LUDLUM UNIVERSAL SOFTWARE MANUAL

April 2015

Version 3.2.2
9.1 E-MAIL .................................................................48
9.2 DATA LOGGING ..................................................48
9.3 WEB INTERFACE ................................................49
  9.3.1 Current Status Page .........................................49
  9.3.2 Location Maps ................................................51
  9.3.3 Device Current Status Page ...............................51
  9.3.4 Device Background Graph Page .......53
  9.3.5 Spectroscopic Graph ......................................55
  9.3.6 Incident Summary Page ....................................56
9.4 DATABASE TABLE PLAN ......................................58
  9.4.1 UniversalConfig Table ...................................58
  9.4.2 Device Table ................................................59
  9.4.2.1 LogInterval Table .......................................60
  9.4.2.2 MapAndLocation Table .................................60
  9.4.2.3 IncidentHistory Table .................................60
  9.4.2.4 History Table ...........................................61
  9.4.2.4.1 HistoryDetectorData Table .........................61
  9.4.2.4.2 M720SpecChannelData Table ......................61
  9.4.2.4.3 M720SpecNuclideData Table ......................62
  9.4.2.4.5 ScanDetectorReading Table .........................62
  9.4.2.5 ScanHistory Table .....................................62
  9.4.2.5.1 SetPoint Table .......................................62
  9.4.2.5.2 M2100ScanType Table ...............................63
  9.4.2.5.3 ScanDetectorDataTable .............................63
  9.4.2.5.3.1 ScanDetectorAlarm Table .......................63
  9.4.2.5.3.2 ScanDetectorFailure Table ......................63
  9.4.2.5.3.3 ScanDetectorReading Table .....................64
  9.4.2.6 CurrentStatus Table ..................................64
10.0 ETHERNET INFORMATION ....................................65
  10.1 IP ADDRESSES ..............................................65
  10.2 ETHERNET CABLE TERMINATION .........................65
11.0 TROUBLESHOOTING ..........................................68
  11.1 UNABLE TO SET THE NETWORK SETTINGS OF THE MODEL 375 ....68
  11.2 TROUBLESHOOTING THE DEVICES ..........................69
    11.2.1 Troubleshooting the Model 375 .......................69
    11.2.2 Troubleshooting the Model 720 .......................70
    11.2.3 Troubleshooting the Models 2100, 4906, 53, and 54 ....70
  11.3 TROUBLESHOOTING THE UNIVERSAL SOFTWARE ............71
    11.3.1 Check the Devices ....................................71
    11.3.2 Check the Connection to the Database ................71
  11.4 TROUBLESHOOTING THE NETWORK ..........................71
    11.4.1 How to Ping a Computer ..............................71
    11.4.2 Ping the Universal from the Device or its Network ....72
    11.4.3 Ping the Device from the Computer with the Universal Software ...72
    11.4.4 Check any Firewalls between the Devices and the Computer with the Universal Software ..........72
    11.4.5 Check any other Firewalls and Routers ................73
  11.5 TROUBLESHOOTING THE SQL DATABASE ....................73
  11.6 TROUBLESHOOTING THE UNIVERSAL SERVICE ..............75
  11.7 TROUBLESHOOTING THE WEB PAGE ........................77
    11.7.1 Web Page does not load ..................................77
    11.7.2 Directory Listing Denied ................................78
    11.7.3 Invalid object name “dbo.xxxx” ........................78
11.7.4 Login failed for user “xxxxx”........................................................................................................78
11.7.5 Web Page loads, but does not show any Devices ........................................................................79
11.7.6 Default Web Site Won’t Start – Unexpected Error 0x8ffe2740 occurred...................................79
11.7.7 Could not load file or assembly ‘App_Licenses’ or one of its dependencies. The module was expected to contain an assembly manifest...............................................................79
11.7.8 Current Status page shows no area monitors.............................................................................80
11.7.9 Current Status page shows device(s) with a status of “Missing”....................................................80
11.8 Troubleshooting 375 FTP Firmware Updates ..............................................................................80
11.9 Replacing 375 Rabbit Ethernet Boards .........................................................................................81
1.0 Introduction

The Ludlum Universal Software is a radiation network software package that collects and displays radiation levels and alarm status from multiple LMI instruments, including area monitors, sample monitors, and portal monitors. Some instruments, such as the 375-10, have Ethernet built in while others can be updated using an Ethernet kit. The Ethernet kit can be installed by the customer, or the area monitors can be sent back to LMI for installation. Using this interface, radiation data may be placed onto the Ethernet network for real-time monitoring, email alerts, and stored into a database for later analysis. A standard web browser is used to view the current status and query the data.

See Section 3 for installation instructions.

The Universal software includes the following components:

- Universal Service
- ASP Web Application
- Area Monitor Utility
- Service Utility
- Device Finder
- Model 720 Central Translator

1.1 Universal Service

The Universal Service is a Windows™ service that listens for connections from compatible devices. Once a connection is made, the Universal service collects and processes the data. Data is logged into an SQL database and can be optionally configured to save data into a comma separated (.CSV) text file. The Universal Service also sends emails when an alarm or failure occurs.

1.2 ASP Web Application

Hosted on Internet Information Service (IIS), the ASP application provides a web interface to view the current status of each device from any computer that
has access to the web server. Also available are the incident summary and time line data for each area monitor.

1.3 Device Finder
The Device Finder application is used to search the network for any compatible devices, and display the IP address and firmware version. Because the Device Finder application uses UDP to find the devices, search results will typically be limited to the local subnet. (This is only intended to work with the Model 375.)

1.4 Service Utility
The Service Utility is used to add and remove devices, configure email settings, and to configure the SQL server database.

1.5 Area Monitor Utility
There are currently two Ethernet firmware versions available for the 375 series area monitors. Version 39801N10 requires the Area Monitor Utility to configure the Ethernet settings. The Ethernet settings of version 39801N12 and later is configured by accessing a web page running on the area monitor.

1.6 Spectroscopic Area Monitor Translator Service
This software allows for communication between the Model 720 Spectroscopic Area Monitor (also known as the PGT Model 2500 Spectroscopic Area Monitor) and the Universal Service. Once installed, the Communicator Service will run every time the Computer is started.
2.0 Software License Agreement

BY INSTALLING THIS SOFTWARE, YOU ARE CONSENTING TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, DO NOT INSTALL THE PRODUCT.

Single User License Grant: Ludlum Measurements, Inc. ("Ludlum") and its suppliers grant to Customer ("Customer") a none exclusive and nontransferable license to use the Ludlum software ("Software") in object code form solely on a single central processing unit owned or leased by Customer or otherwise embedded in equipment provided by Ludlum.

Customer may make one (1) archival copy of the Software provided Customer affixes to such copy all copyright, confidentiality, and proprietary notices that appear on the original.

EXCEPT AS EXPRESSLY AUTHORIZED ABOVE, CUSTOMER SHALL NOT: COPY, IN WHOLE OR IN PART, SOFTWARE OR DOCUMENTATION; MODIFY THE SOFTWARE; REVERSE COMPILE OR REVERSE ASSEMBLE ALL OR ANY PORTION OF THE SOFTWARE; OR RENT, LEASE, DISTRIBUTE, SELL, OR CREATE DERIVATIVE WORKS OF THE SOFTWARE.

Customer agrees that aspects of the licensed materials, including the specific design and structure of individual programs, constitute trade secrets and/or copyrighted material of Ludlum. Customer agrees not to disclose, provide, or otherwise make available such trade secrets or copyrighted material in any form to any third party without the prior written consent of Ludlum. Customer agrees to implement reasonable security measures to protect such trade secrets and copyrighted material. Title to Software and documentation shall remain solely with Ludlum.

LIMITED WARRANTY. Ludlum warrants that for a period of ninety (90) days from the date of shipment from Ludlum: (i) the media on which the Software is furnished will be free of defects in materials and workmanship under normal use; and (ii) the Software substantially conforms to its published specifications. Except for the foregoing, the Software is provided AS IS. This limited warranty extends only to Customer as the original licensee. Customer's exclusive remedy and the entire liability of Ludlum and its suppliers under this limited warranty will be, at Ludlum or its service center's option, repair, replacement, or refund of the Software if reported (or, upon request, returned) to the party supplying the Software to Customer. In no event does Ludlum warrant that the Software is
error free or that Customer will be able to operate the Software without problems or interruptions.

This warranty does not apply if the software (a) has been altered, except by Ludlum, (b) has not been installed, operated, repaired, or maintained in accordance with instructions supplied by Ludlum, (c) has been subjected to abnormal physical or electrical stress, misuse, negligence, or accident, or (d) is used in ultra hazardous activities.

**DISCLAIMER. EXCEPT AS SPECIFIED IN THIS WARRANTY, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE, ARE HEREBY EXCLUDED TO THE EXTENT ALLOWED BY APPLICABLE LAW. IN NO EVENT WILL LUDLUM OR ITS SUPPLIERS BE LIABLE FOR ANY LOST REVENUE, PROFIT, OR DATA, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE EVEN IF LUDLUM OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH.**

**DAMAGES.** In no event shall Ludlum’s or its suppliers’ liability to Customer, whether in contract, tort (including negligence), or otherwise, exceed the price paid by Customer. The foregoing limitations shall apply even if the above-stated warranty fails of its essential purpose. **SOME STATES DO NOT ALLOW LIMITATION OR EXCLUSION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES.**

The above warranty DOES NOT apply to any beta software, any software made available for testing or demonstration purposes, any temporary software modules or any software for which Ludlum does not receive a license fee. All such software products are provided AS IS without any warranty whatsoever.

This License is effective until terminated. Customer may terminate this License at any time by destroying all copies of Software including any documentation. This License will terminate immediately without notice from Ludlum if Customer fails to comply with any provision of this License. Upon termination, Customer must destroy all copies of Software.

