### Table of Contents

#### About This Guide
- v
  - Overview v
  - Target Audience v
  - Organization vi
  - Conventions vi
  - Related Documentation ix
  - Customer Support x

#### UnityOne Overview
- 1
  - Overview 1
  - UnityOne Overview 1
  - UnityOne Environment 2
  - UnityOne 200/400/1200/2400 Chassis Overview 5

#### Prepare the Site
- 9
  - Overview 9
  - Safety Requirements 10
  - Rack and Clearance Requirements 12
  - Ventilation and Location 12
  - Environmental Requirements 13
  - Power Requirements 13
  - System Grounding Requirements 13
  - Cabling Requirements 14
  - Fiber-Optic Connection Guidelines 14
  - Unpack the UnityOne System 15

#### Hardware Installation and Configuration
- 17
  - Overview 17
  - Install the UnityOne Chassis 18
  - Attach Network Connections 21
  - Check LEDs 22
  - UnityOne Setup Wizard 23

#### Setup Wizard
- 25
  - Overview 25
  - Out-of-the-Box Terminal Setup Wizard 26
# List of Figures

<table>
<thead>
<tr>
<th>Figure Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>The UnityOne™ Environment</td>
<td>3</td>
</tr>
<tr>
<td>UnityOne™ Model 1200</td>
<td>4</td>
</tr>
<tr>
<td>DB-9 Connector</td>
<td>23</td>
</tr>
<tr>
<td>RJ-45 Connector</td>
<td>24</td>
</tr>
<tr>
<td>RJ-45 Connector</td>
<td>25</td>
</tr>
<tr>
<td>SFP Transceiver</td>
<td>25</td>
</tr>
</tbody>
</table>
List of Figures
About This Guide

Explain who this book is intended for, how the information is organized, where information updates can be found, and how to obtain customer support if you cannot resolve a problem.

Overview

Welcome to Tipping Point Technologies’ (TPT) UnityOne™ 200/400/1200/2400 Installation and Configuration Guide. The UnityOne is an Intrusion Prevention System (IPS) that provides a unified approach to network security.

This chapter includes the following sections:

• “Target Audience” on page v
• “Organization” on page vi
• “Conventions” on page vi
• “Related Documentation” on page ix
• “Customer Support” on page x

Target Audience

This guide is intended for use by technicians and maintenance personnel responsible for installing, configuring, and maintaining the UnityOne. Users should be familiar with telecommunications products and networking concepts.
Organization

The IPA Installation and Configuration Guide is organized as follows:

About the Guide
Explains who this book is intended for, how the information is organized, where information updates can be found, and how to obtain customer support if you cannot resolve a problem.

Overview
Provides a description of the deployment environment of the UnityOne, including layout and illustrations of hardware components and features.

Prepare the Site
Provides requirements for the installation site and guidelines for electrical and network connections.

Install and Configure the System
Provides installation instructions for the hardware components and procedures for initial configuration tasks.

Appendix A: Technical Specifications
Provides hardware and software specifications for the UnityOne system.

Appendix B: Connector and Pinout Specifications
Provides connector and pinout information for the UnityOne system.

Appendix C: Power Supply Module Replacement
Provides information and instructions for replacing the power supply module for the UnityOne system.

Appendix D: IPS Menu Options
Provides information and instructions for using the LCD buttons of an IPS device.

Conventions

This book, and the other books in this series, follow some conventions for structuring information.

Headings
Every chapter starts with a brief description of the information you can find in that chapter, which correlates with the major headings in that chapter. Each major heading corresponds to a task or concept that is important for you to understand. Headings are of a different size and type to make them easy to skim, whether you are viewing an online or print copy of this document.

Typeface
This book uses the following typeface conventions:
Bold Used for the names of screen elements like buttons, drop-down lists, or fields. For example, when you are done with a dialog, you would click the **OK** button.

Code Used for text a user must type to use the product.

*Italic* Used for book titles, variables, and important terms.

Hyperlink Used for web site and cross reference links.

### Cross References

When a topic is covered in depth elsewhere in this guide, or in another book in this series, a cross reference to the other information will be provided. Cross references within this book will take the form: “for more information about conventions, see page 6, Conventions.” Cross references to other publications will take the form: “for more information about `<topic>`, see *Publication Name*.”

### Messages

Messages are special text that are emphasized by font, format, and icons. There are four types of messages in this book:

- Warning
- Caution
- Note
- Tip

A description of each message type with an example message follows.

#### Warning

Warnings tell you how to avoid physical injury to people or equipment. For people, injury includes anything from temporary conditions, such as pain, to irreversible conditions such as death. For equipment, injury means anything requiring repair. Warnings tell you what you should or should not do, and the consequences of not heeding the warning.

Warnings have an icon to the left showing a white lightning bolt drawn inside of a red octagon. Warnings also start with the word “**WARNING**”, and are presented in bold face type.

**WARNING:**

![Warning Icon] Only trained and qualified personnel should install, replace, or service this equipment. Disconnect the system before servicing.

#### Caution

Cautions tell you how to avoid a serious loss that stops short of physical damage such as the loss of data, time, or security. Cautions tell you what you should or should not do to avoid such losses, and the consequences of not heeding the caution.
Cautions have an icon to the left showing a black exclamation point drawn inside of a yellow triangle. Cautions also start with the word “CAUTION”.

**CAUTION:** Do not type del *.:* from the root (C:\) directory. Typing del *.:* from the root directory will destroy all the program and configuration data that your computer needs to run, and will render your system inoperable.

**Note**
Notes tell you about information that might not be obvious, or that does not relate directly to the current topic, but that may affect relevant behavior.

A note has an icon to the left showing a piece of note paper, and starts with the word “Note”.

**Note:** Most car rental companies no longer allow cash deposits in lieu of a credit card when renting a car. Non-credit card deposits can only be arranged by a lengthy application and approval process.

**Tip**
Tips are suggestions about how you can perform a task more easily or more efficiently.

A tip has an icon to the left showing a light bulb drawn inside and starts with the word “Tip”.

**Tip:** Setting the *logging* parameter to “off” or “minimal” will improve your system’s processing performance, but it will make debugging very difficult in the event of a system crash. During system integration, you can set logging to “full” to ease debugging. After you have finished testing, set logging to “minimal” to improve performance.
Related Documentation

The UnityOne systems have a full set of documentation. These publications are available in electronic format on your installation CDs. For the most recent updates, check the Threat Management Center (TMC) web site at https://tmc.tippingpoint.com.

Table 1: UnityOne Documents

<table>
<thead>
<tr>
<th>Audience</th>
<th>Publication</th>
<th>Location</th>
</tr>
</thead>
</table>
| Hardware Technicians| • Quick Start UnityOne-50  
                      • Quick Start UnityOne-2000  
                      • Quick Start UnityOne 200/400/1200/2400 | printed version in the UnityOne box, UnityOne Documentation CD,  
                                                       https://tmc.tippingpoint.com |
|                     | • UnityOne-50 Installation and Configuration Guide  
                      • UnityOne-2000 Installation and Configuration Guide  
                      • UnityOne 200/400/1200/2400 Installation and Configuration Guide  
                      • UnityOne Zero Power High Availability Installation Guide | UnityOne Documentation CD,  
                                                       https://tmc.tippingpoint.com |
|                     | UnityOne Security Manager System Quick Start Guide | printed version in the UnityOne box, UnityOne Documentation CD,  
                                                       https://tmc.tippingpoint.com, IPS server |
| System Administrators| UnityOne Local Security Manager User's Guide | UnityOne Documentation CD,  
                                                       https://tmc.tippingpoint.com |
|                     | UnityOne Local Security Manager Online Help | available in the LSM application |
|                     | Unity One Command Line Interface Reference | UnityOne Documentation CD,  
                                                       https://tmc.tippingpoint.com |
|                     | UnityOne Security Manager System Quick Start Guide | hard copy in the shipping materials, UnityOne Documentation CD,  
                                                       https://tmc.tippingpoint.com |
|                     | UnityOne Security Management System User's Guide | UnityOne Documentation CD,  
                                                       https://tmc.tippingpoint.com |
|                     | UnityOne Security Management System Online Online Help | available in the SMS application |
|                     | UnityOne Migration Guide | UnityOne Documentation CD,  
                                                       https://tmc.tippingpoint.com |
Customer Support

The TippingPoint Technologies customer support phone number is 1-866-681-8324.

TippingPoint Technologies is committed to providing quality customer support to all of its customers. Each customer is provided with a customized support agreement that provides detailed customer and support contact information. For the most efficient resolution of your problem, please take a moment to gather some basic information from your records and from your system before contacting customer support, including your customer number (on the Customer Support Agreement and shipping invoice that came with your system).

Table 2: Customer Support Information

<table>
<thead>
<tr>
<th>Information</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Your customer number</td>
<td>You can find this number on your Customer Support Agreement and on the shipping invoice that came with your UnityOne system.</td>
</tr>
<tr>
<td>Your IPS serial number</td>
<td>You can find this number on the shipping invoice that came with your UnityOne system.</td>
</tr>
<tr>
<td>Your IPS software version number</td>
<td>You can find this information in the LSM in the System Stats frame, in the Update tab, or by using the CLI show version command.</td>
</tr>
<tr>
<td>Your IPS system boot time</td>
<td>You can find this information in the LSM in the System Stats frame.</td>
</tr>
</tbody>
</table>
UnityOne Overview

This chapter introduces UnityOne concepts and functionality. It provides an overview of the UnityOne Intrusion Prevention System (IPS) Model 200/400/1200/2400.

Overview

In the highly technical era of data transfers and the Internet, the protection of data and networks concern most businesses, corporations, and network administrators. TippingPoint Technologies has studied the issue of data security and network protection from malicious activity and attacks. One of the solutions is the UnityOne Intrusion Prevention System (IPS). The IPS provides constant vigilance of a network, monitoring and managing packets while blocking malicious attacks.

This chapter includes the following topics:

- “UnityOne Overview” on page 1
- “UnityOne Environment” on page 2
- “UnityOne 200/400/1200/2400 Chassis Overview” on page 5

UnityOne Overview

The UnityOne Intrusion Prevention System (IPS) provides total packet inspection from 200 Mbps to 2.4 Gbps per second depending on the selected model. In addition, the IPS integrates Intrusion Prevention, Stateful IP Filtering (traffic management filters), and network discovery security applications into a device with the uniformity and simplicity needed to achieve a high level of protection and prevention with minimal administrative action.

The IPS detects and blocks inappropriate, incorrect, or anomalous activity on the network by comparing network traffic with filters defined by the TippingPoint Technologies (TPT) Threat Management Center (TMC). Devices use filters to scan traffic and recognize header or data content in the attack along with the protocol, service, and the operating system or software the attack affects. The attack filter includes an action set, which defines the reaction when the IPS encounters packets that
match attack filter parameters. In a broad sense, the IPS either drops matching packets or permits them.

The Stateful IP filtering provides service-level, stateful inspection of network traffic. It incorporates filtering functionality to protect mission-critical applications. An administrator can specify a traffic management filter that determines how the system handles traffic to and from a particular service. These filters are specified by the source, destination, and service or protocol of the traffic.

The IPS is responsible for the host and service database used by UnityOne. The IPS scans your network and maintains an inventory of the active hosts and services on those hosts. System administrators can use information collected by the IPS to tune attack and IP filters.

**Core Functionality**

UnityOne provides the following core functionality:

- **Detection and suppression** — Unlike an intrusion detection system (IDS), the IPS identifies and stops malicious traffic on the edge of the network.
- **Filter customization** — Through IP filters, exceptions, and attack filter creation, you can customize UnityOne to meet the specific needs of your enterprise.
- **Real-time threat aggregation** — The TMC collects threat information from throughout the world, converts it to attack filters, and distributes it to UnityOne™ customers.
- **Monitoring** — Enterprise networks are in a constant state of change. Because enterprises regularly reconfigure and add new devices and services, UnityOne monitors the network for these changes using network discovery.
- **Intrinsic Network High Availability** — The data network security is protected against failures in the host and network processors. A fallback state is automatically invoked in the event of a hardware or software failure.

The following sections describe each security application in more detail.

**UnityOne Environment**

The principle component of the UnityOne Model 200/400/1200/2400 environment is the IPS. A single IPS can be installed at the perimeter of your network or on your Intranet or both. It can secure up to 4 network segments. A segment is two ports on an IPS. Members of the segment are hosts connected to those ports. The Local Security Manager (LSM) manages a single IPS. The LSM is a web-based management application that provides on-the-box administration, configuration, and reporting.

The Security Management System (SMS) provides functionality beyond that provided by the LSM. The SMS can manage multiple IPSs. Furthermore, the SMS provides coordination across your UnityOne environment for administration, configuration, and monitoring. Most importantly, the SMS includes enterprise-wide reporting and trend analysis.

From the SMS, you must set an overall security posture for each IPS. The security posture controls how the box responds to traffic that matches IP and attack filters. The IPS is always in Active mode, and reacts to traffic as specified by the appropriate filter.
The LSM and IPS maintain a connection to the Threat Management Center (TMC) which is located at TPT headquarters. The TMC monitors 10,000 sensors around the world for the latest attack information. As a result, your network can be continually inoculated.

The following figure displays a sample UnityOne environment (this example shows the Model 2000 Intrusion Prevention System):

**Figure 1: The UnityOne™ Environment**

Each component of the UnityOne environment is discussed in more detail in the following sections.

