243
  Binding #10: p2moduleCLEIcode.2.15 *** (octets) (zero-length)
  Binding #11: p2TrapLogTime *** (octets) 2006-9-13,2:8:41.45
  Binding #12: p2TrapLogDateTime *** (octets) Wed, 13 Sep 2006 02:08:41 EST
  Binding #13: p2TrapLogValue *** (octets) N/A
  Binding #14: p2TrapLogUnit *** (octets) N/A
  Binding #15: p2TrapLogDescr *** (octets) Log memory is %100 full
```

LogWriteError

An Event trap is sent when an attempt to write to the event log fails. This serves as a backup to alert the management system to a problem writing to the event log.

LogWriteError Example

```
Specific: 9
  Message reception date: 9/13/2006
  Message reception time: 2:44:27.081 PM
  Time stamp: 0 days 00h:28m:22s.13th
  Message type: Trap (v1)
  Protocol version: SNMPv1
  Transport: IP/UDP
  Agent
    Address: 172.24.28.193
    Port: 1039
  Manager
    Address: 172.18.9.66
    Port: 162
  Community: prismatrap
  SNMPv1 agent address: 172.24.28.193
  Enterprise: p2trapEvents
  Bindings (15)
    Binding #1: p2TrapLogSequence *** (int32) 16
    Binding #2: p2TrapLogSeverity *** (int32) warning(3)
    Binding #3: p2TrapLogState *** (int32) event(3)
    Binding #4: p2TrapLogLabel *** (octets) LogWriteError
    Binding #5: p2IcimStatusMsg.0 *** (int32) 0
    Binding #6: p2TrapLogText *** (octets) ICIM2
    Binding #7: p2chassisID.2.15 *** (int32) 2
    Binding #8: p2slotID.2.15 *** (int32) 15
    Binding #9: p2moduleCLLlcode.2.15 *** (octets) 1.2.243
    Binding #10: p2moduleCLEIcode.2.15 *** (octets) (zero-length)
    Binding #11: p2TrapLogTime *** (octets) 2006-9-13,2:8:41.45
    Binding #12: p2TrapLogDateTime *** (octets) Wed, 13 Sep 2006 02:08:41 EST
    Binding #13: p2TrapLogValue *** (octets) N/A
    Binding #14: p2TrapLogUnit *** (octets) N/A
    Binding #15: p2TrapLogDescr *** (octets) Log error, can't log message:
      Password failed: UserName14
```

Module Insert

A ModuleInsert trap is sent when an application module is inserted into a chassis in the ICIM2 or ICIM2-XD domain.

Module Insert Example

```
Specific: 9
Message reception date: 8/22/2006
Message reception time: 4:54:36.478 PM
Time stamp: 0 days 01h:09m:16s.00th
Message type: Trap (v1)
Protocol version: SNMPv1
Transport: IP/UDP
Agent
  Address: 172.2.5.168
  Port: 1034
Manager
  Address: 172.24.3.151
  Port: 162
Community: prismatrap
SNMPv1 agent address: 172.2.5.168
Enterprise: p2trapEvents
Bindings (15)
  Binding #1: p2TrapLogSequence *** (int32) 11
  Binding #2: p2TrapLogSeverity *** (int32) warning(3)
  Binding #3: p2TrapLogState *** (int32) event(3)
  Binding #4: p2TrapLogLabel *** (octets) ModuleInsert
  Binding #5: p2InsertModuleEntry *** (int32) 0
  Binding #6: p2TrapLogText *** (octets) Not available
  Binding #7: p2chassisID.0.11 *** (int32) 0
  Binding #8: p2slotID.0.11 *** (int32) 11
  Binding #9: p2moduleCLLICODE.0.11 *** (octets) SCIATL01
  Binding #10: p2moduleCLEICODE.0.11 *** (octets) CLEICODE
  Binding #11: p2TrapLogTime *** (octets) 2006-8-22,16:54:36.45
  Binding #12: p2TrapLogDateTime *** (octets) Tue, 22 Aug 2006 16:54:36 EST
  Binding #13: p2TrapLogValue *** (octets) N/A
  Binding #14: p2TrapLogUnit *** (octets) N/A
  Binding #15: p2TrapLogDescr *** (octets) A module has been inserted into a
    chassis
```

ModuleRemove

A ModuleRemove trap is sent when an application module is removed from a chassis in the ICIM2 or ICIM2-XD domain.

Module Remove Example

```

Specific: 9
  Message reception date: 8/22/2006
  Message reception time: 4:34:08.853 PM
  Time stamp: 0 days 00h:48m:48s.00th
  Message type: Trap (v1)
  Protocol version: SNMPv1
  Transport: IP/UDP
  Agent
    Address: 172.2.5.168
    Port: 1033
  Manager
    Address: 172.24.3.151
    Port: 162
  Community: prismatrap
  SNMPv1 agent address: 172.2.5.168
  Enterprise: p2trapEvents
  Bindings (15)
    Binding #1: p2TrapLogSequence *** (int32) 10
    Binding #2: p2TrapLogSeverity *** (int32) warning(3)
    Binding #3: p2TrapLogState *** (int32) event(3)
    Binding #4: p2TrapLogLabel *** (octets) ModuleRemove
    Binding #5: p2RemoveModuleEntry *** (int32) 0
    Binding #6: p2TrapLogText *** (octets) Not available
    Binding #7: p2chassisID.0.11 *** (int32) 0
    Binding #8: p2slotID.0.11 *** (int32) 11
    Binding #9: p2moduleCLLICODE.0.11 *** (octets) SCIATL01
    Binding #10: p2moduleCLEICODE.0.11 *** (octets) CLEICODE
    Binding #11: p2TrapLogTime *** (octets) 2006-8-22,16:34:8.84
    Binding #12: p2TrapLogDateTime *** (octets) Tue, 22 Aug 2006 16:34:08 EST
    Binding #13: p2TrapLogValue *** (octets) N/A
    Binding #14: p2TrapLogUnit *** (octets) N/A
    Binding #15: p2TrapLogDescr *** (octets) A module has been removed from a
                  chassis

```

Reboot

The Reboot trap is sent when an ICIM2, ICIM2-XD, or application module has been commanded to reboot, either individually or as a result of a broadcast reboot command.

Reboot Example - Broadcast Reboot Command

```
Specific: 9
Message reception date: 8/28/2006
Message reception time: 2:20:20.014 PM
Time stamp: 0 days 00h:03m:34s.00th
Message type: Trap (v1)
Protocol version: SNMPv1
Transport: IP/UDP
Agent
  Address: 172.2.5.168
  Port: 1032
Manager
  Address: 172.24.3.151
  Port: 162
Community: prismatrap
SNMPv1 agent address: 172.2.5.168
Enterprise: p2trapEvents
Bindings (15)
  Binding #1: p2TrapLogSequence *** (int32) 9
  Binding #2: p2TrapLogSeverity *** (int32) warning(3)
  Binding #3: p2TrapLogState *** (int32) event(3)
  Binding #4: p2TrapLogLabel *** (octets) RebootCommand
  Binding #5: p2IcimStatusMsg *** (int32) 0
  Binding #6: p2TrapLogText *** (octets) Broadcast
  Binding #7: p2chassisID.99.99 *** (int32) 99
  Binding #8: p2slotID.99.99 *** (int32) 99
  Binding #9: p2moduleCLLIcode.99.99 *** (octets) N/A
  Binding #10: p2moduleCLEIcode.99.99 *** (octets) N/A
  Binding #11: p2TrapLogTime *** (octets) 2006-8-28,14:20:20.43
  Binding #12: p2TrapLogDateTime *** (octets) Mon, 28 Aug 2006 14:20:20 EST
  Binding #13: p2TrapLogValue *** (octets) N/A
  Binding #14: p2TrapLogUnit *** (octets) N/A
  Binding #15: p2TrapLogDescr *** (octets) An ICIM/module has been commanded
    to reboot (CH 99 SL 99 indicates a broadcast reboot)
```

Reboot Example - Reboot ICIM2 or ICIM2-XD Command

```
Specific: 9
Message reception date: 8/22/2006
Message reception time: 3:44:20.455 PM
Time stamp: 0 days 00h:10m:17s.00th
Message type: Trap (v1)
Protocol version: SNMPv1
Transport: IP/UDP
Agent
  Address: 172.2.5.168
  Port: 1034
Manager
  Address: 172.24.3.151
  Port: 162
Community: prismatrap
SNMPv1 agent address: 172.2.5.168
Enterprise: p2trapEvents
Bindings (15)
  Binding #1: p2TrapLogSequence *** (int32) 11
  Binding #2: p2TrapLogSeverity *** (int32) warning(3)
  Binding #3: p2TrapLogState *** (int32) event(3)
  Binding #4: p2TrapLogLabel *** (octets) RebootCommand
  Binding #5: p2IcimStatusMsg *** (int32) 0
  Binding #6: p2TrapLogText *** (octets) Broadcast
  Binding #7: p2chassisID.99.99 *** (int32) 99
  Binding #8: p2slotID.99.99 *** (int32) 99
  Binding #9: p2moduleCLLIcode.99.99 *** (octets) SCIATL01
  Binding #10: p2moduleCLEIcode.99.99 *** (octets) CLEIcode
  Binding #11: p2TrapLogTime *** (octets) 2006-8-22,15:44:21.0
  Binding #12: p2TrapLogDateTime *** (octets) Tue, 22 Aug 2006 15:44:21 EST
  Binding #13: p2TrapLogValue *** (octets) N/A
  Binding #14: p2TrapLogUnit *** (octets) N/A
  Binding #15: p2TrapLogDescr *** (octets) An ICIM/module has been commanded
    to reboot (CH 99 SL 99 indicates a broadcast reboot)
```

SelfTest

A SelfTest trap is sent when either the ICIM2, ICIM2-XD, or application module fails its power-on self test.

SelfTest Example - ICIM2 or ICIM2-XD Failure

```
Specific: 9
  Message reception date: 8/25/2006
  Message reception time: 9:43:26.623 AM
  Time stamp: 0 days 00h:00m:57s.00th
  Message type: Trap (v1)
  Protocol version: SNMPv1
  Transport: IP/UDP
  Agent
    Address: 172.2.5.168
    Port: 1024
  Manager
    Address: 172.24.3.151
    Port: 162
  Community: prismatrap
  SNMPv1 agent address: 172.2.5.168
  Enterprise: p2trapEvents
  Bindings (15)
    Binding #1: p2TrapLogSequence *** (int32) 1
    Binding #2: p2TrapLogSeverity *** (int32) warning(3)
    Binding #3: p2TrapLogState *** (int32) event(3)
    Binding #4: p2TrapLogLabel *** (octets) SelfTest
    Binding #5: p2icimSelfTest *** (int32) 0
    Binding #6: p2TrapLogText *** (octets) SelfTest Failed - Error Code 16777232
    Binding #7: p2icimChassisID *** (int32) 0
    Binding #8: p2icimSlotID *** (int32) 15
    Binding #9: p2icimCLLICODE *** (octets) SCIATL01
    Binding #10: p2icimCLEICODE *** (octets) VLLUAA4DAA
    Binding #11: p2TrapLogTime *** (octets) 2006-8-25,9:45:1.76
    Binding #12: p2TrapLogDateTime *** (octets) Fri, 25 Aug 2006 09:45:01 EDT
    Binding #13: p2TrapLogValue *** (octets) N/A
    Binding #14: p2TrapLogUnit *** (octets) N/A
    Binding #15: p2TrapLogDescr *** (octets) An ICIM/module has failed its
      power-on self test
```

SelfTest Example - Module Failure

```
Specific: 9
Message reception date: 8/25/2006
Message reception time: 9:49:50.657 AM
Time stamp: 0 days 00h:01m:39s.00th
Message type: Trap (v1)
Protocol version: SNMPv1
Transport: IP/UDP
Agent
  Address: 172.2.5.168
  Port: 1024
Manager
  Address: 172.24.3.151
  Port: 162
Community: prismatrap
SNMPv1 agent address: 172.2.5.168
Enterprise: p2trapEvents
Bindings (15)
  Binding #1: p2TrapLogSequence *** (int32) 1
  Binding #2: p2TrapLogSeverity *** (int32) warning(3)
  Binding #3: p2TrapLogState *** (int32) event(3)
  Binding #4: p2TrapLogLabel *** (octets) SelfTest
  Binding #5: p2moduleSelfTest.0.0 *** (int32) 0
  Binding #6: p2TrapLogText *** (octets) SelfTest Failed - Error Code 33558528
  Binding #7: p2chassisID.0.0 *** (int32) 0
  Binding #8: p2slotID.0.0 *** (int32) 0
  Binding #9: p2moduleCLLIcode.0.0 *** (octets) SCIATL01
  Binding #10: p2moduleCLEIcode.0.0 *** (octets) CLEIcode
  Binding #11: p2TrapLogTime *** (octets) 2006-8-25,9:51:28.17
  Binding #12: p2TrapLogDateTime *** (octets) Fri, 25 Aug 2006 09:51:28 EDT
  Binding #13: p2TrapLogValue *** (octets) N/A
  Binding #14: p2TrapLogUnit *** (octets) N/A
  Binding #15: p2TrapLogDescr *** (octets) An ICIM/module has failed its
    power-on self test
```

SNTP

This trap is reserved for future use.

UpdateChassisID

The UpdateChassisID trap is sent to indicate that the ICIM2 or ICIM2-XD is rediscovering the domain as a result of one of the following actions.

- The p2icimUpdateChassisID is set to 1 via SNMP.
- The CLI command `set updateid 1` is issued from the ICIM> command prompt.

UpdateChassisID Example

```
Specific: 9
Message reception date: 10/30/2006
Message reception time: 12:39:26.263 PM
Time stamp: 0 days 00h:04m:32s.51th
Message type: Trap (v1)
Protocol version: SNMPv1
Transport: IP/UDP
Agent
  Address: 172.24.28.151
  Port: 1037
Manager
  Address: 172.18.10.23
  Port: 162
Community: prismatrap
SNMPv1 agent address: 172.24.28.151
Enterprise: p2trapEvents
Bindings (15)
  Binding #1: p2TrapLogSequence *** (int32) 14
  Binding #2: p2TrapLogSeverity *** (int32) warning(3)
  Binding #3: p2TrapLogState *** (int32) event(3)
  Binding #4: p2TrapLogLabel *** (octets) UpdateChassisIDs
  Binding #5: p2IcimUpdateChassisIDs *** (int32) 0
  Binding #6: p2TrapLogText *** (octets) ICIM2
  Binding #7: p2chassisID.4.15 *** (int32) 4
  Binding #8: p2slotID.4.15 *** (int32) 15
  Binding #9: p2moduleCLLICODE.4.15 *** (octets) icimCLLICODE7
  Binding #10: p2moduleCLEICODE.4.15 *** (octets) (zero-length)
  Binding #11: p2TrapLogTime *** (octets) 2006-10-30,12:40:9.94
  Binding #12: p2TrapLogDateTime *** (octets) Mon, 30 Oct 2006 12:40:09 EST
  Binding #13: p2TrapLogValue *** (octets) N/A
  Binding #14: p2TrapLogUnit *** (octets) N/A
  Binding #15: p2TrapLogDescr *** (octets) A user requested update for all
               chassis IDs has occurred
```

UserLockout

The UserLockout trap is sent whenever a user is locked out as a result of reaching the failed login attempts threshold. The UserLockout event may result in the following message:

- User <user_name> has reached maximum failed login attempts and been locked out.

UserLockout Example

```
Specific: 9
Message reception date: 3/15/2007
Message reception time: 2:15:02.352 PM
Time stamp: 0 days 00h:21m:11s.61th
Message type: Trap (v1)
Protocol version: SNMPv1
Transport: IP/UDP
Agent
  Address: 190.2.0.110
  Port: 1056
Manager
  Address: 190.2.0.108
  Port: 162
Community: prismatrap
SNMPv1 agent address: 190.2.0.114
Enterprise: p2trapEvents
  Bindings (15)
    Binding #1: p2TrapLogSequence *** (int32) 32
    Binding #2: p2TrapLogSeverity *** (int32) warning(3)
    Binding #3: p2TrapLogState *** (int32) event(3)
    Binding #4: p2TrapLogLabel *** (octets) UserLockout
    Binding #5: p2IcimStatusMsg *** (int32) 0
    Binding #6: p2TrapLogText *** (octets) ICIM2
    Binding #7: p2chassisID.3.15 *** (int32) 3
    Binding #8: p2slotID.3.15 *** (int32) 15
    Binding #9: p2moduleCLLIcode.3.15 *** (octets) ICIMCLLI
    Binding #10: p2moduleCLEIcode.3.15 *** (octets) VLLUAA4DAA
    Binding #11: p2TrapLogTime *** (octets) 2007-3-15,14:15:1.84
    Binding #12: p2TrapLogDateTime *** (octets) Thu, 15 Mar 2007 14:15:01 EDT
    Binding #13: p2TrapLogValue *** (octets) N/A
    Binding #14: p2TrapLogUnit *** (octets) N/A
    Binding #15: p2TrapLogDescr *** (octets) User ferret3 has reached maximum
      failed login attempts and been locked out.
```

Alarm Threshold Modification

The meaning of an alarm value depends on the type of alarm. For example, a p2almValue of 0 (zero) indicates OK for a Boolean alarm type (p2almType = 5 or 6), but signals a Major Low alarm for a Non-Boolean alarm type (p2almType = 1, 2, 3, 4, 7 or 8). For more information, see Module Alarm Table.

The following example illustrates how an alarm threshold may be set, and the subsequent behavior that results from violating the alarm threshold. This behavior includes a module going into an alarm state and a trap being sent.

- 1 First, observe that the actual value of the +24 V rail voltage from DC-to-DC converter B is 24.0095 V, as found in the p2moduleMonitorTable shown below.

Instance	p2monitorIndex(IDX)	p2monitorLabel	p2monitorValue	p2monitorUnit	p2monitorType	p2monitorStateNames
1.0.1	1	ConvA+24	24.1499	V	F	N/A
1.0.2	2	ConvA+5	5.28269	V	F	N/A
1.0.3	3	ConvA-5	-5.26423	V	F	N/A
1.0.4	4	ConvB+24	24.0095	V	F	N/A
1.0.5	5	ConvB+5	5.27484	V	F	N/A
1.0.6	6	ConvB-5	-5.2905	V	F	N/A
1.0.7	7	PSA Inst	1	N/A	S	[0] No, [1] Yes
1.0.8	8	PSB Inst	1	N/A	S	[0] No, [1] Yes
1.0.9	9	ConvAlns	1	N/A	S	[0] No, [1] Yes
1.0.10	10	ConvBlns	1	N/A	S	[0] No, [1] Yes
1.0.11	11	Chas+24V	24.1177	V	F	N/A
1.0.12	12	Chas+5V	5.0277	V	F	N/A

TP479

- 2 Next, moving to the Module Alarm table, we change the minor low limit from 18.4 to 24.9, as shown below.

