

# **LUDLUM UNIVERSAL SOFTWARE MANUAL**

**June 2025**

**Version 3.10.0 and above**



# **LUDLUM UNIVERSAL SOFTWARE MANUAL**

**June 2025**

**Version 3.10.0 and above**



**LUDLUM MEASUREMENTS, INC.**  
501 OAK STREET, P.O. BOX 810  
SWEETWATER, TEXAS 79556  
325-235-5494, FAX: 325-235-4672



# Table of Contents

---

---

<b>INTRODUCTION .....</b>	<b>1</b>
1.1 UNIVERSAL SERVICE.....	1
1.2 ASP WEB APPLICATION.....	1
1.3 DEVICE FINDER.....	2
1.4 SERVICE UTILITY.....	2
1.5 SPECTROSCOPIC AREA MONITOR TRANSLATOR SERVICE .....	2
1.6 DATABASE SETUP UTILITY .....	2
<b>SOFTWARE LICENSE AGREEMENT.....</b>	<b>3</b>
<b>GETTING STARTED.....</b>	<b>6</b>
3.1 SOFTWARE PREREQUISITES .....	6
3.2 MINIMUM REQUIREMENTS .....	6
3.3 INSTALLATION OVERVIEW – SINGLE SERVER.....	6
3.4 INSTALLATION OVERVIEW – MULTIPLE SERVERS .....	7
<b>IIS INSTALLATION .....</b>	<b>8</b>
4.1 IIS SERVER INSTALLATION – WINDOWS SERVER 2022 .....	8
<b>SQL SERVER INSTALLATION .....</b>	<b>14</b>
<b>UNIVERSAL SOFTWARE INSTALLATION .....</b>	<b>15</b>
6.1 INSTALLING THE UNIVERSAL SERVICE AND UTILITIES .....	15
6.2 INSTALLING THE UNIVERSAL WEB APPLICATION .....	15
6.3 CONFIGURING SQL SERVER FOR THE UNIVERSAL SOFTWARE .....	15
6.4 DATABASE SETUP UTILITY .....	16
6.4.1 Server Name .....	17
6.4.2 Create Universal Database using the User .....	17
6.4.3 LmiUniversal Log In .....	17
6.4.3.1 For Windows Authentication Only .....	17
6.4.3.2 For SQL Authentication Only.....	18
6.4.4 Database Action Results.....	18
6.5 CONFIGURE THE SQL CONNECTION .....	18
6.6 CONFIGURING IIS FOR THE UNIVERSAL WEB APPLICATION .....	19
6.7 TESTING THE UNIVERSAL WEB APPLICATION .....	19
<b>DEVICE CONFIGURATION.....</b>	<b>20</b>
7.1 DEVICE FINDER .....	20
7.2 MODEL 375 SERIES AREA MONITORS .....	21
7.2.1 Configuring Network Settings – Web Interface (firmware versions N12 and later) .....	21
7.3 MODEL 2100 SERIES SAMPLE MONITORS, MODEL 4906 HAND AND FOOT MONITORS, MODEL 53 PORTAL MONITORS, MODEL 3500-2502 PORTAL MONITORS, MODEL 54 ARTICLE MONITORS .....	24
7.4 CONFIGURING THE MODEL 720 FIRMWARE .....	24

7.5 CONFIGURING THE MODEL 334A ALPHA AIR MONITORS AND THE MODEL 334AB(-G) ALPHA-BETA(-GAMMA) MONITORS .....	26
<b>CONFIGURING THE SERVICE .....</b>	<b>29</b>
8.1 LMI UNIVERSAL SERVICE UTILITY .....	29
8.1.1 Devices .....	29
8.1.2 Service .....	32
8.1.3 Database .....	36
8.1.4 Location Map .....	37
8.2 CONFIGURING THE MODEL 720 COMMUNICATION SERVICE.....	38
<b>OPERATION .....</b>	<b>40</b>
9.1 E-MAIL .....	40
9.2 DATA LOGGING.....	40
9.3 WEB INTERFACE .....	41
9.3.1 Current Status Page .....	41
9.3.2 Location Maps.....	43
9.3.3 Device Current Status Page .....	43
9.3.4 Device Background Graph Page.....	45
9.3.5 Spectroscopic Graph.....	47
9.3.6 Incident Summary Page.....	48
9.4 DATABASE TABLE PLAN.....	49
9.4.1 Universal Config Table .....	49
9.4.2 Device Table.....	50
9.4.2.1 Log Interval Table.....	51
9.4.2.2 Map and Location Table .....	51
9.4.2.3 Incident History Table.....	51
9.4.2.4 History Table.....	52
9.4.2.4.1 History Detector Data Table .....	52
9.4.2.4.2 M720 Spec Channel Data Table.....	53
9.4.2.4.3 M720 Spec Nuclide Data Table.....	53
9.4.2.5 Scan History Table.....	53
9.4.2.5.1 Set Point Table .....	54
9.4.2.5.2 M2100 Scan Type Table .....	54
9.4.2.5.3 Scan Detector Data Table .....	54
9.4.2.5.3.1 Scan Detector Alarm Table .....	55
9.4.2.5.3.2 Scan Detector Failure Table .....	55
9.4.2.5.3.3 Scan Detector Reading Table.....	55
9.4.2.6 Current Status Table .....	55
9.4.2.7 Command Support Table.....	56
9.4.2.8 Commands Table.....	56
9.4.2.9 IP Addresses Table.....	56
9.4.2.10 M334 Data Table.....	57
9.5 EXPECTED DATABASE SIZE INCREASE FOR RECORDS .....	57
<b>ETHERNET INFORMATION .....</b>	<b>60</b>
10.1 IP ADDRESSES.....	60
10.2 ETHERNET CABLE TERMINATION .....	60
<b>TROUBLESHOOTING .....</b>	<b>63</b>
11.1 UNABLE TO SET THE NETWORK SETTINGS OF THE MODEL 375 OR MODEL 3276.....	63
11.2 TROUBLESHOOTING THE DEVICES.....	64
11.2.1 Troubleshooting the Model 375.....	64

11.2.2 Troubleshooting the Model 720.....	65
11.2.3 Troubleshooting the Models 2100, 4906, 53, 3500-2502, and 54.....	65
11.2.4 Troubleshooting the Model 3276.....	66
11.3 TROUBLESHOOTING THE UNIVERSAL SOFTWARE.....	66
11.3.1 Check the Devices .....	66
11.3.2 Check the Connection to the Database.....	67
11.4 TROUBLESHOOTING THE NETWORK.....	67
11.4.1 How to Ping a Computer.....	67
11.4.2 Ping the Universal from the Device or its Network.....	67
11.4.3 Ping the Device from the Computer with the Universal Software.....	68
11.4.4 Check any Firewalls Between the Devices and the Computer with the Universal Software.....	68
11.4.5 Check any other Firewalls and Routers .....	68
11.5 TROUBLESHOOTING THE SQL DATABASE.....	68
11.6 TROUBLESHOOTING THE UNIVERSAL SERVICE.....	71
11.7 TROUBLESHOOTING THE WEB PAGE .....	73
11.7.1 Web Page Does Not Load .....	73
11.7.2 Directory Listing Denied.....	74
11.7.3 Invalid Object Name “dbo.xxxx” .....	74
11.7.4 Login Failed for User “xxxxxx” .....	74
11.7.5 Web Page Loads, but Does Not Show any Devices .....	75
11.7.6 Default Web Site Won’t Start – Unexpected Error 0x8ffe2740 Occurred.....	75
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.....	75
11.7.8 Current Status Page Shows No Area Monitors .....	76
11.7.9 Current Status Page Shows Device(s) with a Status of “Missing” .....	76
11.8 REPLACING MODEL 375 RABBIT ETHERNET BOARDS .....	76
<b>VERSION HISTORY.....</b>	<b>82</b>
VERSION 3.10.0.....	82
VERSION 3.9.1.....	82
VERSION 3.9.0.....	82
VERSION 3.8.2.....	83
VERSION 3.8.1.....	83
VERSION 3.8.0.....	83
VERSION 3.7.1.....	83
VERSION 3.7.0.....	83
VERSION 3.6.1.....	83
VERSION 3.6.0.....	84
VERSION 3.5.0.....	84
VERSION 3.4.1.....	84
VERSION 3.4.0.....	84
VERSION 3.3.0.....	84
VERSION 3.2.9.....	85
VERSION 3.2.8.....	85
VERSION 3.2.7.....	85
VERSION 3.2.6.....	85
VERSION 3.2.5.....	85
VERSION 3.2.4.....	85





**Section****1**

---

# 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
- Service Utility
- Device Finder
- Model 720 Central Translator
- Database Setup Utility

## 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 timeline 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 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.

**1.6 Database Setup Utility**

This software allows the user to set up or update the Database to the latest version, as well as update or add Users for the database without needing to do so in SQL Manager itself.

**Section****2**

---

## 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 nonexclusive 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.

**Section****3**

## 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.

See the appropriate installation documentation for the above items.

### 3.2 Minimum Requirements

- Supported Operating Systems: Windows Server 2008; Windows Server 2012, Windows Server 2016, Windows Server 2019, Windows Server 2022
- 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 Communication Service. **Section 8.2**

### **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 Communication Service. **Section 8.2**

**Section****4**

## IIS Installation

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 2022

Perform the following steps to install IIS for Windows Server 2022.

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.



Figure 1 – Server Manager

2. Under the **Manage** Tab in the top right of the Server Manager window, select **Add Roles and Features**.
3. In the **Add Roles and Features Wizard** window, check **Web Server (IIS)** and click **Next**. See Figure 2. You may also be asked to add in the IIS Management Console via a pop up window. If so, click the Add Features button.



