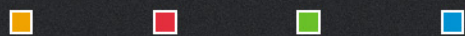




# IN-tact™ 1101

Software Configuration Guide



innovation. results. leadership.



[www.hypercom.com](http://www.hypercom.com)

Part Number: 940433-001

Copyright 2004 by Hypercom Corporation

All rights reserved. Printed in the United States of America.

This publication is propriety to Hypercom and intended solely for use by Hypercom customers. It may not be reproduced or distributed for any purpose without the written permission of Hypercom.

The information Hypercom furnished in this publication is believed to be accurate and reliable. However, Hypercom assumes no responsibility for its use. Hypercom also reserves the right to make changes to the publication at any time without notice.

## **Trademarks**

Hypercom, Term-Master, and the Hypercom logo are registered trademarks of Hypercom Corporation. *IN-tact* is a trademark of Hypercom Corporation.

Hypercom has attempted throughout this publication to distinguish proprietary trademarks from descriptive terms by following the capitalization style the manufacturer uses. Every effort was made to supply complete and correct information. Any error in identifying or reflecting any proprietary marks or notices is inadvertent and unintentional.

## **Acknowledgements**

This product includes software developed by the University of California, Berkeley and its contributors.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

---

# Table of Contents

## Chapter 1 - Introduction

---

|                        |   |
|------------------------|---|
| Product Overview ..... | 1 |
| Product Features ..... | 1 |
| In This Document ..... | 2 |

## Chapter 2 - Software Information

---

|  |   |
|--|---|
| Overview .....                                 | 3 |
| Dial Backup Feature .....                      | 3 |
| Operating Modes .....                          | 4 |
| Operation without an Ethernet Connection ..... | 5 |

## Chapter 3 - Configuring the IN-tact 1101

---

|   |    |
|---|----|
| Overview .....                                  | 7  |
| Before You Begin .....                          | 7  |
| Login and Timeouts .....                        | 8  |
| IP Addressing .....                             | 9  |
| Using Static IP Addressing .....                | 9  |
| Using DHCP .....                                | 9  |
| Required Fields and Validation of Entries ..... | 9  |
| Materials Required .....                        | 10 |
| Operating System Requirements .....             | 10 |
| Data Entry - Use of Special Characters .....    | 10 |
| Internet Browser Recommendations .....          | 10 |
| Configuration Procedure .....                   | 10 |
| Navigation .....                                | 15 |
| Using the Toolbar .....                         | 16 |
| Configuration Screens .....                     | 17 |
| IN-tact 1101 Overview Screen .....              | 17 |
| System Settings Screen .....                    | 19 |
| Ethernet Port Settings Screen .....             | 20 |
| Ethernet Port Advanced Settings Screen .....    | 21 |
| Security Settings Screen .....                  | 23 |
| Web Interface Settings Screen .....             | 24 |
| SNMP Interface Settings Screen .....            | 26 |
| Dial Backup Settings Screen .....               | 27 |
| Advanced Settings Screen .....                  | 30 |
| Time Settings Screen .....                      | 32 |
| Terminal Port Settings Screen .....             | 34 |
| Host Port Settings Screen .....                 | 35 |
| Standard Host Settings Screen .....             | 36 |
| Permanent Mode Settings .....                   | 38 |
| On Demand Mode Settings .....                   | 39 |
| HTTP Host Settings Screen .....                 | 41 |
| Merchant Link Host Settings Screen .....        | 43 |

Transaction Settings Screen ..... 44

**Chapter 4 - Control Panel**

Overview ..... 45

File Management Functions ..... 46

    Loading Firmware ..... 47

    Exporting Firmware to a PC ..... 47

    Loading a Configuration to the IN-tact 1101 ..... 48

    Exporting a Configuration to a PC ..... 48

    Loading SSL Server Certificates to the IN-tact 1101 ..... 48

    Deleting an SSL Server Certificate from the IN-tact 1101 ..... 50

    Load SSL Client Key to IN-tact ..... 50

System Operations Screen ..... 51

Set Date/Time Screen ..... 53

Clear Statistics Screen ..... 54

Dial Backup ..... 55

**Chapter 5 - Status**

Overview ..... 57

System Status Screen ..... 58

Terminal Port ..... 60

Host Port Status Screen ..... 61

    Error Codes ..... 62

Dial Backup Status ..... 63

**Chapter 6 - Diagnostics**

Overview ..... 67

Event Logging Setup ..... 68

Event Log View ..... 69

    Event Log Message Table ..... 70

**Chapter 7 - Configuration Examples**

Overview ..... 75

System Identification - Managed ..... 76

Ethernet Port Settings - Minimal ..... 77

Ethernet Port Settings - Managed ..... 78

Host Processor Setup - Minimal with Single Host ..... 79

Host Processor Setup - Minimal with Multiple Hosts ..... 82

Transaction Routing - Minimal ..... 86

Merchant Terminal Setup - Minimal ..... 87

SNMP Setup - Managed ..... 88

    Determining the NII Value from a Terminal ..... 89

Performing a Hex Dump ..... 90  
 Determining the NIDs in Use ..... 90

**Chapter 8 - SNMP Traps**

---

Overview ..... 91  
 SNMP Usage ..... 92  
   Changing a Configuration ..... 92  
   Setting the configEditionControl Variable ..... 93  
 Trap Definitions ..... 93  
   SNMP Variables Used for Setting Time ..... 94  
   System Error Codes ..... 95  
 Time Zone Table for SNMP ..... 97  
 IN-*tact* 1101 MIB ..... 99



---

# Chapter 1: Introduction

---

## Product Overview

The Hypercom® IN-*tact*™ 1101 is an IP gateway device that provides protocol conversion and secure managed connections for Hypercom Point of Sale (POS) terminals. The product is used to convert transactions on a Hypercom POS LAN (HLAN) to Internet Protocol (IP) transactions over Ethernet UTP. The IN-*tact* 1101 allows you to use your current POS LAN and take advantage of a DSL or cable modem Ethernet connection to access a host using TCP/IP protocol.

The IN-*tact* 1101 is designed to require no programming by the end user. All configuration is done via software prior to delivery at the point of installation. The IN-*tact* unit is shipped from the factory with a default software configuration. Further software configuration, such as unique IP addresses, are usually determined and loaded to flash memory by a deployment center or other customer support group. The unit is then sent to the point of installation where final installation consists of simply connecting the unit to power and to the existing network structure.

---

## Product Features

Basic product features include:

- Connects up to 16 Hypercom terminals via the RS-485 LAN (HLAN) standard at 19.2kbps or 4800bps
- Supports Hypercom TPDU multi-host concepts to route transactions via multiple TCP/IP sessions
- Delivers redundant TCP/IP connection to backup host destinations
- Provides 10/100Mbps auto-sensing support for connection to existing DSL, cable modems, or routers
- Dial backup operation available by connecting an external modem.

- Supports industry-standard Secure Socket Layer (SSL) for secure transactions over the Internet
- Easy-to-install procedure allows devices to be delivered fully configured to customer locations
- Supports SNMP services for use with existing customer-provided management systems
- Includes integrated Web server allowing secure management via standard Web browser.

---

## In This Document

This document provides information for configuring the IN-*tact* 1101 IP gateway device. In this document, you will find:

- General information about the IN-*tact* 1101 software
- Configuration instructions
- Configuration examples
- Information on SNMP traps



---

# Chapter 2: Software Information

---

## Overview

The IN-*tact* 1100 Series IP Gateways are software-driven devices. The functions that a particular model can perform depend on the version of application software that has been loaded into the unit's memory at the factory. Configuration is performed via a Web Server interface, providing the IN-*tact* 1101 with a unique IP address and personality. This document discusses the IN-*tact* 1101 model and how the device is configured using the on-board Web Server. Other operational information, such as loading software updates on the device, viewing the device status, and the Event Log are also discussed.

**NOTE:** It is important to note that the hardware and software function as a matched set called a "model". Self checks are built into the boot process that validate any software loaded on the unit. This prevents programming the unit with an application that is not intended for the specific IN-*tact* 1100 model. In other words, you cannot change the model number or add features from another model just by loading new software.

---

## Dial Backup Feature

In addition to processing IP transactions, the IN-*tact* 1101 features dial backup capability in the event of ISP (or other) outage that affects the ability to process transactions via the device's Ethernet port. A compatible modem must be physically connected to Port 1 (RS-232) on the IN-*tact* 1101 and a working telephone line connected to the modem in order to use the dial backup feature. Currently supported modems include:

- US Robotics 5686e
- Hayes H08-15328-C
- ZOOM 3048C

Other models of modems may also work with the IN-tact 1101. However, unlike supported modems, the Last Modem Connect Speed may not be reported correctly on the Dial Backup Status screen.

Within the IN-tact 1101, availability of the Ethernet port is constantly monitored. Once dial backup is enabled, any outage of the Ethernet port lasting longer than five seconds automatically triggers the device to switch to dial backup mode. Likewise, dial backup is automatically disconnected (based on a period of inactivity you specify) once the Ethernet connection is restored. The IN-tact 1101 can be configured to operate indefinitely in dial mode, if so desired.

---

## Operating Modes

The IN-*tact* 1101 can operate in one of three different modes, referred to as “boot modes”. The boot mode is controlled by whether or not the unit’s Reset button has been activated when power is applied. A description of each of the operating modes is provided below.

**NOTE:** If you have already configured the unit, save your configuration before resetting or erasing the current configuration as described below. See the “File Management Functions” section on page 46 for details on exporting/importing a configuration file.

- **Normal mode** — Upon applying power, the IN-*tact* 1101 loads the programmed application and performs all of its “normal” operating tasks. The unit automatically boots and operates in this mode. This is the normal mode of operation at the point of installation.
- **Factory Default mode** — This mode can only be initiated by pressing and holding the **Reset** button on the back of the unit **while** applying power to the unit. When this mode is initiated, the boot loader software invalidates the downloaded application and all configuration data. This process is called “returning to factory defaults” and removes all user changes as well as any application upgrades that have been installed. This mode reverts the IN-*tact* unit to its original “out-of-the-box” state. The unit must have any upgraded application reloaded and it must also be reconfigured before it can be used to process transactions. The password is reset to the factory default of “12345678”.
- **Erase Configuration mode** — Pressing and holding the **Reset** button **after** power is applied sets this mode. The **Reset** button should be held until the LEDs on the back on the IN-*tact* 1101 unit begin to blink. When this mode is initiated, only the configuration data in flash memory is erased. This process is called “returning to the default configuration” and removes all user changes, but keeps any application upgrades that have been loaded into the IN-*tact* unit. The unit must then be reconfigured, but the application does not need to be reloaded. Press the **Reset** button again to restart the unit. The default password of “12345678” must be used to log in.

---

## Operation without an Ethernet Connection

The IN-*tact* 1101 can be configured to use only the modem with a PPP connection instead of using Ethernet, but an Ethernet connection must initially be available in order to configure the device for this type of operation.

To set up for this type of configuration:

1. Attach the Ethernet cable and log in using the IN-*tact* 1101 IP address.
2. Configure the IN-*tact* 1101, including:
  - Enable Dial Backup
  - Disable DHCP
  - Be sure you have the proper initialization string for your modem type
  - Set to Immediate Mode (if you want the connection to dial without waiting for a transaction)
  - Set to Inactivity Disconnect Timer to zero (if you want the connection to stay up indefinitely)

The recovery timer becomes meaningless when no Ethernet cable is attached.

3. If set to Immediate Mode, when the idle timer expires, the IN-*tact* will immediately dial.
4. Click the **Apply and Restart** button. The device will restart and dial mode will be initiated (when set to Immediate Mode).



---

## Chapter 3: Configuring the IN-tact 1101

---

### Overview

No CD-ROMs or diskettes are required to configure the IN-*tact* 1101. All configuration is done via a resident Web Server application, or alternately, through a SNMP manager. Initial configuration can only be accomplished via the Web Server application. SNMP is disabled by default. You can connect to the Web Server application using an Internet browser. After logging in to the unit, you can use a series of screens to configure the unit to match both the terminal configuration and desired network settings at the point of installation. When all configuration is complete, you must save the settings. The settings are then written to persistent memory within the device and the device restarts. You must then log in to the device again in order to continue. The procedures provided here assume you are configuring the unit for the first time.

The order in which you configure the IN-*tact* is up to you. The Web Server allows you to go to any screen, at any time, in any order. The configuration screens are presented here in the order in which they appear on the navigation tree of the Web Server application. However, once you are familiar with the configuration process, you can configure the device in any order that makes sense to you.

It is important to note that you can export a configuration from one IN-*tact* 1101 and import it into another. This can save time if you are tasked with configuring multiple devices. Rather than having to configure all of the settings on each device, you can configure one, export the configuration, then import it into the other devices and make any necessary minor changes, such as assigning a unique IP address to each device. Procedures for importing and exporting a configuration are in the File Management Functions section on page 28.

---

### Before You Begin

**IMPORTANT:** Read this section before beginning any configuration.

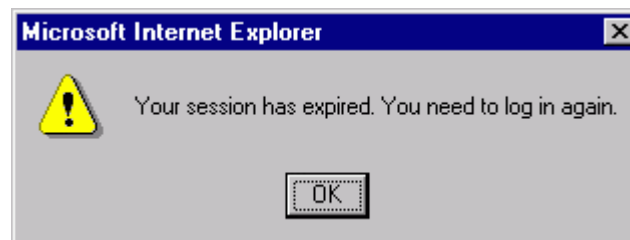
## Login and Timeouts

For security, the Web Server has a five-minute timeout by default. However, this can be changed during configuration to be up to an hour. You can also completely disable the timeout feature. It is suggested that you gather all configuration information, such as terminal CU addresses, host processor configuration, IP address, etc. before you begin the configuration process. If there is no activity within a four-minute period, the following warning appears:



**NOTE:** If you have multiple applications open, it is possible that the warning may not appear in your foreground and could be hidden behind another window. We recommend keeping the Web Server interface maximized on your screen.

If you click **OK** in the warning, the timer resets and a new five-minute “no activity” countdown begins. The warning remains for one minute. If you do not acknowledge it within that time, your session expires and the following message appears:



You are now required to log in to the device again. If you time out due to no activity during the configuration process, your settings are not saved and you will have to start over. If you are viewing the online Help, the session timer continues to run.

The IN-*tact* 1101 automatically logs you out of the Web Server interface when you close the browser window. However, if the web session timeout feature is disabled, the session remains open. For example, if you browse to other sites while configuring the IN-*tact* 1101, it may appear that another session is already in progress when you return to the IN-*tact*'s address.

It is important to understand that only one user may be logged in to the IN-*tact* 1101 Web Server interface at any given time. For example, assume that User 1 has already logged in and has a session in progress. When User 2 attempts to log in, the IN-*tact* Login screen displays with a red message stating "Another user is logged in. If you continue, their session will expire immediately." If User 2 continues to enter the password and log in at this point, User 1 is logged off and that session is closed. A new session is started for User 2. User 1 will see a message stating "Your session is no longer valid. Please log in again." when they select a screen. Any changes made by User 1 that have not been saved with Apply and Restart are discarded.

## IP Addressing

You must determine whether to use static IP addressing or DHCP-assigned IP addressing. This is important because the unit is set to seek a DHCP address by default.

Before configuration, the IN-*tact* 1101 automatically tries to obtain a DHCP address three times when first powered on. If a DHCP address is not found, the unit reverts to and operates at its default static IP address of “**192.168.1.20**”.

**NOTE:** After configuration, if the DHCP option is enabled, the IN-*tact* 1101 will never fall back to a static IP address. It will always seek a DHCP address.

## Using Static IP Addressing

The default IP address is valid until you configure the IN-*tact* 1101. It is assumed that you will assign an IP address during configuration (or leave DHCP enabled). Make note of the new assigned IP address. It is a good idea to write the IP address on a label or tag and physically attach it to the unit for future reference. If you need to reconfigure the unit at some point in the future, use the assigned IP address, not the default IP address. If the IP address is lost or becomes unknown, the only way to reconfigure the unit is to reset it to configuration defaults, which will restore the default IP address. However, you will also have to reconfigure all IN-*tact* 1101 settings if you reset it to configuration defaults.

## Using DHCP

If you are using DHCP to assign addresses on your network, contact your DHCP administrator to obtain the IP address for this unit, based on its MAC address. The unit's MAC address is located on the serial number tag on the bottom of the unit. In most cases, a particular IP address should have already been reserved for the unit and that IP address should be used to contact the unit for configuration.

If a random DHCP IP address is assigned, you must determine what IP address has been assigned to the IN-*tact* 1101 in order to contact it for configuration. This will have to be done through DHCP, you cannot determine a randomly assigned IP address from the IN-*tact* 1101.

## Required Fields and Validation of Entries

At a minimum, you are required to configure at least one host address with a valid IP address or URL and one terminal. Otherwise, an error message indicating an “invalid configuration” appears when you attempt to save the configuration. Error messages will continue to appear, informing you of what is needed, until you have configured at least the minimum the IN-*tact* 1101 needs to operate. In general, validation of individual entries is not performed; you need to check your entries to make certain they are correct.

## Materials Required

You will need the following in order to configure the IN-*tact* 1101:

- A laptop or desktop PC with Internet browser (Microsoft Internet Explorer, version 5.0 or higher. Other browsers are not currently supported.)
- Two standard Ethernet cables (any length) - one to connect your PC to the hub; the other to connect the hub to the IN-*tact* 1101.
- Access to a hub for connections to the PC and IN-*tact* 1101 unit
- IN-*tact* 1101 and power supply connected to standard AC power outlet.

## Operating System Requirements

Windows 2000 Service Pack 3 or higher should be installed on the computer being used to configure the IN-*tact*.

## Data Entry - Use of Special Characters

In general, do not use the "double-quote" special character (like the one surrounding the word) in data entry fields. It is not recognized as a valid character by the IN-*tact* 1101. The exception to this is within dial strings. The double-quote character can be used with no problem when being defined as part of a dial string.

## Internet Browser Recommendations

Some browser settings can cause extra system messages to appear and cause other issues. The following items are suggestions for browser setup while configuring the IN-*tact* 1101:

- If you use a pop-up blocker, either temporarily disable it or enable it to allow pop-ups from the IN-*tact* 1101. Otherwise, pop-up messages from the device may be blocked.
- Enable cookies (no prompt) to avoid numerous browser pop-ups about cookie acceptance
- Active scripting needs to be enabled. By default, active scripting is enabled in Internet Explorer. You can check or change the setting of this option in Internet Explorer by clicking **Tools > Internet Options > Security** tab > **Custom Level**. Scroll down the list to locate the **Active Scripting** option. Click to enable, if it is disabled.
- It is recommended to clear your browser's cache before configuration or anytime you upgrade firmware for the device. This is particularly important after a firmware upgrade, as you may not see the most current Web Server pages unless you clear the browser's cache.

---

## Configuration Procedure

Use this procedure when you are ready to configure the IN-*tact* 1101. If you have not already done so, please read the preceding section before beginning any configuration.

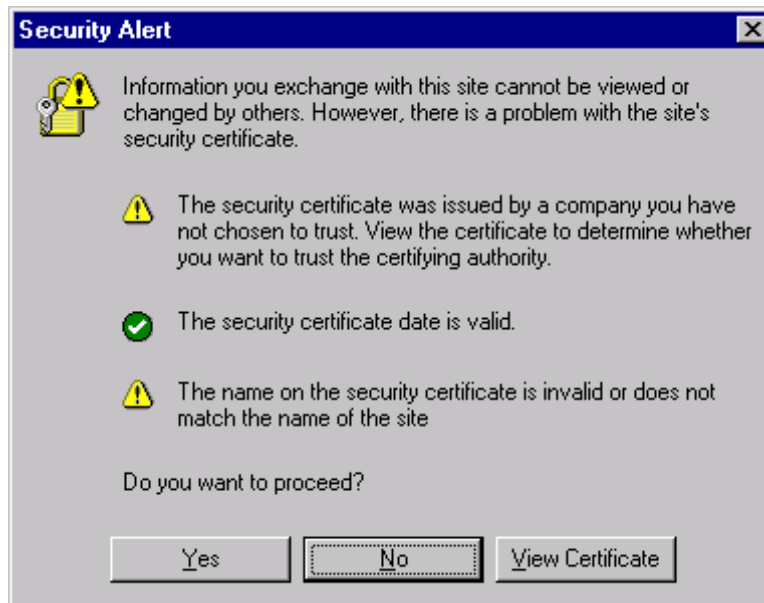
To configure the IN-*tact* 1101:

1. Connect the IN-*tact* 1101 to your PC or to a network hub. Use a standard Ethernet cable to connect the LAN port on the IN-*tact* 1101 to a hub, or directly to an Ethernet port on the PC

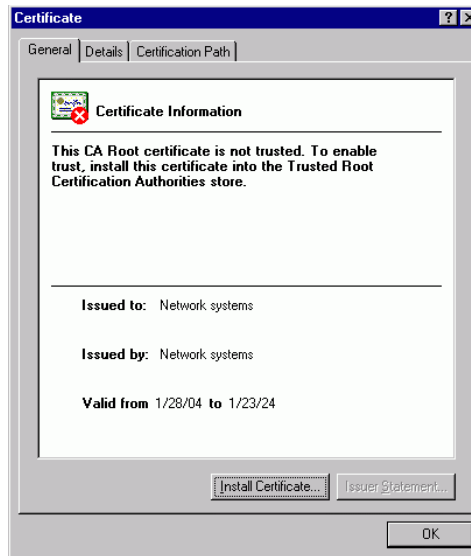


(direct connection to the PC requires a crossover Ethernet cable). Connection to a terminal or terminal network is not required in order to configure the device.

2. Apply power to the IN-*tact* 1101 and power on your PC. By default, the IN-*tact* 1101 seeks a DHCP IP address. Both LEDs on the LAN port will flash in short intervals as the unit seeks a DHCP IP address. This takes about 15 seconds.
3. On your PC, open the Internet browser (Microsoft Internet Explorer 5.0 or higher).
4. In the browser address bar, type the IN-*tact* 1101 IP address (either DHCP assigned or the default static address of 192.168.1.20).
5. Press **Enter**. The IN-*tact* 1101 responds with the following message:



6. Click **Yes** to continue. The Login screen appears.
  - If you click **No**, the Security Alert window closes and the login process is cancelled.
  - If you click **View Certificate**, the Certificate Information window appears.



This window is displayed by Internet Explorer and allows you to view certificate details and install a certificate on your computer.

To install the Hypercom certificate on your machine, click **Install Certificate** and follow the instructions presented by the Import Certificate wizard.



## **IN-tact Login**

To access and configure your IN-tact 1101 device, you need to log in.

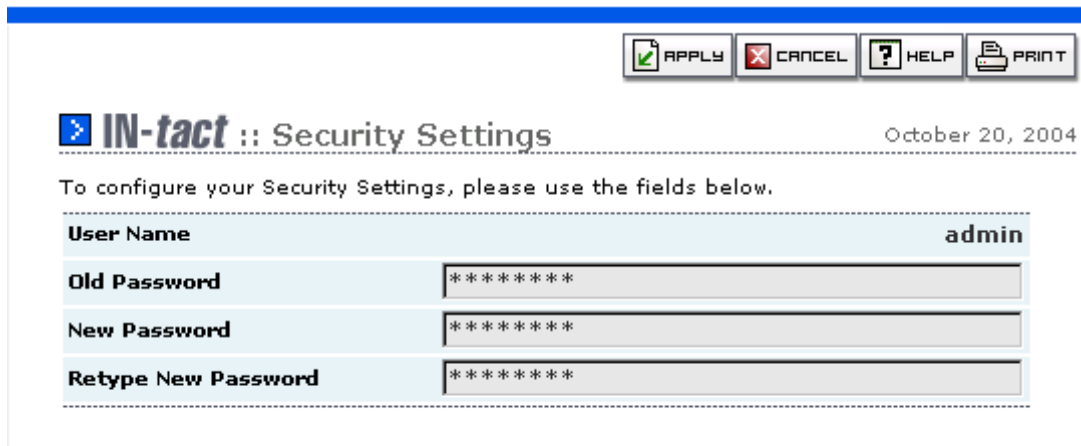
You are connected to Device ID: **0326**

Please enter your password.

