



# 4100U/4100/4120/4020 SafeLINC™ Fire Panel Internet Interface (FPII) Operating Instructions

## Introduction

This publication describes how to operate the Fire Panel Internet Interface (FPII) for the 4100U, 4100, 4120, and 4020 Fire Alarm Systems. Once you perform initial configuration of the FPII per the FPII Installation and Setup Instructions (579-349), you can always refer back to Publication 579-349 as needed for further configuration/installation information. Following the instructions in this publication allows you to finalize configuration of the FPII.

## Inspecting Contents of Shipment

Upon unpacking your Simplex product, inspect the contents of the carton for shipping damage. If damage is apparent, immediately file a claim with the carrier and notify Simplex.

## In this Publication

This publication discusses the following topics:

Topic	See Page
Cautions, Warnings, and Regulatory Information	2
Introduction to the FPII	3
Getting Started	4
The Title Page and Common Operations	5
Email Configuration	8
Security Settings	11
The Title Page and Custom Links	12
Updating Firmware	13
The Summary Screen	15
General Operations	16
Viewing System, Card, and Point Reports	18
Basic Reports	20

# Cautions, Warnings, and Regulatory Information

---

**READ AND SAVE THESE INSTRUCTIONS.** Follow the instructions in this operating manual. These instructions must be followed to avoid damage to this product and associated equipment. Product operation and reliability depends upon proper installation.



**ELECTRICAL HAZARD** - Disconnect electrical power when making any internal adjustments or repairs. Servicing should be performed by qualified Simplex Representatives.



**STATIC HAZARD** - Static electricity can damage components. Therefore, handle as follows:

- Ground yourself before opening or installing components (use the 553-484 Static Control Kit).
- Prior to installation, keep components wrapped in anti-static material at all times.

---

## Caution to the User

The user is cautioned that any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

---

## Service Requirements

In the event of equipment malfunction, all repairs should be performed by Simplex or an authorized agent. It is the responsibility of users requiring service to report the need for service to our Company or to one of our authorized agents. Service can be facilitated through our office at:

Simplex  
Westminster, MA 01441  
Telephone: (978) 731-2500

---

# Introduction to the FPII

---

## Overview

The Fire Panel Internet Interface (FPII) is a module that interfaces to a 4100U, 4100, 4120 (limited models), or 4020 FACP, and it provides the following:

- Ability to access FACP data using Internet Explorer 5.0+ web browser.
- Ability to send e-mail message for prioritized event notification and Dirty/Excessively Dirty detector status information. (The FPII functions as an information kiosk that's accessible via the Internet rather than as a remote annunciator.)

This publication describes the various features of the FPII card and how to operate them. (For setup and configuration of the FPII, refer to Publication 579-349.)

### Notes:

- It is strongly recommended that your operating system and browser contain the latest patch updates.
  - The FPII is for ancillary use only and does not increase the burglary grade of service for the system.
- 

## Requirements

To use the FPII properly, you must meet the following requirements:

- Win98, NT, or 2000 Operating System
  - Internet Explorer (IE) 5.0+ web browser
  - FACP System Firmware: V9.02.02, 10.61, 11.02, or greater
  - 4100U, 4100, 4120, or 4020 FACP
- 

## Assumptions

This publication assumes that you've already successfully completed initial configuration of the FPII per Publication 579-349 (FPII Installation and Setup Instructions). It also assumes that you are able to access the FPII through your assigned DNS name. In addition, it assumes that you are able to log into the FPII and send a test email message to your configured account. When you are able to verify receipt of the test email message via your email account, you are then ready to finalize configuration of the FPII using this publication.

---

# Getting Started

---

## Logging In

To access the FPII, point your web browser to the assigned DNS name that's recorded on the IT Configuration Worksheet (see Publication 579-349 for completed worksheet). For example, if your DNS name is `fpii.your_domain.com`, then point your web browser to [http://fpii.your\\_domain.com/](http://fpii.your_domain.com/) to access the FPII homepage.

**Note:** You may need to adjust your proxy settings in your browser depending on how your MIS/IT Department has configured the network. Because it's difficult to predict all possible configurations, consult with your MIS/IT Department on how to make adjustments to these settings.

On the Primary Login dialog, enter the username and password that have been assigned to you. Then click the Enter button. Use the Reset button to clear the fields if necessary.



**Figure 1. The Primary Login Box**

**Note:** If no other accounts have been created, then you must log in using the User 1 account information recorded on the MIS/IT Configuration worksheet.