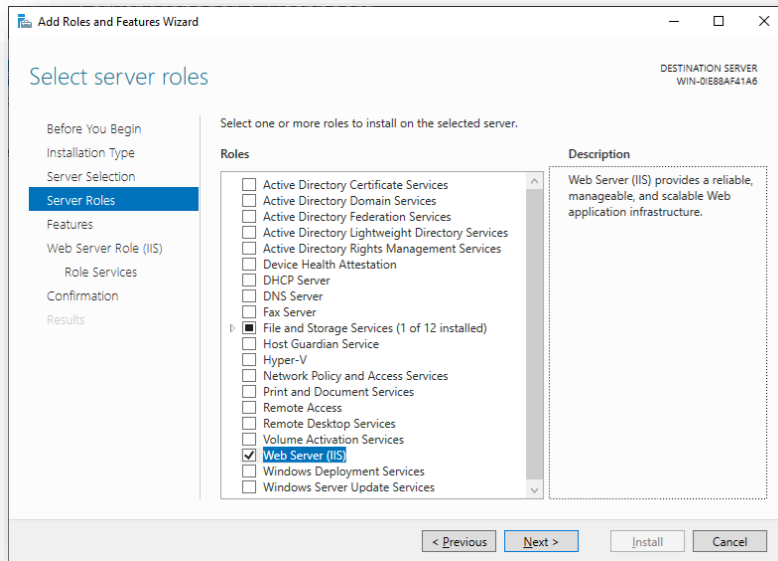


Figure 2 – Add Rules Wizard (Select Server Roles)

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.

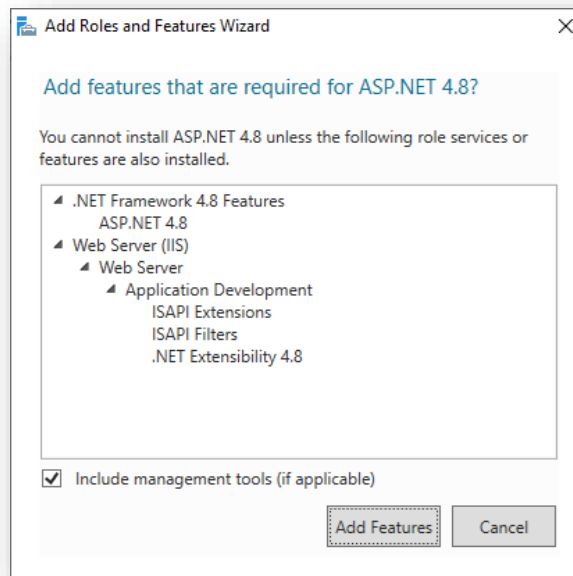


Figure 3 – Add Rules Wizard (Add role services required for ASP.NET)

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. Verify that the selected role services resemble Figure 4, Figure 5, and Figure 6 below, and then click **Next**.

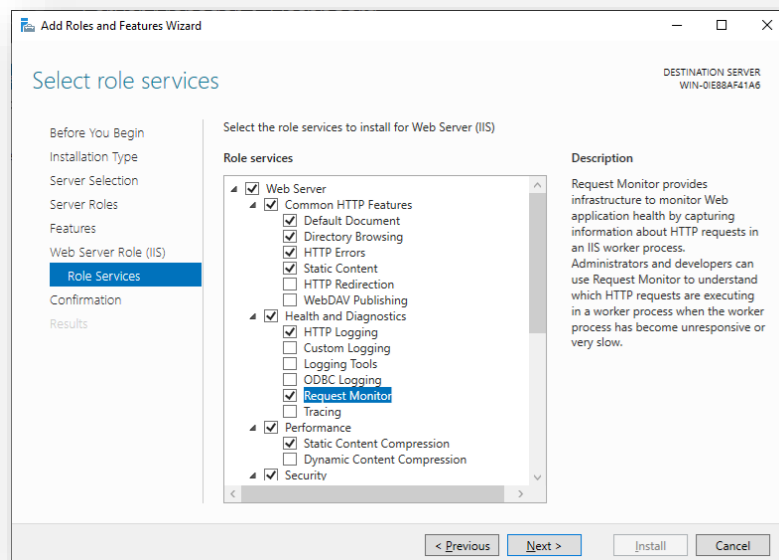


Figure 4 – Add Roles Wizard (Select Role Services 1)

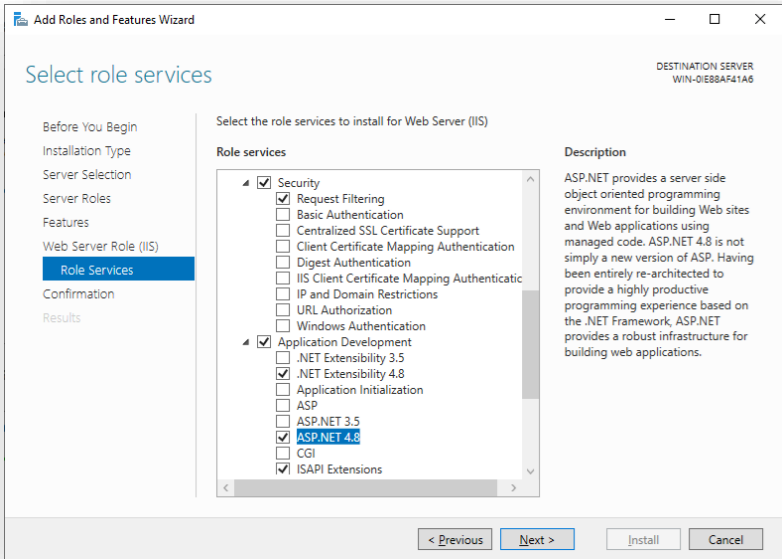


Figure 5 – Add Roles Wizard (Select Role Services 2)

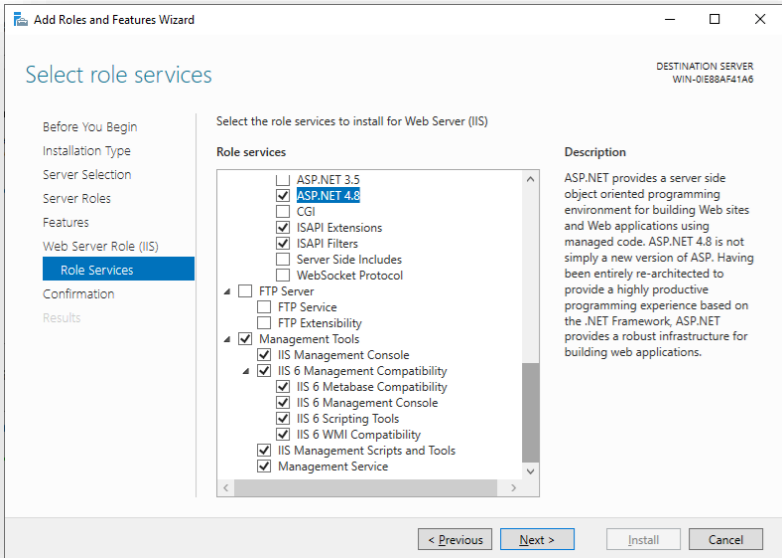


Figure 6 – Add Roles Wizard (Select Role Services 3)

9. Click **Install**. See Figure 7 – Add Roles Wizard (Confirm Installation Selections)

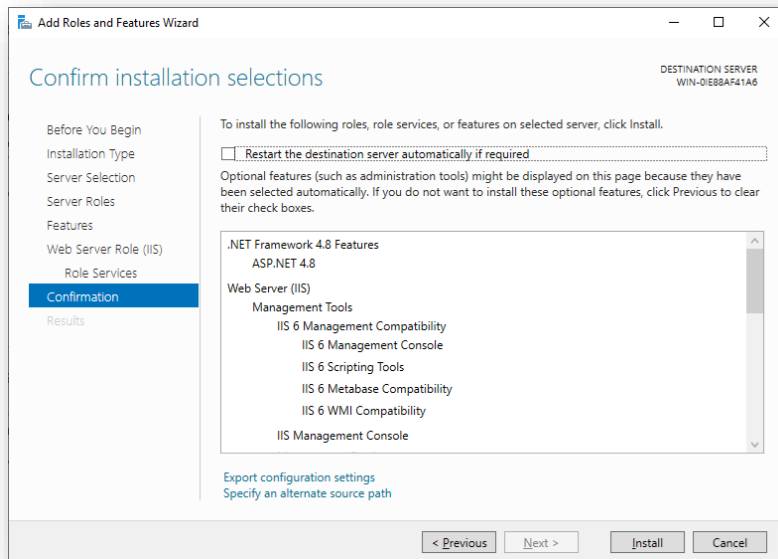


Figure 7 – Add Roles Wizard (Confirm Installation Selections)

10. If Internet Information Services (IIS) is installed successfully, click **Close**. See **Error! Reference source not found.**

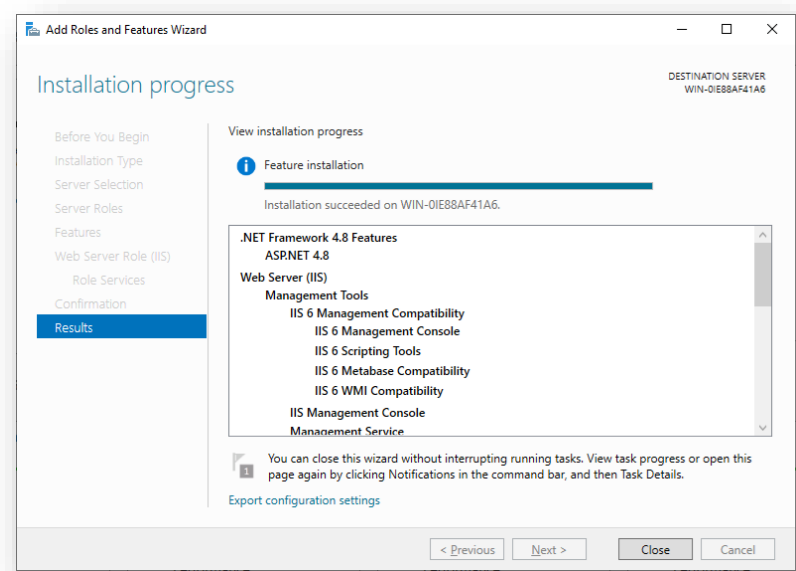


Figure 8– Add Roles Wizard (Installation Results)

**Section****5**

---

**SQL Server Installation**

---

Install SQL Server using the installer provided by Microsoft. The only requirement is to enable SQL Authentication when prompted. SQL Server Management Studio (SQLSMS) should also be installed to make database maintenance easier.

**Section****6**

---

## 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 Server, 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 to create the database, type in the appropriate Username and Password, typically the “sa” username and password.
6. Click Run Setup.
7. If the step succeeded, the program would say so, otherwise resolve the error (typically either the Server Name is wrong or the User you are using to create the does not have permission to create/alter a database).
8. At this time, you may also create or update the User(s) that the Universal software uses to access the database.

#### **6.4 Database Setup Utility**

The Database Setup Utility allows the user to add or update the database used by the Universal Software.