**Username:** admin

**Password:**

7. On the Login screen, enter the default password “12345678” and click **OK**. You must change the password after your initial log in, as well as any time the device detects the default password is in use. The following screen appears:



The screenshot shows a web-based configuration interface for the IN-tact 1101. At the top right, there are four buttons: APPLY (with a green checkmark icon), CANCEL (with a red X icon), HELP (with a question mark icon), and PRINT (with a printer icon). Below these buttons is the page title "IN-tact :: Security Settings" and the date "October 20, 2004". The main content area contains the instruction "To configure your Security Settings, please use the fields below." followed by a form with four fields: "User Name" (containing "admin"), "Old Password" (containing "\*\*\*\*\*"), "New Password" (containing "\*\*\*\*\*"), and "Retype New Password" (containing "\*\*\*\*\*").

|                            |       |
|----------------------------|-------|
| <b>User Name</b>           | admin |
| <b>Old Password</b>        | ***** |
| <b>New Password</b>        | ***** |
| <b>Retype New Password</b> | ***** |

**NOTE:** You must set the password within the five-minute time period; it is suggested you do so immediately. If the time limit expires, you will have to reset the device in order to log in.

**Password guidelines:**

- There is one default user name (admin) and it cannot be changed
- The new password cannot be the same as the default
- The password can be changed whenever necessary on the System Setup - Security screen
- There is no password expiration period; the password you set remains valid until it is changed
- A minimum of eight characters are required, maximum of 32 characters
- Mixed case (upper and lowercase) is permitted

To change the password:

1. Type the current password in the **Old Password** field. For security purposes, your entry will appear as a series of asterisks.
2. Type the new password in the **New Password** field. It must be a minimum of eight characters.
3. Type the new password again in the **Retype New Password** field to confirm.
4. Click **Apply** to continue. The IN-tact 1101 Overview screen appears.

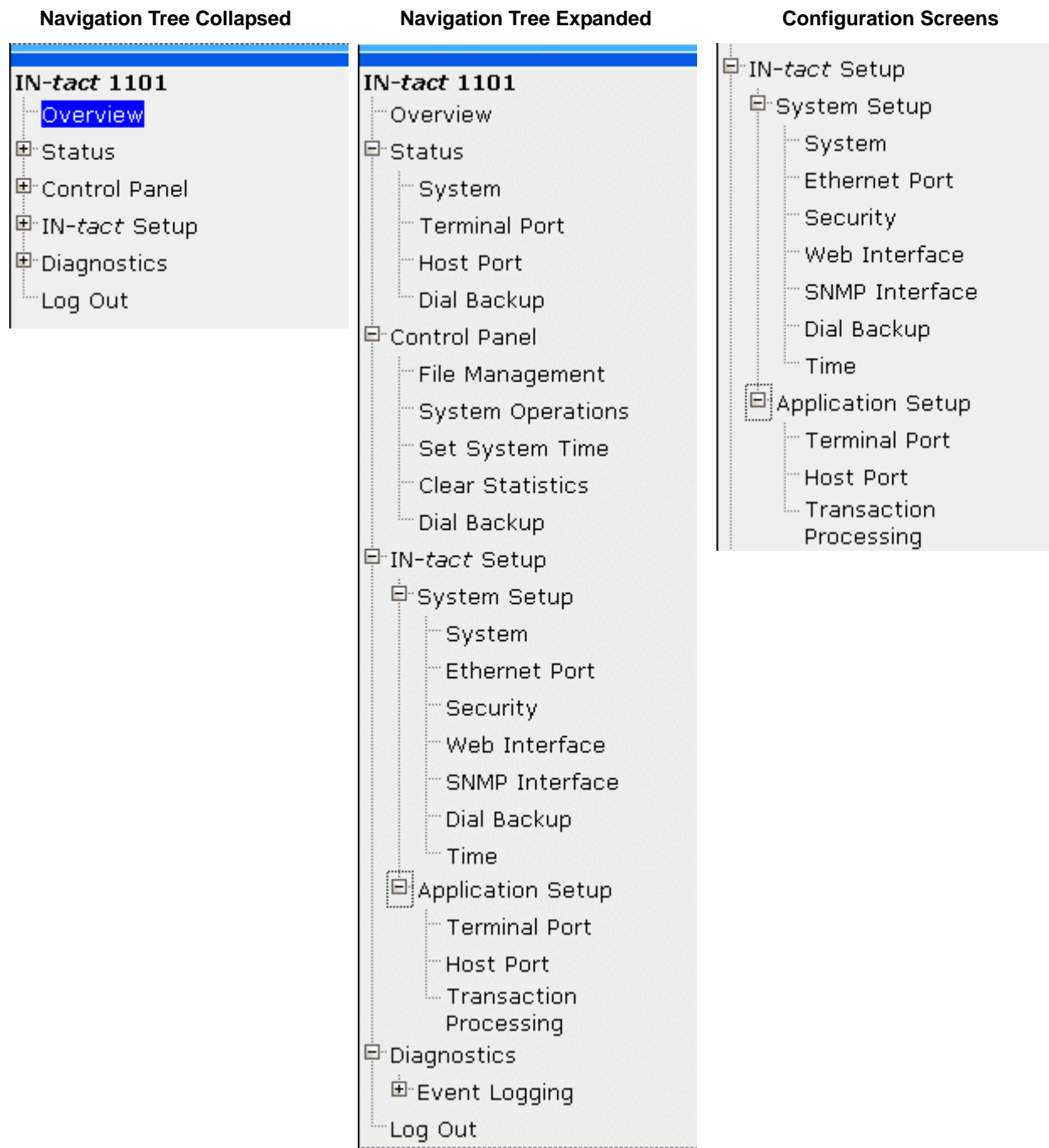
|                      |                                     |
|----------------------|-------------------------------------|
| <b>IN-tact Model</b> | <b>1101</b>                         |
| <b>Description</b>   | <b>IN-tact 1101</b>                 |
| <b>Device ID</b>     | <b>0326</b>                         |
| <b>Location</b>      | <b>Store 1104</b>                   |
| <b>Contact</b>       | <b>Steven Albers - 602-480-0555</b> |
| <b>MAC Address</b>   | <b>00:40:EF:00:00:47</b>            |
| <b>IP Address</b>    | <b>192.168.1.102</b>                |
| <b>IP Gateway</b>    | <b>100.200.100.1</b>                |
| <b>DNS Server</b>    | <b>100.200.100.1</b>                |

At this point, you can use the navigation tree on the left side of the screen to go to any of the configuration screens. Each screen and the entries you should make are explained in the following pages.

## Navigation

The IN-*tact* 1101 configuration navigation tree is easy to understand; its operation is similar to Internet Explorer and other like applications. Shown below are examples of the navigation tree in its initial state of completely collapsed, fully expanded, and a subset of the configuration screens.

- Click on the + or - symbols to expand or close branches of the tree
- Click on any screen name to invoke that screen.



---

## Using the Toolbar

A toolbar displays near the upper-right corner of each IN-*tact* 1101 screen. Only the buttons applicable to the selected screen display.



For example, most configuration screens display both an **Apply** and **Restart** button and a **Save** and **Continue** button. Read-only screens, like Overview, display only a **Help** and **Print** button.

It is important to understand how the buttons work and which one you should use in a particular situation. The purpose and difference between apply and restart and save and continue is explained below.

- **Apply and Restart** - This button writes any changes you have made to persistent memory and immediately restarts the device so that the changes take effect. This can be valuable when making a single change to the configuration. However, because of the time it takes to restart the device, it is more practical to use **Save and Continue** if you are making multiple changes. You must use this button after making a series of changes in order to save them.

In a few cases, like changing passwords and event logging settings, this button is labeled **Apply** rather than **Apply and Restart**. In these cases, your changes are applied immediately and you do not have to restart the device. However, all configuration changes require that the changes first be written to persistent memory, then the device restarted, in order for your changes to become effective.



- **Save and Continue** - This button saves your changes in temporary memory and allows you to continue on to other settings screens without immediately restarting the device. After all changes are made, you must click **Apply and Restart** in order to write the changes to persistent memory. This is valuable when initially configuring the device or making multiple changes. If you time out due to no activity during the configuration process, these temporary settings are not saved and you will have to start over.


**NOTE:** On screens that feature advanced or related options on a second screen, any changes made on the first screen are temporarily saved when you click **Edit** or **Advanced** to access the second screen. You must still use **Apply and Restart** in order to write the changes to persistent memory.

- **Back** - This button appears only on secondary Edit or Advanced option screens. Clicking it returns you to the previous configuration screen.
- **Cancel** - This button cancels any changes you have made on the current screen and resets each field to its previous value. It does not affect any changes you have temporarily saved on other screens. This is valuable if you have made a mistake during data entry, or just want to “start over” on a particular settings screen during configuration.
- **Help** - This button opens on-line Help in a separate window for the screen that is currently displayed. Most of the information contained in this software guide is available in on-line Help.
- **Print** - This button prints a copy of the current screen to your default printer. This can be useful if you like to keep a hardcopy record of the device’s configuration.

## Configuration Screens

### IN-tact 1101 Overview Screen



### IN-tact :: Model 1101 Overview

October 21, 2004

Welcome to the IN-tact Model 1101 Web Browser Management Interface. You can use the menu navigator on the left side of this page to view and change settings for your IN-tact Model 1101 device.

|                      |                                     |
|----------------------|-------------------------------------|
| <b>IN-tact Model</b> | <b>1101</b>                         |
| <b>Description</b>   | <b>IN-tact 1101</b>                 |
| <b>Device ID</b>     | <b>0326</b>                         |
| <b>Location</b>      | <b>Store 1104</b>                   |
| <b>Contact</b>       | <b>Steven Albers - 602-480-0555</b> |
| <b>MAC Address</b>   | <b>00:40:EF:00:00:47</b>            |
| <b>IP Address</b>    | <b>192.168.1.102</b>                |
| <b>IP Gateway</b>    | <b>100.200.100.1</b>                |
| <b>DNS Server</b>    | <b>100.200.100.1</b>                |

The Overview screen is your starting point on the IN-tact 1101 and appears whenever you log in to the device or click Overview on the navigation tree. It provides a quick overview of current settings, along with identification information to help you confirm that you are connected to the correct device. The Overview screen is read only; there are no fields or required entries. Some of the information shown here is the result of your setting on other screens.

| Field         | Description   |
|---------------|---|
| IN-tact Model | Hypercom model number of the unit. This number is important because there are several models within the IN-tact product series. This number cannot be changed.  |
| Description   | Free-form description of the IN-tact device. This information comes from the System Settings screen and can be as descriptive as you wish.  |
| Device ID     | A free-form alphanumeric value (up to 32 characters) entered on the System Settings screen to help identify this IN-tact 1101 from others on your network. Each IN-tact 1101 should be assigned a unique Device ID. |
| Location      | This is the physical location or point of installation for this device, such as "South Phoenix Store" or "Store 632". This information is entered on the System Settings screen.                                    |

| Field       | Description  |
|-------------|--|
| Contact     | This can be the name of the administrator, support group, help desk, or other entity to contact for information about this configuration. This information is entered on the System Settings screen. |
| MAC Address | Current MAC address of the IN- <i>tact</i> 1101. This is not normally changed, but can be configured on the Ethernet Port Settings screen.   |
| IP Address  | Current IP address of the IN- <i>tact</i> 1101. The IP address is set on the Ethernet Port Settings screen.  |
| IP Gateway  | Configured IP address of the IP gateway router if using static addressing; learned IP gateway address if using DHCP. If you need to change this setting, go to the Ethernet Port Settings screen.    |
| DNS Server  | The current DNS server in use. A static DNS server can be configured if DHCP is not being used. If you need to change this setting, go to the Ethernet Port Settings screen.                         |



## System Settings Screen

On the navigation tree, click **IN-tact Setup > System Setup > System**. The System Settings screen appears:

| Field/Button | Description                  |
|--------------|------------------------------|
| Description  | IN-tact 1101                 |
| Device ID    | 0326                         |
| Location     | Store 1104                   |
| Contact      | Steven Albers - 602-480-0555 |

This screen is used to configure basic information about the IN-tact 1101. Entries on this screen also appear on the Overview screen.

| Field/Button | Description   |
|--------------|---|
| Description  | Use this field to define the device type (IN-tact 1101) or its purpose, such as "IP gateway for POS network." The information you decide to include here is up to you; up to 32 characters are accepted.  |
| Device ID    | Enter a unique identifier for the device. This is a free-form alphanumeric value of up to 32 characters, including spaces. An entry is required here; you cannot leave the Device ID blank or use only a space as an entry.                       |
| Location     | Enter the physical location or point of installation for this device, such as "South Phoenix Store" or "Store 632". Up to 256 characters are accepted.  |
| Contact      | Enter the name of the administrator, support group, help desk, or other entity that can be contacted for information about this configuration. You might want to include a phone number or email address here. Up to 256 characters are accepted. |

**NOTE:** Click **Save and Continue** or **Apply and Restart** as appropriate. Keep in mind that your changes are not written to persistent memory until you click **Apply and Restart**.

## Ethernet Port Settings Screen

On the navigation tree, click **IN-tact Setup > System Setup > Ethernet Port**. The Ethernet Port Settings screen appears:

To configure your Ethernet Port Settings, please use the fields below.

|   |                             |
|---|-----------------------------|
| MAC Address                                     | 00 : 40 : EF : 00 : 00 : DC |
| Static IP Address                               | 192.168.1.20                |
| Static Subnet Mask                              | 255.255.255.0               |
| Static Gateway Address                          | 0.0.0.0                     |
| Static DNS Server                               | 0.0.0.0                     |
| <input checked="" type="checkbox"/> Enable DHCP |                             |

Advanced ->

Use this screen to set basic communication parameters for the Ethernet Port on the IN-tact 1101. Only IP version 4 is supported. The MAC address can be changed in the rare event that MAC address filtering or other firewall issues are preventing the provided MAC address from working correctly. If not using DHCP, you are required to configure a valid IP address for the IN-tact 1101 to be operational. You cannot permanently save the configuration until you do so.

| Field/Button           | Description   |
|------------------------|---|
| MAC Address            | Unique address of this IN-tact 1101.  |
| Static IP Address      | Change to match the IP addressing requirements for your network. By default, DHCP is enabled and this field displays "192.168.1.20".  |
| Static Subnet mask     | Change to match the local IP subnet of your network. The default is 255.255.255.0.  |
| Static Gateway Address | Enter the gateway address used to route IP off the local subnet. The default is 0.0.0.0.  |
| Static DNS Server      | Enter the IP address of the DNS server that should be used.   |
| Enable DHCP            | Enabled by default. Click to disable DHCP and use a static IP address. If DHCP is enabled, both of the LEDs on the LAN connector of the IN-tact 1101 will flash in unison when the device is powered on and is attempting to acquire an IP address. |

**NOTE:** Click **Save and Continue** or **Apply and Restart** as appropriate. Keep in mind that your changes are not written to persistent memory until you click **Apply and Restart**. Any changes made on this screen are temporarily saved when you click **Advanced** to access the second screen. You must still use **Apply and Restart** in order to write the changes to persistent memory.

## Ethernet Port Advanced Settings Screen

On the navigation tree, click **IN-tact Setup > System Setup > Ethernet Port > Advanced**. The Ethernet Port Advanced Settings screen appears:

**IN-tact :: Ethernet Port Advanced Settings** April 27, 2005

To configure your Ethernet Port Advanced Settings, please use the fields below.

**Keep Alive**

**Keep Alive Timer (seconds)**

**TCP Window Size**

**Number of Session Retransmits**

**Session Inactivity Timeout (seconds)**

**Restrict Source Port Range**

Several additional settings are available by clicking **Advanced** on the Ethernet Port Settings screen. These settings can be used to “fine tune” IN-tact 1101 performance on your network.

| Field/Button                  | Description   |
|-------------------------------|---|
| Keep Alive                    | Use this checkbox to enable or disable the keep alive features of the IN-tact 1101. This feature is enabled by default.<br><br>During keep alive operation, the IN-tact 1101 holds an established connection open for specified amount of time before automatically disconnecting.<br><br>When enabled, the IN-tact 1101 sends a keep alive message on each host connection at intervals set by the keep alive timer. |
| Keep Alive Timer (seconds)    | Enter the value (in seconds) between keep alive messages set to the host. Five seconds is the minimum, 600 seconds is the maximum. Thirty seconds is the default value.   |
| TCP Window Size               | Use the drop-down list to select the size of the TCP window to be used. Choose a value between 2KB and 8KB. The default value is 2KB.   |
| Number of Session Retransmits | Use the drop-down list to select the number of retransmissions allowed during a session. The default value is 4 and should not be changed.  |

| Field/Button                         | Description   |
|--------------------------------------|---|
| Session Inactivity Timeout (seconds) | Use the up and down arrows to set the number of seconds a session should remain active after no activity is detected. The default is 15 seconds. The minimum setting is five seconds, the maximum is 256 seconds.<br><b>Note:</b> This inactivity timer may have to be increased beyond the default setting to allow for larger messages, particularly when slow baud rates are in use. |
| Restrict Source Port Range           | Use this checkbox to enable or disable restricting the range of source port values for on-demand TCP connections. By default, source port values range from 1024 through 65534. Enabling this option restricts the source port values to the range of 1024 through 1039. Restriction is disabled by default.  |

**NOTE:** Click **Save and Continue** or **Apply and Restart** as appropriate. Keep in mind that your changes are not written to persistent memory until you click **Apply and Restart**.

## Security Settings Screen

On the navigation tree, click **IN-tact Setup > System Setup > Security**. The Security Settings screen appears:

**IN-tact :: Security Settings** October 20, 2004

To configure your Security Settings, please use the fields below.

|                            |       |
|----------------------------|-------|
| <b>User Name</b>           | admin |
| <b>Old Password</b>        | ***** |
| <b>New Password</b>        | ***** |
| <b>Retype New Password</b> | ***** |

This screen is used to set IN-tact 1101 security features. It also appears the first time you log in to the device with the default password. If you have already set the password, you can skip this screen and continue with configuration.

You can change the IN-tact 1101 password whenever necessary. There is one default user name for log in (admin) and it cannot be changed. There is no default time period for password expiration; the password you set remains valid until it is changed.

### Password guidelines:

- A minimum of eight characters are required, maximum of 32 characters
- Any combination of characters is permitted
- Mixed case (upper and lowercase) is permitted
- Default password is "12345678".

To change the password:

1. Type the current password in the **Old Password** field. For security purposes, your entry will appear as a series of asterisks.
2. Type the new password in the **New Password** field. It must be at least eight characters.
3. Type the new password again in the **Retype New Password** field to confirm.
4. Click **Apply** to temporarily save your settings. Your changes are immediately written to persistent memory. The new password is in effect the next time you log in to the IN-tact 1101.

## Web Interface Settings Screen

On the navigation tree, click **IN-tact Setup > System Setup > Web Interface**. The Web Interface Settings screen appears:

**IN-tact :: Web Interface Settings** October 20, 2004

To configure your Web Interface Settings, please use the fields below.

**Restrict Access to Web Server**

Web server access will be restricted to the following addresses:

|              |         |             |                 |
|--------------|---------|-------------|-----------------|
| IP Address 1 | 0.0.0.0 | Subnet Mask | 255.255.255.255 |
| IP Address 2 | 0.0.0.0 | Subnet Mask | 255.255.255.255 |

**Expire Inactive Web Sessions**

Inactive web sessions will expire after this period of inactivity (minutes):

**Inactivity Timeout**

You have the option of restricting access to the IN-tact 1101 web server to a specific IP address (or range of addresses). This is useful in preventing unauthorized access attempts on the device from IP addresses outside your normal range of operation.

You can also disable or change the value of the timeout feature associated with the web interface. This is a security feature. By default, the web session automatically expires after five minutes of no activity. The user is logged out. Any changes made to that point are discarded, unless Apply and Restart has been used to commit the changes to persistent memory. However, there may be situations in which you want to disable the timeout completely, or set it to a different value. For example, a direct "always on" connection to the web server, or while working with or configuring the device.

The IN-tact 1101 automatically logs you out of the web server interface when you close the browser window. However, if the web session timeout feature is disabled, the session remains open. For example, if you browse to other sites while configuring the IN-tact 1101, it may appear that another session is already in progress when you return to the IN-tact's address.

It is important to understand that only one user may be logged in to the IN-tact 1101 web server interface at any given time. For example, assume that User 1 has already logged in and has a session in progress. When User 2 attempts to log in, the IN-tact Login screen displays with a red message stating "Another user is logged in. If you continue, their session will expire immediately." If User 2 continues to enter the password and log in at this point, User 1 is logged off and that session is closed. A new session is started for User 2. User 1 will see a message

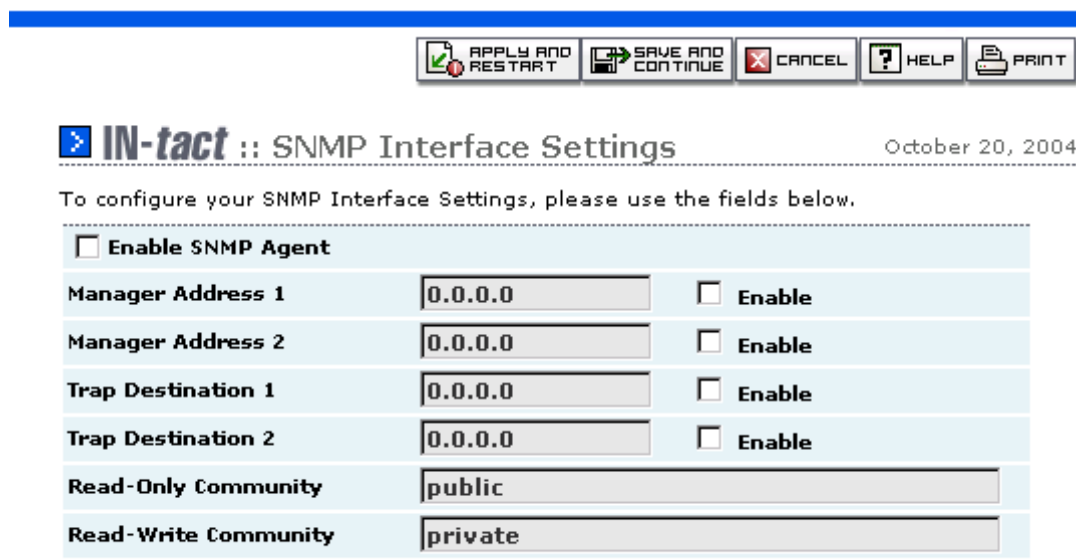
stating "Your session is no longer valid. Please log in again." when they select a screen. Any changes made by User 1 that have not been saved with Apply and Restart are discarded.

| Field/Button                  | Description  |
|-------------------------------|--|
| Restrict Access to Web Server | Use this checkbox to enable a specific range of IP addresses that will be able to contact the Web Server application.  |
| IP Address 1                  | Enter the first IP address that will be able to access the Web Server.   |
| Subnet Mask                   | Enter the corresponding subnet mask for IP address 1. In order to restrict access to only a single IP address, use a mask of 255.255.255.255.                            |
| IP Address 2                  | Enter the second IP address that will be able to access the Web Server.  |
| Subnet Mask                   | Enter the corresponding subnet mask for IP address 2.  |
| Expire Inactive Web Sessions  | Use this checkbox to enable or disable the inactivity timeout feature. This is not a dynamic change; you must Apply and Restart in order for this change to take affect. |
| Inactivity Timeout            | Set the value (in minutes) for how long a web session should stay active with no activity. The default value is 5 minutes. Valid entries are from 5 to 60 minutes.       |

**NOTE:** Click **Save and Continue** or **Apply and Restart** as appropriate. Keep in mind that your changes are not written to persistent memory until you click **Apply and Restart**.

