4100U/4100/4120/4020 SafeLINC™ Fire Panel Internet Interface (FPII) Non-UL-Listed Protected Features User's Guide

Introduction

This publication describes how to use SafeLINC FPII **non-UL-listed** Protected Features. The Protected Features extend Fire Alarm Control Panel (FACP) command-and-control capabilities to the SafeLINC Website for supplementing the Information Kiosk Features. Some Protected Features are located in the Protected Features Menu while other Protected Features are contained in areas such as System Snapshot or Logs and Reports. Certain elements of the Protected Features may not be available to you depending on the capabilities of your host FACP and firmware revision.

In this Publication

This publication discusses the following topics:

Cautions and Warnings

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.

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 your local Simplex product supplier.

Service Requirements

In the event of equipment malfunction, all repairs should be performed by a representative or authorized agent of your local Simplex product supplier. It is the responsibility of users requiring service to report the need for service to your local Simplex product supplier.

Introduction to the SafeLINC FPII

Overview

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

- Ability to access FACP data using Internet Explorer (IE) 5.0+ web browser in conjunction with a Win98, ME, NT, or 2000 operating system.
- Ability to send email messages for prioritized event notification and Dirty/Excessively Dirty detector status information. (The SafeLINC FPII functions as an information kiosk that's accessible via the Internet rather than as a remote annunciator.)
- Ability to email reports for TrueAlarm Sensor Status, TrueAlarm Sensor Service, and historical logs (fire alarm, Priority 2 alarm, trouble, and supervisory).

This publication describes how to:

- Use the command-and-control items from the Protected Features menu.

Note: It is strongly recommended that both your operating system and web browser contain the latest patch updates.

Requirements

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

- Win98, ME, NT, or 2000 Operating System
- Internet Explorer (IE) 5.0+ web browser
- FACP System Firmware: V9.02.02, 10.61, 11.08, or greater (see table below)
- 4100U, 4100, 4120, or 4020 FACP

Table 1. FACP Firmware Revision Compatibility

Firmware Revision	FACP			
	4020	4100	4120	4100U
9.02.02 or greater	X	X		
10.61			X	X
11.08 or greater			X	X

Access Key

The SafeLINC FPII Protected Features are available as a separate firmware release and require an Access Key to enable the Protected Features (Command-and-Control functionality) in your SafeLINC FPII. Locate the label affixed to the accompanying CD-ROM jewel case. Select one of the three options listed; then follow the instructions provided for that option to obtain your Access Key.

Use the space below to record both your MAC Address and Protected Features Access key. Keep this information stored in a safe place for future reference.

MAC Address: **00 : 08 : BD :** _____ **Access Key:** _____

Once the Protected Features firmware image has been installed on your SafeLINC FPII even though the Access Key has *not* been correctly entered on the boot prompt, the SafeLINC FPII will continue to operate normally as an information kiosk. Under these circumstances, no host FACP command and control shall be permitted on the SafeLINC FPII web site.

WARNING: By installing this firmware, you acknowledge that this action voids the SafeLINC FPII UL (Underwriters' Laboratories) Listing! Be sure that you understand the ramifications of this action.

End-User License Agreement (EULA)

Ensure that you agree with the Protected Features EULA Agreement below before using the SafeLINC Protected Features.

End-User License Agreement (EULA) for Protected Features
Software Product License and Waiver of Liability. Important – Read Carefully.
1. **Grant of License.** By installing, copying or otherwise using this software product you agree to be bound by all terms of this end-user license agreement. You may not reverse engineer, decompile, or disassemble this software product. You may transfer this software and user documentation on a permanent basis provided the transferee agrees to accept the terms and conditions of this agreement and you discontinue all use of the product.
2. **Waiver of Liability.** By installing and using this software, you agree not to hold Tyco Electronics Products Group or any of its authorized sales agents responsible for system malfunctions, failures, and/or related problems due to actions based upon having remote Internet access to your fire panel or installed fire system. **This software provides enhanced operating features that are neither approved nor listed for use by Underwriters' Laboratories, Inc.** Use of this software should be restricted only to authorized and trained operators. Failure to do so may result in delayed fire responses. You further agree to release, not sue, and indemnify Tyco Electronics Products Group or any of its authorized sales agents from any and all losses, causes of actions, claims, suits, damages, and demands whatsoever in law or in equity which you or any other person may have against the above upon reason of events, acts, and/or occurrences arising out of or caused by the incorrect use of the SafeLINC Fire Panel Internet Interface Protected Features Software.

Copyright laws and international copyright treaties, as well as intellectual property laws and treaties protect the SafeLINC Fire Panel Internet Interface Enhanced Software. This software product is licensed and not sold.

Getting Started with the SafeLINC FPII Protected Features

Loading the Firmware

Please refer to Publication 579-349 (4100U/4100/4120/4020 SafeLINC Fire Panel Internet Interface [FPII] Installation, Setup, & Operating Instructions) for information on firmware updates and accessing the SafeLINC FPII boot prompt.

Follow the procedure for upgrading the SafeLINC FPII firmware using the firmware image provided on the accompanying CD-ROM. This procedure is outlined in the readme.txt file found in the root directory and varies according to the board revision of the SafeLINC FPII.

Once you have installed the Protected Features firmware, you will need to access the boot prompt to enter the Protected Features Access Key that you just obtained by following the procedure described in the previous section of this publication.

Configuring at the Boot Prompt

Before you begin, it is recommended that you erase the NVRAM prior to entering the Protected Features Access Key. However, erasing the NVRAM will restore the SafeLINC FPII to the factory defaults; therefore, you will have to re-enter all your user account information and MIS/IT configuration worksheet settings.

IMPORTANT: If you elect to erase NVRAM, please reconfigure the SafeLINC FPII using the configuration worksheet settings while making any required changes in the user accounts on the SafeLINC web site. (For a blank configuration worksheet, see the rear of this publication.) Once you have reconfigured the SafeLINC FPII, you may proceed to access the boot prompt.

At the SafeLINC FPII Boot Menu, select the option <P> to configure Protected Features. You will be prompted to enter your Access Key. Enter the unique key exactly as shown in Figure 1. It is case-sensitive and should not contain any spaces.

