Disclaimer

Harmonic reserves the right to alter the equipment specifications and descriptions in this publication without prior notice. No part of this publication shall be deemed to be part of any contract or warranty unless specifically incorporated by reference into such contract or warranty. The information contained herein is merely descriptive in nature, and does not constitute a binding offer for sale of the product described herein. Harmonic assumes no responsibility or liability arising from the use of the products described herein, except as expressly agreed to in writing by Harmonic. The use and purchase of this product do not convey a license under any patent rights, copyrights, trademark rights, or any intellectual property rights of Harmonic. Nothing hereunder constitutes a representation or warranty that using any products in the manner described herein will not infringe any patents of third parties.

Trademark Acknowledgments

Harmonic and all Harmonic product names are trademarks of Harmonic Inc. All other trademarks are the property of their respective owners.

Compliance and Approval

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15, Subpart B of the Federal Communications Commission (FCC) rules.

These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment.

This equipment generates, uses, and can radiate radio frequency energy. It may cause harmful interference to radio communications if it is not installed and used in accordance with the instructions in this manual. Operation of this equipment in a residential area is likely to cause harmful interference. If this occurs, the user will be required to correct the interference at his or her own expense.

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Connections between the Harmonic equipment and other equipment must be made in a manner that is consistent with maintaining compliance with FCC radio frequency emission limits. Modifications to this equipment not expressly approved by Harmonic may void the authority granted to the user by the FCC to operate this equipment.

WEEE/RoHS Compliance Policy

Harmonic Inc. intends to comply fully with the European Union’s Directive 2002/96/EC as amended by Directive 2003/108/EC, on Waste Electrical and Electronic Equipment, also known as “WEEE,” and Directive 2002/95/EC, as amended, on the Restriction of use of Hazardous Substances, also known as “RoHS.”

Harmonic will ensure that product which cannot be reused will be recycled in compliance with the WEEE Directive. To that end, users are advised that (1) Harmonic equipment is not to be discarded in household or office garbage, (2) Harmonic Inc. will pay the freight for shipment of equipment to be disposed of if it is returned to Harmonic, (3) customers should call the normal RMA telephone numbers to arrange for such shipment, and (4) for additional and updated information on this process customers may consult the Harmonic website: http://harmonicinc.com/ah_weee_recycle.cfm.

Harmonic will ensure that its products will be either reused or recycled in compliance with the WEEE Directive. For the latest information concerning Harmonic’s WEEE/RoHS Compliance Policy and its Recycling and Take-Back process, please visit our web site.
产品中的有毒有害物质或元素的名称及含量表
Names and Contents of the Toxic and Hazardous Substances or Elements in the Products if the Part is Present

该表显示哈雷公司产品中可能含有的有毒有害物质元配件的信息，除了来源于元配件供应商的物料成分资料，亦来自其它相关的机构与资料。哈雷产品不一定使用这些元配件。

This table shows those components where hazardous substances may be found in Harmonic products based on, among other things, material content information provided by third party suppliers. These components may or may not be part of the product.

除非特殊注明，哈雷公司产品的环保使用期限 均为 20 年。该环保使用期限的有效条件为：必须遵循该产品使用手册的规定，对该产品进行使用或存储。

The Environmental Protective Use Period for Harmonic products is 20 years unless displayed otherwise on the product. The EPUP period is valid only when the products are operated or stored as per the conditions specified in the product manual.

<table>
<thead>
<tr>
<th>部件名称 (Part name)</th>
<th>有毒有害物质或元素 (Hazardous Substance)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>镉 (Pb)</td>
</tr>
<tr>
<td>印刷线路板 (Printed Circuit Assemblies)</td>
<td>X</td>
</tr>
<tr>
<td>机械组件 (Mechanical Subassemblies)</td>
<td>X</td>
</tr>
<tr>
<td>光学组件 (Optical Subassemblies)</td>
<td>X</td>
</tr>
<tr>
<td>电源 (Power Supplies)</td>
<td>X</td>
</tr>
<tr>
<td>缆线 / 线束 (Cables, harnesses)</td>
<td>X</td>
</tr>
<tr>
<td>屏幕 / 显示器 (Screens, Monitors)</td>
<td>X</td>
</tr>
<tr>
<td>金属零件 (Metal Parts)</td>
<td>O</td>
</tr>
<tr>
<td>塑料 / 发泡材料 (Plastics, foams)</td>
<td>O</td>
</tr>
<tr>
<td>电池 (Batteries)</td>
<td>X</td>
</tr>
</tbody>
</table>

O: 表示在该部件的所有均质材料中，此类有毒有害物质的含量均小于 SJ/T11363-2006 标准所规定的限量。
O: Indicates the content of the toxic and hazardous substances at the homogeneous material level of the parts is below the limit defined in SJ/T11363 2006 standard.

X: 表示至少在该部件的某一均质材料中，此类有毒有害物质的含量超出 SJ/T11363-2006 标准规定的限量。
X: Indicates that the content of the toxic and hazardous substances in at least one of the homogeneous materials of the parts is above the limit defined in SJ/T11363 2006 standard.
## Standards and Agency Approval

The following tables list regulatory standards and agency approvals:

### North America

<table>
<thead>
<tr>
<th>Standards</th>
<th>Agency Approval</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMI: FCC Part 15, Subpart B, ICES-003, Issue 2, Class A</td>
<td>FCC</td>
</tr>
<tr>
<td>Safety: UL 60950, CSA 60950</td>
<td>cTUV-us Mark</td>
</tr>
</tbody>
</table>

### Europe

<table>
<thead>
<tr>
<th>Standards</th>
<th>Agency Approval</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMI/EMC: EN55022, Class A, EN55024</td>
<td>CE</td>
</tr>
<tr>
<td>Safety: EN 60950</td>
<td>TUV-GS-Mark, CE</td>
</tr>
</tbody>
</table>

### Japan

<table>
<thead>
<tr>
<th>Standards</th>
<th>Agency Approval</th>
</tr>
</thead>
</table>

### Australia and New Zealand

<table>
<thead>
<tr>
<th>Standards</th>
<th>Agency Approval</th>
</tr>
</thead>
</table>
Documentation Conventions

This manual uses some special symbols and fonts to call your attention to important information. The following symbols appear throughout this manual:

**DANGER:** The Danger symbol calls your attention to information that, if ignored, can cause physical harm to you.

**CAUTION:** The Caution symbol calls your attention to information that, if ignored, can adversely affect the performance of your Harmonic product, or that can make a procedure needlessly difficult.

**LASER DANGER:** The Laser symbol and the Danger alert call your attention to information about the lasers in this product that, if ignored, can cause physical harm to you.

**NOTE:** The Note symbol calls your attention to additional information that you will benefit from heeding. It may be used to call attention to an especially important piece of information you need, or it may provide additional information that applies in only some carefully delineated circumstances.

**TIP:** The Tip symbol calls your attention to parenthetical information that is not necessary for performing a given procedure, but which, if followed, might make the procedure or its subsequent steps easier, smoother, or more efficient.

In addition to these symbols, this manual uses the following text conventions:

- **Data Entry:** indicates text you enter at the keyboard.
- **User Interface:** indicates a button to click, a menu item to select, or a key or key sequence to press.
- **Screen Output:** shows console output or other text that is displayed to you on a computer screen.
- **Bold:** indicates the definition of a new term.
- **Italics:** used for emphasis, cross-references, and hyperlinked cross-references in online documents.
# Table of Contents

## Chapter 1 Preface
1.1 Installation Guide Organization .............................................. 9  
1.2 Organization of This Manual .................................................. 9

## Chapter 2 ProStream 5000 Overview
2.1 ProStream 5000 Platform Hardware Overview ............................ 11  
2.1.1 ProStream 5000 Platform ............................................... 11

## Chapter 3 Planning a System
3.1 Checklists for Planning .................................................... 13  
3.2 Using the SMC Web Interface .............................................. 14  
3.2.1 Connecting to the SMC .................................................. 14  
3.2.2 Navigating Through the SMC ........................................ 15

## Chapter 4 Hardware Installation and Cabling
4.1 Safety Precautions ......................................................... 19  
4.2 Physical Hardware Installation ............................................ 20  
4.2.1 ProStream 5000 Platform Components ............................... 20  
4.2.2 Unpacking and Initial Installation .................................... 21  
4.2.3 Cabling the ProStream Platform 5000 Series ........................ 22  
4.3 RSA Provisioning ......................................................... 23  
4.4 SIM Provisioning (For ProStream 5000 Platform) ....................... 23

## Chapter 5 Platform Configuration
5.1 Common Configuration ..................................................... 26  
5.1.1 Setting the Static IP Address ......................................... 26  
5.1.2 To create a new routing table entry: ................................. 27  
5.1.3 Setting the Server Name ............................................... 28  
5.1.4 Setting Date and Time ............................................... 29  
5.1.5 Setting up Anti-virus Protection and Viewing Reports ................. 30  
5.1.6 Procedures to change 1+1 virtual IP/application interface IP ......... 34  
5.2 Individual Configuration .................................................. 35  
5.2.1 Network Interface Configuration .................................... 35  
5.2.2 Host Name Resolution ............................................... 37  
5.2.3 Address Resolution .................................................. 38  
5.2.4 DNS Resolution ..................................................... 39  
5.2.5 Network Common Setting ............................................ 40  
5.2.6 Network Load Balance ............................................... 40  
5.2.7 Network Load Balance Port Rules ................................... 41  
5.3 Firewall Setting .......................................................... 43  
5.4 Server Hardening (Lock-Down Protection) .................................. 44  
5.5 SNMP ................................................................. 44  
5.5.1 SNMP Settings ...................................................... 44
<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.5.2</td>
<td>Accepted communities</td>
<td>45</td>
</tr>
<tr>
<td>5.5.3</td>
<td>SNMP Traps setting</td>
<td>46</td>
</tr>
<tr>
<td>5.5.4</td>
<td>Downloading MIB data</td>
<td>47</td>
</tr>
<tr>
<td>5.5.5</td>
<td>Certificate Management</td>
<td>47</td>
</tr>
<tr>
<td>5.5.6</td>
<td>Image Upgrade</td>
<td>48</td>
</tr>
<tr>
<td>5.5.7</td>
<td>User Management</td>
<td>49</td>
</tr>
<tr>
<td>5.5.8</td>
<td>RAIDX Configuration</td>
<td>50</td>
</tr>
<tr>
<td>5.5.9</td>
<td>Managing the RAIDX Diagnostics Log</td>
<td>51</td>
</tr>
<tr>
<td>5.6</td>
<td>NIC Teaming Settings</td>
<td>52</td>
</tr>
<tr>
<td>5.6.1</td>
<td>Switch Fault Tolerance (SFT)</td>
<td>52</td>
</tr>
<tr>
<td>5.6.2</td>
<td>Teaming</td>
<td>52</td>
</tr>
<tr>
<td>5.6.3</td>
<td>Switch Requirements</td>
<td>52</td>
</tr>
<tr>
<td>5.7</td>
<td>Setting up 1+1 Redundancy</td>
<td>53</td>
</tr>
<tr>
<td>5.8</td>
<td>Setting Up 1+1 on SMC</td>
<td>57</td>
</tr>
<tr>
<td>5.8.1</td>
<td>Verification</td>
<td>59</td>
</tr>
<tr>
<td>5.9</td>
<td>NAS Configuration</td>
<td>59</td>
</tr>
<tr>
<td>5.9.1</td>
<td>Creating NAS mounting</td>
<td>59</td>
</tr>
<tr>
<td>5.9.2</td>
<td>Modifying a NAS Mounting</td>
<td>60</td>
</tr>
<tr>
<td>5.9.3</td>
<td>Deleting a NAS Mounting</td>
<td>61</td>
</tr>
<tr>
<td>5.10</td>
<td>Single Sign On (SSO) Configuration</td>
<td>61</td>
</tr>
<tr>
<td>5.10.1</td>
<td>Enabling SSO</td>
<td>61</td>
</tr>
<tr>
<td>5.10.2</td>
<td>Disabling SSO</td>
<td>61</td>
</tr>
<tr>
<td>6.1</td>
<td>Shutting Down and Rebooting the System</td>
<td>62</td>
</tr>
<tr>
<td>6.2</td>
<td>Starting, Stopping, and Restarting Services</td>
<td>63</td>
</tr>
<tr>
<td>6.3</td>
<td>Service Start and Stop</td>
<td>64</td>
</tr>
<tr>
<td>7.1</td>
<td>Anti-Virus Logs and Reports</td>
<td>65</td>
</tr>
<tr>
<td>7.2</td>
<td>Event Logs</td>
<td>65</td>
</tr>
<tr>
<td>7.3</td>
<td>System Message Logger</td>
<td>67</td>
</tr>
<tr>
<td>7.3.1</td>
<td>Category</td>
<td>68</td>
</tr>
<tr>
<td>7.3.2</td>
<td>Destination Settings</td>
<td>69</td>
</tr>
<tr>
<td>7.3.3</td>
<td>Mapping</td>
<td>73</td>
</tr>
<tr>
<td>7.3.4</td>
<td>Activating, Adding, or Removing a Log</td>
<td>75</td>
</tr>
<tr>
<td>7.4</td>
<td>Audit Trail Log</td>
<td>76</td>
</tr>
<tr>
<td>8.1</td>
<td>Viewing Status and System Information</td>
<td>77</td>
</tr>
<tr>
<td>8.1.1</td>
<td>Hardware Identification</td>
<td>78</td>
</tr>
<tr>
<td>8.1.2</td>
<td>Software Information</td>
<td>79</td>
</tr>
<tr>
<td>8.1.3</td>
<td>Diagnostics</td>
<td>80</td>
</tr>
<tr>
<td>8.1.4</td>
<td>Licensing Information</td>
<td>81</td>
</tr>
<tr>
<td>8.1.5</td>
<td>Viewing Disk Usage</td>
<td>82</td>
</tr>
<tr>
<td>8.1.6</td>
<td>Viewing Physical Disk Information</td>
<td>83</td>
</tr>
<tr>
<td>8.2</td>
<td>Viewing Anti-Virus Reports</td>
<td>84</td>
</tr>
</tbody>
</table>
### Table of Contents

8.3 Maintenance ................................................................. 84
8.3.1 Managing RAIDX Arrays .............................................. 84
8.3.2 Server Dump Files .................................................... 88
8.3.3 Backup and Restore Configuration ................................. 89
8.3.4 Restore Profiles ...................................................... 90
8.3.5 Replace a Hard Disk Drive (HDD) ................................. 90
8.3.6 Light Path Diagnostics ............................................... 90
8.3.7 Replace Power Supply ............................................... 91
8.3.8 POST Beep Codes ................................................... 92
8.3.9 Management Events ................................................ 92
8.3.10 1+1 Upgrade Procedures .......................................... 93
8.4 Ping Utility ............................................................... 96
8.5 Contacting Harmonic Support ........................................ 98

Glossary ............................................................................ 99
Chapter 1
Preface

This guide describes how to install and configure the pre-integrated Harmonic solution — Harmonic hardware platforms that are optimized for ProStream 5000 Platform software. It is the first part in the three-part installation process for a ProStream 5000 Platform system.