## SNMP Interface Settings Screen

On the navigation tree, click **IN-tact Setup > System Setup > SNMP Interface**. The SNMP Interface Settings screen appears:



**IN-tact :: SNMP Interface Settings** October 20, 2004

To configure your SNMP Interface Settings, please use the fields below.

|   |                                      |  |
|---|--------------------------------------|--|
| <input type="checkbox"/> <b>Enable SNMP Agent</b> |                                      |  |
| <b>Manager Address 1</b>                          | <input type="text" value="0.0.0.0"/> | <input type="checkbox"/> <b>Enable</b> |
| <b>Manager Address 2</b>                          | <input type="text" value="0.0.0.0"/> | <input type="checkbox"/> <b>Enable</b> |
| <b>Trap Destination 1</b>                         | <input type="text" value="0.0.0.0"/> | <input type="checkbox"/> <b>Enable</b> |
| <b>Trap Destination 2</b>                         | <input type="text" value="0.0.0.0"/> | <input type="checkbox"/> <b>Enable</b> |
| <b>Read-Only Community</b>                        | <input type="text" value="public"/>  |  |
| <b>Read-Write Community</b>                       | <input type="text" value="private"/> |  |

SNMP management of the IN-tact 1101 is optional. The device is capable of hosting two separate SNMP sessions. Use this screen to configure the IP address for each of the sessions. Trap forwarding is optional and can be used independently of SNMP management.

| Field/Button         | Description   |
|----------------------|---|
| Enable SNMP Agent    | Use this checkbox to enable or disable the SNMP agent.  |
| Manager Address 1    | Enter the IP address of the first SNMP manager. Set the checkbox to enable or disable communication with this SNMP manager.                                   |
| Manager Address 2    | Enter the IP address of the second SNMP manager. Set the checkbox to enable or disable communication with this SNMP manager.                                  |
| Trap Destination 1   | Enter the first IP address to which the IN-tact 1101 should forward trap information. Set the checkbox to enable or disable trap forwarding to this address.  |
| Trap Destination 2   | Enter the second IP address to which the IN-tact 1101 should forward trap information. Set the checkbox to enable or disable trap forwarding to this address. |
| Read Only Community  | Enter the SNMP Read Only community string.  |
| Read Write Community | Enter the SNMP Read Write community string.   |

Click **Save and Continue** or **Apply and Restart** as appropriate. Keep in mind that your changes are not written to persistent memory until you click **Apply and Restart**.



## Dial Backup Settings Screen

On the navigation tree, click **IN-tact Setup > System Setup > Dial Backup**. The Dial Backup Settings screen appears:

APPLY AND RESTART
 SAVE AND CONTINUE
 CANCEL
 HELP
 PRINT

**IN-tact** :: Dial Backup Settings
October 20, 2004

To configure your Dial Backup Settings, please use the fields below.

**Enable Dial Backup**

|                                 |                        |   |
|---------------------------------|------------------------|---|
| <b>AT Initialization String</b> | ATE0V0Q0&C1&D2&K0&M4X4 | <input type="button" value="Reset to Default"/> |
| <b>AT Hang Up String</b>        | ATH0                   | <input type="button" value="Reset to Default"/> |

**Enable Primary Dial**

|                                       |  |
|---------------------------------------|--|
| <b>Primary AT Dial String</b>         | ATD  |
| <b>Authentication Methods Allowed</b> | <input checked="" type="checkbox"/> <b>CHAP</b> <input checked="" type="checkbox"/> <b>PAP</b> |
| <b>User Name</b>                      |  |
| <b>Password</b>                       |  |
| <b>Retype Password</b>                |  |

**Enable Alternate Dial**

|                                       |  |
|---------------------------------------|--|
| <b>Alternate AT Dial String</b>       | ATD  |
| <b>Authentication Methods Allowed</b> | <input checked="" type="checkbox"/> <b>CHAP</b> <input checked="" type="checkbox"/> <b>PAP</b> |
| <b>User Name</b>                      |  |
| <b>Password</b>                       |  |
| <b>Retype Password</b>                |  |

The IN-tact 1101 features dial backup capability in the event of ISP (or other) outage that affects the ability to process transactions via the device's Ethernet port. A compatible modem must be physically connected to Port 1 (RS-232) on the IN-tact 1101 and a working telephone line connected to the modem in order to use the dial backup feature. Supported modems include:

- US Robotics 5686e
- Hayes H08-15328-C
- ZOOM 3048C

Other models of modems may also work with the IN-*tact* 1101. However, unlike supported modems, certain status screens may not accurately reflect correct values.

Within the IN-*tact* 1101, availability of the Ethernet port is constantly monitored. Once dial backup is enabled, any outage of the Ethernet port lasting longer than 5 seconds automatically triggers the IN-*tact* 1101 to switch to dial backup mode. Likewise, dial backup is automatically disconnected (based on a period of inactivity you specify) once the Ethernet connection is restored.

This screen allows you to configure basic modem operation. Use the **Advanced** button to display additional modem configuration options.

| Field/Button             | Description  |
|--------------------------|--|
| Enable Dial Backup       | Click this checkbox to enable dial backup operation. By default, this operation is disabled.   |
| AT Initialization String | <p>Enter the initialization string for your modem. This string is sent to the modem every time dial backup starts. This string is sent to the modem every time dial backup starts. Up to 128 characters are accepted in this field. At a minimum, you must specify at least the command AT here; you cannot have a blank initialization string. The IN-<i>tact</i> 1101 looks for the response to the attention command to determine the modem's current state. Also, the IN-<i>tact</i> expects a numeric response. You must include the command V0 in your initialization string to require a numeric response from the modem.</p> <p>Consult the manufacturer's documentation for your specific modem to determine the command set being used and what commands are accepted by the modem. <b>Reset to Default</b> can be used to reset the initialization string to the default US Robotics modem setting of:</p> <pre>ATE0V0Q0&amp;C1&amp;D2&amp;K0&amp;M4X4</pre> <p>If you are using a Hayes or ZOOM modem, the initialization string should be set to:</p> <pre>ATE0V0Q0&amp;C1&amp;D2&amp;K3&amp;Q5W2</pre> |
| AT Hang Up String        | <p>This is similar to the initialization string, except this command string is sent to the modem to cause it to hang up. Enter the hang up string for your modem. Up to 20 characters are accepted in this field. Consult the manufacturer's documentation for your specific modem to determine the command set being used and what commands are accepted by the modem. Reset to Default can be used to reset the hang up string to the default setting of "ATH0". This default can be used for all supported modem types. Any additional commands you want to add to the string should be placed after the AT and before the H0. Any commands entered as part of the Hang Up string are automatically prefixed with "+++".</p>  |
| Enable Primary Dial      | Click this checkbox to enable the primary dial string. This is the first host processor that the modem will attempt to contact in the event of an Ethernet outage.   |
| Primary AT Dial String   | Enter any commands and the phone number to dial in order for the modem to establish contact with the primary host processor. Up to 32 characters are allowed in this field. This string must begin with ATDT (or ATDP for pulse dialing).  |

| Field/Button                   | Description   |
|--------------------------------|---|
| Authentication Methods Allowed | Click the CHAP and PAP checkboxes as necessary to match the authentication being used with this host processor. Both are enabled by default.  |
| User Name/Password             | If authentication is being used, enter both the User Name and Password to be transmitted in the appropriate fields.   |
| Retype Password                | Type the password again in the Retype Password field to confirm the password.   |
| Enable Alternate Dial          | Click this checkbox to enable an alternate dial string. The IN-tact 1101 will automatically attempt to contact this host processor if the primary modem connection is busy or unanswered.   |
| Alternate AT Dial String       | Enter any commands and the phone number to dial in order for the modem to establish contact with the alternate host processor. Up to 32 characters are allowed in this field. This string must begin with ATDT (or ATDP for pulse dialing). |

**NOTE:** Click **Advanced**, **Save and Continue** or **Apply and Restart** as appropriate. Keep in mind that your changes are not written to persistent memory until you click **Apply and Restart**. Any changes made on this screen are temporarily saved when you click **Advanced** to access the second screen. You must still use **Apply and Restart** in order to write the changes to persistent memory.

## Advanced Settings Screen

On the navigation tree, click **IN-tact Setup > System Setup > Dial Backup > Advanced**. The Advanced Dial Backup Settings screen appears:

|   | Hours                | Minutes |
|---|----------------------|---------|
| <b>Inactivity Disconnect Timer</b>  | 0                    | 5       |
| <b>Ethernet Retry Timer</b>   | 0                    | 1       |
| <b>Dialing Mode</b>   | Wait for transaction |         |
| <input checked="" type="checkbox"/> <b>Allow Terminal Program Downloads</b> |                      |         |

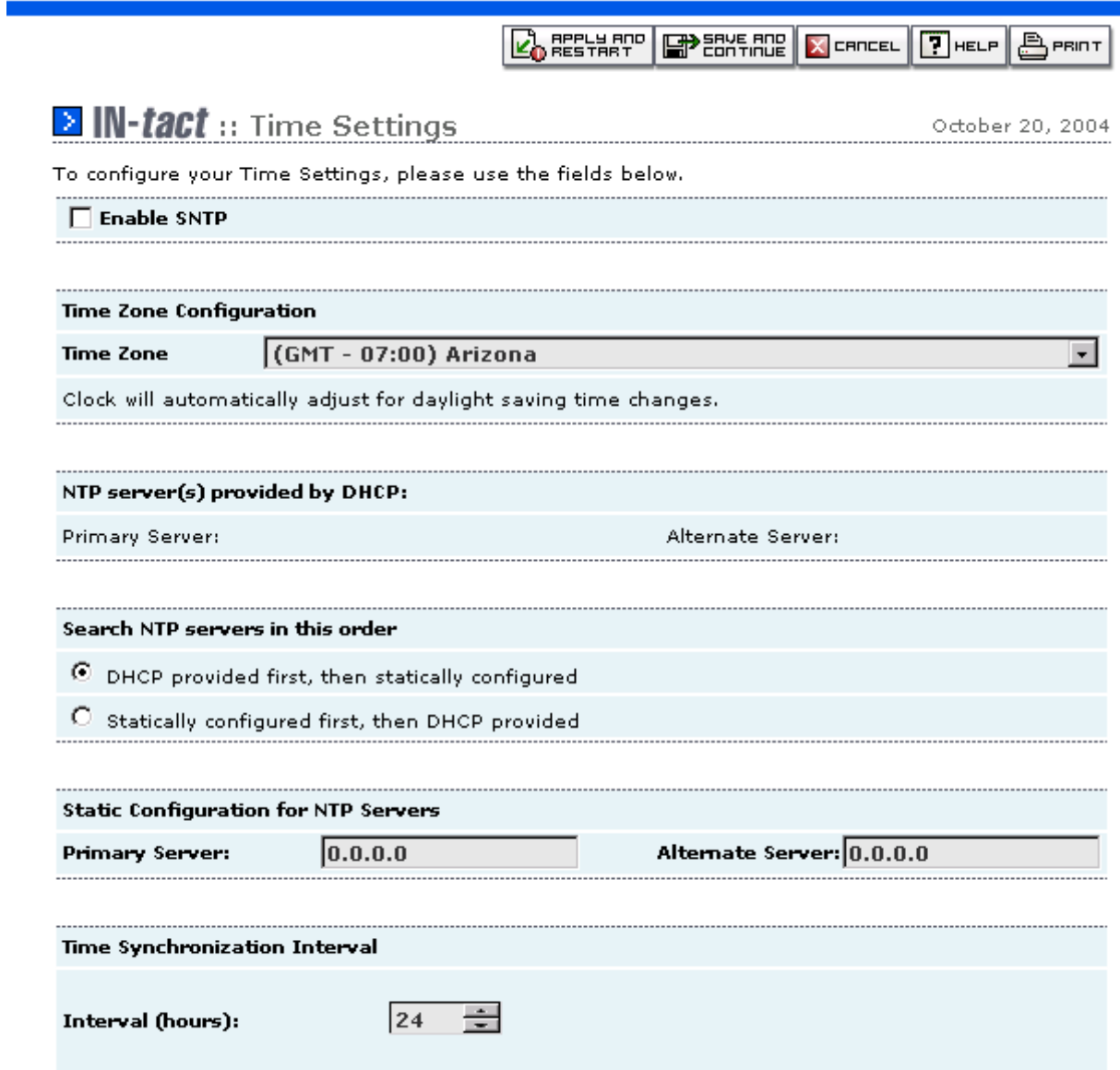
This screen allows you to set several advanced options associated with the dial backup feature. You can specify how long the modem will stay connected with no activity and how often the IN-tact 1101 checks to see if the Ethernet connection has been re-established. You can also control whether dial backup is established immediately upon Ethernet outage or only when a transaction is present from one of the terminals and needs to be processed. Finally, you can control whether or not terminal downloads are accepted while operating in dial backup mode. Because terminal downloads can be lengthy over a modem, you may prefer to allow these only when connected via Ethernet.

| Field/Button                     | Description   |
|----------------------------------|---|
| Inactivity Disconnect Timer      | Use the <b>Hours</b> and <b>Minutes</b> fields to specify the amount of time you would like the IN- <i>tact</i> 1101 to hold the modem connection open after the last transaction was processed. The modem will automatically disconnect after the time you specify here transpires. By default, this is set to five minutes. The valid range of entries is between zero minutes and 24 hours. Setting this value to zero disables the timer and the modem will stay indefinitely connected, regardless of the status of the Ethernet connection. You will have to manually disconnect the modem in this case. The value of Inactivity Disconnect Timer (if not set to zero) must be greater than that of Ethernet Retry Timer. |
| Ethernet Retry Timer             | Use the Hours and Minutes fields to set how often the IN- <i>tact</i> 1101 should retry the Ethernet connection while operating in dial backup mode. If the Ethernet connection has been re-established, the IN- <i>tact</i> 1101 closes the modem connection and reverts to normal IP-based transaction processing as soon as the Inactivity Disconnect Timer expires. By default, the IN- <i>tact</i> 1101 rechecks the Ethernet connection every minute. The valid range of entries is between 1 and 1439 minutes.   |
| Dialing Mode                     | Use the drop-down list to select whether the IN- <i>tact</i> 1101 begins establishing a modem connection immediately upon Ethernet outage, or waits until a transaction has been generated (default).   |
| Allow Terminal Program Downloads | Click this checkbox to enable terminal program downloads while operating in dial backup mode. By default, this option is enabled. However, because terminal downloads can take some time to complete, you may not want them to occur during dial sessions, only via IP sessions.  |

**NOTE:** Click **Back**, **Save and Continue** or **Apply and Restart** as appropriate. Keep in mind that your changes are not written to persistent memory until you click **Apply and Restart**.

## Time Settings Screen

On the navigation tree, click **IN-tact Setup > System Setup > Time**. The Time Settings Screen appears:



**IN-tact :: Time Settings** October 20, 2004

To configure your Time Settings, please use the fields below.

**Enable SNTP**

---

**Time Zone Configuration**

**Time Zone** (GMT - 07:00) Arizona

Clock will automatically adjust for daylight saving time changes.

---

**NTP server(s) provided by DHCP:**

Primary Server: Alternate Server:

---

**Search NTP servers in this order**

DHCP provided first, then statically configured

Statically configured first, then DHCP provided

---

**Static Configuration for NTP Servers**

**Primary Server:** 0.0.0.0 **Alternate Server:** 0.0.0.0

---

**Time Synchronization Interval**

**Interval (hours):** 24

Use this screen to enable and configure SNTP timekeeping on the IN-tact 1101. If enabled, you will not be able to set system time for the device on the Set System Time screen. Instead, the IN-tact 1101 will keep time according to an NTP server.

| Field/Button                         | Description   |
|--------------------------------------|---|
| Enable SNTP                          | Click this checkbox to enable SNTP, the device will automatically obtain current time from a SNTP server on the network. You must <b>Apply</b> and <b>Restart</b> before this change will become effective. SNTP is disabled by default.  |
| Time Zone Configuration              |   |
| Time Zone                            | Use this panel to select the time zone where the IN-tact 1101 is located. This is necessary for the device to correctly calculate local time based on the UTC time received from NTP server(s). Daylight saving time is automatically calculated based on your time zone choice. The default time zone is Arizona (GMT - 07:00).  |
| NTP server(s) provided by DHCP       | If DHCP is enabled and the IN-tact 1101 obtained NTP server information from it, the first two NTP servers are displayed here and are available for time synchronization.   |
| Search NTP servers in this order     | Use this panel to define the preferred search order for NTP servers. Servers are contacted in the order you select. The default search order is DHCP first, then statically-configured.<br><br>There are two choices: <ul style="list-style-type: none"> <li>• Try to connect to DHCP provided NTP servers first, then statically-configured servers.</li> <li>• Try to connect to statically-configured servers first, then DHCP provided servers.</li> </ul>  |
| Static Configuration for NTP Servers | You have the option of configuring up to two NTP servers -- a primary and an alternate. The value entered can be an IP address or a domain name.  |
| Time Synchronization Interval        |   |
| Interval (hours)                     | Time is synchronized on start-up, then periodically according to the interval configured you specify in this panel. The interval is specified in hours, from 1 through 24, with 24 being the default. Time synchronization can be requested whenever necessary by clicking <b>Synchronize Now</b> . This button is only present if you have enabled SNTP and restarted the device. A message displays to inform you that the time synchronization process can take up to 40 seconds as a valid NTP server is contacted. The result (failure or success) is displayed on this page. An SNMP trap is generated when start-up time synchronization fails. After that, a failed synchronization attempt generates an event with no SNMP trap. If successful, the new time is also displayed. A successful manual synchronization resets the synchronization interval. In other words, the countdown until next synchronization is reset to zero at the time you click <b>Synchronize Now</b> . If you are using a SNMP manager to set time synchronization, set your SNMP manager timeout to be at least 45 seconds to allow adequate time for this operation to take place. Time will be synchronized with the first server that successfully responds to the request. An event is recorded stating that time has been successfully synchronized, including the IP address of the NTP server that responded to the time request. |

**NOTE:** Click **Save and Continue** or **Apply** and **Restart** as appropriate. Keep in mind that your changes are not written to persistent memory until you click **Apply and Restart**.

### Terminal Port Settings Screen

On the navigation tree, click **IN-tact Setup > Application Setup > Terminal Port**. The Terminal Port Settings screen appears:

**HLAN Speed** 19200 BPS

| Enabled                             | Description     | CU Address | Enabled                  | Description | CU Address |
|-------------------------------------|-----------------|------------|--------------------------|-------------|------------|
| <input checked="" type="checkbox"/> | Front Counter 1 | 30         | <input type="checkbox"/> |             | 38         |
| <input checked="" type="checkbox"/> | Front Counter 2 | 31         | <input type="checkbox"/> |             | 39         |
| <input checked="" type="checkbox"/> | Drive-thru      | 32         | <input type="checkbox"/> |             | 3A         |
| <input type="checkbox"/>            |                 | 33         | <input type="checkbox"/> |             | 3B         |
| <input type="checkbox"/>            |                 | 34         | <input type="checkbox"/> |             | 3C         |
| <input type="checkbox"/>            |                 | 35         | <input type="checkbox"/> |             | 3D         |
| <input type="checkbox"/>            |                 | 36         | <input type="checkbox"/> |             | 3E         |
| <input type="checkbox"/>            |                 | 37         | <input type="checkbox"/> |             | 3F         |

Use this screen to set the communication parameters for connection to your HLAN terminal network. Your settings here should match the configuration of your terminal network. You are required to configure at least one terminal for the IN-tact 1101 to be operational. You cannot permanently save the configuration until you do so.

| Field/Button | Description  |
|--------------|--|
| HLAN Speed   | Use the drop-down list to select either 19200bps (default) or 4800 bps. The speed selected should match speed set in the terminals.  |
| Enabled      | By default, all terminal addresses are disabled. Use this series of checkboxes to enable any terminal address not being used. You can also use this feature to temporarily disable a terminal that is not responding to poll if it is affecting network performance. |
| Description  | Type a brief text description of each terminal on the HLAN network, such as "Register 1", "Drive-thru", etc. 32 characters are accepted.   |
| CU Address   | A listing of valid HLAN polling addresses. Make certain that the Enabled checkbox is selected and there is a description for each terminal address in use at this location. All unused addresses should be disabled so they are not polled.                          |

**NOTE:** Click **Save and Continue** or **Apply and Restart** as appropriate. Keep in mind that your changes are not written to persistent memory until you click **Apply and Restart**.



## Host Port Settings Screen

On the navigation tree, click **IN-tact Setup > Application Setup > Host Port**. The Host Port Settings screen appears:

October 20, 2004

To configure your Host Port Settings, please use the fields below.

| NII | Description     | Enabled                             | Connection Type |         |
|-----|-----------------|-------------------------------------|-----------------|---------|
| 021 | Acme Processing | <input checked="" type="checkbox"/> | Standard        | Edit... |
| 016 | PaymentMaster   | <input checked="" type="checkbox"/> | HTTP            | Edit... |
| 001 |                 | <input type="checkbox"/>            | Standard        | Edit... |
| 001 |                 | <input type="checkbox"/>            | Standard        | Edit... |
| 001 |                 | <input type="checkbox"/>            | Standard        | Edit... |
| 001 |                 | <input type="checkbox"/>            | Standard        | Edit... |
| 001 |                 | <input type="checkbox"/>            | Standard        | Edit... |
| 001 |                 | <input type="checkbox"/>            | Standard        | Edit... |

This is the first of three screens used to set up host processors. This screen consists of several fields that allow you to configure basic information for each of your host processing functions. Each row represents a unique NII for routing to a specific host function. For example, this could be card approval transactions or other functions like electronics receipt capture or biometrics. Up to eight different NIIs can be configured (some may be different functions provided by the same IP address). However, only the hosts to which the terminals will actually be forwarding information need to be defined.

When you have entered the information as described below, click **Edit** at the end of the row to display the second screen and complete addressing information for that processor. The next screen that appears depends on the connection type. There are different screens for Standard and HTTP.

The third screen displays when you click **Edit** on the second screen and allows you to define options for permanent or on-demand connection types.

To configure a new processor:

1. Enter the National Information Infrastructure (NII) destination of the processor. This is normally matched in the terminal configuration and must be a unique value. You cannot configure two host processors with the same NII value.
2. Enter a text description of the processor or function being performed, up to 32 characters.
3. Use the Enabled checkbox to enable or disable transaction routing to this processor. By default, all entries are disabled. You can use this checkbox to temporarily suspend

transactions to a processor for troubleshooting purposes or other reasons. All IP addressing information remains intact. When you are ready to resume sending transactions to a processor you have disabled, click Enabled to resume normal operation.







- There are three Connection Types - Standard, HTTP, and Merchant Link. Use the drop-down list to choose the appropriate type for this host processor, then click **Edit** at the end of the row.

**NOTE:** Click **Save and Continue** or **Apply and Restart** as appropriate. Keep in mind that your changes are not written to persistent memory until you click **Apply and Restart**. Any changes made on this screen are temporarily saved when you click **Edit** to access the next screen. You must still use **Apply and Restart** in order to write the changes to persistent memory.

### Standard Host Settings Screen

(Used when configuring connections not requiring HTTP protocol)

On the navigation tree, click **IN-tact Setup > Application Setup > Host Port**. Select **Standard** connection type and click **Edit**.