Continued on next page

Configuring at the Boot Prompt, *Continued*

The figure below shows the prompts that follow once you accept the EULA Agreement (see page 4). For the prompts that follow, you will answer Y or N to allow the ability to use the Protected Feature on the SafeLINC FPII website. For example, if you only enabled Clear Logs while leaving the remaining options disabled, then the administrator can only assign Clear Logs access on a per user basis via the SafeLINC FPII web site.

```
SafeLINC FPII Boot Menu
=======================
Choose an option below by pressing a key and then <Enter>:
<N> = Configure the SafeLINC FPII Subnet Mask
<G> = Configure the SafeLINC FPII Gateway
<I> = Configure the SafeLINC FPII Static IP Address
<A> = Configure the SafeLINC FPII Administrator Password
<U> = Configure the SafeLINC FPII 'User 1' Account
<P> = Configure Protected Features (Requires Access Key to Enable)
<H> = Help on the SafeLINC FPII Boot Prompt Options
<D> = Configure the SafeLINC FPII Boot-up Delay
<L> = View the SafeLINC FPII Email Log Entries
<B> = Save Current SafeLINC FPII Configuration Changes and Reboot
<S> = Summary of All SafeLINC FPII Boot Prompt Configurables
<Q> = Quit Without Making Changes and Re-Boot SafeLINC FPII
<E> = Erase SafeLINC FPII NVRAM and Restore Factory Default Settings

Cmd: p

Enter Protected Features Access Key: MB67HK89L2AG

Configure Protected Features
============================
Type Y to enable or N to disable access to the following protected features
on the SafeLINC FPII web site. Press <Enter> after each response:

Enable/Disable points (v9+)?......: y
Enable/Disable Points Option......: Enabled
Perform FACP Diagnostics (v10+)?..: y
Perform FACP Diagnostics Option...: Enabled
Clear Alarm & Trouble Logs (v9+)?.: y
Clear Alarm & Trouble Logs Option.: Enabled
Silence/Acknowledge Points (v9+)?.: y
Silence/Acknowledge Points Option.: Enabled
Restart FACP (v9+)?...............: y
Restart FACP Option...............: Enabled
System Reset (v9+)?...............: y
System Reset Option...............: Enabled
Hardware Reset (v10+)?............: y
Hardware Reset Option.............: Enabled
Remote CFIG Upload (v11.02+)?.....: y
Remote CFIG Upload Option.........: Enabled
Remote CFIG Download (v11.02+)?...: y
Remote CFIG Download Option.......: Enabled
Swap CFIG Data (v10+)?............: y
Swap CFIG Option..................: Enabled
Set FACP Date/Time (v9+)?.........: y
Set Date/Time Option..............: Enabled
```

Figure 1. After Accepting the EULA Agreement & Entering the Access Key

Continued on next page

Configuring at the Boot Prompt, *Continued*

When you have finished, use the option <S> to review your changes (go back and make changes as needed using the boot menu) before pressing <B> when you are ready to save the changes to NVRAM and reboot the SafeLINC FPII.

WARNING: Choose the Protected Features that you wish to make available on the web site because there is no means on the web site to make changes with this list. Changes to this list MUST be performed only at the boot prompt. This is done as a security measure to ensure that any web user cannot override these settings.

Note: Not all Protected Features are available on each revision of firmware. To obtain all the Protected Features, a 4100U system with Revision 11.08 or greater system firmware is required.

Observe the boot-up sequence. If the system is configured properly, you should observe something similar to the figure below. Allow the system to boot into operation.

```
SafeLINC Fire Panel Internet Interface (FPII) Boot Procedure in Progress:
SafeLINC FPII System Firmware Revision 2.00.21
SafeLINC FPII is operating with NON-UL APPROVED firmware.
SafeLINC FPII protected features access key is MB67HK89L2AG.

SafeLINC FPII Static IP Address...: 10.26.3.194
SafeLINC FPII Subnet Mask.........: 255.255.0.0
SafeLINC FPII Default Gateway.....: 10.26.1.254

HARDWARE PARAMETERS:
SafeLINC FPII MAC Address........: 00:08:BD:FF:FF:2D
SafeLINC FPII NVRAM Data Size....: 15423 bytes


**********************************************************************
Press any key in 5 seconds to enter the SafeLINC FPII boot prompt.
**********************************************************************
```

Figure 2. Boot-Up Screen Showing Proper System Configuration

Configuring the User Account for Protected Features

Log into the SafeLINC FPII using any administrator-enabled account. Next, log in as the administrator. Select account to Edit or Create New Account.

Item 13 now appears when the administrator is editing or creating a user account. Only the items that were enabled on the boot prompt appear in the list below. In the previous example, only ***Clear Logs*** would be shown and you have the option of assigning the user the privilege of clearing the logs.

NOTE: Only administrators can make changes to the Protected Features of each user account. Users cannot make these changes under Account Settings.

Figure 3. Screen Showing Account Item 13

Continued on next page

Configuring the User Account for Protected Features, *Continued*

When you have completed editing the user account, press update to save your changes. You will be returned back to the Login Accounts page where you can review the summary of changes for the account you've just edited.

Logging into the FACP

Certain Protected Features may require that you log into the host FACP to gain access. Login levels will vary by Protected Feature; therefore, you will need to log in at the appropriate level.

WARNING: Three unsuccessful login attempts to the host FACP will lock down the SafeLINC FPII for the configurable lockout duration. No access will be allowed during the lockout period.

Log into the host FACP as specified in the panel job configuration. See figure below.

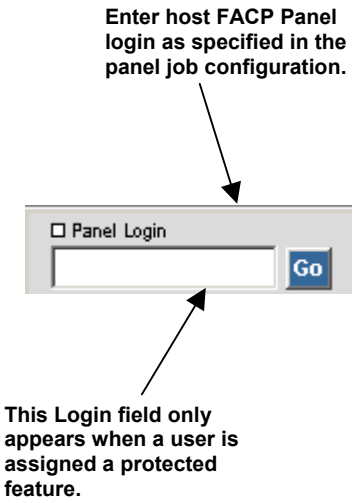

Figure 4. Panel Login Field

SafeLINC FPII Protected Features Menu

Menu Descriptions

Enabled by each individual feature on the boot prompt to allow host FACP command and control functionality on the SafeLINC FPII web site, the Administrator of the site assigns each feature on a per-user account basis on the web site. Certain elements of the Protected Features may not be available to you depending on the capabilities of your host FACP and firmware revision.

System Reset. Performs a System Reset to restore the host FACP to normal operation after an alarm event occurs. Refer to *Resetting Hardware or System and Restarting Panel* for more details.

Hardware Reset. Clears a Class A fault on the host FACP once the fault has been removed. Refer to *Resetting Hardware or System and Restarting Panel* for more details.