The following diagram illustrates the overall process for proper installation of a ProStream 5000 Platform system. Steps A through C are covered in this guide.

![ProStream 5000 Installation Flowchart](image)

Figure 1-1: ProStream 5000 Installation Flowchart

1.1 Installation Guide Organization

The installation procedures for a complete system are covered in three installation guides:

- **Platform Installation and Startup Guide** (this guide) — describes the installation of the underlying ProStream 5000 Platform upon which all applications run.

- **Application Configuration Guide** — describes configuration and use of specific on-demand applications, including VOD. These applications run on top of the ProStream 5000 Platform.

- **Ecosystem Configuration Guide** — describes configuration and use of on-demand applications, including VOD, in specific ecosystems.

You need to follow the procedures in all three guides to ensure the installation of an entire system application. Please refer to the configuration guides to complete the installation of the entire system.

1.2 Organization of This Manual

This installation guide is organized as follows:

- Chapter 1, Preface (this chapter), describes how to use the three installation guides and outlines the guide's organization.

- Chapter 2, ProStream 5000 Overview, describes the ProStream 5000 system and provides product specifications.

- Chapter 3, Planning a System, provides an overview of ProStream 5000 Platform server roles within an application, and describes using the SMC.
Chapter 4, *Hardware Installation and Cabling*, describes the ProStream 5000 Platform hardware installation, cabling, and RSA provisioning.

Chapter 5, *Platform Configuration*, describes configuration of the ProStream 5000 Platform.

Chapter 6, *Platform Operation*, describes basic system startup and shutdown operations.

Chapter 7, *Diagnostic Logs*, describes event logs and the System Message Logger.

Chapter 8, *Maintenance and Troubleshooting*, covers maintenance and monitoring tasks, and Harmonic Support contact information.

*Glossary* provides definitions for the most common abbreviations and acronyms used in this document.
This chapter contains an overview of the ProStream 5000 Platform hardware.

2.1 ProStream 5000 Platform Hardware Overview

Harmonic offers ProStream 5000 Platform models with different form factors. Each chassis is optimized for rack mounting, making it possible to deploy a very compact solution. The ProStream 5000 Platform models are:

- The ProStream 5000. (See 2.1.1 ProStream 5000 Platform on page 11.)

2.1.1 ProStream 5000 Platform

The Prostream 5000 front panel is shown in Figure 2-1 on page 11, and the back panel is shown in Figure 2-2 on page 11.

You can see these components on the front panel:

- A disk enclosure for up to four drives. Each slot has two LEDs that show the power and activity status of each drive.
- Two of the drives are mounted with CF cards. The other two are mounted with SSDs.

![Figure 2-1: Front panel of the ProStream 5000](image1)

![Figure 2-2: Back panel of the ProStream 5000](image2)

You can see these components on the back panel of the ProStream 5000:

- Power supply
- Network interfaces
2.1.1.1 ProStream 5000 G2

Figure 2-3: ProStream 5000 G2 – Front Panel

Figure 2-4: ProStream 5000 G2 – Back Panel
Chapter 3
Planning a System

This chapter provides guidelines for planning a ProStream 5000 Platform system, and gives a description of the System Management Console (SMC).

It contains the following sections:

- Planning your ProStream 5000 Setup and Configuration
- Using the SMC Web Interface

3.1 Checklists for Planning

The following checklists provide a general guideline for the settings you should define or configure:

**ProStream 5000 Platform Checklist**
- RAIDX build / format
- Interface role assignment (streaming / multicast / application)
- IP address assignment
- Routing table configuration
- Host name
- Host table
- Time zone and time server
- Initialize server settings

**Cluster Controller Checklist**
- Interface role assignment (streaming / multicast / application)
- IP address assignment
- Routing table configuration
- Host name
- Host table
- Time zone and time server
- Ensure that the modules are started (start services) — modules to be started depend on the roles defined for each server in the application
- Content ingest trick speed configuration
- Content replication configuration
- Asset management (FTP, Ingest Gateway)
- Middleware
- STB / RTSP
- Catcher
- DRM encryptor

For information about configuring individual modules, see the Platform Application Configuration Guide and the Platform Ecosystem Configuration Guide.
This guide assumes that you have evaluated your application needs, and are ready to begin putting the system together.

3.2 Using the SMC Web Interface

The System Management Console (SMC) is the main interface for configuring, operating, and maintaining the server. SMC is equipped with both an efficient console-based interface and a user-friendly web-based interface.

This section describes:

- Connecting to the SMC
- Navigating Through the SMC

3.2.1 Connecting to the SMC

If the ProStream 5000 Platform server has an IP address, you can access the server over the network to view the web-based SMC. Otherwise, you can connect a monitor, mouse, and keyboard to the server to view SMC locally.

For information about installing a ProStream 5000 Platform server and assigning it an IP address, or information about connecting locally, see 5.1 Common Configuration on page 26.

The web-based SMC displays a GUI that you can use to remotely configure a ProStream 5000 Platform server. When you first open a web browser to the server, the SMC opens to the Status screen.

Figure 3-2 on page 15 shows the information that you see from most cluster nodes and the special status screen that you see from the Cluster Controller.

![Figure 3-1: SMC's status screen](image-url)
The left pane displays a snapshot of the server’s status, or “health.” Most SMC nodes show you:

- The server’s name and the percent of CPU currently being used on it.
- Number of VOD streams active.
- Total broadcast channels, and total that are currently active.
- Status of RAIDX and of LSCP, RTSP, and RSVP protocols (healthy/enabled/disabled).
- Refresh: You can click to start a new refresh. You can reset the auto-refresh time. The current auto-refresh time is shown, and the time of last refresh.

The main pane opens to the Status tab by default:

- **Status** – initial SMC screen with overall status information about the node.
- The server, name and percent of CPU.
- System and RAID free space, and RAID status.
- Streaming status, number of VOD sessions current, and number of broadcast channels on this server.
- Status of protocol interfaces on this server (enabled/disabled).
- What scheduling capabilities are enabled on the server:
  - Whether broadcast channeling can be done through the server.
  - Whether the server can provide XML interface for ingest scheduling.

### 3.2.2 Navigating Through the SMC

This section assume that you have started the SMC and have the initial Status screen loaded. Navigate through the options by clicking a tab name to open it, and making the selections and entries as needed.

If a tab has sub-topics, they are listed.

[Folder] indicates there are more subtopics, [Table] indicates there are no subtopics to click.
For example, the Configuration tab has several subtopic folders, as shown in Figure 3-3 on page 16.

Figure 3-3: Main pane with tabs, topics, and subtopics

<table>
<thead>
<tr>
<th>Item</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AssetMgmt Adapter</td>
<td>[ Folder  ]</td>
<td>Manipulate asset management adapter configuration</td>
</tr>
<tr>
<td>ARAP Adapter</td>
<td>[ Folder  ]</td>
<td>Manipulate ARAP adapter configuration</td>
</tr>
<tr>
<td>SessionMgmt Adapter</td>
<td>[ Folder  ]</td>
<td>Manipulate session management adapter configuration</td>
</tr>
<tr>
<td>AssetController</td>
<td>[ Folder  ]</td>
<td>Manipulate asset controller configuration</td>
</tr>
</tbody>
</table>

The tabs are explained below:

- **Status**
- **Configuration**: Click a subhead to configure selections.
- **Service**: Start, stop, and restart services.
- **Platform**: Click a subhead to configure selections.
- **Operation**: Manage streaming parameters (not available on Cluster Controller servers).
- **Diagnostics**: Access logs and diagnostic information.
- **Software information**: View software version verification.
- **Backup/Restore**: Back up and restore system configuration files.

### 3.2.2.1 Path

The path display shows your position in each tab, and allows you to navigate by clicking the level you wish to move to. Figure 3-4 shows the path for the DRM Profile settings screen.

Figure 3-4: Path display in SMC
3.2.2.2 Buttons

Move to the screen level you want by clicking the menu item or button choice for that screen. Figure 3-5 shows the buttons for DRM Profile and Transcoder Profile.

Figure 3-5: Select button in SMC

To back up one level on each tab, click the file folder icon located below the path display, if one is available. To back up to any level in the path, click the name of the level. For example, in Figure 3-5, if you want to return to Configuration, simply click Configuration in the path.

3.2.2.3 Select

When an entry field shows a Select button, you can type in your entry or click Select to display a list of options to choose from (see Figure 3-5). The list of options will display in a new browser window, and when you click an option, the entry field will be populated with your selection automatically.

3.2.2.4 Tasks

You can create, edit, and delete configuration settings. A Task menu displays on the right side of the screen to offer you the available tasks for the current configuration. Figure 3-6 shows the Task menu for the Routing Table option.

Figure 3-6: Task menu in SMC

3.2.2.5 Data Entry

Entry fields marked with an * (asterisk) are required entries.

NOTE: User-defined names may not contain the following characters: \/* [] : | < > += ; , ? @. They may not consist entirely of any combination of periods (.) or spaces ( ).
In some settings where multiple entries are possible, the Add icon ( ) displays to the right of the field to facilitate adding entries to the setting. The icon appears only when the mouse pointer is positioned on that entry field. See Figure 3-7 for an example of an entry field with the Add icon and its attendant tool buttons.

**Figure 3-7: Add icon in SMC**

![Add icon in SMC](image)

### 3.2.2.6 Apply

On most screens, when you are finished making entries and selections, click the **Apply** button to make the settings active (see Figure 3-8).

**Figure 3-8: Apply settings button**

![Apply settings button](image)
This chapter describes how to install the ProStream 5000 Platform servers on a network, and how to prepare them to be configured for their respective roles.

This chapter has information about:

- Safety Precautions
- Physical Hardware Installation
- RSA Provisioning
- SIM Provisioning (For ProStream 5000 Platform)

4.1 Safety Precautions

To protect your ProStream 5000 Platform equipment from potential damage and to ensure your own personal safety, follow these safety guidelines:

- Never operate ProStream 5000 Platform with the cover removed.
- Before installing ProStream 5000 Platform, unplug the system to prevent electric or system board damage.
- To help prevent electric shock, plug the power cable into properly grounded sources. Use only properly grounded extension cords and adaptors, if they are needed.
- Make sure that nothing is lying on the ProStream 5000 Platform power cable.
- Be sure that the cables are located where they will not be stepped on or tripped over.
- Do not spill food or liquids on your ProStream 5000 Platform unit.
- Do not push any objects into the free slots of your ProStream 5000 Platform unit. Doing so will damage your ProStream 5000 Platform unit and can cause fire or electrical shock, and short out interior components.
- Keep your ProStream 5000 Platform unit away from heat sources and radiators.
- Do not block cooling vents.
- Do not place your ProStream 5000 Platform unit in a closed-in wall unit.
- When you disconnect a cable, pull on its connector or on its strain relief loop, not on the cable itself. Some cables have a connector with locking tabs; if you are disconnecting this type of cable, press in on the locking tabs before disconnecting the cable. As you pull connectors apart, keep them evenly aligned to avoid bending any connector pins.
- When you connect a cable, make sure that both connectors are correctly oriented and aligned before connecting to avoid bending connector pins.
4.2 Physical Hardware Installation

The ProStream Platform 5000 series is based on the IBM System x3650. For detailed instructions on setting up an IBM server, see Chapter 2 of the IBM System x3650 Installation Guide.