IN-tact :: Standard Host Settings

July 29, 2004

To configure your Standard Host Settings, please use the fields below.

|  |                        |
|--|------------------------|
| <b>NII</b>                                 | <b>021</b>             |
| <b>Description</b>                         | <b>Acme Processing</b> |
| <b>Connection Mode</b>                     | Permanent ▾            |
| <input type="checkbox"/> <b>Enable SSL</b> |                        |
| <b>Primary Host Address</b>                | 114.206.100.10         |
| <b>Primary Port</b>                        | 4096                   |
| <b>Alternate Host Address</b>              | 222.164.113.20         |
| <b>Alternate Port</b>                      | 4096                   |

The IN-tact 1101 uses the addressing information entered here to route transactions to the appropriate destination. Both a primary and alternate IP address can be configured for each host processing function. Contact the host processor to obtain the correct IP and port address for routing if unknown.

| Field/Button         | Description  |
|----------------------|--|
| NII                  | This is the NII routing code entered for this processor on the Host Port Settings screen. It is provided as a reminder of which processor you are currently working with.  |
| Description          | This is the description (or name) entered for this processor on the Host Port Settings screen. It is provided as a reminder of which processor you are currently working with.   |
| Connection Mode      | Select either Permanent or On Demand from the drop-down list. A permanent connection is "always on", while On Demand establishes a host connection only when there is a transaction present to process. Further options for the connection type can be defined by clicking the Edit button. The options that display depend on the connection type selected. |
| Enable SSL           | Use this checkbox to enable Secure Socket Layer (SSL) if the host requires this type of encryption.  |
| Primary IP Address   | Enter the primary IP address or URL of the processor.  |
| Primary TCP Port     | Enter the primary port address of the processor.   |
| Alternate IP Address | Enter the alternate IP address or URL of the processor. This is only used if the primary IP address cannot be reached.   |
| Alternate TCP Port   | Enter the alternate port address of the processor.   |

**NOTE:** Click **Back**, **Save and Continue** or **Apply and Restart** as appropriate. Keep in mind that your changes are not written to persistent memory until you click **Apply and Restart**. Any changes made on this screen are temporarily saved when you click **Edit** to access the next screen. You must still use **Apply and Restart** in order to write the changes to persistent memory.

## Permanent Mode Settings

(Used when configuring connections requiring a permanent connection mode)

On the navigation tree, click **IN-tact Setup > Application Setup > Host Port**. Click **Edit**, then select a permanent connection type. Click **Edit** again.

**IN-tact :: Permanent Mode Settings** October 20, 2004

To configure your Permanent Mode Settings, please use the fields below.

|  |                        |
|--|------------------------|
| <b>NII</b>   | <b>021</b>             |
| <b>Description</b>   | <b>Acme Processing</b> |
| <input type="checkbox"/> <b>Include length field in length calculation</b> |                        |

This screen provides an option for how transaction headers are handled for permanent connection types. The Hypercom POS LAN Header and TPDU are required for permanent connections. The only option is whether or not the length field should be included as part of the length calculation. Contact the host processor to obtain the correct settings for this option if unknown.







| Field/Button                               | Description  |
|--|--|
| NII  | This is the NII routing code entered for this processor on the Host Port Settings screen. It is provided as a reminder of which processor you are currently working with.  |
| Description                                | This is the description (or name) entered for this processor on the Host Port Settings screen. It is provided as a reminder of which processor you are currently working with.   |
| Include Length Field in Length Calculation | The first two bytes of the POS LAN header are a length indicator. This option determines whether or not these first two bytes are included as part of the length calculation. This option should be set to match host processor configuration. |

Click **Back**, **Save and Continue** or **Apply and Restart** as appropriate. Keep in mind that your changes are not written to persistent memory until you click **Apply and Restart**. Any changes made on this screen are temporarily saved when you click **Edit** to access the next screen. You must still use **Apply and Restart** in order to write the changes to persistent memory.

## On Demand Mode Settings

(Used when configuring connections requiring a on demand connection mode)

On the navigation tree, click **IN-tact Setup > Application Setup > Host Port**. Click **Edit**, then select an on-demand connection type. Click **Edit** again.

IN-tact :: On Demand Mode Settings
October 20, 2004

To configure your On Demand Mode Settings, please use the fields below.

|  |                        |
|--|------------------------|
| <b>NII</b>   | <b>021</b>             |
| <b>Description</b>   | <b>Acme Processing</b> |
| <input type="checkbox"/> <b>Include Two-byte Message Length Header</b>     |                        |
| <input type="checkbox"/> <b>Include length field in length calculation</b> |                        |
| <input type="checkbox"/> <b>Include TPDU</b>                               |                        |
| <input type="checkbox"/> <b>Use STX/ETX Wrapper</b>                        |                        |
| <input type="checkbox"/> <b>Discard ACKs</b>                               |                        |

This screen allows you to further define options for an on demand connection type. Options include how transaction headers and certain protocol settings are handled by the IN-tact. You may need to change these settings for hosts that use different framing or protocol options. Contact the host processor to obtain the correct settings for these options if unknown.

| Field/Button                               | Description   |
|--|---|
| NII  | This is the NII routing code entered for this processor on the Host Port Settings screen. It is provided as a reminder of which processor you are currently working with.   |
| Description                                | This is the description (or name) entered for this processor on the Host Port Settings screen. It is provided as a reminder of which processor you are currently working with.  |
| Include Two-byte Message Length Header     | Use this checkbox to include a two-byte message length indicator if required for this host connection. This option is disabled by default. The two options below allow further control of the header and should be enabled or disabled according to how the host processor is configured. |
| Include Length Field in Length Calculation | As mentioned above, the first two bytes of the POS LAN header are a length indicator. This option determines whether or not these first two bytes are included as part of the length calculation. This option should be set to match host processor configuration.                        |
| Include TPDU                               | The TPDU is the next five bytes of the POS LAN Header and includes information used for routing purposes. This option determines whether or not these five bytes are included as part of the header. This option should be set to match host processor configuration.                     |







| Field/Button        | Description  |
|---------------------|--|
| Use STX/ETX Wrapper | Use this checkbox to enable Start of Text (STX) and End of Text (ETX) wrappers if required by the host. This option is used primarily for hosts that don't run Visa protocol, but want to use async framing. |
| Discard ACKs        | Use this checkbox to discard any ACKs sent by the terminals, rather than sending them to the host. This option is used primarily for hosts that don't run Visa protocol, but want to use async framing.      |

Click **Back**, **Save and Continue** or **Apply and Restart** as appropriate. Keep in mind that your changes are not written to persistent memory until you click **Apply and Restart**. Any changes made on this screen are temporarily saved when you click **Edit** to access the next screen. You must still use **Apply and Restart** in order to write the changes to persistent memory.

## HTTP Host Settings Screen

(Used when configuring connections requiring HTTP protocol)

On the navigation tree, click **IN-tact Setup > Application Setup > Host Port**. Select **HTTP Connection Type** and click **Edit**.

IN-tact :: HTTP Host Settings
 October 20, 2004

To configure your HTTP Host Settings, please use the fields below.

|  |                      |
|--|----------------------|
| <b>NII</b>   | <b>016</b>           |
| <b>Description</b>   | <b>PaymentMaster</b> |
| <input checked="" type="checkbox"/> <b>Enable SSL</b>                      |                      |
| <input type="checkbox"/> <b>Include Two-byte Message Length Header</b>     |                      |
| <input type="checkbox"/> <b>Include length field in length calculation</b> |                      |
| <input type="checkbox"/> <b>Include TPDU</b>                               |                      |
| <input type="checkbox"/> <b>Use STX/ETX Wrapper</b>                        |                      |
| <input type="checkbox"/> <b>Discard ACKs</b>                               |                      |
| <b>Primary Host Address</b>  | 192.224.80.120       |
| <b>Primary Port</b>  | 4096                 |
| <b>Alternate Host Address</b>  | 224.424.100.60       |
| <b>Alternate Port</b>  | 4096                 |

The IN-tact 1101 uses the addressing information entered here to route transactions to the appropriate destination. Both a primary and alternate IP address or URL can be configured for each host processing function. Contact the host processor to obtain the correct IP and port address for routing if unknown.

| Field/Button                           | Description  |
|--|--|
| NII                                    | This is the NII routing code entered for this processor on the Host Port Settings screen. It is provided as a reminder of which processor you are currently working with.  |
| Description                            | This is the description (or name) entered for this processor on the Host Port Settings screen. It is provided as a reminder of which processor you are currently working with.   |
| Enable SSL                             | Use this checkbox to enable Secure Socket Layer (SSL) if the host requires this type of encryption.  |
| Include Two-byte Message Length Header | Use this checkbox to enable Hypercom's proprietary POS LAN header if required for this host connection. This option is disabled by default. The two options below allow further control of the header and should be enabled or disabled according to how the host processor is configured. |

| Field/Button                               | Description   |
|--|---|
| Include Length Field in Length Calculation | As mentioned above, the first two bytes of the POS LAN header are a length indicator. This option determines whether or not these first two bytes are included as part of the length calculation. This option should be set to match host processor configuration.    |
| Include TPDU                               | The TPDU is the next five bytes of the POS LAN Header and includes information used for routing purposes. This option determines whether or not these five bytes are included as part of the header. This option should be set to match host processor configuration. |
| Use STX/ETX Wrapper                        | Use this checkbox to enable Start of Text (STX) and End of Text (ETX) wrappers if required by the host. This option is used primarily for hosts that don't run Visa protocol, but want to use async framing.  |
| Discard ACKs                               | Use this checkbox to discard any ACKs sent by the terminals, rather than sending them to the host. This option is used primarily for hosts that don't run Visa protocol, but want to use async framing.   |
| Primary Host Address                       | Enter the primary IP address or URL of the processor. Up to 2048 characters can be entered in this field.   |
| Primary Port                               | Enter the primary port address of the processor.  |
| Alternate Host Address                     | Enter the alternate IP address or URL of the processor. Up to 2048 characters can be entered in this field. This is only used if the primary IP address cannot be reached.  |
| Alternate Port                             | Enter the alternate port address of the processor.  |

**NOTE:** Industry standard use of HTTP protocol limits its association to single request/response types of transactions, such as POS credit and debit authorizations. If you require support for multiple and batch-type transactions, you should determine the availability of extended support within the HTTP host server gateway before configuring the IN-*tact* to use HTTP protocol.

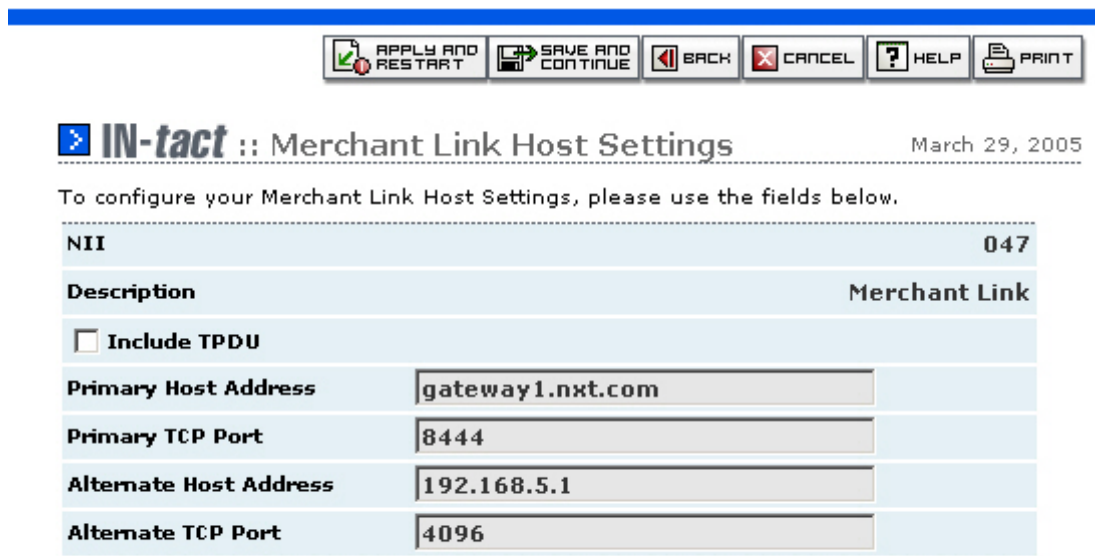
Click **Back**, **Save and Continue** or **Apply and Restart** as appropriate. Keep in mind that your changes are not written to persistent memory until you click **Apply and Restart**.



## Merchant Link Host Settings Screen

(Used when configuring connections that require a Merchant Link gateway)

On the navigation tree, click **IN-tact Setup > Application Setup > Host Port**. Select **Merchant Link** connection type and click **Edit**.



**IN-tact :: Merchant Link Host Settings** March 29, 2005

To configure your Merchant Link Host Settings, please use the fields below.

|  |                      |
|--|----------------------|
| <b>NII</b>                                   | <b>047</b>           |
| <b>Description</b>                           | <b>Merchant Link</b> |
| <input type="checkbox"/> <b>Include TPDU</b> |                      |
| <b>Primary Host Address</b>                  | gateway1.nxt.com     |
| <b>Primary TCP Port</b>                      | 8444                 |
| <b>Alternate Host Address</b>                | 192.168.5.1          |
| <b>Alternate TCP Port</b>                    | 4096                 |

The IN-tact 1101 uses the addressing information entered here to route transactions to the appropriate destination. Both a primary and alternate IP address or URL can be configured for each host processing function. Contact the host processor to obtain the correct IP and port address for routing if unknown.

| Field/Button           | Description  |
|------------------------|--|
| NII                    | This is the NII routing code entered for this processor on the Host Port Settings screen. It is provided as a reminder of which processor you are currently working with.  |
| Description            | This is the description (or name) entered for this processor on the Host Port Settings screen. It is provided as a reminder of which processor you are currently working with.   |
| Include TPDU           | The TPDU is five bytes of the POS LAN Header and includes information used for routing purposes. This option determines whether or not these five bytes are included as part of the header. This option should be set to match host processor configuration. |
| Primary Host Address   | Enter the primary IP address or URL of the processor. Up to 2048 characters can be entered in this field.  |
| Primary TCP Port       | Enter the primary TCP port address of the processor.   |
| Alternate Host Address | Enter the alternate IP address or URL of the processor. Up to 2048 characters can be entered in this field. This is only used if the primary IP address cannot be reached.   |
| Alternate TCP Port     | Enter the alternate TCP port address of the processor.   |

Click **Back**, **Save and Continue** or **Apply and Restart** as appropriate. Keep in mind that your changes are not written to persistent memory until you click **Apply and Restart**.

### Transaction Settings Screen

On the navigation tree, click **IN-tact Setup > Application Setup > Transaction Processing**. The Transaction Settings screen appears:

This screen is used to define various parameters the IN-tact 1101 uses to route transactions and communicate with host processors.

| Field/Button                    | Description  |
|---------------------------------|--|
| Default NII                     | Enter the value of the NII to be used for default transaction routing. The value you enter here must match one of the hosts defined on the Host Port Settings screen or you will not be allowed to permanently save the configuration.   |
| Routing Mode for Known NIIs     | Use the drop-down list to select whether transactions are routed to the host based upon the NII embedded within the transaction, or are routed to the default NII specified above. <b>Note:</b> Selecting the "Route to default NII" option will route <b>all</b> transactions to the default NII, regardless of other settings. |
| Routing Mode for Unknown NIIs   | Use the drop-down list to select whether unknown NIIs are routed to the default NII specified above, or are simply discarded when using embedded NII routing mode. Only applies to embedded NII, does not apply to default NII routing.  |
| Send Initialization Requests to | Use the drop-down list to select whether initialization requests are sent to the host, or instead sent to Term-Master.   |
| Recognize Processing Code 92 As | Use the drop-down list to select whether you want code 92 to be recognized as an initialization request or treated as a transaction.   |
| Recognize Processing Code 94 As | Use the drop-down list to select whether you want code 94 to be recognized as an initialization request or treated as a transaction.   |

**NOTE:** Click **Save and Continue** or **Apply and Restart** as appropriate. Keep in mind that your changes are not written to persistent memory until you click **Apply and Restart**.

---

## Chapter 4: Control Panel

---

### Overview

Each of the Control Panel screens and functions are explained in detail in this section.



As the name suggests, Control Panel functions allow you to control certain IN-*tact* 1101 operations. The screens within the Control Panel port of the navigation tree are:

- **File Management** — Used to perform firmware upgrades and exports, load and export saved configurations, and manage SSL certificates
- **System Operations** — Used to restart the device, restore the previous configuration, reset the device to factory defaults, and set HLAN installation mode
- **Set System Time** — Used to set the year, month, day, hour, and minute. Time on the IN-*tact* 1101 is only valid while the device is powered on and operating. There is no battery-powered timekeeping. In other words, if you power off or reset the device, time will have to be reset in order to be current. Time can be set via a SNTP server on your network, or set manually.
- **Clear Statistics** — A single button on this screen allows you to clear all statistical information captured by the device and start collecting fresh statistical information.
- **Dial Backup** — Allows you to manually establish or disconnect a dial link.

## File Management Functions

On the navigation tree, click **Control Panel > File Management**. The File Management Functions screen appears:

**?** HELP **PRINT**

**IN-tact** :: File Management Functions January 4, 2005

To access your file management functions, please use the fields below.

|   |                            |           |
|---|----------------------------|-----------|
| <b>Load Firmware</b>                              | <input type="text"/>       | Browse... |
|   |                            | Load      |
| <b>Export Firmware To PC</b>                      |                            |           |
|   |                            | Export    |
| <b>Load Configuration To IN-tact</b>              | <input type="text"/>       | Browse... |
|   |                            | Load      |
| <b>Export Configuration To PC</b>                 |                            |           |
|   |                            | Export    |
| <b>Load SSL Server Certificate To IN-tact</b>     | <input type="text"/>       | Browse... |
|   |                            | Load      |
| <b>Delete SSL Server Certificate From IN-tact</b> | No SSL certificates loaded |           |
| <b>Load SSL Client Key To IN-tact</b>             | <input type="text"/>       | Browse... |
| <b>SSL Client Key Password</b>                    | <input type="text"/>       |           |
|   |                            | Load      |

This screen is used to import and export files to/from the IN-tact 1101. This includes upgraded firmware, configuration files, and SSL certificates.

## Loading Firmware

Use this procedure to load and upgrade firmware for the IN-*tact* 1101. This process interrupts normal operations. The IN-*tact* 1101 will automatically reset and load the new firmware once loading is complete.

To load firmware:

1. Download the upgraded firmware to your local machine. Contact Hypercom for further information on firmware upgrades.
2. On the File Management Functions screen, click **Browse** (next to the Load Firmware field) to view a listing of the available firmware.
3. Navigate to and select the firmware upgrade file, then click **Open**. The path and filename now appear in the Upgrade Firmware field.
4. Click **Load** to install the new firmware on your IN-*tact* 1101. The file is copied to a custom partition on the IN-*tact* 1101. During the load process, a pop-up message appears informing you that the loading is in progress to the device cannot be access during the loading process.

If there is an error during the upgrade, the message "Firmware upgrade failed" appears in red below the field. Check that you have a valid image file (.img) or get a new copy of the file from the Hypercom website in case the file on your local machine is corrupted.

If the upgrade is successful, the IN-*tact* 1101 restarts.

5. Log in to the IN-*tact* 1101 again.

## Exporting Firmware to a PC

This function allows you to save the custom image stored on the IN-*tact* 1101 to your local system. This is useful when you are preparing to upgrade and want to keep a copy of the image for backup purposes.

To export:

1. On the File Management Functions screen, click **Export** (next to the Export Firmware to PC field).

The firmware data is read directly from the custom partition in binary form and a temporary file is created.

2. Select a path on your local machine where the firmware image should be saved.
3. Click **OK**.

## Loading a Configuration to the IN-*tact* 1101

This function allows you to load a configuration file from your local machine to the IN-*tact* 1101. This is useful in situations where you may be configuring several units. Rather than having to configure all of the IN-*tact* 1101 settings for each unit, you can simply load a previously exported configuration file that has the correct settings, then make any minor adjustments as necessary.

To load a configuration the IN-*tact* 1101:

1. From the File Management Functions screen, click **Browse** (next to the Load Configuration to IN-*tact* field).
2. Navigate to and select the configuration file (.cfg extension).
3. Click **Open**.
4. Click **Load** to upload the file to the IN-*tact* 1101.

If an error occurs while loading the file, a message in red appears below the field.

If successful, a message appears while the configuration file is loaded. When finished, the IN-*tact* 1101 restarts.

5. Log in to the IN-*tact* 1101 again.

The old configuration file is saved as a backup configuration and the newly uploaded configuration file becomes the current configuration for the device.

**NOTE:** Only the items listed under IN-*tact* Setup are restored when a previous or imported configuration is loaded. Passwords and Event Log settings are not imported with a configuration and must be set on each individual device.

## Exporting a Configuration to a PC

This function allows you to save the current configuration stored on the IN-*tact* 1101 to your local machine.

To export a configuration to a PC:

1. From the File Management Functions screen, click **Export** (next to Export Configuration To PC).

The configuration file is prepared for download.

2. Select a path on your local machine in which to save the file.
3. Click **OK**.

The file can now be loaded to other IN-*tact* units as needed and modified, or simply kept as a backup.

## Loading SSL Server Certificates to the IN-*tact* 1101

This function allows you to upload a new SSL certificate file to the user partition of the IN-*tact* 1101. Multiple user-imported SSL certificates can be stored and active (up to 16). The SSL certificates are only used for secure transactions (financial data traffic), not for the web interface itself. The certificate immediately becomes active; you do not need to restart the device.

To load an SSL certificate:

1. Verify that the certificate is in PEM format. PEM-formatted certificates generally end with a PEM extension and are viewable in Notepad. A typical PEM certificate might appear as:

```
-----BEGIN CERTIFICATE-----
MIIDz2CCAgAwIBAgIBADANBgkqhkiG9w0BAQoFADBTMQswCQYDVQoGEwJVUzEQ
MA4GA1UECBMHQXJpem9uYTEQMA4GA1UEBxMHUghvZW5peDERMA8GA1UEChMISHlw
ZXJjb20xDTALBgNVBAAsTBE5vbmUwHhcNMDQwMzEyMjExMDM5WmcNMjYwMjA1MjEx
MDM5WjBTMQswCQYDVQoGEwJVUzEQMA4GA1UECBMHQXJpem9uYTEQMA4GA1UEBxMH
UGhvZW5peDERMA8GA1UEChMISHlwZXJjb20xDTALBgNVBAAsTBE5vbmUwggEiMA0G
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQc+jOaGep9N126J0czrdq/MTBYuNjW0
S8LZOGsWZn+g0SkAW2mXnGVKRiKGqgOjQWCS7Qhf46/x/XwjUPBLTlLmzMrq2v4
LZHmaC3TCulu7YDloS00429rQM92N2F6tXfytrqvBfZGEGOP3oYVnlyiZyhIpn
n2MPppitjdcRuWynubZkTvs8wN27PaqNA+0o8Qaq0Vvyc0o5HcuuSiTcBUZnrG0T3
6X/YQ+MOYjnU3DrN3D8clEDJVe1GtSfQ0uCBNUkvKmSlpW0aYWFYd+qTqRG8yqV7
9BTUkhPKSIzlrMEuq5YZlrXDnVZREhq0pj8bjGIGAbiYNR7uU8JacWfJAgMBAAGj
ga0wgaowHQYDVR0OBByEPE35+zPtBMS2UnM0Rj5SHE/WEKiCMHsGA1UdIwR0MHKA
FE35+zPtBMS2UnM0Rj5SHE/WEKiCoVekVTBTMQswCQYDVQoGEwJVUzEQMA4GA1UE
CBMHQXJpem9uYTEQMA4GA1UEBxMHUghvZW5peDERMA8GA1UEChMISHlwZXJjb20x
DTALBgNVBAAsTBE5vbmUwCAQAwDAYDVR0TBAAUwAwEB/zANBgkqhkiG9w0BAQoFAAO
AQEAeIF7jXvw2COABnTJmvEGgc0zQ8nOEERuul/SxIrgHjhzSedjTYbaQ2RqGRFW
EliG7VCJxAXf7dfxc/0Uyo/DKpRKNymH5Wu3V579pwIUXNJjqHsAJfI4p/oJudLd
997VX5DEPEiFlrv6Z31T4JrsXjey8BUJmqgxUsFehYB/etYxD4bezICBMB4TQ3ae
iL07Qqn1ifJboXqcntjHcYqHQXAfjlm4//HqKKJaqwFSp4iDMeNnFziQtmPn3K5U
LKZK06zQsyIqaVJI0gViOubSoVsBrfx/tj5oaePkzNz1GE6Te40X3A8rL+35WcgA
raca+309IwWjF83mQqQiKInf8w==
-----END CERTIFICATE-----
```

There may be other sections and other data within the file. If the certificate is not in PEM format, then it must first be converted using OpenSSL (a freely available software package on the Internet) before the *IN-tact* 1101 can use it.