Panel Restart. Gives the user the ability to initiate either a Warm or Cold Start on the host FACP. Refer to *Resetting Hardware or System and Restarting Panel* for more details.

Set FACP Date/Time. Provides the ability to set the host FACP system time and date. Refer to *Setting the FACP Date/Time* for more details.

CFIG Operations. Allows the user the ability to Upload CFIG, Download CFIG, and Swap CFIG data on the host FACP. Refer to *Performing CFIG Operations* for more details.

Diagnostic Operations. Assists the user in locating Earth Faults and NAC wiring problems by providing a useful set of host FACP diagnostic utilities. Refer to *Performing Diagnostic Operations* for more details.

Note: Not all menu items will be shown. There are three things that determine what menu items are shown: configuration on the boot prompt, your host FACP and firmware, and what the SafeLINC administrator assigns for privileges for each user account.

Resetting Hardware or System, and Restarting Panel

The SafeLINC FPII provides several options to perform the following resets and restart capability:

Hardware Reset. Click on *Hardware Reset* to perform a reset of the host FACP hardware. This feature is useful in clearing a Class A fault once the fault has been removed. This reset requires a Level 2 login (Job Default) to the host FACP.

System Reset. Click on *Initiate System Reset* to perform a System Reset to restore the host FACP to normal operation after an alarm event occurs. This reset requires a Level 1 login (Job Default) to the host FACP. See figure below.

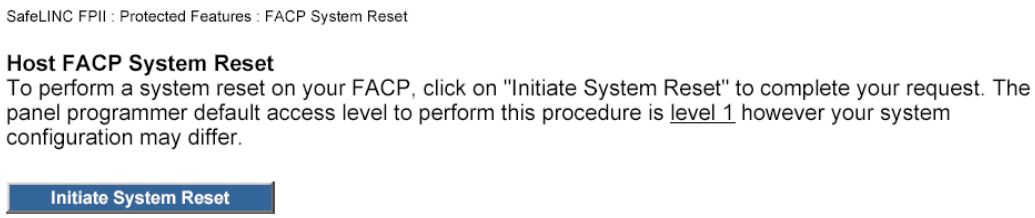

Figure 5. System Reset

Continued on next page

Resetting Hardware or System, and Restarting Panel, *Continued*

Panel Restart. Select the type of host FACP restart; then click on *Perform Restart*. This restart requires a Level 4 login (Job Default) to the host FACP. See figure below.

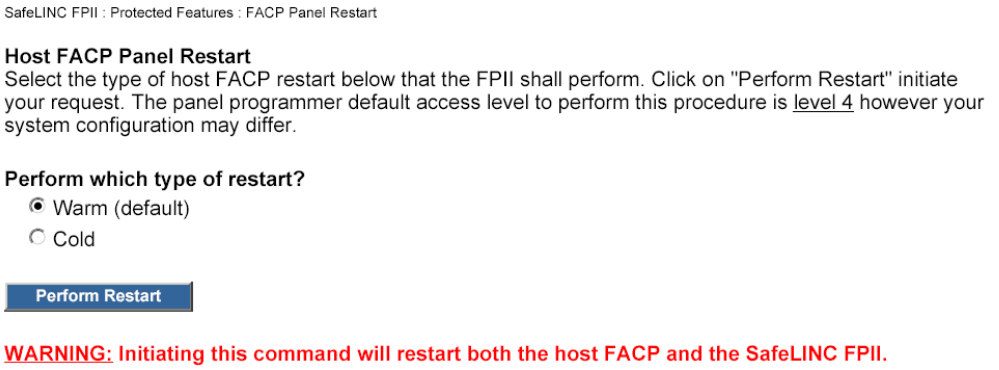

Figure 6. Panel Restart

Setting the FACP Date/Time

The current host FACP system time and date are shown in the boxes on the Set Date/Time web page. Modify the time and date shown; then click on *Update*. Use the *Auto Complete* button to automatically configure the boxes based upon your PC time and date. Then click on *Update*. This update requires Level 3 login (Job Default) to the host FACP. See figure below.

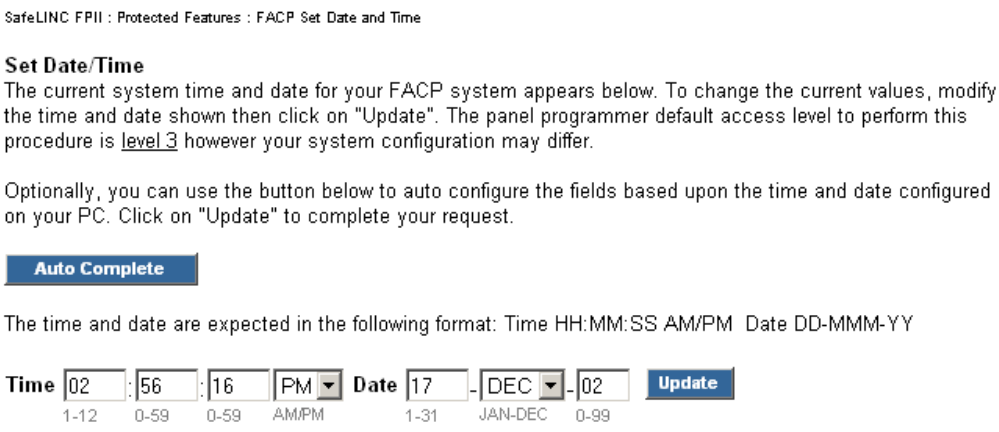

Figure 7. Set Date/Time

Performing CFIG Operations

RECOMMENDATION: It is recommended that you not perform CFIG operations to panels who have network and/or audio capabilities. Perform CFIG operations on standalone panels only.

Upload, Download, and Swap CFIG allow the user to upload (host FACP to client), download (client to host FACP), and swap job configuration data (CFIG) on the host FACP. With Upload and Download CFIG operations, Remote Download must be enabled via the front host FACP keypad interface. Level 4 login (Job Default) to the host FACP is required to use each feature.

Upload CFIG. Transfers the FACP job configuration data from the host FACP to the client PC via email. You can specify an additional email address to email the CFIG image to that specified email address. Requires Rev. 10 host FACP firmware, or better. See figure below.