Software, including technical data, is subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Customer agrees to comply strictly with all such regulations and acknowledges that it has the responsibility to obtain licenses to export, re-export, or import Software.

This License shall be governed by and construed in accordance with the laws of the State of Texas, United States of America, as if performed wholly within the state and without giving effect to the principles of conflict of law. If any portion hereof is found to be void or unenforceable, the remaining provisions of this License shall remain in full force and effect. This License constitutes the entire License between the parties with respect to the use of the Software.
Restricted Rights - Ludlum's software is provided to non-DOD agencies with RESTRICTED RIGHTS and its supporting documentation is provided with LIMITED RIGHTS. Use, duplication, or disclosure by the Government is subject to the restrictions as set forth in subparagraph "C" of the Commercial Computer Software - Restricted Rights clause at FAR 52.227-19. In the event the sale is to a DOD agency, the government's rights in software, supporting documentation, and technical data are governed by the restrictions in the Technical Data Commercial Items clause at DFARS 252.227-7015 and DFARS 227.7202. Manufacturer is Ludlum Measurements, Inc. 501 Oak Street Sweetwater, Texas 79556.
3.0 Getting Started

The LMI Universal Software can run on both desktop and server operating systems and can also be installed on a virtual machine. It is not necessary for all components to be installed on a single computer. SQL Server, Internet Information Service (IIS), and the Universal software can be installed on different systems.

3.1 Software Prerequisites

The following software must be installed on the network and working before installing the LMI Universal software.

- Internet Information Services. See Section 4 for installation instructions.
- SQL Server 2008 or later. Either Express or full versions supported. SQL Server 2008 Express is included on the installation DVD.

See the appropriate installation documentation for the above items.

3.2 Minimum Requirements

- **Supported Operating Systems**: Windows Server 2008; Windows Server 2012
- 32-Bit Systems: Computer with Intel or compatible 1GHz or faster processor (2 GHz or faster is recommended)
- 64-Bit Systems: 1.4 GHz or higher processor (2 GHz or faster is recommended)
- Minimum of 256 MB of RAM (1 GB or more is recommended)
- 1 GB of free hard disk space
- A Compact Flash Card Reader, only for the Model 720 Spectroscopic Area Monitor.
3.3 Installation Overview – Single Server
This is the easiest type of installation where all components are installed on a single computer or virtual machine. The steps are:

1. Install IIS. Section 4
2. Install SQL Server. Section 5
3. Install Universal Software. Section 6
4. Configure Devices on network. Section 7
5. Configure Service. Section 8
6. Configure Model 720 Communicator Service. Section 9

3.4 Installation Overview - Multiple Servers
This is the most common type of installation where an existing SQL Server and Web Server are used. Typically the Universal Software is installed on another computer or virtual machine. The steps are:

1. Install Universal Software. Section 6
2. Configure devices on network. Section 7
3. Configure Service. Section 8
4. Configure Model 720 Communicator Service. Section 9
Refer to all applicable operating system documentation for the correct procedure to install IIS. A Windows Operating System CD may be required to complete installation. After installation, download and install any updates from Windows Update.

4.1 IIS Server Installation – Windows Server 2008
Perform the following steps to install IIS for Windows Server 2008.

Also included are instructions on how to install the Windows Power Shell feature, which is required by SQL Server.

1. Click the **Start Menu** and click **Server Manager** to open the Server Manager window. See Figure 1.
2. Under the **Roles Summary** group box in the middle pane of the Server Manager window, click **Add Roles**.

3. In the **Select Server Roles** window, check **Web Server (IIS)** and click **Next**. See Figure 2.
4. Under the **Application Deployment** node, check the **ASP.NET** option. When the **Add Roles Wizard** pop-up appears, click **Add Required Role Services**. See Figure 3.

5. Scroll down and check the **IIS Management Scripts and Tools** option.

6. Check the **IIS 6 Scripting Tools** option. When the **Add Roles Wizard** pop-up appears, click **Add Required Role Services**.
7. Check the **IIS 6 Management Console** option.

8. Check the **FTP Server** and **FTP Management Console** options.

9. Verify that the selected role services resemble Figure 4 below and Figure 5, then click **Next**.

![Add Roles Wizard](image)

Figure 4 – Add Roles Wizard (Select Role Services 1)
10. Click **Install**. See Figure 6.

![Figure 5 – Add Roles Wizard (Select Role Services 2)](image)

Figure 5 – Add Roles Wizard (Select Role Services 2)

![Figure 6 – Add Roles Wizard (Confirm Installation Selections)](image)

Figure 6 – Add Roles Wizard (Confirm Installation Selections)
11. If Internet Information Services (IIS) is installed successfully, click **Close**. See Figure 7.

![Add Roles Wizard (Installation Results)](image)

**Figure 7 – Add Roles Wizard (Installation Results)**

12. In the Server Manager window under the **Features Summary** group box, click **Add Features**.

13. In the **Add Features Wizard**, check **Windows Power Shell**. See Figure 8.

**NOTE:** If the Windows Power Shell check box is already checked, Windows Power Shell is already installed.
14. Click **Install** to install Windows Power Shell. See Figure 9.

![Add Features Wizard (Select Features)](image)

**Figure 8 – Add Features Wizard (Select Features)**

![Add Features Wizard (Confirm Installation Selections)](image)

**Figure 9 – Add Features Wizard (Confirm Installation Selections)**
15. When installation is complete, click **Close**. See Figure 10.

![Figure 10 – Add Features Wizard (Installation Results)](image)

16. Click the Start Menu/Administrative Tools and click **Services** to open the Services window. See Figure 11.

![Figure 11 - Services](image)
17. Double-click **FTP Publishing Service** to open the FTP Publishing Service Properties window.

18. Click the **Startup type** combo box and select the **Automatic** option.

19. Click the **Start** button to start the FTP Publishing Service.

20. Verify that the FTP Publishing Service Properties window resembles Figure 12 and click **OK**.

21. Close the Services window and the Server Manager window.

![FTP Publishing Service Properties](image)

Figure 12 – FTP Publishing Service Properties
5.0 SQL Server 2008 Express Installation

SQL Server 2008 Express R2 editions (x86 and x64) are included on the installation DVD and can be installed by following the steps below.

Windows PowerShell 2.0 is a prerequisite before installing SQL Server 2008 R2 Express. Install PowerShell through Windows Update before attempting to install SQL Server 2008 R2 Express.

1. Navigate to the SQL Server Express 2008 folder on the DVD and double-click SQLEXPRADV_x86_ENU.EXE to install the 32-bit version or double-click SQLEXPADV_x64_ENU.EXE to install the 64-bit version.

2. If the following window (Figure 13) appears, download and install Microsoft Windows Installer 4.5. Restart the computer if necessary. If the window does not appear, skip to step 3.

3. From the SQL Server Installation Center, click New installation or add features to an existing installation. See Figure 14.
4. Click **New installation or add features to an existing installation**.

5. Accept the **License terms** and click **Next** to continue.
6. From the Feature Selection screen, accept the defaults and click **Next**. See Figure 16.

![Feature Selection](image)

**Figure 16 – Feature Selection**

7. If there are no other instances of SQL Server, accept the defaults and click **Next**. If there are one or more installed instances, check the name of this instance to an appropriate value. When finished configuring the instance, click **Next**. See Figure 17.

![Instance Configuration](image)

**Figure 17 – Instance Configuration**
8. Consult your Network Administrator for the correct user accounts to use. If you are unsure, use the NT AUTHORITY/NETWORK SERVICE account. See Figure 18. Click **Next** after configuring the accounts.

![Figure 18 – Service Accounts](image1.png)

9. Change the Authentication Mode to **Mixed Mode (SQL Server Authentication and Windows Authentication)**. Enter a password for the "sa" user. Click **Next**. See Figure 19.

![Figure 19 – Account Provisioning](image2.png)
10. Select **Install the native mode default configuration** from the Reporting Services Configuration screen and click **Next**. See Figure 20.

![Figure 20 – Reporting Services Configuration](image)

**Figure 20 – Reporting Services Configuration**

11. Click **Next** on the Error Reporting screen. See Figure 21.

![Figure 21 – Error Reporting](image)

**Figure 21 – Error Reporting**
12. After the installation is complete, click the Close button and then close the SQL Server Installation Center. See Figure 22.

![SQL Server 2008 Completed Installation](image)

Figure 22 – SQL Server 2008 Completed Installation
6.0 Universal Software Installation

There are two components to the Universal Software – Service and Web Application. The Universal Web application must be installed on a computer running Internet Information Service (IIS). The following sections below cover how to install the Universal software and configure SQL Server and IIS, but the basic overview is:

- Install Universal Service and utilities
- Install Universal Web application
- Configure SQL Server users
- Configure the Universal Service
- Configure IIS

6.1 Installing the Universal Service and Utilities
To install from the Universal Service Install folder on the installation DVD, run SETUP.EXE and follow the on-screen prompts.

The default installation location is: C:\Program Files\Ludlum Measurements, Inc\LMI Universal Software\.

6.2 Installing the Universal Web Application
IIS and IIS 6.0 Management Compatibility must be installed on the computer before the Universal Web Application will install.

To install from the Web App Install folder on the installation DVD, run SETUP.EXE and follow the on-screen prompts.

The installer will prompt to select the site and virtual directory. The virtual directory will define the URL that will be used to access the web application.
6.3 Configuring SQL Server for the Universal Software

The Universal Service supports both Windows authentication and SQL authentication. The Universal software requires a database called LmiUniversal. Follow the steps below to create the database.