2. Once the file is in PEM format, change the file name to the OpenSSL name. This name consists of an eight-character filename, which is the computer hash value in hexadecimal and the number zero is the filename extension. This can be determined with the following command in OpenSSL:

```
>> openssl x509 -hash -in mycert.pem -noout
```

The result will be an eight-character alphanumeric string, such as “557C3410”. The file must be renamed to add an extension of “.0”. In this case, the renamed file would be “557C3410.0”.

3. On the File Management Functions screen, click **Browse** (next to Load SSL Certificate to *IN-tact*).
4. Navigate to and select the SSL certificate and click **Open**.
5. Click **Load** to upload the certificate to the *IN-tact* 1101.

A red message appears if there is an error with this operation.

If the operation is successful, the certificate becomes active and the name of the file appears in this field. The certificate is now ready for use.

## Deleting an SSL Server Certificate from the IN-*tact* 1101

This function erases the selected SSL certificate file from the IN-*tact* 1101.

To delete an SSL certificate:

1. From the File Management Functions screen, select the stored certificate from the drop-down list (near the bottom of the screen).

**NOTE:** The drop-down list and the **Delete** button are available only when certificates are present in the system.

2. Click **Delete**.

The certificate is physically erased from persistent memory. However, the certificate remains usable by the system until you restart or reset the device.

## Load SSL Client Key to IN-*tact*

Use this function if you need to set up mutual authentication with a server. For mutual authentication, a reciprocal trust relationship must be established between the IN-*tact* and the server. The IN-*tact* must provide a client certificate containing its identity. The server must store a version of the certificate containing the client's identity and public key. This allows the server to trust the client during SSL mutual authentication.

You can load a single certificate and key combination on the IN-*tact*. This combination will be used for all SSL sessions that require mutual authentication. If the IN-*tact* is required to connect to two different hosts, each requiring mutual authentication, those two hosts must be able to accept the same certificate from the IN-*tact*.

Mutual authentication protects only transaction data, not configuration data.

Setting up the Client Key and SSL certificate on the IN-*tact* is a two-step process.

**Step 1** - Enter the path and name of (or use Browse to locate and select) the Client Key. Then, enter the password associated with the SSL client certificate in the SSL Client Key Password field. Click the **Load** button.

The certificate file is transferred to and loaded into the memory of the IN-*tact*. If the file cannot be read (because it is not in PEM format or because the password is invalid), an error is displayed on the web interface.

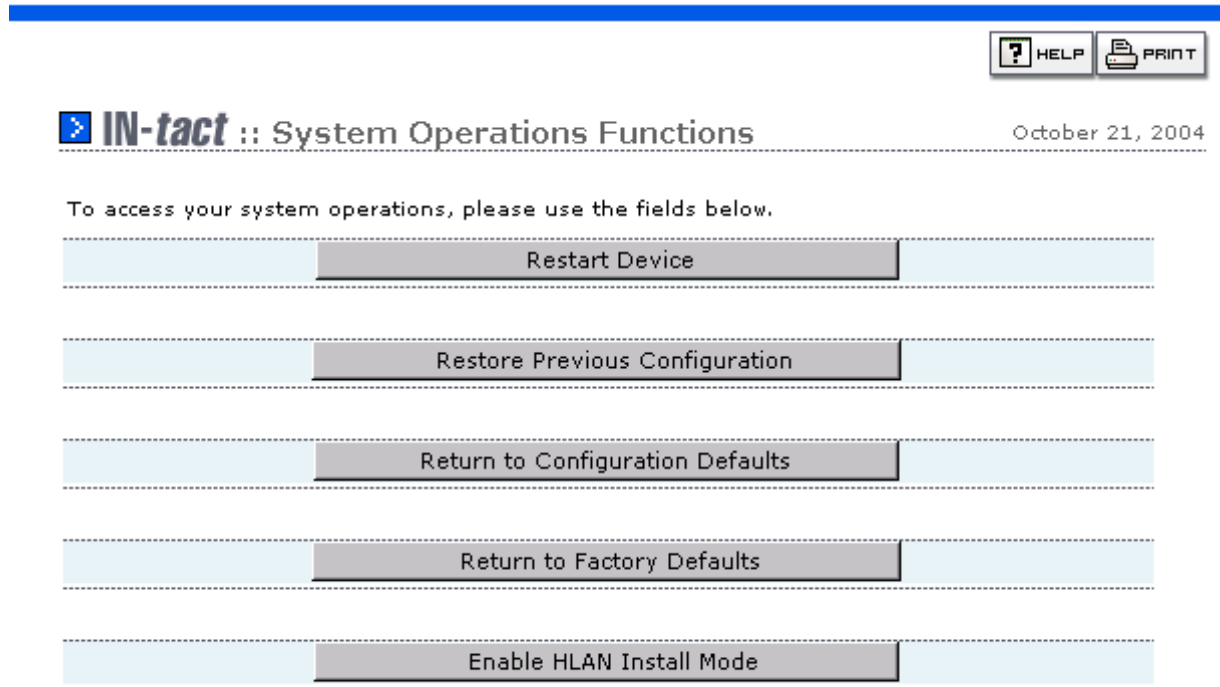
**Step 2** - After loading the Client Key, the File Management screen re-displays. You should now load the SSL certificate that matches the Client Key.

1. In the **Load SSL Client Certificate to IN-*tact*** field, click **Browse** to display a standard Browse dialog box.
2. Navigate to and select the SSL certificate, then click **Open**.
3. Click **Load** to upload the SSL client certificate to the IN-*tact* 1101. A red message displays under the field if there is an error with this operation.



## System Operations Screen

On the navigation tree, click **Control Panel > System Operations**. The System Operations screen appears:



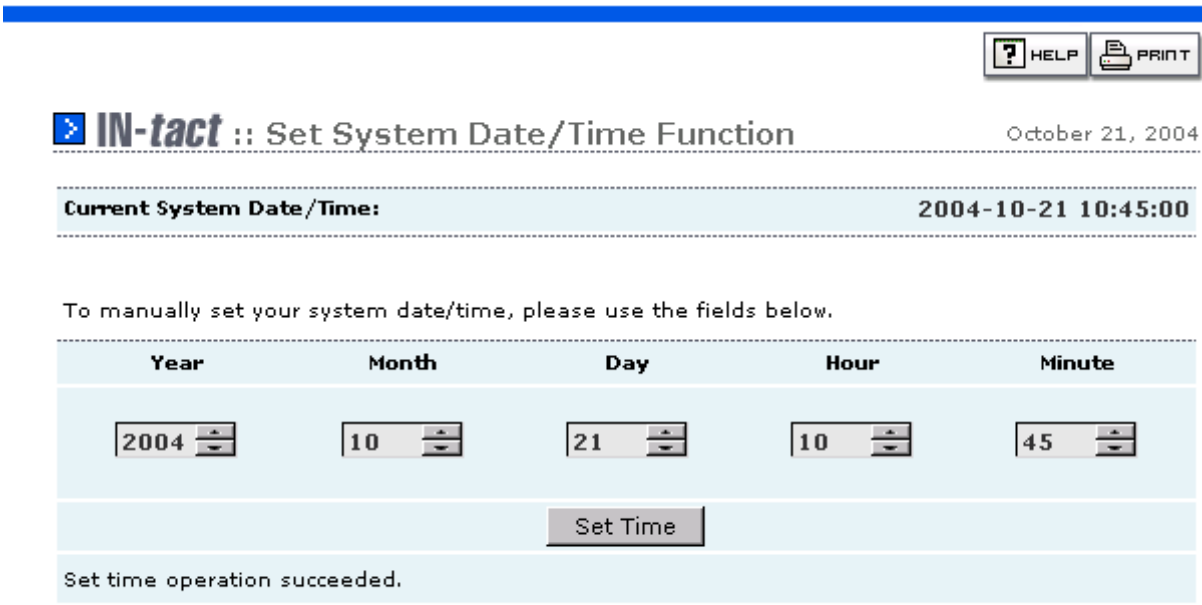
Use this screen to perform various reset functions on the IN-*tact* 1101.

| Field/Button                      | Description   |
|-----------------------------------|---|
| Restart Device                    | Click to perform a hardware reset of the IN- <i>tact</i> 1101. This is the same as a system reboot and causes the IN- <i>tact</i> 1101 to reload all configured information as if you powered off, then back on.  |
| Restore to Previous Configuration | Click to reload the last known configuration. The IN- <i>tact</i> 1101 maintains a copy of the last known configuration as a backup. If you have made configuration changes and something is not working correctly, click this button to reload the last known configuration.   |
| Return to Configuration Defaults  | Use this button to completely erase the current and backup configuration files. The IN- <i>tact</i> 1101 will then perform a restart. A new configuration file based on all of the default settings is built and used to load the unit.<br><br>This operation differs from "Revert to Factory Defaults" as no other files are affected. If you have upgraded firmware, it is untouched and still used. However, you will have to reset the password for the device. |

| Field/Button                | Description   |
|-----------------------------|---|
| Restore to Factory Defaults | <p>Click to erase the current configuration, any upgraded firmware, and restore all settings to those as shipped from the factory.</p> <p><b>WARNING:</b> Use the previous two options only as the last resort! Performing these operations erases all IP addresses and other information and the IN-<i>tact</i> unit will have to be completely reconfigured before it can process any transactions. If the unit is in a remote location, it may be necessary to return it to the deployment center for reconfiguration. Enable DHCP is restored as is the default IP address of 192.168.1.20.</p> |
| Enable HLAN Install Mode    | <p>This is an optional mode of operation used for installation testing of connected terminals prior to making connections to the host processor. It allows you to verify the integrity of your HLAN and terminals before sending any live transactions to the host. Installation mode should always be disabled before beginning normal operations.</p>   |

## Set Date/Time Screen

On the navigation tree, click **Control Panel > Set System Time**. The Set System Date/Time Function screen appears:



HELP PRINT

**IN-tact** :: Set System Date/Time Function October 21, 2004

**Current System Date/Time:** 2004-10-21 10:45:00

To manually set your system date/time, please use the fields below.

| Year | Month | Day | Hour | Minute |
|------|-------|-----|------|--------|
| 2004 | 10    | 21  | 10   | 45     |

Set Time

Set time operation succeeded.

It is important to accurately set the time for the IN-*tact* 1101. Because some diagnostic functions, like event logging, use a wrap-around buffer to capture information, you will not be able to tell when specific events have occurred without a time reference. This is also important for SSL functions; the certificates will not be authenticated correctly.

The IN-*tact* 1101 does not have a battery to maintain time when power is removed. Time is lost after a power reset. The device, however, does include a feature to synchronize time with pre-configured servers using Simple Network Time Protocol (SNTP). See the **System Setup > Time** screen to enable and configure the use of SNTP.

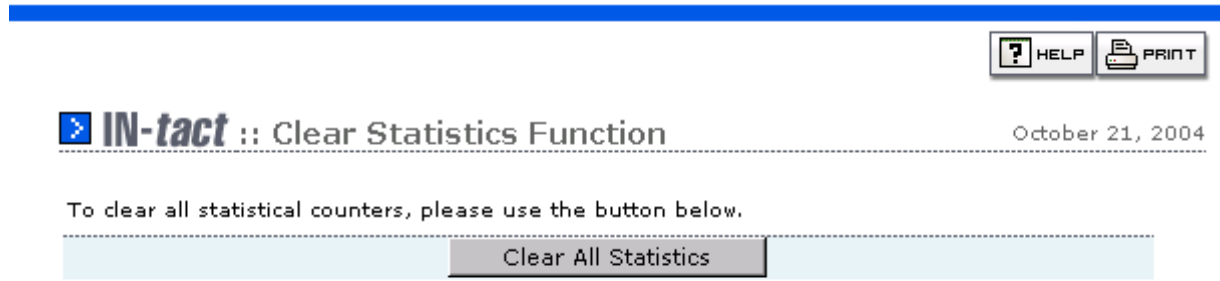
**Current Local Date/Time** - This is a reference that indicates what date and time the IN-*tact* 1101 currently has set.

- If SNTP is enabled, a message appears in red on this screen stating “SNTP time synchronization is enabled. Local time cannot be modified.” The fields normally available to set local time are disabled.
- If SNTP is disabled, the device defaults the date/time to the date of the current firmware build each time power is reset. The date and time fields will be available and can be set using the up/down arrows to the right of each field, or by simply typing your entry into each field. Click Set Time after entering the correct time. The message “Set time operation succeeded.” displays on the screen to acknowledge the new time settings.

**IMPORTANT** - If not using SNTP, time must be reset after any restart of the device. Time on the IN-*tact* 1101 is only valid while the device is powered on and operating. In other words, if you power off or reset the device, time will have to be reset in order to be current. The IN-*tact* 1101 defaults the date and time to the date of the firmware build whenever time is reset.

## Clear Statistics Screen

On the navigation tree, click **Control Panel > Clear Statistics**. The Clear Statistics Function screen appears:



Use this screen to permanently remove all current statistical data from the *IN-tact* 1101. This can be useful when troubleshooting problems and you wish to collect fresh statistical data. When you click **Clear All Statistics**, a confirmation message displays. Clicking **OK** causes all statistical data to be permanently removed. Clicking **Cancel** leaves all statistical data unchanged.

**NOTE:** Clearing statistics does not interrupt normal operations.

## Dial Backup

On the navigation tree, click **Control Panel > Dial Backup**. The Dial Backup Functions screen appears:

To manually dial the primary or the alternate host processor, please use the fields below.

|                 | Dial and Route Transactions Over Dial Link | Dial and Continue Routing Transactions Over Ethernet |
|-----------------|--|--|
| Primary (ATD)   | Dial                                       | Dial   |
| Alternate (ATD) | Dial                                       | Dial   |

To manually disconnect the established dial link, please use the button below.

Disconnect Dial

Dial backup operation is automatic when the IN-*tact* 1101 detects that transactions cannot be routed via the Ethernet port. However, you can also manually control dial backup operation using this screen. This can be useful for testing purposes, during planned outages for maintenance, or any other time you need to immediately control whether transactions are routed via IP or the modem. If you opt to manually begin dial operations, all of the timeout and trigger settings, such as the Inactivity Disconnect Timer (set on the Advanced Dial Backup Settings screen) are still in effect and will apply to dial operations.

| Field/Button  | Description  |
|---|--|
| Primary   | This is the dial string to reach the primary host processor. The dial string is set on the Dial Backup Settings screen.  |
| Dial and Route Transactions over Dial Link                | Click <b>Dial</b> to immediately dial the primary processor, establish connection, and begin routing transactions via the modem.<br><b>Note:</b> Invoking this causes web and SNMP traffic to use the modem.   |
| Dial and Continue Routing Transactions over Ethernet Link | Click <b>Dial</b> to immediately dial the primary/alternate host processor, but do not switch transaction routing from IP to modem. This is useful for testing purposes to make certain that the modem is working properly and connecting with the host processor specified in the primary/alternate dial string. If the Ethernet connection is lost while connected, transactions are automatically routed using the modem. |
| Alternate   | This is the dial string to reach the alternate host processor. The dial string is set on the Dial Backup Settings screen.  |

| Field/Button                               | Description  |
|--|--|
| Dial and Route Transactions over Dial Link | Click <b>Dial</b> to immediately dial the alternate processor, establish connection, and begin routing transactions via the modem.   |
| Disconnect Dial                            | Click to disconnect the modem from either the primary or alternate host processor as soon as possible. If you are connected to the IN- <i>tact</i> via PPP (rather than the Ethernet interface) and click this button, you will be disconnected.<br><br><b>Note:</b> If Disconnect Dial is clicked while in the middle of dialing and/or establishing a PPP connection, the processing of the disconnect is delayed until after the dialing and PPP establishment has completed. |

**NOTE:** Invoking the primary or alternate dial string causes web and SNMP traffic to use the modem. To maintain communication with the IN-*tact* 1101, your web browser or SNMP manager must be configured to use the IP address of the dial port on the IN-*tact* device.

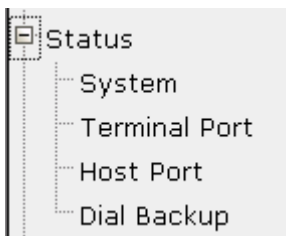
---

## Chapter 5: Status Functions

---

### Overview

Each of the IN-*tact* 1101 status functions are explained in detail in this section.



Status functions allow you to monitor IN-*tact* 1101 operations and view statistical information about transactions, response times, terminal activity, and uptime. This can be useful information when monitoring performance or when troubleshooting possible problems. The screens within the Status portion of the navigation tree are:

- **System** — “At a glance” information about the operational status of the system and terminals, as well as detailed product information, such as part numbers and firmware revisions
- **Terminal Port** — Detailed information about the terminals, including response time measurements
- **Host Port** — Detailed information about traffic to host processors, including the number of transactions routed to each NII
- **Dial Backup** — Detailed information about the current status, any errors, and traffic associated with the dial backup link.

## System Status Screen

On the navigation tree, click **Status > System**. The System Status screen appears:

| IN-tact :: System Status    |                       | October 21, 2004 |
|-----------------------------|-----------------------|------------------|
| <b>Current Status</b>       | OK                    |                  |
| <b>Current Mode</b>         | Normal                |                  |
| <b>System Time</b>          | 10:55:18 (10/21/2004) |                  |
| <b>Uptime</b>               | 1 days (00:15:00)     |                  |
| <b>Terminals Enabled</b>    | 3                     |                  |
| <b>Terminals Active</b>     | 0                     |                  |
| <b>Host Ports Enabled</b>   | 2                     |                  |
| Product Information         |                       |                  |
| <b>Product Part Number</b>  | 010300-002 2P         |                  |
| <b>Platform Part Number</b> | 010300-001 04         |                  |
| <b>Serial Number</b>        | 100004106687          |                  |
| <b>Hardware Part Number</b> | 030545-002 4P         |                  |
| <b>Firmware Name</b>        | IN-tact 1101          |                  |
| <b>Firmware Part Number</b> | 090256-003-A          |                  |
| <b>Build Date/Time</b>      | 2004-10-07 11:08:33   |                  |
| <b>Build Number</b>         | 6                     |                  |
| <b>File Size (bytes)</b>    | 1034086               |                  |




This screen is divided into two sections. The upper portion of the screen provides important “at a glance” information to help you quickly determine whether the IN-tact 1101 and its associated terminals are up and operating correctly. The lower portion of the screen provides reference information about the firmware currently loaded and running on IN-tact 1101. You can use this information to check against the Hypercom web site to see if a newer version of firmware is available. New firmware can be installed by using the File Management function in Control Panel. Click **Refresh** as needed to update the status information on the screen.




| Field/Button                         | Description   |
|--------------------------------------|---|
| Current IN- <i>tact</i> 1101 Status: |   |
| Current Status                       | There are two possible displays:<br><b>OK</b> : indicates that the device has been configured and is working correctly<br><b>Not Configured</b> : indicates that the IN- <i>tact</i> 1101 has not been properly configured. Go to System Setup and configure the device.  |
| Current Mode                         | Indicates whether the IN- <i>tact</i> 1101 is operating in "normal" mode or "install" mode.<br><br>Install mode is used to test terminal communications and should not be left on. Go to <b>Control Panel &gt; System Operations</b> to disable install mode if it is on. |
| System Time                          | Shows you the current time set for the IN- <i>tact</i> 1101.  |
| Uptime                               | Total time that the device has been powered on and operating.   |
| Terminals Enabled                    | Indicates the number of terminals configured. Terminals are configured on the Terminal Port Settings screen.  |
| Terminals Active                     | Indicates the number of configured terminals that are responding to poll and operating correctly. For more detailed information, see the Terminal Status screen.  |
| Host Ports Enabled                   | Indicates the number of host port connections that have been enabled.   |
| Product Information:                 |   |
| Product Part Number                  | Part number (the combination of hardware and software) of the IN- <i>tact</i> device  |
| Platform Part Number                 | Part number of the complete IN- <i>tact</i> 1101 without a firmware load  |
| Serial Number                        | Unique serial number of this IN- <i>tact</i> device   |
| Hardware Part Number                 | Part number of the base printed circuit board within the IN- <i>tact</i> 1101   |
| Firmware Name                        | Filename of the firmware currently loaded on the IN- <i>tact</i> 1101   |
| Firmware Part Number                 | Version of the firmware currently loaded on the IN- <i>tact</i> 1101  |
| Build Date/Time                      | When the firmware was compiled  |
| Build Number                         | Reference number assigned to the firmware   |
| File Size (bytes)                    | Actual size of the image file in bytes  |

## Terminal Port

On the navigation tree, click **Status > Terminal Port**. The Terminal Port Status screen appears:

 REFRESH
  HELP
  PRINT

 **IN-tact :: Terminal Port Status**

July 30, 2004

**Current Terminal Port Status**

| Address | Description     | Status | Msg In | Msg Out | RTM 0-2 | RTM 2-4 | RTM 4-6 | RTM 6+ |
|---------|-----------------|--------|--------|---------|---------|---------|---------|--------|
| 30      | Front Counter 1 | Active | 2345   | 2345    | 2344    | 1       | 0       | 0      |
| 31      | Front Counter 2 | Active | 1634   | 1633    | 1632    | 1       | 0       | 0      |
| 32      | Drive-thru      | Active | 8253   | 8253    | 8250    | 3       | 0       | 0      |

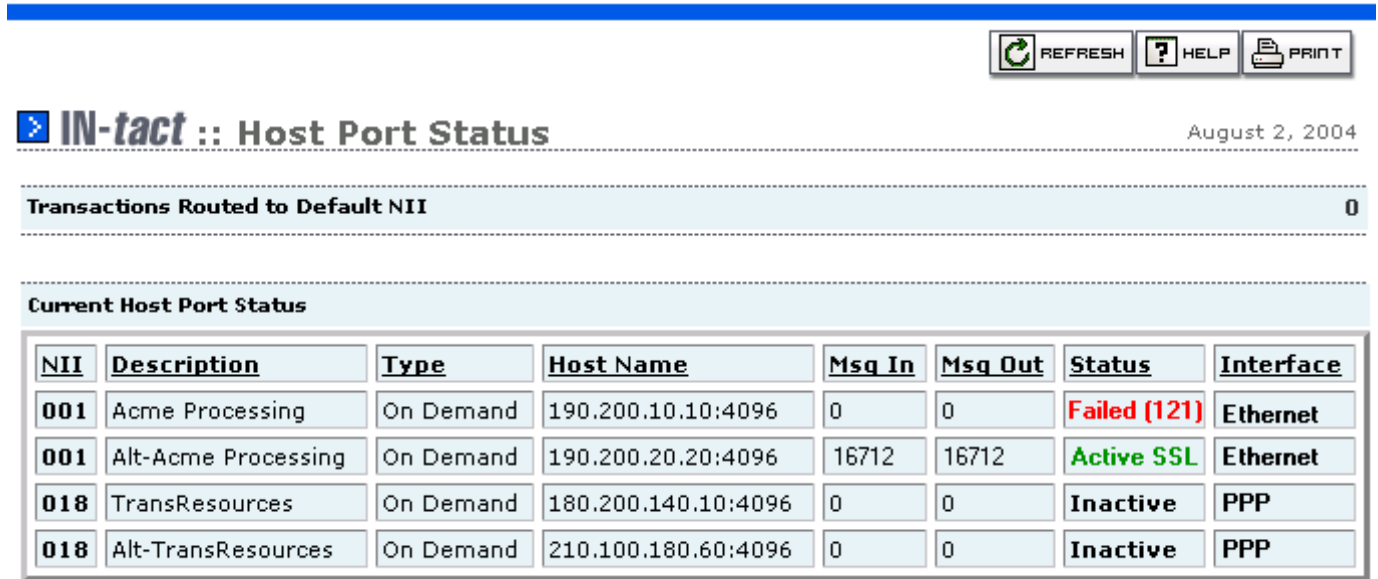
RTM : Response Time Measurement in seconds.