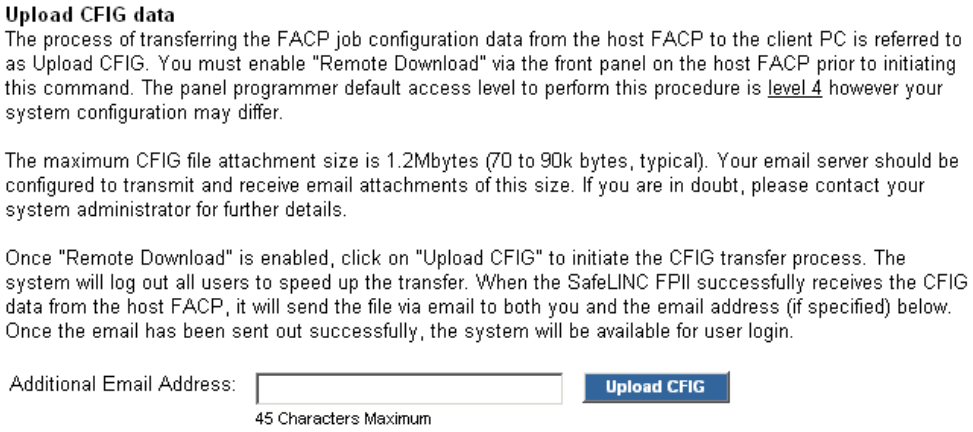

Figure 8. Upload CFIG Operation

Check your email approximately 20 minutes after you have initiated the CFIG Upload procedure for the SafeLINC FPII website. If the operation was successful, you should have received the email with the job file as the attachment.

NOTE: There are events that occur in the panel that may delay the CFIG Operation transfer process. For example, any active alarm condition (Fire or Priority2 event) will automatically pause the transfer procedure until the panel is restored to a non-alarm condition. Upon the clearing of the alarm events, the transfer operation will resume. If the transfer operation fails, you also will be notified via email of the results.

When you receive the email, open it and use the save attachment feature on your email client to recover the job file before saving it to a folder of your choosing. Starting in Programmer revision 11.08, you can use the "unbuild" feature to recover the job file that was sent to you in the .txt format. Refer to the Programmer documentation for further details on how to perform this procedure.

Continued on next page

Performing CFIG Operations, *Continued*

Download CFIG. Transfers the FACP job configuration data from the Client PC to the host FACP using FTP transfer. Requires Rev. 11 host FACP firmware, or better. See figure below.

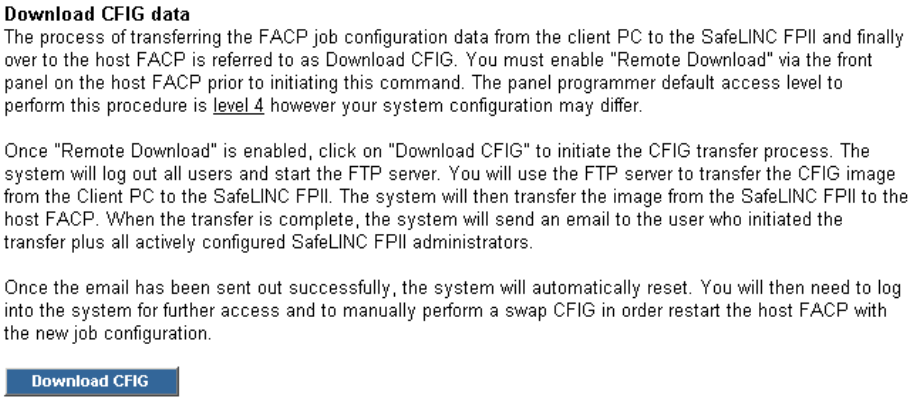

Figure 9. Download CFIG Operation

Once you've clicked on the Download CFIG button, a pop-up dialog box will appear as shown below to confirm your request.

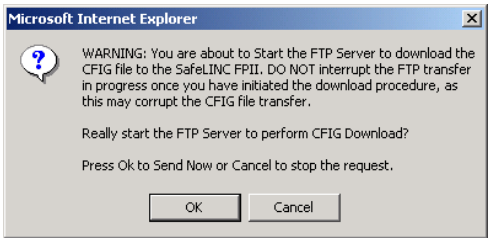

Figure 10. Ready to Start FTP Server

Click OK to start the FTP server. If you have access to the diagnostic port during this operation, you would observe the following output via your favorite terminal emulator:

```
The FTP Server is now awaiting login from any actively configured SafeLINC
FPII user. Open up a DOS window on your PC and navigate to the directory where
the new CFIG .txt file resides. At the DOS prompt in the same directory where
the CFIG .txt file resides, type in:

FTP IP_ADDRESS or DNS_NAME NOTE: Either method is acceptable.

Where IP_ADDRESS is in the form of ddd.ddd.ddd.ddd; d ranges from 0-9. Or,
is the assigned DNS name provided by the MIS/IT department.

Examples: FTP 192.168.0.1<ENTER>  or  FTP fpii.customer-site.com<ENTER>.

When prompted for the User, enter your SafeLINC FPII username. When prompted
for the Password, enter your SafeLINC FPII password. If the login succeeds,
enter BIN at the FTP prompt and press <ENTER>. Next, type PUT job-name.txt
substituting job-name.txt with your CFIG .txt file then press <ENTER>. When
the FTP prompt returns, type BYE to exit FTP and allow the SafeLINC FPII to
transfer the CFIG to the host FACP. If the login fails, type BYE at the FTP
prompt to exit out of FTP because you'll need to repeat the above steps.

SafeLINC FPII: Now Waiting for FTP client login...
```

Continued on next page

Performing CFIG Operations, *Continued*

Download CFIG (continued). Follow these instructions above to access the FTP server. You will interact with the FTP server to transfer the job file to the panel.

Check your email approximately 20 minutes after you have initiated the CFIG Download procedure and successfully transferred the job file to the SafeLINC FPII via FTP. If the operation was successful, you should have received the email notifying you of the results.

NOTE: There are events that occur in the panel that may delay the CFIG Operation transfer process. For example, any active alarm condition (Fire or Priority2 event) will automatically pause the transfer procedure until the panel is restored to a non-alarm condition. Upon the clearing of the alarm events, the transfer operation will resume. If the transfer operation fails, you also will be notified via email of the results.

WARNING: When the CFIG transfer is complete, a trouble will occur at the panel to inform you that a newer CFIG exists but has not been activated. You will need to perform Swap CFIG either via the front panel or via the SafeLINC FPII. ***The SafeLINC FPII will not perform the swap automatically once the transfer is complete. This feature was added for your protection.***

Swap CFIG Data. Allows you to swap the alternate (currently inactive) job configuration (CFIG) data with the Primary (currently active) job data. Requires Rev. 11 host FACP firmware, or better. See figure below.