Instance	p2almIndex(IDX)	p2almLabel	p2almValue	p2almType	p2almNominal	p2almHysteresis	p2almMajorLowLimit	p2almMinorLowLimit	p2almMinorHighLimit
1.0.1	1	Fan 1 Ok	0 (ok)	6	1	N/A	N/A	N/A	N/A
1.0.2	2	Fan 2 Ok	0 (ok)	6	1	N/A	N/A	N/A	N/A
1.0.3	3	Fan 3 Ok	0 (ok)	6	1	N/A	N/A	N/A	N/A
1.0.4	4	ChasTemp	2 (ok)	2	25	1	-40	-35	60
1.0.5	5	ConvAln	0 (ok)	5	1	N/A	N/A	N/A	N/A
1.0.6	6	ConvA+24	2 (ok)	2	24.7	0.1	18	18.4	25.9
1.0.7	7	ConvA+5	2 (ok)	2	5.4	0.1	3.6	3.7	5.9
1.0.8	8	ConvA-5	2 (ok)	2	-5.4	0.1	-5.6	-5.5	-4.6
1.0.9	9	ConvBln	0 (ok)	5	1	N/A	N/A	N/A	N/A
1.0.10	10	ConvB+24	2 (ok)	2	24.7	0.1	18	24.9	25.9
1.0.11	11	ConvB+5	2 (ok)	2	5.4	0.1	3.6	3.7	5.9
1.0.12	12	ConvB-5	2 (ok)	2	-5.4	0.1	-5.6	-5.5	-4.6
1.1.1	1	LasTemp	2 (ok)	3	40	1	-15	-5	5
1.1.2	2	LasBias	2 (ok)	3	75	3	-20	-10	10
1.1.3	3	InRF	2 (ok)	1	0	0.5	-1000	-5	5
1.1.4	4	TxEnable	0 (ok)	6	0	N/A	N/A	N/A	N/A
1.1.5	5	OutPwr	2 (ok)	1	2.9	0.1	-1	-0.5	0.5
1.1.6	6	CwMode	0 (ok)	5	1	N/A	N/A	N/A	N/A

TP480

- 3 Because the actual value (24.0095) of the +24 V rail converter B is less than the Minor Low limit of 24.9, an Enhanced trap for a Minor alarm is sent. A copy of the trap is kept in the Trap Logging table, as shown below.

Instance	p2TrapLogSequence(IDX)	p2TrapLogSeverity	p2TrapLogState	p2TrapLogLabel	p2TrapLogOID	p2TrapLogText
93	93	minor(2)	alarm(1)	ConvB+24	p2almIndex.1.0.10	Module=XD-Chassis, Model=5020
92	92	major(1)	clear(2)	Alarm	p2almIndex.2.3.4	Module=P2-HD-RXF, Model=2015
91	91	major(1)	alarm(1)	Alarm	p2almIndex.2.3.4	Module=P2-HD-RXF, Model=2015
90	90	major(1)	clear(2)	Alarm	p2almIndex.2.3.4	Module=P2-HD-RXF, Model=2015
89	89	major(1)	alarm(1)	Alarm	p2almIndex.2.3.4	Module=P2-HD-RXF, Model=2015
88	88	major(1)	clear(2)	CwMode	p2almIndex.1.1.6	Module=HDTx, Model=1020
87	87	major(1)	alarm(1)	CwMode	p2almIndex.1.1.6	Module=HDTx, Model=1020
86	86	major(1)	clear(2)	CwMode	p2almIndex.1.1.6	Module=HDTx, Model=1020
85	85	major(1)	alarm(1)	CwMode	p2almIndex.1.1.6	Module=HDTx, Model=1020
84	84	major(1)	clear(2)	CwMode	p2almIndex.1.1.6	Module=HDTx, Model=1020
83	83	major(1)	alarm(1)	CwMode	p2almIndex.1.1.6	Module=HDTx, Model=1020
82	82	major(1)	clear(2)	CwMode	p2almIndex.1.1.6	Module=HDTx, Model=1020
81	81	major(1)	alarm(1)	CwMode	p2almIndex.1.1.6	Module=HDTx, Model=1020
80	80	warning(3)	event(3)	UpdateChassisIDs	p2cimUpdateChassisIDs.0	ICIM2

TP481

- 4 Now, we change the minor low limit back to 18.4 in the Module Alarm table, as shown below.

Instance	p2almIndex(IDX)	p2almLabel	p2almValue	p2almType	p2almNominal	p2almHysteresis	p2almMajorLowLimit	p2almMinorLowLimit	p2almMinorHighLimit
1.0.1	1	Fan 1 Ok	0 (ok)	6	1	N/A	N/A	N/A	N/A
1.0.2	2	Fan 2 Ok	0 (ok)	6	1	N/A	N/A	N/A	N/A
1.0.3	3	Fan 3 Ok	0 (ok)	6	1	N/A	N/A	N/A	N/A
1.0.4	4	ChasTemp	2 (ok)	2	25	1	-40	-35	60
1.0.5	5	ConvAIn	0 (ok)	5	1	N/A	N/A	N/A	N/A
1.0.6	6	ConvA+24	2 (ok)	2	24.7	0.1	18	18.4	25.9
1.0.7	7	ConvA+5	2 (ok)	2	5.4	0.1	3.6	3.7	5.9
1.0.8	8	ConvA-5	2 (ok)	2	-5.4	0.1	-5.6	-5.5	-4.6
1.0.9	9	ConvBIn	0 (ok)	5	1	N/A	N/A	N/A	N/A
1.0.10	10	ConvB+24	1 (minor lo...)	2	24.7	0.1	18	18.4	25.9
1.0.11	11	ConvB+5	2 (ok)	2	5.4	0.1	3.6	3.7	5.9
1.0.12	12	ConvB-5	2 (ok)	2	-5.4	0.1	-5.6	-5.5	-4.6
1.1.1	1	LasTemp	2 (ok)	3	40	1	-15	-5	5
1.1.2	2	LasBias	2 (ok)	3	75	3	-20	-10	10
1.1.3	3	InRF	2 (ok)	1	0	0.5	-1000	-5	5
1.1.4	4	TxEnable	0 (ok)	6	0	N/A	N/A	N/A	N/A
1.1.5	5	OutPwr	2 (ok)	1	2.9	0.1	-1	-0.5	0.5
1.1.6	6	CwMode	0 (ok)	5	1	N/A	N/A	N/A	N/A

TP482

When we do this, an Enhanced trap for a Minor clear is generated, and a copy of the trap is kept in the Trap Logging table.

- 5 Finally, returning to the Module Alarm table, we note that the alarm value has changed from 1 (Minor Low) to 2 (OK).

Instance	p2almIndex(IDX)	p2almLabel	p2almValue	p2almType	p2almNominal	p2almHysteresis	p2almMajorLowLimit	p2almMinorLowLimit	p2almMinorHighLimit
1.0.1	1	Fan 1 Ok	0 (ok)	6	1	N/A	N/A	N/A	N/A
1.0.2	2	Fan 2 Ok	0 (ok)	6	1	N/A	N/A	N/A	N/A
1.0.3	3	Fan 3 Ok	0 (ok)	6	1	N/A	N/A	N/A	N/A
1.0.4	4	ChasTemp	2 (ok)	2	25	1	-40	-35	60
1.0.5	5	ConvAIn	0 (ok)	5	1	N/A	N/A	N/A	N/A
1.0.6	6	ConvA+24	2 (ok)	2	24.7	0.1	18	18.4	25.9
1.0.7	7	ConvA+5	2 (ok)	2	5.4	0.1	3.6	3.7	5.9
1.0.8	8	ConvA-5	2 (ok)	2	-5.4	0.1	-5.6	-5.5	-4.6
1.0.9	9	ConvBIn	0 (ok)	5	1	N/A	N/A	N/A	N/A
1.0.10	10	ConvB+24	2 (ok)	2	24.7	0.1	18	18.4	25.9
1.0.11	11	ConvB+5	2 (ok)	2	5.4	0.1	3.6	3.7	5.9
1.0.12	12	ConvB-5	2 (ok)	2	-5.4	0.1	-5.6	-5.5	-4.6
1.1.1	1	LasTemp	2 (ok)	3	40	1	-15	-5	5
1.1.2	2	LasBias	2 (ok)	3	75	3	-20	-10	10
1.1.3	3	InRF	2 (ok)	1	0	0.5	-1000	-5	5
1.1.4	4	TxEnable	0 (ok)	6	0	N/A	N/A	N/A	N/A
1.1.5	5	OutPwr	2 (ok)	1	2.9	0.1	-1	-0.5	0.5
1.1.6	6	CwMode	0 (ok)	5	1	N/A	N/A	N/A	N/A

TP483

System Behavior

ICIM2 as Proxy for Module Information

The user gains access to information about modules in the ICIM2 or ICIM2-XD domain through the ICIM2 or ICIM2-XD via SNMP and the MIBs. A virtual database in the ICIM2 or ICIM2-XD keeps track of data supplied by each module. The ICIM2 or ICIM2-XD periodically refreshes this database to ensure that the information it provides is up-to-date.

In this way, all module information obtained via SNMP is proxied through the ICIM2 or ICIM2-XD. Because the modules never interface directly with SNMP, this proxy behavior differs from that of SNMP Proxy Agents, and the two methods should not be confused with each other.

Delay in the Discovery Process

Depending on when an event occurs in relation to the ICIM2 or ICIM2-XD polling cycle, a user may notice delays in the discovery process.

Such delays may be experienced when inserting or removing a module. For example, if the ICIM2 or ICIM2-XD has just polled a module in chassis 02 slot 06, and the module is removed, it may be several seconds before the ICIM2 or ICIM2-XD realizes that chassis 02 slot 06 is empty. Once the empty slot is detected, and if trap destination is configured, a trap indicating module removal will be sent.

Depending on the number of modules managed by an ICIM2 or ICIM2-XD and the timing of the polling cycle, it may be possible to remove and re-insert a module from chassis 02 slot 06, for example, without the ICIM2 or ICIM2-XD even detecting that it was missing.

Module Removal and Enhanced Traps

If a module is removed, an Enhanced trap is sent. No other traps indicating alarms or clearings are sent for that module. Once again, because of the delay in the discovery process, it may be possible to remove and reinsert a module without traps being sent.

Frequently Asked Questions

How do I configure trap destination?

Trap destination is set up via an entry into the p2TrapRecvTable. Select an index (choices are 0 through 9) that is not currently used for trap destination.

Note: Some element management systems access and populate the first two entries (0 and 1), making them unavailable for user configuration.

- 1 Set p2TrapRecvEnable to enabled (2).
- 2 Set p2TrapRecvAddr to the IP address of the remote entity, in the format 172.0.0.1.
- 3 Set p2TrapRecvTelcoAlarm to enabled (2).

Instance	p2TrapRecvIndex	p2TrapRecvEnable	p2TrapRecvAddr	p2TrapRecvIPC
0	0	enabled(2)	172.18.50.42	enabled(2)
1	1	enabled(2)	172.18.50.3	enabled(2)
2	2	enabled(2)	172.18.50.6	enabled(2)
3	3	disabled(1)	0.0.0.0	disabled(1)
4	4	disabled(1)	0.0.0.0	disabled(1)
5	5	disabled(1)	0.0.0.0	disabled(1)
6	6	disabled(1)	0.0.0.0	disabled(1)
7	7	disabled(1)	0.0.0.0	disabled(1)
8	8	disabled(1)	0.0.0.0	disabled(1)
9	9	disabled(1)	0.0.0.0	disabled(1)

Command	p2TrapRecvSelfTest	p2TrapRecvTelcoAlarm
	disabled(1)	enabled(2)
	disabled(1)	enabled(2)
	disabled(1)	enabled(2)
	disabled(1)	enabled(2)
	disabled(1)	enabled(2)
	disabled(1)	enabled(2)
	disabled(1)	enabled(2)
	disabled(1)	enabled(2)
	disabled(1)	enabled(2)
	disabled(1)	enabled(2)

TP490

Note: Enable the row, or traps will not be sent.

For additional information, see *To Configure Trap Destination* (on page 229), *Trap Types* (on page 230), and *Trap Recv Table* (on page 190).

Why do the same alarm values represent different conditions?

For example, why does an alarm value of zero sometimes mean "OK," and other times indicate a state of alarm? The answer is that the alarm value and the alarm type are inseparably linked, with the meaning of the alarm value inherently connected with the type of alarm.

For example:

- A zero in p2almValue indicates that all is fine for a Boolean (p2almType 5 or 6).
- A zero in p2almValue indicates a major low alarm for a Non-Boolean (p2almType 1, 2, 3, 4, 7 or 8).

For additional information, see the sections on alarms in *Module Alarm Table* (on page 208).

How do Enhanced Traps differ from other trap types?

The Enhanced traps contain additional information in the bindings that is not included in the original proprietary traps.

All proprietary traps are represented with the Enhanced traps. If Enhanced traps are enabled and if the row in the p2TrapRecvTable is enabled, all traps will be sent to the IP address set in that particular row.

All trap settings are documented for completeness only. Information contained in other proprietary traps is expanded upon in the Enhanced traps. Use of the older traps is not recommended, as the new Enhanced trap is more useful. Enabling other traps together with the Enhanced trap will cause two traps to be sent for each event. For more information, see *Prisma II Traps* (on page 227), *Trap Types* (on page 230), and *Enhanced Trap Binding Information* (on page 241).

When do traps associated with module insertion, removal, and alarms occur?

If modules are in a state of alarm, traps are generated at module insertion, module startup, chassis startup, or ICIM2 or ICIM2-XD startup. If p2TrapRecvTable is not configured with IP addresses, rows enabled, and Enhanced traps enabled, no traps are sent for alarms detected at startup.

If a module is inserted after a steady-state condition is reached, a trap is generated when the ICIM2 or ICIM2-XD recognizes the insertion event. This fact is recorded in p2InsertModuleTable. Also, if the module is in a state of alarm, this will be indicated with startup traps. For additional information, see *System Behavior* (on page 267).

Upon removal of a module, and once the ICIM2 or ICIM2-XD detects the change, a trap is generated. Module removal is detected by continued lack of response to internal ICIM2 or ICIM2-XD polling of the module, so it may take several polling cycles to discover that the module was removed. However, no traps will be sent to clear the alarms.

After a module is removed, the ICIM2 or ICIM2-XD keeps no further information on the module except what appears in p2RemoveModuleTable.

After the modules are discovered by the ICIM2 or ICIM2-XD and initial alarms are acknowledged by traps, subsequent alarm traps are edge-triggered. Thus, alarm traps are generated upon module startup, and if there is a change in the state of an alarm following initial discovery.

Tip: Enable the row, set the IP address, and enable Enhanced traps, or startup alarm traps will not be sent or logged.

What is the Trap Logging Table?

The Trap Logging table holds up to 1,000 entries. When the table gets full, each new entry causes the oldest one to age out of the listing, leaving the most recent 1,000 entries.

Instance	p2TaplogSequenceID(x)	p2TaplogSeverity	taplogState	taplogLabel	p2TaplogID	p2TaplogTime	p2TaplogChassisID	p2TaplogSlotID	p2TaplogLLCID	p2TaplogCleid	p2TaplogError
1	1	minor(2)	alarm(1)	INRF	p2aindex.1.2.3	Module=HD1x, Model=1020	1	2	N/A	N/A	N/A
2	2	minor(2)	alarm(1)	INRF	p2aindex.1.3.3	Module=HD1x, Model=1020	1	3	N/A	N/A	200
3	3	minor(2)	alarm(1)	INRF	p2aindex.1.4.3	Module=HD1x, Model=1020	1	4	N/A	N/A	200
4	4	major(1)	alarm(1)	INRF	p2aindex.1.5.3	Module=HD1x, Model=1032	1	5	N/A	N/A	200
5	5	minor(2)	alarm(1)	INRF	p2aindex.1.7.3	Module=HD1x, Model=1032	1	7	N/A	N/A	200
6	6	minor(2)	alarm(1)	INRF	p2aindex.1.8.3	Module=HD1x, Model=1032	1	8	N/A	N/A	200
7	7	minor(2)	alarm(1)	INRF	p2aindex.1.9.3	Module=HD1x, Model=1032	1	9	N/A	N/A	200
8	8	minor(2)	alarm(1)	INRF	p2aindex.1.10.3	Module=HD1x, Model=1032	1	10	N/A	N/A	200
9	9	minor(2)	alarm(1)	INRF	p2aindex.1.11.3	Module=HD1x, Model=1032	1	11	N/A	N/A	200
10	10	minor(2)	alarm(1)	INRF	p2aindex.1.12.3	Module=HD1x, Model=1032	1	12	N/A	N/A	200
11	11	minor(2)	alarm(1)	INRF	p2aindex.1.13.3	Module=HD1x, Model=1032	1	13	N/A	N/A	200
12	12	minor(2)	alarm(1)	INRF	p2aindex.1.14.3	Module=HD1x, Model=1032	1	14	N/A	N/A	200
13	13	minor(2)	alarm(1)	INRF	p2aindex.1.16.3	Module=HD1x, Model=1032	1	16	N/A	N/A	200
14	14	major(1)	alarm(1)	INPw	p2aindex.2.1.1	Module=P2HD-RF, Model=2015	2	1	N/A	N/A	200
15	15	major(1)	alarm(1)	Alarm	p2aindex.2.1.1	Module=P2HD-RF, Model=2015	2	1	N/A	N/A	200
16	16	major(1)	alarm(1)	INPw	p2aindex.2.2.1	Module=P2HD-RF, Model=2015	2	2	N/A	N/A	200
17	17	major(1)	alarm(1)	INPw	p2aindex.2.4.1	Module=P2HD-RF, Model=2015	2	4	N/A	N/A	200
18	18	major(1)	alarm(1)	INPw	p2aindex.2.5.1	Module=P2HD-RF, Model=2015	2	5	N/A	N/A	200
19	19	major(1)	alarm(1)	INPw	p2aindex.2.6.1	Module=P2HD-RF, Model=2015	2	6	N/A	N/A	200
20	20	major(1)	alarm(1)	INPw	p2aindex.2.7.1	Module=P2HD-RF, Model=2015	2	7	N/A	N/A	200
21	21	major(1)	alarm(1)	INPw	p2aindex.2.8.1	Module=P2HD-RF, Model=2015	2	8	N/A	N/A	200
22	22	major(1)	alarm(1)	INPw	p2aindex.2.9.1	Module=P2HD-RF, Model=2015	2	9	N/A	N/A	200
23	23	major(1)	alarm(1)	INPw	p2aindex.2.10.1	Module=P2HD-RF, Model=2015	2	10	N/A	N/A	200
24	24	major(1)	alarm(1)	INPw	p2aindex.2.11.1	Module=P2HD-RF, Model=2015	2	11	N/A	N/A	200
25	25	major(1)	alarm(1)	INPw	p2aindex.2.12.1	Module=P2HD-RF, Model=2015	2	12	N/A	N/A	200
26	26	major(1)	alarm(1)	INPw	p2aindex.2.13.1	Module=P2HD-RF, Model=2015	2	13	N/A	N/A	200
27	27	major(1)	alarm(1)	INPw	p2aindex.2.14.1	Module=P2HD-RF, Model=2015	2	14	N/A	N/A	200
28	28	major(1)	alarm(1)	INPw	p2aindex.2.15.1	Module=P2HD-RF, Model=2015	2	15	N/A	N/A	200
29	29	major(1)	alarm(1)	INPw	p2aindex.2.16.1	Module=P2HD-RF, Model=2015	2	16	N/A	N/A	200
30	30	major(1)	alarm(1)	INPw	p2aindex.2.17.1	Module=P2HD-RF, Model=2015	2	17	N/A	N/A	200
31	31	major(1)	alarm(1)	INPw	p2aindex.2.18.1	Module=P2HD-RF, Model=2015	2	18	N/A	N/A	200
32	32	major(1)	alarm(1)	INPw	p2aindex.2.19.1	Module=P2HD-RF, Model=2015	2	19	N/A	N/A	200
33	33	major(1)	alarm(1)	INPw	p2aindex.2.20.1	Module=P2HD-RF, Model=2015	2	20	N/A	N/A	200
34	34	major(1)	alarm(1)	INPw	p2aindex.2.21.1	Module=P2HD-RF, Model=2015	2	21	N/A	N/A	200
35	35	major(1)	alarm(1)	INPw	p2aindex.2.22.1	Module=P2HD-RF, Model=2015	2	22	N/A	N/A	200
36	36	major(1)	alarm(1)	INPw	p2aindex.2.23.1	Module=P2HD-RF, Model=2015	2	23	N/A	N/A	200
37	37	major(1)	alarm(1)	INPw	p2aindex.2.24.1	Module=P2HD-RF, Model=2015	2	24			

For additional information, see *Prisma II Traps* (on page 227), *Trap Logging Table* (on page 194), and *Enhanced Trap Binding Information* (on page 241).