1. Install the LmiUniversal Database Setup program, found on the installation DVD.
2. Run the LmiUniversal Database Setup program.
3. Type in the Name of the Database, typically just “localhost” or “localhost\SQLEXPRESS”.
4. Choose the appropriate way to access the database: either Windows Authentication if you are logged in as Administrator or SQL Authentication otherwise.
5. If you are using SQL Authentication, type in the appropriate Username and Password, typically the “sa” username and password.
6. Click Run Setup.
7. If the step succeeded, the program will say so and you may close this program, and even uninstall it.
8. A common error is that the login “IIS APPPOOL\ASP.NET v4.0 Classic” failed to be created. If this is the case, you will need to ensure that IIS and .Net v4.0 has been installed on this computer. If the Web Site is being run on another computer, you will need to manually add the “IIS APPPOOL\ASP.NET v4.0 Classic” as a login and give it ownership of the LmiUniversal database.

6.4 Configure the SQL connection

The Universal software uses the connection.config file to store the SQL Server connection settings. This file is modified by the Service Utility application. When the LMI Universal Service Utility is first run, a window is displayed indicating that connection.config file is not found (Figure 23). This message showing up the first time is normal, as there can’t be any saved connection information.
After acknowledging this message, the Service Utility will switch to the SQL Connection tab (Figure 24). Enter the name of the SQL Server and instance name in the Server name field. Select the appropriate authentication method (Windows or SQL) and click Save.

If you are running the Web Site on a different machine than the one running the Universal Software, you will need to Install the Utilities Only version of the Universal Software and repeat this step on that Service Utility.
6.5 Configuring IIS for the Universal Web Application
The Universal web application requires the following settings for the server versions of IIS:

- ASP.NET v4.0 Classic Application Pool
- ISAPI + CGI restrictions should be changed to allow the ASP.NET v4.0.30319 Framework

6.6 Testing the Universal Web Application
Open an Internet browser and type in the URL in the address field. The URL will be the name of the computer and the virtual directory. For example: http://www.ludlums.com/LmiUniversal.
7.0 Device Configuration

7.1 Device Finder
(This utility is intended to work with the Model 375.)

The Device Finder utility can be used to find the network settings of devices that do not have displays. The Device Finder broadcasts a UDP message on port 20034. This can be used to find the network settings of area monitors.

![Device Finder](image)

The MAC address, IP address, and firmware version are shown. Click the Search button to search for devices on the network. Use the filter check boxes to filter the results.

7.2 Model 375 Series Area Monitors
All area monitors from LMI are shipped with a static IP address of 10.10.6.100, unless otherwise specified. Consult the Area Monitor Network Settings report that was sent with the instrument to locate the correct settings.

Since the area monitors are by default shipped with a static IP address, it is STRONGLY recommended that the user connect each Model 375 area monitor, one at a time, to a laptop or PC with a crossover cable before attempting to configure the area monitor.
NOTE: If computer or laptop supports Gigabit Ethernet, then a straight-through cable may be used.

NOTE: If all area monitors are connected to the network at first, it may be impossible to configure them because they may all have the same IP address.

NOTE: The Model 375 Area Monitor CANNOT be configured using the serial port.

Before connecting to your laptop or PC, set the network interface for the following parameters:

- IP address: 10.10.6.101
- Subnet mask: 255.255.255.0
- Default gateway: 10.10.6.1

**7.2.1 Configuring Network Settings – Web Interface (firmware versions N12 and later)**

The Model 375 area monitors are shipped with a static IP address and can be configured using an Internet browser. The default IP address is 10.10.6.100.

The Model 375 area monitor can also be configured for DHCP. If the area monitor is configured for DHCP, it will be necessary to use the Device Finder utility (which is detailed later) to determine the IP address of the area monitor. If the area monitor is configured for DHCP and there is no DHCP server available, the area monitor’s IP address will fall back to 169.254.n.n, where n.n is randomly selected based on the area monitor’s serial number. If the area monitor’s IP address falls back, you will need to use a crossover cable to connect the area monitor to a PC. The Device Finder utility can then be used to show what IP address is assigned to the area monitor.

Open web browser and type the IP address of the area monitor into the address bar. You should see a web page that looks similar to Figure 26.
Use the web interface to perform the following steps.

1. The serial number should be set at the factory; however, you may change the serial number if you wish by entering in the new serial number in the **Serial Number** field.

2. In the **IP Address** field, enter in the appropriate IP address for your Model 375 unit. **NOTE:** If DHCP is desired, enter in 0.0.0.0.

3. In the next three fields, enter in the subnet mask, gateway, and DNS addresses to match your network’s configuration. **NOTE:** If the Model 375 is configured for DHCP, the subnet mask, gateway, and DNS addresses will be set automatically.

![Figure 26 – Model 375 Network Settings](image-url)
4. In the **TCP/IP Port** field, enter in the port number that the Universal service will be listening on. This port number must match the port number set in the Service Utility under the **Service** tab.

5. Use the **Unit Code** control to select the appropriate units for the Model 375. The units should match the actual display units of the area monitor.

6. In the **Supervisor Primary IP Address** text box, enter in the IP address of the computer that will be running the Universal service. If you have a second server set up, enter it in the **Supervisor Secondary IP Address** field. If you do not have a second server running the Universal service, copy the primary IP address into the secondary IP address field.

7. If the Model 375 will be associated with a camera, enter the camera’s IP address into the **Camera IP Address** field. In the **Camera Password** field, enter in the camera’s password.

8. Select whether or not the camera will be enabled or disabled.

9. To save the new settings to the Model 375, enter the password into the **Password** field, then click the **Submit** button. The initial password for a new Model 375 is **password**, all lower-case. If you wish to change the password, enter in the desired new password in the **New Password** and **Confirm New Password** fields before clicking the **Submit** button.

### 7.2.2 Configuring Network Settings – Setup Utility (firmware versions 39801N11 and earlier)

The Area Monitor Utility is used to configure the network settings for any Model 375 area monitors that do not have the web interface firmware installed (versions 39801N11 and earlier). When run, the utility will attempt to find all area monitors that are on the local network using UDP. This utility can be run from any computer. Following is a screen shot of the setup utility.
The Area Monitor Utility uses a broadcast UDP message on port 20034 to find area monitors on the network. Because of this, area monitors that are located in different buildings or cities may not be found. In order to successfully configure the area monitor’s settings, it may be necessary to do one of the following:

1. Connect a laptop directly into the area monitor or use a computer at the same location as the area monitor.

2. Bring the area monitors to the same location as the server. Once they have been configured, move them back to their correct locations.

A list of all Model 375 area monitors found on the network are displayed in the drop-down list at the top. Click Search to search the network again for area monitors.

**Serial Number:** Each area monitor has a unique serial number stamped on the chassis in the lower left-hand corner of the Model 375. Enter this number here. This number is required for proper operation of the service.

**Unit Code:** This code signifies what unit of measurement the readings are displayed in. It should match the display plate located under the Model 375 four-digit (or five-digit) LED display.

**Firmware:** firmware number of Model 375 Ethernet board. Firmware versions 39801n011 and lower only support changing the network settings with this utility. The settings for versions 39801n12 and higher can only be viewed in the
Model 375 Setup Utility and can only be changed through its built-in web interface.

**IP Address:** the IP Address assigned to this area monitor. Set the IP address to 0.0.0.0 to use DHCP. *NOTE:* When DHCP is used, you will see a DHCP label next to the IP address.

**Subnet Mask:** subnet mask assigned to this area monitor

**Gateway:** Gateway address assigned to this area monitor. *NOTE:* When DHCP is used, you will see a DHCP label next to the gateway.

**DNS:** domain name server address assigned to this area monitor. If the area monitor is set up to use DHCP, this address will update automatically. If the area monitor is assigned a static IP and DNS capability is desired, this value MUST be a valid IP address to a domain name server on your network.

**Primary Address:** address of the primary server running the Universal service. It’s possible to run the service on two separate computers. If the primary service is unavailable for any reason, the area monitor will attempt to connect to the secondary service.

**Secondary Address:** address of the secondary server running the Universal service. If the primary service is unavailable for any reason, the area monitors may attempt to communicate to the secondary service to minimize down time.

**Supervisor Port:** The Universal Software service listens on this TCP port number for area monitors. All area monitors that connect to a computer must use the same port number.

**Camera Enabled:** indicates if the camera for this area monitor is enabled. (Note, the Universal Software will independently contact the camera, so this field is unnecessary.)

**IP Address:** the host name or IP Address of the camera. (Note, the Universal Software will independently contact the camera, so this field is unnecessary.)

**Password:** allows the area monitor access to the camera. (Note, the Universal Software will independently contact the camera, so this field is unnecessary.)

### 7.2.3 Updating Model 375 Ethernet Board Firmware Using FTP

Beginning with Ethernet firmware version N10, the Model 375 Area Monitor has the ability to remotely update Ethernet firmware. This saves the user from having to send each area monitor to LMI every time a firmware update is released.
On power-up, the area monitor’s Ethernet board runs a program that is known as the Download Manager (DLM). The DLM attempts to connect to an FTP server located at the Supervisor Primary IP Address. If the firmware version on the FTP server is different from the firmware version stored in the area monitor’s Ethernet board, the DLM will automatically download the firmware update to the Ethernet board.

Perform the following steps on the Supervisor computer to remotely update firmware for instruments in the field:

1. Using Windows Explorer, navigate to the following folder: C:\Inetpub\ftproot.
2. Create a new folder named “Firmware.”
   **NOTE:** The remote firmware update path is case-sensitive, so make sure that the spelling and case are correct for the new folder name.
3. Copy the two firmware files (provided by LMI) into the “Firmware” folder.

Once these steps are completed, simply cycle power in each Model 375 instrument to install any firmware updates. The firmware update should take two to three minutes and will not appear in the Setup Utility during this time.

