

Welch Allyn<sup>®</sup>  
Web Upload<sup>™</sup>  
ADMINISTRATOR MANUAL

Manufactured by Welch Allyn, Inc. Skaneateles Falls, NY U.S.A.



---

**CAUTION:** Federal law restricts this device to sale by or on the order of a physician.

© 2020 Welch Allyn This document contains confidential information that belongs to Welch Allyn, Inc. No part of this document may be transmitted, reproduced, used, or disclosed outside of the receiving organization without the express written consent of Welch Allyn, Inc. Welch Allyn is a registered trademark of Welch Allyn, Inc. Ambulo, H3+, H12+, Hypertension Diagnostics Suite, and VERITAS are trademarks of Welch Allyn, Inc. Microsoft and Windows are trademarks or registered trademarks of Microsoft Corporation. v4.0.0

For patent information, please visit [www.welchallyn.com/patents](http://www.welchallyn.com/patents)

For information about any Welch Allyn product, visit: <https://www.welchallyn.com/en/about-us/locations.html>

Customer Service and Technical Support: <https://www.welchallyn.com/en/other/contact-us.html> 1.888.667.8272,  
[mor\\_tech.support@hillrom.com](mailto:mor_tech.support@hillrom.com)



9515-147-71-ENG REV H  
Revision date: 2020-04



Welch Allyn, Inc.  
4341 State Street Road  
Skaneateles Falls, NY 13153 USA

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

# TABLE OF CONTENTS

---

<b>1. NOTICES.....</b>	<b>2</b>
MANUFACTURER’S RESPONSIBILITY .....	2
RESPONSIBILITY OF THE CUSTOMER .....	2
EQUIPMENT IDENTIFICATION .....	2
<b>2. WARRANTY INFORMATION .....</b>	<b>3</b>
YOUR WELCH ALLYN WARRANTY .....	3
<b>3. USER SAFETY INFORMATION .....</b>	<b>5</b>
<b>4. EQUIPMENT SYMBOLS AND MARKINGS .....</b>	<b>6</b>
SYMBOL DELINEATION .....	6
<b>5. INTRODUCTION.....</b>	<b>7</b>
PURPOSE.....	7
AUDIENCE .....	7
INDICATIONS FOR USE.....	7
WEB SERVER SOFTWARE .....	8
<b>6. INSTALLATION .....</b>	<b>9</b>
6.1 WEB SERVER REQUIREMENTS.....	9
6.2 DETERMINING IF IIS IS INSTALLED .....	9
6.3 INSTALLING IIS ON WINDOWS SERVER (2012 R2, 2016, 2019).....	9
6.4 CONFIGURING SSL AND AUTHENTICATION .....	12
6.5 INSTALLING WEB UPLOAD SERVER SOFTWARE .....	12
6.6 POST-INSTALL IIS CONFIGURATION.....	13
6.7 TESTING THE WEB UPLOAD CLIENT CLICK ONCE DEPLOYMENT .....	17
<b>7. CONFIGURING WEB UPLOAD SERVER SETTINGS .....</b>	<b>18</b>
7.1 WEB UPLOAD SERVER SETTINGS APPLICATION.....	19
7.1.1 THE LISTS TAB .....	20
7.1.2 THE CUSTOMIZE CLIENT TAB .....	21
7.1.3 THE SERVER CONFIGURATION TAB .....	24
7.1.4 THE STORAGE MAINTENANCE TAB .....	26
7.2 CONFIGURE CLICK ONCE PROVIDER URL APPLICATION.....	26
7.3 DIRECTORY NAMING AND DEVICE MAPPING .....	28
7.4 FIREWALL CONFIGURATION.....	32
<b>8. TROUBLESHOOTING.....</b>	<b>33</b>
8.1 EVENT LOGS.....	33
8.2 CREATE DIAGNOSTIC REPORT .....	34
8.3 TROUBLESHOOTING SYMPTOMS.....	35
<b>9. CONFIGURING PROGRAMS THAT USE WEB UPLOAD DATA.....</b>	<b>37</b>
9.1 H-SCRIBE VERSION 4.xx.....	37
9.2 H-SCRIBE VERSION 5.xx.....	37
9.3 HYPERTENSION DIAGNOSTIC SUITE (HDS) .....	37
9.4 ELI PC SERVICE .....	38
<b>APPENDIX A: CONFIGURING SILENT INSTALLS .....</b>	<b>39</b>

# 1. NOTICES

---

## **Manufacturer's Responsibility**

Welch Allyn, Inc. is responsible for the effects on safety and performance only if: Assembly operations, extensions, readjustments, modifications, or repairs are carried out only by persons authorized by Welch Allyn, Inc. The device is used in accordance with the instructions for use.

## **Responsibility of the Customer**

The user of this device is responsible for ensuring the implementation of a satisfactory maintenance schedule. Failure to do so may cause undue failure and possible health hazards.

## **Equipment Identification**

Welch Allyn, Inc. equipment is identified by serial and part numbers on the side, back, or bottom of the device. Care should be taken so that these numbers are not defaced.

## **Copyright and Trademark Notices**

This document contains information that is protected by copyright. All rights are reserved. No part of this document may be photocopied, reproduced, or translated to another language without prior written consent of Welch Allyn, Inc.

## **Other Important Information**

The information in this document is subject to change without notice. Welch Allyn, Inc. makes no warranty of any kind with regard to this material including, but not limited to, implied warranties of merchantability and fitness for a particular purpose. Welch Allyn, Inc. assumes no responsibility for any errors or omissions that may appear in this document. Welch Allyn, Inc. makes no commitment to update or to keep current the information contained in this document.

## **Notice to EU Users and/or Patients:**

Any serious incident that has occurred in relation to the device, should be reported to the manufacturer and the competent authority of the Member State in which the user and/or patient is established.

## **Disposal**

This product and its accessories must be disposed of according to local laws and regulations. Do not dispose of this product as unsorted municipal waste. For more specific disposal information see [www.welchallyn.com/weee](http://www.welchallyn.com/weee).

## 2. WARRANTY INFORMATION

---

### Your Welch Allyn Warranty

WELCH ALLYN, INC. (hereafter referred to as "Welch Allyn") warrants that components within Welch Allyn products (hereafter referred to as "Product/s") will be free from defects in workmanship and materials for the number of years specified on documentation accompanying the product, or previously agreed to by the purchaser and Welch Allyn, or if not otherwise noted, for a period of twelve (12) months from the date of shipment. Consumable, disposable or single use products such as, but not limited to, PAPER or ELECTRODES are warranted to be free from defects in workmanship and materials for a period of 90 days from the date of shipment or the date of first use, whichever is sooner. Reusable product such as, but not limited to, BATTERIES, BLOOD PRESSURE CUFFS, BLOOD PRESSURE HOSES, TRANSDUCER CABLES, Y-CABLES, PATIENT CABLES, LEAD WIRES, MAGNETIC STORAGE MEDIUMS, CARRY CASES or MOUNTS, are warranted to be free from defects in workmanship and materials for a period of 90 days. This warranty does not apply to damage to the Product/s caused by any or all of the following circumstances or conditions:

- a) Freight damage;
- b) Parts and/or accessories of the Product/s not obtained from or approved by Welch Allyn;
- c) Misapplication, misuse, abuse, and/or failure to follow the Product/s instruction sheets and/or information guides;
- d) Accident; a disaster affecting the Product/s;
- e) Alterations and/or modifications to the Product/s not authorized by Welch Allyn;
- f) Other events outside of Welch Allyn's reasonable control or not arising under normal operating conditions.

THE REMEDY UNDER THIS WARRANTY IS LIMITED TO THE REPAIR OR REPLACEMENT WITHOUT CHARGE FOR LABOR OR MATERIALS, OR ANY PRODUCT/S FOUND UPON EXAMINATION BY WELCH ALLYN TO HAVE BEEN DEFECTIVE. This remedy shall be conditioned upon receipt of notice by Welch Allyn of any alleged defects promptly after discovery thereof within the warranty period. Welch Allyn's obligations under the foregoing warranty will further be conditioned upon the assumption by the purchaser of the Product/s (i) of all carrier charges with respect to any Product/s returned to Welch Allyn's principal place or any other place as specifically designated by Welch Allyn or an authorized distributor or representative of Welch Allyn, and (ii) all risk of loss in transit. It is expressly agreed that the liability of Welch Allyn is limited and that Welch Allyn does not function as an insurer. A purchaser of a Product/s, by its acceptance and purchase thereof, acknowledges and agrees that Welch Allyn is not liable for loss, harm, or damage due directly or indirectly to an occurrence or consequence therefrom relating to the Product/s. If Welch Allyn should be found liable to anyone under any theory (except the expressed warranty set forth herein) for loss, harm, or damage, the liability of Welch Allyn shall be limited to the lesser of the actual loss, harm, or damage, or the original purchase price of the Product/s when sold. EXCEPT AS SET FORTH HEREIN WITH RESPECT TO REIMBURSEMENT OF LABOR CHARGES, A PURCHASER'S SOLE EXCLUSIVE REMEDY AGAINST WELCH ALLYN FOR CLAIMS RELATING TO THE PRODUCT/S FOR ANY AND ALL LOSSES AND DAMAGES RESULTING FROM ANY CAUSE SHALL BE THE REPAIR OR REPLACEMENT OF DEFECTIVE PRODUCT/S TO THE EXTENT THAT THE DEFECT IS NOTICED AND WELCH ALLYN IS NOTIFIED WITHIN THE WARRANTY PERIOD. IN NO EVENT, INCLUDING THE CLAIM FOR NEGLIGENCE, SHALL WELCH ALLYN BE LIABLE FOR INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES, OR FOR ANY OTHER LOSS, DAMAGE, OR EXPENSE OF ANY KIND, INCLUDING LOSS OF PROFITS, WHETHER UNDER TORT, NEGLIGENCE OR STRICT LIABILITY THEORIES OF LAW, OR OTHERWISE. THIS WARRANTY IS EXPRESSLY IN LIEU OF ANY OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED

WARRANTY OF MERCHANTABILITY AND THE WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE.