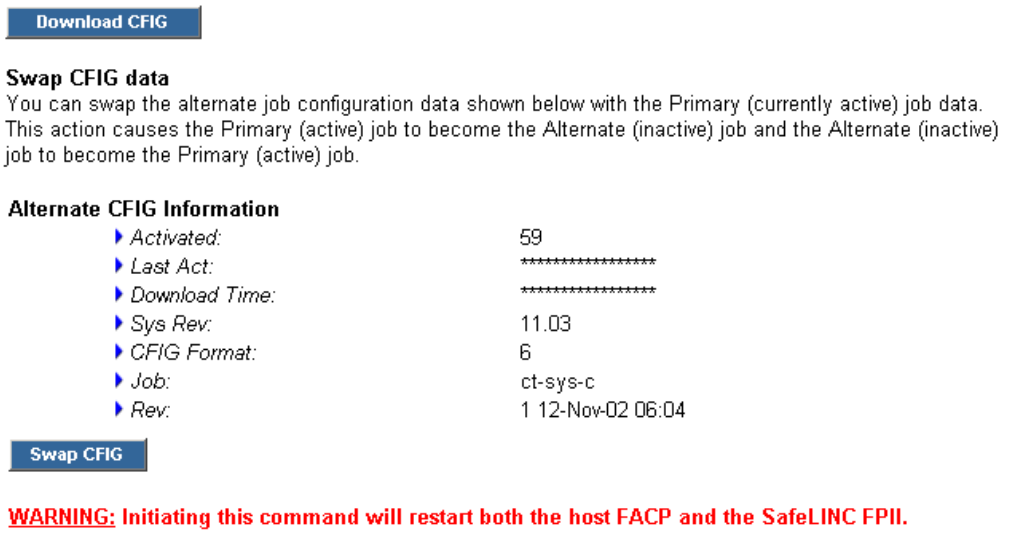

Figure 11. Swap CFIG Data Operation

SafeLINC FPII Protected Features Menu, *Continued*

Performing Diagnostic Operations

For users requiring host FACP diagnostic operations, see below for a description of a useful set of diagnostic utilities to assist the user in locating Earth Faults and NAC wiring problems. Level 2 login (Job Default) to the host FACP is required to use each feature. See figure below.

Earth Fault Latching. Earth Fault Latching provides the option of enabling or disabling Earth Faults on the host FACP. Requires Rev. 10 host FACP firmware, or better.

Earth Fault Searching. Earth Fault Search displays the current raw state of the earth statuses in the host FACP. Requires Rev. 10 host FACP firmware, or better.

NAC Test. The NAC test instructs all supported slave cards to perform a NAC wiring test and report the results. Requires Rev. 10 host FACP firmware, or better.

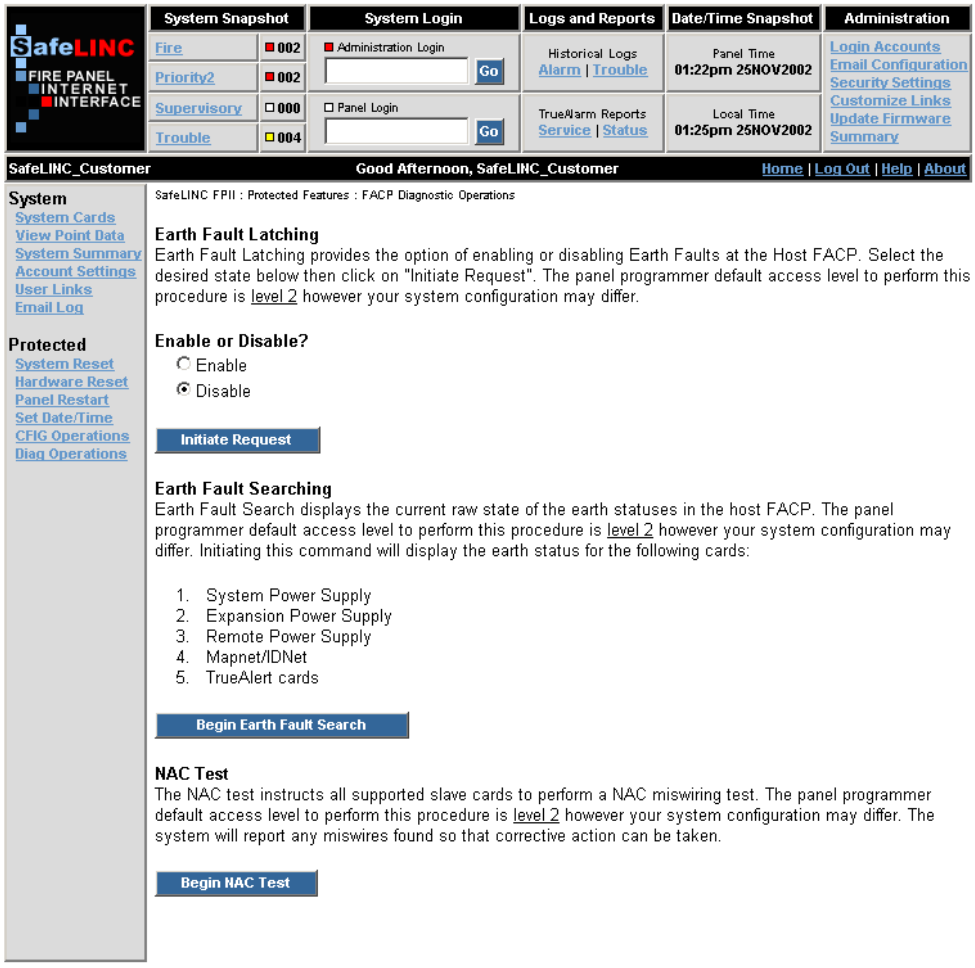

Figure 12. Perform Diagnostic Operations

Other SafeLINC FPII Protected Features

Clearing Alarm and Trouble Logs

Periodically, you may choose to clear the Alarm and Trouble Historical Log entries stored in your host FACP. It is recommended that you use the Email Log feature to email the desired log(s) prior to clearing the selected log. Level 3 login (Job Default) to the host FACP is required to use each feature.

Alarm Log. Located at the bottom of Alarm Historical Logs web page, this feature allows a user to clear the Alarm Historical Log. See figure below.