**NOTE:** If the firmware for your Model 375 Area Monitor’s Rabbit Ethernet board is earlier than N10 and does not support the DLM, or you do not wish to set up an FTP server, the Model 375 Rabbit Ethernet board can be programmed using a Rabbit programming cable (1.27 mm connector), which can be purchased from the rabbit.com website and the free Rabbit Field Utility.

### 7.2.4 Camera Configuration (optional)

By enabling the camera settings in the area monitor and configuring the supported IQeye camera for FTP upload, a camera image can be transmitted at the time of the alarm and displayed along with the incident record. Currently only Ethernet cameras from www.iqeye.com are supported.

Refer to the camera's documentation for getting it connected to your network, and then change the following settings for triggering the camera:

1. Modify the trigger settings, as follows:

   ```
   Actions: FTP
   Motion: disabled
   External Input: disabled
   Time Lapse Period: 0
   Image Size: 1
   Forced Idle time (sec): 5
   # pre-trigger images: 1
   pre-trigger interval (sec): 0.1
   # post-trigger images: 0
   post-trigger interval (sec): 1
   ```
2. Leave the email settings blank. Modify the FTP settings, as follows:

3. FTP hostname: the server’s computer name on the network
   Username: anonymous
   Password: leave blank

4. File name: $ST.jpg
   File path: #######/$SD (#s represent serial number of Model 375 unit)

Repeat camera steps for any additional cameras.

7.3 Model 2100 Series Sample Monitors, Model 4906 Hand and Foot Monitors, Model 53 Portal Monitors, Model 54 Article Monitors
All of the given Monitors default to using DHCP for the Ethernet interface. The embedded computer is running Windows 7 Professional, and the network settings can be configured like a standard desktop computer. After connecting the sample monitor to the network, click Setup > Operational Setup and select the Network tab.

![Network Setup](image)

Figure 28 - Network Setup
Enter the IP Address and port of the server running the Universal service and click the Enabled check-box to turn on the Universal connection. Once enabled, the sample monitor will attempt to make a TCP connection to the specified port and IP address.

### 7.4 Configuring the Model 720 Firmware

Now you need to set up the Model 720 Firmware. First, open the Model 720 by unscrewing the six plastic screws, then pull off the top.

There will be two circuit boards, one smaller and above the other. This smaller board should have a Memory Card sticking out of it. Press the large black lever next to the Memory Card to eject the card and then remove the Memory Card.

Next, plug the card into a Compact Flash card reader and plug the reader into a USB port on your computer.

Go to “My Computer” and click on the new drive, likely “E:” or “F:” Go into the folder labeled “config.” Open the file called CONFIG.INI. Find the line that starts “HEARTBEAT_NOTIFY_FREQUENCY =”. This tells the Model 720 how often – in seconds – it will send out its status when it is not actually alarming.

Though you or your supervisor may decide to use a different time, it is suggested to use 300, which is five minutes. Whatever number you choose, change the number after the equals sign to that number.

Next, find the line that starts “ID_short =”. Change the word after the equals sign (likely Monitor) to MonXXX, where XXX is the Serial Number of the Model 720. For example, if the Model 720 Serial Number was 555555, then the full line would be “ID_short = Mon555555”.

**Note:** Be sure to enter this correctly, as this is how the Model 720 Communication Service identifies which Model 720 is sending it information.

Next, find the line that starts “IP_ADDR =”. Change the IP Address to the one assigned to this Model 720 by your network administrator. After doing that, find the line “TFTP_ADDR =” and change that IP Address to the address of the computer that has the Model 720 Communication Service on it. Save this file and close it.

Also, make sure that the lines IP_NETMASK, IP_GATEWAY, and IP_BRAODCAST are all correct. On a typical network, these should be IP_NETMASK = 255.255.0.0, IP_GATEWAY = N.N.01, and IP_BRAODCAST = N.N.255.255, where the N.N part is your network prefix.
Now find the file called UNIT.INI. Change the same lines as before, except for the HEARTBEAT_NOTIFY_FREQUENCY line, which is not a part of this file. Save and close this file.

Remove the card reader from the computer and then remove the Memory Card from the card reader. Place the Memory Card back into the Model 720 and screw the cover back on.

Repeat for each Model 720.
8.0 Configuring the Service

8.1 LMI Universal Service Utility
The Service Utility is used to configure the Universal service, including adding or removing devices, starting and stopping the service, and setting up email notifications.

Figure 29 – Devices Tab

8.1.1 Devices
The Devices tab is used to maintain the list of devices for the Universal service. The Universal service supports several types of instruments:

- Model 375 Area Monitor
- Model 54 Article Monitor
- Model 4906 Hand and Shoe Monitor
- Model 53 Portal Monitor
Select the device type to see all devices that have been added. Clicking on the serial number in the list will display that device’s configuration information on the right. To edit an existing device, click the **Edit** button. To save the changes, click the **Save** button, or to cancel the changes, click **Cancel**.

To add a new device, select the correct device type from the drop-down list and click the **Add** button. When finished, click the **Save** button to save the device. Allow at least one minute for the changes to be reflected in the Universal service and Web application.

**Serial Number**: Enter the serial number of the device. This number is usually stamped on the outside of the device or displayed on the device's computer screen.

**Name**: A user-defined field that is used to identify the device. This may be left blank, and a name will be generated for you (“Model Number”: “Serial Number”, for example: “4906: 123456” for a Model 4906 Hand and Shoe Monitor with 123456 as its Serial Number).

**Device Enabled**: The device must be enabled for the Universal service to log data or send email alerts.

**Placement Section**:

- **Site**: a user-defined field that is used by the web application to sort and group devices
- **Building**: a user-defined field that is used by the web application to sort and group devices
- **Area**: a user-defined field that is used by the web application to sort and group devices
- **Location**: a user-defined field that is used by the web application to sort and group devices

**Log Interval Section**:

- **Normal Logging (sec)**: specifies the database logging interval in seconds for the device in a normal or non-alarming state. The default is 300 seconds or 5 minutes. (This feature is only used and displayed for the Model 375 and Model 2100.)
• **Alarm Logging (sec):** specifies the database logging interval in seconds for an alarming or failing state. The default is 30 seconds. (This feature is only used and displayed for the Model 375 and Model 2100.)

**Camera Section:**

• **Enabled:** specifies if there is a camera associated with this device.

• **IP Address:** IP address of the camera (See next bullet point).

• **Still Picture Location:** URL of camera that will return a static JPEG image. This is used in conjunction with the Camera’s IP Address to attempt to get a photo at the start of an alarm or failure. So if a camera’s URL for a still picture is “127.0.0.1/now.jpg”, you only need to put “/now.jpg” in this field and “127.0.0.1” in the IP Address field.

**Comment:** a user-defined comment for this device.

**Executable Launch Buttons:**

• **Launch 375 Setup Utility:** (375 Only) Launches the Model 375 Setup Utility, used to configure Model 375 with N10 or Older firmware.

• **Launch Device Finder:** (375 Only) Launches the Device Finder, used to find Model 375s that are already running on the network.

• **Launch 720 Translator:** (720 Only) Launches the Model 720 Translator program, which is used to facilitate communication between Model 720s and the Universal Service.

### 8.1.2 Service

The Service tab is used to configure the various settings that affect the Universal Service.
8.1.2.1 GENERAL

Universal Service Data:

- **Listening Port**: The Listen port number specifies which TCP port the Universal service listens on for incoming connections from the devices. The default value is port 50000.

- **Web Site Location**: is a user-defined field that gives the location of the IIS Universal Web Page. This needs to be filled in if the user wishes to save pictures from cameras and then look at them from the web service.

**Service Status**:

Checks and shows whether the Universal Service is running or stopped. If the button is Green, you can click on it to turn the Service off. If the button is Red, you can click on it to turn the Service On. If the button is any other color, it is either waiting to start (Blue), waiting to stop (Yellow), or in some unknown state (Grey) and is thus not actually on this computer (this is the normal case if you have installed the Utilities Only).
8.1.2.2 EMAIL SERVER INFO

Figure 31 – The Email Server Info Tab

SMTP Info:

- **SMTP Server Name**: The name of the server that hosts your internal email provider. The Universal service will contact this server to deliver the email messages. If there are email addresses that are not intended for the specified server, then email forwarding will need to be configured to allow the messages to continue on to the final destination.

- **SMTP Server Port**: The port the SMTP Server uses to send emails.

- **Email “From” Address**: The email address the alert emails will show they are coming from. Depending on the configuration of the SMTP server, this may have to be a real email address.

**Test Email Server**:

This allows you to send Test Emails to ensure the SMTP server information is correct and that emails within Email Groups (see below) are valid.
8.1.2.3 EMAIL GROUPS

![Email Groups Tab](image)

Figure 32 – The Email Groups Tab

This allows you to create groups of emails and Serial Numbers so that only those who are responsible for certain devices are the only ones to receive an alarm or failure email. At least one Group is necessary to have a working email alert system. Some example Groups are: Supervisors, Repair Technicians, or South Station.

Clicking on the Group’s Name in the list will display that Group’s configuration information on the right. To edit an existing Group, click the Edit button. To save the changes, click the Save button or to cancel the changes, click Cancel.

To add a new Group, click the Add button. When finished, click the Save button to save the device. Allow at least one minute for the changes to be reflected in the Universal service.

**Group Info:**

- **Serial Numbers:** The Serial Numbers This Group will receive alert emails from.

- **Shift 1, 2, and 3:** These tabs allow you to break emails up into shifts so that if there are different people on call for a different shift, but all are responsible a group of devices, each person will receive the appropriate email at the appropriate time.