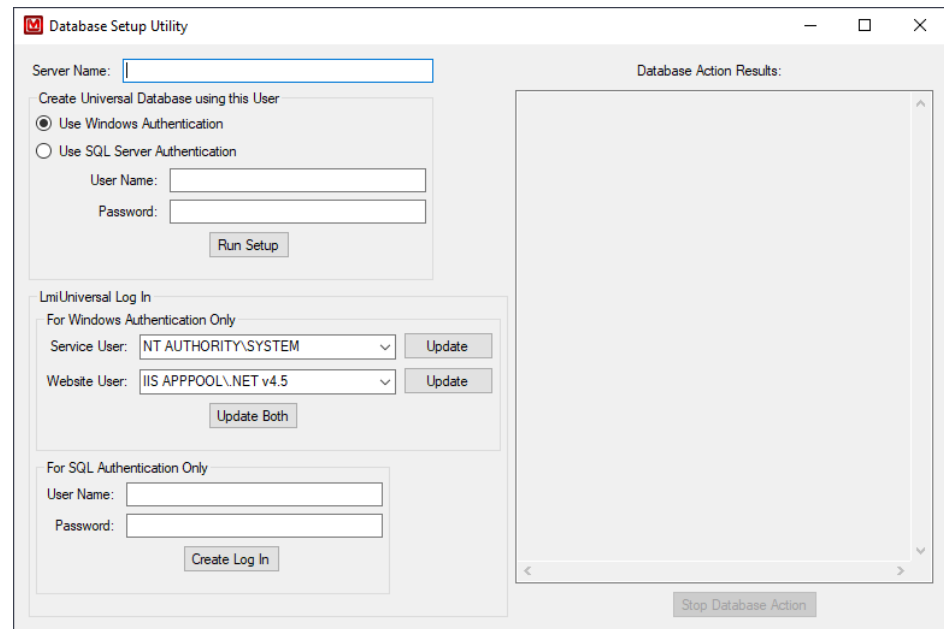


Figure 9 – The Database Setup Utility

#### 6.4.1 Server Name

This is the name of the sever that will host the LmiUniversal database (or is already hosting it), typically “localhost” or “localhost\SQLEXPRESS”.

#### 6.4.2 Create Universal Database using the User

This is the User that will be used to either create/update the LmiUniversal database, update system users to access the LmiUniversal database, or create the User Name and Password for a dedicated User for the LmiUniversal database.

#### 6.4.3 LmiUniversal Log In

This is how to update or add a User or Users that the Universal Software and the website can use to access the database.

##### 6.4.3.1 For Windows Authentication Only

For Windows Authentication Only is if you wish to use Windows Authentication with the Universal Software. Each User selection is an editable drop-down list so that you can fill in the initial value if the other values are not what your current system uses.

The Service will use a Windows provided User that typically already has full database administration privileges; thus, you will rarely need to update it.

The Website will use the name of the App Pool it was installed in as its Windows provided User. We have provided common ones. If you installed the Website into a custom one, you may type that one instead.

#### 6.4.3.2 For SQL Authentication Only

For SQL Authentication Only is if you wish to use a dedicated User to access the LmiUniversal. This User can already exist.

#### 6.4.4 Database Action Results

This is the result of trying to either run the Setup, Update the Users, or creating a User Name and Password.

### 6.5 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 10). This message showing up for the first time is normal, as there can't be any connection information saved.

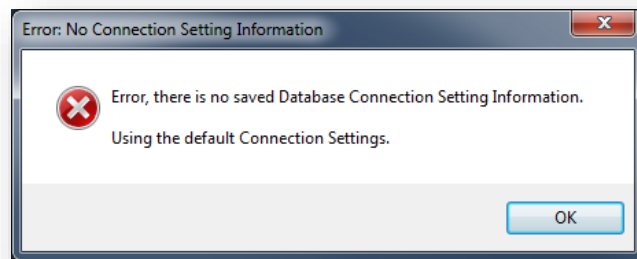


Figure 10 – No Connection

After acknowledging this message, the Service Utility will switch to the SQL Connection tab (Figure 11). 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.

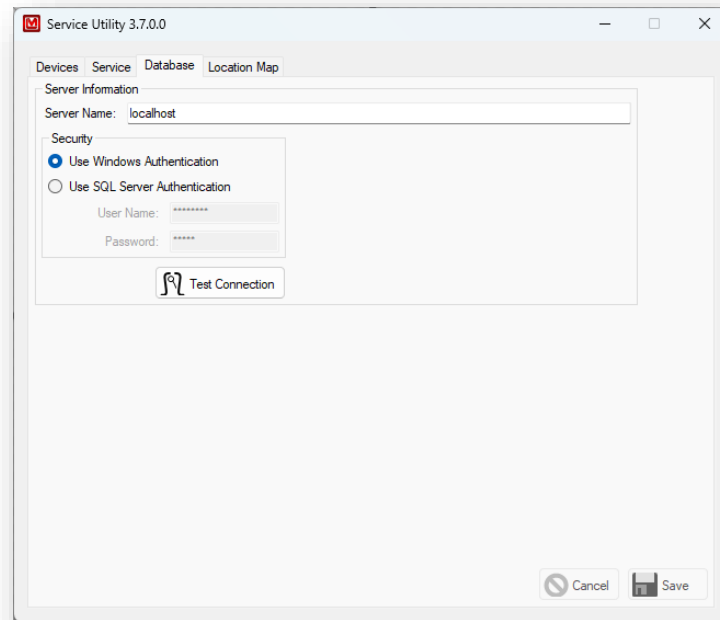


Figure 11 - SQL Connection

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.

## 6.6 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

## 6.7 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://computername/LmiUniversal>.

## Section

## 7

## 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.

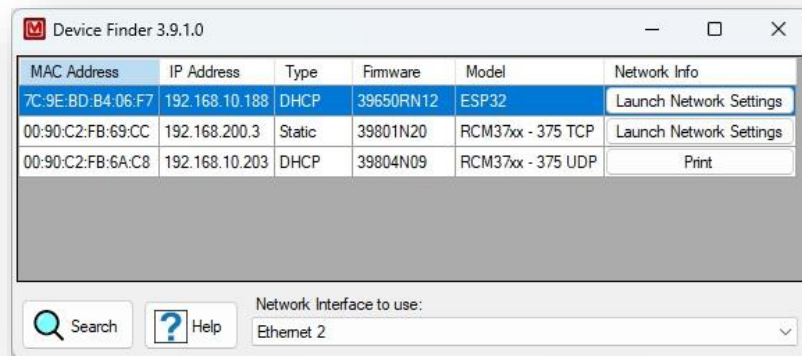


Figure 12 - Device Finder

- The MAC address, IP address, type of connection, firmware version, and Model are shown.
- Click the Search button to search for devices on the network. Due to network latency issues, some devices may not show up on the first try, thus you may need to click this button again to find all devices.
- You may choose which Network Interface to use in case you have multiple network cards. The first Network Interface found with an UP status (can send and receive packets), if any, is initially selected.
- In the Network Info column, there is a choice of two buttons.

- Launch Network Settings: Clicking this button will attempt to open the Device's Network Settings webpage. (See next section.)
- Print: Clicking this button will allow you to print the Network Information the software was able to gather. You will be prompted to input the Model 375 Serial Number. This is only shown for older 375s that do not have a Network Settings webpage.

## 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 the 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 13.

### Model 375 Network Settings

Connection Status	Connected to Supervisor.		
Current Reading	0001.8 kcps		
Firmware Version	39801N15		

Serial Number		<input type="text" value="200000"/>	Serial number of device (000000 - 999999)
IP Address	DHCP	<input type="text" value="0.0.0.0"/>	IP address of device (0.0.0.0 for DHCP)
Subnet Mask		<input type="text" value="255.255.0.0"/>	Subnet mask IP address of device
Gateway	DHCP	<input type="text" value="192.168.0.1"/>	Gateway IP address of device (automatically set for DHCP)
DNS	DHCP	<input type="text" value="192.168.0.9"/>	DNS IP address of device (automatically set for DHCP)
TCP/IP Port		<input type="text" value="50000"/>	Port number of Supervisor service (0-65535)
Unit Code		<input type="text" value="kcps"/> <input type="button" value="v"/>	Units of device
Supervisor Primary IP Address		<input type="text" value="192.168.11.85"/>	First IP address that device will use to attempt to connect to the Supervisor service
Supervisor Secondary IP Address		<input type="text" value="192.168.11.85"/>	Second IP address that device will use to attempt to connect to the Supervisor service
Camera IP Address		<input type="text" value="192.168.199.2"/>	IP address of camera
Camera Password		<input type="password" value="••••••"/>	Password of camera
Camera Enabled		<input type="radio"/> Yes <input checked="" type="radio"/> No	Determines whether or not camera is turned on.

If you wish to change any of the above settings, simply enter the correct password in the "Password" text box, then click on the "Submit" button.

If you wish to change the password, enter the current password in the "Password" text box and the new password in the "New Password" and the "Confirm New Password" text boxes, then click on the "Submit" button.

If you wish to force the area monitor to check for a firmware update, enter the current password in the "Password" text box, then click on the "Check Firmware" button.

Password	<input type="password"/>
New Password (optional)	<input type="password"/>
Confirm New Password (optional)	<input type="password"/>

*Ludlum Measurements, Inc*  
 501 Oak Street  
 Sweetwater, TX 79556  
 (325) 235-5494

Figure 13 – Model 375 Network Settings

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.
4. In the **TCP/IP Port** field, enter 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 is associated with a camera, enter the camera's IP address into the **Camera IP Address** field. In the **Camera Password** field, enter 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.

### 7.3 Model 2100 Series Sample Monitors, Model 4906 Hand and Foot Monitors, Model 53 Portal Monitors, Model 3500-2502 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.