10

Remote Firmware Download Feature

Introduction

The Prisma II Software Upgrade Program (SOUP) is a user-friendly utility that allows users to perform firmware upgrades on Prisma II modules. The SOUP utility simplifies the firmware upgrade process by providing a graphical user interface (GUI) that is easy to use and requires little training.

When connected to a chassis, the SOUP utility shows the user the current versions of firmware on all modules and allows the user to download and activate other versions from system release files. The SOUP works together with the ICIM2 or ICIM2-XD to send the binary image files and appropriate commands to the modules to upgrade their firmware. As the modules are being upgraded, the SOUP displays relevant progress information to the user.

In This Chapter

- Installing the SOUP 272
- Concepts 273
- Usage 275
- Firmware Updates 284

Installing the SOUP

To Install SOUP on Windows

Complete the following steps to install the Prisma II SOUP on Windows.

- 1 Download the Prisma II SOUP installation file to your Windows desktop.
- 2 Double-click the Prisma II SOUP installation icon to start the installation.
- 3 Follow the instructions of the installation wizard.
- 4 After the installation is complete, you will have an icon on the desktop to launch the SOUPLauncher application. There will also be a program group called Prisma II SOUP on your Start button menu.

To Uninstall the SOUP on Windows

Complete the following steps to remove the Prisma II SOUP from your computer.

- 1 Open the **Control Panel** from the Windows Start menu.
- 2 From the Control Panel, open the **Add or Remove Programs** application.
- 3 Find and choose the **Prisma II SOUP** entry in the list of installed programs. If the entry is not present, the program is not installed on the computer or was not installed properly.
- 4 Click the **Change/Remove** button.
- 5 Follow the instructions of the uninstall wizard.

Concepts

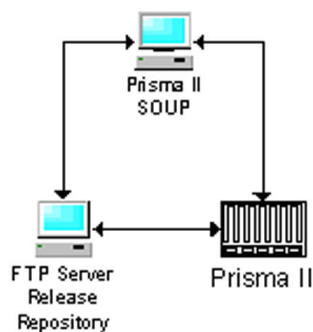
The Chassis and the ICIM2

The ICIM2 or ICIM2-XD acts as the communication interface to all modules in the chassis system. All communication with the chassis system from the SOUP program or the FTP server is managed by the ICIM2 or ICIM2-XD. The physical IP network connection for the chassis system is made through the Ethernet connector on the ICIM2 or ICIM2-XD front panel.

Release Files

The Prisma II SOUP works with system release files. A Prisma II system release contains binary image files for the modules that can be installed in the chassis.

System release files are held in a repository accessible through FTP. The Prisma II SOUP can access this repository to display information about available system releases and let the user choose among them. When the user selects a system release, the ICIM2 or ICIM2-XD retrieves the binary image files and upgrades the installed modules.



Note: Although shown separately above for clarity, the Prisma II SOUP and the FTP Server Release Repository may be resident on the same computer.

The format of a release file is explained in *Firmware Updates* (on page 284).

Active and Inactive Flash

The application modules have two flash memory areas, active and inactive. Each area can hold a copy of the module firmware. Module code always loads from active flash at boot-up. Inactive flash is used only for module firmware upgrades.

When upgrading firmware, the new version is downloaded to inactive flash. The module is then commanded to make the inactive flash active (and vice versa) and reboot, causing the new module code to load from the now active flash.

Concurrency

The upgrade process for a chassis depends on the number of modules in the chassis, the firmware versions that the modules are currently running, and the firmware versions that are currently being stored in the inactive flash area of each module.

The SOUP reads the current state of the modules in the chassis to determine what tasks are necessary to perform the upgrade, and then executes these tasks. For the upgrade process to work correctly, the state of the modules in the chassis must be fully known and not changed by another instance of the program running on a different system. This means that only one instance of the SOUP can be allowed to make any changes in a chassis at a time.

To enforce this, the SOUP attempts to grab a semaphore when it first connects to an ICIM2 or ICIM2-XD in a chassis. A semaphore is a control token that can only be grabbed by one instance of the SOUP at a time, and must be released before another instance can grab it. The attempt fails if the semaphore is already taken by another instance of the program running on another system and already connected to this ICIM2 or ICIM2-XD.

If the SOUP detects that the semaphore is taken, it does not attempt to make any changes to the modules in the chassis. Instead, it displays a message giving the user the option of proceeding in Browse Only mode. In Browse Only mode, the user is able to look at module information, but cannot download new firmware versions or change active or inactive flash areas.

Integration with an NMS (Optional)

The SOUP is designed to integrate into a network management system (NMS) that will handle permission security, access to the SOUP and its features, and actual launching of the SOUP utility.

When invoked, the SOUP requires a number of command line parameters to identify the ICIM2 or ICIM2-XD to be managed, the FTP server address, and the SNMP settings. Among these parameters is a security key that the NMS must retrieve from the ICIM2 or ICIM2-XD and pass to the SOUP.

If this parameter is not correct, or if the program is launched from the command line without it, the SOUP will only allow the user to run in Browse Only mode. In this mode, you can view information from the ICIM2 or ICIM2-XD and modules, but you cannot make changes.

Specifics on launching the SOUP utility vary from one NMS to another. Consult your system administrator for details on running the SOUP from your NMS.

Usage

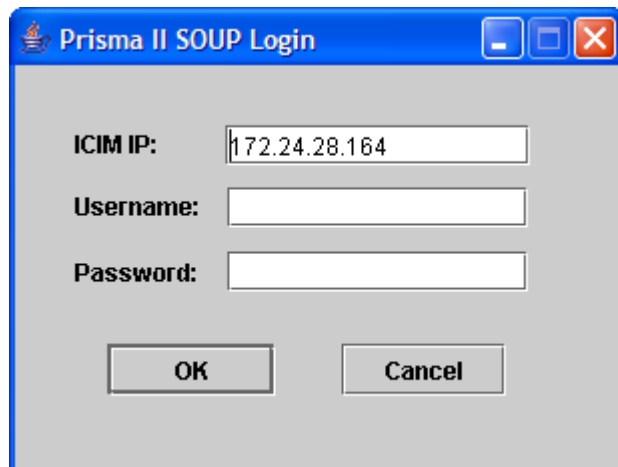
When launched, the SOUP utility first tries to connect to the ICIM2 or ICIM2-XD and retrieve information about the modules it manages. After retrieving the module information, the SOUP connects to the FTP server holding the system release files and retrieves the firmware versions available for each module. Information about new and existing module firmware is then displayed in the SOUP application main screen.

Launching Standalone (Windows Only)

A Windows program called SOUPLauncher also lets Admin users launch the Prisma II SOUP manually as a standalone application.

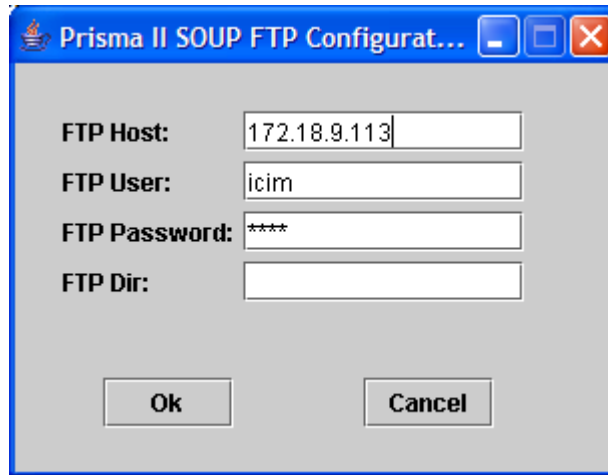
Complete the following steps to launch SOUP as a standalone application.

- 1 Open the Windows Start menu, open the Prisma II SOUP program group, and click the SOUPLauncher program item. The Prisma II SOUP Login window appears as shown in the following illustration.



- 2 In the ICIM IP: field, type the IP address of the ICIM2 or ICIM2-XD to receive the download.
 - 3 Type your Admin username and password in the fields provided.
- Note:** You must be an Admin user to log into the Prisma II SOUP.

- 4 Click **OK**. The Prisma II SOUP FTP Configuration window appears as shown in the following illustration.



Note: This window is bypassed after the first use of SOUPLauncher as long as the initial FTP server configuration remains valid.

- 5 In the FTP Host field, type the IP address of the FTP server to be used for the download.
- 6 In the FTP User and FTP Password fields, type the name and password of a user with permission to access files on the FTP server.
- 7 If the release files are in a folder rather than at the login root directory, type the name of the folder in the FTP Dir field.
If the release files are located at the login root directory, leave this field blank.
- 8 Click **OK** to launch the SOUP application.

After the Prisma II SOUP is running, you can change the FTP configuration if needed by accessing the FTP Server option from the Settings menu. See *FTP Settings* (on page 281) for details.

SOUP Main Screen

This screen serves as the control center for the SOUP utility. Most SOUP operations will be driven from here.

S	Chas #	Slot #	Module Description	Type #	Active Ver	Inactive Ver	Release Ver	Sugg Action
<input type="checkbox"/>	01	00	Fan Tray	5012	1.01.08	1.00.03	1.01.08	None
<input type="checkbox"/>	01	01	Power Supply 1 (Dual)	5013	N/A	N/A	N/A	N/A
<input type="checkbox"/>	01	05	1550nm EM TX FTTP	1031	1.68.00	1.65.00	1.68.00	None
<input type="checkbox"/>	01	06	1550nm EM TX FTTP	1031	1.68.00	1.65.00	1.68.00	None
<input type="checkbox"/>	01	07	1550nm Pre-Amp FTTP	3030	1.01.05	1.00.04	1.01.05	None
<input type="checkbox"/>	01	08	1550nm Pre-Amp FTTP	3030	1.01.05	1.00.04	1.01.05	None
<input type="checkbox"/>	01	09	Optical Switch FTTP	4011	1.01.04	1.00.03	1.01.04	None
<input type="checkbox"/>	01	10	1550nm Post-Amp FTTP	3031	1.01.04	1.00.03	1.01.04	None
<input type="checkbox"/>	01	13	Forward Receiver	2009	N/A	N/A	N/A	N/A
<input type="checkbox"/>	01	15	ICIM Module	5011	1.01.09	1.00.02	1.01.09	None
<input type="checkbox"/>	02	00	Fan Tray	5012	1.01.08	1.00.03	1.01.08	None
<input type="checkbox"/>	02	01	Power Supply 1 (Dual)	5013	N/A	N/A	N/A	N/A
<input type="checkbox"/>	02	05	1550nm Post-Amp FTTP	3031	1.01.04	1.00.03	1.01.04	None
<input type="checkbox"/>	02	07	1550nm Post-Amp FTTP	3031	1.01.04	1.00.03	1.01.04	None
<input type="checkbox"/>	02	09	1550nm Post-Amp FTTP	3031	1.01.04	1.00.03	1.01.04	None
<input type="checkbox"/>	02	11	1550nm Post-Amp FTTP	3031	1.01.04	1.00.03	1.01.04	None
<input type="checkbox"/>	02	13	1550nm Post-Amp FTTP	3031	1.01.04	1.00.03	1.01.04	None
<input type="checkbox"/>	02	15	1550nm Post-Amp FTTP	3031	1.01.04	1.00.03	1.01.04	None
<input type="checkbox"/>	03	00	Fan Tray	5012	1.01.08	1.00.03	1.01.08	None
<input type="checkbox"/>	03	01	Power Supply 1 (Dual)	5013	N/A	N/A	N/A	N/A
<input type="checkbox"/>	03	05	1550nm Post-Amp FTTP	3031	1.01.04	1.00.03	1.01.04	None
<input type="checkbox"/>	03	07	1550nm Post-Amp FTTP	3031	1.01.04	1.00.03	1.01.04	None
<input type="checkbox"/>	03	09	1550nm Post-Amp FTTP	3031	1.01.04	1.00.03	1.01.04	None
<input type="checkbox"/>	03	11	1550nm Post-Amp FTTP	3031	1.01.04	1.00.03	1.01.04	None
<input type="checkbox"/>	03	13	1550nm Post-Amp FTTP	3031	1.01.04	1.00.03	1.01.04	None
<input type="checkbox"/>	03	15	1550nm Post-Amp FTTP	3031	1.01.04	1.00.03	1.01.04	None
<input type="checkbox"/>	04	00	Fan Tray	5012	1.01.08	1.00.03	1.01.08	None
<input type="checkbox"/>	04	01	Power Supply 1 (Dual)	5013	N/A	N/A	N/A	N/A
<input type="checkbox"/>	04	05	1550nm Post-Amp FTTP	3031	1.01.04	1.00.03	1.01.04	None
<input type="checkbox"/>	04	07	1550nm Post-Amp FTTP	3031	1.01.04	1.00.03	1.01.04	None
<input type="checkbox"/>	04	09	1550nm Post-Amp FTTP	3031	1.01.04	1.00.03	1.01.04	None
<input type="checkbox"/>	04	11	1550nm Post-Amp FTTP	3031	1.01.04	1.00.03	1.01.04	None
<input type="checkbox"/>	04	13	1550nm Post-Amp FTTP	3031	1.01.04	1.00.03	1.01.04	None
<input type="checkbox"/>	04	15	1550nm Post-Amp FTTP	3031	1.01.04	1.00.03	1.01.04	None

The table below describes the information displayed in this screen.

Item	Description
ICIM IP Address	The address of the ICIM2 or ICIM2-XD currently connected. This is determined at utility startup and cannot be changed.
CLLI Code	The value of the p2icimCLLIcode SNMP element in the ICIM2 or ICIM2-XD.
Release File	The system release version and date of the current release file. Release files are listed in a drop-down box that the user can choose from to select the desired release.

Item	Description
Modules	<p>This table lists the modules and ICIM2 or ICIM2-XD present in the connected chassis. The table displays one row per module, with each row displaying details about the module.</p> <p>Each row in the table also displays:</p> <ul style="list-style-type: none"> ■ The firmware version contained in the release file for each module according to module type. ■ The Suggested Action, a value determined by the program as explained below.

Suggested Action

The SOUP utility determines a Suggested Action for each module by comparing the firmware version available in the system release file with the firmware version in the module Active and Inactive flash areas. The possible values for the Suggested Action are listed below.

Value	Description
None	No action needed; this module already holds the correct version of the firmware.
DnLoad + Activate	The module is not running the version of the firmware in the release file and that version is not available in the inactive flash. To upgrade the module, the program will need to first download the firmware to the inactive flash in the module, and then activate the firmware.
Activate	The module is not running the version of the firmware in the release file, but it is holding that version in its inactive flash. To upgrade the module, the program just needs to make the inactive flash active.
N/A	There is no information about this module in the system release file.

Screen Functions

The user can then initiate any of the following functions from the main screen.

Function	Description
Details (ICIM)	This function displays a dialog box containing additional details from the ICIM2 or ICIM2-XD to which the program is connected.
Details (Release File)	This function displays a dialog box containing additional details from the release file currently chosen.
Download	The download function looks at the selected modules in the Modules table and determines which ones need to have a new firmware binary image downloaded to their inactive flash. It then presents a dialog to the user with this list before starting the download process.

Function	Description
Activate	The activate function looks at the selected modules in the Modules table and checks that all the modules have a version that matches the release version in either their active or inactive flash. If this is not the case, the program displays an error and does not allow the user to proceed. If it is the case, the program creates a list of the modules whose flash areas will be switched, and then presents the list to the user before starting to send commands to the modules.
DnLoad + Activate	The download and activate function combines the two previous functions into a single step. When called, the program determines which modules need a new binary image download and which need to have their flash areas switched. The program then presents a combined list of modules to the user before proceeding.
Select	This function is a shortcut to select or clear a number of modules in one step. When the button is pressed, a menu is shown that allows the user to select or clear all modules, or to select all modules of a particular type.
Refresh	This function retrieves module information from the ICIM2 or ICIM2-XD and refreshes the Modules table.
Color Coding	Module rows are displayed in different colors to indicate the active, inactive, and current revisions.

Firmware Upgrade Process

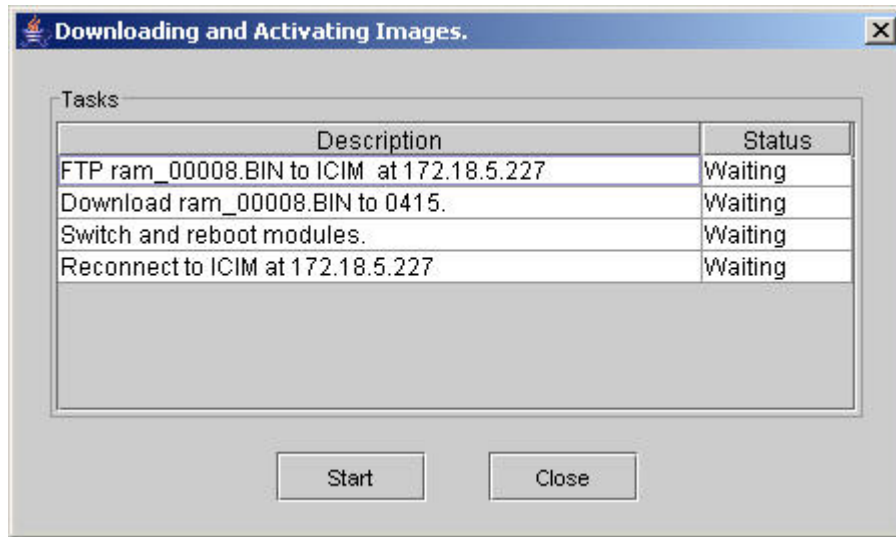
The procedure for upgrading the firmware in the ICIM2, ICIM2-XD, or application module has two main steps:

- Download the new firmware image to the module.
- Make the downloaded firmware image active.

These functions are available through the interface through the two buttons “Download” and “Activate.” They can also be combined into a single action using the “DnLoad + Activate” button.

When any of these functions is selected, the program first determines the tasks required by comparing the active and inactive firmware versions in the module flash areas to the version in the system release file. The list of tasks is then shown to the user in a dialog box, and the program waits for the user to respond.

For example, the task list displayed after the “DnLoad + Activate” button is pressed might appear as shown below.



This dialog shows the tasks necessary to upgrade the ICIM2 or ICIM2-XD to a new firmware version. These tasks are described individually below.

- 1 Transfer the file to the ICIM2 or ICIM2-XD memory. File transfer is done using FTP. The SOUP utility sends the FTP server information to the ICIM2 or ICIM2-XD and then commands it to download the file. The SOUP then polls the ICIM2 or ICIM2-XD until the file transfer is finished or an error occurs.
- 2 Transfer the file from the ICIM2 or ICIM2-XD memory to the inactive flash area of the target module. The SOUP will send the necessary commands to the ICIM2 or ICIM2-XD to start this transfer and then poll the ICIM2 or ICIM2-XD until the transfer is finished or an error occurs. Even when the module being upgraded is the ICIM2 or ICIM2-XD, the binary image still has to be downloaded from the ICIM2 or ICIM2-XD RAM to the inactive flash.
- 3 Switch the active flash pointer on the module and then tell the module to reboot. A module always has a pointer to the flash memory area that it will use to load its firmware on boot-up. After downloading the new image to the inactive flash area, the SOUP will first send a command to the module to switch the flash pointer. Then, it will send a command to reboot the module so that the new firmware is loaded. The reboot command used is a soft reboot, meaning that the module will not go through its full reboot process to minimize service interruption. The ICIM2 or ICIM2-XD performs a hard reboot.