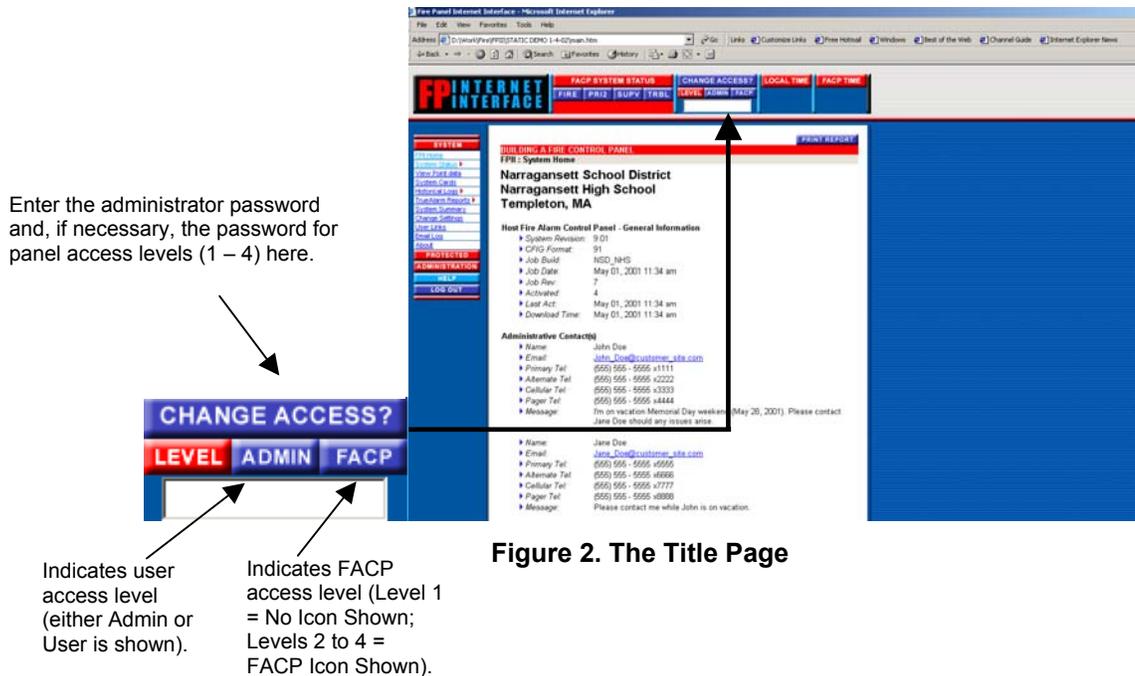
---

# The Title Page and Common Operations

## Configuring the FPII

Once you log in, the Title Page comes up, along with the standard FPII menus and buttons. This section briefly describes the homepage, as well as the menus and options that are available by default.

1. When the title page appears, enter the password into the Change Access box near the top of the screen.



2. If you need to enter an additional password for panel access levels 1 through 4, enter the password into the Change Access box.

**Note:** If you want to change the administrator password, refer to “Changing the Administrator Password” under “Configuring User Accounts” later in this publication.

## The Title Page

The FPII Title Page is the first page users see upon logging into the system. It consists of the following:

- Title information entered on the Custom Links screen
- Print Report button and hyperlink
- Summary of panel information
- Summary of all users designated as Administrators.

*Continued on next page*

# The Title Page and Common Operations, *Continued*

## The Administration Menu



<b>ADMINISTRATION</b>
FPII Administration ▼
<a href="#">Login Accounts</a>
<a href="#">Email Configuration</a>
<a href="#">Security Settings</a>
<a href="#">Customize Links</a>
<a href="#">Update FPII</a>
<a href="#">Summary</a>

For users who have entered the administrative password into the Change Access box, the Administration menu is also on the left side of the screen, under the System menu. The Administration menu contains the following options:

**Login Accounts.** Gives the administrator access to all accounts. Accounts can be configured, edited, and deleted on this screen. Refer to “Configuring User Accounts.”

**Email Configuration.** Lets the administrator set up the email server and customize event messages. Refer to “Email Configuration.”

**Security Settings.** Lets the administrator configure lockout delay, number of login retries, logout duration, address blocking, and more. Refer to “Security Settings.”

**Customize Links.** Contains fields that correspond to the links and information on the Title Page. Refer to “The Title Page and Custom Links.”

**Update FPII.** Allows the administrator to update FPII firmware. Refer to “Updating Firmware.”

**Summary.** Shows a general system summary. Refer to “The Summary Screen.”

## Overview

To set up or edit a user account, or to change the administrator password, click on the Administration icon before clicking the Login Accounts link on the Administration menu. Then follow the instructions in the sections below

## Setting Up a User Account

To set up a user account,

1. Click the Add User button near the bottom of the Login Accounts screen.
2. Enter the basic user information into the Account Configuration fields on the Primary Login Database Entry screen.
  - Username and password are case-sensitive and cannot contain spaces.
  - Username and password must be 6 to 20 characters long.
3. Use the drop-down list boxes in the Account Maintenance section to complete the user setup.
  - Only the primary administrator (User 1) can grant administrative privileges.
  - A disabled account cannot be used until an administrator enables it again.
4. Enter a custom message (if necessary). Custom messages can be up to 180 characters long. You may think of a custom message as a personal outgoing message that appears whenever your name appears.
5. Click the Update button. You are now returned to the Login Accounts screen.

**Note:** The FPII can support a maximum of 20 user accounts.

*Continued on next page*

# The Title Page and Common Operations, *Continued*

## Setting Up a User Account, *Continued*

**Note:** A verification dialog appears if you choose to delete an account. You cannot recover an account once it is deleted.

The Account Information section of the Login Accounts screen now reflects the user settings. A sample account is shown below.