**Threat Suppression Engine**

At the core of UnityOne is a security-specific processor called the Threat Suppression Engine (TSE) that enables intrusion prevention at multi-gigabit speeds. The TSE consists of ASICs and network processors to detect known threats and potentially malicious traffic loads on your network. The TSE inspects and reacts to malicious traffic at ultra-high speeds using SMARTMatch™ filters, preventing attacks from harming your network and resources. The TSE scans packets and traffic, including TCP, UDP, ICMP, and other IP protocols.

**IPS Devices**

Intrusion Prevention System (IPS) devices protect your network by scanning, detecting, and responding to network traffic according to the filters, action sets, and global settings maintained on each device by a client. Each device provides intrusion prevention for your network according to the amount of network connections and hardware capabilities.

UnityOne IPS devices are designed to handle the extremely high demands of carriers and high-density data centers. Even while under attack, UnityOne Intrusion Prevention Systems are extremely low-latency network infrastructure ensuring switch-like network performance. UnityOne also has built-in intrinsic high-availability features, guaranteeing that the network keeps running in the event of system failure.

UnityOne IPS devices are active network defense systems using the Threat Suppression Engine (TSE) to detect and respond to attacks. UnityOne Intrusion Prevention Systems are optimized to provide high
resiliency, high availability security for remote branch offices, small-to-medium and large enterprises and collocation facilities. Each UnityOne can protect network segments from both external and internal attacks. UnityOne Intrusion Prevention Systems are extremely low-latency network infrastructure ensuring switch-like network performance, even while under attack. UnityOne also has built-in intrinsic high-availability features, guaranteeing that the network keeps running in the event of system failure.

IP devices provide the following segments and traffic performance:

- UnityOne-2000 — Up to 20 10/100/1000 segments at an aggregate 2.0 gigabits/second
- UnityOne 50 — One 10/100/1000 segment at an aggregate 50 megabits/second
- UnityOne-200 — Two 10/100 segments at an aggregate 200 gigabits/second
- UnityOne-400 — Four 10/100 segments at an aggregate 400 gigabits/second
- UnityOne-1200 — Four 10/100/1000 segments at an aggregate 1.2 gigabits/second
- UnityOne-2400 — Four 10/100/1000 segments at an aggregate 2.0 gigabits/second

Multiple UnityOne devices can be deployed to extend this unsurpassed protection to hundreds of enterprise zones. You can monitor and manage the devices through local clients or up to 1,000 devices through the SMS Client.

You can also implement an optional device called the Zero Power High Availability (ZPHA). This device provides continued traffic in the event of a power loss in your IPS devices.

**Local Security Manager**

The Local Security Manager (LSM) is responsible for local administration, configuration, and reporting for a single IPS. Through the use of a graphical user interface (GUI), the LSM provides the interfaces, tools, and processes that configure and monitor the IPS. The LSM provides a subset of the management functionality offered through the Security Management System, which is designed to manage several IPS units from a central server.

For more detailed information, see the *UnityOne Local Security Manager User’s Guide*.

**Security Management System**

The Security Management System (SMS) provides a global view and control for the UnityOne environment. It is shipped as a management server and includes an enterprise desktop—the workstation client—through which end users can perform secure, policy-based management tasks for multiple IPSs. It provides facilities similar to the LSM, but supports a larger scope. Most importantly, it provides enterprise-wide reporting.

For more detailed information, see the *UnityOne Security Management System User’s Guide*.

**Threat Management Center**

The Threat Management Center (TMC) is the central intelligence bureau for the UnityOne environment. The TMC performs comprehensive global reconnaissance for emerging threats. It rapidly builds new signatures and algorithms to suppress such threats.
The TMC offers the following end user service:

- **Digital Vaccine** — A subscription service that offers real-time continuous update capability. With Digital Vaccine, the IPSs pull new threat signatures from the TMC on a routine basis.
- **Software Updates** — Updated versions of the software you can use for your UnityOne system, including the Local Security Manager and Security Management System
- **Documentation** — Downloadable PDF files of software and hardware documentation, including release notes
- **Technical Support** — Details information for contacting and receiving technical support for user issues

## UnityOne 200/400/1200/2400 Chassis Overview

The UnityOne 200/400/1200/2400 system comprises a two rack unit (RU, $2 = 3.5$ inches) chassis that uses a front-access, four (Model 200 IPS) or eight-port architecture, supporting connection to two to four network segments. It is rack-mountable on a 19- or 23-inch rack and contains two redundant hot swappable power supplies and three chassis cooling fans. There are no removable cards in the chassis, although some software commands may refer to slot 3 when configuring certain aspects of this IPS model. This is necessary to ensure Command Line Interface (CLI) compatibility with other models of the UnityOne, specifically the UnityOne Intrusion Prevention System Model 2000, which can include up to four Multi-Zone Defense (MZD) modules.

The following figure displays the UnityOne Model 1200 front and rear panels.

**Figure 2: UnityOne Model 1200 - Front Panel**

![UnityOne Model 1200 - Front Panel](image)

**Figure 3: UnityOne Model 1200 - Rear Panel**

![UnityOne Model 1200 - Rear Panel](image)

The following sections describe the UnityOne IPS Model 200/400/1200/2400 hardware components.
Management Processing Function

The management processing function performs the central processing and control functions for the UnityOne system. This section includes the following topics:

- “LEDs” on page 6
- “Power Switch and Audible Alarm” on page 7
- “Liquid Crystal Display (LCD)” on page 8

LEDs

There are two LEDs on the front panel, one for status and one for power. There is a power switch with an LED on the front panel. There are power supply LEDs located on the power modules on the back of the chassis.

The following table details the LED descriptions.

Table 1: LED Descriptions

<table>
<thead>
<tr>
<th>LED</th>
<th>Color</th>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status LED</td>
<td>Amber</td>
<td>Bootup</td>
<td>Indicates that the system is booting up.</td>
</tr>
<tr>
<td></td>
<td>Green</td>
<td>Operational</td>
<td>Indicates that the system is powered and operating properly.</td>
</tr>
<tr>
<td>Power LED</td>
<td>Green</td>
<td>Operational</td>
<td>Indicates that power has been applied and the system is operating properly. This LED is in the center of the Power switch. Pressing this switch when operational shuts down most of the power to the unit.</td>
</tr>
</tbody>
</table>

The following table details the Link and Activity LEDs that are at the upper left and right corners of each segment connector.

Table 2: Segment Port LED Descriptions

<table>
<thead>
<tr>
<th>LED</th>
<th>Color</th>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link (left side LED)</td>
<td>No light</td>
<td>Not-Synchronized</td>
<td>Provides information about whether the port (eight in total) on the module is linked and ready for data to pass through it. No light means the port is not ready or it is malfunctioning.</td>
</tr>
<tr>
<td></td>
<td>Green</td>
<td>Connected/</td>
<td>Green means the port is connected and ready for data.</td>
</tr>
<tr>
<td>Activity (right side LED)</td>
<td>No light</td>
<td>No-Data Traffic</td>
<td>Provides information about whether data is passing through a particular port. No light means that the port is not passing data.</td>
</tr>
<tr>
<td></td>
<td>Blinking amber</td>
<td>Data Traffic</td>
<td>Amber means that port is passing data.</td>
</tr>
</tbody>
</table>
The management port has its own set of LEDs. Depending on your model as REV B (Intel 845) or C (Intel 865), the LEDs may indicate differing activity. See the following information according to REV model.

**Note:** You can determine the rev of the model at the CLI prompt. Use the command `show version` to list the REV model (B or C).

### Table 3: Management Port LED Descriptions (REV B - Intel 845)

<table>
<thead>
<tr>
<th>LED</th>
<th>Color</th>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link</td>
<td>No light</td>
<td>10Mbps</td>
<td>Provides information on the speed of data through the port. No light indicates data passes through the port at 10Mbps.</td>
</tr>
<tr>
<td>Green</td>
<td></td>
<td>100Mbps</td>
<td>Green means the port passes data through at 100Mbps.</td>
</tr>
<tr>
<td>Activity</td>
<td>No light</td>
<td>No-Data Traffic</td>
<td>Provides information about whether data is passing through a particular port. No light means that the port is not passing data.</td>
</tr>
<tr>
<td>Amber</td>
<td>Link Available</td>
<td></td>
<td>Solid amber means the port is available, but not passing data.</td>
</tr>
<tr>
<td>Blinking amber</td>
<td>Data Traffic</td>
<td></td>
<td>Blinking amber means that port is passing data.</td>
</tr>
</tbody>
</table>

### Table 4: Management Port LED Descriptions (REV C - Intel 865)

<table>
<thead>
<tr>
<th>LED</th>
<th>Color</th>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link</td>
<td>No light</td>
<td>No-Data Traffic</td>
<td>Provides information about whether data is passing through a particular port. No light means that the port is not passing data.</td>
</tr>
<tr>
<td>Green</td>
<td>Link Available</td>
<td></td>
<td>Solid green means the port is available, but not passing data.</td>
</tr>
<tr>
<td>Blinking Green</td>
<td>Data Traffic</td>
<td></td>
<td>Blinking green means that port is passing data.</td>
</tr>
<tr>
<td>Activity</td>
<td>No light</td>
<td>10Mbps</td>
<td>Provides information on the speed of data through the port. No light indicates data passes through the port at 10Mbps.</td>
</tr>
<tr>
<td>Amber</td>
<td></td>
<td>100Mbps</td>
<td>Amber means the port passes data through at 100Mbps.</td>
</tr>
</tbody>
</table>

**Power Switch and Audible Alarm**

The power switch on the front panel includes an integrated LED that is lit when power is applied. This unit contains dual redundant hot swappable, universal AC-DC power supplies.
The following table details the power supply LED descriptions.

**Table 5: Power Supply LED Descriptions**

<table>
<thead>
<tr>
<th>LED</th>
<th>Color</th>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power LED</td>
<td>Green</td>
<td>On</td>
<td>Power module is functioning properly and AC power is on</td>
</tr>
<tr>
<td></td>
<td>None</td>
<td>Off</td>
<td>Power module has a failure or AC power to the module is off</td>
</tr>
</tbody>
</table>

The following table details the power supply audible alarm descriptions.

**Table 6: Power Supply Audible Alarm Descriptions**

<table>
<thead>
<tr>
<th>Component</th>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audible Alarm</td>
<td>Off</td>
<td>Power module is functioning properly and AC power is on</td>
</tr>
<tr>
<td></td>
<td>On</td>
<td>Power module has a failure or AC power to one of the power modules is off. The audible alarm can be silenced by correcting the fault or by pressing the red Reset button on the rear of the power supply chassis.</td>
</tr>
</tbody>
</table>

**Liquid Crystal Display (LCD)**
There is a two line LCD on the front panel of the IPS that is under software control and provides operational information during network operations.
2

Prepare the Site

This chapter discusses the requirements necessary to prepare your site for the installation of the UnityOne System.

Overview

Before installing the new UnityOne, you need to gather materials and prepare the network and hardware site. To carefully and correctly install the component(s) you must read through all preparation instructions and requirements.

The chapter consists of the following sections:

- “Safety Requirements” on page 10
- “Rack and Clearance Requirements” on page 12
- “Ventilation and Location” on page 12
- “Environmental Requirements” on page 13
- “Power Requirements” on page 13
- “System Grounding Requirements” on page 13
- “Cabling Requirements” on page 14
- “Fiber-Optic Connection Guidelines” on page 14
- “Unpack the UnityOne System” on page 15
Safety Requirements

If not properly installed and maintained, electrical circuitry equipment like the UnityOne can pose dangers to both personnel and equipment. To prevent accidents, adhere to the following guidelines to ensure general safety:

• Remove any dust from the area and keep the area around the UnityOne system clear and dust-free during and after installation.
• Wear safety glasses if you are working under conditions that might be hazardous to your eyes.
• There are no serviceable parts inside.

**Note:** This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe A respecte toutes les exigences du Règlement sure le matériel brouilleur du Canada.

**Note:** This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: this device may not cause harmful interference, and this device must accept any interference received, including interference that may cause undesired operation.

See the following list of cautions and warnings for further safety guidelines.

**CAUTION:** Before you start the installation procedures, read this entire chapter for important information and safety warnings.

Use proper electromagnetic static discharge (ESD) protection whenever you handle UnityOne equipment.

Do not power up the equipment while you install and connect the system.

If you connect the power improperly and then apply power, the cards and chassis could be damaged.

The equipment rack must be anchored to an unmovable support to prevent it from falling over when one or more servers are extended in front of it on slide assemblies. The equipment rack must be installed according to the manufacturer’s instructions. You must also consider the weight of any other device installed in the rack.

You are responsible for installing an AC power disconnect for the entire rack unit. This main disconnect must be readily accessible, and it must be labeled as controlling power to the entire unit, not just to the server.

Make sure that the chassis cooling fans run continuously while the system is powered.

Use of controls or adjustments or performance of procedures other than those specified herein may result in hazardous radiation exposure.
WARNING: This warning symbol means danger. It tells you how to avoid physical injury to people or equipment. For people, injury includes anything from temporary conditions, such as pain, to irreversible conditions such as death. For equipment, injury means anything requiring repair. Warnings tell you what you should or should not do, and the consequences of not heeding the warning.