This section describes the following:
- ProStream 5000 Platform Components
- Unpacking and Initial Installation
- Cabling the ProStream Platform 5000 Series

4.2.1 ProStream 5000 Platform Components

The basic ProStream 5000 Platform package comes with the following components:

Table 4-1: ProStream 5000 Platform Components

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Documentation</td>
<td>Platform Installation and Startup Guide</td>
</tr>
<tr>
<td>This guide explains how to install, configure, and operate ProStream 5000 Platform servers on a ProStream 5000 Platform system.</td>
<td></td>
</tr>
<tr>
<td>Hardware components</td>
<td>Chassis (x1)</td>
</tr>
<tr>
<td>■ Cooling fan</td>
<td></td>
</tr>
<tr>
<td>■ Locking security cover</td>
<td></td>
</tr>
<tr>
<td>■ 19&quot; rack-mounting kit and rails</td>
<td></td>
</tr>
<tr>
<td>■ HDD enclosure</td>
<td></td>
</tr>
<tr>
<td>■ Flash memory adapter</td>
<td></td>
</tr>
<tr>
<td>■ Power cord</td>
<td></td>
</tr>
<tr>
<td>Network Interface Module (xN)</td>
<td>■ Gigabit Ethernet (UTP)</td>
</tr>
<tr>
<td>■ Dual Gigabit Ethernet (UTP)</td>
<td></td>
</tr>
<tr>
<td>■ Quad Gigabit Ethernet (UTP)</td>
<td></td>
</tr>
<tr>
<td>■ Hex Gigabit Ethernet (UTP)</td>
<td></td>
</tr>
<tr>
<td>Hard disk drive (xN)</td>
<td>■ HDD (SAS) 72 GB 15K</td>
</tr>
<tr>
<td>■ HDD (SAS) 147 GB 15K</td>
<td></td>
</tr>
<tr>
<td>■ HDD (SAS) 300 GB 15K</td>
<td></td>
</tr>
<tr>
<td>Dongle (depending on configuration)</td>
<td>USB license dongle</td>
</tr>
<tr>
<td>Software components</td>
<td>ProStream 5000 Platform software packaged in Compact Flash Card (x1)</td>
</tr>
<tr>
<td>ProStream 5000 Platform software Version 1.1</td>
<td></td>
</tr>
<tr>
<td>Software license (x1)</td>
<td>Base O/S license and client license pack</td>
</tr>
</tbody>
</table>
4.2.2 Unpacking and Initial Installation

1. Choose a suitable location for ProStream 5000 Platform.

2. Unpack ProStream 5000 Platform and its components carefully, and make sure that you have all the required components available.

3. If required, rack-mount the ProStream 5000 Platform by attaching the rack-mounting kit to the chassis with screws. Fasten the rail onto the 19-inch rack. In this way, ProStream 5000 Platform can be securely mounted.

4. Install the hard disk drives into the HDD enclosure properly.
   - Be sure to take appropriate ESD precautions and work in a properly grounded environment.
   - Swing open the main latch on the hard disk drive.
   - Carefully insert the new drive into the drive slot.
   - Ensure that the latch is locked to the HDD enclosure.

5. If AC power is used, make sure that the power supply is switched to the correct voltage (110/220V). The power cord connects to the power connector on ProStream 5000 Platform's rear panel.

   **NOTE:** In case a redundant power supply is used, two power cords are needed instead of one. Ensure that each cord is plugged into a separate power circuit.

6. Insert the flash card into the flash drive of the ProStream 5000 Platform server.
   - Ensure that the server is turned off.
   - Locate the flash memory card slot on the front of the server.
   - Insert the compact flash card. Push the card all the way down until it stays firmly in place. It is properly seated when the card eject button pops up.

7. Make sure that all network connections are connected properly. Ensure that the Gigabit Ethernet ports and the Management/Logging Fast Ethernet ports are connected to the appropriate devices.

8. Insert the appropriate license dongle.
4.2.3 Cabling the ProStream Platform 5000 Series

Connecting cables to the ProStream 5000 Platform is straightforward. Refer to the back panel of the corresponding model for placement of the ports.

4.2.3.1 Connecting the ProStream 5000 Platform server to storage expansion units

Use the SAS cable that comes with the storage expansion unit to connect the storage expansion unit to the ProStream 5000 Platform server in the following sequence:

Table 4-2: Connecting to Storage Expansion Units

<table>
<thead>
<tr>
<th>Connect from:</th>
<th>Connect to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>First expansion unit SAS “In” port</td>
<td>ProStream 5000 Platform server SAS 1 port</td>
</tr>
<tr>
<td>Second expansion unit SAS “In” port</td>
<td>ProStream 5000 Platform server SAS 2 port</td>
</tr>
<tr>
<td>Third expansion unit SAS “In” port</td>
<td>First expansion unit SAS “Out” port</td>
</tr>
<tr>
<td>Fourth expansion unit SAS “In” port</td>
<td>Second expansion unit SAS “Out” port</td>
</tr>
</tbody>
</table>

Figure 4-1 shows the position of the ports on the expansion units.
4.3 RSA Provisioning

RSA (Remote Supervisor Adapter) is an IBM tool that enables:

- Around-the-clock remote access and system management of the server
- Remote management, independent of the status of the managed server
- Remote control of hardware and operating systems
- Web-based management with standard web browsers

The RSA card is installed with the following default settings:

**Table 4-3: ProStream 5000 Platform Default RSA Settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP</td>
<td>10.10.10.10</td>
</tr>
<tr>
<td>Port</td>
<td>80</td>
</tr>
<tr>
<td>Web access user name</td>
<td>superuser</td>
</tr>
<tr>
<td>Web access password</td>
<td>smc!@#321</td>
</tr>
</tbody>
</table>

**NOTE:** All Harmonic ProStream 5000 Platform units have been set to the default values in Table 4-3. For security, Harmonic recommends that you change the default password during your initial session.

To provision the RSA you must give the card a unique IP address, so that you can access it remotely. You should perform this step as you deploy each ProStream 5000 Platform server to the network, and before you deploy another server. For detailed instructions on how to change the IP address, consult the *IBM Remote Supervisory Adapter User Guide*.

To access the RSA remotely:

1. Open a web browser and enter the IP address or host name of the RSA to which you want to connect. If you have not changed the default settings, use the values in Table 4-3.
2. The Enter Network Password window opens. Enter the user name and password. The RSA welcome page opens in your browser.
3. Select a time-out value from the drop-down list. RSA logs you off the web interface if the browser is inactive for the selected number of minutes.
4. Click **Continue** to start the session. The browser opens the System Status page, which gives you a quick view of the server status and the server “health” summary. You can now change the IP address of the RSA interface. Correct RSA setup for all the ProStream 5000 Platform servers in your system facilitates troubleshooting and technical support.

4.4 SIM Provisioning (For ProStream 5000 Platform)

Supermicro Intelligent Management (SIM) module implements IPMI 2.0 technology to provide remote access, monitoring and administration for Supermicro server platforms.

With SIM, server administrators can view a server’s hardware status remotely, receive an alarm automatically if a failure occurs, and power cycle a system that is non-responsive.

The SIM is installed with the default settings in *Table 4-4: Default Setting*. 
NOTE: All Harmonic ProStream 5000 units have been set to the default values in Table 4-4. For security, Harmonic recommends that you change the default password during your initial session.

### Table 4-4: Default Setting

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP</td>
<td>192.168.70.131 (for primary serverboard)</td>
</tr>
<tr>
<td></td>
<td>192.168.70.132 (for secondary serverboard)</td>
</tr>
<tr>
<td>Port</td>
<td>80</td>
</tr>
<tr>
<td>Web access user name</td>
<td>superuser</td>
</tr>
<tr>
<td>Web access password</td>
<td>smc!@#321</td>
</tr>
</tbody>
</table>

To provision the SIM you must give the card a unique IP address, so that you can access it remotely. You should perform this step as you deploy each ProStream Platform server to the network, and before you deploy another server. For detailed instructions on how to change the IP address, consult the *SuperMicro AOC-SIMSO+ User Guide*.

To access the SIM remotely:

1. Open a web browser and enter the IP address or host name of the SIM to which you want to connect. If you have not changed the default settings, use the values in Table 4-4.
2. The Enter Network Password window opens. Enter the user name and password. The IMM welcome page opens in your browser.
3. Click **Continue** to start the session. To get a quick view of the server status and the server “health” summary, select the System Healths > Monitor Sensors for *ProStream 5000 G1* and select the System Healths > Sensor Readings for *ProStream 5000 G2*.

You can now change the IP address of the SIM interface. To facilitate troubleshooting and technical support, ensure that all of the ProStream Platform servers in your system have the correct SIM setup.
This chapter first describes the common initial configuration necessary to place the server on
the network and run the SMC GUI. It then describes the individual settings that vary
depending on the specific role of the server.

This chapter describes how to make the following settings:

- **Common Configuration**
- **Individual Configuration**

For the configuration of specific applications and ecosystems, refer to the *Application
Configuration Guide*, and to the *Ecosystem Configuration Guide* relevant to your installation.

The ProStream 5000 Platform system can be configured in a variety of ways, depending on
the network environment and your video service needs. There are two main types of
platforms: ProStream 5000 Platform and Cluster Controller. Both share a number of common
settings, as seen in Table 5-1.

**Table 5-1: Platform Settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>ProStream 5000 Platform</th>
<th>Cluster Controller Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAIDX build / format</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Interface role assignment (streaming / multicast / application)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>IP address assignment</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Routing table configuration</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Host name</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Host table</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Time zone and time server</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Initialize server settings</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
5.1 Common Configuration

ProStream 5000 Platform is pre-configured to use the Dynamic Host Configuration Protocol (DHCP) to get an IP address and its basic TCP/IP settings.

If your network uses DHCP, the ProStream 5000 Platform obtains its TCP/IP settings automatically when you connect it to the network.

If DHCP is not enabled, then you must connect a pointing device (such as mouse or trackball), a keyboard, and a monitor to the server. After connecting these, you can log in to the System Management Console (SMC) directly and configure the basic TCP/IP information needed to get started and use SMC remotely. See 3.2 Using the SMC Web Interface on page 14 for instructions on using SMC.

After the initial configuration is completed, you can access SMC remotely via HTTP. To do so, open a browser on any machine that can connect to the ProStream 5000 Platform system, and type in the URL for the ProStream 5000 Platform server, using either the IP address or the host name/domain name format.

This section describes the following:
- Setting the Static IP Address
- Setting the static IP address Routing Table Adjustments
- Setting the Server Name
- Setting Date and Time

**NOTE:** These changes take effect after you reboot the ProStream 5000 Platform server. You must reboot before you can use SMC remotely, since it is a web-based console and relies on the IP address or host name to connect.

5.1.1 Setting the Static IP Address

To set the static IP address:

1. Navigate to `/Platform/Network/Interfaces`.

Check the appropriate Local Area Connection link that corresponds to the management network interface, and click **Open** in the **Task** list on the far right of the screen.

**Figure 5-1: Open a network interface**

<table>
<thead>
<tr>
<th>Status</th>
<th>Configuration</th>
<th>Service</th>
<th>Platform</th>
<th>Diagnostics</th>
<th>Software Information</th>
<th>Backup/Restore</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2. Click **Set static IP**.
3. Fill in the **IP address** and **subnet mask** that have been assigned to the ProStream 5000 Platform server using standard dotted-four notation. Enter the **Default Gateway address**, if needed.

4. Click **Apply**.

![Figure 5-2: Setting the static IP address](image)

Routing Table Adjustments

When you install a ProStream 5000 Platform server, the system automatically sets up the routing table. However, you might need to make adjustments to the routing table for your network. You can open existing routing tables entries only for viewing and deleting, not for editing.

5.1.2 To create a new routing table entry:

1. Navigate to `/Platform/Network/Routing Table`.

![Figure 5-3: Platform / Network / Routing Table](image)
2. Click **New** to create a new entry.

2. Click **New** to create a new entry.

**Figure 5–4: Routing Table configuration**

Enter **Network destination**.

Enter **Netmask**.

Enter **Gateway**.

Enter **Metric values (1 to 9999)**.

Enter **Interface**. (Optionally) You usually provide an IP address, but you can enter an interface ID number. If you leave this blank, the ProStream 5000 Platform system will try to discover the most suitable interface to use.

Select a **Type (Active /Persistent)**. This is an optional field:
- **Active**: The routing table entry is static and remains valid until reboot.
- **Persistent**: The routing table entry is persistent and remains valid even after reboot.

3. Click **Apply**.

**NOTE:** The network route cannot take effect unless at least one of the network interfaces can reach the gateway.

### 5.1.3 Setting the Server Name

1. Navigate to `/Platform/General`.

2. Enter new **Host name**.

3. Click **Apply**.
5.1.4 Setting Date and Time

An accurate system date and time are crucial to providing most video services, especially for time-shifted broadcast services. The simplest way to keep accurate time on your network is to use one of the many Network Time Protocol (NTP) servers available in your network.

**NOTE:** If an NTP time server is not available, configure the Cluster Controller server as "Operate as NTP Server". Times in the Cluster Controller and the ProStream Nodes must be synchronized.

To set date and time:

1. Navigate to /Platform/Operating System.

Select the appropriate **Time Zone Region**.
Enter **Local date and time**.

2. Click **Apply**.

### 5.1.5 Setting up Anti-virus Protection and Viewing Reports

To protect your platform from viruses, spyware, and malicious intrusion, ProStream includes anti-virus software in its installation. It has a real-time scan engine to ensure that the server is protected 24 hours a day.

The definition files are kept up to date. By default, this is done offline, with a patch. You can choose to do it online.