Configured Users		Status	Admin Privileges	Emergency Contact
#	Username User Email			
1.	<a href="#">John Doe</a> <a href="#">John_Doe@customer-site.com</a>	<input checked="" type="checkbox"/> Enabled <input type="checkbox"/> Disabled	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	<input checked="" type="checkbox"/> Fire <input checked="" type="checkbox"/> Supv <input checked="" type="checkbox"/> Pri2 <input checked="" type="checkbox"/> Trbl
2.	<a href="#">Jane Doe</a> <a href="#">Jane_Doe@customer-site.com</a>	<input checked="" type="checkbox"/> Enabled <input type="checkbox"/> Disabled	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	<input checked="" type="checkbox"/> Fire <input checked="" type="checkbox"/> Supv <input checked="" type="checkbox"/> Pri2 <input checked="" type="checkbox"/> Trbl
40.	<a href="#">Jim Doe</a> <a href="#">Jim_Doe@customer-site.com</a>	<input checked="" type="checkbox"/> Enabled <input type="checkbox"/> Disabled	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	<input checked="" type="checkbox"/> Fire <input checked="" type="checkbox"/> Supv <input checked="" type="checkbox"/> Pri2 <input checked="" type="checkbox"/> Trbl

**Figure 3. User Information**

## Adding/Editing a User Account

To edit a user account, click the name of the account you want to edit to bring up the Primary Login Database Entry screen, as shown in Figure 3 (above). To add a new user, click on the Add User icon.

## Changing the Administrator Password

The administrator (User 1) has exclusive control over the administrator password. To change the administrator password, follow the prompts in the *Change Administrator's Password* section of the screen. Note that passwords must be between 6 and 20 characters long and cannot contain any spaces. Usernames and passwords are case-sensitive.

**Note:** The Administrator's password is shared among multiple designated Administrators.

**IMPORTANT:** For maximum security, change the Administrator's password often, especially when a user is no longer an employee.

**HINT:** If you forget the administrator's password or login information for the User 1 account, you can reset/override these options via the boot prompt on the Diagnostic Port. You should contact your Simplex representative to assist you in making this change.

*Continued on next page*

# Email Configuration

## Overview

This section describes how to set up the email server, and how to modify custom email messages for all the five types of events.

To set up the email server and configure the text messages sent with each mail, click the Email Configuration item on the Administration menu. Then follow the instructions below.

## Configuring the Email Server

To configure the email server:

1. Use the worksheet to enter information into the configuration fields.
2. Click the Send Test Email hotlink to test your configuration. Click Send Test Email on the verification dialog.



Figure 4. Test Email Box

## Disabling Outgoing Email

When servicing the host FACP, you may choose to globally disable outgoing FPII email to halt unnecessary event email traffic. Click on the Disabled radio button (see figure below) to disable outgoing FPII email. While email is disabled, a reminder email is sent to all FPII administrators once every 24 hours (around 5:30 a.m. daily).

### Disable Outgoing Email

When servicing the host FACP, you may want to globally disable outgoing FPII email to prevent unnecessary event email traffic. A reminder email shall be sent to all FPII configured administrators once every 24 hours around 5:30 am daily until the outgoing FPII email is re-enabled.

The Email Configuration must be operational for this feature to have any affect on the FPII.

Outgoing FPII Email is Currently:  Enabled  Disabled

SMTP Mail Server IP Address:  Port:

FPII Email Account Address:  [Send Test Email](#)

Figure 5. Disabling Outgoing Email

## Email Configuration, *Continued*

### Configuring the Email Health Status Check

To configure the email health status check, you need to enter the time interval (in minutes) to specify how minutes will pass before the FPII checks the configured email server again for proper email connectivity. Clicking the Update button applies your setting. See the figure below.

#### Email Health Status Check

The FPII periodically checks the configured email server specified above to ensure that the FPII email capability is properly maintained. Should the FPII fail to connect to the configured email server, then the status shall be reported under System Summary in the System sub-menu. Specify the checking interval below.

Email Health Status Check Interval:  min (5-30 minutes; default = 15 minutes)

**Figure 6. Email Health Status Check**

### Customizing Event Messages

To customize the messages that will be sent each time an event occurs:

- In the Event Message Customization section of the Email Configuration screen, click the desired message type in the Edit Message column as shown in Figure 7.
  - The Customize Event Message dialog comes up.

	Edit Message	View Message	Send Test Event Email
Click the desired link to change the message configuration for that link.	<a href="#">Fire</a>	<input type="checkbox"/> <a href="#">Default</a> <input checked="" type="checkbox"/> <a href="#">Custom</a>	Test <a href="#">Fire</a> Event Email
	<a href="#">Priority2</a>	<input type="checkbox"/> <a href="#">Default</a> <input checked="" type="checkbox"/> <a href="#">Custom</a>	Test <a href="#">Priority2</a> Event Email
	<a href="#">Supervisory</a>	<input checked="" type="checkbox"/> <a href="#">Default</a> <input type="checkbox"/> <a href="#">Custom</a>	Test <a href="#">Supervisory</a> Event Email
	<a href="#">Trouble</a>	<input checked="" type="checkbox"/> <a href="#">Default</a> <input type="checkbox"/> <a href="#">Custom</a>	Test <a href="#">Trouble</a> Event Email
	<a href="#">FPII Security</a>	<input type="checkbox"/> <a href="#">Default</a> <input checked="" type="checkbox"/> <a href="#">Custom</a>	Test <a href="#">FPII Security</a> Event Email

**Figure 7. Message Table**

- Use the “System shall use:” drop-down list to select either a custom or default message for all messages of this event type. If you select Custom Message, enter the message into the text box. Messages can be up to 480 characters long.
- Click the Update button.
  - Custom messages are appended to the default messages.
  - Custom messages may contain special instructions to other FPII users.