  - The Start Time is when this shift starts. If Shift 1 is the only shift enabled, this field does not need to be any specific value,
otherwise, the Start Time(s) of the other shift(s) will indicate when the next shift will take over.

- The Enabled checkbox allows you to indicate that the current shift information should be used. Please note that you must have Shift 1 enabled to have any emails sent for this group.

- The Alarm Emails list allows you to specify what emails will receive emails when a device alarms.

- The Failure Emails list allows you to specify what emails will receive emails when a device enters a failure state.

- **Edit Group Name:** You can edit the name of the current group, if you so desire. The Group Names are for your benefit.

### 8.1.2.4 EMAIL TEMPLATES

![Image of Email Templates Tab](image.png)

Figure 33 – The Email Templates Tab

This tab allows you to slightly customize the emails that are sent out.

- **Subject:** Changes the Subject of the Alarm or Failure Email.

- **Message:** Allows you to have a custom message for either the Alarm or Failure Email.
8.1.2.5 DATABASE MAINTENANCE

The Delete Old Records section allows the user to specify if and when device records are deleted. The user is allowed to choose between deleting records older than a given number of days ago, a given number of weeks ago, or a given number of months ago. The number can be anywhere from 1 to 999. This will apply to all devices.

8.1.3 Database
The Database tab is used to configure the connection settings for connecting to the SQL Server database.
Specify either Windows or SQL authentication. If SQL authentication is used, enter the user name and password that will be used to log into the SQL database.

You can also test the connection to check to see if the provided information is correct.

8.1.4 Location Map
The Location Map tab allows you to place instruments onto one or more images that should be a floor plan or map of the area. This allows you to view the devices’ status on an image rather than a simple list. Each instrument can only be on one image at a time, but you may have any number of instruments spread across any number of images.

To use this feature, you need to have all of the desired images in the Maps folder of the Web Site, as well as have the Web Site Location field of the Database General tab filled in and saved.

Select the image you want to place some of the instruments on. The software supports .BMP, JPG, and .PNG. The image will be temporarily scaled to fit the screen.

To place an instrument, select its name from the list next to the image. Now click where you want the instrument to be shown on the image. Where you click will be the upper-left corner of where the device will be shown.

To move an instrument already on the image, select its name from the list next to the image and just click to where you want the instrument to be. It will be moved to this new location.
To remove an instrument, you can do one of two things. If you want to remove an instrument from being shown at all, select its name from the list next to the image, and then click on the Remove button underneath the list. If you want to move an instrument from one image to another, just select that image, then that instrument, and then click where you want the instrument to be on this new image.

Please note that if you have an instrument that is disabled (the Enabled Checkbox is unchecked on the Devices tab), it will not show up on the map, even if you place it there.

8.2 Configuring the Model 720 Communication Service

Once the Universal Server is installed, now the Communication Service needs to be set up. Go to the computer with the Model 720 Translator Service installed on it. Click on Start, All Programs, Ludlum Measurements, Inc, 720 Translator.

If all of the options are grayed out, then click on the green button next to “Running.” This will stop the Model 720 Translator Service and allow you to change these settings. Remember to turn the Service back on when you are done by clicking that button again, which is now red and says “Stopped.”

Add a new Model 720 by typing in its Serial Number and its IP Address. The Serial Number must match the one given in section 7.4 (minus the “Mon” prefix). The Add button will light up once you have a valid and unique IP Address and Serial Number typed in.

Modify a Model 720 by selecting it in the list, changing the appropriate fields in the “Edit Selected Model 720 section,” and clicking the Update button. Deleting a Model 720 is similar, only clicking the Delete Button instead.

Test the connection to the Model 720s either in one go (by clicking on the “Test All Model 720 Connections” button) or individually (by selecting the Model 720 in the list and then clicking on the “Test Connection” button).

You may also need to change the Port Number that it used to communicate with the Universal Service, which is defaulted to port 50000.
Figure 37 – Model 720 Translator
Section 9

9.0 Operation

The LMI Universal service listens for TCP connections from the devices on the defined port number. When a connection is made, the service will start processing messages from the device.

**NOTE:** If any enabled devices are missing, a “missing” status will be generated for each unit.

9.1 E-Mail

When an alarm or failure occurs, the service will send out an email using the address list specified by the shift definition. The device must be in a non-alarming state for 60 seconds before another alarm or fail event will be triggered.

**Example E-Mail message**

Subject: [ALARM]

A High Alarm condition has occurred.
Lobby
60.80 cpm
Contact RSO x3332

LMI
Main
Engineering

237025
This message generated automatically by:
LMI Universal Software - version 3.2.2

A user-defined string can be defined for the subject and body of the email (see above).

An email pertaining to a Model 720 will also include any detected Isotopes and the confidence it has correctly detected it.

9.2 Data Logging

There are effectively two different types of devices that work with the Universal Software. The first type is an Interval-based device, which sends out a message every two seconds, no matter what state it is in. The second type is an Event-based device, which will send a message with a status and a background reading
once every five minutes, and a full message whenever an alarm, failure, or scan occurs.

For the Interval Types (Models 375 and 2100), the data is logged on two different intervals, depending on the status of the device. The normal log interval is used when the device is not alarming or failing. The alarm log interval is used when the area monitor is alarming or failing. Typically the alarm log interval is set to log data at a faster rate to collect more information during an alarm.

The Model 720 is similar to an Event device in that it sends a heartbeat (typically at five-minute intervals), but when it detects radiation, it will gather data for about 30 seconds before sending an alarm message.

9.3 Web Interface

The LMI Universal web application allows users anywhere on the network with appropriate network access to view current status, a list of “incidents” (radiation alarms or instrument failures), or to view a particular instrument’s readings in graph form. The user need only use a standard web browser such as Internet Explorer or Mozilla Firefox to access the webpage. To access the webpage, enter the URL of the web application. This is typically:

http://servername/LmiUniversal

9.3.1 Current Status Page

The Current Status page allows the user to view a simplified version of the current information for all or a selected group of instruments. This shows the name of the device, its status, the last time data was saved in the database, and a link to the camera, if available.

Clicking on the Name of the Device will take you to its Current Status Page (see below).

You can also click on the link called Incident History, which will take you to the Incident History Page.

Figure shows an example of the Current Status page.
The page dynamically updates itself every 10 seconds, which means that the user never has to refresh the page in order to get the most recent information. The color-coded Status column indicates one of four possible states: OK, Failure, Alarm, and Missing. If an instrument is either alarming or missing, an audible tone will sound. This tone can be customized by replacing the “alarm.wav” file, located where the web application is installed.

**NOTE:** If you choose to change the audible tone, the new tone must be named exactly the same as the old tone (alarm.wav).

By default, all devices are displayed. To narrow down the list, use the drop-down boxes to apply a filter to the list as shown in Figure 39.
9.3.2 Location Maps
This is similar to the Current Status page, only this page shows any pictures in the Maps folder of the Web Site, along with any associated devices on each picture.

Like the Current Status page, you can click on the name of the device to go to its Current Status page. If there isn’t a Last Message Time, then the device has yet to send a message at all. The colored status line shows the simplified status of the device, and if there is a camera, an icon will show up at the bottom of the instrument’s box.

You can choose which image to look at by using the drop-down box labeled Map. By default, all devices are displayed. To narrow down which devices are shown, use the drop-down box marked Device Type to only show devices of a certain type.

9.3.3 Device Current Status Page
Each Device has a Current Status Page to show its full status and background reading(s). All of them have a similar format to the following given example (a model 375 Current Status Page).
Figure 40 – Example of a Current Status Page

- **Last Updated:** This is the last time the page was refreshed.

- **Serial Number:** The Serial Number of the Device.

- **Last Message:** The last time a message was saved into the database. If no messages were ever saved in the database, then “???” will appear here instead of a time (similar to the example picture). This is here to see that if the status is missing, when the last message was sent.

- **Status and Comment:** Here the Full status is shown, if available or different from the simplified “Ok,” “Alarm,” or “Fail” status from the Main Current Status Page. The Model 720s also have an extra field here to show what, if any, Isotopes it is currently detecting.

- **Background Reading(s):** Depending on the type of device, this may show either a single background reading (as the example, or the Model 720), multiple readings (for the Model 2100), or attempt to mimic the user interface of the device (for the Models 4906, 53, and 54).
• **Placement:** The user-defined Placement of the Device, the Site, Building, Area, and Location.

• **Links:** Any other WebPages you can reach from the current page:
  
  o **Camera:** If available, will take you to the camera associated with the device. It will not be shown if no link was provided.

  o **Background Graph:** Click on this to go to the Device specific Background Graph (see below).

  o **Spectroscopic Graph:** (Model 720 only) Click on this to go to the Model 720 Spectroscopic Graph (see below). This link will attempt to use the latest spectroscopic reading.

  o **Scan History:** (Models 2100, 4906, 53, and 54 only) Click on this to go to the Device specific Scan History Page (see below).

• **Error:** If an error occurred, a description of it will appear here.

### 9.3.4 Device Background Graph Page

The Graph page allows the user to view the background readings as a graph plotted over time. Graphing features include the ability to plot readings using presets of today, yesterday, this week, last week, or a user-defined interval for a specific serial number. The Graph also shows Statistics of the background readings, the maximum value in the range, the minimum value in the range, and the average of the range. Clicking on a point on the plot will show detailed information about that point.

It’s possible to zoom in around that point by selecting a zoom value in the Zoom drop-down box.

For Devices with multiple readings, an extra section will allow you to change the color of the line that represents a certain detector’s background plot.