Real-time scans protect the server by scanning files when they are accessed or modified. This includes opening, running, copying, moving, renaming, and creating files. The scan profile is tuned to minimize the impact on both streaming and ingest performance.

In addition, more complete scans supplement the real-time scans. These scans are more extensive, but require a little more CPU load. You can set the weekly schedule for times when your CPU usage is lowest.

When a risk is detected, the software will attempt to clean the risk. It will also send a ProStream alarm, an SNMP trap, and an NMX alarm. You can review logs and reports from the management console in path: **/Operation / Anti Virus / Log**.

To set up anti-virus software, and to view reports, navigate to **/Operation / Anti Virus**.

**Figure 5-7: Operation / Anti Virus**

<table>
<thead>
<tr>
<th>Status</th>
<th>Configuration</th>
<th>Service</th>
<th>Platform</th>
<th>Operation</th>
<th>Diagnostics</th>
<th>Software Information</th>
<th>Backup/Restore</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Anti Virus" /></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Manipulate the anti virus**

**Path: / Operation / Anti Virus**

<table>
<thead>
<tr>
<th>Item</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Version" /></td>
<td>Table</td>
<td>Display the anti virus version</td>
</tr>
<tr>
<td><img src="image" alt="Schedule Scan" /></td>
<td>Table</td>
<td>Configure scheduled scan</td>
</tr>
<tr>
<td><img src="image" alt="Live Update" /></td>
<td>Table</td>
<td>Configure live update</td>
</tr>
<tr>
<td><img src="image" alt="Log" /></td>
<td>Folder</td>
<td>Display the log of anti virus</td>
</tr>
</tbody>
</table>

Complete the **Version**, **Schedule Scan (optional)**, and **Live Update** sections to set up the anti-virus software. Use the **Log** folder tab to view the anti-virus reports.
5.1.5.1  **View Anti-virus Version Information**

To see information about the anti-virus program installed on your server, navigate to **Operation / Anti Virus / Version**.

<table>
<thead>
<tr>
<th>Status</th>
<th>Configuration</th>
<th>Service</th>
<th>Platform</th>
<th>Operation</th>
<th>Diagnostics</th>
<th>Software Information</th>
<th>Backup/Restore</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Version</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Path: / Operation / Anti Virus / Version*

<table>
<thead>
<tr>
<th>Name</th>
<th>Symantec Antivirus</th>
</tr>
</thead>
<tbody>
<tr>
<td>Program</td>
<td>11.0.3001.2190</td>
</tr>
<tr>
<td>Scan engine</td>
<td>81.2.0.25</td>
</tr>
<tr>
<td>Virus definition</td>
<td>20081006.041</td>
</tr>
</tbody>
</table>

5.1.5.2  **Schedule the Anti-virus Scan**

Now schedule the scans.

1. Navigate to **/Operation / Anti Virus / Schedule Scan**.

   ![Schedule anti-virus scan operation](image)

   Scans are always scheduled weekly. Enter the **Day of the week** and **Time** (using a 24-hour clock) that you want the weekly scan to begin.

   2. Click **Apply**.

5.1.5.3  **Enable Anti-virus Live Updates**

To enable or disable live updates of anti-virus scans, follow these steps:

1. Navigate to **/Operation / Anti Virus / Live Update**.
2. Select **Enable** or **Disable**.
3. Click **Apply**.
5.1.5.4 View Anti-virus Logs and Reports

To view reports, navigate to Operation / Anti Virus / Logs.

**Figure 5-9: Anti-virus Logs**

<table>
<thead>
<tr>
<th>Item</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk History</td>
<td>[ Table ]</td>
<td>Display the risk history</td>
</tr>
<tr>
<td>Scan History</td>
<td>[ Table ]</td>
<td>Display the scan history</td>
</tr>
<tr>
<td>Event Log</td>
<td>[ Table ]</td>
<td>Display the event log</td>
</tr>
</tbody>
</table>

There are three reports to view in the anti-virus Log File section:

- Risk History
- Scan History
- Event Log

**Figure 5-10: Anti-virus log: risk history**

The anti-virus Risk History log tab shows information about risks:

- **Risk**: The name of the risk.
- **File**: The name of the infected file.
- **Action**: The action the anti-virus program took to the infected file.
- **Date**: The date and time when the risk was found.
Chapter 5 Platform Configuration

Common Configuration

Figure 5-11: Anti-virus log: scan history

<table>
<thead>
<tr>
<th>Scan status</th>
<th>Scan type</th>
<th>Started time</th>
<th>Completed time</th>
<th>Total files scanned</th>
<th>Total files infected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan Complete</td>
<td>Scheduled scan</td>
<td>10/7/2008 9:00:00 PM</td>
<td>10/7/2008 9:02:45 PM</td>
<td>14272</td>
<td>1</td>
</tr>
<tr>
<td>Scan Complete</td>
<td>Scheduled scan</td>
<td>10/6/2008 9:00:00 PM</td>
<td>10/6/2008 9:02:45 PM</td>
<td>14274</td>
<td>0</td>
</tr>
</tbody>
</table>

The anti-virus Scan History log table shows information about the anti-virus scan:

- **Scan status**: The status of a particular scan operation.
- **Scan type**: The type of scan, usually a Scheduled scan.
- **Started time**: The date and time when the scheduled scan started.
- **Completed time**: The date and time when the scheduled scan completed.
- **Total files scanned**: The number of files that were scanned.
- **Total files infected**: The number of files that were found to be infected.

Figure 5-12: Anti-virus log: event log

<table>
<thead>
<tr>
<th>Event</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>New virus definition file loaded. Version: 101006wo.</td>
<td>10/7/2008 9:02:45 PM</td>
</tr>
<tr>
<td>New virus definition file loaded. Version: 101005s.</td>
<td>10/6/2008 9:02:45 PM</td>
</tr>
</tbody>
</table>

The anti-virus Event Log lists the events that were discovered, with the time and date of each occurrence.
5.1.6 Procedures to change 1+1 virtual IP/application interface IP

Assumption: The 1+1 clustering is already setup/running.

On slave machine, follow these steps:

1. Navigate to "SMC / Configuration / Clustering / Clustering Configuration"
   - Click Disable to slave machine 1+1.

2. Navigate to /SMC / Platform / Network / Interfaces to change the application interface IP.

3. Navigate to SMC / Configuration / Clustering / Clustering Configuration to Change 1+1 interface IP settings.
   - The "Cluster Local Interface IP" should be chosen as the new application interface IP. Change the "Cluster Virtual Interface IP" if necessary.
   - Click Apply after changing the settings.

4. Configure IP settings for other modules.

5. Repeat steps (1) to (4) on master machine.
   - The Previous Virtual IP will become unreachable after performing the steps 1 on master machine.

6. On master machine, Navigate to "SMC / Configuration / Clustering / Clustering Configuration".
   - Click Enable to Enable 1+1 on master machine.

7. Reboot the master machine.

8. Verify that the master machine is up and services are running.
   - The new Virtual IP will become available.

9. Repeat steps 6 and 8 on slave machine.

10. Verify the clustering state.
    - MasterReady,SlaveReady if running properly.

11. The 1+1 Clustering will become normal with new Virtual IP and application IP.
5.2 Individual Configuration

Make the following settings according to the requirements of the role the server will perform.

This section describes the configuration for the following tasks:

- Network Interface Configuration
- Host Name Resolution
- Address Resolution
- DNS Resolution
- SNMP
- Certificate Management
- Image Upgrade
- User Management
- RAIDX Configuration

5.2.1 Network Interface Configuration

The server can be configured with a number of Ethernet interfaces. You can configure the function for each of these interfaces depending on the role the server will play in the system, and the capabilities of the interface. For example, you should reserve the Gigabit interfaces for streaming functions. Standard Ethernet interfaces could serve as multicast, application, or management interfaces. You can configure a single interface to serve more than one function.

Table 5-2 gives an overview of the interface tasks that can be assigned.

<table>
<thead>
<tr>
<th>Network Interface Function</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multicast</td>
<td>Use for content distribution and session management communication between the ProStream 5000 Platform nodes. IP multicast support is required on the multicast network.</td>
</tr>
<tr>
<td>Application</td>
<td>Use for system management and monitoring activities. Management traffic includes web interface access, remote desktop access, SSH (secure shell), and FTP content upload. Monitoring traffic includes SNMP and Syslog. Use for server-to-server traffic among the servers within the application, including communication between the Cluster Controller, Ingest Datapath, and the ProStream 5000 Platform servers, or between the ProStream 5000 Platform servers, or between the Harmonic ProStream 5000 Platform VOD system and other ecosystem servers such as the BMS, Middleware, and DRM Encryptor.</td>
</tr>
<tr>
<td>Network Interface Function</td>
<td>Explanation</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Streaming</td>
<td>Use to connect the ProStream 5000 Platform Streaming Servers to the CPE devices in an IP public network.</td>
</tr>
<tr>
<td>Primary Streaming</td>
<td>Use as the only streaming interface that can be used for some deployment configurations. For example, use it when NLB is enabled.</td>
</tr>
</tbody>
</table>
To configure a network interface:

1. Navigate to /Platform/Network/Interfaces

![Network Interfaces](image1)

2. Check a Local Area Connection link, and click **Open** to see the settings for that link.

![Set primary usage for network interface](image2)

3. Click **Apply**.

### 5.2.2 Host Name Resolution

To configure host name resolution:

1. Navigate to /Platform/Network/Host Name Resolution.
5.2 Platform Configuration

5.2.1 Individual Configuration

Figure 5-15: Changing the Host name

Host name. Create a New host by clicking the Task > New on the right, or select an existing one to edit and then click Task > Open.

If creating a new one, enter Host name and IP address. Enter IP Address. Optionally, you can enter a Comment, a user-defined description that will appear only in this screen.

2. Click Apply.

CAUTION: These changes are made directly to the host tables. Be very careful to enter all information correctly, or networking might not work as expected.

5.2.3 Address Resolution

Address resolution maps the IP address to the physical MAC address for use with the Address Resolution Protocol (ARP).

To create a new address resolution entry in the address translation tables:

1. Navigate to /Platform/Network/Address Resolution.
2. Click New on the Task bar on the right.

Figure 5-16: New address resolution for ARP table
3. Enter the **IP Address**.

4. Enter **MAC address**. If a Local interface address is present, this specifies the IP address of the interface that owns the translation table you are modifying. If not present, the settings are applied to the translation table for the first applicable interface that the system discovers on the host.

5. Click **Apply**.

---

**CAUTION:** These changes are made directly to the ARP tables. Be very careful to enter all information correctly, or networking might not work as expected.

---

### 5.2.4 DNS Resolution

To configure DNS Resolution:

1. Navigate to **Platform/Network/DNS Resolution**.

2. Enter options:

   **Append DNS Suffixes.** Choose one option from the drop-down menu: either **Append primary DNS suffixes** or **Append user-defined DNS suffixes**.

   If appending primary DNS suffixes, select a value for **Append parent suffixes of the primary DNS suffixes** (True / False). **Append user-defined DNS suffixes** is available only if you are appending user-defined DNS suffixes.

   To add an entry to the **Append user-defined suffixes in specified order (Domain)** field, move the mouse pointer to the right of **no entry** to display the **Add** icon. Click the icon. See Figure 5-18.

   Enter **user-defined suffixes** in specified order. Use the icons and arrows to the right...
of the field to make changes.

3. Click **Apply**.

### 5.2.5 Network Common Setting

Set network common settings for the system.

1. Navigate to **Platform / Network / Common Setting**.

![Figure 5-19: Network common setting](image)

**Multicast keep alive interval**. Enter a time in seconds. The server will check its multicast connection with other servers at this regular intervals.

2. Click **Apply**.

### 5.2.6 Network Load Balance

Use network load balancing to spread network traffic across a number of hosts. The load balancing uses clustering to enhance the scalability and availability of mission-critical IP-based services.

You can enable the network load balancing for each network interface role.

Follow these steps to set the parameters:

1. Navigate to **Platform / Network / Network Load Balance / Operation**.

![Figure 5-20: Network Load Balance Operation Settings](image)
**Interface role.** The column shows the role you can alter.

**Interface IP.** The IP address of the interface.

**Cluster IP.** The IP address used for the network load balanced cluster when enabled.

**Cluster subnet mask.** This will be used for the load-balancing cluster when it is enabled.

**Host priority.** This parameter specifies a unique ID for each host. If a new host joins the cluster, and its priority conflicts with another host in the cluster, the host is not accepted as part of the cluster. The rest of the cluster will continue to handle the traffic as before. A message describing the problem is written to the event log.

**NLB status.** Indicates whether network load balancing is enabled or disabled on this server.

2. To change settings, click to select a row in the table, then click the **Open** bar on the right of the window. The operation setting window opens:

![Figure 5-21: Configure Network Load Balancing](image)

The buttons under the path allow you to request several functions:

You can **Enable** or **Disable** load balancing for this interface role.

If you disable, click **Drain** to gracefully stop the network load balancing; new sessions will not be directed to this host, but the host will stay active long enough to handle loads it already has.

If you change parameters for **Cluster IP**, **Cluster subnet mask**, or **Host priority**, click **Apply** to set the changes.