Only trained and qualified personnel should install, replace, or service this equipment. Disconnect the system before servicing.

This product requires short-circuit (overcurrent) protection, to be provided as part of the building installation. Install only in accordance with national and local wiring regulations.

Do not operate the system unless all cards and top cover is in place.

During this procedure, wear grounding wrist straps to avoid ESD damage to cards and modules.

Risk of explosion if battery is replaced by an incorrect type. Dispose of used batteries according to the instructions.

To reduce the risk of fire, use only No. 26 AWG or larger telecommunication line cord.

This equipment is to be installed and maintained by service personnel only as defined by AS/NZS 3260 Clause 1.2.14.3 Service Personnel.

This unit is intended for installation in restricted access areas only.

When connecting equipment to IT power distributions, Phase to phase voltage must not exceed 240 V.

WARNING: This product is a Class 1 laser product. Do not stare into the laser beam or view it directly with optical instruments. Install covers for the laser connectors when they are not in use.

The ports on the front of the UnityOne are Safety Extra-Low Voltage (SELV) circuits. SELV circuits should only be connected to other SELV circuits.

Do not work on the system or connect or disconnect cables during periods of lightning activity.
To prevent the unit from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature of 104° F (40° C). To prevent airflow restriction, allow at least 3 inches (7.6 cm) of clearance around the ventilation openings.

Only trained and qualified personnel should install, replace, or service this equipment. Disconnect the system before servicing.

Read all of the installation instructions before you connect the system to its power source.

Never touch uninsulated telephone wires or terminals unless the telephone line has been disconnected at the network interface.

**Rack and Clearance Requirements**

Tipping Point recommends that you mount the UnityOne system in a standard 19-or 23-inch rack. The vertical hole spacing on the rack rails must meet standard EIA-310-C requirements, which call for a one inch (2.54 cm) spacing. Ensure that you have a minimum of three inches clearance at the side of the ventilation slots.

**Ventilation and Location**

Ventilation and proper location are essential to the proper operation of the UnityOne system.

To ensure that the UnityOne receives adequate ventilation,

- When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.
- Ensure that the unit is positioned properly on the rack
- Proper and adequate ventilation is facilitated by a cool air intake on the front of the unit, with hot air exhausted through the back of the chassis.
- There should be three inches clearance at the ventilation openings.
Environmental Requirements

In order for the UnityOne to run properly, your environment must meet the proper criteria.

The following table details the recommendations for temperature, humidity, and altitude settings for the Service Provider (SP) environment.

Table 1: Environmental Requirements for the UnityOne

<table>
<thead>
<tr>
<th>Environmental Specifications</th>
<th>Description</th>
</tr>
</thead>
</table>
| Temperature                 | 0 to 40 °C (32 to 104 °F) — Operating
                                          -20 to 80° C (-4 to 176 °F) — Storage |
| Humidity                    | 5 to 95% (non-condensing)                         |
| Altitude                    | No degradation up to 13K feet above sea level     |

Power Requirements

The UnityOne requires two inputs of Alternating Current (AC): 100-240 VAC @ 6-3A, 60/50Hz.

System Grounding Requirements

Damage from Electromagnetic Static Discharge (ESD) can occur when electronic components are improperly handled. Its results can be complete or intermittent system failures. Therefore, proper ESD protection is required whenever you handle equipment. It is not necessary to open the Unity One Model 200/400/1200/2400 chassis to add or remove any components. The following general grounding guidelines apply in the event that a redundant power supply module must be replaced.

Follow these guidelines to prevent ESD damage of the UnityOne system and its components:

- Always use an ESD wrist strap when adding or removing components from the chassis.
- Avoid touching the circuit boards or connectors on all cards and modules.
- Avoid contact between the printed circuit boards and clothing. The wrist strap only protects components from ESD voltages on the body. ESD voltages on clothing can still cause damage.
- Place a removed component board-side-up on an antistatic surface or in a static-shielding container that is also grounded to the same point as the IPS. If you plan to return the component to the factory, immediately place it in a static-shielding container.
Grounding

Before handling the UnityOne cards or modules, you must first ground yourself to the chassis. This action helps to prevent ESD damage, which can have devastating effects on the components.

Note: To complete this procedure, you must use an ESD grounding strap.

To ground yourself

STEP 1 Attach one end of the ESD grounding strap to your wrist. Ensure that it makes good contact with your skin.

STEP 2 Locate the grounding jack situated at the rear of the unit near the power supplies.

STEP 3 Plug the other end of the ESD grounding strap into the grounding jack.

Cabling Requirements

The UnityOne ships with the following cables:

- Two AC power cables for the power supplies
- Fiber optic cables for SFP connections
- Null modem cable (DB-9 FM - DB-9 FM) for (COM) port

Note: The UnityOne IPS can use Lucent Connector (LC) fiber-optic cables in single-mode or multi-mode. The module also supports Category 5 Ethernet cables for the 10/100/1000 Ethernet connections.

Fiber-Optic Connection Guidelines

The UnityOne IPS can use fiber-optic connectors. The connector type is a Small Form-Factor Pluggable (SFP) fiber optic connector that is LC-Duplex compatible. The UnityOne also supports the following fiber-optic media:

- Multi-Mode Short Reach Fiber (MMSRF)
- Single-Mode Intermediate Reach Fiber (SMIRF)
- Single-Mode Long Reach Fiber (SMLRF)

WARNING: Fiber-optic connections and connectors are Class 1 laser products. Do not look into the connectors and always cover the connectors when not in use. Do not remove the SFP transceivers from the port even if the port is not being used.
Unpack the UnityOne System

Each system chassis is securely packaged in a shipping box.

**CAUTION:** ESD can damage the UnityOne if you do not take necessary precautions. Installation and maintenance personnel should be properly grounded using ground straps to eliminate the risk of ESD damage to the equipment. All cards and modules are subject to ESD damage whenever they are removed from the chassis.

Use caution when opening the UnityOne boxes.

To unpack the UnityOne system, complete the following steps:

**STEP 1** Inspect the packing container. If you see any damage or other signs of mishandling, inform both the local freight provider and TippingPoint before unpacking. Your freight provider can provide you with the procedures necessary to file a claim for damages.

**STEP 2** Carefully open the box.

**STEP 3** Remove all packing material.

**STEP 4** Verify the contents in the shipping package. Compare the packing list to your shipment and to your order. Are all items included? If items are missing, contact your TippingPoint sales or field representative.

**STEP 5** Remove the chassis from the box.

**STEP 6** Open the accessory kit. It contains the cables, documentation, and management software.

**STEP 7** Inspect all the equipment inside for damage. If you think any equipment might be damaged, contact your freight provider for how to lodge a damage claim. Also, contact your TippingPoint sales or field representative for instructions.
Hardware Installation and Configuration

This chapter discusses how to install and configure the UnityOne Intrusion Prevention System and its components.

Overview

After you have completed preparation procedures and unpacked the UnityOne IPS, you can install and configure the components. The UnityOne IPS ships with the following pre-installed components:

- One custom processor card with four (Model 200) or eight Ethernet ports
- A host processor card to control, configure, monitor, and store network traffic
- Two redundant hot swappable AC-DC power supplies
- A minimum 30 GB disk drive
- An integrated fan assembly (three fans)
- A 32 character LCD Display

Prior to installation, you should also obtain the Unity One Command Line Interface Reference. After installation of the components, you will need to run through the UnityOne Setup Wizard as part of the installation and configuration procedures. See Chapter 4, “Setup Wizard” for more information.

This chapter includes the following sections:

- “Install the UnityOne Chassis” on page 18
- “Attach Network Connections” on page 21
- “Check LEDs” on page 22
- “UnityOne Setup Wizard” on page 23
TNHA Hardware Configuration

During the unpacking and installation of the UnityOne IPS device, you should consider the following for Transparent Network High Availability (TNHA) configuration. Before configuring the TNHA settings, you must consider and perform specific hardware and software configurations for the devices and the network. These configuration settings include the following:

- The network and devices must have a secure connection to a partner for the TNHA to function.
- TNHA uses SSLv3. It also communicates on TCP port 9591.
- TNHA devices can only connect and communicate with a partner configured to talk to likewise configured machines. In other words, both machines participating must point to each other.

**WARNING: Security caveat:** A hi-jacked IPS or a rogue IPS that “steals” the IP address of a TRHA partner can communicate with a legitimate IPS.

Install the UnityOne Chassis

To install the UnityOne you must do the following:

- Determine Total Rack Space
- Bolt the UnityOne to the Rack
- Connect the Dual Power Supply

Determine Total Rack Space

Before you install the chassis, you should determine the total rack space that is required to install your system. The required rack space will increase if you plan to install multiple systems.

The UnityOne system fits in either a 19-inch or a 23-inch wide rack. See the following table for individual rack space requirements.

**Table 1: Rack Space Requirements**

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Configuration Type</th>
<th>Min/Max Number of Chassis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Size of Rack</td>
<td>Typical</td>
<td>21 chassis maximum on a seven foot rack</td>
</tr>
<tr>
<td>(Total number of chassis must be &lt; or = 42 RU) Each UnityOne IPS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>requires 2RU.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Equipment Building Systems (NEBS)</td>
<td>Typical</td>
<td>7 chassis generating &lt; or = 196 Watts</td>
</tr>
<tr>
<td>(Total number of chassis must generate: &lt; or = 1372 Watts)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Bolt the UnityOne to the Rack

Use the following guidelines when bolting the UnityOne to the rack:

**WARNING: To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable.**

- If the rack comes with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack.
- If the rack is partially filled, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.
- If you plan to expand your system to include additional UnityOne systems in the future, allow space in the rack for additions. During the initial installation, keep in mind the weight distribution and stability of the rack.

Connect the Dual Power Supply

After you have bolted the UnityOne to the rack, you need to attach the dual power supply AC connections. This section details various options for connections. To gain the protection for these options, follow the diagrams for the connections to your dual power supply.

**Note:** You should apply AC power to both power supplies to insure uninterrupted service to the UnityOne and to avoid audible alarms.

You can also receive a Right Angle IEC Receptacle power cord for the device. You can use this cable for connecting power to the device in cases where you may not have enough room for a straight power connection cable. This cable helps in situations when you need to install a device in a tight rack with a door. The 90 degree bend in the female end of the cable prevents the cord from being pinched between the device and the door.

**Note:** Cable cord retention latch will not work with right angle power connectors.

The following figure displays connections to provide protection against power supply failure.

**Figure 1: Protection for Power Supply Failure**
The following figure displays connections to provide protection against power supply failure and power failure on the one power feed circuit.

**Figure 2: Protection for Power Supply Failure and One Power Feed Circuit**

![Diagram](image1)

The following figure displays connections to provide protection against power supply failure and power failure on both power feed circuits.

**Figure 3: Protection for Power Supply Failure and Both Power Feed Circuits**

![Diagram](image2)

The following figure displays connections to provide maximum protection against power supply failure and power failure on both power feed circuits.

**Figure 4: Maximum Protection for Power Supply Failure and Both Power Feed Circuits**

![Diagram](image3)
Attach Network Connections

The IPS can act as a simple Layer 2 switch or can aggregate and redirect up to 2.0 Gigabits per second (Gbps) of traffic. The IPS Model 200/400/1200/2400 contains four copper RJ-45 ports (Model 200) or eight ports, either fiber-optical, copper RJ-45 or a combination of both.

**WARNING:** Optical ports on this module are classified as Class 1 Lasers. Protection plugs should be installed when ports are not in use. The SFP transceivers should not be removed from the optical ports, even if the ports are not being used.

To connect to optical ports

**STEP 1** Locate the optical port. It is a duplex port.

**STEP 2** Plug the LC-duplex fiber-optic cable connector into the SFP transceiver (comes pre-installed)

**STEP 3** Plug the other end of the fiber-optic cable into your network.

**STEP 4** Repeat the above-listed steps for all other optical ports.

**STEP 5** Cover any unused SFP ports with protective covers.

To connect to copper (RJ-45) ports

**STEP 1** Locate the RJ-45 port on the module.

**STEP 2** Plug one end of the Category 5 cable into the RJ-45 port.

**STEP 3** Plug the other end of the cable into your network port.

**STEP 4** Repeat the above-listed steps for each copper port on the MZD module.

To connect to a COM port

**STEP 1** Locate the COM port.

**STEP 2** Connect one end of the null modem cable to the IPS COM port.

**STEP 3** Connect the other end of the modem cable to the COM port on your PC or terminal.

**STEP 4** Perform the set-up procedure using the LSM or the SMS (refer to the appropriate user guide).
Check LEDs

When you connect power to the system, the system completes a series of component checks. It then displays LEDs to show the status of each component. See the following sections for information about LEDs for individual components.

The following table provides a detailed description of the LEDs.