Trouble Log. Found at the bottom of Trouble Historical Logs web page, this feature allows a user to clear the Trouble Historical Log. See figure below.

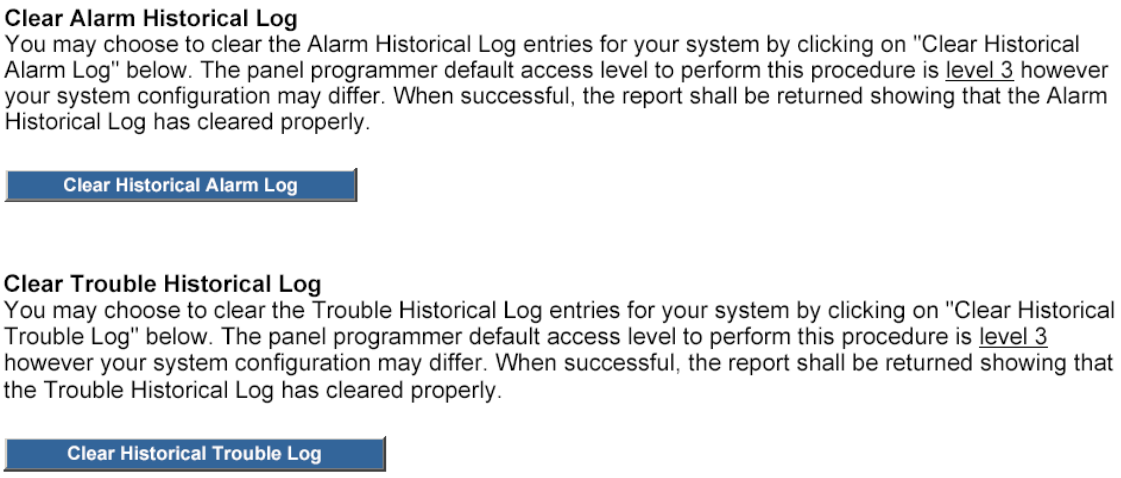

Figure 13. Clear Alarm and Trouble Logs

Silencing/ Acknowledging Points

All active system events are listed under the four events types: Fire, Priority2, Supervisory and Trouble. You have the capability to acknowledge specific system alarm events and silence the audible alarms. Level 1 login (Job Default) to the host FACP is required to use each feature.

WARNING: Make sure you fully understand the consequences of these actions. Failure to do so may result in LOSS OF LIFE. If you are uncertain, DO NOT USE these features.

Fire and Priority 2 Events. Use the *Silence* button to silence audible alarms on your host FACP. To acknowledge individual points shown in each event list, use the *Ack* button next to each point. If "Yes" appears next to the point, the point still requires acknowledgement but you do not have the required privileges (as assigned by your administrator) to acknowledge the point. See figure below for sample screen on acknowledging and silencing fire event points.

Supervisory and Trouble Events. To acknowledge individual points shown in each event list, use the *Ack* button next to each point. If "Yes" appears next to the point, the point still requires acknowledgement but you do not have the required privileges (as assigned by your administrator) to acknowledge the point.

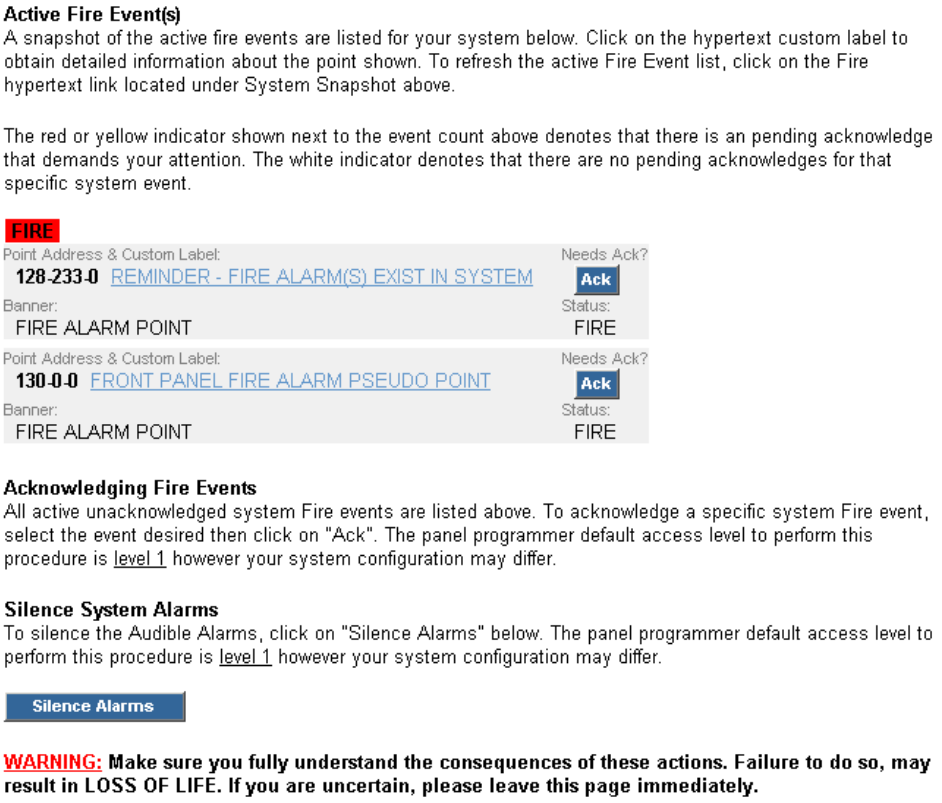

Figure 14. Silence/Acknowledge Fire Event Points

Continued on next page

Silencing/ Acknowledging Points, *Continued*

Supervisory and Trouble Events. To acknowledge individual points shown in each event list, use the *Ack* button next to each point. If "Yes" appears next to the point, the point still requires acknowledgement but you do not have the required privileges to acknowledge the point. See figure below for sample screen on acknowledging trouble event points.