### 5.2.7 Network Load Balance Port Rules

A range of ports are used for network load balancing. To see the properties for the port rules:

1. Navigate to **Platform / Network / Network Load Balance / Port Rules**.
Figure 5-22: Network Load Balancing Port Rules

<table>
<thead>
<tr>
<th>Status</th>
<th>Configuration</th>
<th>Service</th>
<th>Platform</th>
<th>Operation</th>
<th>Diagnostics</th>
<th>Software Information</th>
<th>Backup/Restore</th>
</tr>
</thead>
</table>

Network Load Balance Port Rules

Path: / Platform / Network / Network Load Balance / Port Rules

All of the properties of the Port Rules display in the columns.

- **Port rule name** is the unique name of the port rule.
- **Start port** is the number of the first port in the range of ports used.
- **End port** is the number of the last port in the range of ports used.
- **Associated module** is the module that uses the port to serve requests.
- **Associated interface** is the interface that the port rule applies to.
- **Port status** is the status of the port rule (enabled or disabled).

2. To see information about a specific Port rule name, click to check it in the first column, then click **Open** on the right side of the screen. A new window opens:

Figure 5-23: Port Rules for a specific port rule name

```
<table>
<thead>
<tr>
<th>Status</th>
<th>Configuration</th>
<th>Service</th>
<th>Platform</th>
<th>Operation</th>
<th>Diagnostics</th>
<th>Software Information</th>
<th>Backup/Restore</th>
</tr>
</thead>
</table>

Network Load Balance Port Rules

Path: / Platform / Network / Network Load Balance / Port Rules

Port rule name: Application:8080
Start port: 8080
End port: 8080
Associated module: SML_Adapters
Associated interface: Application
Port status: ENABLED
```
5.3 Firewall Setting

A firewall blocks incoming traffic on a network interface. It protects the platform from port attacks and virus intrusion attempts. When configured and enabled, it allows only specified incoming TCP/UDP ports to pass through.

To enable or disable a configured firewall:

1. Navigate to Platform / Network / Firewall Setting.

   ![Figure 5-24: Enable or disable active firewall settings](image)

<table>
<thead>
<tr>
<th>Status</th>
<th>Firewall on Application Interface</th>
<th>Port allowed</th>
<th>Firewall on Multicast Interface</th>
<th>Port allowed</th>
<th>Firewall on Primary Streaming Interface</th>
<th>Port allowed</th>
<th>Firewall on Streaming Interface</th>
<th>Port allowed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Active</td>
<td></td>
<td>Status</td>
<td></td>
<td>Status</td>
<td></td>
<td>Status</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enable</td>
<td>TCP: 21 22 80 161 554 556 557 559 1801 3399 5998 8080 8554 10021 23679</td>
<td>Enable</td>
<td>TCP: 554</td>
<td>Enable</td>
<td>TCP: 554 557 8554 10021</td>
<td>Enable</td>
<td>TCP: 554 557 8554 10021</td>
</tr>
</tbody>
</table>

- **Status** (read-only) shows whether the firewall is active or updating. This is the global status.

2. You can enable or disable the firewall setting on specific interfaces. Select Enable or disable for the following firewall settings:

   **Firewall on the Application Interface.** Select Enable or Disable. Below are the incoming ports allowed.

   **Firewall on Multicast Interface.** Select Enable or Disable. Below are the incoming ports allowed.

   **Firewall on the Primary Streaming Interface.** Select Enable or Disable. Below are the incoming ports allowed.

   **Firewall on the Streaming Interface.** Select Enable or Disable. Below are the incoming ports allowed.
5.4 Server Hardening (Lock-Down Protection)

To dependably deliver the best performance, ProStream 5000 must run on a stable, reliable and predictable environment. To protect against trojans, backdoors, or virus code, only trusted code and signed applications are allowed. Software and patches are checked when an install is attempted.

If either of these is true, the installation is not allowed and an alarm is triggered:
- The binary is not digitally signed by Harmonic, Inc. or by a Harmonic trusted party (for example, Symantec).
- The software tries to execute on an unauthorized folder (for example, \temp).

5.5 SNMP

The SNMP settings determine how the ProStream 5000 Platform server interacts on the network. This section includes:
- SNMP Settings
- Accepted communities
- SNMP Traps setting
- Downloading MIB data

5.5.1 SNMP Settings

1. Navigate to Platform/SNMP Configuration.

![SNMP Configuration](image)

Check / Uncheck Send authentication trap.

Check / Uncheck Accept SNMP packets from any host.
(Optional) **Accept SNMP packets from following host.** If **Accept SNMP packets from any host** is unchecked, you can add entries. Move the pointer to the right of no Entry to display the **Add** icon. Click the icon, then enter the name of a host.

2. Click **Apply**.

### 5.5.2 Accepted communities

You can designate a list of accepted communities that can use the SNMP services from the current server, and the access rights for that community.

To configure the accepted communities settings:

1. Navigate to **Platform /SNMP Configuration /Accepted communities**.

2. Create a new accepted community name, or edit (Open) an existing one.

*Figure 5-26: Accepted communities configuration*

![Accepted communities configuration](image)

*Figure 5-27: Configure a new Accepted community*

![Configure a new Accepted community](image)
Accepted community name. Enter a name if creating a new one. The name will be used by the SNMP client for identification purposes.

Community right. Select one: None / Notify / Read Only / Read and Write / Read and Create).

3. Click Apply.

5.5.3 SNMP Traps setting

To assign traps destinations:
1. Navigate to Platform/SNMP Configuration / Traps setting.

![Figure 5-28: SNMP Traps Setting](image)

2. To edit (Open) an existing one, checkmark the box beside it, then click Open from the Task list.
   To create a new one, click New in the Task list.

![Figure 5-29: New SNMP Trap](image)
Community name. Enter a name. (see also 5.5.2 Accepted communities on page 45).

Move the mouse pointer to the right of no entry to display the Add icon.

**Trap destinations.** Click the plus icon at no entry, to open an entry field and add traps destinations. To enter multiple destinations, click the Add icon next to the entry field.

3. Click **Apply**.

### 5.5.4 Downloading MIB data

You can download the MIB files for the components of this ProStream 5000 Platform server and view them or save them to disk.

1. Navigate to /Platform/SNMP Configuration.
2. Click **Download mibs**.
3. Depending on your browser settings, you will be prompted to save or view the mib.zip file.

### 5.5.5 Certificate Management

You can load certificates for use with security authentication for certain requests, for example NDS RTSP setup requests. ProStream 5000 Platform currently supports the following certificates:

- X.509
- Base-64 encoded X.509
- P7B
- SPC
- PEM

**To load a certificate:**

1. Navigate to **Platform/Certificate/Load Certificate**.
   
   Click **Load Certificate**.

   Enter a certificate name and path, or click Browse to select a certificate path.

   Enter your password.

2. Click **Apply**.

![Figure 5-30: Load Certificate](image)

**To view or delete a certificate:**

1. Navigate to **Platform/Certificate/Show Certificates**.
2. Select a certificate, and then click **Open** (to view) or **Delete** (to remove).

### 5.5.6 Image Upgrade

Occasionally Harmonic releases patches to the ProStream 5000 Platform operating system. In that event, you will need to load the patch in each ProStream 5000 Platform server.

Before you upgrade a ProStream 5000 node, put it in offline mode.

Sometimes, an upgrade will require you to re-create user accounts. Before you start the upgrade, make a record of all the user accounts.

**NOTE:** Before upgrading, make a record of your user accounts. After the upgrade, check to see if you need to re-create any of them.

First download the patch to a location on the network. To load a patch:

1. Log in to the FTP server of the ProStream 5000 to be upgraded.
2. Navigate to `/Virtual/Upgrade`.
3. Upload the upgrade package (the cab file) using binary mode.
4. Connect to the SMC web interface of the ProStream 5000 and navigate to `/Software Information / Image Upgrade`. You will see a list view if there are multiple upgrade packages available. If there is only one upgrade package available, the upgrade interface will open directly.
If there are multiple upgrade packages, select one here, then click **Open** on the Task list.

5. Click **Start Patch** to apply the upgrade package.

6. At the end of the image upgrade, check your user accounts. Recreate any that have been deleted.

### 5.5.7 User Management

You can add or delete user accounts.

To add a user:
1. Navigate to Platform/Users.

   ![Figure 5-34: Add User]

   Click New.

   Enter a Name.

   Enter a Password. It must be a minimum of 6 characters. It cannot be changed for 48 hours.

2. Click Apply.

### 5.5.8 RAIDX Configuration

RAIDX is a software-based RAID system. For information about how to view the physical disk information for the current system, see 8.1.6 Viewing Physical Disk Information on page 83. For RAIDX monitoring tasks, see 8.3.1 Managing RAIDX Arrays on page 84.

This option is not available on the Cluster Controller.

1. Navigate to Operation /RAIDX.

2. Click Build.

   ![Figure 5-35: Build RAIDX]
No. of sub RAID to build. Enter a number. The suggested number of disks to construct a sub RAID is 6. For example, if your ProStream 5000 Platform system has 30 disks, enter 5 (calculate 30/6 = 5).

No. of disk to build. Enter a number, equal to or less than the maximum number of disks on this ProStream 5000 Platform system.

3. Click Apply.

5.5.9 Managing the RAIDX Diagnostics Log

You can open the list of RAIDX diagnostic logs and select one to view it.

1. Navigate to Operation / RAIDX diagnostics log.

2. Click the checkbox to select a log in the list, then click the Open bar under the Task menu on the right.
5.6 NIC Teaming Settings

Teaming means that a team of ports functions as a single virtual network interface, and does not appear any different to other network devices than a non-teamed port.

5.6.1 Switch Fault Tolerance (SFT)

Switch Fault Tolerance (SFT) provides a failover relationship between two ports when each port is connected to a separate switch. SFT supports two ports per team.

This teaming mode provides automatic redundancy for your server’s network connection. If the primary port fails, the secondary port takes over. SFT supports two to eight ports per team. This teaming mode works with any switch; all team members must be connected to the same network.

While SFT will also work with hubs, it is only recommended to be used for troubleshooting purposes.

5.6.2 Teaming

A team of ports functions as a single virtual network interface and does not appear any different to other network devices than a non-teamed port.

5.6.3 Switch Requirements

Spanning Tree Protocol (STP) must be enabled on the switch, except that the ports connected to the teamed ports should have Port Fast or Edge Port enabled. This teaming mode works with any switch.

Teams configured in SFT must have all members in the same subnet (same layer 3 broadcast domain) in both single and multiple switch environments.

To set this up on SMC:

1. Navigate to / Platform / Network / Teaming / Setting (See Figure 5-37.)

2. Click New to create a new teaming on adapter.
3. The window changes, and now has a place for you to enter a name. (See Figure 5-38.)

4. Enter the name for your teaming.

5. Select the adapters to be included in the teaming.

6. To delete the teaming on adapter, click **Delete**.

### 5.7 Setting up 1+1 Redundancy

To set up 1+1 redundancy, first set up the clustering database. You will alternate between the master and slave machines to configure the settings.

**Note.**

*If any of the following actions failed on master:*

- SMC will redirect to the step 2 on master.
- User needs to click the next step on slave to fail the slave action and SMC redirect the slave to step 3.

*If any of the following actions failed on slave:*

- SMC will redirect to the step 3 on slave.
- User needs to click the next step on master to fail the master.

1. On both the master and the slave machines, open SMC and navigate to **Configuration / Clustering / Clustering Database**. (See Figure 5-39.)

   You will open the master with Master side setup. You will open the slave with Slave side setup.
2. On the master machine, click the Description Master side setup. A new window opens. (See Figure 5-40.)

Figure 5-40: Configure Clustering: Master side setup

3. On the slave machine, click the Description Slave side setup. A new window opens. (See Figure 5-41.)

Figure 5-41: Configure cluster: Slave side setup
4. On the master machine, click **Initialize master DB mirroring connection**. (See Figure 5-42.)

   **Figure 5-42: Master: Initialize DB mirroring connection**

   ![Master side setup screen](image)

   For the Slave IP, enter the slave machine interface that the server will use to make the back-to-back connection.

   Click **Apply** and wait for the operation to complete. When it is done you see blue text, **Method invoked successfully**.

5. On the slave machine, click **Making mirroring connection with master**. (See Figure 5-43.)

   **Figure 5-43: Slave: Make mirror connection with master**

   ![Slave side setup screen](image)

   For the Master IP, enter the instance that the server will use to make the back-to-back connection.

   Click **Apply** and wait for the operation to complete.
6. On the master machine, click **Making mirroring connection with slave**, and wait for the operation to complete.  

   ![Figure 5-44: Master – Make mirroring connection](image)

7. When the operation completes, click **Creating database(s) on master**, and wait for the operation to complete. (See Figure 5-45.)

   ![Figure 5-45: Creating databases on master](image)

8. When the operation is complete, go to the slave machine. On the slave machine, click **Creating database(s) on slave**. See Figure 5-46.)

   ![Figure 5-46: Creating databases on slave](image)

   **NOTE:** This operation will be in pending state until user performs step 9 on master machine within 1 minute. The timeout for this operation is 1 minute and the operation will be failed if user fails to perform step 9.
9. On the master machine, click Start the database mirroring (see Figure 5-47), and wait for both operations to complete: first the master’s Start the database (Step 9), and then the slave’s Creating database(s) (Step 8).