Table 2: LED Descriptions for the IPS

<table>
<thead>
<tr>
<th>LED</th>
<th>Color</th>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Amber</td>
<td>Boot up</td>
<td>Indicates that the IPS is in the process of booting up. Or if it stays amber the IPS may be faulty and should be returned to the manufacturer.</td>
</tr>
<tr>
<td></td>
<td>Solid green</td>
<td>Power On</td>
<td>Indicates that the IPS has power and is functioning properly.</td>
</tr>
<tr>
<td></td>
<td>No light</td>
<td>Power Off</td>
<td>Indicates that the power is not on.</td>
</tr>
<tr>
<td>Power (in button)</td>
<td>No light</td>
<td>Power Off</td>
<td>Indicates that the power is not on.</td>
</tr>
<tr>
<td></td>
<td>Solid green</td>
<td>Power On</td>
<td>Indicates that power has been applied to the chassis.</td>
</tr>
<tr>
<td>Activity</td>
<td>No light</td>
<td>No data traffic</td>
<td>Provides information about whether data is passing through a particular port. Off means that the port is not passing data.</td>
</tr>
<tr>
<td></td>
<td>Blinking Amber</td>
<td>Data traffic</td>
<td>Amber means that port is passing data.</td>
</tr>
<tr>
<td>Link</td>
<td>No light</td>
<td>Not synchronized</td>
<td>Provides information about whether the port (eight in total) on the module is linked and ready for data to pass through it. Off means the port is not ready or it is malfunctioning.</td>
</tr>
<tr>
<td></td>
<td>Green</td>
<td>Connected/ Synchronized</td>
<td>Green means the port is connected and ready for data.</td>
</tr>
</tbody>
</table>
UnityOne Setup Wizard

Once you have powered on, the UnityOne Setup wizard displays on your COM port terminal. The wizard prompts you to perform basic configuration tasks and periodically input information. You can run the wizard through one of the following processes:

• Out-of-the-Box Terminal Setup Wizard — Runs when the setup wizard is activated for the first time or later with the setup command. This wizard is run on a serial port connected system, such as a workstation and laptop.

• Out-of-the-Box LCD Setup Wizard — Runs directly on the LCD panel, overriding any serial port connected system. You can access the device through a serial connected workstation or laptop after the setup completes.

• Additional Configuration — After you run the setup wizard using serial terminal or IPS LCD, you can further configure your system using subsequent setup commands through the Command Line Interface (CLI).

See Chapter 4, “Setup Wizard” for detailed instructions.
4 Setup Wizard

This chapter discusses how to configure the UnityOne Intrusion Prevention System and its components. The chapter includes step-by-step instructions for using the Setup Wizard through the Command Line Interface and the LCD Setup Wizard through the device LCD.

Overview

After you have unpacked and installed the UnityOne IPS, you can configure the components using the Setup Wizard. You can use one of two configuration methods for your IPS device:

- **Out-of-the-Box Terminal Setup Wizard** — Runs when the setup wizard is activated for the first time or later with the `setup` command. This wizard is run on a serial port connected system, such as a workstation and laptop. For more information on CLI commands, see the *Unity One Command Line Interface Reference*.

- **Out-of-the-Box LCD Setup Wizard** — Runs directly on the LCD panel, overriding any serial port connected system. You can access the device through a serial connected workstation or laptop after the setup completes.

**Note:** You can only run the Out-of-the-Box LCD Setup Wizard on an IPS device. IPS devices do not have a LCD panel for entering values.

- **Additional Configuration** — After you run the setup wizard using serial terminal or IPS LCD, you can further configure your system using subsequent setup commands through the CLI. See “Additional Configuration” on page 48 for details.

**Note:** If you need to return to the setup wizard after running the initial setup, see the *Unity One Command Line Interface Reference*. The commands and process for updating settings using the CLI are listed in “Chapter 1, UnityOne Startup Configuration.”
This chapter includes the following sections:

- “Out-of-the-Box Terminal Setup Wizard” on page 26
- “Out-of-the-Box LCD Setup Wizard” on page 37
- “Additional Configuration” on page 48

**TNHA Software Configuration**

During the unpacking and installation of the UnityOne IPS device, you should consider the following for Transparent Network High Availability (TNHA) configuration. Before configuring the TNHA settings, you must consider and perform specific hardware and software configurations for the devices and the network. These configuration settings include the following:

- The network and devices must have a secure connection to a partner for the TNHA to function.
- TNHA uses SSLv3. It also communicates on TCP port 9591.
- TNHA devices can only connect and communicate with a partner configured to talk to likewise configured machines. In other words, both machines participating must point to each other.

**WARNING: Security caveat: A hi-jacked IPS or a rogue IPS that “steals” the IP address of a TRHA partner can communicate with a legitimate IPS.**

**Out-of-the-Box Terminal Setup Wizard**

The Out-of-the-Box Setup Wizard runs on a workstation or laptop connected to the serial port of the IPS device. Through a set of prompts, you can enter and configure the IPS. These settings include the following:

- Account security access and super-user setup
- IP addresses, ports, and options for the host management port
- Settings for the default gateway
- Options for the timekeeping settings, such as daylight saving and SNTP servers
- Server options for web, CLI, and SNMP
- Settings for the NMS and SMS
- Various settings not covered directly in the wizard such as ethernet addresses, management port routes, default e-mail contacts, and remote syslog settings

**Note:** For detailed information on commands, see the *Unity One Command Line Interface Reference*. The guide also includes these Out-of-the-Box Setup Wizard instructions.

After you have configured the IPS, you can run the setup again using the `setup` command in the Command Line Interface. See the *Unity One Command Line Interface Reference* for more information and command descriptions.
The Out-of-the-Box Setup Wizard runs on a workstation or laptop connected to the serial port of the device. The configuration dialogs run are shown in the following table:

**Table 1: Out-of-the-Box Setup Wizard Configuration Settings**

<table>
<thead>
<tr>
<th>Out-of-the-Box Setup</th>
<th>Subsequent Setups</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Security Level</td>
<td>—</td>
<td>account security level</td>
</tr>
<tr>
<td>Super-user Data</td>
<td>—</td>
<td>super-user login name</td>
</tr>
<tr>
<td></td>
<td></td>
<td>super-user password</td>
</tr>
<tr>
<td>Host Management Port Options</td>
<td>Host Management Port Options</td>
<td>IP address&lt;br&gt;network mask&lt;br&gt;host name&lt;br&gt;location</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>Default Gateway</td>
<td>gateway address</td>
</tr>
<tr>
<td>Timekeeping Options</td>
<td>Timekeeping Options</td>
<td>SNTP or CMOS clock&lt;br&gt;timezone&lt;br&gt;daylight saving time&lt;br&gt;DST&lt;br&gt;SNTP:&lt;br&gt;primary SNTP server&lt;br&gt;secondary SNTP server&lt;br&gt;CMOS clock:&lt;br&gt;date&lt;br&gt;time</td>
</tr>
<tr>
<td>Web, CLI, and SNMP Server Options</td>
<td>Web, CLI, and SNMP Server Options</td>
<td>HTTPS or HTTP&lt;br&gt;SSH and/or telnet&lt;br&gt;SNMP</td>
</tr>
<tr>
<td>NMS Configuration</td>
<td>NMS Configuration</td>
<td>NMS IP address and port&lt;br&gt;NMS community string</td>
</tr>
<tr>
<td>Restricted SMS Access</td>
<td>Restricted SMS Access</td>
<td>SMS IP address</td>
</tr>
<tr>
<td>—</td>
<td>Ethernet Ports</td>
<td>enable ports&lt;br&gt;line speed&lt;br&gt;duplex setting&lt;br&gt;auto negotiation</td>
</tr>
<tr>
<td>—</td>
<td>Management Port Routes</td>
<td>destination network&lt;br&gt;gateway&lt;br&gt;mask</td>
</tr>
<tr>
<td>—</td>
<td>Default E-Mail Contact</td>
<td>TO: email&lt;br&gt;FROM: email&lt;br&gt;email domain&lt;br&gt;SMTP server IP&lt;br&gt;email aggregation period</td>
</tr>
</tbody>
</table>
This section includes the following sections:

- “Account Security Level” on page 28
- “Super-User Data” on page 29
- “Host Management Port Options” on page 31
- “Default Gateway Options” on page 32
- “Timekeeping Options” on page 33
- “Web, CLI, and SNMP Server Options” on page 34
- “NMS Settings” on page 36
- “Restricted SMS Access” on page 36
- “Additional Configuration” on page 48

When the terminal setup wizard runs, the following screen displays:

```
Welcome to the TippingPoint Technologies Initial Setup wizard.
Press any key to begin Initial Setup Wizard or use LCD panel.
```

Press any key to begin the Out-of-the-Box (or Initial) Setup Wizard. When you press any key, you see the following:

```
You will be presented with some questions along with default values in brackets[]. Please update any empty fields or modify them to match your requirements. You may press the ENTER key to keep the current default value. After each group of entries, you will have a chance to confirm your settings, so don't worry if you make a mistake.
```

Continue to the following section for instructions on account security.

**Account Security Level**

The Security Level dialog enables you to set the security level settings for account access. It includes the following settings:

## Table 1: Out-of-the-Box Setup Wizard Configuration Settings

<table>
<thead>
<tr>
<th>Out-of-the-Box Setup</th>
<th>Subsequent Setups</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>---</td>
<td>Remote Syslog Server</td>
<td>IP address</td>
</tr>
</tbody>
</table>
**Account Security Level**

The security level and restrictions for entering user names and passwords. The default setting is 2 from the following options:

**Example**

There are three security levels for specifying user names and passwords:

- **Level 0**: User names and passwords are unrestricted.
- **Level 1**: Names must be at least 6 characters long without spaces. Passwords must be at least 8.
- **Level 2**: Includes Level 1 restrictions and requires the following: 2 alphabetic characters, 1 numeric character, 1 non-alphanumeric character (special characters such as ! ? and *).

Please specify a security level to be used for initial super-user name and password creation. As super-user, you can modify the security level later on via Command Line Interface (CLI) or Local Security Manager (LSM).

Security level [2]:

**Super-User Data**

The Super-User Data dialog includes the following settings:

**Super-User Name**

A login name for the super-user account. See [Valid Login Names](#) below.

**Super-User Password**

A login password for the super-user account. See [Valid Passwords](#) below.
Valid Login Names
A valid login name must meet the restrictions of the set security level. The levels require the following:

- Level 0 — Any length and format is allowed for the user name and password. You must not include spaces.
- Level 1 and 2 — It must contain at least six (6) characters and no spaces.

Table 3: Login Name Examples

<table>
<thead>
<tr>
<th>Valid Login Names</th>
<th>Invalid Login Names</th>
</tr>
</thead>
<tbody>
<tr>
<td>fjjohnson</td>
<td>fredj (too short)</td>
</tr>
<tr>
<td>fredj123</td>
<td>fred j 123 (contains spaces)</td>
</tr>
<tr>
<td>fredj-123</td>
<td>fj123 (too short)</td>
</tr>
<tr>
<td>fredj-*123</td>
<td>fj 123 (contains spaces)</td>
</tr>
</tbody>
</table>

Valid Passwords
A valid password must meet the restrictions of the set security level. The levels require the following:

- Level 0 — No restrictions. Any length and format is allowed for the user name and password.
- Level 1 — It must contain at least eight (8) characters.
- Level 2 — It must contain at least eight (8) characters with the following restrictions:
  - it must contain at least two alphabetic characters
  - it must contain at least one numeric character
  - it must contain at least one non-alphanumeric character—a non-alphanumeric character includes any character that is not a digit or a letter. You can use spaces.

Table 4: Password Examples for Level 2 Security

<table>
<thead>
<tr>
<th>Valid Passwords</th>
<th>Invalid Passwords</th>
</tr>
</thead>
<tbody>
<tr>
<td>my-pa55word</td>
<td>my-pa55 (too short)</td>
</tr>
<tr>
<td>my-b1rthday</td>
<td>mybirthday (must contain numeric)</td>
</tr>
<tr>
<td>myd*g'snam3</td>
<td>mydogsnam3 (must contain a non-alphanumeric character)</td>
</tr>
</tbody>
</table>
**Example**
The Super-user Data dialog follows:

Please enter a user name that we will use to create your super-user account. Spaces are not allowed.

Name: superuser
Do you wish to accept [superuser] <Y,[N]>: y

Please enter your super-user account password:
Verify password:
Saving information...Done

Your super-user account has been created.

You may continue initial configuration by logging into your device. After logging in, you will be asked for additional information.

The login prompt should appear in approximately 90 seconds.

**Host Management Port Options**
The Host Management port is the Ethernet port located on the host processor module. You use the Host Management or the serial port to connect to your UnityOne device when you use the Command Line Interface and when you use the LSM.

**Host IP Address**
The Host IP address is the IP address through which you access your UnityOne device. The Host IP address must meet the following criteria:

- must be standard IP v 4 address format (“111.111.111.111”).
- daylight saving must be contained within your local network, but must not be contained within any of the subnets that will be passing traffic through the Multi-Zone Defense Module.
- must be accessible from the workstation from which you will perform IPS management activities.

**CAUTION:** When configuring the Host Management Port, you must assign it an IP address outside of any of the subnets that will be connected through the Multi-Zone Defense Module interface card. If you assign the management port an IP address that is within any of the subnets connected through the Multi-Zone Defense Module interface card, your interfaces will not perform reliably.

**Network Mask**
The network mask for the subnet on which the IPS is located.

**Host Name**
The host name of the IPS. Use the same name that the IPS will be known as on your network.

**Host Location**
The host location is the physical location of the IPS. It is for informational purposes only.
Example
The Host Management Port options dialog follows:

The host management port is used to configure and monitor this device via a network connection (e.g., a web browser).