## 3. USER SAFETY INFORMATION

---



### **WARNING:**

Means there is the possibility of personal injury to you or others.



### **Caution:**

Means there is the possibility of damage to the device.

### **Note:**

Provides information to further assist in the use of the device.



### **WARNING(S)**

- Reference Ambulo™ 2400, HSCRIBE™, H3+™, H12+™, and WAM PC user manuals for all warnings.
- Device is a computer-based software application intended for use on a computer separate from the HSCRIBE, Hypertension Diagnostics Suite, and ELI PC Service systems. Holter recordings from H12+ and H3+ digital recorders, BP recordings from Ambulo 2400 monitors, and resting ECG waveform recordings from WAM PCs are transferred using Welch Allyn Web Upload and then analyzed by HSCRIBE, Hypertension Diagnostics Suite, and ELI PC Service.
- The Welch Allyn Web Upload server software is designed to operate on a Microsoft® Windows® Windows Server 2012 R2 64-bit, Windows Server 2016 and Windows Server 2019 operating systems. Before attempting to use the device for clinical applications, the user must read and understand the contents of both the user and administrator manual as well as any accompanying documents. Contact Welch Allyn service for additional training options.
- This manual gives important information about the use and safety of this software application. Deviating from operating procedures, misuse or misapplication of the software application, or ignoring specifications and recommendations could result in increased risk of harm to users, patients and bystanders, or damage to the system.



### **Caution(s)**

- Reference HSCRIBE Holter Analysis user manual for cautions relating to the Holter analysis system.
- Reference H12+ or H3+ digital recorder user manuals for all cautions relating to the recorder.
- Reference Ambulo 2400 Ambulatory Blood Pressure Monitor user manual for all cautions relating to the blood pressure recorder.
- Reference ELI PC Service manual for cautions related to processing WAM PC recordings.
- Reference WAM PC manual for cautions related to that device.

## 4. EQUIPMENT SYMBOLS AND MARKINGS

---

### Symbol Delineation



**WARNING** The warning statements in this manual identify conditions or practices that could lead to illness, injury, or death. In addition, when used on a patient applied part, this symbol indicates defibrillation protection is in the cables. Warning symbols will appear with a grey background in a black and white document.



**CAUTION** The caution statements in this manual identify conditions or practices that could result in damage to the equipment or other property, or loss of data.



Do not dispose as unsorted municipal waste. Requires separate handling for waste disposal according to local requirements



welchallyn.com

For information about any Welch Allyn product, contact your local Welch Allyn representative:  
[www.welchallyn.com/about/company/locations.htm](http://www.welchallyn.com/about/company/locations.htm)



Reorder Number



## 5. INTRODUCTION

---

### Purpose

This administrator's manual explains how to install and configure the Welch Allyn Web Upload server software. Use this manual as a reference as well as a troubleshooting guide.

**NOTE:** *This manual may contain screen shots. Any screen shots are provided for reference only. Consult the actual screen in the host language for specific wording.*

### Audience

This manual is written and intended for users that are familiar with Microsoft Windows and have a basic understanding of computer operations.

### Indications for Use

This software is indicated for use in a clinical setting where recorded Holter ECG, resting ECG, and ambulatory blood pressure (ABP) data will be transmitted from a remote site over the Internet/Intranet to a central web server. The data is then imported and analyzed by the Hscribe Holter analysis system, ELI PC Service, or Hypertension Diagnostic Suite for review by trained medical personnel.

### Welch Allyn Web Upload Overview

The Welch Allyn Web Upload solution collects ECG data from H3+ digital Holter recorders and H12+ compact flash (CF) memory cards, ABP data from Ambulo 2400 ambulatory blood pressure recorders, and resting ECG recordings from WAM PCs. It uses an Internet/Intranet connection to transfer the recording data to a central web server. The Client software is also used to prepare the Holter, ABP, and resting recorders for new tests. The Welch Allyn Web Upload solution may be referenced as Mortara Web Upload in portions of this manual or on screen.

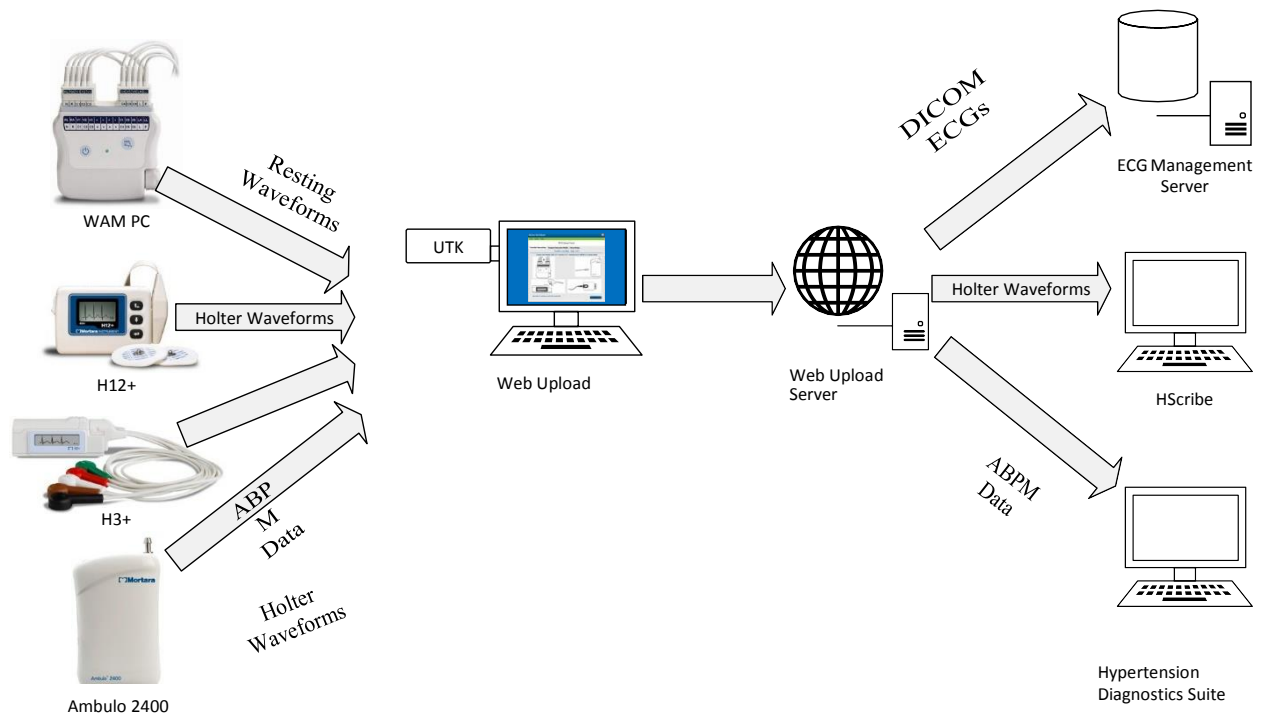
The Welch Allyn Web Upload Client is installed on a site's computer using one of the two methods:

- (1) From a web browser by an administrative user. The setup procedure prompts for a local data storage location, automatically creates directories, and configures to allow non-administrative use. After initial installation, the Client runs as a standalone application that will automatically update whenever a new version becomes available on the web server.
- (2) By running a standalone silent Web Upload Client installer. This setup does not prompt users for local data storage directory. The local storage directory and other configuration information is read from *WebUploadInstallConfig.xml.xml* file (see Appendix A) in Silent Client installer folder. The client standalone application does not automatically update when a new version becomes available on the web server. To update the Web Upload client to latest version, the existing Web Upload client software should be uninstalled, and the new version installed.

The Welch Allyn Web Upload Client software automatically detects H3+ recorder, WAM PC, and Ambulo 2400 connections, as well as H12+ CF memory card insertions. The user is prompted to move through data transfer and recorder preparation steps in a wizard-like manner. Demographic fields may be populated automatically or through a user selection when XML orders exist.

Recordings are managed on the Recordings page. The user can upload individual recordings or batch upload all recordings not yet transferred. The Welch Allyn Web Upload Client can also be configured to automatically initiate uploads as new recordings are stored.

Troubleshooting tools are available in the Welch Allyn Web Upload Client. Information can be copied to the clipboard and sent via e-mail to web server administrators.



## Web Server Software

The software is composed of two components:

### Welch Allyn Web Upload Client

This component allows remote sites to install the upload client on their computers. The sites will be instructed to browse to a page (publish.htm) on the web server that provides an **Install** button. Clicking on the Install button initiates the installation. Sites will need to visit this web page only once.

### Web Services

This component handles requests from the upload Client such as receiving recordings and retrieving configuration data.