- 4 If one of the modules is the ICIM2 or ICIM2-XD, as it is in this case, the SOUP loses contact with the chassis while rebooting. If the SOUP detects that one of the modules is the ICIM2 or ICIM2-XD, it waits after sending the reboot command until it regains its connection to the ICIM2 or ICIM2-XD.

FTP Settings

To upgrade firmware for Prisma II application modules, an FTP server is needed to transfer system release files and firmware binary images. When the Prisma II SOUP utility is launched from a network management system (NMS), information about the FTP server must be passed to it in the command line. When launched as a standalone application using SOUPLauncher, this information is requested from the user.

Specifically, the SOUP needs the FTP server address, the user and password to log into the server, and an optional subdirectory path for the location of the system release files. If the SOUP is running in Administrator level, you can look at and change these settings by first clicking on **Settings** in the main menu bar, and then choosing **FTP Server**.

A dialog box displaying the FTP server information opens, allowing you to change and test the settings.

The table below describes the fields in the FTP Settings dialog box.

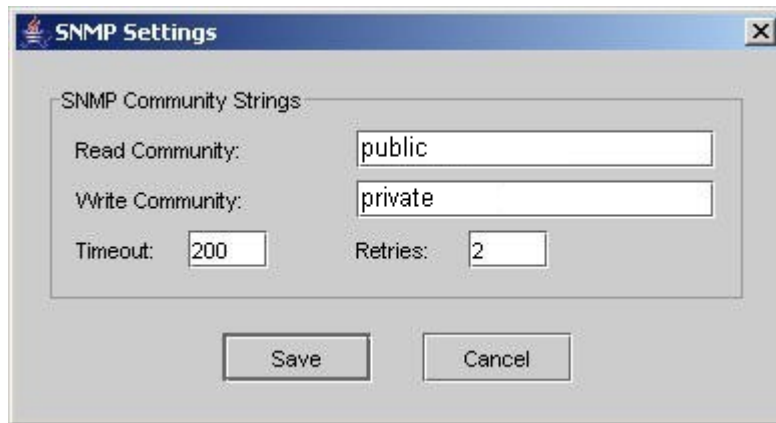
Item	Description
FTP Server Address	The address of the FTP server. This can be an IP address or a name that can be resolved by the computer running the SOUP.
Directory on FTP Server	The path to the system release files within the FTP server; for example, /dload/Prisma2 .
User	The user name to log into the FTP server.
Password	The password to log into the FTP server.

SNMP Settings

SNMP Settings are passed to the SOUP utility by an NMS as command line parameters. If launched using SOUPLauncher, this information is retrieved from the ICIM2 or ICIM2-XD after a successful login.

To connect to the ICIM2 through SNMP, the SOUP utility needs the SNMP Read and Write community strings. If the SOUP is running in Administrator mode, you can browse and change the SNMP settings by first clicking on **Settings** in the main menu bar, and then choosing **SNMP Settings**.

The SNMP Settings dialog appears as shown in the following illustration.



In addition to the Read and Write community strings, the Administrator can change:

- The timeout value (in milliseconds) to use when communicating with the ICIM2 or ICIM2-XD.
- The number of retries for SNMP messages.

These two settings are saved locally by the SOUP utility.

FTP Server

The SOUP utility and the ICIM2 work together with an FTP server to perform firmware upgrades. The FTP server makes the binary image files available to the ICIM2 and acts as a repository for system release files. The only requirement for the FTP server is that it be accessible through TCP/IP by both the SOUP and the ICIM2.

Consult your system administrator for details on how to configure an FTP server for this application.

Firmware Updates

New system release files are distributed when a firmware update becomes available. System release files package the firmware binary images for the different modules and provide version information for those images. These files are produced and distributed by the manufacturer, and are not intended to be created or modified by end users in any manner.

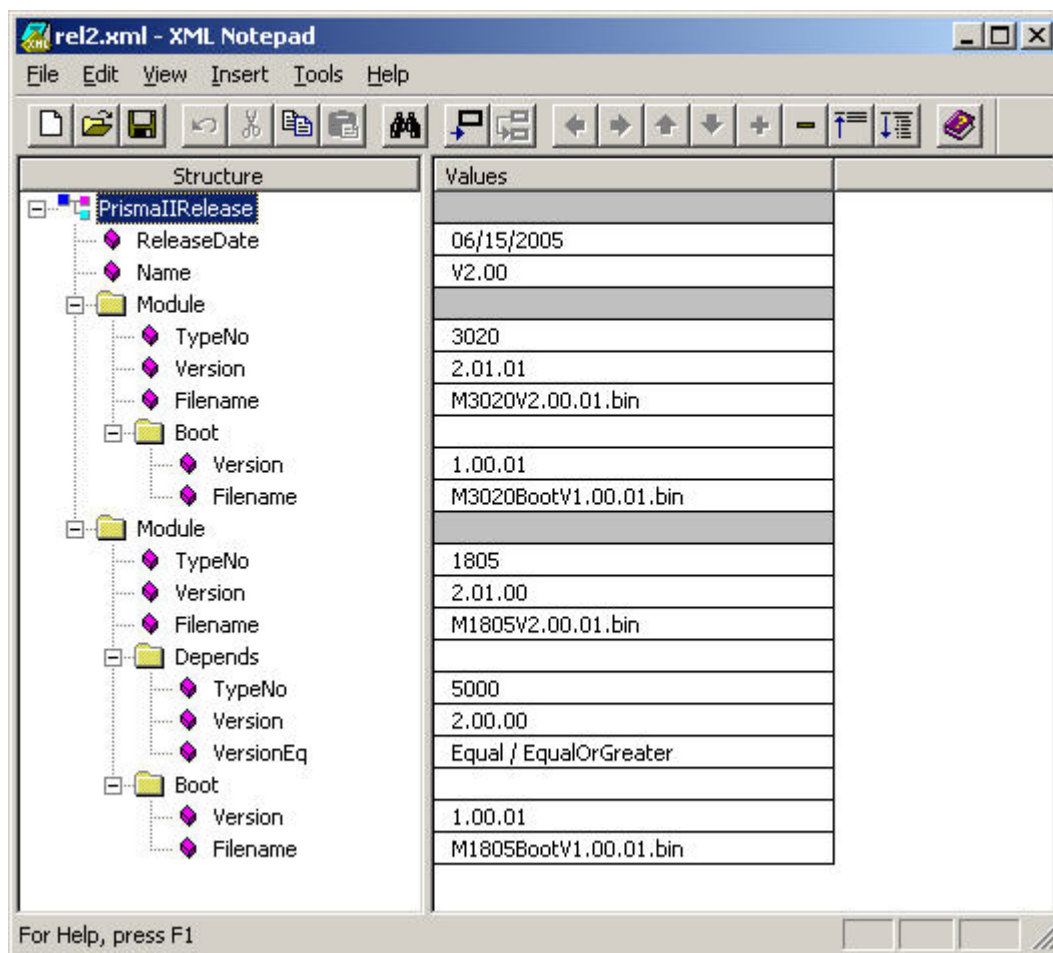
**CAUTION:**

Do not try to perform a firmware update that would result in downgrading ICIM2 or ICIM2-XD firmware below system release 2.02.09. Earlier system releases may incorrectly identify the ICIM2 or ICIM2-XD slot number and fail to connect with the ICIM2 or ICIM2-XD when completing the download.

The following is a sample system release file. The information contained in the XML file is listed in the table below.

Item	Description
PrismaIIRelease	The root element in the file identifies this to be a Prisma II system release file.
ReleaseDate	The official release date.
Name	A descriptive name for the system release, typically a system version number.

Item	Description
Module	<p data-bbox="574 268 1386 365">One or more module elements containing information about the versions contained in this system release file for a particular module type.</p> <ul style="list-style-type: none"> <li data-bbox="574 386 1127 415">■ TypeNo – The target module type number. <li data-bbox="574 436 1256 466">■ Version – The version of the firmware for the module. <li data-bbox="574 487 1386 550">■ Filename – The file name of the binary image holding the module firmware. <li data-bbox="574 571 1386 1184"> <ul style="list-style-type: none"> <li data-bbox="574 571 1386 667">■ Boot – An element containing information about the boot image necessary to run this version of the firmware. (ICIM2 or ICIM2-XD only) <ul style="list-style-type: none"> <li data-bbox="623 680 1127 709">– Version – The version of the boot image. <li data-bbox="623 722 1273 751">– Filename – The file name that holds the boot image. <li data-bbox="574 772 1386 932">■ Depends – An optional element containing information about dependencies of this version of the firmware to other modules and their version. These elements are used to make sure that when an upgrade is performed, any dependencies across modules are enforced. <ul style="list-style-type: none"> <li data-bbox="623 945 1321 974">– TypeNo – The type number of the module depended on. <li data-bbox="623 987 1305 1050">– Version – The version of the firmware necessary in the module on which it depends. <li data-bbox="623 1062 1386 1184">– VersionEq – A comparison operator to use when looking at the version in the module. This can either be Equal for strict equality, or EqualOrGreater to accept a matching or newer version.



Structure	Values
PrismaIIRelease	
ReleaseDate	06/15/2005
Name	V2.00
Module	
TypeNo	3020
Version	2.01.01
Filename	M3020V2.00.01.bin
Boot	
Version	1.00.01
Filename	M3020BootV1.00.01.bin
Module	
TypeNo	1805
Version	2.01.00
Filename	M1805V2.00.01.bin
Depends	
TypeNo	5000
Version	2.00.00
VersionEq	Equal / EqualOrGreater
Boot	
Version	1.00.01
Filename	M1805BootV1.00.01.bin

For Help, press F1

11

Maintenance and Troubleshooting

Introduction

This chapter provides information to assist you in maintaining and troubleshooting the platform.

Qualified Personnel

Only appropriately qualified and skilled personnel should attempt to maintain or troubleshoot chassis faults.



WARNING:

Allow only qualified and skilled personnel to install, operate, maintain, and service these products. Otherwise, personal injury or equipment damage may occur.

In This Chapter

■ Maintenance	289
■ Troubleshooting	290
■ Fan Ok Alarms	292
■ ChasTemp Alarm.....	293
■ ConvAIn Alarm.....	294
■ ConvA+24 Alarm.....	295
■ ConvA+5 Alarm.....	297
■ ConvA-5 Alarm.....	299
■ ConvBIn Alarm	301
■ ConvB+24 Alarm	302
■ ConvB+5 Alarm	304
■ ConvB-5 Alarm.....	306
■ Cleaning Optical Connectors	308
■ Connecting Optical Cables	312

Maintenance

The following maintenance is recommended to ensure optimal performance.

Frequency	Maintenance Required
Yearly	<ul style="list-style-type: none"> ■ Check all parameters and test points. ■ Record data. ■ Make adjustments as needed. ■ Make sure all cables are mated properly. ■ Inspect cables for stress and chafing. ■ Make sure all retaining screws are tight. ■ Replace chassis air filter. Depending on office environment cleanliness/filtration, the chassis air filter may require more frequent servicing.
When needed	Carefully clean the module with a soft cloth that is dampened with mild detergent.

Maintenance Record

It may be helpful to establish a maintenance record or log for this equipment. You may want to record laser power level, laser temperature readings, laser bias current, or power supply voltages, as well as the filter change dates.

Large variations in any of the parameters above should be investigated prior to failure.

Troubleshooting

This section provides general information on servicing and troubleshooting this equipment. The troubleshooting information describes the most common alarms and gives typical symptoms, causes, and items to check before contacting Customer Service.

Chassis Troubleshooting

The main function of the chassis is to distribute power and establish communication links for the application modules installed in the chassis. Most troubleshooting involves the modules installed in the chassis, but in some instances, you will need to troubleshoot the chassis itself.

The table below describes the most common problems and gives typical symptoms, possible causes, and items to check before contacting Customer Service.



WARNING:

Avoid electric shock and damage to this product! Do not open the enclosure of this product. There are no user-serviceable parts inside. Refer servicing to qualified service personnel.

Symptom	Possible Causes	Solutions
ON indicator is not illuminated	Power supply connection loose	Check that all power supply connections are secure.
	Loss of system power	Check that power is present at receptacle.
	Power failure; backup in use	Check other displays and indicators for power indication.
	Module indicator burned out	Contact Customer Service for an indicator replacement.
ALARM indicator is on or flashing	Application module in alarm	Consult NMS for module alarms (see module documentation for details).
	Chassis failed power-up self-test	Check that all power supply connections are secure. Check AC OK and DC OK LED indicators on power supplies.

ICIM indicator is off	ICIM not installed or not fully seated	Confirm that chassis is part of an ICIM2 or ICIM2-XD daisy chain (no need for separate ICIM2 or ICIM2-XD). If not, check that ICIM2-XD is fully seated in back of chassis.
-----------------------	--	---

Alarm Troubleshooting

The Prisma II XD Platform generates certain alarms that are specific to the chassis, its fan assembly, and its power supply components.

Parameter	Function
Fan 1_Ok	Fan 1 operating status
Fan 2_Ok	Fan 2 operating status
Fan 3_Ok	Fan 3 operating status
ChasTemp	Chassis internal temperature
ConvAIn	DC-to-DC converter A -48 VDC input
ConvA+24	DC-to-DC converter A +24 VDC output
ConvA+5	DC-to-DC converter A +5 VDC output
ConvA-5	DC-to-DC converter A -5 VDC output
ConvBIn	DC-to-DC converter B-48 VDC input
ConvB+24	DC-to-DC converter B +24 VDC output
ConvB+5	DC-to-DC converter B +5 VDC output
ConvB-5	DC-to-DC converter B -5 VDC output

Troubleshooting information for each of these alarms is provided in the following sections of this chapter.

Other alarms may occur as a result of fault conditions in specific application modules. For information on troubleshooting alarms for specific application modules, see the appropriate module documentation.

Additional Assistance

If you need additional assistance, telephone one of our Technical Service Centers or your local sales subsidiary. The chapter *Customer Support Information* (on page 313) contains a list of telephone numbers.

Fan Ok Alarms

The Fan Ok alarms (Fan 1_Ok, Fan 2_Ok, Fan 3_Ok) indicate a problem with the function of the three fans in the fan assembly. Each alarm triggers when its corresponding fan is inoperative, whether due to failure of the fan itself or to a disconnected or broken wiring harness.

Fan Alarm Parameters

Alarm	Function	Major Low Threshold	Minor Low Threshold	Minor High Threshold	Major High Threshold	Hysteresis	Typical Range/ Nom. Value
Fan 1_Ok	Fan 1 status	na	na	na	na	na	OK or Fault
Fan 2_Ok	Fan 2 status	na	na	na	na	na	OK or Fault
Fan 3_Ok	Fan 3 status	na	na	na	na	na	OK or Fault

Suggested Actions

- 1 Check for obstruction causing lack of rotation on fan in alarm. If present, rectify condition.
- 2 If no obstruction, remove fan assembly and check for breaks in fan wiring or loose connectors.
- 3 If all fan wiring is intact and one or more fans do not rotate, replace fan assembly.



CAUTION:

For a chassis under power, field replacement of the fans, AC-to-DC bulk power supply modules, or DC-to-DC converter assemblies must be completed in two minutes or less to prevent possible chassis overheating due to temporary removal of the fan assembly.

- 4 If these steps do not clear the alarm, contact Customer Service for assistance.

ChasTemp Alarm

This alarm indicates a problem with fan temperature. It triggers when the chassis internal temperature is outside the threshold levels.

ChasTemp Alarm Parameters

Alarm	Function	Major Low Threshold	Minor Low Threshold	Minor High Threshold	Major High Threshold	Hysteresis	Typical Range/ Nom. Value
ChasTemp	chassis internal temperature	-40°C	-35°C	60°C	65°C	1°C	-40°C to 65°C

The factory default range for ChasTemp is -40°C to 65°C. While these values can be user-adjustable, they must be left at the default values. Failure to do so may result in improper operation or alarming, or may lead to equipment damage.

Suggested Actions

- 1 Verify that the conditioned ambient airflow is within chassis temperature alarm threshold set-points. If not, rectify the condition.
- 2 Look for and remove any air flow obstructions at the chassis air intake and exhaust areas. *Momentary* fan assembly removal may be needed for this inspection.



CAUTION:

For a chassis under power, field replacement of the fans, AC-to-DC bulk power supply modules, or DC-to-DC converter assemblies must be completed in two minutes or less to prevent possible chassis overheating due to temporary removal of the fan assembly.

- 3 If these steps do not clear the alarm, contact Customer Service for assistance.

ConvAln Alarm

This alarm indicates one or more of the following conditions:

- Absence of AC input power to the AC-to-DC bulk power supply module in slot A, if present
- Absence of DC input power to the DC-to-DC converter module for power supply slot A
- Absence of DC-to-DC converter module for power supply slot A

Note: This alarm can be temporarily disabled for servicing by setting the AlmMuteA control parameter to 1 (ON) via the CLI or ICIM Web Interface. See the *Prisma II Platform Remote User Interface Guide, System Release 2.03*, part number 4025477 for details.

ConvAln Alarm Parameters

Alarm	Function	Major Low Threshold	Minor Low Threshold	Minor High Threshold	Major High Threshold	Hysteresis	Typical Range/ Nom. Value
ConvAln	Slot A power status	na	na	na	na	na	OK or Fault

Suggested Actions

- 1 Check the chassis power cord and confirm that the alarming AC-to-DC bulk power supply module is fully seated.
- 2 If the line voltage is feeding only the alarming power supply, check the line for both proper voltage *and* polarity. If the line voltage and polarity are acceptable, replace the power supply module.
- 3 If the line voltage is feeding more than one chassis with no indication of alarm on any other power supply, replace the alarming power supply module.
- 4 If these steps do not clear the alarm, contact Customer Service for assistance.

ConvA+24 Alarm

This alarm indicates the status of the +24 VDC output voltage from the DC-to-DC converter in slot A of the chassis. It triggers when this output voltage is outside the threshold levels.

ConvA+24 Alarm Parameters

Alarm	Function	Major Low Threshold	Minor Low Threshold	Minor High Threshold	Major High Threshold	Hysteresis	Typical Range/ Nom. Value
ConvA+24	DC-to-DC Converter Slot A +24 VDC output voltage	18.0 V DC	18.4 V DC	25.9 V DC	26.1 V DC	0.1 V DC	23.8 to 25.6 V DC

While the threshold values can be user-adjustable, they must be left at the default values. Failure to do so may result in improper operation or alarming, or may lead to equipment damage.

Suggested Actions

- 1 Access the DC-to-DC converter in alarm as described below, and confirm that it is fully seated. If necessary, reseal the converter.
- 2 Check that the status LED of the converter in alarm is unlit. If the LED is lit, replace the converter.
- 3 Confirm that the alarm is caused by the voltage exceeding or falling below *factory-set* threshold values. If so, replace the converter.
- 4 If these steps do not clear the alarm, contact Customer Service for assistance.

To Access the DC-to-DC Converter

Complete the following steps to access the DC-to-DC converter for inspection or replacement.



CAUTION:

- Before removing an AC-to-DC bulk power supply module from the chassis, disable AC input power to the module by disconnecting the associated AC power cord.
- Before removing a DC-to-DC converter assembly from the chassis, disable DC input power to the converter assembly by disconnecting the associated AC power cord (if AC operated) or DC power-passing cable (if DC operated).
- Do not disable power to both sides of the chassis at the same time when such action may cause a loss of service.



CAUTION:

For a chassis under power, field replacement of the fans, AC-to-DC bulk power supply modules, or DC-to-DC converter assemblies must be completed in two minutes or less to prevent possible chassis overheating due to temporary removal of the fan assembly.

- 1 Using the CLI or ICIM Web Interface, temporarily set AlmMuteA or AlmMuteB to 1 (ON) to mute any alarms from the power supply section to be serviced. See the *Prisma II Platform Remote User Interface Guide, System Release 2.03*, part number 4025477 for details.