See Figure 41 for a screen shot of the Graph page.
If you want a smoother graph, increase the smoothing factor (any integer between 1 and 10) to accomplish this, as demonstrated in Figure 42 and Figure 43.
9.3.5 Spectroscopic Graph

The Spectroscopic Graph page shows the spectroscopic ID of any detected radiation at the given time. This graph is similar to the regular graph, but the x-axis goes by the channel rather than by date. Unlike the regular graph, this graph is not allowed to zoom in or out, as there is no more or less relevant data to look through, nor can this graph be smoothed, as that would distort the data. Finally, since it is not a value through time, you cannot look at it for a range of dates, but only one date and time per view. You can use the button marked “Add 1 min.” to move forward in time by one minute.
9.3.6 Incident Summary Page
The Incident Summary page keeps track of any incidents that take place on any or all instruments that are connected to the Supervisor service. Incident data can be saved to a comma-delimited file (.CSV).

The user can select a time period to view incident data in the same manner as the Background Graph pages. The user can also narrow down the incident list to a particular site, building, area, and location in the same manner as the main Current Status page.

By clicking the Edit text in the second to last column, you can add or edit a comment describing the Incident, usually what occurred and how it was resolved.

The default view shown when the Incident Summary page is first loaded is shown in Figure 45.
If a camera logo appears next to an alarm incident, this means that an image was taken at the time of the incident and is available for viewing. Click the camera image to open a separate window and view the image. If the red camera logo appears next to an alarm incident, this means that the camera for that unit was enabled but is either malfunctioning or missing.

An example of the time and location filters in use is shown in Figure 46.
9.4 Database Table Plan

The Database is built to maximize the lifespan of the instrument data input. To accomplish this, it is set up as a Relational Database, with many small tables that reference other tables as their parent table, most leading back to a single root table.

9.4.1 UniversalConfig Table

The UniversalConfig table is the only stand-alone table. It should not be necessary to modify or look at this table during normal operation. It stores many of the settings the Universal Service uses to run.

Data it stores

- When the data was last updated.
- The port to listen on.
- The email settings (From, who to send to, what title to use, etc.).
The website location (for use with the camera).

The old record deletion schedule (number of days/weeks/months, whether to archive, and whether or not to do it at all).

9.4.2 Device Table
The Device is the root table for all other tables in the database. It stores the general information unique to each device.

Data it stores

- When the data was last updated.
- Whether or not the device is enabled, and thus will store data.
- A number that represents the Type of the Device (M375 = 0, M54 = 1, M4906 = 2, M53 = 3, M2100 = 4, M720 = 5, M375-P = 6).
- The Device's Attributes (Name, Serial Number)
- Location Data (Site, Building, Area, Location)
- The Camera data for the camera connected to the device (whether or not the camera is enabled, where to look for a still shot and streaming view).
- The Comments for this particular device, defined by the User.

Child Tables

- LogInterval (0 to 1 connections)
- MapAndLocation (0 to 1 connections)
- IncidentHistory (0 to many connections)
- History (0 to many connections)
- ScanHistory (0 to many connections)
- CurrentStatus (0 to 1 connections, special)
9.4.2.1 LogInterval Table
The LogInterval table stores the times the device will use to log the readings from the device, if applicable to the device (currently, only Model 375, 375-P, and 2100 devices use this table).

Data it stores
- Number of minutes to log the readings when alarming.
- Number of minutes to log the readings otherwise.

9.4.2.2 MapAndLocation Table
The MapAndLocation table stores the location of the device when showing a map for the website.

Data it stores
- X and Y locations on the map (image shown on website)
- X and Y locations on the picture (image of map scaled to Service UI)
- The map to associate with.

9.4.2.3 IncidentHistory Table
The IncidentHistory table stores any incidents (alarms, failures, etc.) and their associated data.

- A number representing the status of the Incident (0 = OK, 1 = Failure, 2 = Alarm, 3 = Missing)
- The start time of the incident.
- The end time of the incident (null if ongoing).
- The picture to show for the incident.
- The user-defined comment for the Incident.
9.4.2.4 History Table
The History table stores the normal readings of the detector(s) of the device (or the background readings for some devices).

Data it stores

- The time of the Readings.
- The units the Readings are in.

Child Tables

- HistoryDetectorData (0 to many connections)
- M720SpecChannelData (0 to many connections)
- M720SpecNuclideData (0 to many connections)

9.4.2.4.1 HistoryDetectorData Table
The HistoryDetectorData table stores the actual reading(s) of the Detector.

Data it stores

- The Reading’s name.
- The Reading’s value.

9.4.2.4.2 M720SpecChannelData Table
The M720SpecChannelData table stores the Model 720 channel and its current reading.

Data it stores

- The Channel’s ID (0-255)
- The Channel’s reading in counts.
9.4.2.4.3 M720SpecNuclideData Table
The M720SpecNuclideData table stores the isotope(s) that the Model 720 thinks it might be reading.

Data it stores

- The name of the isotope it suspects it is detecting.
- How confident it is that it is detecting this isotope.

9.4.2.5 ScanHistory Table
The ScanHistory table stores the readings taken for a scan.

Data it stores

- The time of the scan’s completion.
- The number of seconds the scan took.
- The count rate units selected during the scan.
- The activity units selected during the scan.
- The ID associated with the scan (typically an ID of what was scanned, if applicable and provided.)

Child Tables

- SetPoint (0 to many connections)
- M2100ScanType (0 to 1 connection)
- ScanDetectorData (0 to many connections)

9.4.2.5.1 SetPoint Table
The SetPoint table stores Set Points of the Scan, such as the values it should have alarmed at.

Data it stores

- The Name of the Set Point.
The Value of the Set Point.

9.4.2.5.2 M2100ScanType Table
The M2100ScanType table stores what type of scan the Model 2100 took, if provided (usually Steel or Slag).

Data it stores
- The Scan Type.

9.4.2.5.3 ScanDetectorDataTable
The ScanDetectorData table stores any pan detector data for each scan.

Data it stores
- The Name of the Detector.
- The Serial Number of the Detector.

Child Tables
- ScanDetectorAlarm (0 to many connections)
- ScanDetectorFailure (0 to many connections)
- ScanDetectorReading (0 to many connections)

9.4.2.5.3.1 ScanDetectorAlarm Table
The ScanDetectorAlarm table stores any alarms that happened during a scan.

Data it stores
- The Name of the Alarm that occurred.

9.4.2.5.3.2 ScanDetectorFailure Table
The ScanDetectorFailure table stores any failures that happened during a scan.
**Data it stores**

- The Name of the Failure that occurred.

### 9.4.2.5.3.3 ScanDetectorReading Table

The ScanDetectorReading table stores the Readings that were taken during a scan.

**Data it stores**

- The Name of the Reading.
- The value of the Reading.

### 9.4.2.6 CurrentStatus Table

The CurrentStatus table stores a scratchpad of information regarding the current status of the device. This table is special in that it is weakly connected to the latest reading (updated and maintained by the Universal service itself), as well as strongly connected to a parent device.

**Data it stores**

- The latest History row for the current status information.
- A number that represents the status (0 = OK, 1 = Failure, 2 = Alarm, 3 = Missing), similar to the IncidentHistory table.
- A string that is also a representation of the current status.
- A string that shows any alarm or failure that the current device is experiencing.
10.0 Ethernet Information

10.1 IP Addresses

Note: Never connect a device into your network unless you are sure the IP Address and network mask are configured correctly. Failure to do so may disrupt your network.

Each device on a network has a unique address. This number is called the Internet Protocol (IP) address. This number can either be dynamically or statically assigned. A static IP address is assigned to the device manually. A dynamic IP address is automatically assigned by a Dynamic Host Configuration Protocol (DHCP) server. The format is a 32-bit numeric address written as four numbers separated by periods (dots). Each of the four numbers ranges from 0 to 255.

10.2 Ethernet Cable Termination

Looking at the connector with the pins at the top facing you, pin 1 is on the left. Pin 8 is on the right.

Pin 1 – White/Orange

Pin 2 – Orange
Pin 3 – White/Green

Pin 4 – Blue

Pin 5 – White/Blue

Pin 6 – Green

Pin 7 – White/Brown

Pin 8 – Brown

**Tools required for cable termination**

- Wire Strippers
- Network Cable Tester
- Network Cable Crimper
- RJ-45 connectors appropriate for cable conductor type.
- Category 5E Network Cable, Stranded or Solid conductor.

Stranded cable is generally used where the network cable can be moved, such as patch cables. Solid cable is used where the cable will be fixed, such as internal wiring in walls.

If possible, save some of the extra cable that has been pulled into where the switch is located. This extra cable can be used to make patch cables, if necessary.

1. Strip off approximately 2.5 cm (1 in.) of the cable jacket.

2. Untwist the four pairs and straighten them out.

3. Arrange them in a fan shape, following the color order above, with the White/Orange wire on the left, and the Brown wire on the right.

4. Bring the wires together until they touch. Double-check the order.

5. Cut the wires to make a 90° angle approximately 1.3 cm (0.5 in.) from the end of the jacket. The wires must be cut straight so that they fit all the way into the connector to make good contact with the pins.

6. Align Pin 1 of the cable with Pin 1 of the connector and insert the cable into the connector. Push firmly so the wires go all the way to the top of
the connector and the jacket goes into the connector by about 0.5 cm (3/16 in.). Again, check to make sure the colors are in the right order.

7. Place the connector into the crimp tool and squeeze the handle hard.

8. Inspect the connector to make sure all pins were crimped.

9. Repeat steps 1-8 for the other end.

10. Use a cable tester to test the cable for shorts and crossed wires.
11.0 Troubleshooting

The most common issues when setting up the hardware and software are:

- Unable to set the network settings of the Model 375
- A device is reported as “MISSING”
- Errors when accessing the webpage

The first two are almost always a network issue, while the last is usually a problem with the server configuration. For troubleshooting purposes, start with the device and work back to the server.