### Understanding Email Event Notification

Since email event notification operates differently according to the event message being sent, a description of each event notification is given below.

**Fire and Priority2** - For event types FIRE and PRIORITY2, one email is sent immediately to all actively configured users who’ve elected to receive FIRE and/or PRIORITY2 event email. This message always takes priority over all other system events.

**Supervisory** - When a Supervisory event occurs, a 30-second timer in the FPII begins. During this time interval, all supervisory events are collected and combined into a single email message. When the 30-second timer expires, the FPII completes the email message by sending it to all actively configured users who've elected to receive supervisory event email. Supervisory event email is only superseded by Fire and Priority2 events, which take precedence. The process is repeated until no more supervisory events are detected.

*Continued on next page*

## Email Configuration, *Continued*

---

### **Understanding Email Event Notification, *Continued***

**Trouble** - When a Trouble event occurs, a 30-second timer in the FPII begins. During this time interval, all trouble events are collected and combined into a single email message. When the 30-second timer expires, the FPII completes the email message by sending it to all actively configured users who've elected to receive trouble event email. Trouble event email is only superseded by Fire and Priority2 events, which take precedence. The process is repeated until no more trouble events are detected.

**FPII Security Violations** - Sent to all configured FPII administrators who've elected to receive these event types, this message is sent out immediately upon detecting the event (like a Fire or Priority2 event). A Security Violation message is only superseded by Fire and Priority2 events, which take precedence. If the FPII is in the locked state as a result of a security violation, it will unlock for any of the four events: Fire, Priority2, Supervisory, and Trouble. This feature permits the configured users to immediately gain access to the system if needed.

---

# Security Settings

---

## Overview

The administrator can configure security settings, such as lockout delay, number of retries for logging in, and IP address blocking.

To customize the security settings, click the Security Settings item on the Administration menu. Then follow the instructions below.

---

## Security Settings

Enter or select the required security settings.

**Automatic Lockout Delay.** The Lockout Delay period is the amount of time the FPII can remain idle before logging the user out and returning the host FACP to the lowest access level (3-30 minutes; default is 10 minutes).

**Note:** The FPII returns to the host FACP at the lowest login level after 10 minutes of inactivity, or when the user logs out or is automatically logged out.

**Login Retries.** Specify the number of incorrect logins (1-20 times; default is 3 times) allowed before the FPII enters lockout. (All users will be unable to log in during lockout.)

**FPII Lockout Duration.** Specify the amount of time each lockout will last (0-24 hours; default is 1 hour).

**Note:** If an event occurs while the FPII is in the lockout state, the lockout duration expires upon detecting the event that allows users to log in.

**Local Configuration Options.** These options specify whether you must configure the FPII on the same sub-domain on which the FPII resides, or on any domain. For example, if the FPII is at 192.168.0.1 and you are accessing the FPII from 193.168.0.2 with the “Local” option enabled, you would not be able to modify the IP blocking features. The same rule applies to Email and User Account options. To disable the “Local” option, you must access the FPII on the same sub-domain (for example: 192.168.0.4 is on the same sub-domain as 192.168.0.1).

*Configure IP blocking locally.*

*Configure email accounts locally.*

*Configure user accounts locally.*

**Network Status Check.** Specify a time interval (in minutes) for when the FPII checks for the presence of its configured network gateway. (With 30 minutes being the default interval, you can change the interval anywhere from 0 minutes to 4 hours. Entering 0 minutes disables this feature.)

Although this feature does not guarantee that the entire network is operational, it does confirm that the FPII can communicate on the network.

**IP Address Blocking.** Enter one or more IP addresses from which users will *not* be able to access the FPII. Separate each address with a semicolon. You can use a wildcard (asterisk [\*]) as a wildcard that denotes any number or numbers). For example, 192.168.0.\* will block out 192.168.0.0 through 192.168.0.255.

Use this feature to lock out undesired and problematic users.

When you have completed the settings, click the Update button at the bottom of the screen. If you wish to reset the screen to the default settings, click the Reset button.

---

# The Title Page and Custom Links

## Setting Up the Title and User Links Pages

Any Administrator can set up the title page (the page that comes up when you click FPII Home in the System Menu) and the user links page (which comes up when you click User Links in the System Menu). The title page and the links page are both configurable from the Custom Links screen.

To set up the title and user links pages, click the Customize Links item on the Administration menu. Then follow the instructions on the screen.

The panel location description appears in the red bar at the top of the screen.

The title fields are typically used to describe the building or facility in which the panel is installed.

Enter an address to appear as a link on the User Links page.

Enter a description to appear below the link.