Enter Management IP Address []:111.222.33.44
Enter Network Mask [255.255.255.0]:
Enter Host Name [myhostname]:nds-corpnet-1
Enter Host Location [room/rack]: rack 3 - middle

    Host IP: 216.136.56.239
    Network Mask: 255.255.255.0

    Host Name: nds-corpnet-1
    Host Location: rack 3 - middle

Enter [A]ccept, [C]hange, or [E]xit without saving [C]: A

Default Gateway Options
The Default Gateway options enable you to set up the routing information the IPS needs to communicate with other networks.

Note: If the IPS Host Management Port and the workstation from which you will manage the IPS are on different subnets, you must define a default gateway or an additional route to enable network-based management of your IPS.

Default Gateway
The default gateway is the IP address through which communications with other subnets are routed. If the IPS sends a message to an IP address outside of its subnet, the message and the reply will go through the default gateway.

Example
The Default Gateway Options dialog follows:

The default gateway is a router that enables this device to communicate with other devices on the management network outside of the local subnet.

Do you require a default gateway? <Y,[N]>: y

Enter Gateway Address:
(0.0.0.0 removes the default) [0.0.0.0]: 111.222.33.200

    Gateway Address: 111.222.33.200
Enter [A]ccept, [C]hange, or [E]xit without saving [C]: a

Tip: Using additional routes instead of a default gateway helps assure that your Management Port will only communicate with explicitly authorized network segments.
Timekeeping Options

The IPS can keep time using its internal CMOS clock or it can use an Internet Simple Network Time Protocol (SNTP) server. If you decide to use SNTP for timekeeping, the UnityOne IPS comes with two SNTP servers defined as the default primary and secondary SNTP servers:

- National Institute of Standards and Technology (192.43.244.18)
- US Naval Observatory (192.5.41.40)

**Note:** If you use the CLI show sntp command, the IPS displays the current settings for Primary Addr and Secondary Addr. If SNTP timekeeping is turned off (conf t no sntp), the last SNTP servers defined (or default if never defined) will be shown. (conf t and cft are useful abbreviations for configure terminal.)

**CAUTION:** Using external SNTP servers could possibly make your IPS susceptible to a man-in-the-middle attack. It is more secure to use an SNTP server on a local, protected network.

Time Zone

The time zone option enables you to calculate and show the local time. System logs are kept in Universal Time (UTC), but the IPS calculates local time for display purposes. Entering the proper time zone enables the IPS to display local time properly.

Primary Time Server

The SNTP server that your IPS will use to keep time. A valid entry will meet the following criteria:

- a valid IP address for an SNTP primary time server

Daylight saving Time

The daylight saving time option enables you to turn off and on an option for calculating time based on the time of year.

Secondary Time Server

The SNTP server that your IPS will use to keep time should the primary server be unavailable. A valid entry will meet the following criteria:

- a valid IP address for an SNTP secondary time server
Example
The Timekeeping Options dialog follows:

Timekeeping options allow you to set the time zone, enable or disable daylight saving time, and configure or disable SNTP.

Would you like to modify timekeeping options? <Y,[N]>: y

Enter time zone or '?' for complete list [GMT]: CST
Automatically adjust clock for daylight saving changes? [Yes]: n
Do you want to enable the SNTP client? [No]: y
Enter Primary SNTP Server address [192.43.244.18]:
Enter Secondary SNTP Server address [192.5.41.40]:

TimeZone: CST
DST enabled: No
SNTP enabled: Yes
SNTP Primary Server: 192.43.244.18
SNTP Secondary Server: 192.5.41.40
Enter [A]ccept, [C]hange, or [E]xit without saving [C]:

Web, CLI, and SNMP Server Options
The Web, CLI, and SNMP Server Options dialog enables you to turn your IPS servers on and off. You should always use the secure Web and CLI servers (HTTPS and SSH) when conducting normal operations. You should only use the non-secure (HTTP and telnet) servers for troubleshooting if you cannot get the secure alternatives running for some reason.

Note: You do not need to run any servers at all if you wish to control your IPS only through the serial port, but you will not be able to manage filters, if you choose to do this. You can turn off all servers by using the following commands:

• conf t server no http
• conf t server no https
• conf t server no ssh
• conf t server no telnet

You must reboot your IPS for changes to HTTP or HTTPS to take effect

Secure and Non-Secure Operation
You can enable the secure and non-secure servers for the CLI (SSH and telnet). You cannot enable both the secure and non-secure servers for the Web. This is to prevent inadvertent security lapses within your network security infrastructure. In practical terms, this means that if you enable the HTTPS server the HTTP server is disabled.

SMS Operation
The HTTPS server is required for SMS management. The implication of this is that if you will be using the SMS to manage your IPS devices, you cannot run the non-secure HTTP server.
Default Server Settings
The default settings of the Web, CLI, and SNMP servers are:

**Table 5: Default Web, CLI, and SNMP Server Options**

<table>
<thead>
<tr>
<th>Name</th>
<th>Default Setting</th>
<th>Required By</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH</td>
<td>ON</td>
<td>secure CLI over network</td>
</tr>
<tr>
<td>Telnet</td>
<td>OFF</td>
<td>non-secure CLI over network</td>
</tr>
<tr>
<td>HTTPS</td>
<td>ON</td>
<td>SMS, secure LSM</td>
</tr>
<tr>
<td>HTTP</td>
<td>OFF</td>
<td>non-secure LSM</td>
</tr>
<tr>
<td>SNMP</td>
<td>ON</td>
<td>SMS, NMS</td>
</tr>
</tbody>
</table>

**SSH Server**
The SSH Server enables encrypted terminal communications. The SSH server must be enabled to establish a secure CLI session over your network.

**Telnet Server**
The telnet server enables telnet connections to the IPS. The telnet server can be enabled to run non-secure CLI sessions over your network.

> **CAUTION:** The Setup Wizard enables you to activate the telnet server. Telnet is not a secure service. If you enable telnet, you endanger the security of your UnityOne device. Use SSH instead of telnet when you are conducting normal operations.

**HTTPS Server**
The HTTPS server is a web server. It enables you to perform encrypted file transfers over your network. The HTTPS server must be enabled to use SMS management. You can also run the LSM using the HTTPS server.

**HTTP Server**
The HTTP server is a web server. You may disable the HTTP server and use the HTTPS server to run the LSM. You can enable the HTTP server to run non-secure LSM session on your network.

> **CAUTION:** The Setup Wizard enables you to activate HTTP. HTTP is not a secure service. If you enable HTTP, you endanger the security of your UnityOne device. Use HTTPS instead of HTTP for normal operations.

> **Note:** When you modify HTTPS from its current setting, you must reboot to enact the changes. After rebooting, the IPS will run the new setting for the HTTP or HTTPS server. You can use the CLI `reboot` command.
SNMP Server

The SNMP Server provides access to interface counters and other statistics, configuration data, and general system information via the Simple Network Management Protocol (SNMP). The SNMP server must be enabled to use SMS management or to allow NMS access.

Example

The Server Options dialog follows:

```
Server options allow you to enable or disable each of the following servers: SSH, Telnet, HTTPS, HTTP, and SNMP.
Would you like to modify the server options? <Y, [N]>: y

Enable the SSH server? [Yes]: y
Enable the Telnet server? [No]: n
Enable the HTTPS server ('No' disables SMS access)? [Yes]: y
Enable the HTTP server? [No]: n
Enable the SNMP agent ('No' disables SMS and NMS access)? [Yes]: y

SSH: Yes
Telnet: No
HTTPS: Yes
HTTP: No
SNMP: Yes
```

Enter [A]ccept, [C]hange, or [E]xit without saving [C]: e

NMS Settings

The NMS Options dialog enables you to configure the Network Management System (NMS) settings available for the device. This feature enables monitoring of the device by a restricted NMS, such as HP OpenView™.

Example

The NMS Options dialog follows:

```
A Network Management System (NMS) such as HP OpenView (TM) can be used to monitor and receive traps from your TippingPoint device.

Would you like to configure a Network Management System? <Y, [N]>: y
```

Restricted SMS Access

The Restricted SMS Access dialog enables you to restrict access for the device regarding the Security Management System (SMS). This option restricts the access to your device to accept management only from a specific SMS at the specified IP address.
Example
The Restricted SMS Access dialog follows:

You have the option to restrict access to your device by TippingPoint Security Management Systems (SMSs) such that only an SMS at a specified IP address can manage the device.

Would you like to restrict SMS access? <Y,[N]>: y

Complete Setup
After completing the Out-of-the-Box Terminal Setup Wizard, continue to “Additional Configuration” on page 48 for instructions on additional configuration options for the UnityOne system.

Out-of-the-Box LCD Setup Wizard
The LCD Setup Wizard enables you to configure your IPS device if you do not have a workstation or laptop connected to the serial port. TippingPoint Technologies recommends using the Out-of-the-Box Terminal Setup Wizard to configure your device.

The LCD Setup Wizard allows you to configure a portion of the setting for the device. This configuration wizard enables you to enter enough information to connect via SSH or LSM to complete all available customer settings.

Note: The LCD saves the entered values after the LCD Setup Wizard steps complete. At any time during the setup, you can cancel the setup through the LCD by pressing the Cancel Button repeatedly, returning to the first option.

If canceled, the LCD displays the following at the first step:

Setup in process via serial port

At this point, you can return to a serial terminal to continue the Out-of-the-Box Setup Wizard. See “Out-of-the-Box Terminal Setup Wizard” on page 26 for instructions.
The configuration dialogs run are listed in the following table:

**Table 6: LCD Setup Wizard Configuration Settings**

<table>
<thead>
<tr>
<th>LCD Setup</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Begin Setup</td>
<td>—</td>
</tr>
<tr>
<td>Super-user Data</td>
<td>super-user login name</td>
</tr>
<tr>
<td></td>
<td>super-user password</td>
</tr>
<tr>
<td>Host Management Port Options</td>
<td>IP address</td>
</tr>
<tr>
<td></td>
<td>network mask</td>
</tr>
<tr>
<td></td>
<td>host name</td>
</tr>
<tr>
<td>Default Gateway Options</td>
<td>gateway address</td>
</tr>
<tr>
<td>Timekeeping Options</td>
<td>timezone</td>
</tr>
<tr>
<td></td>
<td>daylight saving time</td>
</tr>
</tbody>
</table>

This section includes the following sections:

- “Using the LCD Panel” on page 38
- “Begin Setup” on page 40
- “Super-User Account” on page 41
- “Host Management Port” on page 43
- “Default Gateway Options” on page 45
- “Timekeeping Options” on page 46
- “Complete Setup” on page 47
- “Additional Configuration” on page 48

**Using the LCD Panel**

When you run the Setup Wizard through the LCD of the device, you use the buttons on the front panel of IPS device. The device includes an LCD panel and set of buttons for entering and selecting values. The IPS devices all have similar panels.
The following image displays the general layout of the IPS panel.

**Figure 1: Device Front Panel**

![Device Front Panel Image]

The following table details the buttons available on the front panel.

**Table 7: LCD Panel Buttons**

<table>
<thead>
<tr>
<th>Button</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Select Button" /></td>
<td><strong>Select Button</strong> Use to choose a Yes or accept option. This button accepts a configuration you enter and continues to the next step of the setup wizard. You must press this button before you enter configuration settings during the LCD Setup Wizard or when using the LCD menu options.</td>
</tr>
<tr>
<td><img src="image" alt="Cancel Button" /></td>
<td><strong>Cancel Button</strong> Use to cancel an option or step backwards through the setup wizard. Each time you use the cancel button, the setup backs up to the previous step. You can use this button to return to the first entry menu, allowing you to choose the Out-of-the-Box Setup Wizard used through a serial connected workstation or laptop.</td>
</tr>
<tr>
<td><img src="image" alt="Option Selection Buttons" /></td>
<td><strong>Option Selection Buttons</strong> Use to select an option or configure settings. These buttons provide the ability to select, Yes, No, and numbers. For entering numbers, you use the up button to increase and down button to decrease.</td>
</tr>
<tr>
<td><img src="image" alt="Movement Buttons" /></td>
<td><strong>Movement Buttons</strong> Use to move forward and back through a line of configuration settings. You use these buttons to enter and edit IP and device name settings.</td>
</tr>
</tbody>
</table>

**Note:** For instructions on using the IPS menu options, see Appendix D, “IPS Menu Options.”
**Begin Setup**

A welcome message and instructions display when the Setup Wizard starts up on a serial port connected workstation or laptop. This message displays the first time it runs. The message includes information regarding the Setup Wizard. To run setup on the device through the LCD, do not press any key.

**Note:** You can only run the LCD Setup Wizard on an IPS device. IPS devices do not have a LCD panel for entering values.

```
/boot/ - Volume is OK
/opt/ - Volume is OK
/usr/ - Volume is OK
/log/ - Volume is OK
```
Welcome to the TippingPoint Technologies Initial Setup wizard.

Press any key to begin Initial Setup Wizard or use LCD panel.

To begin the setup and configuration, go to the device. At the device, the LCD displays the following message:

Setup via LCD?

To begin the setup, press the Select Button. A series of messages display, indicating that the device is doing the following:

Press "check" To
Accept & Proceed

Press "x" to
Cancel & Backup

Generate
Name & Password

CopyTheFollowing
Name & Password

On a workstation or laptop connected to the serial port, the following message displays:

Initial Setup is currently in progress via the LCD panel.
No input here is possible till LCD operation is complete or canceled.