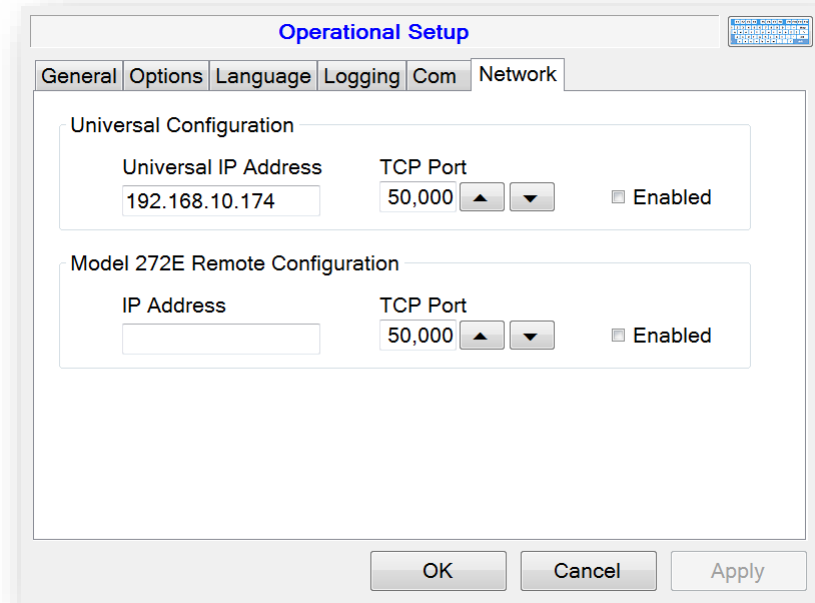


Figure 14 - Network Setup

Enter the IP Address and port of the server running the Universal service and click the Enabled checkbox 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 it at 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 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\_BROADCAST are all correct. On a typical network, these should be IP\_NETMASK = 255.255.0.0, IP\_GATEWAY = N.N.01, and IP\_BROADCAST = 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.

## **7.5 Configuring the Model 334A Alpha Air Monitors and the Model 334AB(-G) Alpha-Beta(-Gamma) Monitors**

The Model 334 will need to be set up in a specific way to correctly send data to the Universal. You need to know the IP Address of the 334.

Since the Model 334s are running Windows CE, you can check and modify the IP Address similarly to any Windows computer. You will need to close the Model 334's program. There are two scenarios for how to find the IP Address of the device. You may also use the steps in the Fixed IP Address to change the IP Address if need be.

### **Fixed IP Address**

1. Open the Start menu.
2. Go to Settings.
3. Select Network and Dial Up Connections.
4. In the Network and Dial Up Connections screen, select the appropriate Ethernet Connection, typically ENET followed by a number, such as ENET1 or ENET2. If no Ethernet Connection is displayed, then this device cannot connect to the internet, please contact Ludlum Measurements to order the appropriate part.
5. If the Specify an IP Address choice is checked, then the IP Address is what is in the IP Address field. Otherwise, see below.

### **DHCP**

1. Open the Start Menu.
2. Go to Programs.
3. Select Command Prompt.
4. Type in ipconfig. You will need to select the keyboard icon in the lower right-hand corner of the screen and once that pops up, select the Command Prompt Window for the key presses to register in the Command prompt.

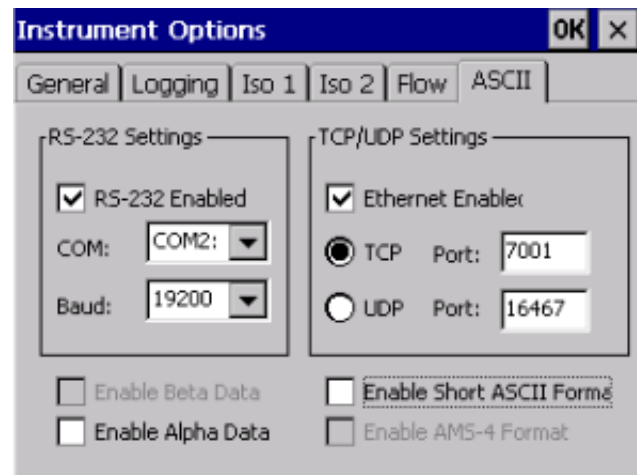
5. If an Ethernet Adapter's data is displayed, then the IP Address is in the IPv4 Address field. Otherwise, this device cannot connect to the internet. Please contact Ludlum Measurements to order the appropriate part.

It is suggested that you note the IP Address and whether it is Fixed or DHCP for future reference.

Once you are done, you may start the Model 334 software again. You can do this either by selecting the M334 icon or by rebooting the system (hold the power button on the right side of the device for 5 seconds).

Once the Software is running, in the ribbon bar at the top of the screen, select Monitor, and then select Instrument Options.

In the Instrument Options screen, go the ASCII tab (the final tab). Ensure that the TCP option is selected and the port is set to 7001, which should be the default.



For the Model 334AB(-G), ensure that both the Enable Beta Data and Enable Alpha Data checkboxes are checked.

The screenshot shows the 'Beta' tab of the 'Instrument Options' dialog box. The 'General' tab is selected. The 'RS-232 Settings' section on the left includes a checkbox for 'RS-232 Enabled' (unchecked), a 'COM:' dropdown menu (set to 'COM2:'), and a 'Baud:' dropdown menu (set to '19200'). The 'TCP/UDP Settings' section on the right includes a checkbox for 'Ethernet Enabled' (checked), a radio button for 'TCP' (selected) with a 'Port:' field set to '7001', and a radio button for 'UDP' (unselected) with a 'Port:' field set to '16467'. Below these sections are four checkboxes: 'Enable Beta Data' (checked), 'Enable Alpha Data' (checked), 'Enable Short ASCII Format' (checked), and 'Enable AMS-4 Format' (unchecked). At the bottom are 'OK' and 'Cancel' buttons.

Once you are done, you may close the Instrument Options by clicking Ok.

**Section****8**

## 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.

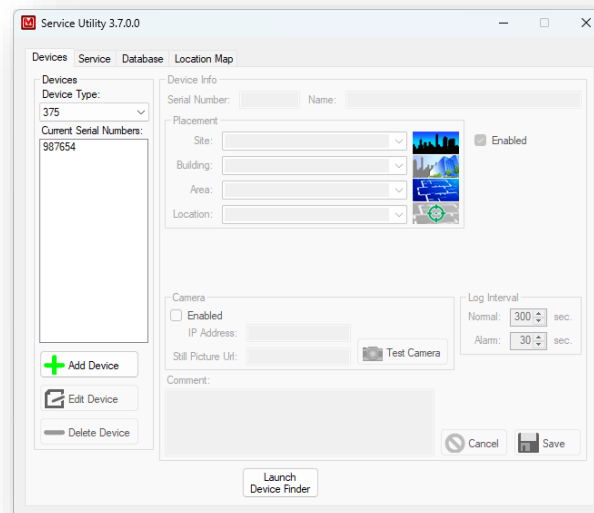


Figure 15 – Devices Tab

#### 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
- Model 2100 Sample Monitor

- Model 720 Spectroscopic Area Monitor
- Model 375P Area Monitor
- HBP-29 Body Monitor
- Model 3500-2502 Portal Monitor
- Model 3276 Area Monitor
- Model 334A Air Monitor
- Model 334AB(-G) Alpha-Beta Particulate Monitor

Select the device type to see all the 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

**Device:**

- **IP Address:** specifies the IP Address of the Device, so that the Status can be retrieved. (This feature is only used and displayed for the HBP-29, M334A, and M334AB(-G).)

**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, Model 375P, Model 2100, and Model 3276.)
- **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, Model 375P, Model 2100, and Model 3276.)

**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 Device Finder:** (375, 375P, and 3276 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 (see Figure 16).

#### 8.1.2.1 GENERAL

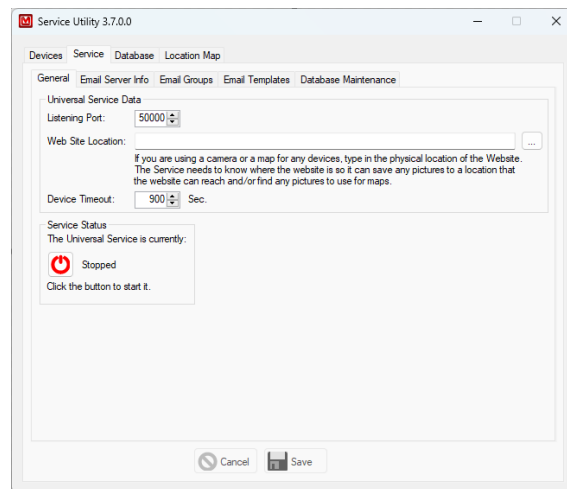


Figure 16 – The General Tab

#### 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.
- **Device Timeout:** The amount of time (in seconds) until a device is declared “Missing” by the software.

#### 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).



## 8.1.1.2.2 EMAIL SERVER INFO

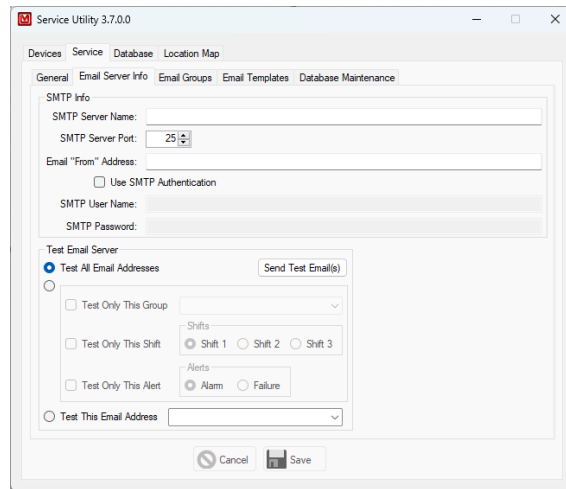


Figure 17 – The Email Server Info Tab

**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 Figure 18) are valid.

## 8.1.2.3 EMAIL GROUPS

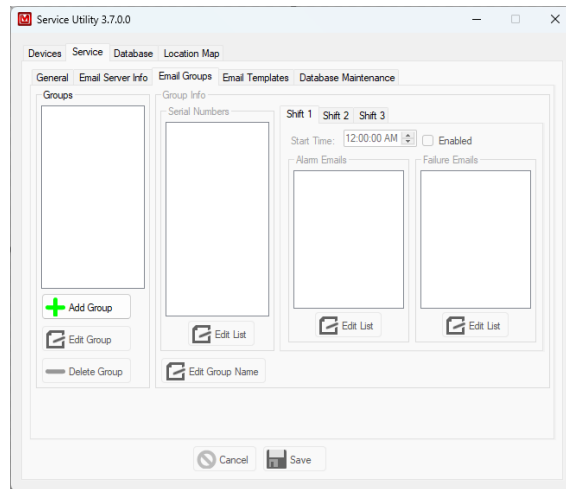


Figure 18 – The Email Groups Tab

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 desire. The Group Names are for your benefit.