This screen provides a table that allows you to quickly analyze the status of all enabled terminals and see response time measurements (RTM). From these, you can determine what your average (or normal) response time is over a period of time. No configuration is done here; all terminal configuration is done on the Terminal Port Settings screen. You can click **Refresh** as needed to update the status displayed on this screen.

| Field/Button | Description   |
|--------------|---|
| Address      | Terminal's CU (or polling) address  |
| Description  | Description assigned in the Terminal Port Settings screen                     |
| Status       | Current status of the terminal, either Active, Idle, or No Response           |
| Msg In       | Total number of messages received by the IN-tact 1101 from the terminal       |
| Msg Out      | Total number of messages sent from the IN-tact 1101 to the terminal           |
| RTM 0-2      | Number of total transactions that were processed between zero and two seconds |
| RTM 2-4      | Number of total transactions that were processed between two and four seconds |
| RTM 4-6      | Number of total transactions that were processed between four and six seconds |
| RTM 6+       | Number of total transactions that processing took longer than six seconds.    |

## Host Port Status Screen

On the navigation tree, click **Status > Host Port**. The Host Port Status screen appears:



**Transactions Routed to Default NII** 0

**Current Host Port Status**

| NII | Description         | Type      | Host Name           | Msg In | Msg Out | Status       | Interface |
|-----|---------------------|-----------|---------------------|--------|---------|--------------|-----------|
| 001 | Acme Processing     | On Demand | 190.200.10.10:4096  | 0      | 0       | Failed (121) | Ethernet  |
| 001 | Alt-Acme Processing | On Demand | 190.200.20.20:4096  | 16712  | 16712   | Active SSL   | Ethernet  |
| 018 | TransResources      | On Demand | 180.200.140.10:4096 | 0      | 0       | Inactive     | PPP       |
| 018 | Alt-TransResources  | On Demand | 210.100.180.60:4096 | 0      | 0       | Inactive     | PPP       |

This screen provides a table that allows you to quickly analyze the status of all enabled host processors. There are generally two entries for each host processor, one for the primary IP/URL and one for the alternate IP/URL. Click **Refresh** as needed to update the status.

| Field/Button | Description  |
|--------------|--|
| NII          | NII number assigned to the host on the Host Processor Settings screen  |
| Description  | Text description assigned to the host on the Host Processor Settings screen  |
| Type         | Connection type, either Permanent or On Demand   |
| Host Name    | Primary or Alternate host address configured in the Host Processor Settings screen. Either an IP address or URL. For long host names, place the mouse cursor on the Host Name field (hover) to display a pop-up tool tip that shows the complete URL host address. |
| Msg In       | Total number of messages received from the host processor by the IN-tact 1101  |
| Msg Out      | Total number of messages sent from the IN-tact 1101 to the host processor  |

| Field/Button | Description   |
|--------------|---|
| Status       | <p>Indicates the current status of the host processor. Valid status indications are color-coded and described below. Refer to the following table for the meaning of the most common failure codes.</p> <p>Active — on demand connection<br/>           Active SSL — on demand connection with SSL<br/>           Connect — permanent connection<br/>           Connect SSL — permanent connection with SSL<br/>           Enabled — an idle on demand connection<br/>           Failed — see error codes listed below<br/>           Inactive — an idle permanent connection or an on demand connection that isn't configured.</p> |
| Interface    | <p>Indicates the interface (Ethernet or PPP) that can be used to reach the host processor. If the host processor cannot be reached at all, "Unknown" is displayed here. When the host address is specified as a DNS name instead of an IP address, the initial interface appears as "Unknown". Once a transaction has been routed to that host and the DNS server successfully resolves the host name, the interface type is then correctly shown as "Ethernet" or "PPP".</p>   |

## Error Codes

| Code | Description                       | Explanation  |
|------|-----------------------------------|--|
| 100  | DNS error                         | The associated host name cannot be found by the Domain Name Server (DNS). This is because the DNS is not responding or it cannot find the name.  |
| 110  | Socket creation error             | Internal socket creation error. Please refer to the Event Log for the specific failure.  |
| 120  | General connection error          | The session cannot be connected to the host. Please refer to the Event Log for the specific reason.  |
| 121  | Connection refused                | The session cannot be connected to the host because the host refused the connection. This generally means that the host application is not running or is not configured to use the TCP port.                         |
| 122  | Connection timed out              | The session cannot be connected to the host because the host did not respond. This generally means that the IP address for the host is wrong or the network is preventing the IN-tact 1101 from contacting the host. |
| 130  | General SSL error                 | The session failed because of an SSL error. Please refer to the Event Log for the specific reason.   |
| 131  | SSL certificate validation failed | The session failed because the SSL certificate from the host could not be verified.  |
| 132  | SSL timeout                       | The session failed because the SSL negotiation did not complete within the required timeframe.   |

## Dial Backup Status

On the navigation tree, click **Status > Dial Backup**. The Dial Backup Status screen appears:

| IN-tact :: Dial Backup Status         |                   | October 21, 2004 |
|---------------------------------------|-------------------|------------------|
| <b>Current Status</b>                 | Not enabled       |                  |
| <b>Primary Failure Code</b>           | 0                 |                  |
| <b>Alternate Failure Code</b>         | 0                 |                  |
| <b>Current Mode</b>                   | Wait for Txn      |                  |
| <b>Uptime</b>                         | 0 days (00:00:00) |                  |
| <b>Last Modem Connect Speed</b>       | Unknown           |                  |
| <b>Inactivity Timer Disconnects</b>   | 0                 |                  |
| <b>Dial Attempts</b>                  | 0                 |                  |
| <b>Failed Dial Attempts</b>           | 0                 |                  |
| <b>Failed Authentication Attempts</b> | 0                 |                  |
| <b>Unexpected Disconnects</b>         | 0                 |                  |
| <b>User Messages In</b>               | 0                 |                  |
| <b>User Messages Out</b>              | 0                 |                  |
| <b>PPP IP Address</b>                 | 0.0.0.0           |                  |
| <b>Peer IP Address</b>                | 0.0.0.0           |                  |

Use this screen to determine the current status of dial backup operations. Three fields are of particular value when troubleshooting - **Current Status**, **Primary Failure Code** and **Alternate Failure Code**. Explanations of the status messages or codes that can be displayed in these fields are provided on the following pages to help you quickly diagnose any possible problems. Use **Refresh** to update the status/statistics displayed on this screen as necessary.

| Field/Button                   | Description   |
|--------------------------------|---|
| Current Status                 | This field displays the current status of the modem as detected by the IN-tact 1101. Refer to Table 5-1 on page 64 for status message explanations. |
| Primary/Alternate Failure Code | Refer to Table 5-2 on page 65 for failure codes and their explanations.   |
| Current Mode                   | Indicates the Dialing Mode setting on the Advanced Dial Backup Settings screen, either Immediate or Wait for Transaction.                           |
| Uptime                         | Cumulative time that PPP has been connected.  |

| Field/Button                   | Description  |
|--------------------------------|--|
| Last Modem Connect Speed       | The last reported connection speed of the modem. This value is not reset when you clear statistics for the IN- <i>tact</i> 1101. |
| Inactivity Timer Disconnects   | The number of times the modem link was disconnected due to no transactions or inactivity.  |
| Dial Attempts                  | Total number of dial commands attempted.   |
| Failed Dial Attempts           | Number of attempted dial commands that failed.   |
| Failed Authentication Attempts | Number of PPP negotiations that failed due to an invalid user ID or password.  |
| Unexpected Disconnects         | Number of times the link was disconnected due to an unexpected condition or situation (cable being removed, power outage, etc.). |
| User Messages In               | Number of messages received from the host processor via the dial link. This does not include Ethernet or SNMP traffic.           |
| User Messages Out              | Number of messages sent to the host processor via the dial link. This does not include Ethernet or SNMP traffic.                 |
| PPP IP Address                 | The IP address assigned to the PPP interface.  |
| Peer IP Address                | The IP address of the other end of the PPP link.   |

**TABLE 5-1. Status Messages**

| Status Message                  | SNMP Code | Explanation   |
|---------------------------------|-----------|---|
| Dial Backup Feature Not Enabled | 0         | The feature is disabled by default. Go to the Dial Backup Settings screen to enable this feature.                                       |
| Disconnected/Modem Not Present  | 1         | The IN- <i>tact</i> 1101 was not able to detect a modem attached to the serial port (port 1). Check the modem cabling and power.        |
| On Hook/Modem Present           | 2         | The IN- <i>tact</i> 1101 was able to detect a modem. However, the modem is currently not in use.  |
| Dialing/Primary                 | 3         | The modem is currently dialing the primary dial string.   |
| Dialing/Alternate               | 4         | The modem is currently dialing the alternate dial string.   |
| Negotiating/Primary             | 5         | The modem has successfully connected using the primary dial string and is negotiating PPP.  |
| Negotiating/Alternate           | 6         | The modem has successfully connected using the alternate dial string and is negotiating PPP.  |
| Connected/Primary               | 7         | A PPP session has been established using the primary dial string.   |
| Connected/Alternate             | 8         | A PPP session has been established using the alternate dial string.   |
| Failure                         | 9         | The modem was unable to establish a PPP connection. Please refer to the primary and alternate Failure Codes for additional information. |
| Initializing Modem              | 10        | The modem is being initialized.   |

**TABLE 5-1. Status Messages**

| Status Message          | SNMP Code | Explanation   |
|-------------------------|-----------|---|
| Query Modem/Not Working | 11        | The modem did not respond to a basic modem model query command. Please use one of the supported modem types: <ul style="list-style-type: none"> <li>• US Robotics 5686e</li> <li>• Hayes H08-15328-C</li> <li>• ZOOM 3048C</li> </ul> |
| Modem Hanging Up        | 12        | The modem is in the process of disconnecting.   |

**TABLE 5-2. Failure Codes**

| Status Message | Explanation  |
|----------------|--|
| 0              | Normal operation.  |
| 100            | Unable to initialize modem. Check modem initialization string.   |
| 101            | PPP negotiation failed. Check CHAP/PAP settings along with user ID and password.                                     |
| 102            | Modem dialing failed, no additional information. Enable DBU debug messages and check Event Log for more information. |
| 103            | Modem reported "No Carrier".   |
| 104            | Modem reported "Error".  |
| 105            | Modem reported "No Response" within 45 seconds.  |
| 106            | Modem reported "No Dial Tone".   |
| 107            | Modem reported "Busy".   |
| 108            | Modem reported "No Answer".  |





---

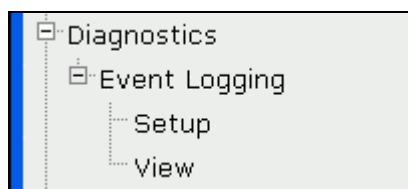
## Chapter 6: Diagnostics

---

### Overview

The IN-*tact* 1101 provides event logging in order to help you isolate and troubleshoot specific events that occur on the terminal network. An event is an asynchronous message generated by the system when it encounters a specific situation. The event message contains the severity of the situation and a description.

Keep in mind that not all events captured in the Event Log indicate a problem; many are part of normal operation. Additionally, some events may be transient, while others are persistent. The Event Log provides a window in which to view what is happening and make a determination about any actions you should take.



The screens within the Diagnostics portion of the navigation tree are:

- **Event Logging Setup** — Used to set the level of severity of events you wish to monitor. You also set an optional IP address here for forwarding captured events to a system log (syslog)
- **Event Logging View** — Provides a scrolling window for reviewing captured events. Also allows you to export the Event Log for later review. Notepad is the recommended application for reviewing the Event Log.

## Event Logging Setup

On the navigation tree, click **Diagnostics > Event Logging > Setup**. The Event Logging Setup screen appears:

In order to use the Event Log, you must set up the *IN-tact* 1101 to capture specific events. Use the following information to enable event logging. Also, it is important to note that SNMP traps are not filtered by the Event Log settings specified here.

| Field/Button | Description   |
|--------------|---|
| Severity     | <p>Select the severity level of events to log from the drop-down list.</p> <p>There are four levels of events and they are listed in order of severity below with Error being the highest. The severity level you select will capture those events, as well as any events that are more critical. For example, if you select the Warning level, both Warning and Error level events will be captured, but not Info or Debug level events.</p> <p><b>Error</b> — In most cases, these events will have some impact on operations and transactions may not be processing correctly. Error events usually requires an interaction or attention on your part. Some error events should be exported and forwarded to Hypercom for analysis, as they may indicate a firmware problem.</p> <p><b>Warning</b> — These events are indications that should be monitored. They do not necessarily indicate a failure, but cover operations like polls being lost and then restored. Warnings often indicate a transient event.</p> <p><b>Info</b> — These events simply provide information; they are not indicative of a problem, but are useful in analyzing what is happening with the device.</p> <p><b>Debug</b> — These events are related to the internal operation of the <i>IN-tact</i> 1101 and are not generally useful to anyone but system engineers. These events record buffer allocations and memory addresses to analyze software operation within the device. You may be asked to select this level of logging when working with Hypercom technical support.</p> |
| Send To      | <p>Click the <b>Syslog</b> checkbox to send the events to a system log at another location. You must provide an IP address of where to forward the events.</p>  |

| Field/Button | Description  |
|--------------|--|
| Apply        | Click when finished setting the Event Log configuration options. The configuration is saved to persistent memory. Any changes are immediately applied; you are not required to reset the device in order for your changes to take place. |

## Event Log View

On the navigation tree, click **Diagnostics > Event Logging > View**. The Event Log View screen appears:

EXPORT REFRESH HELP PRINT

IN-tact :: Event Log View October 21, 2004

**Current Event Log Data**

|         |            |          |     |                          |
|---------|------------|----------|-----|--------------------------|
| Warning | 2004-10-21 | 11:40:04 | ETH | Cannot create session to |
| Warning | 2004-10-21 | 11:40:09 | ETH | Cannot create session to |
| Warning | 2004-10-21 | 11:40:14 | ETH | Cannot create session to |
| Warning | 2004-10-21 | 11:40:19 | ETH | Cannot create session to |
| Warning | 2004-10-21 | 11:40:24 | ETH | Cannot create session to |
| Warning | 2004-10-21 | 11:40:29 | ETH | Cannot create session to |
| Warning | 2004-10-21 | 11:40:34 | ETH | Cannot create session to |
| Warning | 2004-10-21 | 11:40:39 | ETH | Cannot create session to |
| Warning | 2004-10-21 | 11:40:44 | ETH | Cannot create session to |
| Warning | 2004-10-21 | 11:40:49 | ETH | Cannot create session to |
| Warning | 2004-10-21 | 11:40:54 | ETH | Cannot create session to |
| Warning | 2004-10-21 | 11:40:59 | ETH | Cannot create session to |
| Warning | 2004-10-21 | 11:41:04 | ETH | Cannot create session to |
| Warning | 2004-10-21 | 11:41:09 | ETH | Cannot create session to |
| Warning | 2004-10-21 | 11:41:14 | ETH | Cannot create session to |
| Warning | 2004-10-21 | 11:41:19 | ETH | Cannot create session to |
| Warning | 2004-10-21 | 11:41:24 | ETH | Cannot create session to |
| Warning | 2004-10-21 | 11:41:29 | ETH | Cannot create session to |
| Warning | 2004-10-21 | 11:41:34 | ETH | Cannot create session to |

The Event Log View window allows you to see any events that have occurred and have been logged. You must first set up event logging in order to capture specific event. See the Event Logging Setup screen for details on what can be captured in the Event Log.

Specified events appear in the scrolling window of the Event Log View screen as they occur. You must use **Refresh** to update the Event Log and bring the most current events into the window; the Event Log is not automatically updated at any preset interval.

Use **Export** to create a text file of the events in your browser window. You can then save the file as necessary. Use your browser's **Back** button to return to IN-tact 1101 Event Log View screen after you save the file. Notepad can be used for viewing the saved file, but you must associate the .dat file extension with Notepad in order to do so.

To configure the Notepad association for .dat files:

1. Click **Start > Settings > Control Panel > Folder Options**.
2. Click the File Types tab.
3. If you have DAT file type registered, go to step 6.
4. Click **New** to open the "Create new extension" dialog, type DAT in the edit box.
5. Click **Advanced** and use "Text Document" as the associated file type from the drop-down list.
6. Click **Advanced** to open the "Edit File Type" dialog.
7. You can click **Change Icon** to change the icon to one you will readily recognize.
8. Click **New** to open the "New Action" dialog (or click **Edit** to open the "Edit Action" dialog if you have "Open" action defined).
9. Type **Open** in the Action edit box, click **Browse** and navigate to the folder where Notepad.exe is located, such as C:\WINNT\system32\notepad.exe.
10. Type C:\WINNT\system32\notepad.exe %1 in the edit box labeled with "application used to perform action".
11. Click **OK** at each of the prompts to acknowledge and close the open dialogs.

The following table lists all of the events that can occur, their severity level, and whether or not an SNMP trap is generated because of the event. SNMP traps are explained in Chapter 8.

### Event Log Message Table

| Event Log Message Text                                       | Severity Level | SNMP Trap |
|--|----------------|-----------|
| <b>Event Logger Events</b>                                   |                |           |
| Bad log message - - invalid subsystem 0x%x                   | Warning        | Yes       |
| Bad log message - - invalid ordinal 0x%x for subsystem 0x%x  | Warning        | Yes       |
| <b>Kernel Event</b>  |                |           |
| Assert failed in function %s line %d                         | Error          | Yes       |
| <b>SDLC Events</b>   |                |           |
| Improperly formatted SDLC message received from address %02x | Warning        | Yes       |
| Terminal %02x poll lost - - %d                               | Warning        | Yes       |
| Terminal %02x poll restored                                  | Warning        | Yes       |
| Unable to remove header prior to sending rx data to client   | Error          | Yes       |
| Initial offset too large for the buffer                      | Error          | Yes       |
| Initial length too large for the buffer                      | Error          | Yes       |
| Unable to format buffer from pool %d                         | Error          | Yes       |

| Event Log Message Text  | Severity Level | SNMP Trap |
|---|----------------|-----------|
| Error attempting to add a header to a buffer                                  | Error          | Yes       |
| Retrieved an application frame which is not a buffer msg %d                   | Error          | Yes       |
| Mailbox %d is full - - message discarded                                      | Error          | Yes       |
| Unable to acquire buffer from pool %d   | Error          | Yes       |
| Internal state error for address %02x eDropState=0x%2x                        | Error          | Yes       |
| Unable to cancel POSIX resource %d  | Error          | Yes       |
| Retrieved an invalid event message %x   | Error          | Yes       |
| Error reading from HDLC - - %s  | Error          | Yes       |
| Invalid length %d bytes read from HDLC  | Error          | Yes       |
| <b>SCC Event</b>  |                |           |
| Receive buffers exhausted. Frame discarded.                                   | Error          | Yes       |
| <b>TCP/IP/Ethernet Interface Events</b>                                       |                |           |
| Cannot create session to %s:%d - %s   | Warning        | Yes       |
| Cannot create SSL session to %s:%d - %s                                       | Warning        | Yes       |
| Persistent session to host %s:%d established                                  | Info           | No        |
| Persistent SSL session to host %s:%d established                              | Info           | No        |
| Persistent session to host %s:%d closed                                       | Warning        | Yes       |
| Ethernet link lost  | Error          | Yes       |
| Ethernet link restored  | Warning        | Yes       |
| Received invalid length 0x%04x from %s:%d. Restarting session                 | Error          | Yes       |
| DNS lookup of name %s failed  | Warning        | No        |
| No DNS server configured  | Error          | Yes       |
| <b>Web Server Events</b>  |                |           |
| Invalid administrator password entered from %s                                | Info           | No        |
| Administrator logged in from %s   | Warning        | Yes       |
| Administrator logged out from %s  | Warning        | Yes       |
| Administrator password changed by %s  | Warning        | Yes       |
| Login session from %s timed out   | Warning        | Yes       |
| Maximum failed login attempts   | Warning        | Yes       |
| <b>HLAN to IP Events</b>  |                |           |
| Improperly formatted message from terminal %02x - - message discarded         | Error          | Yes       |
| Transaction from terminal %02x - - NII %03X routed to default NII             | Info           | Yes       |
| Transaction from terminal %02x - - no route to NII %03X - - message discarded | Warning        | Yes       |
| Transaction memory full   | Error          | Yes       |
| Open error on subsystem %d  | Error          | Yes       |

| Event Log Message Text   | Severity Level | SNMP Trap |
|--|----------------|-----------|
| Mailbox full for NII %3X   | Error          | Yes       |
| Unable to route data from TCP for destination index %02X%02X                                 | Error          | Yes       |
| Invalid data from TCP  | Error          | Yes       |
| Using backup host for NII %03X   | Warning        | Yes       |
| Restored primary host for NII %03X   | Info           | No        |
|  |                |           |
| <b>Log Interface Events</b>  |                |           |
| Invalid Registry IFace fields @addr:0x%08x   | Error          | Yes       |
| Get requested @addr:0x%08x for illegal Item ID=0x%08x  | Error          | Yes       |
| Get requested @addr:0x%08x for invalid subrange - Item ID=0x%08x                             | Error          | Yes       |
| Get requested @addr:0x%08x of Item ID=0x%08x invalid subset index=%d.                        | Debug          | No        |
| Get requested @addr:0x%08x of non-provided Item ID=0x%08x                                    | Debug          | No        |
| Put requested @addr:0x%08x for invalid subrange - Item ID=0x%08x                             | Error          | Yes       |
| Illegal data interface usage from @addr:0x%08x   | Error          | Yes       |
|  |                |           |
| <b>Dial Backup Events</b>  |                |           |
| Unable to initialize modem using init string: XX   | Warning        | No        |
| Unable to establish modem connection using dial string: XX                                   | Warning        | No        |
| Unable to establish PPP connection using dial string: XX                                     | Warning        | No        |
| Switched from test mode to normal dial mode  | Info           | No        |
| Dial backup subsystem started  | Info           | No        |
| Dial backup established using IP address: XX   | Info           | Yes       |
| Dial backup disconnecting from IP address: XX  | Info           | Yes       |
|  |                |           |
| <b>SNTP Events</b>   |                |           |
| SNTP not configured, default date and time are currently in use. Corrective action required. | Warning        | Yes       |
| No response from NTP server or server not found. Using default date and time                 | Warning        | Yes       |
| No response from NTP server or server not found.   | Warning        | No        |
| System time has been synchronized per NTP host XX  | Info           | No        |
| Unable to translate NTP host name XX via DNS   | Warning        | No        |
|  |                |           |
| <b>TXN Router Events</b>   |                |           |
| Message sent to channel %02x   | Debug          | No        |
| Message received from channel %02x   | Debug          | No        |
|  |                |           |
| Transaction from channel %02x -- NII %03X routed to default NII                              | Info           | Yes       |
| Transaction from terminal %02x -- no route to NII %03X -- message discarded                  | Warning        | Yes       |
| Transaction memory full  | Error          | Yes       |

| <b>Event Log Message Text</b>                                | <b>Severity Level</b> | <b>SNMP Trap</b> |
|--|-----------------------|------------------|
| Transacton open error %d                                     | Error                 | Yes              |
| Mailbox full for NII %3X                                     | Error                 | Yes              |
| Unable to route data from TCP for destination index %02X%02X | Error                 | Yes              |
| Invalid data from TCP  | Error                 | Yes              |
| Using backup host for NII %03X                               | Warning               | Yes              |
| Restored primary host for NII %03X                           | Info                  | No               |





---

# Chapter 7: Configuration Examples

---

## Overview

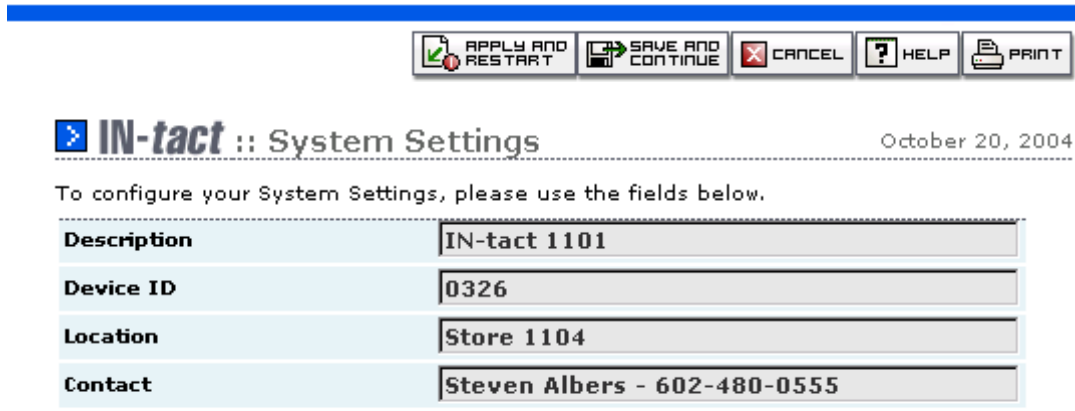
This section provides examples of how to configure the IN-*tact* 1101 to meet various needs. The examples assume a basic knowledge of the IN-*tact* 1101 purpose and illustrate the versatility of the product. They are not intended to be a replacement for the actual steps required to configure the device. Complete configuration details, including step-by-step instructions, are contained elsewhere in this document.