- 2 Temporarily disconnect AC or DC power from the power supply section being serviced.
- 3 Remove the fan assembly from the chassis and set it aside.
- 4 Locate the DC-to-DC converter assemblies mounted horizontally on a ledge inside the fan assembly opening. The converter on the left side is for power supply section A, while the converter on the right is for power supply section B.
- 5 To remove a DC-to-DC converter, grasp both edges and pull gently until the converter board disengages from the midplane bus. Then slide the converter board out of the chassis.
- 6 To reinsert a DC-to-DC converter, slide the converter board into the chassis until it rests against with the connector on the midplane bus. Then push the converter firmly into the midplane connector.
- 7 Reinstall the fan assembly.
- 8 Reconnect AC or DC power to the power supply section being serviced.
- 9 Set AlmMuteA or AlmMuteB to 0 (OFF) to enable alarms from the power supply section.

ConvA+5 Alarm

This alarm indicates the status of the +5 VDC output voltage from the DC-to-DC converter in slot A of the chassis. It triggers when this output voltage is outside the threshold levels.

ConvA+5 Alarm Parameters

Alarm	Function	Major Low Threshold	Minor Low Threshold	Minor High Threshold	Major High Threshold	Hysteresis	Typical Range/ Nom. Value
ConvA+5	DC-to-DC Converter Slot A +5 VDC output voltage	3.6 V DC	3.7 V DC	5.9 V DC	6.1 V DC	0.1 V DC	4.9 to 5.3 V DC

While the threshold values can be user-adjustable, they must be left at the default values. Failure to do so may result in improper operation or alarming, or may lead to equipment damage.

Suggested Actions

- 1 Access the DC-to-DC converter in alarm as described below, and confirm that it is fully seated. If necessary, reseal the converter.
- 2 Check that the status LED of the converter in alarm is unlit. If the LED is lit, replace the converter.
- 3 Confirm that the alarm is caused by the voltage exceeding or falling below *factory-set* threshold values. If so, replace the converter.
- 4 If these steps do not clear the alarm, contact Customer Service for assistance.

To Access the DC-to-DC Converter

Complete the following steps to access the DC-to-DC converter for inspection or replacement.



CAUTION:

- Before removing an AC-to-DC bulk power supply module from the chassis, disable AC input power to the module by disconnecting the associated AC power cord.
- Before removing a DC-to-DC converter assembly from the chassis, disable DC input power to the converter assembly by disconnecting the associated AC power cord (if AC operated) or DC power-passing cable (if DC operated).
- Do not disable power to both sides of the chassis at the same time when such action may cause a loss of service.



CAUTION:

For a chassis under power, field replacement of the fans, AC-to-DC bulk power supply modules, or DC-to-DC converter assemblies must be completed in two minutes or less to prevent possible chassis overheating due to temporary removal of the fan assembly.

- 1 Using the CLI or ICIM Web Interface, temporarily set AlmMuteA or AlmMuteB to 1 (ON) to mute any alarms from the power supply section to be serviced. See the *Prisma II Platform Remote User Interface Guide, System Release 2.03*, part number 4025477 for details.
- 2 Temporarily disconnect AC or DC power from the power supply section being serviced.
- 3 Remove the fan assembly from the chassis and set it aside.
- 4 Locate the DC-to-DC converter assemblies mounted horizontally on a ledge inside the fan assembly opening. The converter on the left side is for power supply section A, while the converter on the right is for power supply section B.
- 5 To remove a DC-to-DC converter, grasp both edges and pull gently until the converter board disengages from the midplane bus. Then slide the converter board out of the chassis.
- 6 To reinsert a DC-to-DC converter, slide the converter board into the chassis until it rests against with the connector on the midplane bus. Then push the converter firmly into the midplane connector.
- 7 Reinstall the fan assembly.
- 8 Reconnect AC or DC power to the power supply section being serviced.
- 9 Set AlmMuteA or AlmMuteB to 0 (OFF) to enable alarms from the power supply section.

ConvA-5 Alarm

This alarm indicates the status of the -5 VDC output voltage from the DC-to-DC converter in slot A of the chassis. It triggers when this output voltage is outside the threshold levels.

ConvA-5 Alarm Parameters

Alarm	Function	Major Low Threshold	Minor Low Threshold	Minor High Threshold	Major High Threshold	Hysteresis	Typical Range/ Nom. Value
ConvA-5	DC-to-DC Converter Slot A -5 VDC output voltage	-5.6 V DC	-5.5 V DC	-4.6 V DC	-4.5 V DC	0.1 V DC	-5.3 to -4.9 V DC

While the threshold values can be user-adjustable, they must be left at the default values. Failure to do so may result in improper operation or alarming, or may lead to equipment damage.

Suggested Actions

- 1 Access the DC-to-DC converter in alarm as described below, and confirm that it is fully seated. If necessary, reseal the converter.
- 2 Check that the status LED of the converter in alarm is unlit. If the LED is lit, replace the converter.
- 3 Confirm that the alarm is caused by the voltage exceeding or falling below *factory-set* threshold values. If so, replace the converter.
- 4 If these steps do not clear the alarm, contact Customer Service for assistance.

To Access the DC-to-DC Converter

Complete the following steps to access the DC-to-DC converter for inspection or replacement.



CAUTION:

- Before removing an AC-to-DC bulk power supply module from the chassis, disable AC input power to the module by disconnecting the associated AC power cord.
- Before removing a DC-to-DC converter assembly from the chassis, disable DC input power to the converter assembly by disconnecting the associated AC power cord (if AC operated) or DC power-passing cable (if DC operated).
- Do not disable power to both sides of the chassis at the same time when such action may cause a loss of service.



CAUTION:

For a chassis under power, field replacement of the fans, AC-to-DC bulk power supply modules, or DC-to-DC converter assemblies must be completed in two minutes or less to prevent possible chassis overheating due to temporary removal of the fan assembly.

- 1 Using the CLI or ICIM Web Interface, temporarily set AlmMuteA or AlmMuteB to 1 (ON) to mute any alarms from the power supply section to be serviced. See the *Prisma II Platform Remote User Interface Guide, System Release 2.03*, part number 4025477 for details.
- 2 Temporarily disconnect AC or DC power from the power supply section being serviced.
- 3 Remove the fan assembly from the chassis and set it aside.
- 4 Locate the DC-to-DC converter assemblies mounted horizontally on a ledge inside the fan assembly opening. The converter on the left side is for power supply section A, while the converter on the right is for power supply section B.
- 5 To remove a DC-to-DC converter, grasp both edges and pull gently until the converter board disengages from the midplane bus. Then slide the converter board out of the chassis.
- 6 To reinsert a DC-to-DC converter, slide the converter board into the chassis until it rests against with the connector on the midplane bus. Then push the converter firmly into the midplane connector.
- 7 Reinstall the fan assembly.
- 8 Reconnect AC or DC power to the power supply section being serviced.
- 9 Set AlmMuteA or AlmMuteB to 0 (OFF) to enable alarms from the power supply section.

ConvBIn Alarm

This alarm indicates one or more of the following conditions:

- Absence of AC input power to the AC-to-DC bulk power supply module in slot B, if present
- Absence of DC input power to the DC-to-DC converter module for power supply slot B
- Absence of DC-to-DC converter module for power supply slot B

Note: This alarm can be temporarily disabled for servicing by setting the AlmMuteB control parameter to 1 (ON) via the CLI or ICIM Web Interface. See the *Prisma II Platform Remote User Interface Guide, System Release 2.03*, part number 4025477 for details.

ConvBIn Alarm Parameters

Alarm	Function	Major Low Threshold	Minor Low Threshold	Minor High Threshold	Major High Threshold	Hysteresis	Typical Range/Nom. Value
ConvBIn	Slot B power status	na	na	na	na	na	OK or Fault

Suggested Actions

- 1 Check the chassis power cord and confirm that the alarming AC-to-DC bulk power supply module is fully seated.
- 2 If the line voltage is feeding only the alarming power supply, check the line for both proper voltage *and* polarity. If the line voltage and polarity are acceptable, replace the power supply module.
- 3 If the line voltage is feeding more than one chassis with no indication of alarm on any other power supply, replace the alarming power supply module.
- 4 If these steps do not clear the alarm, contact Customer Service for assistance.

ConvB+24 Alarm

This alarm indicates the status of the +24 VDC output voltage from the DC-to-DC converter in slot B of the chassis. It triggers when this output voltage is outside the threshold levels.

ConvB+24 Alarm Parameters

Alarm	Function	Major Low Threshold	Minor Low Threshold	Minor High Threshold	Major High Threshold	Hysteresis	Typical Range/ Nom. Value
ConvB+24	DC-to-DC Converter Slot B +24 VDC output voltage	18.0 V DC	18.4 V DC	25.9 V DC	26.1 V DC	0.1 V DC	23.8 to 25.6 V DC

While the threshold values can be user-adjustable, they must be left at the default values. Failure to do so may result in improper operation or alarming, or may lead to equipment damage.

Suggested Actions

- 1 Access the DC-to-DC converter in alarm as described below, and confirm that it is fully seated. If necessary, reseal the converter.
- 2 Check that the status LED of the converter in alarm is unlit. If the LED is lit, replace the converter.
- 3 Confirm that the alarm is caused by the voltage exceeding or falling below *factory-set* threshold values. If so, replace the converter.
- 4 If these steps do not clear the alarm, contact Customer Service for assistance.

To Access the DC-to-DC Converter

Complete the following steps to access the DC-to-DC converter for inspection or replacement.

**CAUTION:**

- Before removing an AC-to-DC bulk power supply module from the chassis, disable AC input power to the module by disconnecting the associated AC power cord.
- Before removing a DC-to-DC converter assembly from the chassis, disable DC input power to the converter assembly by disconnecting the associated AC power cord (if AC operated) or DC power-passing cable (if DC operated).
- Do not disable power to both sides of the chassis at the same time when such action may cause a loss of service.

**CAUTION:**

For a chassis under power, field replacement of the fans, AC-to-DC bulk power supply modules, or DC-to-DC converter assemblies must be completed in two minutes or less to prevent possible chassis overheating due to temporary removal of the fan assembly.

- 1 Using the CLI or ICIM Web Interface, temporarily set AlmMuteA or AlmMuteB to 1 (ON) to mute any alarms from the power supply section to be serviced. See the *Prisma II Platform Remote User Interface Guide, System Release 2.03*, part number 4025477 for details.
- 2 Temporarily disconnect AC or DC power from the power supply section being serviced.
- 3 Remove the fan assembly from the chassis and set it aside.
- 4 Locate the DC-to-DC converter assemblies mounted horizontally on a ledge inside the fan assembly opening. The converter on the left side is for power supply section A, while the converter on the right is for power supply section B.
- 5 To remove a DC-to-DC converter, grasp both edges and pull gently until the converter board disengages from the midplane bus. Then slide the converter board out of the chassis.
- 6 To reinsert a DC-to-DC converter, slide the converter board into the chassis until it rests against with the connector on the midplane bus. Then push the converter firmly into the midplane connector.
- 7 Reinstall the fan assembly.
- 8 Reconnect AC or DC power to the power supply section being serviced.
- 9 Set AlmMuteA or AlmMuteB to 0 (OFF) to enable alarms from the power supply section.

ConvB+5 Alarm

This alarm indicates the status of the +5 VDC output voltage from the DC-to-DC converter in slot B of the chassis. It triggers when this output voltage is outside the threshold levels.

ConvB+5 Alarm Parameters

Alarm	Function	Major Low Threshold	Minor Low Threshold	Minor High Threshold	Major High Threshold	Hysteresis	Typical Range/ Nom. Value
ConvB+5	DC-to-DC Converter Slot B +5 VDC output voltage	3.6 V DC	3.7 V DC	5.9 V DC	6.1 V DC	0.1 V DC	4.9 to 5.3 V DC

While the threshold values can be user-adjustable, they must be left at the default values. Failure to do so may result in improper operation or alarming, or may lead to equipment damage.

Suggested Actions

- 1 Access the DC-to-DC converter in alarm as described below, and confirm that it is fully seated. If necessary, reseal the converter.
- 2 Check that the status LED of the converter in alarm is unlit. If the LED is lit, replace the converter.
- 3 Confirm that the alarm is caused by the voltage exceeding or falling below *factory-set* threshold values. If so, replace the converter.
- 4 If these steps do not clear the alarm, contact Customer Service for assistance.

To Access the DC-to-DC Converter

Complete the following steps to access the DC-to-DC converter for inspection or replacement.

**CAUTION:**

- Before removing an AC-to-DC bulk power supply module from the chassis, disable AC input power to the module by disconnecting the associated AC power cord.
- Before removing a DC-to-DC converter assembly from the chassis, disable DC input power to the converter assembly by disconnecting the associated AC power cord (if AC operated) or DC power-passing cable (if DC operated).
- Do not disable power to both sides of the chassis at the same time when such action may cause a loss of service.

**CAUTION:**

For a chassis under power, field replacement of the fans, AC-to-DC bulk power supply modules, or DC-to-DC converter assemblies must be completed in two minutes or less to prevent possible chassis overheating due to temporary removal of the fan assembly.

- 1 Using the CLI or ICIM Web Interface, temporarily set AlmMuteA or AlmMuteB to 1 (ON) to mute any alarms from the power supply section to be serviced. See the *Prisma II Platform Remote User Interface Guide, System Release 2.03*, part number 4025477 for details.
- 2 Temporarily disconnect AC or DC power from the power supply section being serviced.
- 3 Remove the fan assembly from the chassis and set it aside.
- 4 Locate the DC-to-DC converter assemblies mounted horizontally on a ledge inside the fan assembly opening. The converter on the left side is for power supply section A, while the converter on the right is for power supply section B.
- 5 To remove a DC-to-DC converter, grasp both edges and pull gently until the converter board disengages from the midplane bus. Then slide the converter board out of the chassis.
- 6 To reinsert a DC-to-DC converter, slide the converter board into the chassis until it rests against with the connector on the midplane bus. Then push the converter firmly into the midplane connector.
- 7 Reinstall the fan assembly.
- 8 Reconnect AC or DC power to the power supply section being serviced.
- 9 Set AlmMuteA or AlmMuteB to 0 (OFF) to enable alarms from the power supply section.

ConvB-5 Alarm

This alarm indicates the status of the -5 VDC output voltage from the DC-to-DC converter in slot B of the chassis. It triggers when this output voltage is outside the threshold levels.

ConvB-5 Alarm Parameters

Alarm	Function	Major Low Threshold	Minor Low Threshold	Minor High Threshold	Major High Threshold	Hysteresis	Typical Range/ Nom. Value
ConvB-5	DC-to-DC Converter Slot B -5 VDC output voltage	-5.6 V DC	-5.5 V DC	-4.6 V DC	-4.5 V DC	0.1 V DC	-5.3 to -4.9 V DC

While the threshold values can be user-adjustable, they must be left at the default values. Failure to do so may result in improper operation or alarming, or may lead to equipment damage.

Suggested Actions

- 1 Access the DC-to-DC converter in alarm as described below, and confirm that it is fully seated. If necessary, reseal the converter.
- 2 Check that the status LED of the converter in alarm is unlit. If the LED is lit, replace the converter.
- 3 Confirm that the alarm is caused by the voltage exceeding or falling below *factory-set* threshold values. If so, replace the converter.
- 4 If these steps do not clear the alarm, contact Customer Service for assistance.

To Access the DC-to-DC Converter

Complete the following steps to access the DC-to-DC converter for inspection or replacement.

**CAUTION:**

- Before removing an AC-to-DC bulk power supply module from the chassis, disable AC input power to the module by disconnecting the associated AC power cord.
- Before removing a DC-to-DC converter assembly from the chassis, disable DC input power to the converter assembly by disconnecting the associated AC power cord (if AC operated) or DC power-passing cable (if DC operated).
- Do not disable power to both sides of the chassis at the same time when such action may cause a loss of service.

**CAUTION:**

For a chassis under power, field replacement of the fans, AC-to-DC bulk power supply modules, or DC-to-DC converter assemblies must be completed in two minutes or less to prevent possible chassis overheating due to temporary removal of the fan assembly.

- 1 Using the CLI or ICIM Web Interface, temporarily set AlmMuteA or AlmMuteB to 1 (ON) to mute any alarms from the power supply section to be serviced. See the *Prisma II Platform Remote User Interface Guide, System Release 2.03*, part number 4025477 for details.
- 2 Temporarily disconnect AC or DC power from the power supply section being serviced.
- 3 Remove the fan assembly from the chassis and set it aside.
- 4 Locate the DC-to-DC converter assemblies mounted horizontally on a ledge inside the fan assembly opening. The converter on the left side is for power supply section A, while the converter on the right is for power supply section B.
- 5 To remove a DC-to-DC converter, grasp both edges and pull gently until the converter board disengages from the midplane bus. Then slide the converter board out of the chassis.
- 6 To reinsert a DC-to-DC converter, slide the converter board into the chassis until it rests against with the connector on the midplane bus. Then push the converter firmly into the midplane connector.
- 7 Reinstall the fan assembly.
- 8 Reconnect AC or DC power to the power supply section being serviced.
- 9 Set AlmMuteA or AlmMuteB to 0 (OFF) to enable alarms from the power supply section.

Cleaning Optical Connectors

Note: The proper procedure for cleaning optical connectors depends on the connector type. The following describes general instructions for cleaning optical connectors. Many companies have established procedures for cleaning conductors which should be followed. If your company has established procedures, the following instructions should be considered along with your procedures.

Cleaning fiber-optic connectors can help prevent interconnect problems and aid system performance. When optical connectors are disconnected or reconnected, the fiber surface can become dirty or scratched. If not addressed, this dirt or damage may lead to interconnect problems and reduced system performance.

Fiber-optic connectors should be inspected prior to mating and cleaned as needed to remove all dust and contaminants without leaving any residue. Connectors should be visually inspected after cleaning to confirm that they are clean and undamaged.

Recommended Equipment

The following equipment is recommended to clean the ends of fiber-optic connectors.

- CLETOP or OPTIPOP ferrule cleaner (CLETOP Type A for SC, Type B for LC)
- Compressed air (also called “canned air”)
- Lint-free wipes moistened with optical-grade (99%) isopropyl alcohol
- Bulkhead swabs for LC or SC type connectors (choose appropriate type)
- Optical connector scope

Tips for Optimal Fiber-Optic Connector Performance

Follow these guidelines to ensure optimal connector performance.

- Do not connect or disconnect optical connectors while optical power is present.
- Always use compressed air before cleaning the fiber-optic connectors.
- Always use end caps on connectors when they are not in use.
- Always use compressed air to clean the end caps.
- If you have any degraded signal problems, clean the fiber-optic connector.
- Advance a clean portion of the ferrule cleaner reel for each cleaning.
- Turn off optical power before making or breaking optical connections in order to avoid microscopic damage to fiber mating surfaces.

To Clean Optical Connectors

Note: The proper procedure for cleaning optical connectors depends on the connector type. The following describes general instructions for cleaning optical connectors. Many companies have established procedures for cleaning connectors which should be followed. If your company has established procedures, the following instructions should be considered along with your procedures.



WARNING:

- **Avoid personal injury! Use of controls, adjustments, or performance of procedures other than those specified herein may result in hazardous radiation exposure.**
- **Avoid personal injury! The laser light source on this equipment emits invisible laser radiation. Avoid direct exposure to the laser light source.**
- **Avoid personal injury! Viewing the laser output with optical instruments (such as eye loupes, magnifiers, or microscopes) may pose an eye hazard.**
- Connect or disconnect fiber *only* when equipment is OFF or in Service mode.