#### 8.1.2.4 EMAIL TEMPLATES

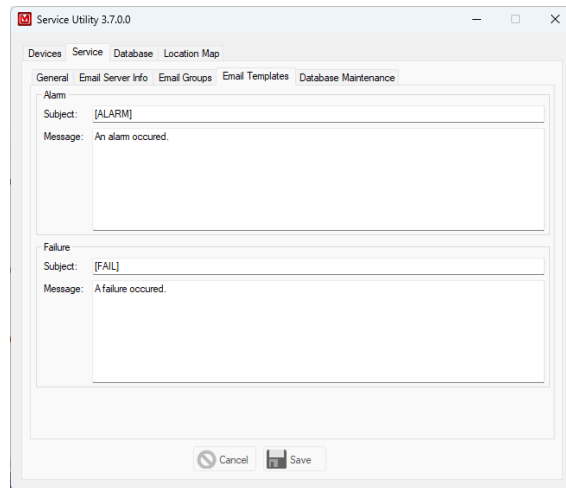


Figure 19 – The Email Templates Tab

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.

## 8.1.1.2.5 DATABASE MAINTENANCE

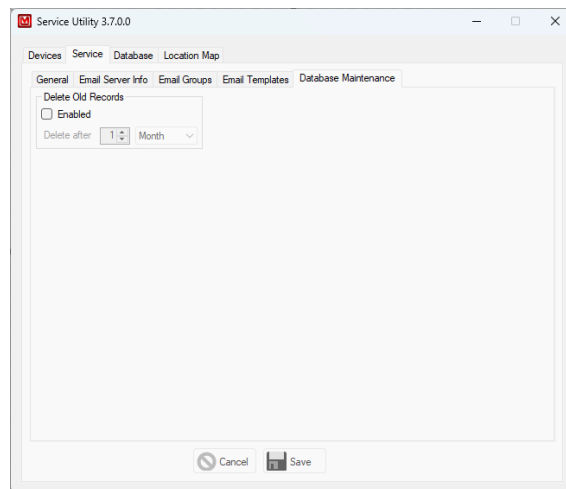


Figure 20 – The Database Maintenance Tab

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.

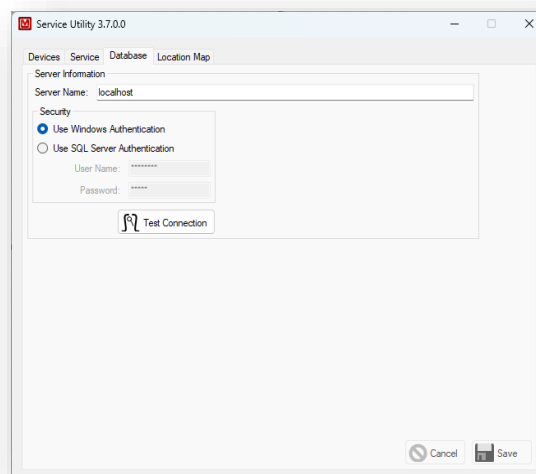


Figure 21 - SQL Connection Tab

Specify either Windows or SQL authentication. If SQL authentication is used, enter the username and password that will be used to log into the SQL database.

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

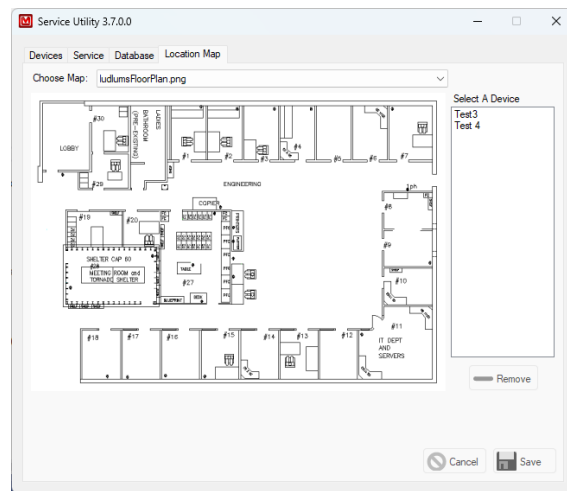


Figure 22 – Location Map Tab

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 (see Figure 23). 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.

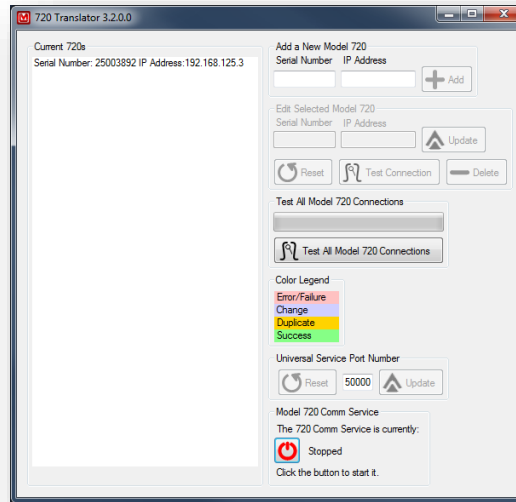


Figure 23 – Model 720 Translator

**Section****9****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, 2100, and 3276), 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 needs to 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 Figure 24).

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

**Error! Reference source not found.** shows an example of the Current Status page.

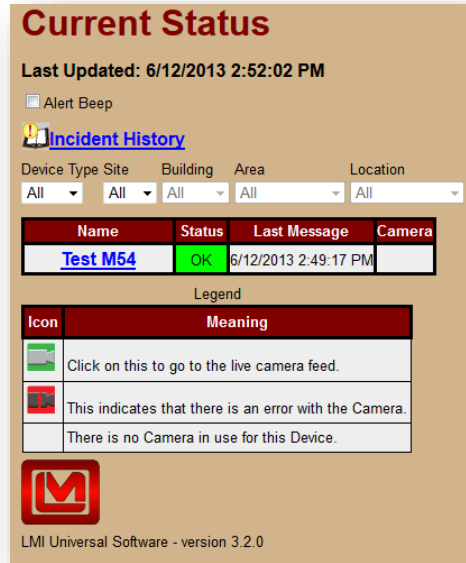


Figure 24 – Current Status

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 25.



Figure 25 – Example of filtered Current Status

### 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 example in Figure 26 (a Model 375 Current Status Page).



Figure 26 – 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.
- **Clear Alarm:** This is only on the Model 375 page for Devices that have been modified to receive commands. This button will clear any active alarm and set the status to “OK” on a Device if it is connected to the network.

- **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, 3500-2502, 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:
  - **Serial Number:** (Model 375 and Model 3276 only) Click on the Serial Number to go to the Network Settings Page for the Device.
  - **Camera:** If available, will take you to the camera associated with the device. It will not be shown if no link was provided.
  - **Background Graph:** Click on this to go to the Device specific Background Graph (see Figure 27).
  - **Spectroscopic Graph:** (Model 720 only) Click on this to go to the Model 720 Spectroscopic Graph. This link will attempt to use the latest spectroscopic reading.
  - **Scan History:** (Models 2100, 4906, 53, 3500-2502, and 54 only) Click on this to go to the Device specific Scan History page.
- **Error:** If an error occurs, 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 27 for a screen shot of the Graph page.

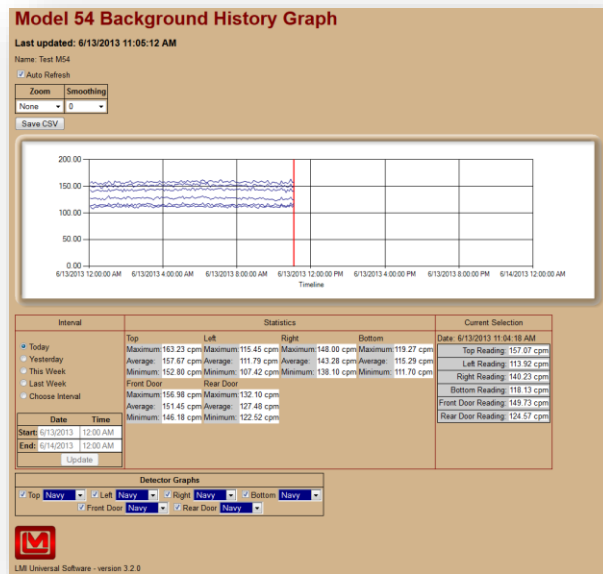


Figure 27 – Graph

If you want a smoother graph, increase the smoothing factor (any integer between 1 and 10) to accomplish this, as demonstrated in Figure 28 and Figure 29.

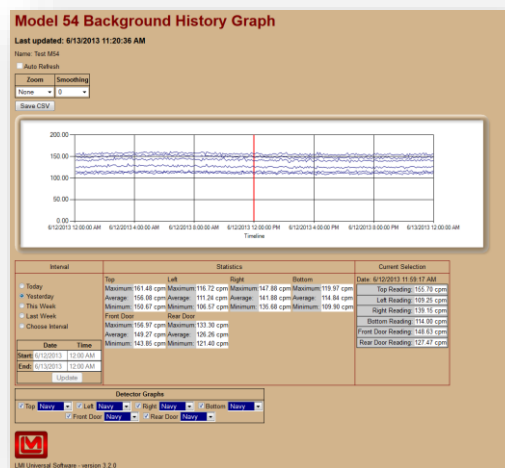


Figure 28 – Graph with no smoothing

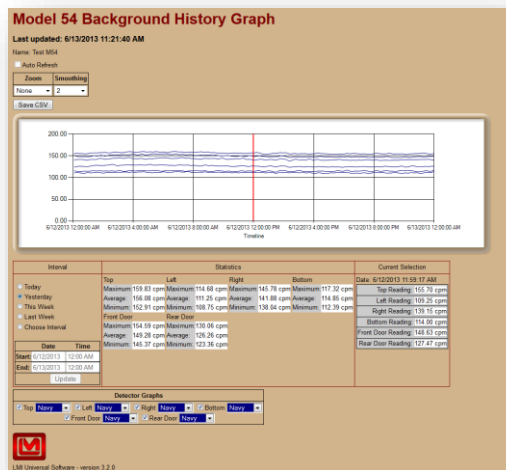


Figure 29 – Graph with a smoothing value of 2

### 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.” (see Figure 30) to move forward in time by one minute.

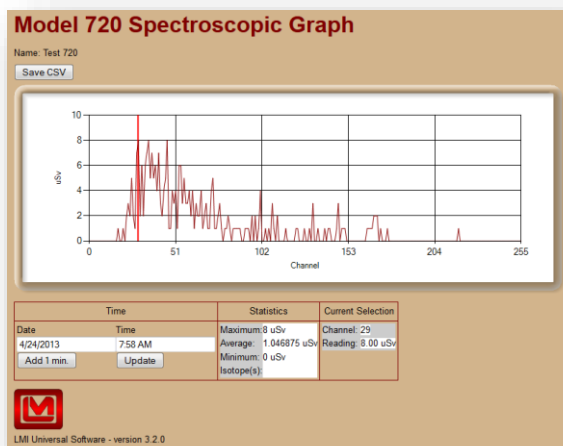


Figure 30 – Spectroscopic Graph

### 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 31.

**Incident History**

Last Updated: 6/13/2013 2:59:24 PM

[Main Status Page](#)