Super-User Account

After generating the super-user account, the Setup Wizard displays the super-user account name and password. You can regenerate these by pressing the Cancel Button. This section includes the following:

• “To Configure the Super-User Name” on page 42
• “To Configure the Super-User Password” on page 43

CAUTION: You must copy down the displayed super-user user name and password to access and manage the device. The account information displays according to the instructions in this section on the LCD panel.

Super-User Name

A login name for the super-user account. By default, the user name follows security access settings for level 2 account security access.

Super-User Password

A login password for the super-user account. By default, the password follows security access settings for level 2 account security access.
**Account Security Level**
The security level and restrictions for entering user names and passwords. The default setting is 2, which includes the following settings:

- User names must be at least 6 characters long without spaces.
- Passwords must be at least 8 characters long and include the following:
  - 2 alphabetic characters
  - 1 numeric character
  - 1 non-alphanumeric character (special characters such as ! ? and *)

**To Configure the Super-User Name**
The LCD displays the following message about the super-user name:

```
SuperUser Name
22q2st
```

**STEP 1** Copy down the super-user account name exactly as displayed. The user name is case sensitive.

**STEP 2** To accept, press the **Select Button**.

**STEP 3** To cancel and regenerate the name, press the **Cancel Button** once. The wizard will return to the following prompt, generating a new user name and password:

```
Generating User Name & Password
```
To Configure the Super-User Password

The LCD displays the following message about the super-user password:

```
SuperUser Passwd
07/IjuWD
```

**STEP 1** Copy down the super-user account password exactly as displayed. The password is case sensitive.

**STEP 2** To accept, press the Select Button.

**STEP 3** To cancel and regenerate the password, press the Cancel Button twice. The wizard will step back two levels in the setup to the prompt, generating a new user name and password:

```
Generating User
Name & Password
```

Host Management Port

The Host Management port is the Ethernet port located on the host processor module. You will use the Host Management or the serial port to connect to your UnityOne device when you use the Command Line Interface and when you use the LSM. Through the LCD, you can configure the host name, management IP address, and network mask.

This section including the following configuration steps:

- “To Configure the Host Name” on page 44
- “To Configure the Management IP” on page 44
- “To Configure the Network Mask” on page 45

Host Name

The host name of the IPS. Use the same name that the IPS will be known as on your network.

Host IP Address

The Host IP address is the IP address through which you access your UnityOne device. The Host IP address must meet the following criteria:

- must be standard IP v 4 address format (“111.111.111.111”).
- IP address must be contained within your local network, but must not be contained within any of the subnets that will be passing traffic through the Multi-Zone Defense Module.
- must be accessible from the workstation from which you will perform IPS management activities.

**CAUTION:** When configuring the Host Management Port, you must assign it an IP address outside of any of the subnets that will be connected through the Multi-Zone Defense Module interface card. If you assign the management port an IP address that is within any of the subnets connected through the Multi-Zone Defense Module interface card, your interfaces will not perform reliably.
**Network Mask**
The network mask for the subnet on which the IPS is located.

**To Configure the Host Name**
The LCD displays the following message about the host name:

```
Host Name
ips00
```

**STEP 1** The Setup Wizard generates the last two characters of the host name. You can modify only these two numbers.

**STEP 2** To move forward and back through the number places, press the Movement Buttons.

**STEP 3** To increase or decrease the number of the selected place, press the Option Selection Buttons.

**STEP 4** To accept the change and save, press the Select Button. To regenerate the number, press the Cancel Button three times. The wizard will return to the following prompt, generating a new user name, password, and IPS device name:

```
Generating User Name & Password
```

**To Configure the Management IP**
The LCD displays the following message about the Management IP address:

```
Management IP?
127.000.000.001
```

**STEP 1** The Setup Wizard defaults the management IP address as 127.000.000.001. You can enter the IP address using the panel buttons.

**Note:** The Setup Wizard removes leading zeros in the IP address. If one set of numbers should be a 10, enter 010. And for a 1, enter 001.

**STEP 2** To move forward and back through the number places, press the Movement Buttons.

**STEP 3** To increase or decrease the number of the selected place, press the Option Selection Buttons.

**STEP 4** To accept the change and save, press the Select Button. To cancel and move back a level, press the Cancel Button.
To Configure the Network Mask
The LCD displays the following message about the Network Mask:

Netmask?
255.255.255.000

**STEP 1**  The Setup Wizard defaults the network mask to 255.255.255.000. You can enter a different IP using the panel buttons.

*Note:* The Setup Wizard removes leading zeros in the IP address. If one set of numbers should be a 10, enter 010. And for a 1, enter 001.

**STEP 2**  To move forward and back through the number places, press the **Movement Buttons**.

**STEP 3**  To increase or decrease the number of the selected place, press the **Option Selection Buttons**.

**STEP 4**  To accept the change and save, press the **Select Button**. To cancel and move back a level, press the **Cancel Button**.

Default Gateway Options
The Gateway and Routing options enable you to set up the routing information the IPS needs to communicate with other networks.

*Note:* If the IPS Host Management Port and the workstation from which you will manage the IPS are on different subnets, you must define a default gateway or an additional route to enable network-based management of your IPS.

Default Gateway
The default gateway is the IP address through which communications with other subnets are routed. If the IPS sends a message to an IP address outside of its subnet, the message and the reply will go through the default gateway.

To Configure the Gateway
The LCD displays the following message:

Gateway Needed?
yes

**STEP 1**  The Gateway option defaults as yes. To change the option between yes and no, press the **Option Selection Buttons**.

**STEP 2**  To accept the change and save, press the **Select Button**. To cancel and move back a level, press the **Cancel Button**.

**STEP 3**  If you select yes and press the **Select Button**, the LCD prompts with the following:

Gateway IP?
000.000.000.000

Note: The Setup Wizard removes leading zeros in the IP address. If one set of numbers should be a 10, enter 010. And for a 1, enter 001.
STEP 4  You can enter a different IP using the panel buttons.

Note: The Setup Wizard removes leading zeros in the IP address. If one set of numbers should be a 10, enter 010. And for a 1, enter 001.

STEP 5  To move forward and back through the number places, press the Movement Buttons.

STEP 6  To increase or decrease the number of the selected place, press the Option Selection Buttons.

STEP 7  To accept the change and save, press the Select Button. To cancel and move back a level, press the Cancel Button.

**Timekeeping Options**

The IPS can keep time using its internal CMOS clock or it can use an Internet Simple Network Time Protocol (SNTP) server. If you decide to use SNTP for timekeeping, the UnityOne IPS comes with two SNTP servers defined as the default primary and secondary SNTP servers:

- National Institute of Standards and Technology (192.43.244.18)
- US Naval Observatory (192.5.41.40)

**Note:** If you use the CLI `show sntp` command, the IPS displays the current settings for Primary Addr and Secondary Addr. If SNTP timekeeping is turned off (`conf t no sntp`), the last SNTP servers defined (or default if never defined) will be shown. (`conf t` and `cft` are useful abbreviations for configure terminal.)

**CAUTION:** Using external SNTP servers could possibly make your IPS susceptible to a man-in-the-middle attack. It is more secure to use an SNTP server on a local, protected network.

**Time Zone**

The time zone option enables you to calculate and show the local time. System logs are kept in Universal Standard Time (UST) (also known as Greenwich Mean Time and Universal Time), but the IPS calculates local time for display purposes. Entering the proper time zone enables the IPS to display local time properly.

**Daylight Saving Time**

The daylight saving time option enables you to turn off and on an option for calculating time based on the time of year.
To Configure the Time Zone
The LCD displays the following message:

Time Zone?
GMT

**STEP 1** The Time Zone option defaults as Universal Standard Time (UST) (also known as Greenwich Mean Time and Universal Time). To change the option between the available time zones, press the **Option Selection Buttons**. Pressing the up button selects time zones with a later time zone than GMT. Pressing the down button selects time zones with an earlier time zone than GMT.

**STEP 2** To accept the change and save, press the **Select Button**. To cancel and move back a level, press the **Cancel Button**.

To Configure the Daylight Saving Time
The LCD displays the following message:

Daylight Saving?
yes

**STEP 1** The Time Zone option defaults as **yes**. To change the option between yes and no, press the **Option Selection Buttons**.

**Note:** Selecting **yes** sets the IPS to automatically adjust for daylight saving time.

**STEP 2** To accept the change and save, press the **Select Button**. To cancel and move back a level, press the **Cancel Button**.

Complete Setup
The final setup prompt displays:

Finished Setup--
Accept Values?

After entering all of the configuration settings, you can save and end the LCD Setup Wizard. If you need to change settings, you can press the **Cancel Button** to back up through the levels to make changes. Once you press the **Select Button**, the settings are saved.
Any workstation or laptop connected to the serial port displays the following message:

Initial Setup via the LCD panel is finished.

The LCD displays the following:

Loading
Run Level 1

The LCD message will change, running through all of the levels. After all setup steps complete, the device then displays the operating system and Digital Vaccine versions on the LCD. On the screen of a connected workstation or laptop, the loading completes and provides a login prompt.

Note: To run portions of the setup again or to configure further settings, refer to the Unity One Command Line Interface Reference. Using the setup command in the CLI, you can modify and configure settings such as timekeeping, SMS, NMS, servers, contacts, and Intrinsic Network HA.

After completing the Out-of-the-Box LCD Setup Wizard, continue to “Additional Configuration” on page 48 for instructions on additional configuration options for the UnityOne system.

Additional Configuration

After you have run the initial setup wizard through the Command Line Interface or on an IPS LCD, you can further configure your IPS. These subsequent setup options include the following:

- “Ethernet Port Settings” on page 48
- “Management Port Routing Options” on page 50
- “Default Email Contact Information” on page 51
- “Remote Syslog Server” on page 52

Ethernet Port Settings

The Ethernet port configuration dialog does not run in the Out-of-the-Box Setup Wizard. You can only access the Ethernet Port Setup by using the setup command in the CLI.

Tip: You can configure Ethernet ports individually using the `conf t interface` ethernet command.

CAUTION: When you configure an Ethernet port using the command line interface, the port will be shut down. Use the `conf t int ethernet <slot> <port> no shutdown` command to restart the port.
**Segments**
A segment is a contiguous port pair on your Multi-Zone Defense Module. A defense module has up to 5 segments, depending on the model of the IPS. Segments are referred to by a combination of the slot number in which their module is installed and the number of their port pair. For example, if a Multi-Zone Defense (MZD) Module is installed in Slot 7, from left to right, the segments for that module would be called: 7:1, 7:2, 7:3, 7:4, and 7:5. In the Intrusion Prevention System configurations, where the MZD equivalent defaults to a slot 3 designation, the segments are 3:1, 3:2, 3:3, and 3:4.

**Ethernet Port Options**
The Ethernet Port Options dialog enables you to set individual port values for the IPS Ethernet interface.

**Line Speed**
The line speed setting for port. A valid entry will meet the following criterion:

- either 10, 100, or 1000

**Duplex Setting**
The duplex setting for the port. A valid entry must be one of the following:

- copper - full or half
- fiber optic - full

**Auto Negotiation**
The auto negotiation setting determines whether the port will negotiate its speed based on the connection it can make. A valid entry must be one of the following:

- on
- off

**Example**
An excerpt of the Ethernet Port Options dialog follows (note that the reference to a Multi-Zone Defense Module is on a UnityOne Intrusion Prevention System, or Model 2000):

Would you like to modify the Ethernet ports <Y,[N]>:y
We will now configure your Ethernet ports.

Configure slot 3 (Multi-Zone Defense Module)? <Y,[N]>:y
Configure port 1 (Ethernet Port)? <Y,[N]>:y
This port is currently enabled, would you like to disable it?
<Y,[N]>:n
Please enter values for the following options
   Line speed [1000]:
   Duplex setting [Full]:
   Auto negotiation [On]:

The settings entered for slot 6, port 1 are as follows:
   Line speed: 1000
   Duplex setting: Full
   Auto negotiation: On
Enter [A]ccept, [C]hange, or [E]xit without saving [C]: a

Configure Port 2 (Ethernet Port)? <Y,[N]>:

CAUTION: When you configure a Ethernet port using the command line interface, the port will be shut down. Use the `conf t int ethernet <slot> <port> no shutdown` command to restart the port.

Management Port Routing Options

The Management Port Routing options dialog does not run in the Out-of-the-Box Setup Wizard. You can only access the Management Port Routing options by using the `setup` command in the CLI.

These options enable you to configure your UnityOne device to be managed from a different network than the one to which the management port is connected. You can define up to 12 routes that your Management Port can use to communicate with other subnets.

CAUTION: Define additional routes with care. The broader a definition of additional routes you use, the greater the chance that an unauthorized user can reach your IPS.

Destination Network

The destination network is the IP network address of the subnet with which you want the IPS to communicate.

Gateway

The gateway is the IP address on the IPS subnet that can communicate with the destination network.

Mask

The mask is the IP mask that you wish to apply to traffic taking this route.