- Do not apply power to this equipment if the fiber is unmated or unterminated.
- Do not look into an unmated fiber or at any mirror-like surface that could reflect light that is emitted from an unterminated fiber.
- Do not view an activated fiber with optical instruments such as eye loupes, magnifiers, or microscopes.
- Use safety-approved optical fiber cable to maintain compliance with applicable laser safety requirements.

Fiber Optic Connector Cleaning Instructions

Connector cleanliness is crucially important for optimum results in fiber-optic communications links. Even the smallest amount of foreign material can make it impossible to obtain the expected insertion and return losses. This can reduce the range of the equipment, shorten its expected service life, and possibly prevent the link from initializing at all.

New equipment is supplied with clean optical connectors and bulkheads. All optical connectors (bulkheads and jumpers) should be inspected using an appropriate optical scope prior to connector mating. If endface contamination is observed, the connector should be cleaned and then re-inspected to verify cleaning.

Connectors and Bulkheads

Most fiber-optic connectors are of the physical contact (PC) type. PC type connectors are designed to touch their mating connectors, thereby preventing air gaps which cause reflections. For optimum performance, *all* dirt must be removed.

Bulkheads can also become dirty enough to affect performance, either from airborne dust or from contamination introduced by connectors.



WARNING:

Avoid damage to your eyes! Do not look into any optical connector while the system is active. Even if the unit is off, there may still be hazardous optical levels present.

Important: Read the above warning before performing cleaning procedures.

Cleaning Connectors

Important:

- All external jumper connectors must be cleaned before inserting them into the optical module.
- Before you begin, remove optical power from the module or ensure that optical power has been removed.

Complete the following steps to clean fiber-optic connectors that will be connected to the optical module.

- 1 Inspect the connector through an optical connector scope. If the connector is damaged, e.g., scratched, burned, etc., replace the jumper.
- 2 If the connector is dirty but otherwise undamaged, clean the connector as follows:
 - a Make several swipes across the face of the connector with the appropriate ferrule cleaner. This will remove dust and some films.
 - b Listen for a slight "squeak" typically generated during this process, indicating a clean connector.
 - c Inspect the connector again through the scope to confirm that it is clean.
- 3 If a second inspection indicates that further cleaning is needed:
 - a Use 99% isopropyl alcohol and a lint-free wipe to clean the connector.
 - b Use the appropriate ferrule cleaner again to remove any film left over from the alcohol.
 - c Inspect the connector again through the scope and confirm that it is clean.
- 4 If necessary, repeat steps 3a-3c until the connector is clean.

Cleaning Bulkheads

Important:

- Do not detach the bulkhead from the module front panel for cleaning under any circumstances. There is little or no slack in the fiber attached to the bulkhead, and any attempt to remove the bulkhead will risk damage to the fiber.
- It is generally more difficult to clean bulkhead connectors and verify their condition due to the inaccessibility of the fiber end face. For this reason, you should *only* attempt to clean a bulkhead connector when a dirty connector is indicated.

Complete the following steps to clean the bulkhead.



WARNING:

- **Avoid personal injury!** Use of controls, adjustments, or performance of procedures other than those specified herein may result in hazardous radiation exposure.
- **Avoid personal injury!** The laser light source on this equipment emits invisible laser radiation. Avoid direct exposure to the laser light source.
- **Avoid personal injury!** Viewing the laser output with optical instruments (such as eye loupes, magnifiers, or microscopes) may pose an eye hazard.

- 1 Insert a dry bulkhead swab into the bulkhead and rotate the swab several times.
- 2 Remove the swab and discard.

Important: Swabs may be used only once.

- 3 Check the bulkhead optical surface with a fiber connector scope to confirm that it is clean. If further cleaning is needed:
 - a Moisten a new bulkhead swab using a lint-free wipe moistened with optical-grade (99%) isopropyl alcohol.
 - b With the connector removed, fully insert the bulkhead swab into the bulkhead and rotate the swab several times.
 - c Remove the swab and discard. Swabs may be used only once.
 - d Repeat steps 1 and 2 with a new dry bulkhead swab to remove any excess alcohol or residue.
 - e Check with a fiber connector scope again to confirm that there is no dirt or alcohol residue on the optical surface.
 - f If any alcohol residue remains, repeat steps 3d-3f.
- 4 Mate all connectors to bulkheads and proceed to **Verifying Equipment Operation** below.
- 5 It is also recommended that all connectors be visually inspected after cleaning to verify the connector is clean and undamaged.

Verifying Equipment Operation

Perform circuit turn-up. If the equipment does not come up, i.e., fails verification or indicates a reflection problem, clean the connectors and bulkheads again.

For Further Assistance

If you have any questions or concerns about cleaning fiber-optic connectors, contact Customer Service using the contact information provided in *Customer Support Information* (on page 313).

Connecting Optical Cables

Important: It is recommended that all connections be made with the optical power off. This will reduce the risk of damage to fiber-optic connectors.

Note: Observe laser safety precautions. Refer to *Laser Safety* (on page xxv) for further information.

To Connect Optical Cables



CAUTION:

High power density exists on fiber when optical power is present. To avoid microscopic damage to fiber mating surfaces, turn off optical power or reduce power below 15 dBm before making or breaking optical connections.

Complete the following steps for each optical cable connection to be made and on every module to be installed.

- 1 Clean the end of the fiber to be connected as described in *Cleaning Optical Connectors* (on page 308).
- 2 Connect the optical cable to the module connector.
- 3 Route the cable to the appropriate destination.
- 4 Clean the remaining cable end, and then connect the cable to the mating module connector.

Note: Remember to observe minimum bend radius and other accepted handling practices when working with fiber-optic cables.

- 5 After cable installation is complete, return the module control settings to their original states.

12

Customer Support Information

Introduction

This chapter contains information on obtaining product support and returning products to Scientific Atlanta.

In This Chapter

- Obtaining Product Support 314
- Return Product for Repair 316

Obtaining Product Support

IF...	THEN...
you have general questions about this product	contact your distributor or sales agent for product information or refer to product data sheets on www.cisco.com .
you have technical questions about this product	call the nearest Technical Service center or Scientific Atlanta office.
you have customer service questions or need a return material authorization (RMA) number	call the nearest Customer Service center or Scientific Atlanta office.

Support Telephone Numbers

This table lists the Technical Support and Customer Service numbers for your area.

Region	Centers	Telephone and Fax Numbers
North America	SciCare™ Services Atlanta, Georgia United States	For <i>Technical Support</i> , call: <ul style="list-style-type: none"> ■ Toll-free: 1-800-722-2009 ■ Local: 678-277-1120 (Press 2 at the prompt) For <i>Customer Service</i> or to request an RMA number, call: <ul style="list-style-type: none"> ■ Toll-free: 1-800-722-2009 ■ Local: 678-277-1120 (Press 3 at the prompt) ■ Fax: 770-236-5477 ■ E-mail: customer.service@sciatl.com
Europe, Middle East, Africa	Belgium	For <i>Technical Support</i> , call: <ul style="list-style-type: none"> ■ Telephone: 32-56-445-197 or 32-56-445-155 ■ Fax: 32-56-445-053 For <i>Customer Service</i> or to request an RMA number, call: <ul style="list-style-type: none"> ■ Telephone: 32-56-445-133 or 32-56-445-118 ■ Fax: 32-56-445-051 ■ E-mail: elc.service@sciatl.com
Japan	Japan	<ul style="list-style-type: none"> ■ Telephone: 81-3-5908-2153 or +81-3-5908-2154 ■ Fax: 81-3-5908-2155 ■ E-mail: yuri.oguchi@sciatl.com
Korea	Korea	<ul style="list-style-type: none"> ■ Telephone: 82-2-3429-8800 ■ Fax: 82-2-3452-9748 ■ E-mail: kelly.song@sciatl.com
China (mainland)	China	<ul style="list-style-type: none"> ■ Telephone: 86-21-6485-3205 ■ Fax: 86-21-6485-3205 ■ E-mail: xiangyang.shan@sciatl.com
All other Asia-Pacific countries & Australia	Hong Kong	<ul style="list-style-type: none"> ■ Telephone: 852-2588-4746 ■ Fax: 852-2588-3139 ■ E-mail: support.apr@sciatl.com

Region	Centers	Telephone and Fax Numbers
Brazil	Brazil	<p>For <i>Technical Support</i>, call:</p> <ul style="list-style-type: none"> ■ Telephone: 55-11-3845-9154 ext 230 ■ Fax: 55-11-3845-2514 <p>For <i>Customer Service</i> or to request an RMA number, call:</p> <ul style="list-style-type: none"> ■ Telephone: 55-11-3845-9154, ext 109 ■ Fax: 55-11-3845-2514 ■ E-mail: luiz.fattinger@sciatl.com
Mexico, Central America, Caribbean	Mexico	<p>For <i>Technical Support</i>, call:</p> <ul style="list-style-type: none"> ■ Telephone: 52-3515152599 ■ Fax: 52-3515152599 <p>For <i>Customer Service</i> or to request an RMA number, call:</p> <ul style="list-style-type: none"> ■ Telephone: 52-55-50-81-8425 ■ Fax: 52-55-52-61-0893 ■ E-mail: karla.lugo@sciatl.com
All other Latin America countries	Argentina	<p>For <i>Technical Support</i>, call:</p> <ul style="list-style-type: none"> ■ Telephone: 54-23-20-403340 ext 109 ■ Fax: 54-23-20-403340 ext 103 <p>For <i>Customer Service</i> or to request an RMA number, call:</p> <ul style="list-style-type: none"> ■ Telephone: 770-236-5662 ■ Fax: 770-236-5888 ■ E-mail: veda.keillor@sciatl.com

Return Product for Repair

You must have a return material authorization (RMA) number to return a product. Contact the nearest customer service center and follow their instructions.

Returning a product to Scientific Atlanta for repair includes the following steps:

- *Obtaining an RMA Number and Shipping Address* (on page 316)
- *Completing the Scientific Atlanta Transmission Networks Repair Tag* (on page 317)
- *Packing and Shipping the Product* (on page 320)

Obtaining an RMA Number and Shipping Address

You must have an RMA number to return products.

RMA numbers are only valid for 60 days. RMA numbers older than 60 days must be revalidated by calling a customer service representative before the product is returned. You can return the product after the RMA number is revalidated. Failure to comply with the above may delay the processing of your RMA request.

Complete the following steps to obtain an RMA number and shipping address.

- 1 Contact a customer service representative to request a new RMA number or revalidate an existing one.

Refer to *Support Telephone Numbers* (on page 314) to find a customer service telephone number for your area.

- 2 Provide the following information to the customer service representative:
 - Your company name, contact, telephone number, email address, and fax number
 - Product name, model number, part number, serial number (if applicable)
 - Quantity of products to return
 - A reason for returning the product and repair disposition authority
 - Any service contract details
- 3 A purchase order number or advance payment to cover estimated charges will be requested at the time a customer service representative issues an RMA number.

Notes:

- For credit card or cash in advance customers, a proforma invoice will be sent to you upon completion of product repair listing all charges incurred.
- Customer service must receive a purchase order number within 15 days after you receive the proforma invoice.

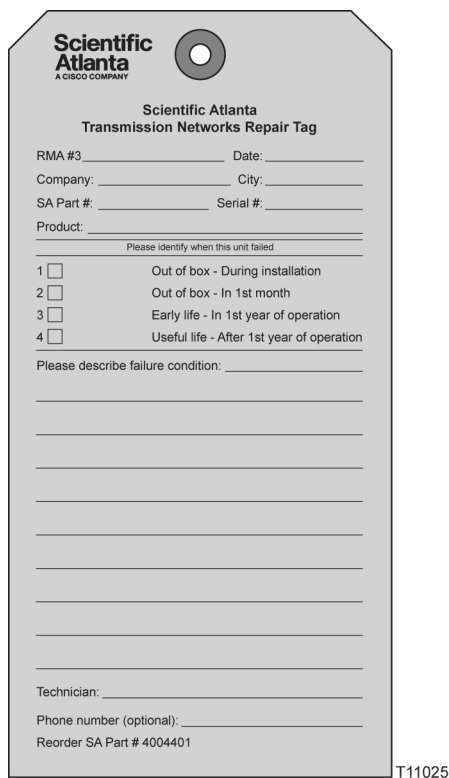
- In-warranty products can accrue costs through damage, misuse, cosmetics, or if no problem is found. Products incurring costs will not be returned to you without a valid purchase order number.
- 4 Once an RMA number has been issued, a confirmation e-mail or fax will be sent to you detailing the RMA number, product and product quantities authorized for return, together with shipping address details and RMA terms and conditions.
Note: Alternatively, you may obtain an RMA fax request form, complete and fax it to a customer service representative, or e-mail your completed request form to: customer.service@sciatl.com.
- 5 Go to *Completing the Scientific Atlanta Transmission Networks Repair Tag* (on page 317).

Completing the Scientific Atlanta Transmission Networks Repair Tag

Product returned for repair, both in-warranty and out-of-warranty, should have a repair tag attached to the product detailing the failure mode. A supply of tags can be obtained free of charge by calling a customer service representative.

The Scientific Atlanta Transmission Networks repair tag provides important failure information to the Scientific Atlanta repair department. This information will reduce the amount of time needed to repair the unit and return it to you. This information can also reduce the cost of out-of-warranty repairs.

It is best to have the Scientific Atlanta Transmission Networks repair tag completed by a person knowledgeable about the failure symptoms of the unit to be returned for repair. The tag should be securely attached to the failed unit with the elastic string, tape, or another method and returned to Scientific Atlanta.



Scientific Atlanta
A CISCO COMPANY

**Scientific Atlanta
Transmission Networks Repair Tag**

RMA #3 _____ Date: _____
 Company: _____ City: _____
 SA Part #: _____ Serial #: _____
 Product: _____

Please identify when this unit failed

1 ☐ Out of box - During installation
 2 ☐ Out of box - In 1st month
 3 ☐ Early life - In 1st year of operation
 4 ☐ Useful life - After 1st year of operation

Please describe failure condition: _____

Technician: _____
 Phone number (optional): _____
 Reorder SA Part # 4004401

T11025

Complete the following steps to fill out the Scientific Atlanta Transmission Networks repair tag.

1 Complete header information.



Scientific Atlanta
A CISCO COMPANY

**Scientific Atlanta
Transmission Networks Repair Tag**

RMA #3 _____ Date: _____
 Company: _____ City: _____
 SA Part #: _____ Serial #: _____
 Product: _____

T11026

- **RMA Number:** Enter the RMA number provided by the Scientific Atlanta customer service representative. All RMA numbers start with "3" and are followed by 7 additional digits. An RMA number is required to return products to Scientific Atlanta.
- If you are the technician who is filling out this tag, you may not have the RMA number. Leave it blank for now. Someone else in your organization, who has the number, can fill it in later.
- **Date:** Enter the date the unit was removed from service. If this date is unknown, enter the date you are completing the repair tag.

- **Company and City:** Enter the company name and city of the customer who owns the unit to be returned for repair.
 - **SA Part # and Serial #:** Enter the part number and serial number of the unit you are returning for repair. The part number and serial number can usually be found on a bar code label on the outside of the unit. If this information can't be found leave this blank.
 - **Product:** Enter the model description of the unit you are returning for repair. For example, Model 6940/44 Node, Multimedia Tap, RF Signal Manager, etc.
- 2** Complete time of failure information.

Please identify when this unit failed	
1 <input type="checkbox"/>	Out of box - During installation
2 <input type="checkbox"/>	Out of box - In 1st month
3 <input type="checkbox"/>	Early life - In 1st year of operation
4 <input type="checkbox"/>	Useful life - After 1st year of operation

This information will help the repair technician understand the failure mode. If the time to failure is unknown, leave this information blank.

- 3** Complete the failure description and technician information:

[illegible]

- **Failure Description:** Include as much information as possible. For example:
 - Which feature is not working or which specification is not being met? For example, does the problem affect audio, video, status monitoring and control, forward path, reverse path, cosmetics, all functions, etc.
 - If it is a multi-port product, which port is not working or if all ports are not working?
 - If the unit has degraded performance or is completely failed.

- If the failure happens only at specific environmental conditions (i.e., at hot temperature).
- If the failure is intermittent or constant.
- How you were powering the unit when it failed? (DC vs. AC, voltage levels, etc.)

Important: Descriptions like “bad unit,” “failed,” or “no HBO” are not specific enough to be helpful.

- Technician and Phone Number: Enter the name and phone number of the technician completing the failure description information. A Scientific Atlanta representative may want to call this person to better understand the problem.
- 4 Attach the repair tag to the unit you are returning for repair. Use the elastic string provided, tape, or another method to securely attach the tag.
 - 5 Go to *Packing and Shipping the Product* (on page 320).

Packing and Shipping the Product

Complete the following steps to pack the product and ship it to Scientific Atlanta.

- 1 Are the product’s original container and packing material available?
 - If yes, pack the product in the original container using the original packing material.
 - If no, pack the product in a sturdy corrugated box, that is suitable to the method of shipment, and cushion it with packing material.

Important: You are responsible for delivering the returned product to Scientific Atlanta safely and undamaged. Shipments damaged due to improper packaging may be refused and returned to you at your expense.

Note: PLEASE DO NOT RETURN ANY POWER CORDS, ACCESSORY CABLES, OR OTHER ACCESSORY PRODUCTS. Instructions for ordering replacement power cords, accessory cables, or other accessories can be provided by a customer service representative.

- 2 Write the following information on the outside of the shipping container:
 - RMA number
 - Your name
 - Your complete address
 - Your telephone number
 - "Attention: Factory Service"

Important: The RMA number should be clearly marked on all returned product, boxes, packages, and accompanying paperwork. RMAs received by the factory service receiving department that are not clearly marked may experience delays in the processing of RMA requests. All returned product should be marked to the attention of Factory Service.

- 3 Ship the product to the address provided by the customer service representative in the confirmation e-mail or fax.

Note: Scientific Atlanta does not accept freight collect. Be sure to prepay and insure all shipments. For both in-warranty and out-of-warranty repairs, you are responsible for paying your outbound freight expense, any applicable import and/or export duties and taxes. Scientific Atlanta will pay the return freight expense for in-warranty repairs.

International Shipments: International shipments should be consigned to Scientific Atlanta with the notified party on the Airway Bill stated as "Expeditors International for Customs Clearance".

- 4 On receipt of product returned under an RMA number, a receipt notification e-mail or fax will be sent to you by Repair Receiving confirming receipt of product and quantities received. Please check the receipt notification to assure the product and quantity of product received by Scientific Atlanta matches what you shipped.

A

Prisma II Permitted CLI Commands

Introduction

The following tables summarize the available CLI commands for the Prisma II Platform. Each table lists the commands available for one of the four major CLI prompts: CLI, */* MODULE, TERMINAL, and ICIM.

Entries shown in parenthesis () are module-specific and must be typed in full. Hints are given to display available entries for those cases. All other entries may be abbreviated to the shortest unambiguous form, as explained in the CLI online help screens.

Note: Some commands are limited to Admin level users only.

For further information and assistance when working with CLI, type **help** at the appropriate CLI prompt, and then press **Enter** to display the corresponding help screens.

In This Appendix

■ From CLI	324
■ From ICIM	325
■ From */* MODULE	331
■ From TERMINAL	334

From CLI

ALARM	
CLEAR	
DATE	
EXIT	
HELP	ALARM
	CLEAR
	COMMANDS
	DATE
	EDIT
	EXIT
	ICIM
	LOGOUT
	MANUAL
	MODULE
	TERMINAL
	WHO
	WHOAMI
ICIM	
LOGOUT	
MANUAL	
MODULE	
TERMINAL	
WHO	
WHOAMI	
'?'	