Interval		Incident Summary							
<input type="radio"/> Today <input type="radio"/> Yesterday <input type="radio"/> This Week <input type="radio"/> Last Week <input checked="" type="radio"/> Choose Interval		<b>Site Number Of Incidents</b> LMI 5 Incidents.							
<table border="1"> <thead> <tr> <th>Date</th> <th>Time</th> </tr> </thead> <tbody> <tr> <td>Start: 5/2/2013</td> <td>12:00 AM</td> </tr> <tr> <td>End: 6/9/2013</td> <td>12:00 AM</td> </tr> </tbody> </table>		Date	Time	Start: 5/2/2013	12:00 AM	End: 6/9/2013	12:00 AM	<input type="button" value="Update"/>	
Date	Time								
Start: 5/2/2013	12:00 AM								
End: 6/9/2013	12:00 AM								

Device Type Site Building Area Location

All All All All All

Name	Starting Time	Ending Time	Picture	Full Status	Incident Comment
Test at Walls	5/29/2013 10:38:46 AM	5/29/2013 10:43:31 AM		RadiationAlarm	Test Alarm
Test at Walls	5/29/2013 3:40:28 PM	5/29/2013 3:43:32 PM		RadiationAlarm	
Test at Walls	5/30/2013 9:28:51 AM	5/30/2013 9:33:34 AM		Fail.	
Test at Walls	5/30/2013 9:39:08 AM	5/30/2013 9:43:34 AM		RadiationAlarm	
Test M54	6/5/2013 2:51:36 PM	6/5/2013 2:52:22 PM		Alarming	

Legend

Icon	Meaning
	Click on this to go to the saved picture from the camera.
	This indicates that there is an error with the picture.
	There is no picture for this Incident.

LMI Universal Software - version 3.2.0

Figure 31 – Incident Summary



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 32.

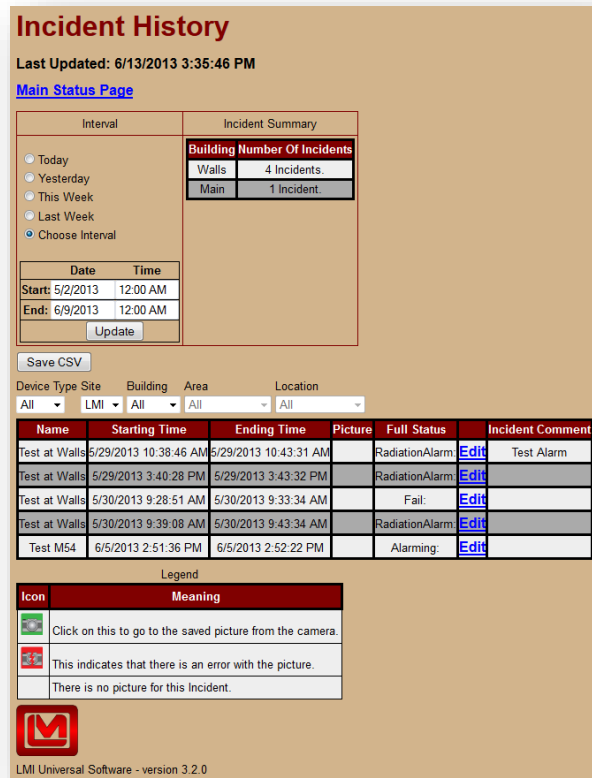


Figure 32 – Filtered Incident Summary

## 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 Universal Config Table

The Universal Config 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 stored***

- 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 stored***

- 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, HBP-29 = 7, M3500-2502 = 8, M3276 = 9, M334A = 10, M334AB = 11).
- 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 Log Interval Table**

The Log Interval 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 stored***

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

#### **9.4.2.2 Map and Location Table**

The Map and Location table stores the location of the device when showing a map for the website.

##### ***Data stored***

- 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 Incident History Table**

The Incident History 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 showing 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 stored***

- 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 History Detector Data Table**

The History Detector Data table stores the actual reading(s) of the Detector.

##### ***Data stored***

- The Reading's name.
- The Reading's value.

##### ***Child Tables***

- M334Data (0 to many connections)

#### **9.4.2.4.2 M720 Spec Channel Data Table**

The M720Spec Channel Data Table stores the Model 720 channel and its current reading.

##### ***Data stored***

- The Channel's ID (0-255)
- The Channel's reading in counts.

#### **9.4.2.4.3 M720 Spec Nuclide Data Table**

The M720 Spec Nuclide Data table stores the isotope(s) that the Model 720 thinks it might be reading.

##### ***Data stored***

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

#### **9.4.2.5 Scan History Table**

The Scan History table stores the readings taken for a scan.

##### ***Data stored***

- 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 Set Point Table**

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

##### ***Data stored***

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

#### **9.4.2.5.2 M2100 Scan Type Table**

The M2100 Scan Type Table stores what type of scan the Model 2100 took, if provided (usually Steel or Slag).

##### ***Data stored***

- The Scan Type.

#### **9.4.2.5.3 Scan Detector Data Table**

The Scan Detector Data Table stores any pan detector data for each scan.

##### ***Data stored***

- 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 Scan Detector Alarm Table**

The Scan Detector Alarm Table stores any alarms that happened during a scan.

##### ***Data stored***

- The Name of the Alarm that occurred.

#### **9.4.2.5.3.2 Scan Detector Failure Table**

The Scan Detector Failure table stores any failures that happened during a scan.

##### ***Data stored***

- The Name of the Failure that occurred.

#### **9.4.2.5.3.3 Scan Detector Reading Table**

The Scan Detector Reading Table stores the Readings that were taken during a scan.

##### ***Data stored***

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

#### **9.4.2.6 Current Status Table**

The Current Status 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 stored***

- 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 Incident History 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.

#### **9.4.2.7 Command Support Table**

The Command Support table stores whether certain Model 375s can receive a command, specifically a remote acknowledgement of an alarm.

##### ***Data stored***

- The Serial Number of the Model 375.
- A number that indicates the command level of the Model 375, either 0 for no command supported or 1 to acknowledge an alarm.

#### **9.4.2.8 Commands Table**

The Command Support table stores any commands to be sent to Model 375s.

##### ***Data stored***

- The Serial Number of the Model 375.
- The Command to send to the Model 375.

#### **9.4.2.9 IP Addresses Table**

The Command Support table stores the IP Addresses of certain devices that the Universal Software needs to communicate with directly.

##### ***Data stored***

- The IP Address of the device.



#### 9.4.2.10 M334 Data Table

The M334 Data table stores the extra data coming from the Model 334.

##### *Data stored*

- Status Code is the Status Code that the Model 334 reports.
- Measurement type is the type of the Measurement - either 'A' for Acute or 'C' for Chronic.
- Elapsed Time is the time in seconds since either the Model 334 was turned on or the Pump was reset.
- MDC is the current Minimum Detectable Concentration.
- Estimated Worker Dose is the estimated worker dose, an alternate reading to display.
- MDD is the current Minimum Detectable Dose.
- Sample Flow Rate is the current Flow Rate for the pump.
- Total Sample Volume is the current total volume sampled since a filter change.

### 9.5 Expected Database Size Increase for Records

These tables are the expected size increase in bytes for a single device of each type. The main difference for most devices between the Maximum Value and the Typical Value is an assumption that the device has sent a Unit of the maximum length of 10 characters. This is unlikely due to most Units being four characters long, thus is the assumed length for Typical Values.

The following are outliers:

- M720: Its large size comes primarily from the Spectroscopic data.
- HBP-29: No data is stored for this device.
- M334A: Though the size of the Units is fixed (the two Units are only 3 characters long), the possible Name in the Detector Data History table is variable. The Typical Value is assumed to have a six-character name.

- M334AB(-G): Same as the M334A, but now there are two Detector Data History rows.

Device	Maximum Size (bytes)	Typical Size (bytes)
M375	57	45
M4906	226	214
M53	206	194
M2100	167	155
M720	6373	6361
M375-P	57	45
HBP-29	N/A	N/A
M3500-2502	122	110
M2376	57	45
M334A	161	113
M334AB(-G)	298	202

Some devices can also take a scan, which is saved along with the normal readings. These are far more variable since there could be 0 or more Alarms and 0 or more Failures, both of which are text based and reflect whatever the device has sent. The Maximum Sizes and Typical Sizes assume a single Alarm and Failure have been saved, as well as the full 30 characters of each are in use. The values also include the regular data size as well.

Device	Maximum Size (bytes)	Typical Size (bytes)
M54	2143	2131
M4906	2064	2741
M53	1934	1922
M2100	1206	1194
M3500-2502	1850	1838

**Section****10****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.

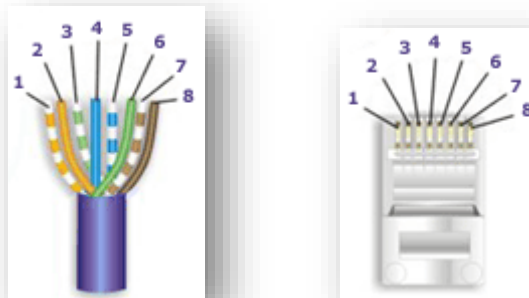
**10.2 Ethernet Cable Termination**

Figure 33 – Connector with pins

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.

**Section****11**

## 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 or Model 3276**

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 the 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 the 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, 3500-2502, 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, 3500-2502, 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.

#### **11.2.4 Troubleshooting the Model 3276**

##### **11.2.1.1 CHECK THE SETTINGS OF THE MODEL 3276**

Use a web browser to connect to the Model 3276 itself.