Example

The Management Port Routing options dialog follows:

Would you like to modify management port routes <Y,[N]>: y

Currently, the additional routes are as follows:

<table>
<thead>
<tr>
<th>#</th>
<th>Destination</th>
<th>Gateway</th>
<th>Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>111.222.0.0</td>
<td>111.222.33.200</td>
<td>255.255.0.0</td>
</tr>
<tr>
<td>2</td>
<td>&lt;empty&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>&lt;empty&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>&lt;empty&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>&lt;empty&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>&lt;empty&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>&lt;empty&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>&lt;empty&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>&lt;empty&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>&lt;empty&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>&lt;empty&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>&lt;empty&gt;</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Enter [A]ccept, [C]hange, or [E]xit without saving [C]:c
Enter the number of the entry you want to change []:1
Destination network []:
   Mask []:
   Gateway []:
The new route is added to the list and displayed, offering further options, including [R]emove.

**Default Email Contact Information**

The Default Alert options dialog does not run in the Out-of-the-Box Setup Wizard. You can only access the Management Port Routing options by using the `setup` command in the CLI.

These options enable you to establish the default sender and recipient for filter alert e-mails.

**TO email address**
The TO email address is the email address to which alert notifications will be sent. A valid entry must meet the following criteria:

- must be less than 129 characters long
- must be a valid email address. For example: johndoe@mycompany.com

**FROM email address**
The FROM email address is the address that alert notifications will contain in the from field. A valid entry will meet the following criteria:

- must be less than 129 characters long
- must be a valid email account name on the SMTP server
- must be a valid email address on the SMTP server

**Domain**
The Domain Name is the domain name of the SMTP server. A valid entry will meet the following criteria:

- must be a valid domain name with a DNS entry on the network the UnityOne device is located on
- must be the domain name where the SMTP server is located

**Email Server IP address**
The email Server IP address should be the address where the SMTP server is located. A valid entry will meet the following criterion:

- must be a valid IP address for an SMTP server

**Period**
The Period is the aggregation period for email alerts. The first time a filter that calls for email notification is triggered, the system sends an email notification to the target named in the filter. At the same time, the aggregation timer starts. The UnityOne device counts additional filter triggers, but does not email another notification until it sends a count of all filter triggers that occurred during that
period. The timer continues to count and send notifications at the end of each period. A valid entry will meet the following criterion:

- an integer between 1 and 10,080 representing minutes between notifications

**Example**

The Default Email Contacts Dialog follows:

Would you like to modify the default Email contact? <Y,[N]>: y
Enter TO: email address (128 max. characters)
Must be a full email address (e.g., sender@company.com) []: employee@company.com
Enter FROM: email address (128 max. characters)
Must be a full email address (e.g., recipient@company.com []): tpt3@company.com
Enter FROM: Domain Name (128 max. characters, e.g., company.com) []: company.com

Enter email server IP address []: 1.2.3.4
Enter period (in minutes) that email should be sent (1 - 10080) [1]: 5

To: employee@company.com
From: tpt3@company.com
Domain: company.com
Email Server: 1.2.3.4
Period (minutes): 5

Enter [A]ccept, [C]hange, or [E]xit without saving [C]: a

**Remote Syslog Server**

The Remote Syslog Server dialog does not run in the Out-of-the-Box Setup Wizard. You can only access the Management Port Routing options by using the `setup` command in the CLI.

A remote syslog server is another channel that you can use to report filter triggers. Remote syslog sends filter alerts to a syslog server on your network.

**CAUTION:** Only use remote syslog on a secure, trusted network. Remote syslog, in adherence to RFC 3164, sends clear text log messages using the UDP protocol. It does not offer any additional security protections. Therefore, you should not use remote syslog unless you can be sure that syslog messages will not be intercepted, altered, or spoofed by a third party.

**Tip:** For more information about syslog, consult the syslog server documentation that came with your operating system or syslog software.
This appendix provides hardware and software specifications for the UnityOne IPS. This appendix contains the following sections:

- Hardware specifications
- Software specifications

## Hardware Specifications

This section details the specifications for the hardware components:

The following table provides technical specifications for the UnityOne Intrusion Prevention System.

<table>
<thead>
<tr>
<th>Specification</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dimensions</td>
<td>2RU’s— 3.5 in. x 17.25 in. x 15.0 in. (8.9 cm x 43.8 cm x 30.5 cm) Rack mountable in a 19” and 23” front or center mount racks.</td>
</tr>
<tr>
<td>Weight</td>
<td>27 lb (12.3 kg)</td>
</tr>
<tr>
<td>Management Interface</td>
<td>One 10/100 Ethernet interface.</td>
</tr>
<tr>
<td>Serial Interface</td>
<td>DB-9 interface - COM1, 115200 baud, parity: none</td>
</tr>
</tbody>
</table>
Table 1: UnityOne IPS Specifications

<table>
<thead>
<tr>
<th>Specification</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Interfaces</td>
<td>4 (Model 200) or 8 Gigabit Ethernet (GigE) copper or optical interfaces, supporting up to 2.0 Gbps of traffic.</td>
</tr>
</tbody>
</table>
| Power Requirements                  | 100 to 240 VAC, 6-3 amperes @ 50-60 Hz  
Maximum Power Consumption: 300 Watts                                                                 |
| Service Provider operating requirements | Temperature  
0 to 40 ° C (32 to104 ° F) — Operating  
-20 to 70° C (-4 to 158 ° F) — Storage  
Altitude  
No degradation up to 13K feet  
Humidity  
5% to 95% (non-condensing)                                                                 |

Technical Specifications

The following table provides technical specifications on the Model 200/400/1200/2400 hardware.

Table 2: Model 200/400/1200/2400 Hardware Specifications

<table>
<thead>
<tr>
<th>Specification</th>
<th>Detail</th>
<th>Description</th>
</tr>
</thead>
</table>
| Internal hardware                   | Processor | Pentium 4 card at 2.8 GHz with 256MB of DRAM. Hard drive capacity of minimum30 GB  
1st level cache: 32 KB on CPU full-speed cache  
2nd level cache: 256 KB on CPU full-speed cache  
BIOS: 2 Mb of VxWorks Flash | PCI, 32 bits at 33 MHz                                                                 |
| Power consumption                   |        | Max 300W                                                                                                                                 |
| External interfaces                 |        | Two: one 10/100 Ethernet, one DB-9 serial.                                                                                               |
| Bus interface                       |        | PCI bus, PCI Industry Consortium Manufacturing Group (PICMG)-compliant                                                                 |
| Software requirements and network management requirement |        | TPT Security Management Software (SMS) Version 1.3 and above.                                                                            |
To run the UnityOne Intrusion Prevention System (IPS), you need one of the following software applications/devices.

### Table 2: Model 200/400/1200/2400 Hardware Specifications

<table>
<thead>
<tr>
<th>Specification</th>
<th>Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum data rates (per port)</td>
<td>1.25 Gigabit per second</td>
</tr>
<tr>
<td>External interfaces</td>
<td>4-8 ports (depending on model, standard copper or fiber or a combination of each)</td>
</tr>
<tr>
<td>Laser Modules (SFP) - not available on all IPS models</td>
<td>850 nanometers, Multi Mode: 500m</td>
</tr>
</tbody>
</table>

### Software Specifications

To run the UnityOne Intrusion Prevention System (IPS), you need one of the following software applications/devices.

### Table 3: Software Specifications for the UnityOne IPS

<table>
<thead>
<tr>
<th>Specification</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UnityOne Security Management System (SMS) Software, Version 1.2 and above. (optional)</td>
<td>SMS can optionally be used to manage multiple UnityOne Intrusion Prevention Systems.</td>
</tr>
<tr>
<td>1 Windows-based PC running Windows 9x, NT or 2000</td>
<td>Must be attached to your network (PC needs a serial port available)</td>
</tr>
</tbody>
</table>
Connector and Pinout Specifications

This appendix provides connector and pinout information for the UnityOne system. This appendix contains the following sections:

- Management Processor Connectors
- Port Connectors

Management Processor Connectors

See the following sections for information on Management Processor connectors.

DB-9 (COM) Connector

The following figure displays a -DB-9 connector.

Figure 1: DB-9 Connector

![DB-9 Connector Diagram](image-url)
**DB-9 Connector Pinout**
The following table details the pinout information for the DB-9 connector.

**Table 1: DB-9 Connector Pinouts**

<table>
<thead>
<tr>
<th>Pin Number</th>
<th>Signal Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Data Carrier Detect (DCD)</td>
</tr>
<tr>
<td>2</td>
<td>Receive Data (RxD)</td>
</tr>
<tr>
<td>3</td>
<td>Transmit Data (TxD)</td>
</tr>
<tr>
<td>4</td>
<td>Data Terminal Ready (DTR)</td>
</tr>
<tr>
<td>5</td>
<td>Ground (GND)</td>
</tr>
<tr>
<td>6</td>
<td>Data Set Ready (DSR)</td>
</tr>
<tr>
<td>7</td>
<td>Request to Send (RTS)</td>
</tr>
<tr>
<td>8</td>
<td>Clear to Send (CTS)</td>
</tr>
<tr>
<td>9</td>
<td>Ring Indicator (RI)</td>
</tr>
</tbody>
</table>

**RJ-45 Connector**
The following figure displays the RJ-45 connector.

**Figure 2: RJ-45 Connector**

The following table details the pinout information for the RJ-45 connector.

**Table 2: RJ-45 Connector Pinouts**

<table>
<thead>
<tr>
<th>Pin Number</th>
<th>Signal Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Transmit positive (Tx+)</td>
</tr>
<tr>
<td>2</td>
<td>Transmit negative (Tx-)</td>
</tr>
<tr>
<td>3</td>
<td>Receive positive (Rx+)</td>
</tr>
<tr>
<td>4</td>
<td>Ground (GND)</td>
</tr>
<tr>
<td>5</td>
<td>Ground (GND)</td>
</tr>
<tr>
<td>6</td>
<td>Receive negative (Rx-)</td>
</tr>
<tr>
<td>7</td>
<td>Ground (GND)</td>
</tr>
<tr>
<td>8</td>
<td>Ground (GND)</td>
</tr>
</tbody>
</table>
Port Connectors

The UnityOne IPS supports two types of port connectors, one of which, the RJ-45, has pinouts shown below. The other type, the fiber-optic connector, has no pinouts and is not shown here.

The following figure displays an RJ-45 connector.

**Figure 3: RJ-45 Connector**

The following table details the pinout information for the RJ-45 connector.

<table>
<thead>
<tr>
<th>Pin Number</th>
<th>Signal Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Twisted Pair 1 positive (TP1+)</td>
</tr>
<tr>
<td>2</td>
<td>Twisted Pair 1 negative (TP1-)</td>
</tr>
<tr>
<td>3</td>
<td>Twisted Pair 2 positive (TP2+)</td>
</tr>
<tr>
<td>4</td>
<td>Twisted Pair 3 positive (TP3+)</td>
</tr>
<tr>
<td>5</td>
<td>Twisted Pair 3 negative (TP3-)</td>
</tr>
<tr>
<td>6</td>
<td>Twisted Pair 2 negative (TP2-)</td>
</tr>
<tr>
<td>7</td>
<td>Twisted Pair 4 positive (TP4+)</td>
</tr>
<tr>
<td>8</td>
<td>Twisted Pair 4 negative (TP4-)</td>
</tr>
</tbody>
</table>

Small Form-Factor Pluggable Transceivers

The IPS can also have Small Form-Factor Pluggable (SFP) transceivers; see Figure 4 for an illustration of an SFP transceiver. If your IPS includes fiber optic ports, ensure that the SFP transceivers are installed, even if the ports are not currently being used.

The following figure displays the SFP transceiver.

**Figure 4: SFP Transceiver**
The following table details the SFP transceiver information.

**Table 4: SFP Transceiver Information**

<table>
<thead>
<tr>
<th>Fiber Input</th>
<th>Signal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Left side</td>
<td>Transmit</td>
</tr>
<tr>
<td>Right side</td>
<td>Receive</td>
</tr>
</tbody>
</table>
Power Supply Module Replacement

This appendix provides information for replacing a power supply module. It includes the following section:

- “Replacement Procedures” on page 61

Replacement Procedures

The power supply system contains two hot swappable AC-DC power supply modules. When the power supply is faulty or needs replacing, an alarm will sound. To replace a faulty power supply module, see the following instructions.

**WARNING:** Power supply module removal and replacement should be performed by quality personnel. The procedure could result in electrical shock hazards if performed incorrectly.

To replace the power supply

**STEP 1** When a fault occurs with a power module, an audible alarm sounds. This alarm can be silenced by pressing the red Reset button located at the rear of the chassis next to the inside mounted power module.

**STEP 2** Locate the faulty power module by checking the LEDs on the power modules. The faulty module's LED will be off.

**STEP 3** Move the retention bracket to access the power cord and module:
STEP A  Loosen the screw of the retention bracket that is used to hold the power cord and faulty power module in place.

STEP B  Rotate the bracket 90 degrees.

STEP C  Tighten the retention bracket screw to hold the bracket out of the way.

STEP 4  Unplug the AC power cord to remove power from the faulty module.

**WARNING:** Failure to remove the power cord from the power supply prior to removal could result in an electrical shock hazard.

STEP 5  To remove the faulty power module, press down the latching lever located at the top of the faulty module and pull the module from the chassis.

**WARNING:** The power supply module may be hot when removed. You should take precautions in handling the module to prevent contact with hot surfaces. The cover of the power modules is used as a heat sink and can reach temperatures of 50 degrees Celsius under a full load.

STEP 6  To install the power supply module replacement (PWRSP-0000000007), position the replacement in the open slot. Push the module in until the latching lever locks in place.