Figure 5-47: Start the database mirroring

<table>
<thead>
<tr>
<th>Status</th>
<th>Configuration</th>
<th>Service</th>
<th>Platform</th>
<th>Operation</th>
<th>Diagnostics</th>
<th>Software Information</th>
<th>Backup/Restore</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Master side setup</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Path: /Configuration/Clustering/Clustering Database/Master side setup

- Initialize master DB mirroring connection
- Making mirroring connection with slave
- Creating database(s)
- Start the database mirroring
- Re-initialize database mirroring
- Start re-initialize database mirroring connection
- End re-initialize database mirroring connection ip

5.8 Setting Up 1+1 on SMC

On the System Management Configuration, you need to specify these settings:

- Set CORBA Option Parameter IP, the MediaPrismController Management Interface Local Binding IP, and the Catcher Profile IP, to use the virtual IP which will be shared between the Master and Slave systems (labeled Cluster Virtual Interface IP further down this guide).

- CORBA Option Parameter is set as: /Platform/CORBA Naming Service/

- Management Interface Local Binding Address is set as: /Configuration/Media Prism/Media Prism Controller/

- Catcher Profile IP is set at: /Configuration/Media Prism/Media Prism Controller/Catcher Profile

For the 1+1 SRS setup, follow these steps:

1. Open the SMC interface on both the master machine and the slave machine.
2. On both the master and the slave machines, open the SMC and navigate to /Clustering /Clustering Configuration. (See Figure 5-48.)
Chapter 5 Platform Configuration

Setting Up 1+1 on SMC

Figure 5-48: Clustering configuration (for both master and slave)

<table>
<thead>
<tr>
<th>Status</th>
<th>Configuration</th>
<th>Service</th>
<th>Platform</th>
<th>Operation</th>
<th>Diagnostic</th>
<th>Software Information</th>
<th>Backup/Restore</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Clustering Configuration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Manipulate Clustering Configuration

Path: / Configuration / Clustering / Clustering Configuration

- **Private Interface IP**: The IP of the local interface where the 1+1 servers are making back to back connection.
- **Cluster Local Interface IP**: The IP of the local interface that the server will use as the cluster virtual interface.
- **Cluster Virtual Interface IP**: The virtual IP that the cluster will expose to the external network. Connection made to this IP from external network will be directed to the machine that assumed the master role. Please ensure that both machines use the same value for this field.
- **Cluster Virtual Interface Mask**: The network mask of the cluster virtual IP. Please ensure both machines use the same value for this field.
- **Node Identifier**: Identifier for the node.

NOTE: Ensure that the value entered in the Node Identifier field is different on the two machines.

3. Click **Apply** to save the changes.
4. Click **Enable** to start clustering.

After pressing enable, the SMC console will lose connection to the server due to NLB setting. You must reload the SMC after a few minutes to check the status.

The system will need to be rebooted after reloading the SMC.
5.8.1 Verification

The smc page will show clustering status if 1+1 setup has succeeded. The Clustering State should show ‘Local-MasterReady’ and ‘Remote-SlaveReady’ and vice versa for the other server.

![Figure 5-49: Verification](image)

5.9 NAS Configuration

This section gives instructions on how to mount a NAS (Network Attached Storage) to AsiaPlatform.

5.9.1 Creating NAS mounting

1. Navigate to /Platform/Network/NAS mounting.

![Figure 5-50: NAS Mounting](image)

2. Click New to create a new mounting.
3. **Name** is the alias to be used in the application configuration. Please refer to the specific application guide.

**NAS Persist Storage folder Path** is the folder share name at the NAS.

**Local IP Range Start** is the starting local IP address that will connect to the NAS.

**Local IP Count** is the number of IP addresses that will connect to the NAS. The IP addresses are continuously starting from the Local IP Range Start.

**NAS IP Range Start** is the starting IP address of the NAS.

**NAS IP Count** is the number of IP addresses available for NAS mounting. The IP addresses are continuous starting from the NAS IP Range Start.

If you would like NAS to require a login, please check **NAS Persist Storage Require Login** and fill in the login information.

Select the NAS type, Asia Platform currently supports **NFS** and **CIFS**.

Check **NAS Persist Storage Require Mount** so that the system will perform NAS mounting automatically.

Determine if you would want the application to take the effect **Now** or **After Reboot**.

4. Click **Apply** to save the changes.

### 5.9.2 Modifying a NAS Mounting

Select the mounting and click **Open**.
5.9.3 Deleting a NAS Mounting

Select the mounting and click Delete.

5.10 Single Sign On (SSO) Configuration

The Single Sign On feature is supported via the RADIUS protocol. After setting up the SSO, the authentication of SMC and another application GUI will be authenticated by the configured RADIUS server.

5.10.1 Enabling SSO

2. Check Enable RADIUS Authentication.
   - RADIUS Server Hostname: The IP address of the hostname of the RADIUS server.
   - RADIUS Server Port: The port number that the RADIUS server is listening to.
   - RADIUS Shared Secret: The shared secret with the RADIUS server.
3. Click Apply to save the change

5.10.2 Disabling SSO

2. Uncheck Enable RADIUS Authentication.
3. Click Apply to save the change.
This chapter describes the following operating procedures:

- Shutting Down and Rebooting the System
- Starting, Stopping, and Restarting Services
- Service Start and Stop

6.1 Shutting Down and Rebooting the System

To shut down or reboot the system:
1. Navigate to /Operating System.
2. Choose one of the following options:
   - Reboot
   - Shut down
   - Synchronize time; the message “Method is invoked successfully.” will be returned.
3. Click Apply.

![Figure 6-1: Shut down or reboot](image)
6.2 Starting, Stopping, and Restarting Services

To start, stop, or restart a service:

1. Navigate to /Service.

2. Click the radio button for a service (for example, AMI Adapters). Depending on its current state, the Task menu offers the available actions for that service. Unavailable actions are greyed. You can also double-click the service name to access its state and mode settings.

3. Click Start the service /Stop the service /Restart the service.

Figure 6-2: Manage Services

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Service Description</th>
<th>Current State</th>
<th>Start Mode</th>
<th>Affected Modules</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMI Adapters</td>
<td>Interfaces with external component for asset management functions.</td>
<td>Running</td>
<td>Soft</td>
<td></td>
</tr>
<tr>
<td>Asset Controller</td>
<td>Manages multiple Ingest and Playout modules to perform cluster level asset related operations.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FTP</td>
<td>FTP server</td>
<td>Running</td>
<td>Soft</td>
<td></td>
</tr>
<tr>
<td>SMJ Adapters</td>
<td>Interfaces with external component for session management functions such as session setup, session detail recording and etc.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Session Controller</td>
<td>Manages multiple playout modules to perform cluster level session related operations.</td>
<td>Running</td>
<td>Soft</td>
<td>SMJ Adapters</td>
</tr>
</tbody>
</table>
6.3 Service Start and Stop

To start or stop a service:
1. Navigate to /Service.
2. Select a service name.
3. Select an action from the Task list.

The “Kill the service” button is dimmed out, except when the service state is Starting or Pending Start. You can use it if you were trying to start the service, but want to cancel. For example, if it is unusually slow to start up, you might want to cancel your request and check to be sure the system itself is not in trouble.

Figure 6-3: Services start and stop

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Service Description</th>
<th>Current State</th>
<th>Start Mode</th>
<th>Affected modules</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTP</td>
<td>FTP server</td>
<td>Running</td>
<td>Soft</td>
<td></td>
</tr>
<tr>
<td>Ingest Module</td>
<td>Acquires the content from source, pre-process MPEG-TS content streams/files in real-time, transfers the pre-processed content to multiple Streaming Nodes. Optionally, sends pre-processed clear content to and receives encrypted content from DRM encryptor.</td>
<td>Running</td>
<td>Soft</td>
<td>Schedule Module Node Controller</td>
</tr>
<tr>
<td>Node Controller</td>
<td>Manages multiple Ingest and Playout modules to</td>
<td>Running</td>
<td>Soft</td>
<td></td>
</tr>
</tbody>
</table>
Chapter 7
Diagnostic Logs

This chapter describes the ProStream 5000 Platform diagnostic logging feature. It includes the following sections:
- Anti-Virus Logs and Reports
- Event Logs
- System Message Logger

7.1 Anti-Virus Logs and Reports
You can view logs and reports posted by the anti-virus software included in ProStream 5000. From the System Management Console, navigate to /Operation / Anti Virus / Logs. For more information, see 5.1.5.4 View Anti-virus Logs and Reports on page 32.

7.2 Event Logs
There are three log files available via SMC to help you track status and identify trouble spots:
- The Application log contains events that have been logged by application programs; these are helpful in troubleshooting problems with a specific application, for example an on-demand application.
- The Security log contains events related to possible security breaches, such as invalid password attempts.
- The System log contains events that have been logged by the operating system or its components; these are helpful in troubleshooting operating system or device issues.

Each log provides information about the type of event, the source of the event, the date and time the event occurred, and an event identifier. You can view these details for any specific event in any of the three logs.

For each log, you can:
- Select a specific type of event to display (for example, errors or warnings)
- Display events from a specific source module or application
- Restrict the display to events logged between particular days and times

To access the event log files from SMC, navigate to /Diagnostics /Event Log and select a log type.

For example, to see application logs, select Security from /Diagnostics /Event Log. Figure 7-1 on page 66 shows a security event log.
4. To view specific details, select an ID, then click **Open** from the Task button on the right. Figure 7-2 shows the Application Event Log details for ID 10.
7.3 System Message Logger

To use the System Message Logger you must:

■ Create a Category of messages to log
■ Designate the Destination settings
■ Create a Mapping of Category and Destination
■ Activate the log (Mapping)

Figure 7-3 shows the System Message Logger menu.

Figure 7-3: System Message Logger

These System Message Logger menu items are described in the following sections.

■ Category
■ Destination Settings:
  ■ File log destination
  ■ Scheduled file log destination
  ■ Event log destination
  ■ Network log destination
  ■ Syslog destination
■ Mapping
■ Activating, adding, or removing a log
7.3.1 Category

The Category defines a message scope.

To create, edit, or delete a message category and set the scope for that category:
1. Navigate to Diagnostics/System Message Logger/Category

   ![Category list](image)

2. Create a (New) category name, or edit (Open) an existing one (see Figure 7-4).

   ![Message Category](image)

3. Enter Category name, if creating a new one (see Figure 7-4).
4. Click Apply.
7.3.2 Destination Settings

After you set the Category for a log, you can configure the Destination settings. This section describes the following:

- File Log Destination — rotates log files according to file size
- Scheduled File Log Destination — rotates log files according to time stamp
- Event Log Destination — writes to the system event log with the specified source name
- Network Log Destination — writes the log to a specified port number
- Syslog Destination — writes the log using syslog protocol

7.3.2.1 File Log Destination

File Log Destination rotates the log file according to the log file size.

To configure File Log Destination settings:

1. Navigate to Diagnostics/System Message Logger/File Log.

2. Click File Log Destination.

3. Create a new file log destination, or edit (Open) an existing one from the list.
4. Enter Destination name, if creating a new one.
5. Enter Log file name.
6. Enter Log file size (in Bytes).
7. Enter Maximum number of files generated (minimum of 1).
8. Click Apply.

7.3.2.2 Scheduled File Log Destination

Scheduled File Log Destination rotates the log file according to a time stamp.

To configure Scheduled File Log Destination settings:
2. Click File Log Destination.
3. Create a (New) file log destination, or edit (Open) an existing one.
4. Enter **Destination name** (if creating a new one).
5. Enter **Log file** name.
6. Enter **File rotation scheme** (Crontab format).
7. Enter **Maximum number of files generated** (min 1).
8. Click **Apply**.

### 7.3.2.3 Event Log Destination

Event Log Destination writes the log to the system event log with a specified source name. To configure Event Log Destination settings:

1. Navigate to **Diagnostics/System Message Logger/Event Log**.
2. Click **Event Log Destination**.
3. Create a **(New)** event log destination, or edit **(Open)** an existing one.

![Figure 7-9: Event Log Destination](image)

4. Enter **Destination name**.
5. Enter **Source name**.
6. Select **Log level** (Error / Warning / Information).
7. Click **Apply**.
7.3.2.4 Network Log Destination

Network Log Destination writes the log file to a specified port number. You can retrieve the log via telnet to the machine and port.

To configure Network Log Destination settings:
1. Navigate to Diagnostics/System Message Logger/Network Log.
2. Click Network Log Destination.
3. Click (New), or select an existing log to (Open) or (Delete).

4. Enter Destination name.
5. Enter Port number (1025 to 65535).
6. Click Apply.

7.3.2.5 Syslog Destination

Syslog Destination writes the log file using syslog protocol.
1. Navigate to Diagnostics/System Message Logger/Syslog.
2. Click the Syslog Destination button.

3. Create a (New) syslog destination, or edit (Open) an existing one.
4. For new ones, enter a Destination name.
5. Enter **IP address** (IP where the syslog daemon is located).
6. Select **Protocol** (TCP or UDP).
7. Enter **Port number** (binding port of syslog daemon).
8. Select **Facility** (log type):
   - Kernel message
   - User level
   - Mail system
   - System daemons
   - Security or authorization message
   - System log internal
   - Line printer subsystem
   - Network news subsystem
   - UUCP subsystem
   - Clock daemon
   - Private security or authorization message
   - Ftp daemon
9. Select **Level**:
   - Emergency
   - Alarm
   - Critical
   - Error
   - Warning
   - Notice
   - Info
   - Debug
10. Click **Apply**.

### 7.3.3 Mapping

You build a mapping of the category and destination settings to relate a specific category to specific destination settings. The mapping can then be activated (see 7.3.4 Activating, Adding, or Removing a Log on page 75).