Confirm that the Supervisor IP Address is the IP Address of the computer that is running the Universal Software. 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.

### **11.3 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 accidentally 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 milli-seconds:
        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, 375P, 720, OR 3276

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, 3500-2502, 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, 3500-2502, 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 username, and database password in the Universal Server Utility all match your SQL Server configuration.

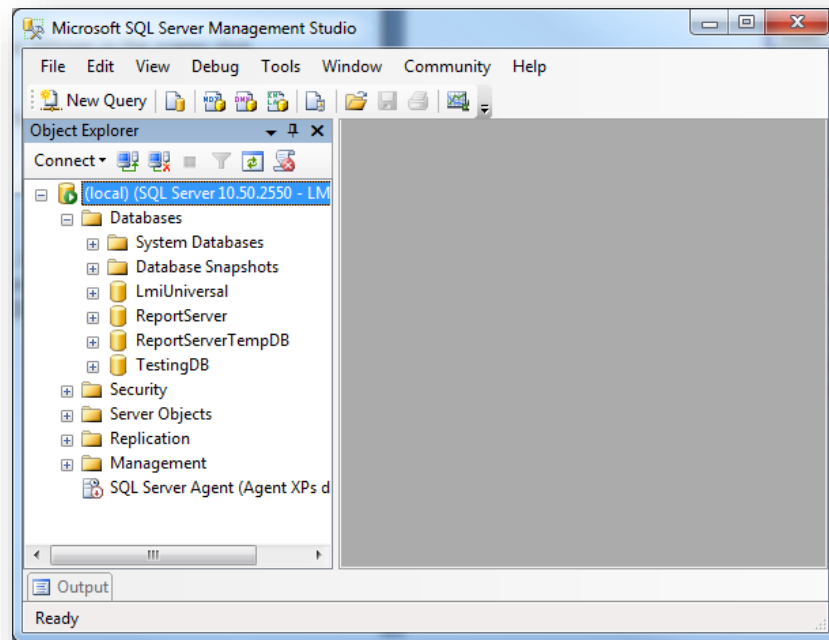


Figure 34 - SQL Server Management Studio Express

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."

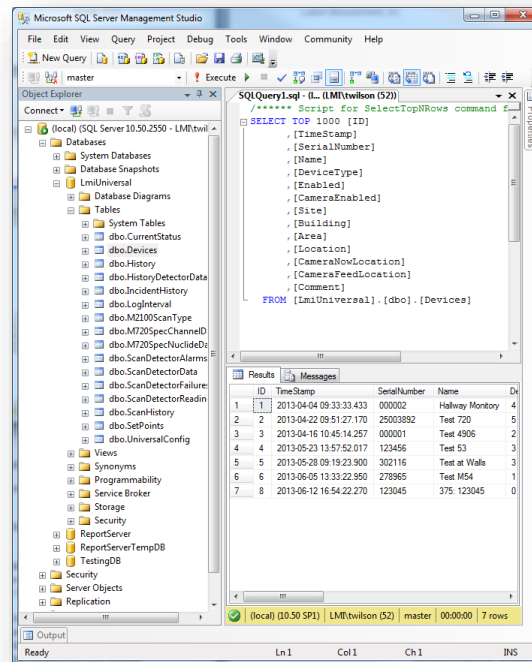


Figure 35 - Showing dbo.Device table in the LmiUniversal database

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, hence forth 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.

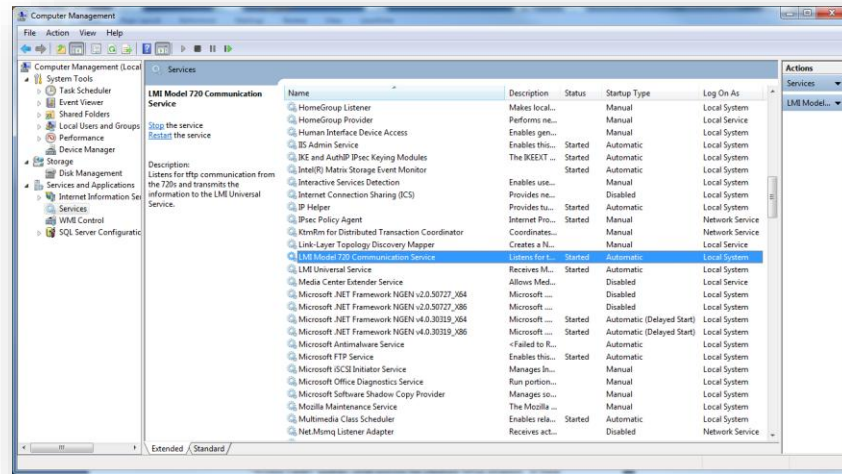


Figure 36 - Services

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 (see Figure 37).

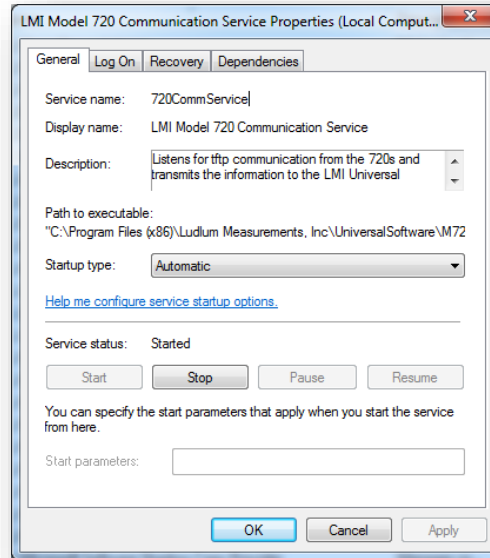


Figure 37 – Properties of the Universal Service

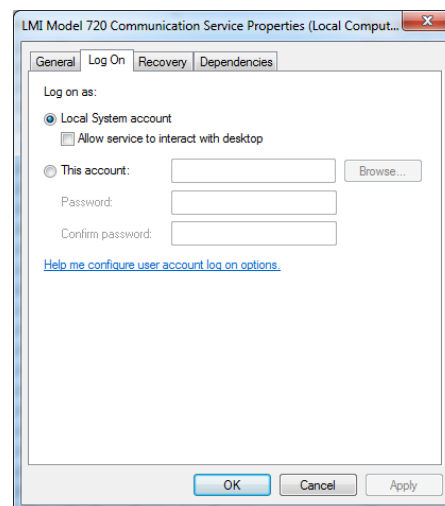


Figure 38 - Log On of the Universal Service

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.**

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 Software” section on page 15. 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 35.

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 Section 8

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, and 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 19.

Click the plus icon next to the “Security” folder and 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 19.

Open the Universal Service Utility. Click the “Database Settings” tab and verify that the username and password matches the username and password from the

login properties window in SQL Server Management Studio. When the username 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.

#### **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, and then click “Run.” Type “cmd,” without the quotation marks, and click “Enter.” In the command window, type in 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, and 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 Replacing Model 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 39 shows an external Ethernet board, while Figure 40 shows an internal Ethernet board.



Figure 39 – External Ethernet Board

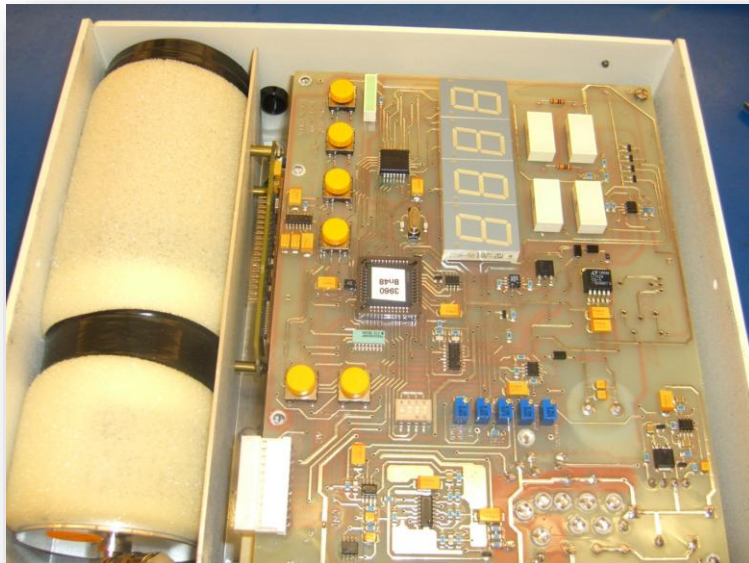


Figure 40 – Internal Ethernet Board

### Replacing an External Rabbit Ethernet Board

1. Remove the four screws from the corners of the Ethernet board. See Figure 41.



Figure 41 – External Rabbit Ethernet Board Removal

2. Disconnect the 3-pin MTA connector from the Ethernet board to separate it from the area monitor. See Figure 42.

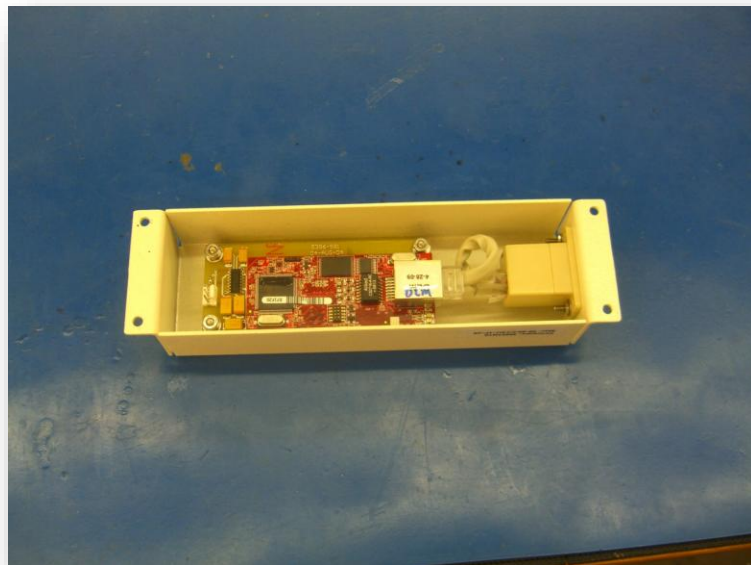


Figure 42 – External Rabbit Ethernet Board disconnected

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 43.