From ICIM

ALARM		
EVENTLOGCLEAR		
EVENTLOGFILTER	HARDWARE	ON/OFF
	PROVISIONING	ON/OFF
	SYSTEM	ON/OFF
EXIT		
FILE	IP	(IP_ADDRESS)
	NAME	(FILENAME)
	PASSWORD	(PASSWORD)
	PATH	(PATH)
	USER	(USERNAME)
HELP		
IKE *	ADD	(IP_ADDRESS)
	DELETE	(IP_ADDRESS)
INFO	ACTIVEREV	
	ATTNSTATUS	
	BOOTREV	
	CHASSIS	
	CLEI *	
	CLLI *	
	COMMREAD	
	COMMTRAP	
	COMMWRITE	
	DEVTYPE	
	DOWNLDCMD	
	DOWNLDDIR	
	DOWNLDFILE	
	DOWNLDRESULT	
	DOWNLDSEM	
	DOWNLDSIG	
	DOWNLDSTATE	

12BAppendix A
Prisma II Permitted CLI Commands

	DOWNLDTGT	
	DOWNLDUSER	
	FTPSEVER	
	FTPUSER	
	GATEWAY	
	HWREV	
	INACTIVEREV	
	IP	
	IPSEC *	
	LOCKOUT	
	MAC	
	MANDATA	
	NEXTIMAGE	
	PREVIOUSIP	
	SELFTEST	
	SERIAL	
	SIZE	
	SLOT	
	SMC	
	STATUSMSG	
	SUBNET	
	SWDATE	
	SWREV	
	THRESHOLD	
	TIMEOUT	
	TOS	
	TZONE	
	UPDATEID	
IPROUTE	ADD	(DESTINATION)
		(GATEWAY)
	DELETE	(DESTINATION)
		(GATEWAY)
IPSEC *	DISABLE	

	ENABLE	
LOGOUT		
MANUAL		
REBOOT		
SET	CLLI *	(CLLI)
	CLOCK	(DATE_TIME)
	COMMREAD	(READ_STRING)
	COMMTRAP	(TRAP_STRING)
	COMMWRITE	(WRITE_STRING)
	GATEWAY	(GATEWAY)
	IP	(IP_ADDRESS)
	LOCKOUT	(INTERVAL)
	STATUSMSG- CLEARKEY	(1)
	SUBNET	(SUBNET_MASK)
	THRESHOLD	(THRESHOLD)
	TIMEOUT	(TIMEOUT)
	TZONE	(TIMEZONE)
	UPDATEID	(1)
SHOW	ACTIVEREV	
	ATTNSTATUS	
	BOOTREV	
	CHASSIS	
	CLEI *	
	CLLI *	
	CLOCK	
	COMMREAD	
	COMMTRAP	
	COMMWRITE	
	DEVTYPE	
	DOMAIN	
	DOWNLDCMD	
	DOWNLDDIR	
	DOWNLDFILE	

12BAppendix A
Prisma II Permitted CLI Commands

	DOWNLDRESULT	
	DOWNLDSEM	
	DOWNLDSIG	
	DOWNLDSTATE	
	DOWNLDTGT	
	DOWNLDUSER	
	EVENTLOG	
	EVENTLOGALL	
	EVENTLOGFILTER	
	FILE	
	FTPSERVER	
	FTPUSER	
	GATEWAY	
	HWREV	
	IKE *	
	INACTIVEREV	
	IP	
	IPROUTE	
	IPSEC *	
	LOCKOUT	
	LOCKEDUSERS	
	MAC	
	MANDATA	
	NEXTIMAGE	
	PREVIOUSIP	
	PROVISIONING	
	SELFTEST	
	SERIAL	
	SIZE	
	SLOT	
	SMC	
	SNTP *	
	STATUSMSG	

	SUBNET	
	SWDATE	
	SWREV	
	THRESHOLD	
	TIMEOUT	
	TOS	
	TRAPS	
	TZONE	
	UPDATEID	
	USER	
SNTP *	INTERVAL	
	IP	
	MODE	
	STATE	
	TIMEOUT	
TRAPS	DISABLE	(INDEX)
		(IP_ADDRESS)
	ENABLE	(INDEX)
		(IP_ADDRESS)

USER	ADD	(USER_ID)	ADMIN	DISABLE
				ENABLE
			READ	DISABLE
				ENABLE
			READWRITE	DISABLE
				ENABLE
	CHANGE	ACCESS_RIGHTS	(USER_ID)	ADMIN
				READ
				READWRITE
		ACCOUNT_STATUS	(USER_ID)	DISABLE
				ENABLE
		PASSWORD	(USER_ID)	(PASSWORD)
	DELETE	(USER_ID)		
	UNLOCK	(USER_ID)		

12BAppendix A
Prisma II Permitted CLI Commands

'?'				
-----	--	--	--	--

* Reserved for future use.

From */* MODULE

ALARM	DOMAIN		
	MODULE		
CHASSIS	(digits)		
	*		
	[range]		
EXIT			
HELP			
INFO	ALARM	(ALARMNAME)	HYSTERESIS
		use show alarms *	INDEX
			LABEL
			LIMITADJUST
			MAJORHIGH
			MAJORLOW
			MINORHIGH
			MINORLOW
			NOMINAL
			RANGEHI
			RANGELO
			TYPE
			VALUE
	CONTROL	(CONTROLNAME)	INDEX
		use show control *	LABEL
			RANGEHI
			RANGELO
			RANGESTEP
			STATENAMES
			TYPE
			UNITS
			VALUE
	MODULE	ACTIVEREV	
		BOOTREV	
		CLEI ¹	

12BAppendix A
Prisma II Permitted CLI Commands

		CLLI ¹	
		CODEREV	
		DATECODE	
		DEVTYPE	
		DOWNLOADABLE	
		INACTIVEREV	
		MANDATA	
		MODTYPE	
		NAME	
		NEXTIMAGE	
		NUMANALOGCONTROLS	
		NUMCONTROLS	
		NUMDIGITALCONTROLS	
		NUMMONITS	
		NUMOFALARMS	
		SCRIPTREV	
		SELFTEST	
		SERIAL	
		TOS	
	MONITOR	(MONITORNAME)	INDEX
		use show mon *	LABEL
			STATENAMES
			TYPE
			UNITS
			VALUE
LOGOUT			
MANUAL			
MODID	digits		
	*		
	[range]		
RESET			
SET	ALARMPARAM	(ALARMNAME)	HYSTERESIS
			MAJORHIGH

			MAJORLOW
			MINORHIGH
			MINORLOW
	CONTROL	(CONTROLNAME)	(VALUE)
	MODULE	CLLI ¹	(CLLI)
SHOW	ALARMPARAM	(ALARMNAME)	HYSTERESIS
		use show alarms *	MAJORHIGH
			MAJORLOW
			MINORHIGH
			MINORLOW
	ALARMSTATE	(ALARMNAME)	
	CONTROL	(CONTROLNAME)	
	MODULE		
	MONITOR	(MONITORNAME)	
SLOT	digits		
	*		
	[range]		
'?'			

¹ Reserved for future use.

From TERMINAL

ALARM	
COLSEP	(string)
EXIT	
HEADERS	(digits)
HELP	
LOGOUT	
MANUAL	
PAGING	(digits)
PATTERN	REGEX
	WILDCARD
SHOW	
'?'	

B

Features Available via Remote User Interface

Introduction

This appendix lists the features of the remote user interface and identifies the availability (CLI, Web Interface, or both) and required user access level (Read-Only, Read-Write, or Admin) for each feature.

In This Appendix

■ Overview	336
■ ICIM Data.....	337
■ Module Data	340
■ Current Alarms	341
■ Module Alarms	342
■ Module Controls	343
■ Module Monitors	344
■ System Information	345
■ User Management.....	346

Overview

The tables below list the features available via either the CLI or the Web Interface.

Symbols appearing in the cells of these tables have the meanings described below.

- In the CLI or Web column:
 - An asterisk (*) indicates that the corresponding interface (CLI or Web) supports this feature.
 - A dash (-) indicates that the corresponding interface (CLI or Web) does not support this feature.
- In the Read-Only User, Read-Write User, or Admin User security column:
 - A dash (-) indicates that this feature is not available to the corresponding access level.
 - The letter R indicates that the corresponding access level has Read-Only access to this feature.
 - The letter RW indicates that the corresponding access level has Read-Write access to this feature.

Note: The hierarchy of access goes from Read-Only to Read-Write to Admin. So, if a Read-Only user has the privilege to view a particular data element, a Read-Write user would be able to view the same data element. Similarly, if a Read-Write user is able to view or edit a data element, an Admin level user would be able to do the same.

ICIM Data

Feature	CLI	Web	Read-Only User Privilege	Read-Write User Privilege	Admin User Privilege
IP address	* ¹	*	R	R	RW
Active rev	*	*	R	R	R
Attnstatus	*	-	R	R	R
Boot rev	*	-	R	R	R
Chassis	*	*	R	R	R
CLEI ²	*	*	R	R	R
CLLI ²	*	*	R	RW	RW
Clock	* ¹	*	R	R	RW
Commread	*	-	-	-	RW
Commwrite	*	-	-	-	RW
Commtrap	*	-	-	-	RW
DevType	*	-	R	R	R
Domain	*	*	R	R	R
Downldcmd	*	-	R	R	R
Downlddir	*	-	R	R	R
Downldfile	*	-	R	R	R
Downldresult	*	-	R	R	R
Downldsem	*	-	R	R	R
Downldsig	*	-	R	R	R
Downldstate	*	*	R	R	R
Downldtgt	*	-	R	R	R
Downlduser	*	-	R	R	R
Eventlog	*	-	-	-	R
Eventlogall	*	*	-	-	R
File	*	-	-	R	RW
Ftpserver	*	-	R	R	R
Ftpuser	*	-	-	-	R
Gateway	* ¹	*	R	R	RW

13BAppendix B
Features Available via Remote User Interface

Feature	CLI	Web	Read-Only User Privilege	Read-Write User Privilege	Admin User Privilege
Hwrev	*	*	R	R	R
Inactiverrev	*	*	R	R	R
IKE ²	*	-	-	-	RW
IProute	*	-	R	R	RW
IPSec ²	*	-	R	R	RW
LockedUsers	*	*	-	-	R
LockoutInterval	*	*	R	R	RW
MAC	*	*	R	R	R
Mandata	*	*	R	R	R
Nextimage	*	-	R	R	R
Previousip	*	-	R	R	R
Provisioning	*	-	R	R	R
Reboot	*	-	-	-	W
Selftest	*	*	R	R	R
Serial	*	*	R	R	R
Size	*	*	R	R	R
Slot	*	*	R	R	R
Smc	*	*	R	R	R
SNTPInterval ²	*	-	-	-	RW
SNTPIPAddress ²	*	-	-	-	RW
SNTPLastUpdate ²	*	-	-	-	R
SNTPMode ²	*	-	-	-	RW
SNTPState ²	*	-	-	-	RW
SNTPTimeout ²	*	-	-	-	RW
Statusmsg	*	-	R	R	R
Statusmsgclearkey	*	-	-	-	W
Subnet	* ¹	*	R	R	RW
Swdate	*	-	R	R	R
Swrev	*	-	R	R	R
sysDescr	-	*	R	R	R

Feature	CLI	Web	Read-Only User Privilege	Read-Write User Privilege	Admin User Privilege
sysLocation	-	*	R	R	R
sysUptime	-	*	R	R	R
Threshold	* ³	*	R	R	RW
Timeout	* ³	*	R	R	RW
TOS	*	*	R	R	R
Traps	* ³	*	R	R	RW
Timezone	* ¹	*	R	R	RW
Updateid	*	-	R	R	RW
User	*	*	-	-	RW

¹ May be modified through the CLI but not through the Web Interface.

² Reserved for future use.

³ May be read through the CLI but not through the Web Interface.

Module Data

Feature	CLI	Web	Read-Only User Privilege	Read-Write User Privilege	Admin User Privilege
Active rev	*	*	R	R	R
Boot rev	*	-	R	R	R
Chassis	*	*	R	R	R
CLEI ¹	*	*	R	R	R
CLLI ¹	*	*	R	RW	RW
Device Type	*	*	R	R	R
Downloadable	*	*	R	R	R
Inactive Rev	*	*	R	R	R
Module Name	*	*	R	R	R
Module Type	*	*	R	R	R
Reset	*	-	-	-	W
Selftest	*	*	R	R	R
Serial	*	*	R	R	R
Slot	*	*	R	R	R
Time of Service	*	*	R	R	R

¹ Reserved for future use.

Current Alarms

Feature	CLI	Web	Read-Only User Privilege	Read-Write User Privilege	Admin User Privilege
Current Alarms	*	*	R	R	R

Module Alarms

Feature	CLI	Web	Read-Only User Privilege	Read-Write User Privilege	Admin User Privilege
Hysteresis	*	*	R	RW	RW
Label	*	*	R	R	R
MajorHigh	*	*	R	RW	RW
MajorLow	*	*	R	RW	RW
MinorHigh	*	*	R	RW	RW
MinorLow	*	*	R	RW	RW
RangeHigh	*	*	R	R	R
RangeLow	*	*	R	R	R
Type	*	*	R	R	R
Value	*	*	R	R	R

Module Controls

Feature	CLI	Web	Read-Only User Privilege	Read-Write User Privilege	Admin User Privilege
High	*	*	R	R	R
Label	*	*	R	R	R
Low	*	*	R	R	R
Step	*	*	R	R	R
Units	*	*	R	R	R
Value	*	*	R	RW	RW

Module Monitors

Feature	CLI	Web	Read-Only User Privilege	Read-Write User Privilege	Admin User Privilege
Label	*	*	R	R	R
Units	*	*	R	R	R
Value	*	*	R	R	R

System Information

Feature	CLI	Web	Read-Only User Privilege	Read-Write User Privilege	Admin User Privilege
Event Log Filter	* ⁴	*	R	R	RW
Event Log Clear	*	*	-	-	R/Clear
Max Login Attempts	* ⁴	*	R	R	RW
Inactivity Timeout	* ⁴	*	R	R	RW
Lockout Interval	*	*	R	R	RW
Trap Receive Table	* ⁴	*	R	R	RW

⁴ May be read through the CLI but not through the Web Interface.

User Management

Feature	CLI	Web	Read-Only User Privilege	Read-Write User Privilege	Admin User Privilege
Add user	*	*	-	-	RW
Change user	*	*	-	-	RW
Current users	*	*	-	-	R
Delete user	*	*	-	-	RW
Unlock user	*	- ¹	-	-	RW

¹ A user account may be unlocked through the Web Interface by enabling the account.

C

Module Parameter Descriptions

Introduction

This appendix provides control, alarm, monitor, and manufacturing data parameters for this equipment. The examples shown in the tables are for guidance only.



CAUTION:

The warranty may be voided and the equipment damaged if you operate the equipment above the specified temperature limits (0 to 50°C). Specification temperature limits are measured in the air stream at the fan inlet and may be higher than room ambient temperature.

In This Appendix

■ XD Chassis Parameters	348
-------------------------------	-----

XD Chassis Parameters

XD Chassis Configurable Parameters

Parameter Name (LCI)	ICIM2 Abbreviation	Description	Value	Default
Mute Converter A Alarm	AlmMuteA	Alarm muting for power section A	0 (OFF) 1 (ON)	0 (OFF)
Mute Converter B Alarm	AlmMuteB	Alarm muting for power section B	0 (OFF) 1 (ON)	0 (OFF)

XD Chassis Alarm Data Parameters

Parameter Name (LCI)	ICIM2 Abbrev.	Nominal Value	Major Low Limit	Minor Low Limit	Minor High Limit	Major High Limit	Hys-teresis	Operating Range
Fan 1 Status	Fan 1_Ok	na	na	na	na	na	na	OK or Fault
Fan 2 Status	Fan 2_Ok	na	na	na	na	na	na	OK or Fault
Fan 3 Status	Fan 3_Ok	na	na	na	na	na	na	OK or Fault
Chassis Temperature	ChasTemp	25°C	-40°C	-35°C	60°C	65°C	1°C	-40°C to 65°C
Converter A Input Status	ConvAIn	na	na	na	na	na	na	OK or Fault
+24V Converter A	ConvA+24	24.7 VDC	18.0 VDC	18.4 VDC	25.9 VDC	26.1 VDC	0.1 VDC	23.8 to 25.6 VDC
+5V Converter A	ConvA+5	5.4 VDC	3.6 VDC	3.7 VDC	5.9 VDC	6.1 VDC	0.1 VDC	4.9 to 5.3 VDC
-5V Alarm Converter A	ConvA-5	-5.4 VDC	-5.6 VDC	-5.5 VDC	-4.6 VDC	-4.5 VDC	0.1 VDC	-5.3 to -4.9 VDC
Converter B Input Status	ConvBIn	na	na	na	na	na	na	OK or Fault
+24V Converter B	ConvB+24	24.7 VDC	18.0 VDC	18.4 VDC	25.9 VDC	26.1 VDC	0.1 VDC	23.8 to 25.6 VDC
+5V Converter B	ConvB+5	5.4 VDC	3.6 VDC	3.7 VDC	5.9 VDC	6.1 VDC	0.1 VDC	4.9 to 5.3 VDC
-5V Converter B	ConvB-5	-5.4 VDC	-5.6 VDC	-5.5 VDC	-4.6 VDC	-4.5 VDC	0.1 VDC	-5.3 to -4.9 VDC

XD Chassis Operating Status Parameters

Parameter Name (LCI)	ICIM2 Abbreviation	Function	Initial Value	Typical Value (Op.)
PS A Installed	PSA Inst	1 if power supply A installed and powered, 0 if not	1 or Yes (Installed)	1 or Yes (Installed)
Converter A Installed	ConvAIns	1 if converter A is installed, 0 if not	1 or Yes (Installed)	1 or Yes (Installed)
+24V Converter A	ConvA+24	measured +24 V DC of slot A	24.12 V	24.12 V
+5V Converter A	ConvA+5	measured +5 V DC of slot A	5.29 V	5.29 V
-5V Converter A	ConvA-5	measured -5 V DC of slot A	-5.30 V	-5.30 V
PS B Installed	PSB Inst	1 if power supply B installed and powered, 0 if not	0 or No (Not inst)	1 or Yes (Installed)
Converter B Installed	ConvBIns	1 if converter B is installed, 0 if not	1 or Yes (Installed)	1 or Yes (Installed)
+24V Converter B	ConvB+24	measured +24 V DC of slot B	24.2 V	24.2 V
+5V Converter B	ConvB+5	measured +5 V DC of slot B	5.1 V	5.1 V
-5V Converter B	ConvB-5	measured -5 V DC of slot B	-5.03 V	-5.03 V
+24V Chassis	Chas+24	chassis +24 V bus	24.14 V	24.2 V
+5V Chassis	Chas+5	chassis +5 V bus	5.08 V	5.2 V
-5V Chassis	Chas-5	chassis -5 V bus	-5.05 V	-5.2 V
Chassis Temperature	ChasTemp	chassis internal temperature	26.5°C	26.5°C

Note: All monitored values may vary from module to module. The values shown above are examples only.