See 7.3.1 Category on page 68 and the relevant log destination information in this section for more information about Category and Destination settings.

The steps to create, edit, or delete a mapping are the same for all logs:
1. Navigate to **Diagnostics/System Message Logger/File Log**. Click **Mapping**.
2. To edit, select a map in the list, then click Open from the Task list on the far right.
3. Or, to create a mapping, click New.

Figure 7-12 shows the screen for a new mapping.

Figure 7-13: File Log Mapping
4. Enter **Mapping name** if creating a new mapping.
5. Select **Category**. A new window will pop up with choices.
6. Select **Log destination**. A new window will pop up with choices.
7. Click **Apply**.

### 7.3.4 Activating, Adding, or Removing a Log

To activate a log:

1. Navigate to `/Diagnostics/System Message Logger`.
2. You see a list of activated file logs.
   - Category
   - File Log
   - Scheduled File Log
   - Event Log
   - Network Log
   - Syslog

Figure 7-14 shows the **File Log** screen.

![Figure 7-14: Activated File Log](image-url)
3. Click **Select**, and choose a log from the pop-up window, or click the Add icon that appears when you move the mouse pointer over an entry field to add a log.

4. Click **Apply**. The log will be activated.

You can download a File log or a Scheduled File log via FTP, and navigate to `/Virtual/Logs/SystemMessageLogger`.

### 7.4 Audit Trail Log

All the user action performed in SMC or via the management application interface will be logged. It is facilitated by System Message Logger with the Scope PlatformAudit and is enabled by default with the default setting as in **Figure 7-15: File Log**. To change the setting, please refer to 7.3.2.1 *File Log Destination*.

To rotate the audit trail log based on schedule instead of log file size, please refer to 7.3.2.2 *Scheduled File Log Destination*.
This chapter shows how to view ProStream 5000 system status and settings and how to perform routine maintenance tasks.

To accurately troubleshoot a problem, you need to know what version of software you are running, hardware configuration information, and the ProStream 5000 Platform modules licensed for use on your system.

The System Management Console (SMC) is an easy way to monitor status and view the system settings.

This chapter includes the following sections:

- Viewing Status and Information
  - Diagnostics Tab
    - Hardware Identification
    - Software Information
  - Diagnostics
  - Licensing Information
  - Viewing Disk Usage
  - Viewing Physical Disk Information

- Viewing anti-virus information

- Diagnostics Tab

- Maintenance Operations:
  - Managing RAIDX Arrays
  - Server Dump Files
  - Backup and Restore Configuration
  - Restore Profiles
  - Replace a Hard Disk Drive (HDD)
  - Light Path Diagnostics
  - Replace Power Supply
  - POST Beep Codes

- The Ping Utility

- Contacting Harmonic Support, which contains contact information, including web address, mailing address, and contact phone numbers for Harmonic Inc.

### 8.1 Viewing Status and System Information

A snapshot of general status information is always available in the left pane of the System Management Console.
Select the Status tab to display more system information as shown in Figure 8-1:

**Server**
Identifies the current server and shows what percentage of the CPU is currently being used. This allows you to monitor for overload conditions.

**Storage**
Provides system and RAID free space amounts, and a basic health status for the RAIDX array.

**Streaming**
Shows the number of video-on-demand streams currently in progress and the number of broadcast channels in use.

**Protocol**
Shows which protocols are currently enabled and which are disabled. To change the protocols being used, select the Configuration tab and choose Stream Control from the list.

**Scheduler**
Shows which Program Scheduler options are currently enabled and which are disabled.

### 8.1.1 Hardware Identification

When troubleshooting a problem, it is important to know exactly what hardware is installed on your system and how it is configured.

To find configuration information:
1. Navigate to **Platform/Hardware Identification**.

   ![Figure 8-2: Hardware Identification](image)

   **Status** | **Configuration** | **Service** | **Platform** | **Operation** | **Diagnostics** | **Software Information** | **Backup/Restore**
---|---|---|---|---|---|---|---
```
Hardware Identification
```
show system hardware configuration
Path: / Platform / Hardware Identification
```
[Verify Hardware and Download Log] [Download Fingerprint XML]
```
Configuration number: 89-1580-01 (STL-2204-0)

2. (Optional) Click **Verify Hardware and Download log** to download a text file with complete system identification information.

3. (Optional) Click **Download Fingerprint XML** to download an xml file that includes your complete hardware configuration.

   You can use this for troubleshooting. For example, if you get a “hardware identification inconsistent” message, you can compare to find any differences between the certified hardware configuration and the actual current configuration.

### 8.1.2 Software Information

It is also important to know what version of software is installed. To see the software version:

1. Navigate to **Software Information/Version**.

   ![Figure 8-3: Software information](image)

   **Status** | **Configuration** | **Service** | **Platform** | **Operation** | **Diagnostics** | **Software Information** | **Backup/Restore**
---|---|---|---|---|---|---|---
```
Version
```
Display the image version
Path: / Software Information / Version
```
[Verify software version] [Download software version verification log]
```
Product name: StreamLinerimage
Product version: 6.1.400
Build number: 15

You can click **Verify software version** to confirm that the loaded software matches the installation disk. If it is not a match, you will get a message that says “Software verification result: Inconsistent found”.

You can click **Download software version verification log** to download a text file with complete system identification information.
8.1.3 Diagnostics

Open the diagnostics tab to read the event log, and open the system message logger.

![Diagnostics Tab](image)

**Figure 8-4: Diagnostics Tab**

<table>
<thead>
<tr>
<th>Item</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>License</td>
<td>[Folder]</td>
<td>Display various component capabilities</td>
</tr>
<tr>
<td>Remote Update</td>
<td>[Table]</td>
<td>Remote update of component capabilities</td>
</tr>
<tr>
<td>Event Log</td>
<td>[Folder]</td>
<td>Display event log</td>
</tr>
<tr>
<td>System Message Logger</td>
<td>[Folder]</td>
<td>Manipulate the system message logger</td>
</tr>
</tbody>
</table>
8.1.4 Licensing Information

To display a list of the terms of your ProStream 5000 Platform license, and features including the limits on stream count and bandwidth:

1. Navigate to Diagnostics/License.

![Figure 8-5: License information](image)

<table>
<thead>
<tr>
<th>Item</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ingest</td>
<td>[ Table ]</td>
<td>Display ingest capabilities</td>
</tr>
<tr>
<td>Content Management</td>
<td>[ Table ]</td>
<td>Display content management capabilities</td>
</tr>
<tr>
<td>Playout</td>
<td>[ Table ]</td>
<td>Display playout capabilities</td>
</tr>
<tr>
<td>RaidX</td>
<td>[ Table ]</td>
<td>Display RaidX capabilities</td>
</tr>
<tr>
<td>Program Scheduling</td>
<td>[ Table ]</td>
<td>Display program scheduling capabilities</td>
</tr>
</tbody>
</table>

2. Choose a component in the list to check specific allowances. Ingest is shown in Figure 8-6.

![Figure 8-6: Ingest Capabilities license information](image)

<table>
<thead>
<tr>
<th>Path: / Diagnostics / License / Ingest</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum number of concurrent network job</td>
</tr>
<tr>
<td>Maximum number of concurrent file job</td>
</tr>
<tr>
<td>Maximum session bandwidth</td>
</tr>
</tbody>
</table>
8.1.5 Viewing Disk Usage

View the storage capacity and usage for the hard disk storage on the ProStream 5000 Platform system to monitor how much space is available.

8.1.5.1 View System Volume Usage

In the dynamic video streaming environment, it is important to know how much disk space is currently available and how much is in use, so you can balance disk loads appropriately.

SMC shows you the volume information for all volumes installed on this ProStream 5000 Platform system. The information displayed includes total space, available space, and percentage of use. This allows you to track usage, and change volume characteristics if necessary.

To view system volume information, navigate to Platform/Storage/System Volume

**Figure 8-7: Display system volume information**

<table>
<thead>
<tr>
<th>Status</th>
<th>Configuration</th>
<th>Service</th>
<th>Platform</th>
<th>Operation</th>
<th>Diagnostics</th>
<th>Software Information</th>
<th>Backup/Restore</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>System Volume</td>
<td></td>
</tr>
<tr>
<td>Path:</td>
<td>/ Platform / Storage / System Volume</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Total disk space</th>
<th>Available disk space</th>
<th>Utilization</th>
<th>Hardware RAID Level</th>
<th>Hardware RAID Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>(MegaBytes)</td>
<td>(MegaBytes)</td>
<td>Percent</td>
<td>Not enabled</td>
<td>Not enabled</td>
</tr>
<tr>
<td>3669</td>
<td>1206</td>
<td>67.1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
8.1.5.2 View Data Volume Usage

To view data volume information, navigate to Platform/Storage/Data Volume

![Figure 8-8: Display data volume information](image)

<table>
<thead>
<tr>
<th>Status</th>
<th>Configuration</th>
<th>Service</th>
<th><strong>Platform</strong></th>
<th>Operation</th>
<th>Diagnostics</th>
<th>Software Information</th>
<th>Backup/Restore</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Data Volume</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Display data volume information

**Path:** / Platform / Storage / Data Volume

Total disk space (Megabytes) 1430469
Available disk space (Megabytes) 1129555
Utilization (Percent) 21.0
Hardware RAID Level Not enabled
Hardware RAID Status Not enabled

8.1.6 Viewing Physical Disk Information

Physical disk information can be useful for constructing RAIDX. See 5.5.8 RAIDX Configuration on page 50 for more information about RAIDX.

NOTE: This option is not relevant for Cluster Controllers.

To view physical disk statistics, navigate to Operation/Physical Disk Information.

![Figure 8-9: Physical Disk Information](image)
8.2 Viewing Anti-Virus Reports

To see logs from the anti-virus software installed on your ProStream 5000 clusters, open the System Management Console to **Operation / Anti Virus / Logs**.

![Figure 8-10: Anti-virus logs and reports](image)

For more information, see 5.1.5.4 View Anti-virus Logs and Reports on page 32.

8.3 Maintenance

This section has information about the following maintenance procedures:
- RAIDX arrays
- Server dump files
- Backing up and restoring configuration
- Restoring profiles
- Replacing the hard disk drive
- Diagnosing a light path
- Replacing the power supply
- POST beep codes

8.3.1 Managing RAIDX Arrays

For information about the RAIDX diagnostic log, see Managing the RAIDX Diagnostics Log on page 51.

These RAIDX maintenance tasks are addressed in this section:
- View the RAIDX array status
- Rebuild RAIDX Array
- Expand RAIDX Array
- Extend FS
- Verify
- Format Disk
- Mark Disk Offline
- View the RAIDX diagnostic log
NOTE: These options are not relevant for Cluster Controllers.

8.3.1.1 View the RAIDX array status

From the RAIDX screen you can see the following:
- The current health status for each disk in the RAIDX array
- The configuration for the array as a whole
- Disk status for the RAIDX array

To view the RAIDX screen, navigate to Operation/RAIDX.

Figure 8-11: RAIDX Main Panel
8.3.1.2 Rebuild RAIDX Array

To build or rebuild an array:
1. Navigate to Operation/RAIDX.
2. Click Build.

Figure 8-12: Building and re-building a RAIDX array

3. Enter the sub RAID ID.
4. Enter the physical disk ID.
5. Click Apply.

8.3.1.3 Expand RAIDX Array

When you add storage to an existing ProStream 5000 Platform server, you must then expand the RAIDX array.

To expand an array:
1. Navigate to Operation/RAIDX.
2. Click Expand.
3. Enter the number of the sub RAID to expand.
4. Click Apply.

Figure 8-13: Expand RAIDX
8.3.1.4 Extend FS

To extend the file system so that it recognizes the storage in the RAIDX array:
1. Navigate to Operation/RAIDX.
2. Click Extend FS. The message "Method is invoked successfully" is returned.

8.3.1.5 Verify

To verify the validity of the RAIDX system:
1. Navigate to Operation/RAIDX.
2. Click the Verify button. The message "Method is invoked successfully" is returned.

8.3.1.6 Format Disk

**CAUTION:** Formatting an existing RAIDX volume will cause all data in the volume to be destroyed. This operation is needed only when you are building a new RAIDX volume and should not be used unless you intend to reformat the whole volume.

1. Navigate to Operation/RAIDX.
2. Click Format.

![Figure 8-14: Format Procedure](image)

3. Check Dismount.
4. Click Apply.
5. Click OK to register the information.
6. Reboot the system so the change will take effect.

8.3.1.7 Mark Disk Offline

**CAUTION:** RAIDX performance will be degraded. This operation is typically used for testing, or for taking a faulty disk offline so that service will not be affected during disk replacement.

To mark a disk offline:
1. Navigate to Operation/RAIDX.
2. Select a disk from the Logical disk ID list.
3. Click Mark Disk Offline.
4. Select a Logical disk ID to take offline, and click the **Mark Disk Offline** button.

**8.3.1.8 Using the RAIDX Diagnostic Log**

To see the diagnostic logs for RAIDX, navigate to **Operation / RAIDX diagnostics log**.

To open any item in the list, click the checkbox, then click the **Open** button on the right.

**8.3.2 Server Dump Files**

In the event of a module crash on a ProStream 5000 Platform server, the server creates dump files. Harmonic Support uses these dump files to diagnose specific problems on the server.