Figure 43 – External Rabbit Ethernet Board removed from case

### Replacing an Internal Rabbit Ethernet Board

1. Remove the outer case from the area monitor. See Figure 45.

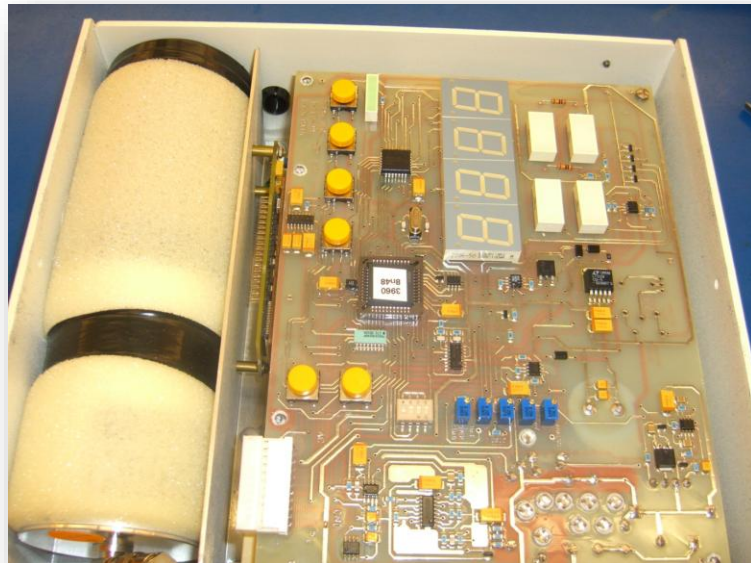


Figure 44 – Outer Case Removal

2. Remove the four screws from the corners of the main board and disconnect the MTA connector. See Figure 45.



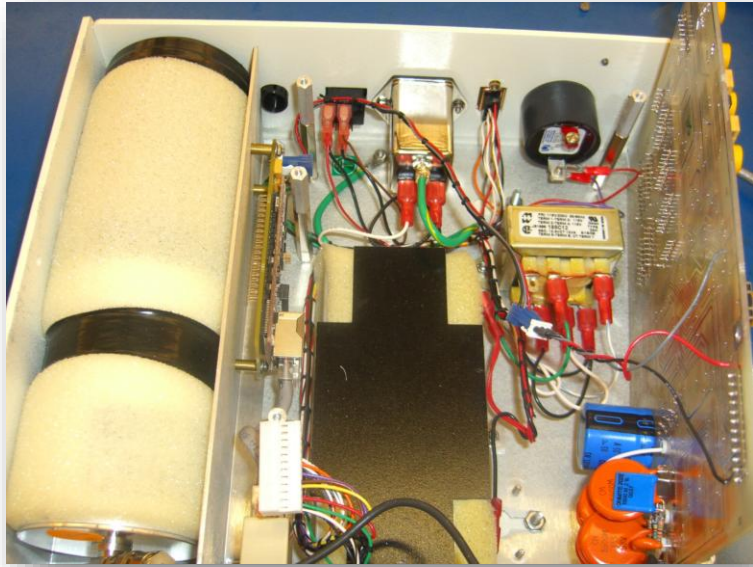


Figure 45 – Disconnecting the MTA Connector

3. Remove the two nuts from the corners of the bracket holding the Ethernet board. See Figure 46.

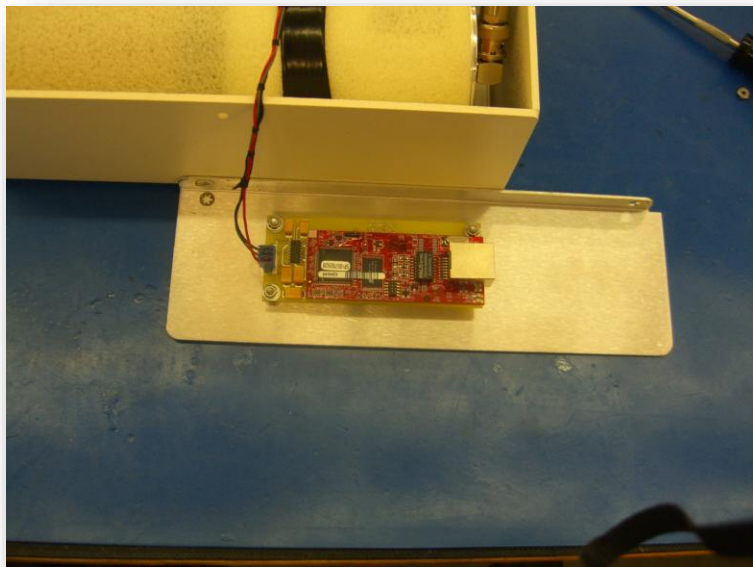


Figure 46 – Internal Rabbit Ethernet Board



4. Remove the three nuts from the corners of the Ethernet board. See Figure 47.

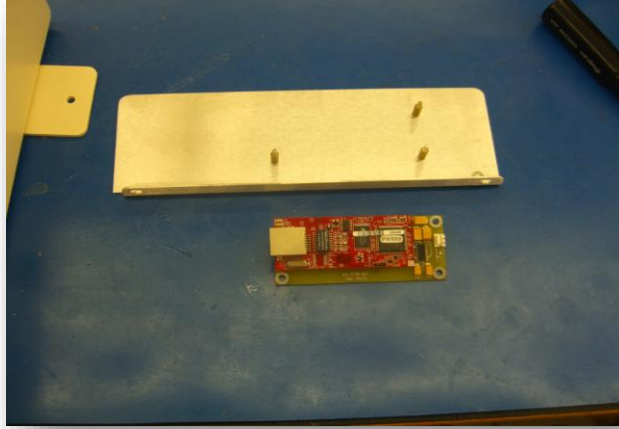


Figure 47 – Internal Rabbit Ethernet Board Removal

**Section****12**

---

**Version History**

---

This is a description of the changes and bug fixes for each version of the Universal Software.

**Version 3.10.0**

Features:

- Added the 334A, 334AB, and 334AB-G.

Bug Fixes:

- Fixed bug where an HBP-29 could not be saved if its IP Address was invalid or was not on the network.

**Version 3.9.1**

Features:

- Changed the Device Finder to be capable of running independently from the Universal Software.
- Added a way to select which Network Interface to use when searching for Devices with the Device Finder.
- Added a way to print the Network Information for a Model 375 using a Rabbit Board with N09 or older firmware.

**Version 3.9.0**

Features:

- Added the 3276 – previously, it was treated as a 375 instead.
- Changed the error message when more than one unit was found for the readings of a Background Graph.
- Added the Device's Serial Number to the Incident History page and to the printed CSV file.
- Added the Device's Serial Number and Name to the printed CSV for the Background Graph page.
- Added the Device's Serial Number and Name to the printed CSV for the Scan Graph page.

Bug Fixes:

- Fixed bug where Interval Devices (375, 375P, 2100, 3276) would take an extra 2 seconds to save to the database.
- Fixed a deadlock error when the webpage would try to read from the database while the Service was attempting to save to it.

**Version 3.8.2**

Features:

- Added a check to use SSL if the Email Server responds that it needs it.

Bug Fixes:

- Fixed bug where Emails would not get sent when trying to use the SMTP Authentication.
- Fixed bug where the Failure Message text would be overwritten by the Failure Subject text.

**Version 3.8.1**

Bug Fixes:

- Fixed bug where the High Gamma Energy and Low Gamma Energy lines were not being displayed on the Model 2100 Background Graph.
- Fixed bug where the Sample Count was being displayed as “X counts” rather than “X.XX (units)” in the Model 2100 Scan History.

**Version 3.8.0**

Features:

- Added the Model 3500-2502.

**Version 3.7.1**

Features:

- Changed it so that SQL Username and Password fields are no longer hidden behind asterisks.

Bug Fixes:

- Fixed bug where the SQL Username and Password would be swapped when saved.
- Fixed bug where the Edit and Delete Group buttons would stay enabled after saving a Group.

**Version 3.7.0**

Features:

- Added the ability to set the Device Timeout time. Previously, it had always been 15 minutes.
- Changed the Database Setup to still add the tables even when there is a premade, but empty database.
- Added a warning that deleting a Device will delete its records.

Bug Fixes:

- Fixed corrupted mp3 for the website alarm.
- Fixed bug where the Location Map would always show Devices as “Missing”.

**Version 3.6.1**

Bug Fixes:

- Fixed bug where the Location Map would try to connect to a non-existent “Current Status” page for the HBP-29.

- Fixed bug where the Location Map page would not reload correctly.

### **Version 3.6.0**

Features:

- Removed the Filter Checkboxes in the Device Finder.
- Removed the M375 Older Setup Utility as it has been deemed no longer necessary.

### **Version 3.5.0**

Features:

- Updated the Device Finder to correctly recognize the new ESP32 board (the replacement for the Rabbit Board).

### **Version 3.4.1**

(Released bug fix for 3.4.0)

Bug Fixes:

- Fixed bug where the Version Number of the database was not updated to 3.

### **Version 3.4.0**

(Unreleased version)

Features:

- Added the ability to send SMTP emails.

Bug Fixes:

- Fixed bug where the buttons in certain popup windows in the Service Utility would not work as intended.

### **Version 3.3.0**

Features:

- Added the HBP-29.
- Added a Version number to the database to make it easier to update older versions of the database.
- Added ability to use a separate account to create the database via the Database Updater rather than the one used by the Universal Software to access the database.
- Added a way for the user to create the IIS App Pool user, if needed, for an automatic login by the Universal Webpage.

Bug Fix:

- Fixed bug where certain characters in the name of a Device would not allow its Current Status page to be displayed.

**Version 3.2.9**

Features:

- Added ability to clear the alarm for the 375 if the 375 supports it.
- Add ability to go to the Model 375 Network Settings page.

**Version 3.2.8**

Features:

Bug Fixes:

- Fixed bug where the Utilities Only version of the programs would not have the correct icon.
- Added ability for the Service to parse multiple messages from a Device that came in a single large batch due to network issues.

**Version 3.2.7**

Features:

- Removed the creation of a default App Pool user for the Universal Webpage by the Database Setup, as there is no longer a guarantee it would be correct.

**Version 3.2.6**

Bug Fixes:

- Fixed bug where 375P would not log to the database.

**Version 3.2.5**

Bug Fixes:

- Fixed bug where the Location Map would not always have the correct link to the Device's Current Status page.

**Version 3.2.4**

Bug Fixes:

- Fixed bug where Test Emails would attempt to send emails to groups without emails and thus would treat it as a failure.