11.1 Unable to set the network settings of the Model 375

The Ethernet settings can be configured in one of two ways, depending on the firmware version. Firmware versions 39801n11 and earlier use UDP communication and require the use of the Setup Utility. Firmware versions 39801n12 and higher can be configured by accessing the area monitor by its IP address in a web browser. The Setup Utility can still be used to see the area monitor and its network settings, but it will not be able to change them.

If the area monitor cannot be seen in the Setup Utility and has firmware 39801n11 or older, try one or more of the following:

1. Move the area monitor to the same network (location) as the server and connect it to the network there.

2. Connect a laptop loaded with the Model 375 Setup Utility directly to the area monitor using a crossover cable if necessary. The network settings on the laptop do not matter, but the network card needs to be configured for 10 Mbs/ Half-duplex.

3. Disable or modify the firewall settings to allow traffic on UDP port 20034. If you are not sure how to add a rule to the firewall, temporarily disable the firewall. If you still cannot see the area monitor in the Model 375 Setup Utility, re-enable the firewall as this is not the cause.
4. Cycle the power on the area monitor.

5. Try pinging the area monitor if you know its IP Address. See instructions below. If possible, try from the server and from a computer on the same network as the area monitor.

If the area monitor cannot be seen in the Setup Utility or by a web browser and has firmware 39801n12 or newer, try one or more of the following:

1. Disconnect all area monitors that are not working except for one. If the area monitors have the default settings, then they will all be set to the same IP address, which will make it difficult to access them.

2. Try pinging the area monitor. See instructions below. If possible, try from the server and from a computer on the same network as the area monitor.

3. If you can see it with the setup utility but not in a web browser, contact your IT department as they may need to change your computer’s security settings to see the web page running on the area monitor.

4. Cycle power on the area monitor.

11.2 Troubleshooting the Devices

Some basic things to ensure are that the device is turned on, connected to AC power, and that a network cable is connected to it. For the Models 2100, 4906, 53, and 54, the Supervisor Software needs to be running on the instrument (it starts up automatically when you turn on the machine).

11.2.1 Troubleshooting the Model 375

11.2.1.1 Check the Settings of the Model 375

If the Model 375 has N11 or older firmware, run the Model 375 Setup Utility. Otherwise, use a web browser to connect to the Model 375 itself.

Confirm that the Supervisor IP Address is the IP Address of the computer that is running the Universal Software. If you are using the Model 375 Setup Utility, make note of the IP Address of the 375 itself. The IP Address is 0.0.0.0, then use the IP Address in the drop-down list at the top of the screen, which is the real (server supplied) IP Address.

Confirm that the TCP/IP Port is the port the Universal Software is listening on.
11.2.1.2 Check the Ethernet Status Lights

If the cover is removed from the area monitor to expose the Ethernet board, there are two status LEDs that can be used to help troubleshoot connectivity problems. These LEDs are located near the Ethernet connector.

The yellow LED is the activity indicator, and the green LED is the link indicator. When powering on the area monitor, the green LED will blink once. This will indicate that the Ethernet board is getting power. With an Ethernet cable connected, the green LED will be steady ON, which indicates a link to the network. The yellow LED should blink to indicate network activity. Depending on network activity, the light may blink occasionally or may blink very fast.

11.2.2 Troubleshooting the Model 720

11.2.2.1 Check the Settings on the Memory Card

Get the memory card from the Model 720. Make note of the IP_ADDR, TFTP_ADDR, and the ID_SHORT. The IP_ADDR is the IP Address of the Model 720. This should be both unique and a valid IP Address on your intranet. The TFTP_ADDR should be the IP Address of the computer that is running the Universal Software. The ID_SHORT is the Serial Number this Model 720 is sending out via the translator. It should be prefixed with “Mon.” For example, if the Model 720 Serial Number is 555555, then the line should look like this: “ID_SHORT= Mon555555”.

This information should be in both the UNIT.INI and the CONFIG.INI.

11.2.2.2 Check the 720 Translator’s Settings

Run the Model 720 Translator program. Confirm that the Model 720 is in the list with the correct Serial Number (555555 from the previous example). Also make sure that it has the same IP Address as the IP_ADDR that you checked earlier. If it is not, add a new entry (using the text boxes at the top of the program, clicking the Add button when you are done as it is lit up) or edit the incorrect one by clicking on it in the list and changing the incorrect information (using the text boxes in the middle of the program, and clicking the Update button when you are done and it is lit up).

Confirm that the Universal Port Number is the same one as the one the Universal Software is listening on.

11.2.3 Troubleshooting the Models 2100, 4906, 53, and 54

Go to the Settings screen and click on the Operational Setup button. From there, go to the Network tab. Check to ensure that the Universal IP Address is the IP Address of the computer running the Universal Software. Ensure that
the Universal Port is the Port Number the Universal is listening on. And finally, ensure that Enabled is checked next it then.

11.3 Troubleshooting the Universal Software
Run the Utility Service on the Computer with the Universal Software.

11.3.1 Check the Devices
Go to the Devices tab and ensure that all of the devices are in the correct list and that each one is enabled. If a device is in the wrong list, Delete it from that list and Add it to the correct one (keeping all of the information the same, such as the Name, Site, Building, Area, Location, any Camera Information, and the Comment).

If a device was accidently disabled, click on the Edit button, check the “Enabled” check box and Save it.

11.3.2 Check the Connection to the Database
Go to the Database tab and click on the Test Connection Button. If this fails, ensure that you have the correct server name (and instance name if needed) as well as the correct log-in if you are using SQL Authentication.

11.4 Troubleshooting the Network
Most network problems stem from one computer not being able to talk to another. We can check whether a computer can talk to another by pinging from one to the other.

11.4.1 How to Ping a Computer
Go to the computer you want to ping from and open a Command Prompt. You do this by clicking Start, going to All Programs -> Accessories -> Command Prompt.

For this example, we'll pretend that the computer you are trying to ping has the IP Address “192.168.10.66”.

Type in “ping 192.168.10.66” without any quotation marks and then hit the Enter key. The computer will take over and start typing in lines of its own. If all went well, the screen should look similar to the following:

C:>ping 192.168.10.66
Pinging 192.168.10.66 with 32 bytes of data:

Reply from 192.168.10.66: bytes=32 time<1ms TTL=128
Reply from 192.168.10.66: bytes=32 time<1ms TTL=128
Reply from 192.168.10.66: bytes=32 time<1ms TTL=128
Reply from 192.168.10.66: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.10.66:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milliseconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

There should be no lost packets, and the time for each packet should be less
than 100 ms. If there are any lost packets or error messages, then either the
device is not properly configured on the network, or there is a problem with the
network.

11.4.2 Ping the Universal from the Device or its Network

11.4.2.1 Model 375 or 720

Find a computer on the same network as the device and try to ping the
computer with the Universal Software.

11.4.2.2 Model 2100, 4906, 53, 54

Go to the device and temporarily turn off the Supervisor. To do so, click on the
Exit button and type in the master password. Then Click on the button “Exit
Supervisor.”

From there, try to ping the computer with the Universal Software.

Once done, turn the Supervisor program back on by clicking on the icon on the
desktop that says “Model XXXX Supervisor” where XXXX is either 2100,
4906, 53, or 54.

11.4.3 Ping the Device from the Computer with the Universal
Software

Go to the computer with the Universal Software and try to ping the Device.

If you don’t know the IP Address of the device, either see previous sections
11.2.1 or 11.2.2 on how to find the IP Addresses for Model 375s and 720s or go
to the device and type “ipconfig” into the Command Prompt (without the
quotes). The IP Address on the line IPv4 will be the device’s IP Address.

11.4.4 Check any Firewalls between the Devices and the Computer
with the Universal Software

All Devices need the TCP port chosen by the user to be open (defaulted to
50000), so any firewalls running on the computer with the Universal Software
(or on any routers between the device and the computer) need to allow both the
IP Address of the Device and the Computer to communicate and allow the
TCP Port to be open.
The 375 Setup Utility (for N11 and older) and Device Finder need UDP port 20034 open to talk to or search for 375s.

Model 720 devices need UDP ports 244 and 69 open to communicate between them and the 720 Translator Service.

11.4.5 Check any other Firewalls and Routers
If you have the SQL Database and/or the Website on a different machine, ping Universal Software <-> SQL Database and Universal Website <-> SQL Database. To communicate with an SQL Database, TCP ports 1433 and the range from 1024 and 5000 need to be open, and of course so to do the IP Addresses of the computers in question.

11.5 Troubleshooting the SQL Database.
Go to the computer with the SQL Database and run the SQL Server Management Studio (SQL Server Management Studio Express if you are running an Express version of a Microsoft SQL Server).

Make sure that the server name, database user name, and database password in the Universal Server Utility all match your SQL Server configuration.

Figure 48 - SQL Server Management Studio Express

Click on the plus sign next to the word Databases. The database “LmiUniversal” should appear in the list opened up beneath it. If it does not,
install and run the Database Setup program. In the LmiUniversal Database, click the plus sign next to the word “tables.” If nothing except the folder “System Tables” appears, install and run the Database Setup program. If there are tables, check the tables “dbo.Devices,” “dbo.History,” and “dbo.CurrentStatus.”

![Database Setup](image)

**Figure 49 - Showing dbo.Device table in the LmiUniversal database**

Check a table by right-clicking on it and then clicking on “Select top 1000 rows.” In the “dbo.Devices” table, you should see the device you are looking for. Make note of the number in the ID column, henceforth referred to as the device’s ID number. In the “dbo.CurrentStatus” table, look for the device’s ID number in the column labeled Devices_ID. If it is not there, then the device has never sent a message to the Universal or the Universal has been unable to save the message to the database. Please check the previous sections to ensure that both the device(s) and the Universal Software are set up correctly.