The screenshot shows the 'BUILDING A FIRE CONTROL PANEL' interface. At the top right is a 'PRINT REPORT' button. Below the title bar, the page is titled 'FPII : FPII Administration : Custom Links'. The 'Customize Your Title Page' section contains three text input fields: 'Line 1: Narragansett School District', 'Line 2: Narragansett High School', and 'Line 3: Templeton, MA'. The 'Specify Your Panel Location' section has a text input field containing 'BUILDING A FIRE CONTROL PANEL'. The 'Custom Links' section contains two link entries. 'Link 1' has the URL 'http://www.customer-site.com/maintenance/' and a description 'Customer-site Maintenance Website - Here you'll find the latest information on the emergency procedures as governed by this'. 'Link 2' has the URL 'http://www.simplexgrinnell.com/' and a description 'The SimplexGrinnell Website is where you'll find the latest information and datasheets for both the Simplex and Grinnell products currently installed at your facility.' Each link entry includes a character count (50 Characters Maximum) and a remaining character count (180 Characters Maximum).

Figure 8. Custom Links Screen

When you are done entering the information, click the Update button at the bottom of the screen. If you wish to blank out all the fields, click the Reset button.

# Updating Firmware

## Overview

The administrator has the capability of updating system firmware. This section covers this capability.

## Firmware Update Procedure

**Note:** To minimize any chance of error, reboot the system before performing this procedure.

Be sure to read this procedure carefully before you attempt to update the firmware in the FPII. Failure to do so may render the FPII inoperable. To avoid any mistakes, verify your entries carefully before pressing the Enter key.

**IMPORTANT:** Only experienced administrators or Simplex Technical Representatives should use the Update FPII screen. Improper use of the Update FPII screen may render the FPII inoperable.

1. Log into the FPII using any Administrator-enabled account.
2. Log in as the Administrator in the header area.
3. When the menu returns, click Administration and then Update FPII. You need to have logged in successfully to perform this step.
4. Now click the Start FTP Server. You should obtain the screen shown in Figure 9.

**Note:** The FPII reboots after 10 minutes of inactivity once the FTP Server is started. The system also reboots upon successful update of the FPII firmware.

**HINT:** If you accidentally start the FTP server, don't do anything and the FPII reboots after 10 minutes of FTP inactivity.

**BUILDING A FIRE CONTROL PANEL** PRINT REPORT

**FPII : FPII Administration : Update FPII (System Firmware)**

**Update FPII System Firmware**  
You can update the FPII System Firmware via the internet. It is strongly recommended that this feature be used by qualified personnel only. Failure to perform the procedure correctly may render the FPII inoperable.

**Starting the FTP Server**  
Using the button below, the FPII system shall issue a prompt to confirm the update of the system firmware by starting FTP Server. Starting the FTP server will allow the upload of the binary image firmware update to the FPII (host PC to FPII). **WARNING: DO NOT interrupt the FTP transfer in progress** once you have initiated the file transfer to the FTP Server as this may render the FPII inoperable. Once the FTP Server has started and the new firmware is successfully uploaded, then system will automatically reset. You will then need to log into the system for further access.

**Current Firmware Information**

- ▶ MAC Address: 00:50:BA
- ▶ Firmware Build: 1.01.00

Start FTP Server

Microsoft Internet Explorer

WARNING: You are about to Start the FTP Server to update the FPII Firmware. DO NOT interrupt the FTP transfer in progress once you have initiated the upload procedure, as this may render the FPII inoperable.

Do you really want to start the FTP Server?

Press Ok to Send Now or Cancel to stop the request.

OK Cancel

[Back to Top](#) | [Print Report](#)



Copyright ©2001-2002 SimplexGrinnell LP. All rights reserved. SIMPLEX and TRUEALARM are used by SimplexGrinnell under license from the trademark owner, ADT Services AG, an affiliated Tyco company.