STEP 7  Plug in the AC power cord and check to see that the power module status LED is green.

STEP 8  Replace the retention bracket:

  STEP A  Loosen the retention clip screw.
  
  STEP B  Rotate the bracket into a locked position.
  
  STEP C  Retighten the retention clip screw.
IPS Menu Options

This appendix provides information on the IPS menu options and LCD messages. On the front panel of the IPS device, you can access a set of options to review the status of the IPS and perform some functions. The LCD also displays messages regarding the state and alerts of the device.

The appendix includes the following sections:

- “IPS LCD Panel” on page 64
- “Backlight Set” on page 65
- “Contrast Set” on page 66
- “Halt OS” on page 66
- “Layer 2 Fallback/Recover System” on page 67
- “Serial # Query” on page 68
- “Reload OS” on page 68
- “Reset Log Alert” on page 68
- “IPS Messages” on page 69
IPS LCD Panel

The IPS device provides a LCD display and set of buttons on the front panel for use during the LCD Setup Wizard and to use options directly on the IPS. The buttons allow you to enter and select values that display on the LCD. The IPS devices all have similar panels. The following image displays the general layout of the IPS panel.

Figure 1: Device Front Panel

The following table details the buttons available on the front panel.

Table 1: LCD Panel Buttons

<table>
<thead>
<tr>
<th>Button</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Select Button" /></td>
<td>Select Button Use to choose a Yes or accept option. This button accepts a configuration you enter and continues to the next step of the setup wizard. You must press this button before you enter configuration settings during the LCD Setup Wizard or when using the LCD menu options.</td>
</tr>
<tr>
<td><img src="image" alt="Cancel Button" /></td>
<td>Cancel Button Use to cancel an option or step backwards through the setup wizard. Each time you use the cancel button, the setup backs up to the previous step. You can use this button to return to the first entry menu, allowing you to choose the Out-of-the-Box Setup Wizard used through a serial connected workstation or laptop.</td>
</tr>
<tr>
<td><img src="image" alt="Option Selection Buttons" /></td>
<td>Option Selection Buttons Use to select an option or configure settings. These buttons provide the ability to select, Yes, No, and numbers. For entering numbers, you use the up button to increase and down button to decrease.</td>
</tr>
<tr>
<td><img src="image" alt="Movement Buttons" /></td>
<td>Movement Buttons Use to move forward and back through a line of configuration settings. You use these buttons to enter and edit IP and device name settings.</td>
</tr>
</tbody>
</table>
To enable the LCD menu, press the Select Button. The device displays the following:

Menu--
up/down to view

To move through the available menu choices, press the Option Selection Buttons. The LCD message describes them as the up/down buttons.

**Timeout**
While using the panel buttons, you must make selections within a certain amount of time or the panel will timeout. The IPS LCD will timeout after 15 seconds of inactivity and return to the default display. To return to the options menu, press the Select Button and Option Selection Buttons.

**LCD Menu Overview**
The LCD menu of the IPS provides the following options:

- **Backlight Set** — Increases or decreases the brightness of the LCD panel
- **Contrast Set** — Increases or decreases the contrast of the LCD panel
- **Halt OS** — Halts the entire IPS and deactivates the panel buttons. You use this option prior to unplugging the device.
- **HA Query State** — Displays the High Availability (HA) state of the IPS
- **Layer 2 Fallback/Recover System** — Places the IP in Layer 2 Fallback. Once in Fallback mode, the option is replaced with the Recover option. When selected, the Recover option places the IPS back in normal mode.
- **Serial # Query** — Displays the IPS device's serial number
- **Reload OS** — Reboots the IPS
- **Reset Log Alert** — Resets the syslog alert for the device and LSM

These options allow you to perform some system review and configurations outside of the Local Security Manager, Security Management System, and Command Line applications.

**Backlight Set**
When you set the backlight, the device increases or decreases the light of the LCD display.

**STEP 1** On the LCD panel, press the Select Button. The buttons activate.

**STEP 2** Press the Option Selection Buttons buttons to move to the Backlight Set option.

**STEP 3** Select the option by pressing the Select Button. The LCD displays the following:

Backlight 44
        |||||||

**STEP 4** Press the Option Selection Buttons buttons to increase or decrease the contrast.
When you press up, the vertical bars are replaced with >. When you press down, the vertical bars are replaced with <. The following example increases the setting.

```
Backlight 50
<<<<<<<
```

**STEP 5** Press **Select Button** to enter the change. The LCD prompts for verification:

```
Backlight 50
Are You Sure?
```

**STEP 6** Press **Select Button** to verify the change. Press **Cancel Button** to cancel the change.

LCD returns to the default display.

---

**Contrast Set**

When you set the contrast, the device increases or decreases the contrast of the LCD display.

**STEP 1** On the LCD panel, press the **Select Button**. The buttons activate.

**STEP 2** Press the **Option Selection Buttons** buttons to move to the **Contrast Set** option.

**STEP 3** Select the option by pressing the **Select Button**. The LCD displays the following:

```
Contrast 15
<<<<<
```

**STEP 4** Press the **Option Selection Buttons** buttons to increase or decrease the contrast.

When you press up, the vertical bars are replaced with >. When you press down, the vertical bars are replaced with <. The following example increases the setting.

```
Contrast 16
<<<<<<<
```

**STEP 5** Press **Select Button** to enter the change. The LCD prompts for verification:

```
Contrast 16
Are You Sure?
```

**STEP 6** Press **Select Button** to verify the change. Press **Cancel Button** to cancel the change.

LCD returns to the default display.

---

**Halt OS**

When you halt the system, the device performs an orderly shutdown to prepare for having the power turned off or removal of the IPS. You use this option when you need to replace a power supply or unplug the device. By halting the system, you end network traffic from the device and deactivate the panel buttons.
**STEP 1**  On the LCD panel, press the Select Button. The buttons activate.

**STEP 2**  Press the Option Selection Buttons buttons to move to the Halt OS? option.

**STEP 3**  Select the option by pressing the Select Button. The LCD prompts for verification:

Are you sure?

**STEP 4**  If you want to halt the system, select yes using the Option Selection Buttons and press the Select Button. Press Cancel Button to cancel. The system performs an orderly shutdown and is halted.

To restart the system, you must power the system down and turn it back on.

**HA Query State**

When you query for the HA state, the device displays the current High Availability state of the device.

**STEP 1**  On the LCD panel, press the Select Button. The buttons activate.

**STEP 2**  Press the Option Selection Buttons buttons to move to the HA Query State option.

**STEP 3**  Select the option by pressing the Select Button. The LCD displays one of the following:

- The LCD displays Normal if the device is not in Layer 2 Fallback.
- The LCD displays the cause for the mode change, such as watchdog.

**Layer 2 Fallback/Recover System**

When you fallback a system, you manually place the device in Layer 2 Fallback, also known as Intrinsic Network HA. If the device is in Fallback mode, the menu displays a Recover option. The Recover option manually takes the device out of Layer 2 Fallback, returning it to a normal mode.

**To place the device in Fallback mode**

**STEP 1**  On the LCD panel, press the Select Button. The buttons activate.

**STEP 2**  Press the Option Selection Buttons buttons to move to the Layer2 Fallback? option.

**STEP 3**  Select the option by pressing the Select Button. The LCD prompts for verification:

Are you sure?

**STEP 4**  If you want to place the device in Layer 2 Feedback, select yes using the Option Selection Buttons and press the Select Button. The system is placed in Layer 2 Fallback mode.

**To place the device in Recover mode**

**STEP 1**  On the LCD panel, press the Select Button. The buttons activate.

**STEP 2**  Press the Option Selection Buttons buttons to move to the Recover? option.
STEP 3 Select the option by pressing the Select Button. The LCD prompts for verification:

Are you sure?

STEP 4 If you want to return the system to a normal mode, select yes using the Option Selection Buttons and press the Select Button. The system is removed from Layer 2 Fallback to a normal mode.

### Serial # Query

When you query for the serial number, the device displays the serial number for the IPS device.

**STEP 1** On the LCD panel, press the Select Button. The buttons activate.

**STEP 2** Press the Option Selection Buttons buttons to move to the Serial # Query option.

**STEP 3** Select the option by pressing the Select Button. The LCD displays the serial number for the device.

### Reload OS

When you reload a system, you reboot the device. The device performs an orderly shutdown and reloads the operating system. You should perform this function when you want to recover from a system error or when a setup option requires a reboot of the device.

**STEP 1** On the LCD panel, press the Select Button. The buttons activate.

**STEP 2** Press the Option Selection Buttons buttons to move to the Reload OS? option.

**STEP 3** Select the option by pressing the Select Button. The LCD prompts for verification:

Are you sure?

**STEP 4** If you want to halt the system, select yes using the Option Selection Buttons and press the Select Button. The system performs an orderly shutdown and reboots, which reloads the operating system.

### Reset Log Alert

When you reset the log alert, the device resets the syslog alert and the syslog alert icon in the LSM.

**STEP 1** On the LCD panel, press the Select Button. The buttons activate.

**STEP 2** Press the Option Selection Buttons buttons to move to the Reset Log Alert? option.

**STEP 3** Select the option by pressing the Select Button. The LCD prompts for verification:

Are you sure?

**STEP 4** Press Select Button. LCD returns to the default display.
IPS Messages

IPS Messages

When the IPS device panel is not activated or in-use, it cycles through a set of system information. The information only displays if it has a value other than zero (0).

Table 2: IPS Messages

<table>
<thead>
<tr>
<th>Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permit/Block Stats</td>
<td>Displays the stats: (p)ermit or (b)lock</td>
</tr>
<tr>
<td>Sys log CRIT &amp; ERR alert</td>
<td>Displays alert of a reset from the LSM as usual or from the LCD menu options listed in this table</td>
</tr>
<tr>
<td>Thermal Alert</td>
<td>Displays if the CPU’s Thermal Control Circuit has stepped down the CPU’s speed</td>
</tr>
<tr>
<td>Memory Usage Alert</td>
<td>Displays the state: yellow or red</td>
</tr>
<tr>
<td>Disk Space Usage Alert</td>
<td>Displays the state: yellow or red</td>
</tr>
<tr>
<td>Intrinsic HA Alert</td>
<td>IPS device in is Layer 2 Fallback mode</td>
</tr>
<tr>
<td>Disk Alert</td>
<td>Displays the state of the hard disk: yellow or red</td>
</tr>
</tbody>
</table>

**WARNING:** If the IPS displays the "Thermal Alert","CPU TCC set" alert, the device’s CPU has reached an unsafe operating temperature. To reset the state, you must reboot the IPS. In the event that this message displays, you should contact the TAC.
Index

A
account security levels 28, 42
level 0 29
level 1 29
level 2 29
action set 1
additional config 23, 48
default email contact 51
ethernet port 48
mgmt port routing 50
remote syslog server 52
auto negotiation 49

B
backlight set 65
buttons
cancel (x) 39, 64
movement (left & right) 39, 64
option selection (up & down) 39, 64
select (check) 39, 64

C
cabling requirements 14
Lucent Connector 14
modem cable 14
chassis
install 18
bolt to rack 19
dual power supply 19
rack space 18
overview 5
front panel 5
rear panel 5
Class A digital apparatus 10
CLI 5
CMOS 27, 33
COM port 21
Command Line Interface 5
configuration
additional config 23, 48
default email contact 51
ethernet port 48
mgmt port routing 50
remote syslog server 52
LCD setup wizard 23, 37
begin setup 40
complete setup 47
config settings 38
default gateway 45
host mgmt port 43
panel overview 38

buttons 39
super-user 41
timekeeping 46
overview 25
terminal setup wizard 23, 26
account security 28
config settings 27
default gateway 32
host mgmt port 31
NMS 36
SMS 36
super-user 29
timekeeping 33
web/CLI/SNMP 34
connector & pinout specs 57
mgmt processor connectors 57
DB-9 (COM) 57
DB-9 pinout 58
RJ-45 connector 58
port connectors 59
connector & pinout specifications 59
pluggable transceivers 59
contrast set 66
copper (RJ-45) ports 21
core functionality 2
customer support x

D
daylight saving time 27, 33, 46
DB-9 (COM) 57
DB-9 pinout 58
default email contact 51
domain 51
e-mail server IP 51
FROM 51
period 51
TO 51
default gateway 32, 45
destination network 50
devices 3
Digital Vaccine 5
domain 51
DST 27, 46
dual power supply
connect 19
duplex setting 49

E
Electromagnetic Static Discharge 13
electromagnetic static discharge 10
email server IP 51
environmental requirements 13
ESD 10, 13
ethernet port 48
options 49
auto negotiation 49
duplex setting 49
line speed 49
segments 49

F
FCC rules 10
fiber optic connection
MMSRF 14
SMIRF 14
SMLRF 14
fiber-optic connection 14
FROM email address 51

G
gateway 50
guide
conventions vi
cautions vii
notes viii
tips viii
warnings vii
customer support x
organization vi
overview vi
related documentation ix
target audience v

H
HA query state 67
halt OS 66
hardware installation 17
host management port 31, 43
host IP 31, 43
host location 31
host name 31, 43
network mask 31, 44
host name 43
HTTP 27, 34
server 35
HTTPS 27, 34
server 35

I
INHA 2
installation hardware 17
chassis 18
bolt to rack 19