## 6. INSTALLATION

---

### 6.1 Web Server Requirements

The web server must meet the following requirements:

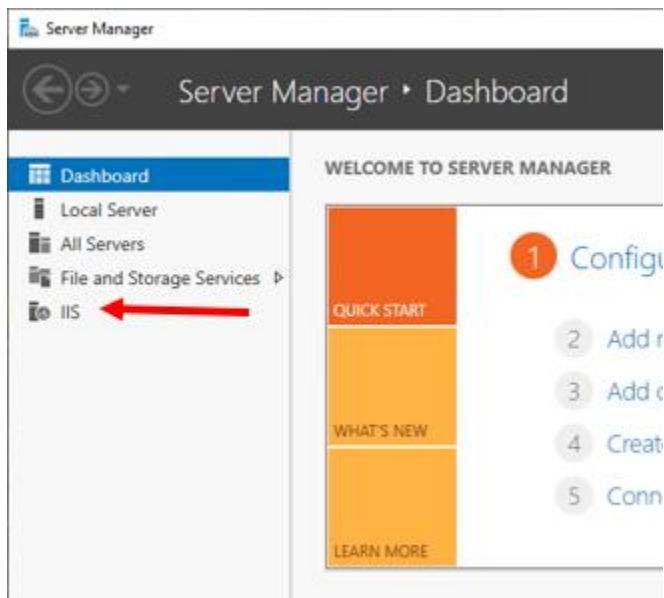
- Windows Server 2012 R2 64-bit, Windows Server 2016 or Windows Server 2019.
- Sufficient CALs (Client Access Licenses) for the expected client load from the remote sites
- Enough disk space to handle anticipated volume of recordings
- Microsoft IIS 8 if running Windows Server 2012 R2
- Microsoft IIS 10 if running Windows Server 2016 or 2019
- IIS must be configured to use ASP .NET v4.5 or later for ASP web pages
- .NET 4.6.1

### 6.2 Determining if IIS is installed

The Welch Allyn Web Upload software requires the Web Server (IIS) roles.

To determine if IIS is already installed, launch **Server Manager** from *Start -> Administrative Tools* or from the icon in the Quick Launch toolbar of the Taskbar.

If the Web Server role has already been installed you will see an IIS item in the left pane of Server Manager.



### 6.3 Installing IIS on Windows Server (2012 R2, 2016, 2019)

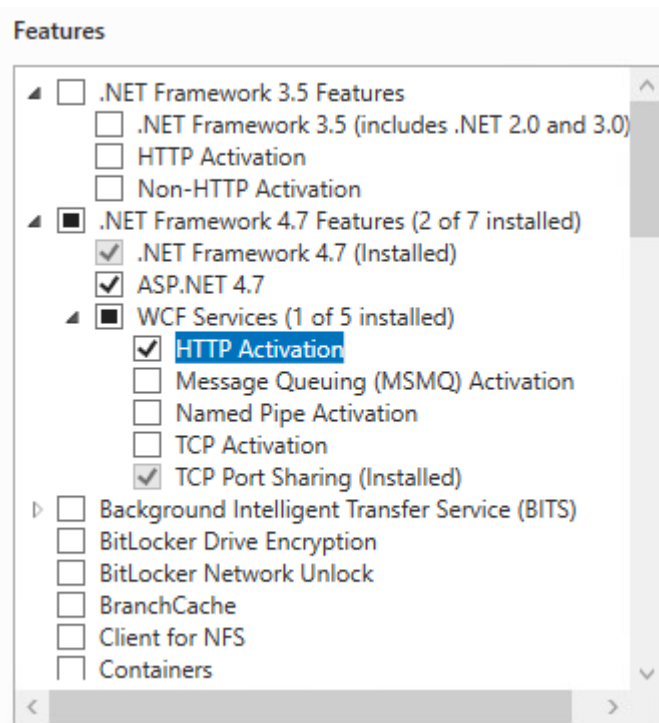
IIS must be installed on the web server before installing the Welch Allyn Web Upload software.

1. Launch **Server Manager** from *Start -> Administrative Tools* or from the icon in the Quick Launch toolbar of the Taskbar.
2. Click **Add Roles and Features**.

3. On the Before You Begin page, click **Next >**.
4. On the Select installation type page, select **Role-based or feature-based installation**. Then click **Next >**.
5. On the Select destination server page, select **Select a server from the server pool**. Verify the local server is highlighted in the *Server Pool*. Then click **Next >**.
6. On the Select server roles page, check **Web Server (IIS)**. A popup dialog will appear to add the IIS Management Console feature (required for the Web Server role). Click on Add Features, and then click **Next >**.
7. On the Select features page, accept the default selections in **.NET Framework 4.7 Features** and **add**:
  - a. ASP.NET 4.7
  - b. WCF Services \ HTTP Activation

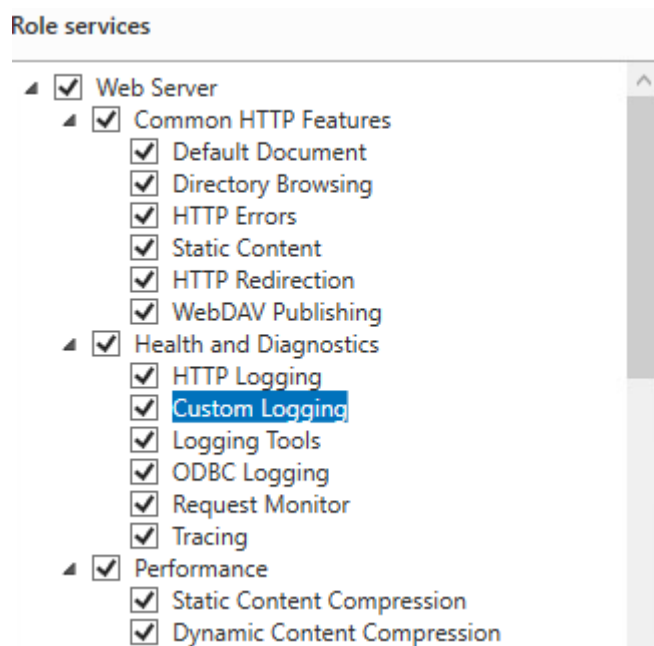
NOTE: For Server 2012 R2 the references throughout will be to .Net 4.5.

For Server 2016 the references throughout will be to .Net 4.6.

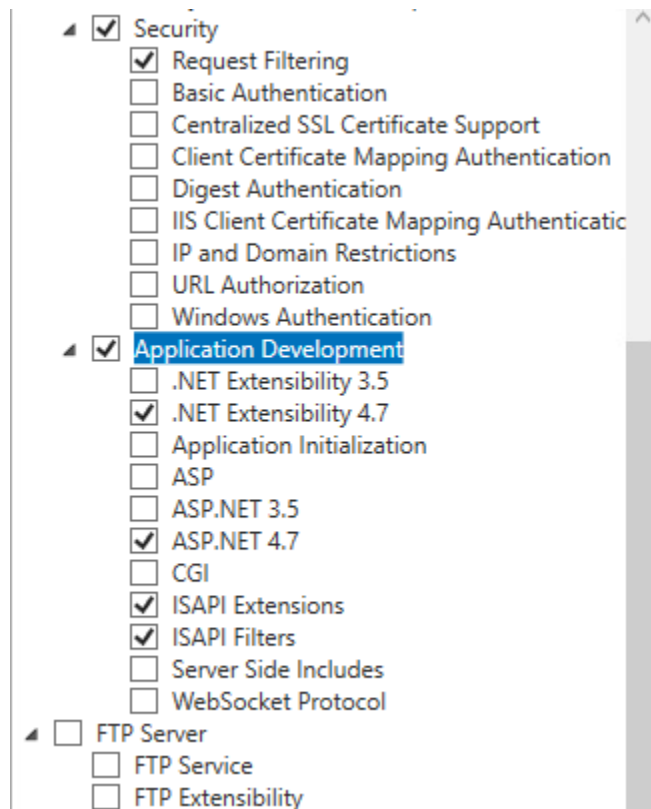


8. Clicking on HTTP Activation will bring up another dialog to Add Features That Are Required For HTTP Activation (e.g. ASP.NET 4.7, etc.). Click on Add Features, and then click **Next >**.

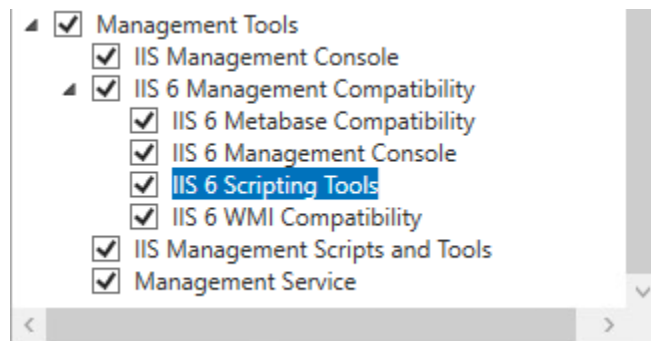
9. On the Select role services page, accept the default selections and **add**:
  - a. Check all items under Common HTTP Features, Health and Diagnostics and Performance.



- b. Security, Application Development and FTP Server defaults are fine.



- c. Select all items under Management Tools.



10. Click **Next >**.
11. On Confirm installation selections page, view the list of features to be installed. Then click **Install**.
12. On the Installation progress page, monitor the installation. When it is done, click **Close**.
13. **Close** the **Server Manager** application.

## 6.4 Configuring SSL and Authentication

If your system will be using SSL to secure communications, obtain and install an SSL certificate on the server **before** installing the Web Upload Server software.

See also *Limiting Access to Authenticated Users* in section 6.6 *Post-Install IIS Configuration* if you will be using basic authentication to limit access to the host site. If basic authentication is enabled, install an SSL certificate to secure the transmission of the plain text passwords

## 6.5 Installing Web Upload Server Software

- Insert Welch Allyn Web Upload installation media and open the "Server Install" folder.
- Double click on **setup.exe**.

The Welch Allyn Web Upload Server Setup wizard-installer screen will guide you through the required installation steps.