XD Chassis Manufacturing Data Parameters

XD Chassis

Parameter Name (LCI)	ICIM2 Abbreviation	Typical Values
Generic Name	na	Chassis

14B Appendix C
Module Parameter Descriptions

Parameter Name (LCI)	ICIM2 Abbreviation	Typical Values
Description	Module Name	P2-XD-CHASSIS
Module Type	Module Type	5020
Manufacturing Data	na	<NULL>
Serial Number [1]	Serial #	AAFHJTT
Day Code [1]	Date Code	K06
Module ID	na	<NULL>
CLLI Code [1]	na	<NULL>
CLEI Code [1]	na	<NULL>
Software Version [1]	Sw Ver	1.01.05
Script Version	na	N/A
Time of Service [1]	In Service Hours	372

ICIM2-XD

Parameter Name (LCI)	ICIM2 Abbreviation	Typical Values
Generic Name	na	ICIM
Description	Module Name	P2-ICIM2-XD
Module Type	Module Type	5011
Manufacturing Data	na	ICIM2
Serial Number [1]	Serial #	~AAVGTHZ
Day Code [1]	Date Code	C07
Module ID	na	<NULL>
CLLI Code [1]	na	<NULL>
CLEI Code [1]	na	<NULL>
Hardware Revision	na	BdRev87A
Software Version [1]	Sw Ver	2.03.01
In Service Hours [1]	In Service Hours	372

Note: [1] These values may vary from module to module. The values shown above are examples only.

Glossary

A

ampere. A unit of measure for electrical current.

ac, AC

alternating current. An electric current that reverses its direction at regularly recurring intervals.

AD

administration.

Admin

administrator.

AGC

automatic gain control. A process or means by which gain is automatically adjusted in a specified manner as a function of input level or other specified parameters.

AWG

American Wire Gauge. A U.S. standard for wire conductor sizes.

binding

A parameter representing the physical or logical objects associated with a trap.

CAT5

category 5 Ethernet cable.

CBN

common bonding network.

CCB

client controller board or chassis control board.

Glossary

CENELEC

Comité Européen de Normalisation ELECTrotechnique. The European Committee for electro-technical standardization.

CLEI

common language equipment identifier. CLEI code is globally unique ten-character intelligent code, assigned by Telcordia, that identifies communications equipment in a concise, uniform feature-oriented language, which describes product type, features, source document and associated drawings and vintages.

CLI

command line interface. A command reference software that allows the user to interact with the operating system by entering commands and optional arguments.

CLLI

common language location identification. A CLLI code is typically an 11-character alphanumeric descriptor used to identify network elements and their locations.

COM

communication.

CSV

comma-separated values. A data file format supported by many spreadsheet programs, in which fields are separated by commas. Also referred to as comma delimited.

dc, DC

direct current. An electric current flowing in one direction only and substantially constant in value.

EEPROM

electrically erasable programmable read-only memory.

EIA

Electronic Industries Association. A United States association that provides standards for use between manufacturers and purchasers of electronic products.

EMC

electromagnetic compatibility. A measure of equipment tolerance to external electromagnetic fields.

ESD

electrostatic discharge. Discharge of stored static electricity that can damage electronic equipment and impair electrical circuitry, resulting in complete or intermittent failures.

FCC

Federal Communications Commission. Federal organization set up by the Communications Act of 1934 which has authority to regulate all inter-state (but not intra-state) communications originating in the United States (radio, television, wire, satellite, and cable).

FTP

file transfer protocol. Allows users to transfer text and binary files to and from a personal computer, list directories on the foreign host, delete and rename files on the foreign host, and perform wildcard transfers between hosts.

FTTP

fiber-to-the-premises. Fiber optic service to the subscriber's premises.

HDRx

high density receiver.

HDTx

high density transmitter.

HTTP

hypertext transport protocol. A communication protocol used to request and transmit files over the Internet and other networks.

HW

hardware.

Hz

hertz. A unit of frequency equal to one cycle per second.

I/O

input/output.

ICIM

intelligent communications interface module.

Glossary

ID

identifier.

IEC

International Electro-technical Commission.

in-lb

inch-pound. A measure of torque defined by the application of one pound of force on a lever at a point on the lever that is one inch from the pivot point.

IP

Internet protocol. A standard that was originally developed by the United States Department of Defense to support the internetworking of dissimilar computers across a network. IP is perhaps the most important of the protocols on which the Internet is based. It is the standard that describes software that keeps track of the internetwork addresses for different nodes, routes, and outgoing/incoming messages on a network. Some examples of IP applications include email, chat, and Web browsers.

LCD

liquid crystal display. A display medium made of liquid crystal. Liquid crystal's reflectance changes when an electric field is applied. Commonly used in monitors, televisions, cell phones, digital watches, etc.

LCI

local craft interface.

LED

light-emitting diode. An electronic device that lights up when electricity passes through it.

MIB

management information base. SNMP collects management information from devices on the network and records the information in a management information base. The MIB information includes device features, data throughput statistics, traffic overloads, and errors.

MSO

multiple system operator. A cable company that operates more than one cable system.

nm

nanometer. One billionth of a meter.

Nm

Newton meter. A measure of torque defined by the application of one Newton of force on a lever at a point on the lever that is one meter from the pivot point. (1 Nm = 0.737561 ft-lb)

NMS

network management system. A software system designed specifically to monitor a network and to facilitate troubleshooting.

NTP

network time protocol.

OID

object identifier.

OMI

optical modulation index.

PR

provisioning.

PWR

power.

QAM

quadrature amplitude modulation. A phase modulation technique for representing digital information and transmitting that data with minimal bandwidth. Both phase and amplitude of carrier waves are altered to represent the binary code. By manipulating two factors, more discrete digital states are possible and therefore larger binary schemes can be represented.

RF

radio frequency. The frequency in the portion of the electromagnetic spectrum that is above the audio frequencies and below the infrared frequencies, used in radio transmission systems.

RMA

return material authorization. A form used to return products.

RO

read-only.

Glossary

RTC

real time clock.

RW

read-write.

RX

receive or receiver.

SE

security.

semaphore

In programming, a control token (variable or abstract data type) used to restrict access to a resource. The Scientific Atlanta SOUP program uses a semaphore to prevent multiple instances of the SOUP from running and trying to change Prisma II EMS chassis parameters at the same time.

SMC

status monitoring and control. The process by which the operation, configuration, and performance of individual elements in a network or system are monitored and controlled from a central location.

SNMP

simple network management protocol. A protocol that governs network management and the monitoring of network devices and their functions.

SOUP

software upgrade program. A utility used to update firmware in Prisma II EMS application modules.

SY

system.

TNCS

Transmission Network Control System. A Scientific Atlanta application that allows status monitoring and control of all transmission equipment located in headends and hubs plus optical nodes, power supplies, and amplifiers in the outside plant. TNCS provides access to and information on the entire network in an easy to understand, topology driven, graphical user display.

trap

An unsolicited message sent by a network device to notify a network or element management system of an alarm or other condition that requires administrative attention.

TX

transmit or transmitter.

V AC

volts alternating current.

V DC

volts direct current.

XD

extreme density.

Index

A

- A • 351
- About Traps • 227
- ac, AC • 351
- Accessing the Module Detail Information • 118
- Active and Inactive Flash • 273
- AC-to-DC Bulk Power Supply Features • 55
- AC-to-DC Bulk Power Supply Illustration • 55
- AC-to-DC Bulk Power Supply Modules • 52
- AD • 351
- Additional Assistance • 291
- Admin • 351
- AGC • 351
- ALARM IN and OUT Connections • 72
- ALARM IN and OUT Terminal Blocks • 73
- Alarm Severity Mappings • 213
- Alarm Threshold Modification • 265
- Alarm Troubleshooting • 291
- Application Modules • 37
- AWG • 351

B

- Basic SNMP Setup • 105
- Before You Begin • 60
- binding • 351

C

- Cable Requirements • 111
- CAT5 • 351
- CBN • 351
- CCB • 352
- CENELEC • 352
- Chassis and Slot Numbering • 41
- Chassis Back Panel Features • 44
- Chassis Configuration • 41
- Chassis Dimensions • 65
- Chassis Features • 39
- Chassis Front Panel Features • 43
- Chassis Illustrations • 42
- Chassis Midplane • 44
- Chassis Power Supply Architecture • 47

- Chassis Troubleshooting • 290
- Chassis Wiring and Fusing • 6, 61, 76
- Chassis-to-Chassis ICIM2 Activation • 71
- Chassis-to-Chassis ICIM2 Connections • 3
- ChasTemp Alarm • 293
- ChasTemp Alarm Parameters • 293
- Checking Manufacturing Data using LCI • 131
- Checking the Module Alarms using LCI • 127
- Checking the Operating Status • 124
- Cleaning Optical Connectors • 308
- Clearing the Event Log • 159
- CLEI • 352
- CLI • 352
- CLI Parameters • 95
- CLLI • 352
- COM • 352
- Completing the Scientific Atlanta Transmission Networks Repair Tag • 317
- Computer Requirements • 111
- Concepts • 273
- Concurrency • 274
- Configuring for Remote Network Access • 106
- Configuring the Module using LCI • 125
- Connecting Optical Cables • 89, 312
- Connecting RF Cables • 90
- Connecting the ICIM2 to Additional Chassis • 68
- Connecting Your Computer to the Chassis • 115
- Connector Interface Panel • 67
- ConvA+24 Alarm • 295
- ConvA+24 Alarm Parameters • 295
- ConvA+5 Alarm • 297
- ConvA+5 Alarm Parameters • 297
- ConvA-5 Alarm • 299
- ConvA-5 Alarm Parameters • 299
- ConvAIn Alarm • 294
- ConvAIn Alarm Parameters • 294
- ConvB+24 Alarm • 302
- ConvB+24 Alarm Parameters • 302
- ConvB+5 Alarm • 304
- ConvB+5 Alarm Parameters • 304
- ConvB-5 Alarm • 306

ConvB-5 Alarm Parameters • 306
 ConvBIn Alarm • 301
 ConvBIn Alarm Parameters • 301
 CSV • 352
 Current Alarm Table • 214
 Current Alarms • 341
 Customer Support Information • 313

D

DC Power Connectors • 78
 dc, DC • 352
 DC-to-DC Converter Illustration • 56
 DC-to-DC Converters • 56
 Default Community Strings • 105
 Delay in the Discovery Process • 267
 Downloading and Viewing the Event Log
 Remotely • 164

E

EEPROM • 352
 EIA • 352
 Electrical Input Voltages • 54
 Electrical Power Connections • 6, 76
 EMC • 353
 Enhanced Trap Alarms • 245
 Enhanced Trap Binding Information • 241
 Enhanced Trap Events • 248
 Equipment Configuration • 91
 ESD • 353
 Event Action IDs • 155
 Event Log • 153
 Event Log Fields • 154
 Event Log File Management • 183
 Event Log-Related Traps • 162
 External Alarms Connections • 72

F

Fan Alarm Parameters • 292
 Fan Assembly • 45, 74
 Fan Assembly Illustration • 51
 Fan Ok Alarms • 292
 Fan Operation • 51
 FCC • 353
 Firmware Updates • 284
 Firmware Upgrade Process • 279
 Frequently Asked Questions • 268
 From */* MODULE • 331
 From CLI • 324
 From ICIM • 325
 From TERMINAL • 334

FTP • 353
 FTP Server • 283
 FTP Settings • 281
 FTTTP • 353

H

Hardware Installation • 59
 HDRx • 353
 HDTx • 353
 How do Enhanced Traps differ from other trap
 types? • 269
 How do I configure trap destination? • 268
 HTTP • 353
 HW • 353
 HyperTerminal Session Setup • 92
 Hz • 353

I

I/O • 353
 ICIM • 354
 ICIM Data • 337
 ICIM Front Panel • 104
 ICIM IN and ICIM OUT Cables • 5, 70
 ICIM IN and ICIM OUT Connectors • 3
 ICIM Introduction • 102
 ICIM MIB • 169
 ICIM2 as Proxy for Module Information • 267
 ICIM2-XD • 37
 ICIM2-XD Block Diagram • 57, 103
 ICIM2-XD Front Panel Features • 58, 104
 ICIM2-XD Illustration (Front Panel) • 58, 104
 ICIM2-XD Operation • 101
 ID • 354
 IEC • 354
 in-lb • 354
 Insert Module Table • 223
 Installing Application Modules • 86
 Installing LCI • 112
 Installing the ICIM2-XD • 85
 Installing the Power Supply • 75
 Installing the SOUP • 272
 Integration with an NMS (Optional) • 274
 Introduction • 33, 134, 154, 168
 IP • 354

L

Laser Warning • 102
 Launching Standalone (Windows Only) • 275
 LCD • 354
 LCI • 354

LCI Function • 110
 LCI Introduction • 110
 LCI Module Tree • 117
 LCI Operation • 109
 LED • 354
 Login • 95

M

Maintenance • 289
 Maintenance and Troubleshooting • 287
 Maintenance Record • 289
 Master-Slave Illustration • 73
 Master-Slave Operation • 72
 MIB • 354
 Midplane Bus Connectors • 45
 Modifying Module Alarm Limits using LCI • 129
 Module Alarm Table • 208
 Module Alarms • 342
 Module Control Table • 220
 Module Controls • 343
 Module Data • 340
 Module Details Window • 118
 Module MIB • 199
 Module Monitor Table • 217
 Module Monitors • 344
 Module Removal and Enhanced Traps • 267
 Module Table • 200
 Module Tree • 117
 Mounting the Chassis in a Rack • 65
 MSO • 354

N

nm • 355
 Nm • 355
 NMS • 355
 NTP • 355

O

Obtaining an RMA Number and Shipping Address • 316
 Obtaining Product Support • 314
 OID • 355
 OMI • 355
 Operating Environment • 61
 Operating the ICIM2-XD • 105
 Overview • 102, 336

P

Packing and Shipping the Product • 320

Power Inlet Illustration • 9, 79
 Power Inlets • 54
 Power Supply Configurations • 52
 Power Supply Cooling Fans • 81
 Power Supply Requirements • 75
 PR • 355
 Prisma II Enterprise MIBs • 168
 Prisma II ICIM2-XD • 57
 Prisma II Traps • 227
 Prisma II XD Chassis • 39
 Prisma II XD Platform • 36
 PWR • 355

Q

QAM • 355
 Quick Start Guide • 1

R

Rack Location Requirements • 63
 Recommended Equipment • 308
 Related Publications • 35
 Release Files • 273
 Remote Firmware Download Feature • 271
 Remote Reboot of ICIM2 and Modules • 226
 Remove Module Table • 223
 Replacing the Default Admin Account • 137
 Required Equipment and Tools • 60
 Return Product for Repair • 316
 RF • 355
 RMA • 355
 RO • 356
 RTC • 356
 RW • 356
 RX • 356

S

SE • 356
 semaphore • 356
 Setting Event Log Filter Parameters • 160
 Setting Trap Receive Parameters • 107
 Site Requirements • 61
 SMC • 356
 SNMP • 356
 SNMP Considerations • 105
 SNMP Management • 167
 SNMP Parameters • 100
 SNMP Settings • 282
 SNTP Time Synchronization • 186
 SOUP • 356
 SOUP Main Screen • 277

- Starting LCI Software • 116
- Step 1
 - Install the Chassis in a Rack • 2
- Step 10
 - Perform Chassis-to-Chassis ICIM2 Activation (Optional) • 25
- Step 11
 - Make Changes to Traps and Enterprise MIBs • 26
- Step 12
 - Make Physical Connections to Modules • 28
- Step 13
 - Verify System Release and Module Firmware Versions • 29
- Step 14
 - Install and Use the Firmware Update (SOUP) Utility (Optional) • 30
- Step 2
 - Make Chassis-to-Chassis ICIM2 Connections • 3
- Step 3
 - Make Electrical Power Connections • 6
- Step 4
 - Install the ICIM2 • 14
- Step 5
 - Set Network Parameters from the Command Line Interface (CLI) • 15
- Step 6
 - Connect the ICIM2-XD to the Network • 19
- Step 7
 - Install Modules in the Chassis • 20
- Step 8
 - Set Additional Parameters via CLI (Optional) • 22
- Step 9
 - Set and Verify SNMP Community Strings • 23
- Suggested Actions • 292, 293, 294, 295, 297, 299, 301, 302, 304, 306
- Support Telephone Numbers • 314
- SY • 356
- System Behavior • 267
- System Information • 345
- System Requirements • 111
- T**
- Telnet Session • 98
- The Chassis and the ICIM2 • 273
- Tips for Optimal Fiber-Optic Connector Performance • 308
- TNCS • 356
- To Access the DC-to-DC Converter • 295, 297, 299, 302, 304, 306
- To Access the Module Details, Double-Click the Chassis • 119
- To Access the Module Details, Double-Click the Module • 121
- To Access the Module Details, Right-Click the Chassis • 120
- To Access the Module Details, Right-Click the Module • 122
- To Change the Chassis ID Number • 4, 69
- To Check Alarms using LCI • 127
- To Check Manufacturing Data using LCI • 131
- To Check the Operating Status using LCI • 124
- To Clean Optical Connectors • 309
- To Configure Trap Destination • 229
- To Connect a Computer to the Chassis • 115
- To Connect Optical Cables • 89, 312
- To Connect RF Cables • 90
- To Enable Power Passing • 83
- To Install SOUP on Windows • 272
- To Install the Chassis in a Rack • 2, 65
- To Install the DC-to-DC Converter • 81
- To Install the ICIM2-XD • 14, 85
- To Install the LCI Software • 112
- To Install the Module • 20, 86
- To Install the Power Cord • 9, 79
- To Install the Power Supply in the Chassis • 10, 80
- To Make ICIM IN and ICIM OUT Cable Connections • 3, 68
- To Modify Alarm Limits using LCI • 129
- To Monitor the Power Supply • 83
- To Remove the Fan Assembly • 74
- To Remove the Module • 87
- To Set Additional Users for ICIM2 or ICIM2-XD Access • 22, 96
- To Set and Verify SNMP Community Strings • 97
- To Set Control Parameters using LCI • 125
- To Set the Clock • 96
- To Set Up a HyperTerminal Serial Port Session • 92
- To Set Up a Telnet CLI Session • 19, 98
- To Share Power Between Two Chassis • 11
- To Start LCI Software • 116
- To Uninstall the SOUP on Windows • 272
- trap • 357
- Trap Handling • 189

- Trap Logging Auxiliaries • 194
- Trap Logging Table • 194
- Trap Receiving Configuration • 228
- Trap Recv Table • 190
- Trap Types • 230
- Troubleshooting • 290
- TX • 357
- Typical Chassis Block Diagram • 42

U

- Unpacking and Inspecting the Chassis • 60
- Unused Slots • 64
- Usage • 275
- User Lockout • 148
- User Management • 133, 346

V

- V AC • 357
- V DC • 357
- Viewing the Event Log • 157

W

- Warning Labels • xxvii
- What is the Trap Logging Table? • 270
- When do traps associated with module insertion, removal, and alarms occur? • 269
- Where can I find trap definitions? • 270
- Why do the same alarm values represent different conditions? • 268
- Working With User Accounts • 141

X

- XD • 357
- XD Chassis • 37
- XD Chassis Alarm Data Parameters • 348
- XD Chassis Configurable Parameters • 348
- XD Chassis Control Board • 45
- XD Chassis Fan Assembly • 37, 51
- XD Chassis Manufacturing Data Parameters • 349
- XD Chassis Operating Status Parameters • 349
- XD Chassis Parameters • 348
- XD Platform Components • 36



Scientific Atlanta, A Cisco Company
5030 Sugarloaf Parkway, Box 465447
Lawrenceville, GA 30042

678.277.1000
www.scientificatlanta.com

This document includes various trademarks of Cisco Systems, Inc. Please see the Notices section of this document for a list of Cisco Systems, Inc., trademarks used in this document. Product and service availability are subject to change without notice.

© 2008 Cisco Systems, Inc. All rights reserved.
June 2008 Printed in United States of America

Part Number 4025479 Rev A