Figure 9. Start FTP Server Verification Screen

Continued on next page

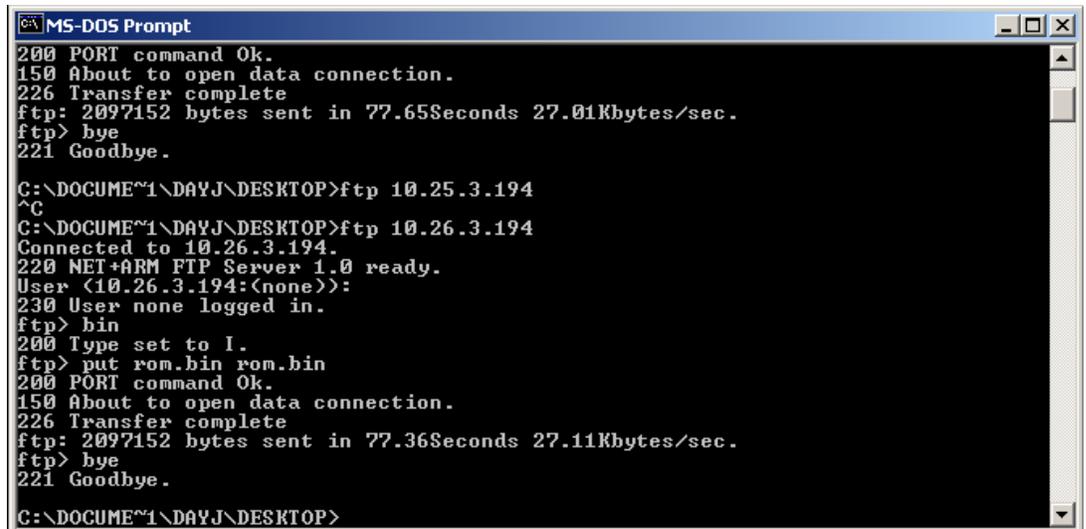
## Updating Firmware, *Continued*

### Firmware Update Procedure, *Continued*

5. In the dialog box, click OK to start the FTP Server. Observe the diagnostics port using your favorite Terminal program to see that a message appears about starting the FTP server (Starting FTP Server). Refer to Publication 579-349 (FPII Installation and Setup Instructions) if you require information on setting up the terminal program.
6. Now open up a DOS window. You will use DOS FTP to upload the new image.

**Note:** You must use DOS FTP to perform this procedure properly. Do not attempt to use another FTP program or your update procedure will fail.

7. Navigate to the same directory as the ROM.BIN image. The image should be in its own directory to minimize the chance of errors.
8. At the DOS prompt, type *ftp 10.26.3.194* (substituting the IP address of your FPII card for the IP address example of 10.26.3.194) and press <ENTER>. Figure 10 shows a snapshot of the DOS window from an update performed on a typical FPII card.



```
MS-DOS Prompt
200 PORT command Ok.
150 About to open data connection.
226 Transfer complete
ftp: 2097152 bytes sent in 77.65Seconds 27.01Kbytes/sec.
ftp> bye
221 Goodbye.

C:\DOCUME~1\DAYJ\DESKTOP>ftp 10.25.3.194
^C
C:\DOCUME~1\DAYJ\DESKTOP>ftp 10.26.3.194
Connected to 10.26.3.194.
220 NET*ARM FTP Server 1.0 ready.
User (10.26.3.194:(none)):
230 User none logged in.
ftp> bin
200 Type set to I.
ftp> put rom.bin rom.bin
200 PORT command Ok.
150 About to open data connection.
226 Transfer complete
ftp: 2097152 bytes sent in 77.36Seconds 27.11Kbytes/sec.
ftp> bye
221 Goodbye.

C:\DOCUME~1\DAYJ\DESKTOP>
```

**Figure 10. Typical DOS Window When Using DOS FTP**

9. At the *User (10.26.3.194:(none)):* prompt, press <ENTER>.
10. At the prompt, type *bin* and press <ENTER>. This command sets the file transfer mode to binary.
11. At the prompt, type *put rom.bin rom.bin* and press <ENTER>. Since this step is very important, make sure that you've typed it in correctly before pressing <ENTER>. The file transfer begins. Observe the dialog window. You should see the flash erase and then a series of counts writing 32k blocks. The counts stop at the number 64.
12. Back in the DOS window, you see the ftp prompt return. Type in *bye* then press <ENTER>. This command closes the ftp session with the FPII.
13. In the dialog window, you see *Download complete, rebooting...*
  - The FPII Update Procedure is now complete.

# The Summary Screen

## Viewing a Summary of Administrative Changes

For a summary of all administrative changes you've made, click the Summary item on the Administration menu. The following sections come up:

**Login Accounts.** In-depth user information appears in this section, as shown in the figure below.

Configured Users				
#	Username User Email	Account Status	Admin Privileges	Emergency Contact
1.	<a href="#">John_Doe</a> <a href="mailto:John_Doe@customer-site.com">John_Doe@customer-site.com</a>	<input checked="" type="checkbox"/> Enabled <input type="checkbox"/> Disabled	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	<input checked="" type="checkbox"/> Fire <input checked="" type="checkbox"/> Pri2 <input checked="" type="checkbox"/> Supv <input checked="" type="checkbox"/> Trbl
2.	<a href="#">Jane_Doe</a> <a href="mailto:Jane_Doe@customer-site.com">Jane_Doe@customer-site.com</a>	<input checked="" type="checkbox"/> Enabled <input type="checkbox"/> Disabled	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	<input checked="" type="checkbox"/> Fire <input checked="" type="checkbox"/> Pri2 <input checked="" type="checkbox"/> Supv <input checked="" type="checkbox"/> Trbl
40.	<a href="#">Jim_Doe</a> <a href="mailto:Jim_Doe@customer-site.com">Jim_Doe@customer-site.com</a>	<input checked="" type="checkbox"/> Enabled <input type="checkbox"/> Disabled	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	<input checked="" type="checkbox"/> Fire <input checked="" type="checkbox"/> Pri2 <input checked="" type="checkbox"/> Supv <input checked="" type="checkbox"/> Trbl

Figure 11. The Login Accounts Summary

**Email Configuration.** Lists email server IP address, port number, and account username.

**Event Message Customization – Message Status.** Lists whether the messages are custom or default.

**Security Settings.** Lists the settings made on the Security Settings screen.

**Custom Links.** Lists the contents of the Title Page, complete with hypertext custom links.

**Boot Prompt Configurables.** Lists the contents of the configurable items from the boot prompt. The MAC address is also displayed here, too. No passwords are shown.