1. On the page Welcome to the Welch Allyn Web Upload Server 4.1.0 Setup Wizard, click **Next >**

Enter *domain name or IP address* of the web site hosting the upload site. This field must not be left blank.

- If the host site will be accessed via public Internet, enter the full domain name or public IP address of the web server. Do not include the name of the virtual directory.
- If the host site will be accessed via local network only, enter a local IP that is accessible by all intended clients.

Do not include "http:" at the start, or use "/" at the end. Do not include any leading or trailing spaces. EXAMPLES: www.acmescanning.com; 65.120.23.120; cardiacservices.net.

2. Click **Next >**

Enter *client application* name. This field must not be left blank.

The name entered here is combined with the domain name (or IP) and will appear in the client's Start/Program menu. EXAMPLES:

Domain name (or IP)	Client application name	Name in client's Start/Program menu
www.acmescanning.com	Upload	www.acmescanning.com Upload
research.com	Study 3009A	research.com Study 3009A

Use only letters, numbers, spaces, and dashes. Do not use any type of punctuation. Do not include any leading or trailing spaces. Limit length to 30 characters.

3. Click **Next >**

Enter *virtual directory* name. This field must not be left blank.

This is the name of the IIS virtual directory that the web server software will be installed in. The name must be unique and not conflict with any existing web site directories.

Use only letters or numbers. Do not use any spaces or punctuation. Limit length to 24 characters.  
EXAMPLES: upload; webupload; hscribeupload

4. Click **Next >**

The Welch Allyn Web Upload Server Confirm installation screen is displayed; the installer is ready to install.

5. Click **Next >**

Welch Allyn Web Upload Server installation is initiated. A setup.exe window may appear behind the main installer window asking to invalidate the signature of this executable. Click **Yes** to continue.

6. After the **Installation Complete** screen is displayed, click **Close**.

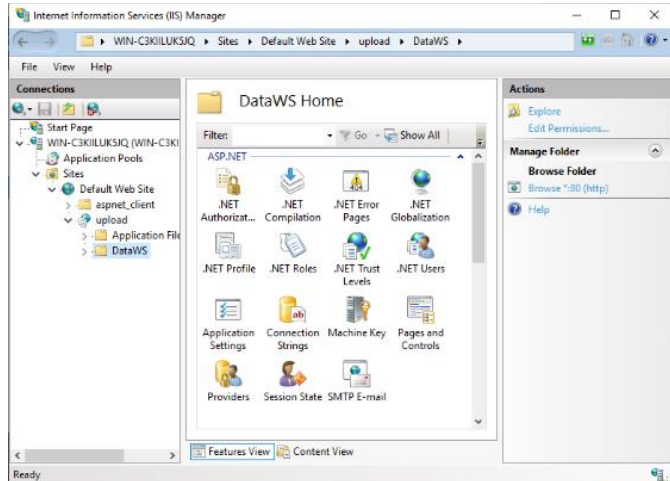
## 6.6 Post-Install IIS Configuration

The following IIS configuration steps must be performed by an administrative user after the installer has run. Screen shots provided are from Windows 2019 Server. Installation steps are the same for Windows Server 2012 R2.

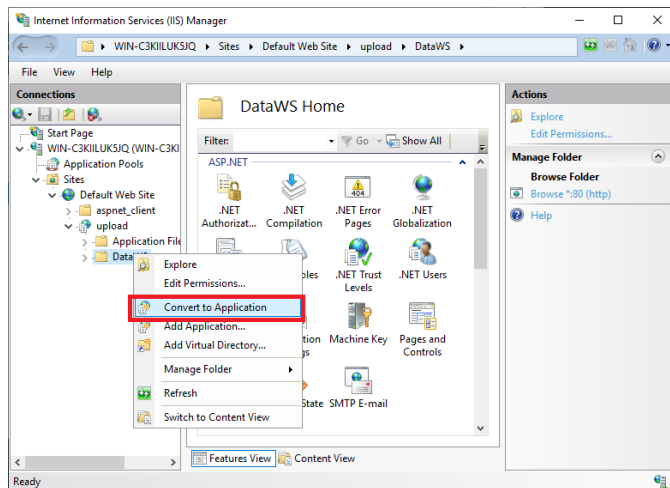
### Creating the Web Application and configuring the application pool

1. Run Control Panel/Administrative Tools/Internet Information Services (IIS) manager.

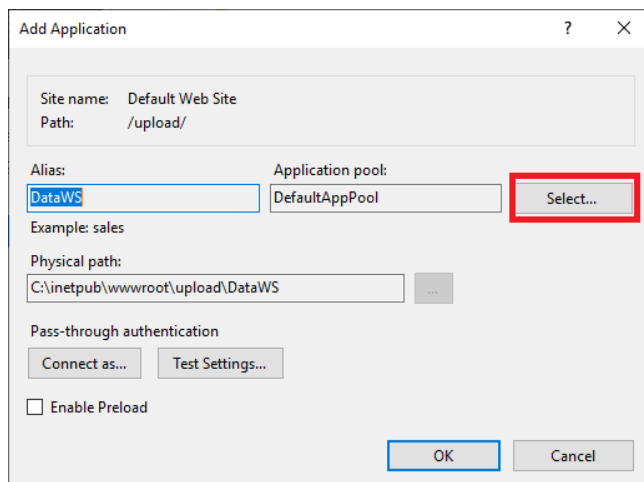
- Open the IIS manager; open the default web site followed by the selected virtual directory.



- Right click the DataWS folder and select **Convert to Application**.

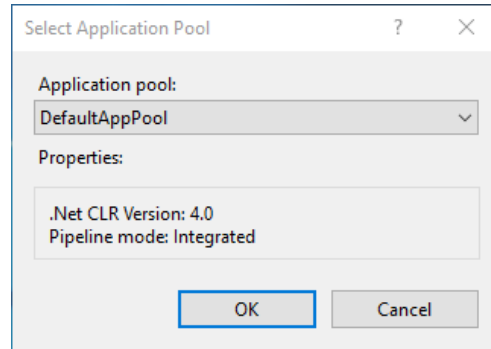


- Select the desired Application pool: use "DefaultAppPool", or create a new one if needed.

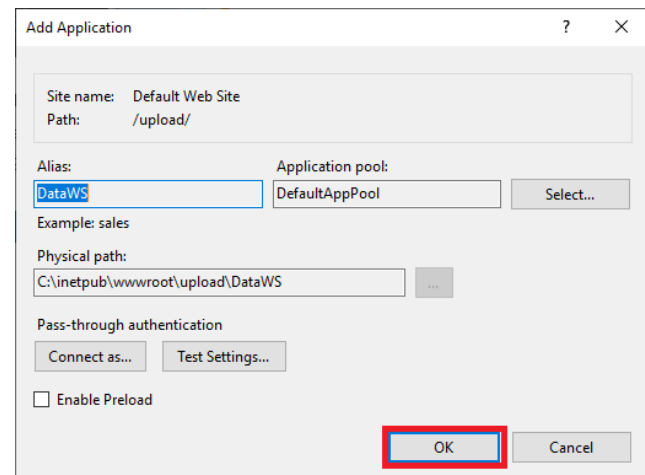




5. Select your application pool and click **OK**.



6. Click **OK**.



## Limiting Access to Authenticated Users

The default installation configures the web site for anonymous access. If the web site is accessible from the Internet and is configured for anonymous access, any Internet user can install the client application from the server and upload recordings to the server.

Disabling anonymous access limits access to only authenticated users; the client upload application will prompt users for a name, password, and domain. User accounts may be:

- Accounts on the local web server
- Accounts within Active Directory

Basic authentication is available for both types of user accounts. Digest authentication can be used only when the user account is in Active Directory and is configured to “Store password using reversible encryption”.

Basic authentication sends passwords on the network/Internet in plain text (unencrypted). If using basic authentication, use SSL to secure the transmissions of passwords.

There are two options for limiting access to authenticated users. You may select one or both options.

1. Limit access to publish.htm: limits access to web page that allows users to install client application.

**NOTE:** *publish.htm* will download the *setup.exe* application for the user to run. That application will request **WebUploadApplication.application** and files in the **Application+Files/WebUplodApplication<version>** folder from the web server. *Setup.exe* requests those files anonymously, so do not restrict access to those files and folders, and leave Anonymous Access enabled on the website.

2. Limit access to web services: only authenticated users will be able to upload recordings.

### **IIS Configuration for Authenticated Access to publish.htm**

It is recommended to use a Security Group to manage the users that have permission to install the client. In the steps below, a group called "WebUpload Installers" is used as an example.

1. Create a **Security Group**, e.g. **WebUpload Installers**. Add the appropriate users to this security group.
2. Launch **IIS Manager**.
3. Browse to the application website and then open the IIS **Authentication** feature. *NOTE: this is the website/folder that contains **publish.htm** and the **Application Files** folder.*
4. **Enable Basic** or **Digest Authentication** as appropriate. *NOTE: do not disable Anonymous Authentication.*
5. Next, in the Content View, select **publish.htm** and then right-click and select **Edit Permissions...**
6. Go to **Security** tab.
7. Click **Advanced**.
8. Click **Disable inheritance**. Use the default setting "Convert inherited permissions to into explicit permission on this object."
9. Select **Users** (<hostname>\Users) and click **Remove**.
10. Select **IIS\_IUSRS** and click **Remove**.
11. Click **Add**.
12. Click **Select a principal**, and then find the **WebUpload Installers** security group.
  - a. Type = **Allow**
  - b. Basic permissions = **Read & execute, Read**
13. Click OK, OK, OK.