If the Device’s ID is in the “dbo.CurrentStatus” table, then check the “dbo.History” table. If it is not there, then the device has never sent a message to the Universal or the Universal has been unable to save the message to the
database. Please check the previous sections to ensure that both the device(s) and the Universal Software are set up correctly.

11.6 Troubleshooting the Universal Service

First make sure the Universal Service is running. Launch the Services Manager by selecting “Run…” from the Start Menu. Type in “services.msc” without quotes and press enter. The Services console should display.

![Services Console](image)

Check that the Universal Service status is “Started” and that the Startup Type is set to “Automatic.”

If the service is not started, click the Start Service button in the toolbar. If the Startup type is not “Automatic,” the service will not start automatically when the computer is started. Right-click Universal Service and select Properties.
Make sure the properties for the service match the settings in the screen shot above.

**NOTE:** It can take up to one minute before any data is saved in the database after the service has been started.
If the service is running and configured correctly, check to make sure that the
service is successfully logging to the database.

To do this, go to the Start Menu and open SQL Server Management Studio
under the “Microsoft SQL Server” program group. If you are running an
express version of Microsoft SQL Server, open SQL Server Management Studio
Express.

Click the plus icon next to “Databases” in the left pane. Click the plus icon next
to “LmiUniversal,” then click the plus icon next to the Tables folder. Your
screen should now look like Error! Reference source not found.70.

If you have restarted the Universal Service, the “dbo.Device” table should
appear within 60 seconds. If the “dbo.Device” table is not created within that
time, refer to the “Configuring SQL Server for the Universal Service” section on
page 24. Also, make sure that the server name, database user name, and
database password in the Universal Server Utility all match your SQL Server
configuration.

Right-click the “dbo.Device” table in the left pane and click “Select Top 1000”.
Your screen should now resemble Figure 70.

If data is being logged into the “area_monitor” table, the Universal Service is
running correctly.

If data is not being logged into the “dbo.Device” table, first check to make sure
that your area monitors have been added to the Service Utility. For more
information on the Service Utility, refer to page 56.

If your area monitors appear in the Supervisor Service Utility, use the Universal
Setup Utility to verify that the destination IP address matches that of the
computer hosting the database. Also make sure that the network settings for
each area monitor are correct in accordance with their location on your network.

11.7 Troubleshooting the Web Page
The following is a list of errors that are commonly encountered with the
Universal Webpage.

11.7.1 Web Page does not load
First, open the IIS Manager. The IIS Manager is located in the Control Panel,
under “Administrative Tools.”

Click the plus icon next to your computer name, then click the plus icon next to
the “Web Sites” folder. Click “Default Web Site” and see if it is running. If it is
stopped, click the Play button under the Menu bar to start the web site.
If the Web Site is running and you still get this error, check to see if the “LmiUniversal” virtual directory is included in the Default Web Site. If it is not, refer to the “Configuring Internet Information Services” section for instructions on how to add the LmiUniversal virtual directory.

11.7.2 Directory Listing Denied
First, open the IIS Manager. The IIS Manager is located in the Control Panel, under “Administrative Tools.”

Click the plus icon next to your computer name. Click the plus icon next to the “Web Sites” folder. Click the plus icon next to “Default Web Site.” Right-click the “LmiUniversal” virtual directory, then click “Properties.”

Click the “Default Documents” tab. The first default document listed should be “default.aspx.” If CurrentStatus.aspx is not in the list, add it and move it to the top of the list.

If you have any further questions on how to add a default document to a virtual directory, refer to the “Configuring Internet Information Services” section.

11.7.3 Invalid object name “dbo.xxxx”
If you get this error, then the “xxxx” table does not exist in the SQL Server database.

Install and run the Database Setup utility.

11.7.4 Login failed for user “xxxxxx”
The most common reason for this error is that the username and/or password that is set in the Universal Service Utility does not match the username and password that is set in Microsoft SQL Server.

Go to the Start Menu and open SQL Server Management Studio under the “Microsoft SQL Server” program group. If you are running an express version of Microsoft SQL Server, open SQL Server Management Studio Express.

Click the plus icon next to the “Databases” folder. Make sure that the “LmiUniversal” database is present. If it is not present, refer to the “Configuring SQL Server for the Universal Service” section on page 43.

Click the plus icon next to the “Security” folder, click the plus icon next to the “Logins” folder. If you have not created a login for the Universal Service, refer to the “Configuring SQL Server for the Universal Service” section on page 43.

Open the Universal Service Utility. Click the “Database Settings” tab and verify that the user name and password matches the user name and password from the login properties window in SQL Server Management Studio. When the user
name and password is set correctly, click “Save Settings” in the Supervisor Server Utility.

**NOTE:** You may need to restart the Supervisor service at this time. Refer to page 77 for instructions on restarting the Supervisor service.

**11.7.5 Web Page loads, but does not show any Devices**

Some versions of Windows have web page access SQL Databases under a separate login when using Windows Authentication. If you find that this is the case, all you need to do is create another SQL login called NT AUTHORITY\SYSTEM. This will be exactly like the first login you created using Windows Authentication, making it default to LmiUniversal and marking it as a db_owner of LmiUniversal.

**11.7.6 Default Web Site Won’t Start – Unexpected Error 0x8ffe2740 occurred**

If you get this error, another program on your computer is using TCP port 80, which is the port that IIS uses to host the web page.

Click the Start Menu, then click “Run.” Type “cmd,” without the quotation marks, and click “Enter.” In the command window, type the following:

```
netstat –anop TCP|find “:80”
```

This will give you some details of what process is using TCP port 80. The only information needed here is the PID (process identifier).

The next step is to match this PID with an actual process that you can identify. To do this, type the following command in the command window:

```
tasklist /SVC /FI “PID eq xxxx”
```

where xxxx represents your PID number. This should give you a clear picture of what program is in use. Configure the offending program to use a different TCP/IP port, or shut the program down.

**11.7.7 Could not load file or assembly ‘App_Licenses’ or one of its dependencies. The module was expected to contain an assembly manifest.**

Go to the Control Panel, then click “Add/Remove Programs.” Click “Microsoft .NET Framework 4.0.” Click the “Change/Remove” button. Select the “Repair” option and click “Next.” Follow the prompts to repair your Microsoft .NET Framework installation.

If this does not resolve the error, call Ludlum Measurements for further assistance.
11.7.8 Current Status page shows no area monitors
The Web Page will only display area monitors that are added to the Supervisor service. To add an area monitor to the Supervisor service, use the Model 375 Supervisor Server Utility.

For instructions on how to use the Universal Service Utility, refer to page 56.

11.7.9 Current Status page shows device(s) with a status of “Missing”
Verify that the device in question is powered on and connected to the network.

Please note that model 720s may take 5 to 10 minutes to send their first message.

Verify that Windows Firewall is not turned on. If it is desired to use Windows Firewall in conjunction with the Universal Service, configure Windows Firewall to allow the Universal Service through the firewall.

If this doesn’t fix the problem, use either the web interface (firmware versions N12 and later) or the Setup Utility (firmware versions N11 and earlier) to verify that the destination IP address matches that of the computer hosting the Supervisor service. Also make sure that the network settings for the area monitor are correct in accordance with their location on the network.

11.8 Troubleshooting 375 FTP Firmware Updates
Go through the following steps to troubleshoot the FTP firmware updates:

1. Verify that there is a folder named “Firmware” in the $C:\Inetpub\ftproot$ folder. If the Firmware folder does not exist, create it.
   **NOTE:** The name of the Firmware folder is case sensitive!

2. Verify that the two firmware files provided by LMI are in the correct folder, which is $C:\Inetpub\ftproot\Firmware$.

3. Verify that the two firmware files provided by LMI have the correct extensions. The 39801Nxx.bin file should have its .bin extension, while the file titled “FirmwareVersion” should have NO extension.

4. Make sure that the FTP Publishing Service is running. To do this, go to “Run” in the Start Menu and type “services.msc,” without the quotes. Scroll through the list of services and click “FTP Publishing Service.” If the service is stopped, start the service.
5. Use either the web interface or the Setup Utility (discussed on page 49) to verify that the Destination IP Address of the area monitor is the same as the computer that is hosting the FTP site.

6. Verify that all firewalls, including Windows Firewall, are turned off on the computer hosting the FTP site.

11.9 Replacing 375 Rabbit Ethernet Boards

The following steps will assist the user in replacing the Rabbit Ethernet board on the Model 375 Area Monitor.

The Model 375 Area Monitor will either have the Rabbit Ethernet board mounted to the side of the Area Monitor or inside of the area monitor. Refer to the appropriate instructions for your type of Model 375 Area Monitor.

Figure 53 shows an external Ethernet board, while Figure 54 shows an internal Ethernet board.

![Figure 53 – External Ethernet Board](image-url)
Replacing an External Rabbit Ethernet Board

1. Remove the four screws from the corners of the Ethernet board. See Figure 55.
2. Disconnect the 3-pin MTA connector from the Ethernet board to separate it from the area monitor. See Figure 56.

3. Disconnect the CAT-5 cable from the Rabbit board.

4. Remove the four nuts from the corners of the Rabbit board to separate the Rabbit board from its case. See Figure 57.

Replacing an Internal Rabbit Ethernet Board

1. Remove the outer case from the area monitor. See Figure 58.
2. Remove the four screws from the corners of the main board and disconnect the MTA connector. See Figure 59.
3. Remove the two nuts from the corners of the bracket holding the Ethernet board. See Figure 60.

![Figure 60 – Internal Rabbit Ethernet Board](image)

4. Remove the three nuts from the corners of the Ethernet board. See Figure 61.
Figure 61 – Internal Rabbit Ethernet Board Removal