To view dump files:
1. Navigate to **Platform/Node**.
8.3.3 Backup and Restore Configuration

It is good practice to keep a backup file of your existing configuration, and it is a good idea to store a copy on a server that is not part of the configuration. The backup process restores all the necessary information from the user browser machine, not the server machine.

To back up or restore system configuration files:

1. Navigate to the Backup/Restore tab.

   Click Configuration Backup/Restore. A new window opens.

   Figure 8-17: Backup / Restore Window

2. Click Save Configuration. when the process is complete, you will see a window with a message.
8.3.4 Restore Profiles

To restore profiles:

1. Navigate to Backup / Restore / Configuration Backup/Restore
2. Click the Restore Profiles button. A new window opens:

![Figure 8-18: Restore Profiles Window]

3. Click the checkmark the profile you want restored. Then click the Task button to restore it.
   - If you want to restore the configuration on a different server, copy the configuration file to that server. Then, choose the FullRestore profile option to tell ProStream 5000 to do a complete full restore, using the saved configuration file.
   - When upgrading the server machine, you will want to use the Custom profile so that the restore process restores the saved configuration.
4. If you do not see the profile you want on the list, click to checkmark the Search button, then click Task on the right to start the search.

8.3.5 Replace a Hard Disk Drive (HDD)

To replace an HDD:

1. Read the safety information in 4.1 Safety Precautions on page 19.
2. Move the handle on the drive to the open position (perpendicular to the drive).
3. Pull the hot-swap drive assembly from the bay.
4. Install the new hard disk drive in the hot-swap bay:
   - Make sure that the tray handle is open (perpendicular to the drive).
   - Align the drive assembly with the guide rails in the bay.
   - Gently push the drive assembly into the bay until the drive stops.
   - Push the tray handle to the closed (locked) position.
5. Check the hard disk drive status LED to verify that the hard disk drive is operating correctly.
6. If you need to reconfigure the disk array, see 8.3.1 Managing RAIDX Arrays on page 84 for information about how to configure the new HDD.

8.3.6 Light Path Diagnostics

To use the light path diagnostics:
1. Slide the latch to the left on the front of the operator information panel, and pull the panel forward. This reveals the light path diagnostics panel. Lit LEDs on this panel indicate the type of error that has occurred.

2. Note any LEDs that are lit, and then push the light path diagnostics panel back into the server.

3. Look at the system service label on the top of the server, which gives an overview of internal components that correspond to the LEDs on the light path diagnostics panel. For more detailed information, refer to page 52 of the Problem Determination and Service Guide.

4. Remove the server cover and look inside the server for lit LEDs. A lit LED on or beside a component identifies a component that is causing the error.

![Light Path Diagnostics](image)

Figure 8-19: Light Path Diagnostics

### 8.3.7 Replace Power Supply

To replace a power supply:

1. Read the safety information in 4.1 Safety Precautions on page 19 and Installation guidelines on page 87 of the Problem Determination and Service Guide. For full details, see page 118 of the Problem Determination and Service Guide.

2. If only one power supply is installed, turn off the server and peripheral devices.

3. Disconnect the power cord from the power supply that you are removing.

4. Grasp the power-supply handle.

5. Press the orange release latch down and hold it down.

6. Pull the power supply part of the way out of the bay.

7. Release the release latch; then, support the power supply and pull it the rest of the way out of the bay.

8. Slide the replacement power supply into the bay until the retention latch clicks into place. Ensure that there are adequate cooling fans installed.

9. Connect the power cord for the new power supply to the power cord connector on the power supply.

10. Connect the power cord to a properly grounded electrical outlet.

11. Make sure that the DC power LED and the AC power LED on the power supply are lit, indicating that the power supply is operating correctly.
8.3.8 POST Beep Codes

When you turn on the power, the server performs a series of tests to check the operation of the server components and some optional devices. These tests are called power-on self-test (POST). If POST is completed without detecting any problems, a single beep sounds, and the server startup is completed. If POST detects a problem, more than one beep might sound, or an error message might be displayed.

See the Problem Determination and Service Guide for full details on beep codes and possible resolutions.

8.3.9 Management Events

Management events fired by both AsiaPlatform and the applications will be logged for troubleshooting purpose. There are two pages for the events:

1. Current Alarms. This page lists all the currently asserted non-transient management event.

![Figure 8-20: Current Alarm for Management Events](image)
2. Alarm History. This page lists all the logged management events up to 3 months.

![Figure 8-21: Alarm History for Management Events](image)

### 8.3.9.1 Searching alarm history

To help searching for particular event to aid troubleshoot. Check the **Search** checkbox and the management events can be search by date, type, severity, source module and service affecting.

### 8.3.10 1+1 Upgrade Procedures

1. Temporarily remove slave node from cluster.
   - Access SMC of slave node and go to **Configuration / Clustering / Clustering Configuration**.
Press the **Disable** button as shown in Figure 8-22.

**Figure 8-22: Before clustering is disabled**

<table>
<thead>
<tr>
<th>Status</th>
<th>Configuration</th>
<th>Service</th>
<th>Platform</th>
<th>Operation</th>
<th>Diagnostics</th>
<th>Software Information</th>
<th>Backup/Restore</th>
</tr>
</thead>
</table>

- Path: / Configuration / Clustering / Clustering Configuration

- Private Interface IP *  
  - 192.168.10.134
- Cluster Local Interface IP *  
  - 172.31.1.134
- Cluster Virtual Interface IP *  
  - 172.31.1.135
- Cluster Virtual Interface Mask *  
  - 255.255.255.0
- Node Identifier ( 1 to 32 ) *  
  - 2
- Clustering Status  
  - Enabled
- Clustering State  
  - Local- SlaveReady(ID:12345678), Remote - MasterReady(ID:87654321)

After **Disable** button is pressed SMC will be displayed as shown in Figure 8-23.

**Figure 8-23: After clustering is disabled**

- Path: / Configuration / Clustering / Clustering Configuration

- Private Interface IP *  
  - 192.168.10.134
- Cluster Local Interface IP *  
  - 172.31.1.134
- Cluster Virtual Interface IP *  
  - 172.31.1.135
- Cluster Virtual Interface Mask *  
  - 255.255.255.0
- Node Identifier ( 1 to 32 ) *  
  - 2
- Clustering Status  
  - Disabled
- Clustering State  
  - Local - NotStarted, Remote - NotPresent

2. Follow normal upgrade procedures to apply patch to slave node.
3. Rejoin slave node to cluster.
   - Access SMC of slave node and go to **Configuration / Clustering / Clustering**
Configuration.

- Press the **Enable** button as shown in Figure 8-24.

**Figure 8-24: Before clustering is enabled**

<table>
<thead>
<tr>
<th>Path: / Configuration / Clustering / Clustering Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Status</strong></td>
</tr>
<tr>
<td>------------</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

- After **Enable** button is pressed SMC will be displayed as follows:

**Figure 8-25: After clustering is enabled and not reboot**

<table>
<thead>
<tr>
<th>Path: / Configuration / Clustering / Clustering Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Status</strong></td>
</tr>
<tr>
<td>------------</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
Reboot the server. SMC will be displayed as follows:

Figure 8-26: After clustering is enabled and rebooted

- The newly joined (and upgraded) node will be a slave node.

4. To upgrade the remaining master node:
   - Access SMC of master node and go to Configuration / Clustering.
   - Press the Failover button. Refresh the page until the status shows: "Local – SlaveReady (ID:…) Remote - MasterReady (ID:…)" which means that failover to slave node is completed.
   - Repeat step 1 to 3 on this node.

Note:
- If CORBA Option Parameter (SMC / Platform / CORBA Naming Service) is modified to use cluster virtual IP, CORBA Naming service will not be available before rebooting the server is completed.
- After finishing step 2 and during step 3, some services may not be able start as the slave node has not joined the cluster yet. This is expected and node status will return to normal after rebooting the server is completed.

8.4 Ping Utility

To use the Ping utility:
1. Navigate to Platform/Network/Network Utilities.
2. Click Ping.
3. Enter a destination (host name or host IP).
4. Click Apply.
Figure 8-27: Ping utility

Network Utilities

Path: / Platform / Network / Network Utilities

Ping

Destination *
8.5 Contacting Harmonic Support

The Harmonic Customer and Technical Support groups are available to help you with any questions or problems you may have regarding Harmonic products.

For assistance from within the U.S. and Canada, call toll free:
1.888.MPEGTWO (673.4896)

For assistance from outside the U.S. and Canada, call:
1.408.490.6477

The fax number is 408.490.6770.

The email address is techhelp@harmonicinc.com.

The corporate address for Harmonic Inc. is:
Harmonic Inc.
549 Baltic Way
Sunnyvale, CA 94089, U.S.A.
Attn: Customer Support

The corporate telephone numbers for Harmonic Inc. are:
Tel. 1.800.788.1330 (from the U.S. and Canada)
Tel. +1.408.542.2500 (outside the U.S. and Canada)
Fax. +1.408.490.6708

The web address for Harmonic Inc. is www.harmonicinc.com.
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARP</td>
<td>Address Resolution Protocol</td>
</tr>
<tr>
<td>ARAP</td>
<td>Advanced Resource Allocation Protocol</td>
</tr>
<tr>
<td>CIFS</td>
<td>Common Internet File System</td>
</tr>
<tr>
<td>CO</td>
<td>Central Office</td>
</tr>
<tr>
<td>CORBA</td>
<td>Common Object Request Broker Architecture</td>
</tr>
<tr>
<td>CPE</td>
<td>Customer Premises Equipment</td>
</tr>
<tr>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name System</td>
</tr>
<tr>
<td>DRM</td>
<td>Digital Rights Management</td>
</tr>
<tr>
<td>DSLAM</td>
<td>Digital Subscriber Line Access Multiplexer</td>
</tr>
<tr>
<td>HDD</td>
<td>Hard disk drive</td>
</tr>
<tr>
<td>HFC</td>
<td>Hybrid fibre coax</td>
</tr>
<tr>
<td>IA</td>
<td>Intel Architecture</td>
</tr>
<tr>
<td>IDP</td>
<td>Ingest datapath</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>ISA</td>
<td>Interactive Services Architecture</td>
</tr>
<tr>
<td>LSCP</td>
<td>Lightweight Streaming Control Protocol</td>
</tr>
<tr>
<td>MPEG</td>
<td>Moving Picture Experts Group</td>
</tr>
<tr>
<td>MPTS</td>
<td>Multi Program Transport Stream</td>
</tr>
<tr>
<td>MSMQ</td>
<td>Microsoft Message Queue</td>
</tr>
<tr>
<td>NGOD</td>
<td>Comcast’s Next Generation On Demand</td>
</tr>
<tr>
<td>NTP</td>
<td>Network Time Protocol</td>
</tr>
<tr>
<td>NPVR</td>
<td>Network Personal Video Recorder</td>
</tr>
<tr>
<td>NVOD</td>
<td>Near Video on Demand</td>
</tr>
<tr>
<td>OPEX</td>
<td>Operating expense</td>
</tr>
<tr>
<td>PAT</td>
<td>Program Association Table</td>
</tr>
<tr>
<td>PID</td>
<td>Packet Identifier</td>
</tr>
<tr>
<td>POST</td>
<td>Power-On Self-Test</td>
</tr>
<tr>
<td>PMT</td>
<td>Program Mapping Table</td>
</tr>
<tr>
<td>Acronym</td>
<td>Definition</td>
</tr>
<tr>
<td>---------</td>
<td>------------</td>
</tr>
<tr>
<td>PSIP</td>
<td>Program and System Information Protocol</td>
</tr>
<tr>
<td>QAM</td>
<td>Quadrature Amplitude Modulation</td>
</tr>
<tr>
<td>RAID</td>
<td>Redundant Array of Independent Disks</td>
</tr>
<tr>
<td>RSVP</td>
<td>Resource Reservation Protocol</td>
</tr>
<tr>
<td>RTSP</td>
<td>Real Time Streaming Protocol</td>
</tr>
<tr>
<td>SCP</td>
<td>Secure Copy</td>
</tr>
<tr>
<td>SDX</td>
<td>Service Deployment System (Juniper® Networks)</td>
</tr>
<tr>
<td>SFS</td>
<td>Streaming File System</td>
</tr>
<tr>
<td>SIMD</td>
<td>Single instruction, multiple data</td>
</tr>
<tr>
<td>SMC</td>
<td>Server Management Console</td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management Protocol</td>
</tr>
<tr>
<td>SMP</td>
<td>Session Management Protocol</td>
</tr>
<tr>
<td>SNC</td>
<td>Single node cluster</td>
</tr>
<tr>
<td>SOAP</td>
<td>Simple Object Access Protocol</td>
</tr>
<tr>
<td>SPTS</td>
<td>Single program transport stream</td>
</tr>
<tr>
<td>SVP</td>
<td>Secure video processor</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission control Protocol</td>
</tr>
<tr>
<td>TD</td>
<td>Topology Discovery</td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td>URI</td>
<td>Uniform resource identifier</td>
</tr>
<tr>
<td>URL</td>
<td>Uniform resource locator</td>
</tr>
<tr>
<td>USB</td>
<td>Universal serial bus</td>
</tr>
<tr>
<td>UTP</td>
<td>Unshielded twisted pair</td>
</tr>
<tr>
<td>VOD</td>
<td>Video On Demand</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual private network</td>
</tr>
</tbody>
</table>