The screen examples on the following pages illustrate the ease of configuring the IN-*tact* 1101 via its Web Server application. Two basic scenarios are identified:

- **Minimal** — Configuration of the items shown is the minimum requirement for the IN-*tact* 1101 to operate and process transactions
- **Managed** — Configuration of the items shown is optional and only required if the IN-*tact* 1101 is to be managed via SNMP and/or a web browser.

## System Identification - Managed

This screen allows unique descriptions to be defined for each *IN-tact* device. This information is essential when multiple *IN-tact* devices are deployed on a network in order to identify each of the devices. The information entered is returned in a status display when browsing the *IN-tact* 1101 settings. The Device ID field is alphanumeric and its entry is sent to an SNMP manager when SNMP is utilized for network monitoring purposes. All entries are free-form text and it is up to the user's discretion to define a numbering and/or identification scheme.








| IN-tact :: System Settings <span style="float: right;">October 20, 2004</span> |                              |
|--|------------------------------|
| To configure your System Settings, please use the fields below.                |                              |
| <b>Description</b>   | IN-tact 1101                 |
| <b>Device ID</b>   | 0326                         |
| <b>Location</b>  | Store 1104                   |
| <b>Contact</b>   | Steven Albers - 602-480-0555 |


A Device ID must be entered in order to complete configuration requirements. It is also worthwhile to provide a description and location.

## Ethernet Port Settings - Minimal

These settings establish the unique identity of the IN-*tact* 1101's Ethernet port. DHCP is enabled by default. However, you can disable DHCP and assign a static IP address if necessary.

---

 **IN-*tact*** :: Ethernet Port Settings
January 3, 2005

To configure your Ethernet Port Settings, please use the fields below.

|  |                             |
|--|-----------------------------|
| <b>MAC Address</b>                                     | 00 : 40 : EF : 00 : 00 : DC |
| <b>Static IP Address</b>                               | 192.168.1.20                |
| <b>Static Subnet Mask</b>                              | 255.255.255.0               |
| <b>Static Gateway Address</b>                          | 0.0.0.0                     |
| <b>Static DNS Server</b>                               | 0.0.0.0                     |
| <input checked="" type="checkbox"/> <b>Enable DHCP</b> |                             |






Advanced ->

These values must be synchronized with the IP addressing scheme of the network:

| Field/Button           | Description  |
|------------------------|--|
| MAC Address            | Vendor-supplied hardware address and should not be changed   |
| Static IP Address      | Default address assigned to all IN- <i>tact</i> units. Unless static IP addresses are assigned to each IN- <i>tact</i> 1101 on the network, this can be left as default.   |
| Static Subnet Mask     | Default value and need not be changed unless static IP addresses are assigned  |
| Static Gateway Address | This field is only required if static IP addressing is in use and the IN- <i>tact</i> 1101 is not sharing the same LAN segment as its host destinations. The address of the local gateway router should be entered here if not on the same segment |
| Static DNS Server      | Enabled by default. This function is required when static IP addresses are not being used.   |
| Enable DHCP            | Enabled by default. This function is required when static IP addresses are not being used.   |

## Ethernet Port Settings - Managed

These settings establish the unique identity of the IN-*tact* 1101's Ethernet port. These values will need to be synchronized with the IP addressing scheme of the network. In this case, DHCP has been disabled and static IP addressing is being used.

▶ IN-*tact* :: Ethernet Port Settings
January 5, 2005

To configure your Ethernet Port Settings, please use the fields below.

|   |                             |
|---|-----------------------------|
| <b>MAC Address</b>                          | 00 : 40 : EF : 00 : 00 : DC |
| <b>Static IP Address</b>                    | 200.120.240.08              |
| <b>Static Subnet Mask</b>                   | 255.255.255.0               |
| <b>Static Gateway Address</b>               | 200.120.100.100             |
| <b>Static DNS Server</b>                    | 200.120.100.120             |
| <input type="checkbox"/> <b>Enable DHCP</b> |                             |

Advanced ->

| Field/Button           | Description   |
|------------------------|---|
| MAC Address            | Normally not changed.   |
| Static IP Address      | Reserved IP address   |
| Static Subnet Mask     | Reserved subnet mask  |
| Static Gateway Address | Optionally, this value can be defined if the ISP identifies it as needed. In this configuration, static addressing is used. |
| Static DNS Server      | Enter the IP address of the DNS server  |
| Enable DHCP            | Disabled by clearing the checkbox   |

## Host Processor Setup - Minimal with Single Host

This is an example of a single host processor configuration for a fictional processor, i.e., Acme Processing. There are three screens involved with configuring a host processor (Figs. 1, 2, & 3).

| NII | Description     | Enabled                             | Connection Type |
|-----|-----------------|-------------------------------------|-----------------|
| 021 | Acme Processing | <input checked="" type="checkbox"/> | Standard        |
| 001 |                 | <input type="checkbox"/>            | Standard        |
| 001 |                 | <input type="checkbox"/>            | Standard        |
| 001 |                 | <input type="checkbox"/>            | Standard        |
| 001 |                 | <input type="checkbox"/>            | Standard        |
| 001 |                 | <input type="checkbox"/>            | Standard        |
| 001 |                 | <input type="checkbox"/>            | Standard        |
| 001 |                 | <input type="checkbox"/>            | Standard        |

Figure 1. Host Port Settings Screen - Single Host

By restricting the table to a single host processor entry, the end-user terminals are expected to send all POS transactions to a single destination. At least one host processor must be defined.

| Field/Button    | Description  |
|-----------------|--|
| NII             | The use of the NII value allows those terminals initialized with the same NII to be matched for transmission of all traffic to the associated primary IP address |
| Description     | A free-form text entry used to identify the processor  |
| Enabled         | Allows you to temporarily disable, but not delete, a processor   |
| Connection Type | Defines whether a Standard or HTTP connection is being used by the processor   |
| Edit            | Displays the related connection type screen (See Figure 2) and allows you to define addresses  |

**IN-tact :: Standard Host Settings** November 11, 2004

To configure your Standard Host Settings, please use the fields below.

|  |   |
|--|---|
| <b>NII</b>                                 | 021   |
| <b>Description</b>                         | Acme Processing   |
| <b>Connection Mode</b>                     | Permanent <input type="button" value="Edit..."/>        |
| <input type="checkbox"/> <b>Enable SSL</b> |   |
| <b>Primary Host Address</b>                | 210.100.200.10  |
| <b>Primary TCP Port</b>                    | 4096  |
| <b>Alternate Host Address</b>              | 210.100.100.10  |
| <b>Alternate TCP Port</b>                  | 4096  |
| <b>Visa Protocol</b>                       | Visa Transparent <input type="button" value="Edit..."/> |

Figure 2. Standard Host Settings Screen - Single Host

The second host processor setup page is used to define connection mode, IP addressing, and SSL usage:

| Field/Button           | Description  |
|------------------------|--|
| NII                    | The value is carried over from the first configuration screen  |
| Description            | The text is carried over from the first configuration screen   |
| Connection Mode        | Defines the permanent or on-demand TCP operation to be in use. This is the normal operation for use with any host LAN server providing TCP/IP connectivity |
| Enable SSL             | Click to enable where encryption and authentication are required to be performed by the IN-tact device   |
| Primary Host Address   | Destination address of the hosting LAN server  |
| Primary Port           | Assigned socket to which all TCP traffic will be sent  |
| Alternate Host Address | Optional entry that defines where to route transactions in the event the primary IP/URL address is unavailable   |
| Alternate TCP Port     | Socket associated with the alternate IP address.   |
| Visa Protocol          | Choose whether to use Visa Transparent, Full Transparent, or Spoofed Mode to match host requirements.  |

| Field/Button  | Description     |
|---|-----------------|
| NII   | 022             |
| Description   | Acme Processing |
| <input type="checkbox"/> Include length field in length calculation |                 |

Figure 3. Permanent Mode Settings Screen

| Field/Button  | Description  |
|---|--|
| NII   | NII currently being configured   |
| Description   | The processor currently being configured   |
| <input type="checkbox"/> Include length field in length calculation | The first two bytes of the POS LAN Header are a length indicator. This option determines whether or not these first two bytes are included as part of the length calculation. This option should be set to match host processor configuration. |

## Host Processor Setup - Minimal with Multiple Hosts

This is an example of a multiple host processor configuration. Three screens are used to define the host processors in use (Figures 4, 5 & 6).

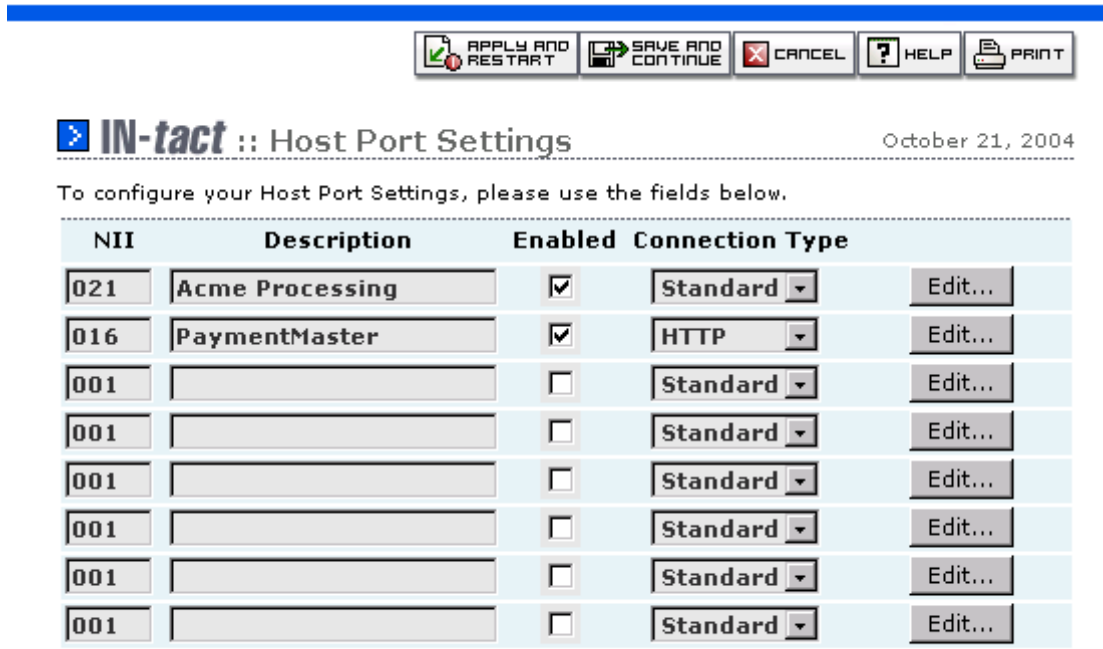








Figure 4. Host Port Settings Screen - Multiple Hosts

By defining and enabling multiple host processors, the end-user terminals send POS transactions to the destination specified in the NII portion of the TPDU sent from the terminal per each transaction (see Figure 3).

| Field/Button    | Description   |
|-----------------|---|
| NII             | Allows those terminals initialized with the same NII to be matched for transmission of all traffic to the associated primary IP address |
| Description     | A free-form text entry used to identify the processor   |
| Enabled         | Allows you to temporarily disable, but not delete, a processor  |
| Connection Type | Defines whether a Standard or HTTP connection is being used by the processor  |
| Edit            | Displays the related connection type screen (see Figure 4) and allows you to define IP addresses.                                       |



---

**IN-tact** :: HTTP Host Settings October 21, 2004

To configure your HTTP Host Settings, please use the fields below.

|  |                      |
|--|----------------------|
| <b>NII</b>   | <b>016</b>           |
| <b>Description</b>   | <b>PaymentMaster</b> |
| <input checked="" type="checkbox"/> <b>Enable SSL</b>                      |                      |
| <input type="checkbox"/> <b>Include Two-byte Message Length Header</b>     |                      |
| <input type="checkbox"/> <b>Include length field in length calculation</b> |                      |
| <input type="checkbox"/> <b>Include TPDU</b>                               |                      |
| <input type="checkbox"/> <b>Use STX/ETX Wrapper</b>                        |                      |
| <input type="checkbox"/> <b>Discard ACKs</b>                               |                      |
| <b>Primary Host Address</b>  | 192.224.80.120       |
| <b>Primary Port</b>  | 4096                 |
| <b>Alternate Host Address</b>  | 224.424.100.60       |
| <b>Alternate Port</b>  | 4096                 |

Figure 5. HTTP Host Settings Screen - Multiple Hosts

The second host processor setup page is used to define connection mode, IP addressing, and SSL usage:

| Field/Button                               | Description  |
|--|--|
| NII  | The value is carried over from the first configuration screen  |
| Description                                | The text is carried over from the first configuration screen   |
| Enable SSL                                 | Enable where encryption and authentication are required to be performed by the IN-tact device  |
| Include Two-byte Message Length Header     | Use this checkbox to enable Hypercom's proprietary POS LAN header if required for this host connection. This option is disabled by default. The two options below allow further control of the header and should be enabled or disabled according to how the host processor is configured. |
| Include Length Field in Length Calculation | As mentioned above, the first two bytes of the POS LAN header are a length indicator. This option determines whether or not these first two bytes are included as part of the length calculation. This option should be set to match host processor configuration.                         |

| Field/Button           | Description   |
|------------------------|---|
| Include TPDU           | The TPDU is the next five bytes of the POS LAN Header and includes information used for routing purposes. This option determines whether or not these five bytes are included as part of the header. This option should be set to match host processor configuration. |
| Use STX/ETX Wrapper    | Use this checkbox to enable Start of Text (STX) and End of Text (ETX) wrappers if required by the host. This option is used primarily for hosts that don't run Visa protocol, but want to use async framing.  |
| Discard ACKs           | Use this checkbox to discard any ACKs sent by the terminals, rather than sending them to the host. This option is used primarily for hosts that don't run Visa protocol, but want to use async framing.   |
| Primary Host Address   | Destination address of the hosting LAN server   |
| Primary Port           | Assigned socket to which all TCP traffic will be sent   |
| Alternate Host Address | Optional entry that defines where to route transactions in the event the primary IP/URL address is unavailable  |
| Alternate Port         | Socket associated with the alternate IP address   |

**NOTE:** Because this is an HTTP connection type, **Connection Mode** is not used for this processor.

**IN-tact** :: Permanent Mode Settings January 5, 2005

To configure your Permanent Mode Settings, please use the fields below.






|  |                        |
|--|------------------------|
| <b>NII</b>   | <b>022</b>             |
| <b>Description</b>   | <b>Acme Processing</b> |
| <input type="checkbox"/> <b>Include length field in length calculation</b> |                        |

Figure 6. Permanent Mode Settings Screen

| Field/Button                               | Description  |
|--|--|
| NII  | NII currently being configured   |
| Description                                | The processor currently being configured   |
| Include length field in length calculation | The first two bytes of the POS LAN Header are a length indicator. This option determines whether or not these first two bytes are included as part of the length calculation. This option should be set to match host processor configuration. |

## Transaction Routing - Minimal

Each *IN-tact* 1101 should be provisioned with a standard set of routing rules.

---

**IN-tact** :: Transaction Settings
October 20, 2004

To configure your Transaction Settings, please use the fields below.

|   |                         |
|---|-------------------------|
| <b>Default NII</b>                      | 021                     |
| <b>Routing Mode For Known NIIs</b>      | Route to embedded NII ▾ |
| <b>Routing Mode For Unknown NIIs</b>    | Route to default NII ▾  |
| <b>Send Initialization Requests To:</b> | Term-Master ▾           |
| <b>Recognize Processing Code 92 As:</b> | Transaction ▾           |
| <b>Recognize Processing Code 94 As:</b> | Transaction ▾           |

The rules determine how transactions will be routed between the terminal and host:

- The default NII value is needed to supply a single destination to where all transactions that cannot be matched to an NII defined in the Host Processor settings should be routed. This must match one of the configured Host NII values.
- The “route to embedded NII” selection provides to the ability to match the NII received from the terminal to the host destination selected to receive that transaction
- The Routing Mode for Unknown NIIs allows a choice as to where to route those transactions that cannot be routed due to no NII match. They can be routed to the default NII or simply discarded.
- The Send Initialization Requests To selection allows all initialization to be sent to Term-Master or to a host processor
- The Recognize Code 92 and Code 94 As settings should be left at default.

## Merchant Terminal Setup - Minimal

The site survey checklist provides the information needed to verify the number and location of the terminals in use at the merchant location.



### IN-tact :: Terminal Port Settings

October 20, 2004

To configure your Terminal Port Settings, please use the fields below.






HLAN Speed 19200 BPS ▾

| Enabled                             | Description     | CU Address | Enabled                  | Description | CU Address |
|-------------------------------------|-----------------|------------|--------------------------|-------------|------------|
| <input checked="" type="checkbox"/> | Front Counter 1 | 30         | <input type="checkbox"/> |             | 38         |
| <input checked="" type="checkbox"/> | Front Counter 2 | 31         | <input type="checkbox"/> |             | 39         |
| <input checked="" type="checkbox"/> | Drive-thru      | 32         | <input type="checkbox"/> |             | 3A         |
| <input type="checkbox"/>            |                 | 33         | <input type="checkbox"/> |             | 3B         |
| <input type="checkbox"/>            |                 | 34         | <input type="checkbox"/> |             | 3C         |
| <input type="checkbox"/>            |                 | 35         | <input type="checkbox"/> |             | 3D         |
| <input type="checkbox"/>            |                 | 36         | <input type="checkbox"/> |             | 3E         |
| <input type="checkbox"/>            |                 | 37         | <input type="checkbox"/> |             | 3F         |

- HLAN speed should be determined prior to installation and configured into the terminals during installation
- The terminal addresses (CU address) conform to how each terminal will be configured during installation
- Terminals are enabled by clicking in the **Enabled** checkbox.

## SNMP Setup - Managed

The managed approach to provisioning allows the use of Simplified Network Management Protocol (SNMP) to be enabled.

---

**IN-tact** :: SNMP Interface Settings October 21, 2004

To configure your SNMP Interface Settings, please use the fields below.

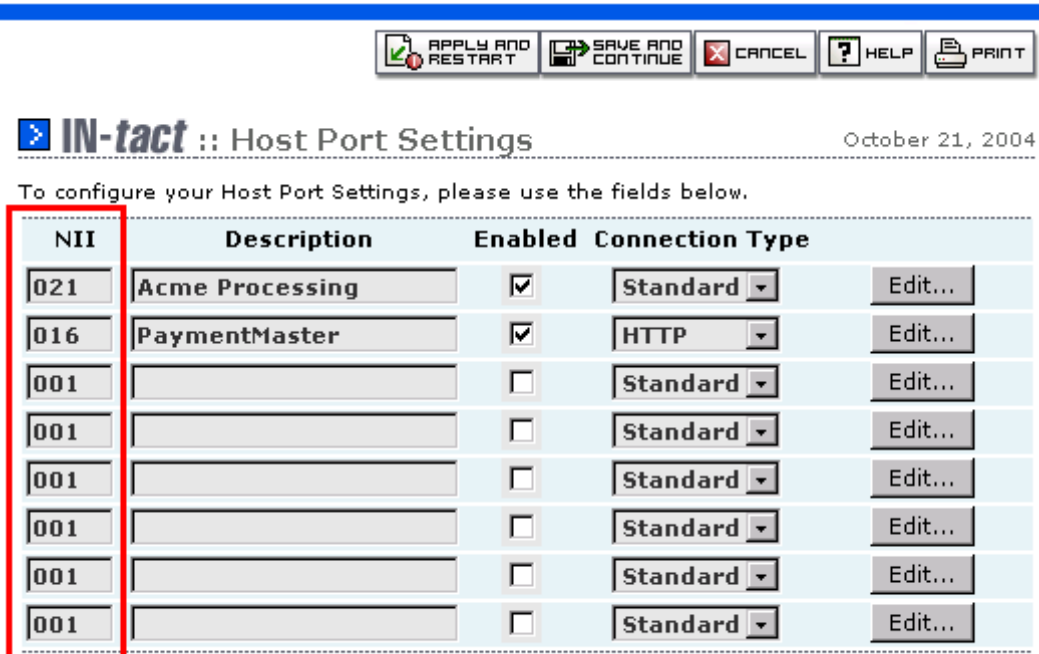
|  |  |   |
|--|--|---|
| <input checked="" type="checkbox"/> <b>Enable SNMP Agent</b> |  |   |
| Manager Address 1  | <input type="text" value="200.120.140.010"/> | <input checked="" type="checkbox"/> <b>Enable</b> |
| Manager Address 2  | <input type="text" value="0.0.0.0"/>         | <input type="checkbox"/> <b>Enable</b>            |
| Trap Destination 1   | <input type="text" value="200.120.100.100"/> | <input checked="" type="checkbox"/> <b>Enable</b> |
| Trap Destination 2   | <input type="text" value="0.0.0.0"/>         | <input type="checkbox"/> <b>Enable</b>            |
| Read-Only Community  | <input type="text" value="public"/>          |   |
| Read-Write Community   | <input type="text" value="private"/>         |   |

- An SNMP manager station at the ISO headquarters is assigned to receive information from the *IN-tact* devices by entering its IP address into the **Manager Address** and **Trap Destination** fields. Multiple SNMP managers may be utilized - one for traps, one for gets and sets, depending on network configuration, by enabling the second **Manager Address** and **Trap Destination** fields
- The community name fields are required to identify the *IN-tact* devices to the SNMP manager. These values are discretionary names selected for use and synchronized with the SNMP manager.

**NOTE:** If the *IN-tact* is behind a NAT firewall, ports 80 and 443 will require port forwarding in order to access the web interface of the *IN-tact* 1101. To use SNMP remote management, additional setup of the router may be required. SNMP port addresses 161 and 162 will need to be accessible. You may also have to configure Virtual Server Settings within the router to set up both ports 80 and 443 as TCP for the web interface, and ports 161 and 162 as UDP for SNMP access. Refer to the router documentation for more information on performing these setup items.

## Determining the NII Value from a Terminal

An important part of configuring the IN-tact 1101 is determining any NII codes in use. The NII code is used to route transactions from the terminal to the correct host processor. In the IN-tact 1101, this configuration is done on the **IN-tact Setup > Application Setup > Host Port Settings** screen.



APPLY AND RESTART   SAVE AND CONTINUE   CANCEL   HELP   PRINT

**IN-tact** :: Host Port Settings October 21, 2004

To configure your Host Port Settings, please use the fields below.

| NII | Description     | Enabled                             | Connection Type |         |
|-----|-----------------|-------------------------------------|-----------------|---------|
| 021 | Acme Processing | <input checked="" type="checkbox"/> | Standard        | Edit... |
| 016 | PaymentMaster   | <input checked="" type="checkbox"/> | HTTP            | Edit... |
| 001 |                 | <input type="checkbox"/>            | Standard        | Edit... |
| 001 |                 | <input type="checkbox"/>            | Standard        | Edit... |
| 001 |                 | <input type="checkbox"/>            | Standard        | Edit... |
| 001 |                 | <input type="checkbox"/>            | Standard        | Edit... |
| 001 |                 | <input type="checkbox"/>            | Standard        | Edit... |
| 001 |                 | <input type="checkbox"/>            | Standard        | Edit... |

In some cases, all terminals may route to a single processor. In other cases (like this example), multiple processors may be used. Knowing the correct NII codes to use becomes even more critical in these cases. For customers who do not use NII routing, this procedure can be ignored.