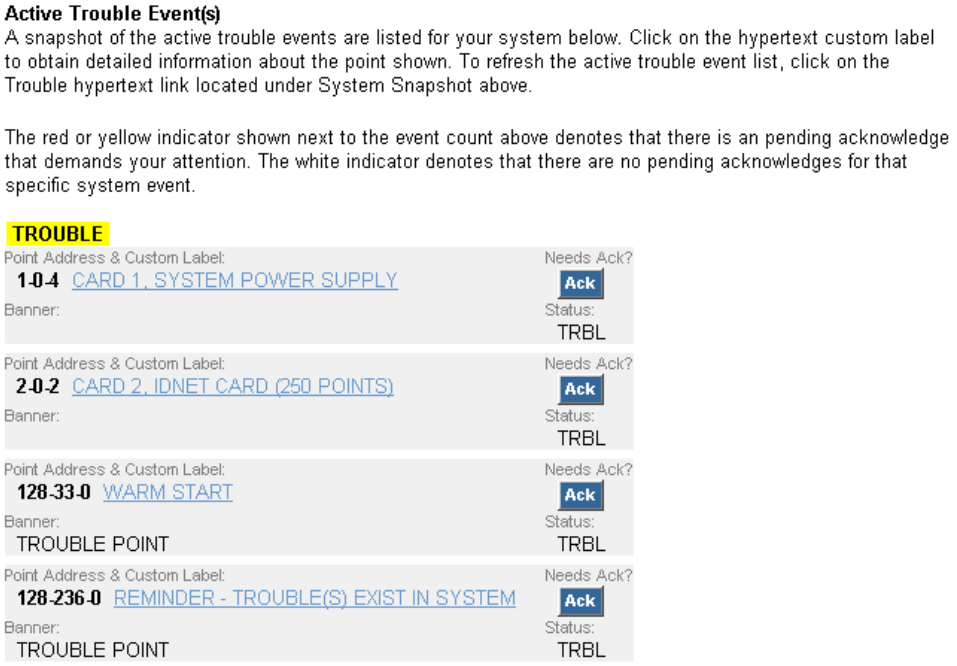

Figure 15. Acknowledge Trouble Event Points

NOTE: When the FACP is configured for Global Acknowledge, you must still acknowledge each point individually.

This feature was intended to make you think about your actions.

Enabling/Disabling Points

The SafeLINC FPII allows the user to view specific points on both local and remote (networked) host FACPs using the View Point Data web page. Using the same page, you may also change the status of each point queried if the Administrator enabled this feature in your account. Level 4 login (Job Default) to the host FACP is required to use this feature.

The SafeLINC FPII provides the ability to Enable or Disable points under the following web pages:

View Point Data. Query the specific point desired. To enable or disable the point returned, select the desired state before clicking on the *Update Point Status* button located near the bottom of the page.

Continued on next page

Enabling/Disabling Points, *Continued*

System Events Snapshot. When a point appears in any of the four host FACP system event lists, click on the point's custom label to obtain a detailed query for the selected point. When the point query results are returned, you are presented with the option to enable or disable the selected point. Select the desired state before clicking on the *Update Point Status* button located near the bottom of the page. See figure below

Service and Status Reports. Select the desired report before selecting the point by clicking on the point's custom label. When the point query results are returned, you are presented with the option to enable or disable the selected point. Select the desired state before clicking on the *Update Point Status* button located near the bottom of the page.

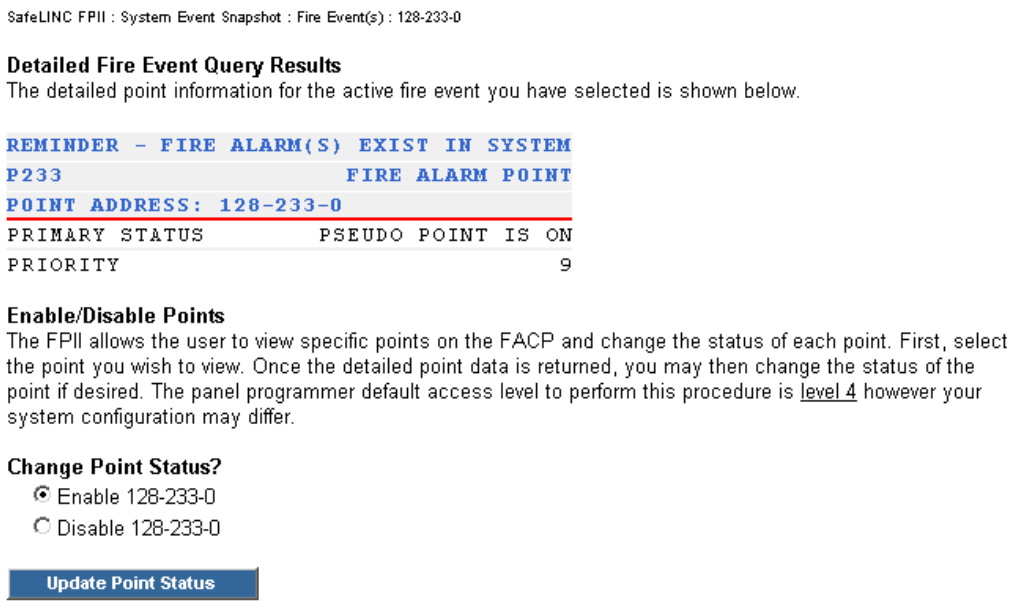

Figure 16. Enable/Disable Points

MIS/IT Configuration Worksheet

SafeLINC Fire Panel Internet Interface MIS/IT Configuration Worksheet

About the SafeLINC Fire Panel Internet Interface
The SafeLINC Fire Panel Internet Interface (FPII) is a module that mounts internally to a fire alarm control panel (FACP) located on your premises to provide the ability to access FACP information using the Internet Explorer 5.0+ web browser. The SafeLINC FPII has the ability to send FACP event notification via email and requires a SMTP email account to function properly. To interface the FACP to your Internet LAN, an EIA/TIA-568A CAT-5 (10/100-BaseT)-compliant Ethernet drop to the panel is required. This connection requires a standard Ethernet RJ-45 terminating connector. It is strongly recommended that the SafeLINC FPII be installed behind your network firewall to maintain maximum security for your network.

Before You Approach Your MIS/IT Department
Find the MAC address that is printed on a label located near the SafeLINC FPII's P12 connector. Carefully record this number below because your MIS/IT department will need this information to configure the SafeLINC FPII properly on your network. The format of the MAC address will look something similar to 00:08:BD:1C:48:1A. As an alternative to finding the MAC address on the label, follow the procedures in the SafeLINC FPII Installation, Setup, and Operating Instructions (Publication 579-349) to gain access to the SafeLINC FPII boot prompt. The MAC address will be displayed initially upon boot-up.