### **IIS Configuration for Authenticated Access to Web Services**

It is recommended to use a Security Group to manage the users that have permission to use the client. In the steps below, a group called "WebUpload Users" is used as an example.

1. Create a **Security Group**, e.g. **WebUpload Users**. Add the appropriate users to this security group.
2. Launch **IIS Manager**.
3. Browse to the WebUpload services website and open the IIS **Authentication** feature. *NOTE: this is the website/folder that contains **DataServices.asmx**, typically called **DataWS**.*
4. **Enable Basic** or another method as appropriate, e.g. **Digest Authentication**.
5. **Disable Anonymous Authentication**.
6. Go back to the **Features View** of the DataWS application.
7. Select **Authorization Rules** under IIS.
8. Remove the rule to allow **Anonymous Users**.

9. Add a new **Allow** rule for:
  - a. Specified roles or user groups: **WebUpload Users** (or whatever security group was used in step 1.)
  - b. Click **OK**

## 6.7 Testing the Web Upload Client Click Once Deployment

The storage directory used by the web service and the web service identity **must** be configured before the web site is operational. This configuration is performed within the Mortara Instrument Inc/WebUpload Server Settings program.

See section 7.1.3 The Server Configuration Tab for information on changing these settings.

The web page **publish.htm** is copied to the web server during installation; it will be used by client computers to install the upload client. The URL of this web page is determined by:

- domain or IP address of the web server
- virtual directory specified during installation
- SSL configuration

**NOTE:** Configuring the web site for SSL will result in secure communications between the client application and the web server. To use SSL, you must first obtain a Web Server SSL certificate from an issuing authority (Verisign, GoDaddy, etc.). SSL requires the use of Port 443. Be sure to open this port in the firewall configuration.

Using *mycompany.com* as the domain and *upload* as the virtual directory name, the URL of the web page would be *http://mycompany.com/upload/publish.htm* (or *https://mycompany.com/upload/publish.htm* with SSL configuration).

The test may be performed locally (on the web server) or from a remote computer. A test performed locally will not test the web server's connectivity to the Internet because it will succeed even in the presence of firewall(s) or other network problems. Testing from a remote computer--outside all firewalls--will verify the customer's ability to connect to the web site.

Open web browser and browse to the URL of the web page. See Section 8 Troubleshooting if any the following tests fail.

A page displays similar to the one shown.

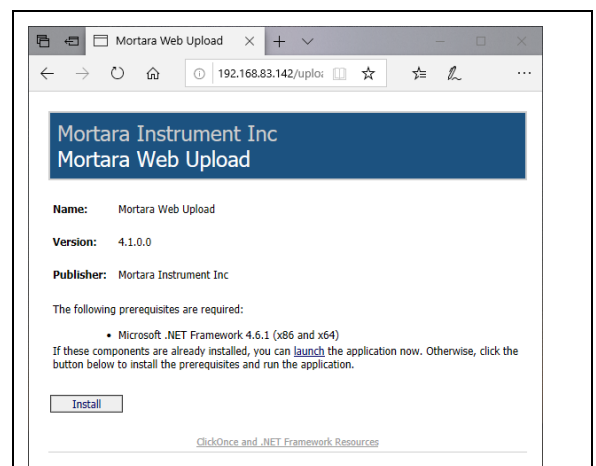
1. Once at the web page, click **Install**.

An Application Install – Security Warning will display listing the company name, IP address, and Publisher.

2. Click **Install**.

Installation will proceed and display a progress bar. When finished, an Application Setup screen displays requesting the location for a new storage directory.

3. Click **Save**.



## 7. CONFIGURING WEB UPLOAD SERVER SETTINGS

---

A program named “Web Upload Server Settings” is installed during the Web Upload Server software installation. This program is used to modify the following List settings to:

- Edit or add indications
- Edit or add referring physicians
- Edit or add hook up technicians
- Edit or add visits
- Edit or add a diary annotation
- Edit or add a medication
- Edit or add races

This program is used to customize the Client settings to:

- Modify the content and/or appearance of the client application header
- Modify web server (web.config) settings
- Use Clinical Research Demographic Data Collection, or
- Use Healthcare Demographic Data Collection

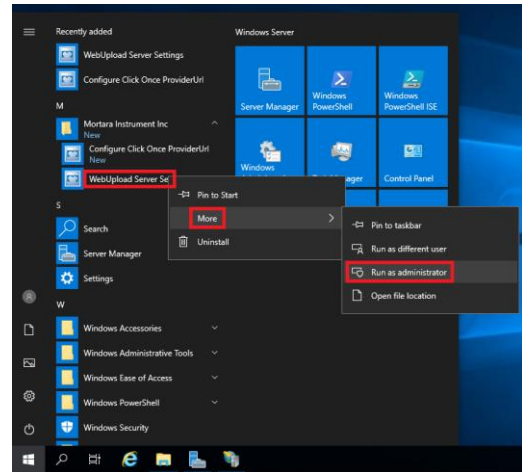
The program also contains utilities for:

- Retrieving and viewing event logs from a remote webserver
- Retrieving and viewing event logs from the local webserver
- Creating a diagnostic report to aid in web server troubleshooting
- Maintenance of the storage directory

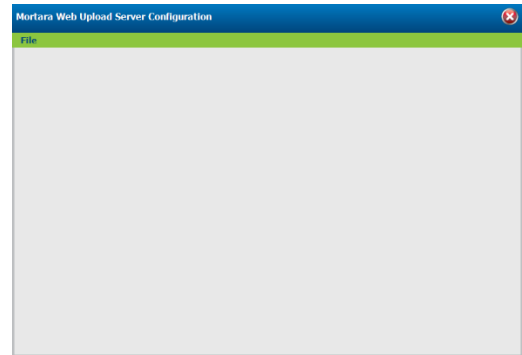
A second application “Configure Click Once Provider URL” can be used to change the URL from which the Web Upload Client is deployed.

### 7.1 Web Upload Server Settings Application

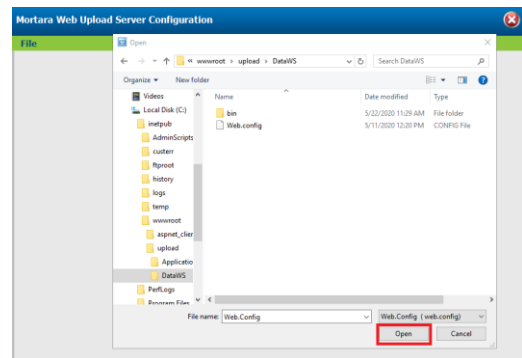
1. Right click on “Mortara Instrument Inc/WebUpload Server Settings” in the start menu. Select More, then Run as administrator to run start the server setting application as an administrator.



2. Click on **File** to open the menu.

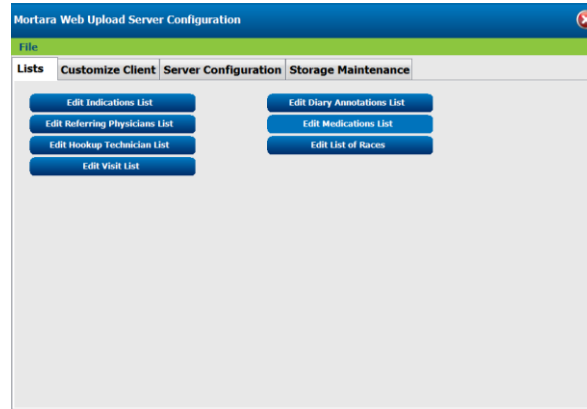


3. Select **Open Web.Config...** from the menu.
4. Navigate to the **DataWS** folder and open Web.Config. The folder location depends on:
  - The location of the base web site. On most servers this will be c:\inetpub\wwwroot or d:\inetpub\wwwroot.
  - The name of the virtual directory that was entered during the installation procedure. The example assumes “Upload” was entered.



### 7.1.1 The Lists Tab

After you open **web.config**, the following screen with the Lists tab selected will appear.



#### Server Lists

The Lists tab allows you to manage the data in seven lists:

- Indications List
- Diary Annotations List
- Referring Physicians List
- Medications List
- Hook Up Technicians List
- Visit List
- List of Races

Data in these lists will be automatically updated in all client applications.

The client application uses the list data as choices in the screens for patient demographic entry and diary entry.

#### Adding a List Item

1. Click on the button for the list you wish to modify.
2. Click **Add**.
3. Enter the text for the item.
4. Click **Save**.

#### Moving a List Item

1. Click on the button for the list you wish to modify.
2. Click on the item you wish to move.
3. Click **Move Up** or **Move Down**.
4. Click **Save**.

## Removing a List Item

1. Click on the button for the list you wish to modify.
2. Click on the item you wish to remove.
3. Click **Remove**.
4. Click **Save**.

## Editing a List Item

1. Click on the button for the list you wish to modify.
2. Click on item you wish to modify
3. Enter your changes.
4. Click **Save**.

### 7.1.2 The Customize Client Tab

The Customize Client tab selection allows you to control the content and appearance of the header area within the client application.

The screenshot shows the 'Mortara Web Upload Server Configuration' window with the 'Customize Client' tab selected. The window contains the following elements:

- Title Bar:** Mortara Web Upload Server Configuration
- Menu:** File
- Tabs:** Lists, **Customize Client**, Server Configuration, Storage Maintenance
- Radio Buttons:**
  - Use Clinical Research Demographic Data Collection
  - Use Healthcare Demographic Data Collection
- Title:** [Empty text input field]
- Font:** Arial (dropdown menu)
- Font Style:**  Bold,  Italic,  Underline
- Font Size:** 14 (dropdown menu)
- Text Alignment:** MiddleCenter (dropdown menu)
- Position title over:**  Yes,  No
- Scale image to full width:**  Yes,  No
- Text Color:** Text Color Sample, [Select Color... button]
- Buttons:** Save, Delete Image..., Import Image...