By defining and enabling multiple host processors, the end-user terminals send POS transactions to the destination specified in the NII portion of the TPDU sent from the terminal per each transaction. The use of the NII value allows those terminals initialized with the same NII to be matched for transmission of all traffic to the associated primary IP address. Other entries on the screen define the IP address or URL used for routing, whether or not an SSL configuration is needed (encryption and authentication are required to be performed by the IN-tact device), and whether the connection is established on a permanent or on-demand basis.

The NII value can be extracted from the terminal by doing a hex dump. The hex dump can be forwarded to the ISO or support center that is configuring the IN-tact 1101.

## Performing a Hex Dump

To perform a hex dump on a terminal:

### ICE Series Terminals

1. Enter function 99 on the terminal.
2. Enter the password = 028510.
3. Press the **Init TBL** key.
4. Press the **Print** key.

The terminal will now start printing a hex dump.

### T Series Terminals

1. Enter function 99 on the terminal. Press **Enter**.
2. Enter the password = 028510. Press **Enter**.
3. Enter 99 again. Press **Enter**.

The terminal will now start printing a hex dump.

## Determining the NII's in Use

To determine the NII's in use from the hex dump:

1. Locate the first data segment labeled "Acquirer ID". There will be a separately labeled data segment for each host processor being used. You will need to extract the NII for each processor being used. In some cases, there may be no NII (all zeroes).

In the data segment, there are four phone number fields. There are easily identified because each one is followed by a series of "FF" bytes. These generally occupy the first four rows.

2. At the end of the "FF" bytes, count seven more bytes into the hex datastream (remember, a hex byte is two characters).

The next two bytes (four characters) identify the NII. In most cases, the NII bytes appear on the fifth row and start with the seventh character. See the following example:

**Example Terminal Data Segment Showing NII Location**

```

AQUIRER ID:01
NASHVILLE NASHVILLE
RAW DATA (HEX BYTES)
01014E41534856494C4C45204E41534856494C4C
452018002319082FFFFFFFFFFFFFFFF300118002319
082FFFFFFFFFFFFFFFF300118002319082FFFFFFFF
FFFF300118002319082FFFFFFFFFFFFFFFF30010000
Row 5 → 00000000023031323334353620303030303030
Seventh Character ↑
3032383835333538300000000000000000000000
000000000000000000000003100000000000003120
2020202020202020202020202020202020202020
2020202020202020202020202020202020202020
202020
    
```



---

## Chapter 8: SNMP Traps

---

### Overview

The IN-*tact* 1101 SNMP agent is capable of sending out traps (asynchronous notifications) to the configured SNMP manager IP addresses. SNMP manager addressing is configured on the **System Setup > Management** screen. See page 24 for details on configuring this option. Each trap includes the following fields:

| Field         | Description   |
|---------------|---|
| enterprise    | Identifies the subsystem that generated the trap. The value is taken from sysObjectID in the system group (MIB-II).   |
| agent-addr    | The IP address of the object generating the trap.   |
| generic-trap  | One of the predefined trap types: <ul style="list-style-type: none"><li>• coldStart (0): The sending entity is reinitializing itself so that the agent's configuration or the protocol-entity implementation may be altered. Typically, this is an unexpected restart due to a crash or major fault.</li><li>• warmStart (1): The sending entity is reinitializing itself so that neither the agent's configuration nor the protocol-entity implementation is altered. Typically, this is a routine restart.</li><li>• linkDown (2): Signals a failure in one of the agent's communication links.</li><li>• linkUp (3): Signals that one of the agent's communication links has come up.</li><li>• authenticationFailure (4): Signals that the sending entity has received a protocol message that failed authentication.</li><li>• egpNeighborLoss (5): Signals that an EGP neighbor for which the sending protocol entity was an EGP peer has been marked down and the peer relationship no longer exists.</li><li>• enterpriseSpecific (6): Signifies that the sending entity recognizes that some enterprise-specific event has occurred. The specific-trap field indicates the type of trap.</li></ul> |
| specific-trap | A code that more specifically indicates the nature of the trap.   |

| Field             | Description   |
|-------------------|---|
| time-stamp        | The time between the last initialization of the network entity that issued the trap and the generation of the trap. |
| variable_bindings | Additional implementation-specific information relating to the trap.  |

---

## SNMP Usage

SNMP requests act on a variable-per-variable basis. However, in most cases, you will want to modify multiple variable first, then after all the changes are done, submit the whole configuration and apply all of the changes at the same time. To accomplish this, the following provisions were made:

- SNMP Get requests are served from the actual configuration the device is using
- SNMP Set requests are cached by the SNMP agent and retained until the configuration is committed
- An additional MIB variable is included in the System Configuration group to let the user control the edition operation. The variable name is configEditionControl and its possible values are:
  - noAction
  - editing
  - applyCfgChanges
  - discardCfgChanges

### Changing a Configuration

To begin a configuration change, you can modify a variable in the System Configuration group. The SNMP agent automatically changes the configEditionControl value to “editing”. A timer starts to give you a period of time to use the SNMP interface for configuration changes. This expires after 30 minutes of no activity. A detailed explanation of this timeout feature is described below.

Another possibility is to manually set the configEditionControl value to “editing” before changing any other variable. The resulting behavior is the same.

Once an edition has started, you can modify as many variables as needed. When all of the changes have been made, set the configEditionControl value to “applyCfgChanges”. This tells the SNMP agent to validate the cached configuration and, if successful, commit it to flash.

Before committing a configuration to flash, it is validated. If correct, it is saved and the device resets. If there is a problem with the validation, the MIB variable “lastSNMPErrors” contains the error code and the MIB variable “lastSNMPErrorsString” contains the corresponding error message. You can obtain these values using SNMP Get requests. The SNMP agent keeps the cached configuration in memory, so you can review and fix the problem, then try to commit again.

## Setting the configEditionControl Variable

Once the configEditionControl variable is set to “editing”, it cannot be set to the same value. A second request to do so will fail. This mechanism helps avoid collisions by different managers when changing a configuration. You can also get the current value for this variable to verify that no one else is using the SNMP interface for configuration changes.

The configEditionControl variable can also be set to “discardCfgChanges” to make the SNMP agent disregard any changes cached so far.

If the period of time specified by the timer elapses without any new SNMP Set request received by the SNMP agent, all of the changes cached so far are disregarded and configEditionControl is changed to “noAction” automatically.

**NOTE:** Setting time on the IN-*tact* 1101 via SNMP resets the device. Any other “sets” you may have made and not committed via “applyCfgChanges” will be lost. Therefore, always set time as a separate operation if configuring the device with an SNMP manager. You can then make any other configuration changes as necessary and commit them when ready.

## Trap Definitions

The following traps can be sent to the SNMP manager to alert you to possible problems. The “System Error” trap can indicate many different conditions; the specific error is denoted by a four-digit code within the text of the trap message. These messages are used by Hypercom Engineering to diagnose specific problems within the IN-*tact* 1101. The following System Error Code table correlates the error code to problem description.

| Trap                              | File Name                   | Description  |
|-----------------------------------|-----------------------------|--|
| TCP Connection Failed (1)         | (trapTCPConnFailed)         | Issued due to a TCP connection failure while attempting to make a connection   |
| SSL Failure (2)                   | (trapSSLFailure)            | Issued when an SSL failure occurs. Includes certificate authentication failure or any other denial of service during negotiation           |
| Permanent connection lost (3)     | (trapPermanentConnLost)     | Issued when an unexpected disconnect from a host occurs while in permanent mode  |
| Message routed to default NII (4) | (trapMsgRoutedToDefaultNII) | Issued when a message is sent to the default NII while in embedded routing mode  |
| Message discarded (5)             | (trapMsgDiscarded)          | Issued when an undeliverable, non-routable message is discarded based on discard option set or loss of terminal with transaction in flight |
| Invalid Host Message (6)          | (trapInvalidHostMessage)    | Issued when an improperly formatted message is received from a host  |

| Trap                               | File Name                    | Description   |
|------------------------------------|------------------------------|---|
| Switched to Alternate Host (7)     | (trapSwitchedToAlternate)    | Issued when switching to alternate IP address due to loss of keep alive or loss of TCP session when in permanent TCP mode                                     |
| Invalid Terminal Message (8)       | (trapInvalidTerminalMessage) | Issued when an improperly formatted message is received from a terminal   |
| Terminal Poll Lost (9)             | (trapTerminalPollLost)       | Issued when a transition from receiving responses to SDLC poll to no response is detected   |
| Terminal Poll Restored (10)        | (trapTerminalPollRestored)   | Issued when a transition from no poll response to receiving a poll response is detected   |
| Admin Logged In (11)               | (trapAdminLoggedIn)          | Issued whenever anyone logs in to the IN- <i>tact</i> 1101 using the "admin" User ID and password   |
| Admin Logged Out (12)              | (trapAdminLoggedOut)         | Issued whenever "admin" logs out of the IN- <i>tact</i> 1101  |
| Admin Password Changed (13)        | (trapAdminPasswordChanged)   | Issued whenever the password for the User ID "admin" is changed   |
| Session Timed Out (14)             | (trapSessionTimedOut)        | Issued when the five-minute timer expires during a session. The session is closed and the user is logged out  |
| Maximum Failed Login Attempts (15) | (trapMaxFiledLoginAttempts)  | Issued whenever the three consecutive failed attempts were made to log in to the IN- <i>tact</i> 1101   |
| System Error (99)                  | (trapSystemError)            | Issued when the device detects an unexpected condition. A four-digit code within the trap identifies the unexpected condition. Refer to the Error Code table. |

## SNMP Variables Used for Setting Time

The following variables are provided in order to use SNMP to configure SNTP:

| Variable                   | Description  |
|----------------------------|--|
| SntpStatus                 | Read-write variable with two choices: enabled and disabled.  |
| TimeZone                   | Read-write variable. Refer to the Time Zone Table for SNMP to determine the numerical identifier of the time zone you wish to set. |
| PrimaryNTPServerFromDHCP   | Read-only variable. Displays the primary NTP server assigned by DHCP, if any.  |
| AlternateNTPServerFromDHCP | Read-only variable. Displays the alternate NTP server assigned by DHCP, if any.  |
| NtpServersSearchOrder      | Read-write variable with two choices: dhcpFirst and staticFirst.   |
| StaticPrimaryNTPServer     | Read-write variable. IP address or name of static primary NTP server.  |

| Variable                    | Description   |
|-----------------------------|---|
| StaticAlternateNTPServer    | Read-write variable. IP address or name of static alternate NTP server. |
| SntpSynchronizationInterval | Read-write variable. Integer with valid values from 1 through 24.       |

For manual time synchronization, the SynchronizeSNTP variable can be used. It is a read-write variable with noAction and synchronize as its values.

## System Error Codes

| Error Code | Error Description   | SNMP Trap |
|------------|---|-----------|
|            | <b>Event Logger Events</b>                                  |           |
| 00-00      | Bad log message -- invalid subsystem 0x%x                   | Yes       |
| 00-01      | Bad log message -- invalid ordinal 0x%x for subsystem 0x%x  | Yes       |
|            |   |           |
|            | <b>Kernel Events</b>  |           |
| 01-00      | Assert failed in function %s line %d                        | Yes       |
| 01-01      | Configuration saved -- restarting                           | Yes       |
| 01-02      | System error -- restarting                                  | Yes       |
| 01-03      | Reverting to default configuration                          | Yes       |
| 01-04      | Reverting to factory default                                | Yes       |
| 01-06      | Start: LAN MAC %s IP %s                                     | Yes       |
|            |   |           |
|            | <b>SDLC Events</b>  |           |
| 02-05      | Unable to remove header prior to sending rx data to client  | Yes       |
| 02-06      | Initial offset too large for the buffer                     | Yes       |
| 02-07      | Initial length too large for the buffer                     | Yes       |
| 02-08      | Unable to format buffer from pool %d                        | Yes       |
| 02-09      | Error attempting to add a header to a buffer                | Yes       |
| 02-10      | Retrieved an application frame which is not a buffer Msg %d | Yes       |
| 02-11      | Mailbox %d is full -- message discarded                     | Yes       |
| 02-12      | Unable to acquire buffer from pool %d                       | Yes       |
| 02-13      | Internal state error for address %02x eDropState=0x%2x      | Yes       |
| 02-14      | Unable to cancel POSIX resource %d                          | Yes       |
| 02-15      | Retrieved an invalid event message %x                       | Yes       |
| 02-16      | Error reading from HDLC -- %s                               | Yes       |
| 02-17      | Invalid length %d bytes read from HDLC                      | Yes       |
|            |   |           |
|            | <b>SCC Event</b>  |           |
| 03-00      | Receive buffers exhausted. Frame discarded.                 | Yes       |
|            |   |           |

| Error Code | Error Description   | SNMP Trap |
|------------|---|-----------|
|            | <b>TCP/IP/Ethernet Interface Events</b>   |           |
| 04-08      | Ethernet link lost - If the dial backup link is not established when the Ethernet link is lost, this message appears only in the Event Log, but not in the syslog or SNMP trap destination. | Yes       |
| 04-09      | Ethernet link restored  | Yes       |
| 04-11      | Received invalid length 0x%04X from %s:%d. Restarting session   | Yes       |
|            |   |           |
|            | <b>Web Server Event</b>   |           |
| 05-06      | Configuration file imported from %s   | Yes       |
|            |   |           |
|            | <b>HLAN to IP Events</b>  |           |
| 06-00      | Improperly formatted message from terminal %02x -- message discarded  | Yes       |
| 06-03      | Transaction memory full   | Yes       |
| 06-04      | Open error on subsystem %d  | Yes       |
| 06-05      | Mailbox full for NII %3X  | Yes       |
| 06-06      | Unable to route data from TCP for destination index %02X%02X  | Yes       |
|            |   |           |
|            | <b>Log Interface Events</b>   |           |
| 08-01      | Invalid Registry IFace fields @addr:0x%08x  | Yes       |
| 08-02      | Get requested @addr:0x08x%08x for illegal Item ID=0x%08x  | Yes       |
| 08-03      | Get requested @addr:0x%08x for invalid subrange - Item ID=0x%08x  | Yes       |
| 08-06      | Put requested @addr:0x%08x for invalid subrange - Item ID=0x%08x  | Yes       |
| 08-07      | Illegal data interface usage from @addr:0x%08x  | Yes       |

## Time Zone Table for SNMP

| Time Zone   | Displayed Name       | Numerical Identifier |
|---|----------------------|----------------------|
| (GMT - 12:00) Eniwetok, Kwajalein                               | Pacific/Kwajalein    | 1                    |
| (GMT - 11:00) Midway Island, Samoa                              | Pacific/Midway       | 2                    |
| (GMT - 10:00) Hawaii  | US/Hawaii            | 3                    |
| (GMT - 09:00) Alaska  | US/Alaska            | 4                    |
| (GMT - 08:00) Pacific Time (US & Canada); Tijuana               | US/Pacific           | 5                    |
| (GMT - 07:00) Arizona   | US/Arizona           | 6                    |
| (GMT - 07:00) Chihuahua, La Paz, Mazatlan                       | America/Chihuahua    | 7                    |
| (GMT - 07:00) Mountain Time (US & Canada)                       | US/Mountain          | 8                    |
| (GMT - 06:00) Central Time (US & Canada)                        | US/Central           | 9                    |
| (GMT - 06:00) Mexico City, Tegucigalpa                          | America/Mexico_City  | 10                   |
| (GMT - 06:00) Saskatchewan                                      | Canada/Saskatchewan  | 11                   |
| (GMT - 05:00) Bogota, Lima, Quito                               | America/Bogota       | 12                   |
| (GMT - 05:00) Eastern Time (US & Canada)                        | US/Eastern           | 13                   |
| (GMT - 05:00) Indiana (East)                                    | US/East-Indiana      | 14                   |
| (GMT - 04:00) Atlantic Time (Canada)                            | Canada/Atlantic      | 15                   |
| (GMT - 04:00) Caracas, La Paz                                   | America/Caracas      | 16                   |
| (GMT - 04:00) Santiago  | America/Santiago     | 17                   |
| (GMT - 03:30) Newfoundland                                      | Canada/Newfoundland  | 18                   |
| (GMT - 03:00) Brasilia  | America/Sao_Paulo    | 19                   |
| (GMT - 03:00) Buenos Aires, Georgetown                          | America/Buenos_Aires | 20                   |
| (GMT - 02:00) Mid-Atlantic                                      | America/Noronha      | 21                   |
| (GMT - 01:00) Azores  | Atlantic/Azores      | 22                   |
| (GMT - 01:00) Cape Verde Is.                                    | Atlantic/Cape_Verde  | 23                   |
| (GMT) Casablanca, Monrovia                                      | Africa/Casablanca    | 24                   |
| (GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London    | Europe/London        | 25                   |
| (GMT + 01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna  | Europe/Amsterdam     | 26                   |
| (GMT + 01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague | Europe/Belgrade      | 27                   |
| (GMT + 01:00) Brussels, Copenhagen, Madrid, Paris               | Europe/Brussels      | 28                   |
| (GMT + 01:00) Sarajevo, Skopje, Warsaw, Zagreb                  | Europe/Sarajevo      | 29                   |
| (GMT + 01:00) West Central Africa                               | Africa/Bangui        | 30                   |
| (GMT + 02:00) Athens, Istanbul, Minsk                           | Europe/Athens        | 31                   |
| (GMT + 02:00) Bucharest   | Europe/Bucharest     | 32                   |
| (GMT + 02:00) Cairo   | Africa/Cairo         | 33                   |
| (GMT + 02:00) Harare, Pretoria                                  | Africa/Harare        | 34                   |
| (GMT + 02:00) Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius     | Europe/Helsinki      | 35                   |

| Time Zone   | Displayed Name     | Numerical Identifier |
|---|--------------------|----------------------|
| (GMT + 02:00) Jerusalem                             | Asia/Jerusalem     | 36                   |
| (GMT + 03:00) Baghdad                               | Asia/Baghdad       | 37                   |
| (GMT + 03:00) Kuwait, Riyadh                        | Asia/Kuwait        | 38                   |
| (GMT + 03:00) Moscow, St. Petersburg, Volgograd     | Europe/Moscow      | 39                   |
| (GMT + 03:00) Nairobi                               | Africa/Nairobi     | 40                   |
| (GMT + 03:30) Tehran                                | Asia/Tehran        | 41                   |
| (GMT + 04:00) Abu Dhabi, Muscat                     | Asia/Muscat        | 42                   |
| (GMT + 04:00) Baku, Tbilisi                         | Asia/Baku          | 43                   |
| (GMT + 04:30) Kabul                                 | Asia/Kabul         | 44                   |
| (GMT + 05:00) Ekaterinburg                          | Asia/Yekaterinburg | 45                   |
| (GMT + 05:00) Islamabad, Karachi, Tashkent          | Asia/Karachi       | 46                   |
| (GMT + 05:30) Chennai, Kolkata, Mumbai, New Delhi   | Asia/Calcutta      | 47                   |
| (GMT + 05:45) Kathmandu                             | Asia/Katmandu      | 48                   |
| (GMT + 06:00) Almaty, Novosibirsk                   | Asia/Almaty        | 49                   |
| (GMT + 06:00) Astana, Dhaka                         | Asia/Dhaka         | 50                   |
| (GMT + 06:00) Sri Jayawardenepura                   | Asia/Colombo       | 51                   |
| (GMT + 06:30) Rangoon                               | Asia/Rangoon       | 52                   |
| (GMT + 07:00) Bangkok, Hanoi, Jakarta               | Asia/Bangkok       | 53                   |
| (GMT + 07:00) Krasnoyarsk                           | Asia/Krasnoyarsk   | 54                   |
| (GMT + 08:00) Beijing, Chongqing, Hong Kong, Urumqi | Asia/Hong_Kong     | 55                   |
| (GMT + 08:00) Irkutsk, Ulaan Bataar                 | Asia/Irkutsk       | 56                   |
| (GMT + 08:00) Kuala Lumpur, Singapore               | Asia/Kuala_Lumpur  | 57                   |
| (GMT + 08:00) Perth                                 | Australia/Perth    | 58                   |
| (GMT + 08:00) Taipei                                | Asia/Taipei        | 59                   |
| (GMT + 09:00) Osaka, Sapporo, Tokyo                 | Asia/Tokyo         | 60                   |
| (GMT + 09:00) Seoul                                 | Asia/Seoul         | 61                   |
| (GMT + 09:00) Yakutsk                               | Asia/Yakutsk       | 62                   |
| (GMT + 09:30) Adelaide                              | Australia/Adelaide | 63                   |
| (GMT + 09:30) Darwin                                | Australia/Darwin   | 64                   |
| (GMT + 10:00) Brisbane                              | Australia/Brisbane | 65                   |
| (GMT + 10:00) Canberra, Melbourne, Sydney           | Australia/Canberra | 66                   |
| (GMT + 10:00) Guam, Port Moresby                    | Pacific/Guam       | 67                   |
| (GMT + 10:00) Hobart                                | Australia/Hobart   | 68                   |
| (GMT + 10:00) Vladivostok                           | Asia/ Vladivostok  | 69                   |
| (GMT + 11:00) Magadan, Solomon Is., New Caledonia   | Asia/Magadan       | 70                   |
| (GMT + 12:00) Auckland, Wellington                  | Pacific/Auckland   | 71                   |
| (GMT + 12:00) Fiji, Kamchatka, Marshall Is.         | Pacific/Fiji       | 72                   |
| (GMT + 13:00) Nukualofa                             | Pacific/Tongatapu  | 73                   |



---

## IN-*tact* 1101 MIB

The MIB used by the SNMP agent within the IN-*tact* 1101 can be downloaded from the Hypercom website at <http://www.hypercom.com>. It is in the Products/IP Gateway device section of the site.

**World Headquarters/****North America:**

Hypercom Corporation  
2851 W. Kathleen Road  
Phoenix, Arizona 85053,  
USA  
[www.hypercom.com](http://www.hypercom.com)

Tel: +1.602.504.5000  
Fax: +1.602.866.5380

**HYC Latin America:**

Hypercom Industria e Comercio LTDA  
Centro Empresarial Atibaia  
Rodovia Dom Pedro 1, KM 07, 5 Av.  
Tegula, 888-Ponte Alta  
Atibaia 12940-000, Brazil

Tel: +55.11.4417.7000  
Fax: +55.11.4417.7060

**HYC EMEA:**

Hypercom EMEA  
Unit 2, Woking Eight  
Forsyth Road  
Woking, GU21 5SB,  
United Kingdom

Tel: +44.1483.718600  
Fax: +44.1483.718601

**HYC Asia:**

Hypercom Asia  
21/F Metro Centre II  
21 Lam Hing Street  
Kowloon Bay, Kowloon  
Hong Kong

Tel: +85.2.2561.6800  
Fax: +85.2.2561.5890

©2004 Hypercom Corporation, all rights reserved. Hypercom and the Hypercom logo are registered trademarks of Hypercom Corporation. Optimum is a trademarks of Hypercom Corporation. All other products or services mentioned in this document are trademarks, service marks, registered trademarks or registered service marks of their respective owners.

Celebrating 26 years of technology excellence, innovation and leadership, Hypercom Corporation is a leading global provider of electronic payment solutions that add value at the point-of-transaction for consumers, merchants and acquirers, and yield increased profitability for its customers. Widely recognized as the global payment technology innovator, Hypercom delivers comprehensive card payment terminal, network and server solutions that help merchants and financial institutions generate revenues and increase profits.

Headquartered in Phoenix, Arizona, Hypercom's card payment terminal, network and server solutions are leading the transformation of electronic payments in more than 100 countries.