Record the FPII MAC Address: 00 : 08 : BD : ____ : ____ : ____ *Ex: 00:08:BD:1C:48:1A*

Minimum Parameters Required to Boot SafeLINC FPII – IT/MIS Department to Complete This Section
Now you may take this worksheet to your MIS/IT department for assistance in obtaining the parameters required for the SafeLINC FPII to operate properly on your local network. The parameters requested below are the minimum requirements necessary for the FPII to boot successfully into operation. ***WARNING: Do not attempt to boot the FPII using random entries; serious consequences may result. You can inadvertently affect other computers and networked devices on your network or, even worse, the Internet.***

Below are the minimum parameters for the SafeLINC FPII to successfully boot into operation on your network. Your MIS/IT department must complete this section using the MAC address that you've provided from your SafeLINC FPII above.

MIS/IT Assigned FPII Static IP Address: ____ . ____ . ____ . ____ *Ex: 192.168.0.1*

To configure the static IP address, type I at the FPII boot prompt. To verify your entry, type S to review a summary of all boot prompt configurables.

MIS/IT Assigned FPII Gateway: ____ . ____ . ____ . ____ *Ex: 192.168.254.1*

To configure the gateway, type G at the FPII boot prompt. To verify your entry, type S to review a summary of all boot prompt configurables.

MIS/IT Assigned FPII Subnet Mask: ____ . ____ . ____ . ____ *Ex: 255.255.0.0*

To configure the subnet mask, type N at the FPII boot prompt. To verify your entry, type S to review a summary of all boot prompt configurables.

MIS/IT Assigned FPII DNS Name: ____ *Ex: fpii.your_domain.com*

The FPII DNS name is not a required boot prompt menu parameter. It is used to access the FPII and is described below.

NOTE: The DNS Name Assignment requires an entry on the DNS server that maps to the FPII Static IP address or MAC address depending on your type of server.

Additional Parameters Required for SafeLINC FPII Email Support – IT/MIS Department to Complete This Section
Below are the minimum required parameters for the SafeLINC FPII to enable email functionality. Most email server configurations do not allow email relaying for network security reasons. Therefore, the SafeLINC FPII requires a valid email account to log into and send email as required. The account should not be configured to receive email because the SafeLINC FPII lacks the functionality to do so. All incoming email on this account should be simply deleted. This account should be dedicated to the fire panel so that it can be distinguished among other email accounts.

SMTP Email Server IP Address: ____ . ____ . ____ . ____ *Ex: 192.168.0.1*

SMTP Email Server Port: 25 *Fixed at Port 25 (not configurable)*

SMTP Email Account Address: ____ *Ex: fire_panel@customer-site.com*

Continued on next page

SafeLINC FPII MIS/IT Configuration Worksheet, *Continued*

SafeLINC FPII Administrator's Account – SafeLINC FPII Administrator to Complete This Section
In addition to the parameters obtained above, the SafeLINC FPII requires a username and password for the first user (Administrator) before a successful boot can proceed. This is the username and password that you will use to gain access the SafeLINC FPII via the Internet. To administer the SafeLINC FPII, the SafeLINC FPII Administrator's password is also required. Keep the information in this section private and store this sheet in a secure place.

FPII User 1 Username: _____ *Ex: John_Doe*

FPII User 1 Password: _____ *Ex: Password*

To configure the 'User 1' account, type U at the FPII boot prompt. You will be first prompted to enter the username followed by the password for this account. Enter the information as it appears above. To verify your entry, type S to review a summary of all boot prompt configurables.

FPII Administrator's Password: _____ *Ex: Admin_Pw*

To configure the FPII Administrator Password, type A at the FPII boot prompt. Enter the password as it appears above. To verify your entry, type S to review a summary of all boot prompt configurables.

Once you have successfully completed this sheet with the assistance of your MIS/IT department, you will be ready to configure the SafeLINC FPII via the diagnostic port and boot prompt. Using the above parameters, return to the SafeLINC FPII boot prompt to configure the SafeLINC FPII. The Email Support parameters are not required for the boot prompt configuration but will be required once you are able to access the SafeLINC FPII via your web browser.

At the SafeLINC FPII boot prompt, select the letter option to be configured followed by a carriage return. Help is available by typing H; typing S summarizes all the parameters as they are currently configured. If you wish to extend the boot-up delay, type D and enter the value in seconds. When you have finished entering the parameters from above and have verified they are correct (using S), type B to save the options into memory and reboot the SafeLINC FPII. Your SafeLINC FPII should now be configured for use on the network.

Accessing the SafeLINC FPII for the first time on your Network
You cannot proceed with the SafeLINC FPII Email configuration until you can access the SafeLINC FPII at the assigned DNS name from above. For example, if your DNS name is: fpii.your_domain.com then point your web browser to: http://fpii.your_domain.com/ to access the SafeLINC FPII homepage. You may need to adjust your proxy settings in your browser depending on how your MIS/IT department has configured the network. Because it is difficult to predict all possible configurations, please consult with your MIS/IT department on how to make adjustments to these settings. Refer back to earlier sections of Publication 579-349 for more details.

Once you can successfully access the SafeLINC FPII using your web browser, log into the SafeLINC FPII entering your username and password in the areas provided. Upon successful login, you will arrive at the homepage of the SafeLINC FPII. To access the administration area, you must use the Administrator's password in box provided at the top of the page. Enter the Administrator's password and press the carriage return. A new menu icon titled, Administration, will appear on the top right menu if the login was successful.

Next, click on the Login Accounts link and then scroll down to edit your account (the only one listed) and complete the information requested. You must provide a valid email address to test out the email configuration set-up described below. When you have finished editing your account, click Update to complete the request.

The last step is to configure the email configuration parameters in order for the SafeLINC FPII to send out email. Click on the Email Configuration link. The information provided by your MIS/IT department from above is used to complete the email configuration options. Fill in the information requested and press Update to complete the request. To verify that email is working properly, click on Send Test Email and then follow the directions. To verify that the email was sent properly, use your mail client and check the email account where you expect to receive email. This account should be the same as the email address provided in Login Accounts section. You may need to click on Send/Receive in your email client to see if you have received your email message. In addition, you may also check the email log on the SafeLINC FPII to verify that the SafeLINC FPII connected to the mail server successfully and delivered the message. To do so, locate the System menu and click the Email Log link. Review the log entries. If the SafeLINC FPII reports an error in the log, you will need to re-verify your email configuration settings on the SafeLINC FPII.

Congratulations! The SafeLINC FPII is now configured for general use. You will still need to configure some additional options and add user accounts as needed. Please refer to Publication 579-349 for how to operate the SafeLINC FPII.