Mortara Web Upload Server Configuration

File

Lists Customize Client **Server Configuration** Storage Maintenance

Use Clinical Research Demographic Data Collection  
 Use Healthcare Demographic Data Collection

Title

Font

Font Style  Bold  Italic  Underline

Font Size  Text Alignment

Position title over  Yes  No Scale image to full width  Yes  No

Text Color **Text Color Sample**

WWW.MortaraWebUpload.com

1. Click on the **Customize Client** tab.
2. Make your changes using the drop-down lists, check boxes and radio buttons.



Feature	Description	Values
Use Clinical Research Demographic Data	The WebUpload client will display the following demographic fields: <ul style="list-style-type: none"> <li>• Subject primary and secondary ID</li> <li>• Subject initials</li> <li>• Subject sex and birthdate</li> <li>• Investigator name</li> </ul>	
Use Healthcare Demographic Data	The WebUpload client will display the following demographic fields: <ul style="list-style-type: none"> <li>• Patient ID</li> <li>• Patient first and last name</li> <li>• Patient sex and birthdate</li> <li>• Referring physician name</li> </ul>	
Ready-Only	When using <i>Healthcare Demographic Data</i> , the demographics are not editable after the data is copied from the recorder.	
Title	Title displayed at the top of the WebUpload client software. This helps the user verify where the recordings will be sent.	
Font	Font for the <i>Title</i> .	<ul style="list-style-type: none"> <li>• Arial</li> <li>• Arial Black</li> <li>• Comic Sans MS</li> <li>• Courier New</li> <li>• Franklin Gothic Medium</li> <li>• Georgia</li> <li>• Impact</li> <li>• Lucida Console</li> <li>• Lucida Sans Unicode</li> <li>• Microsoft Sans Serif</li> <li>• Palatino Linotype</li> <li>• Tahoma</li> <li>• Time New Roman</li> <li>• Veranda</li> </ul>
Font Style	Font Style for the <i>Title</i> . Any combination of styles can be selected.	<ul style="list-style-type: none"> <li>• Bold</li> <li>• Italic</li> <li>• Underline</li> </ul>
Font Size	Font Size for the <i>Title</i> .	Ranges from 8 to 32 points.
Text Alignment	Alignment of the <i>Title</i> text within the title area.	<ul style="list-style-type: none"> <li>• Top Left</li> <li>• Top Center</li> <li>• Top Right</li> <li>• Middle Left</li> <li>• Middle Center</li> <li>• Middle Right</li> <li>• Bottom Left</li> <li>• Bottom Center</li> <li>• Bottom Right</li> </ul>

Feature	Description	Values
Position title over		<ul style="list-style-type: none"> <li>• Yes</li> <li>• No</li> </ul>
Scale image to full width	If <i>Yes</i> , scales the imported <i>Title</i> background image to be 780 pixels wide.	<ul style="list-style-type: none"> <li>• Yes</li> <li>• No</li> </ul>
Text Color	Color <i>Title</i> text.	
Select Color... Button	Button for selecting <i>Title</i> text color.	
Delete Image... Button	Button to delete the previously imported <i>Title</i> background image.	
Import Image... Button	Button to select a JPEG file for the <i>Title</i> background image. The <i>Title</i> area is 780 pixels wide. The minimum height is 60 pixels, but the WebUpload client will display an image as tall as 100 pixels. Images taller than 100 pixels will be cropped.	
Save Button	Button to Save the client customization settings.	

3. Use **Import Image...** to insert a picture or a logo. You can also **Delete Image...**
4. Click **Save** to save your changes. The Welch Allyn Web Upload client application is automatically updated with any changes you make here.

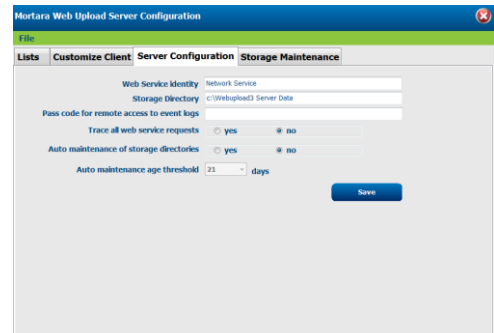
### 7.1.3 The Server Configuration Tab

This tab page allows you to configure settings used by the web services.

1. Click on the **Server Configuration** tab.
2. Make your changes using the drop-down lists, radio buttons and text boxes.

Refer to details below and on the next pages for each item.

3. Click **Save** to save your changes.



#### Web Service Identity

The Web Service Identity must be set to the identity of the Application Pool assigned to the DataWS virtual directory. The program will supply a default Web Service Identity of 'Network Service' which will be appropriate for most servers. The web service identity is not stored in the configuration. It is used to adjust the security of the storage directory to allow sufficient access to the web application and is required only when the storage directory is changed.

#### Storage Directory

Enter the complete path to the folder you wish to use for data storage. The folder should be located on a local hard disk drive. This folder will be used to store all uploaded Holter and ABP recordings and configuration

information. You may enter the name of an existing folder or a new folder. A new folder is preferred. Be sure to enter a complete path which must include a drive letter. For security reasons, do not use a path that is an IIS virtual directory or a path this is parented by a virtual directory. Do not use any path that is parented by inetpub or inetpub/wwwroot.

It is recommended that the storage directory be set only once. If you change it, the data stored in the original directory will not be moved to the new one. You must manually move any data you wish to preserve across a directory change.

### **Pass Code for Remote Access to Event Logs**

You may optionally enter a pass code to allow remote access to the web server event logs. By default, the pass code is empty which prevents all event log remote access. Entering a pass code will allow remote access to the event logs to all persons with knowledge of the pass code. Remote access to the event logs may be useful to remote users who are assisting in troubleshooting web server or client issues.

### **Trace All Web Service Requests**

Enable this option to turn on tracing of all web service activity. When this option is enabled, all web service requests will create any entry in the event log. This option will have a significant negative impact of web server performance and should not be enabled permanently. It should be enabled only when diagnosing server or client problems. This option is disabled by default.

### **Auto Maintenance of Storage Directories**

When this option is enabled, the web service will automatically delete incomplete data directories that are older than the age specified by the age threshold.

An incomplete data directory is a directory that contains a recording that was not completely uploaded. This option is disabled by default.

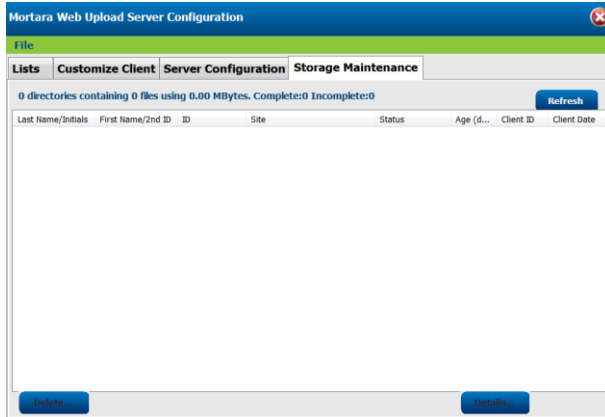
If this option is disabled, the web site administrator is encouraged to occasionally use the Storage Maintenance page to delete old and abandoned upload directories.

### **Auto Maintenance Age Threshold**

This setting controls how old an abandoned recording must be before it is deleted by the auto-maintenance process described above.

## 7.1.4 The Storage Maintenance Tab

This tab page provides the web site administrator a summary of all existing upload directories. It also allows the administrator to easily identify and delete old and abandoned recordings.



Each uploaded recording is stored in its own directory. Each item in the list represents one upload directory. The list can be sorted on any column by clicking on the column header.

Because a recording is automatically deleted by the HSCRIBE and HDS system or ELI PC Service after it has been successfully acquired, this list will not display recordings that have been imported.

A status of 'partial' will be displayed for recordings that have not been completely uploaded. These uploads will not be available to an HSCRIBE or HDS system or ELI PC Service until they are complete.

A status of 'complete' will be displayed for recordings that are completely uploaded. These recordings will be available to an HSCRIBE or HDS system or ELI PC Service.

The Age column is calculated using the age of the most recent file in the upload directory.

The Client ID column identifies the source of the uploaded recording. Each client application is assigned a client id. The application client id is available in the **About** menu.

To view the complete details for a recording, select the recording in the list and click the **Details** button.

## 7.2 Configure Click Once Provider URL Application

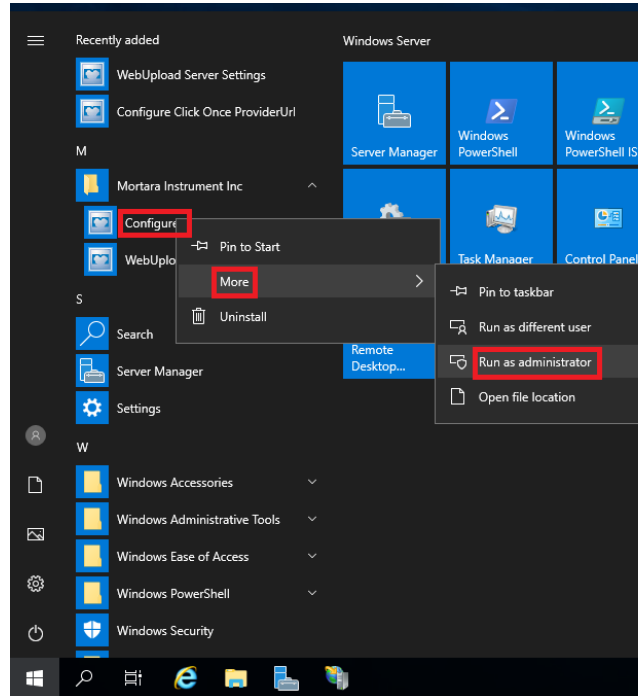
This step is required when:

- The domain you entered during the installation was incorrect. A user attempting to install the client upload application from your web server will get an error message similar to the message in Section 8.3.
- You need to move the web site to a different URL.