# General Operations

## The System Menu

SYSTEM MENU
<a href="#">FPII Home</a>
<a href="#">System Status</a> ▶
<a href="#">View Point data</a>
<a href="#">System Cards</a>
<a href="#">Historical Logs</a> ▶
<a href="#">TrueAlarm Reports</a> ▶
<a href="#">System Summary</a>
<a href="#">Change Settings</a>
<a href="#">User Links</a>
<a href="#">Email Log</a>
<a href="#">About</a>

The System menu is always on the left side of the screen, regardless of the page you are on. The System menu contains the following options:

**FPII Home.** Opens the Title Page. Refer to the subtopic “The Title Page.”

**System Status.** *Click once to expand.* Opens information on Fire, Priority 2, Supervisory, or Trouble events, depending on which item you choose. Refer to the subtopic “Checking the System Status.”

**View Point Data.** Lists all the points in the system. Refer to the section “Viewing System, Card, and Point Reports.”

**System Cards.** Lists all the cards in the system. Refer to the section “Viewing System, Card, and Point Reports.”

**Historical Logs.** *Click once to expand.* Opens alarm and trouble logs. Refer to the section “Viewing System, Card, and Point Reports.”

**TrueAlarm Reports.** *Click once to expand.* Opens service and status reports. Refer to the section “Viewing System, Card, and Point Reports.”

**System Summary.** Lists some basic FPII and panel information. Refer to the section “Viewing System, Card, and Point Reports.”

**Change Settings.** Gives the user access to account settings (password, email, etc.).

**User Links.** Links to sites entered into the Custom Links page.

**Email Log.** A log of the last 25 emails sent by the FPII. This log is primarily used as a diagnostic tool during email configuration.

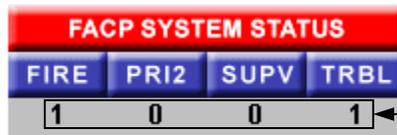
**About.** Basic information about the FPII.

## Checking the System Status

System Status ▼
<a href="#">Fire Events</a>
<a href="#">Priority 2 Events</a>
<a href="#">Supervisory Events</a>
<a href="#">Trouble Events</a>

An alternate way of getting event information is to expand the System Status menu and click one of the events.

You can always tell whether there is an urgent condition by looking at the numbers under the FIRE, PRI2, SUPV, and TRBL buttons on the top of the screen.



This example shows 1 Fire event, no Priority 2 or Supervisory events, and 1 Trouble.

**Figure 12. System Status Buttons**

Press any one of the four buttons for detailed information on the alarm, supervisory, or trouble event. The screen will display important information about the event, including the point address, the custom point description, how the event was triggered, and whether the event has been acknowledged. Emergency contacts are also shown, along with email, phone, and pager listings.

### Notes:

- All users that are designated as emergency contacts for the event selected will be shown following the display of specific event information.
- The events counts are not dynamically updated. They are updated the next time a web page is requested from the FPII. Think of them as snapshots of the panel.

**HINT:** To update the event counts, click on the FPII logo at the upper left of the page, or click on any of the four event icons shown in Figure 12.

*Continued on next page*

# General Operations, *Continued*

## Checking the System Status, *Continued*

Use "Panel Location" field in Custom Links screen to configure this description

### BUILDING A FIRE CONTROL PANEL FPIL : System Status : Fire Events

PRINT REPORT

#### Active Fire Event(s)

The active fire events are listed for your system below. Click on the hypertext custom label to obtain detailed information about the point shown.

Point Address & Custom Label:	Needs Acknowledgement?
2-234-1 <a href="#">M1-234</a>	NO
Banner: SMOKE DETECTOR	Status: FIRE
Point Address & Custom Label:	Needs Acknowledgement?
2-235-1 <a href="#">M1-235</a>	NO
Banner: MONITOR ZONE	Status: FIRE
Point Address & Custom Label:	Needs Acknowledgement?
2-236-1 <a href="#">M1-236</a>	NO
Banner: WATERFLOW MONITOR	Status: FIRE
Point Address & Custom Label:	Needs Acknowledgement?
128-233-0 <a href="#">REMINDER - FIRE ALARM(S) EXIST IN SYSTEM</a>	YES
Banner: FIRE ALARM POINT	Status: FIRE

Click on the Point Description for detailed information on the event.

#### Emergency Contact(s)

- ▶ Name: John Doe
- ▶ Email: [John\\_Doe@customer\\_site.com](mailto:John_Doe@customer_site.com)
- ▶ Primary Tel: (555) 555 - 5555 x1111
- ▶ Alternate Tel: (555) 555 - 5555 x2222
- ▶ Cellular Tel: (555) 555 - 5555 x3333
- ▶ Pager Tel: (555) 555 - 5555 x4444
- ▶ Message: I'm on vacation Memorial Day weekend (May 28, 2001). Please contact Jane Doe should any issues arise.
  
- ▶ Name: Jane Doe
- ▶ Email: [Jane\\_Doe@customer\\_site.com](mailto:Jane_Doe@customer_site.com)
- ▶ Primary Tel: (555) 555 - 5555 x5555
- ▶ Alternate Tel: (555) 555 - 5555 x6666
- ▶ Cellular Tel: (555) 555 - 5555 x7777
- ▶ Pager Tel: (555) 555 - 5555 x8888
- ▶ Message: Please contact me while John is on vacation.

Click the Email field to send an email to the emergency contact.

All users designated as emergency contacts for this event type are listed.

Figure 13. Event Screen

## Printing Reports

The contents of any given page can be printed out via the button in the upper right corner. The same option appears at the bottom of each page.

PRINT REPORT

- You can print out the data on the current page by clicking the PRINT REPORT button near the upper right side of the page, or by clicking the Print Report option at the bottom of the page. Refer to your browser documentation for information about printing.

# Viewing System, Card, and Point Reports

---

## Overview

The FPII web pages allow you to view general and specific system data. This section describes how to bring up summary data for the host panel, as well as individual cards and points.

---

## Viewing TrueAlarm Service Reports

To view TrueAlarm service reports, select TrueAlarm Reports: Service Report on the System menu.

TrueAlarm service reports display the device number and custom label for each point, as well as:

**Alarm At.** The percentage of a value/ number of units of a value (for example, smoke on a smoke detector) that the device needs to sense to go into alarm.

**Average Value.** The number of units of a value (for example, smoke on a smoke detector) that the device currently detects on average.

**Current/% Alarm.** The current number of units of a value/ percentage of a value (for example, smoke on a smoke detector) that the device currently senses.

**Peak/% Alarm.** The highest number of units of a value/ percentage of a value (for example, smoke on a smoke detector) that the device has sensed.

**Current State.** Shows the message the device is sending to the panel (Normal, Alarm, Trouble, Supervisory, No Response, etc.).

---

## Viewing TrueAlarm Status Reports

To view TrueAlarm status reports, select TrueAlarm Reports: Status Report on the System menu.

TrueAlarm status reports display the zone name and custom label for each point, as well as:

**Current Sensitivity.** The percentage of a value (for example, smoke on a smoke detector) that must be detected by the device to go into alarm.

**Current State.** Shows the message the device is sending to the panel (Normal, Alarm, Trouble, Supervisory, No Response, etc.).

**Almost Dirty.** Displays \*YES\* when the average device sensitivity is close to alarm levels. You must turn on P132 for this field to display data. Turning on P132 causes all Almost Dirty detectors to display a trouble at the panel.

---

## Viewing Point Summaries

**IMPORTANT: For all pages, you must wait until the page finishes loading before clicking on another link.**

To find information about a specific point, click the View Point Data item on the System menu.

A screen comes up, showing the expected point number formats for each type of point. Below the list of expected point formats is a list of card addresses and corresponding card types. Below that are a drop-down list and an empty number field.

Use the drop-down list to select the type of point you want a report on. Next, enter the point number, using the list of expected point number formats as a guide. Click Update to bring up the report.

The point report that comes up is identical to what you see if you had clicked on the point as a hyperlink. Refer to “Report Items” under “Basic Reports,” above.

---

*Continued on next page*

## Viewing System, Card, and Point Reports, *Continued*

---

### Viewing Card Summaries

To find information about a specific card, click the System Cards item on the System menu.

The System Cards screen comes up, showing the number and description for each card in the system.

Click on the hyperlink for a card to bring up a screen that lists every sub-point for that card, as well as each sub-point's status if applicable.

---

### Viewing the FPII/Host Panel Summary

For information about the FPII module and its host panel, click the System Summary item on the System menu.

The System Summary report includes the following information for those systems supporting these features:

**FPII – Status.** Lists statuses for the network, email, and FTP server.

**Host FACP – General Information.** Lists serial numbers for the FACP and system cards (if supported by the host FACP).

**Host FACP – Status.** Lists the status for slave communications.

---

### Viewing Alarm and Trouble Logs

You can view alarm and trouble logs with the FPII web pages.

- To view a log of past alarms, click Historical Logs: Alarm Logs on the System menu.
- To view a log of past troubles, click Historical Logs: Trouble Logs on the System menu.

Each log includes the time and location for each event that occurred.

---

# Basic Reports

---

## Overview

When you click on a Custom Label for any event, a screen comes up that summarizes the address corresponding to that label. This section explains the details of the summary report.

---

## Report Items

Here are some of the items that may be displayed whenever a system point is shown as a hyperlink.

**Current Device.** Displays whether the device is seen correctly by the system.

**Device.** The device status (Alarm, Trouble, Supervisory, No Answer, etc.).

**Test State.** Shows whether the device is self-testing, and the results of a self-test.

**Present Sensitivity Selected.** The percentage of a value (for example, smoke on a smoke detector) that must be detected by the device to go into alarm.

**Average Value.** The number of units of a value (for example, smoke on a smoke detector) that the device currently detects on average.

**Alarm Level.** The number of units of a value (for example, smoke on a smoke detector) that the device needs to sense to go into alarm.

**Value.** The current number of units of a value (for example, smoke on a smoke detector) that the device is detecting.

**Peak.** The highest number of units of a value (for example, smoke on a smoke detector) that the device has detected in the past.

**Trouble Threshold.** The value that the device needs to cause the display of a trouble message.

**Enabled State.** Shows whether the device is enabled or disabled. Devices may be enabled or disabled via the FPII.

**Unverified.** System points that are not returning a value.

---