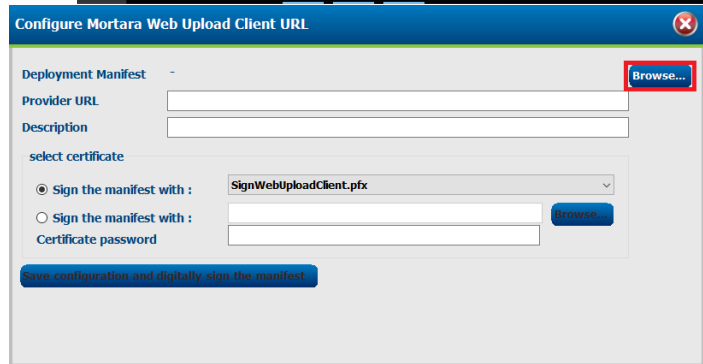
To remedy these situations, the Deployment Provider URL contained within the deployment manifest needs to be updated.

**NOTE:** The following examples assume the name "Upload" was assigned to the virtual directory and the "Default Web Site" was selected during the installation.

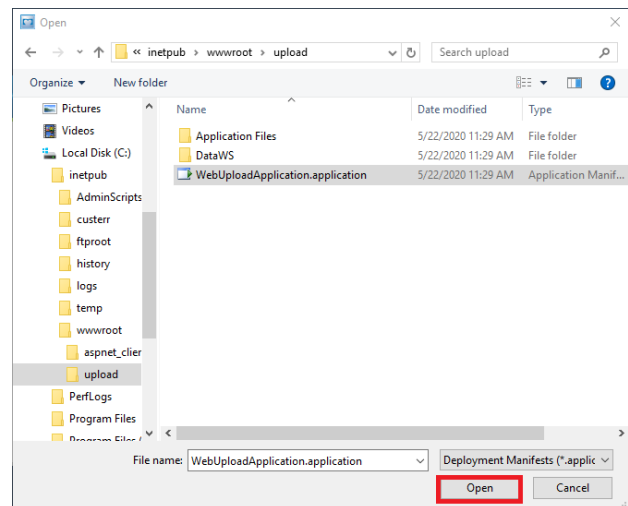
1. Right click on "Mortara Instrument Inc/Configure Click Once Provider URL" in the start menu. Select More, then Run as administrator to run start the configure URL application as an administrator.



2. Click **Browse**.

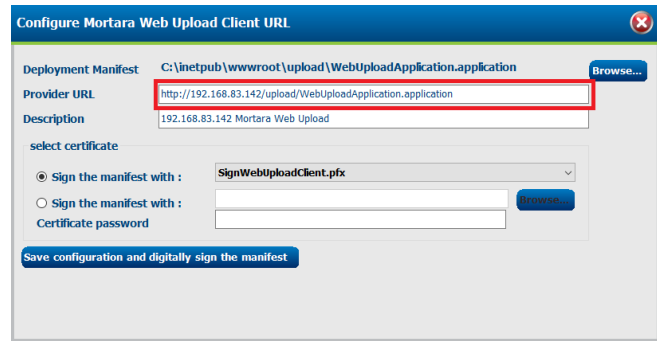


3. Use the **Open File** dialog to navigate to the upload virtual directory and open WebUploadApplication.application.

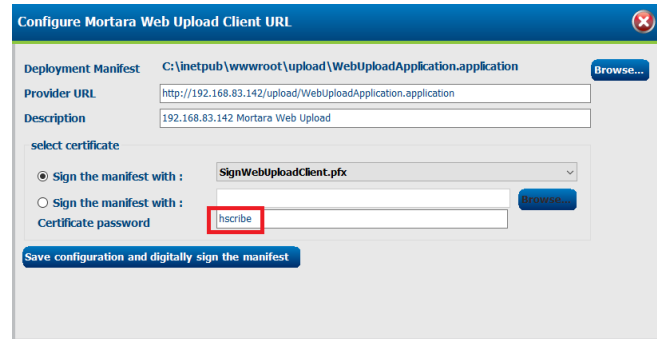


4. Enter the correct Provider URL.

Changing the Description field is allowed only if no users have installed the client application from your web site. Changing the Description field after the client application has been installed will require the installed applications to be removed and reinstalled.



5. Enter a certificate password of **hscribe**.
6. Click the **Save configuration and digitally sign the manifest** button.
7. Exit the program by clicking the close 'X' box.



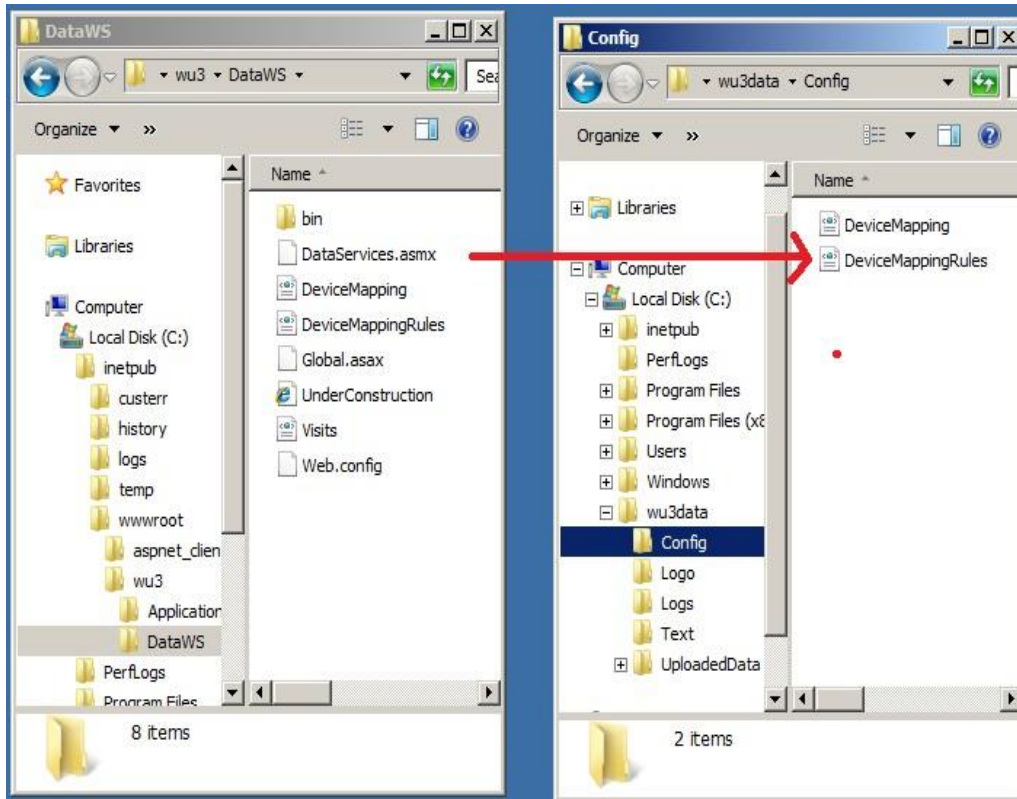
### 7.3 Directory Naming and Device Mapping

Welch Allyn Web Upload supports configurable rules for controlling the directory name of uploaded Holter and Ambulo 2400 recordings. These rules can be manually configured on the server and will apply to all client uploads.

**NOTE:** These rules will also apply to WAM PC recordings exported by WebUpload, but the ELI PC Service will automatically consume the recordings and export them into its Output Directory using its own filename scheme. These settings therefore have limited utility for WAM PC recordings.

The installation process does not automatically install support for these rules and the following steps must be followed in order for these rules to be available:

1. Copy the DeviceMappingRules.xml from the inetpub\wwwroot\YOURNAMEHERE\DataWS\ directory to the Config directory in the configured Data Storage Directory.
2. Copy the DeviceMapping.xml from the inetpub\wwwroot\YOURNAMEHERE\DataWS\ directory to the Config directory in the configured Data Storage Directory.



The rules are configured by editing the xml files. Care must be taken when editing the xml files because a violation of the XML syntax rules will result in a malformed and unusable XML file. If this occurs, the web site will remain operational but will refer to the default set of rules described later in this section.

### Renaming Rules

The renaming rules are broken down into two files:

1. DeviceMappingRules.xml
2. DeviceMapping.xml

### **DeviceMappingRules.xml**

This file contains two items which control naming rules for known and unknown devices. A known device is a device whose serial number is contained in DeviceMapping.xml. An unknown device is a device whose serial number is not contained in DeviceMapping.

<b>DeviceMappingRules.xml</b>
<pre> &lt;?xml version="1.0" encoding="utf-8"?&gt; &lt;DeviceMapping&gt;   &lt;NamingRules&gt;     &lt;NamingRule status="known" prefix="" delimiter="" suffix="" includeSiteName="true"       includeStudyName="true" order="studyFirst" /&gt;     &lt;NamingRule status="unknown" prefix="Unknown Device " delimiter="" suffix=""       includeSiteName="true" includeStudyName="true" order="studyFirst" /&gt;   &lt;/NamingRules&gt; &lt;/DeviceMapping&gt;           </pre>

Attribute name	Description
status*	Must be 'known' or 'unknown'. A known NamingRule will apply to all uploads for known (mapped) devices. . An unknown NamingRule will apply to all uploads for unknown (unmapped) devices.
delimiter	Optional, may be blank. If nonblank, this text will be inserted into the directory name between the study and site name.
suffix	Optional, may be blank. If nonblank, this text will inserted into the start of the directory name.
prefix	Optional, may be blank. If nonblank, this text will inserted at the end of the directory name.
includeSiteName	Must be 'true' or 'false'. If true, the directory name will contain the site name.
includeStudyName	Must be 'true' or 'false'. If true, the directory name will contain the study name.
order	Must be 'siteFirst' or 'studyFirst'. If it is 'siteFirst' the site name will precede the study name. If it is 'studyFirst' the study name will precede the site name.
* do not edit this attribute	

**DeviceMapping.xml**

This file contains directory naming rules for recordings from individual devices. Devices are identified by their serial number. Welch Allyn Holter recorders have a 10 or 12 digit serial number. ABP devices have a 5 digit serial number.

```

DeviceMapping.xml
<?xml version="1.0" encoding="utf-8"?>
<DeviceMapping>
  <Devices>
    <Device serialNumber="106262972165" studyName="Study 3908-A" siteName="Cardio Fusion Site-1" />
    <Device serialNumber="103103309160" studyName="Study 2710" siteName="West Elm Street" />
  </Devices>
</DeviceMapping>

```

Attribute name	Description
serialNumber	The Holter/ABP device serial number.
studyName	The name of the study this device is associated with. This name will always override the study name entered at the client, even if this name is blank.
siteName	The name of the site this device is associated with. This name will always override the site name entered at the client, even if this name is blank.

**Default Naming Rules**

Default rules for unknown devices	
Attribute name	Value
delimiter	-
suffix	(blank)
prefix	Unknown Device
includeSiteName	true
includeStudyName	true
order	studyFirst



Default rules for known devices	
Attribute name	Value
delimiter	-
suffix	(blank)
prefix	(blank)
includeSiteName	true
includeStudyName	true
order	studyFirst

## Invalid Characters

Some characters are invalid to use in directory names and will be automatically replaced with an '\_' (underscore).

invalidPathChars		{char[0x00000024]}
[0x00000000]		0x0022 '"'
[0x00000001]		0x003c '<'
[0x00000002]		0x003e '>'
[0x00000003]		0x007c ' '
[0x00000004]		0x0000 '\0'
[0x00000005]		0x0001 ' '
[0x00000006]		0x0002 ' '
[0x00000007]		0x0003 'L'
[0x00000008]		0x0004 'J'
[0x00000009]		0x0005 'I'
[0x0000000a]		0x0006 '—'
[0x0000000b]		0x0007 '\a'
[0x0000000c]		0x0008 '\b'
[0x0000000d]		0x0009 '\t'
[0x0000000e]		0x000a '\n'
[0x0000000f]		0x000b '\v'
[0x00000010]		0x000c '\f'
[0x00000011]		0x000d '\r'
[0x00000012]		0x000e '␣'
[0x00000013]		0x000f '␣'
[0x00000014]		0x0010 '†'
[0x00000015]		0x0011 '◄'
[0x00000016]		0x0012 '‡'
[0x00000017]		0x0013 '‡'
[0x00000018]		0x0014 '⌘'
[0x00000019]		0x0015 '⌘'
[0x0000001a]		0x0016 '‡'
[0x0000001b]		0x0017 '‡'
[0x0000001c]		0x0018 '‡'
[0x0000001d]		0x0019 '‡'
[0x0000001e]		0x001a '→'
[0x0000001f]		0x001b '←'
[0x00000020]		0x001c ''
[0x00000021]		0x001d ''
[0x00000022]		0x001e ''
[0x00000023]		0x001f ''

invalidFileNameChars		{char[0x00000029]}
[0x00000000]		0x0022 '"'
[0x00000001]		0x003c '<'
[0x00000002]		0x003e '>'
[0x00000003]		0x007c ' '
[0x00000004]		0x0000 '\0'
[0x00000005]		0x0001 ' '
[0x00000006]		0x0002 ' '
[0x00000007]		0x0003 'L'
[0x00000008]		0x0004 'J'
[0x00000009]		0x0005 'I'
[0x0000000a]		0x0006 '—'
[0x0000000b]		0x0007 '\a'
[0x0000000c]		0x0008 '\b'
[0x0000000d]		0x0009 '\t'
[0x0000000e]		0x000a '\n'
[0x0000000f]		0x000b '\v'
[0x00000010]		0x000c '\f'
[0x00000011]		0x000d '\r'
[0x00000012]		0x000e '␣'
[0x00000013]		0x000f '␣'
[0x00000014]		0x0010 '†'
[0x00000015]		0x0011 '◄'
[0x00000016]		0x0012 '‡'
[0x00000017]		0x0013 '‡'
[0x00000018]		0x0014 '⌘'
[0x00000019]		0x0015 '⌘'
[0x0000001a]		0x0016 '‡'
[0x0000001b]		0x0017 '‡'
[0x0000001c]		0x0018 '‡'
[0x0000001d]		0x0019 '‡'
[0x0000001e]		0x001a '→'
[0x0000001f]		0x001b '←'
[0x00000020]		0x001c ''
[0x00000021]		0x001d ''
[0x00000022]		0x001e ''
[0x00000023]		0x001f ''
[0x00000024]		0x003a ':'
[0x00000025]		0x002a '*'
[0x00000026]		0x003f '?'
[0x00000027]		0x005c '\\'
[0x00000028]		0x002f '/'

## 7.4 Firewall Configuration

Incoming HTTP port 80 and/or HTTPS port 443 must be open to the web server.

## 8. TROUBLESHOOTING

---

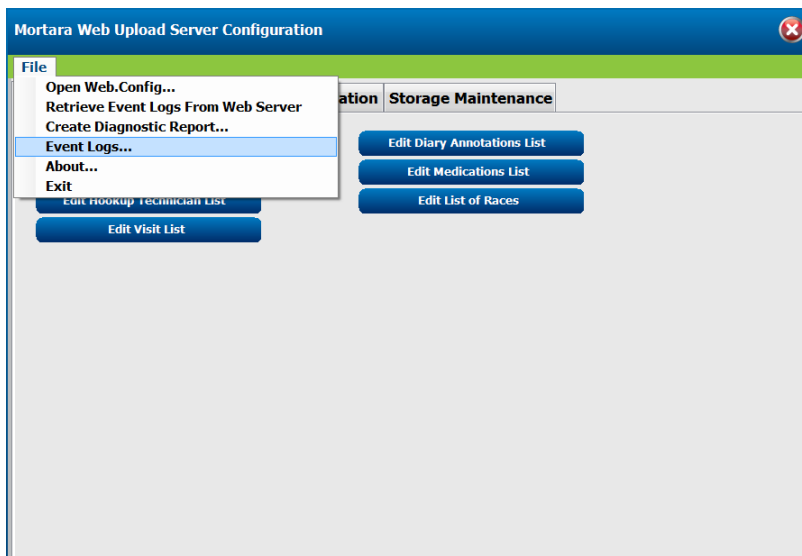
### 8.1 Event Logs

The web service records significant events and errors in event log files. Event log files are maintained for one month. Event log files older than one month will be automatically deleted.

#### Local Event Logs

To view event logs for your local web server follow these steps.

1. Open the **Web Upload Server Settings** application as described in Section 7.
2. Select **Event Logs** from the file menu.



When first opened, the Event Logs window will display the entries for the current date. The date and time range may be changed to display entries for another date range.

**NOTE:** The date range works backwards from the specified date.

The type and category selections can be used to filter the list to display only the selected type and/or category.

The **Copy to Clipboard** button will copy information for all entries into the Windows clipboard where it can be pasted into an email program or text editor.

The **Details** button becomes enabled when an individual entry has been selected. Clicking this button will open another window that displays additional information for the log entry.

## Remote Event Logs

Event logs may be retrieved remotely only if the server is configured to allow remote retrieval. See Section 7.1.3. Event logs may be retrieved from a remote web server and displayed.

1. Select **Retrieve Event Logs from Web Server** from the **File** menu.
2. Enter the URL of the web service you wish to retrieve from. Be sure to include `http://` at the beginning of the URL.
3. Select the date and number of days you wish to retrieve.  
*NOTE: The date range works backwards from the selected date.*
4. Click the **Search** button.
5. Enter the pass code and click **OK**.

## 8.2 Create Diagnostic Report

The diagnostic report can be created to facilitate and coordinate troubleshooting efforts with off-site personnel.

### Save Report to Local Disk

1. Open the **Web Upload Server Settings** application as described in Section 7.
2. Select **File > Create Diagnostic Report** from the menu.
3. Use the **Browse...** button to select the directory where the report is to be stored.
4. Select the check boxes for the Report Contents you wish to include with the diagnostic report.



5. Select the **Save Report** button to save the diagnostic report to your specified directory.

Name	Date modified	Type	Size
DataStorageSummary.txt	02/27/2013 9:07 PM	Text Document	1 KB
DirectoryPermissions.txt	02/27/2013 9:07 PM	Text Document	8 KB
iisInfo.txt	02/27/2013 9:07 PM	Text Document	90 KB
Log_2013_2_27_1.xml	02/27/2013 3:06 PM	XML Document	2 KB
UploadClientFiles.txt	02/27/2013 9:07 PM	Text Document	6 KB
web.config	02/27/2013 2:09 PM	CONFIG File	3 KB
WebUploadApplication.application.txt	02/27/2013 1:50 PM	Text Document	6 KB

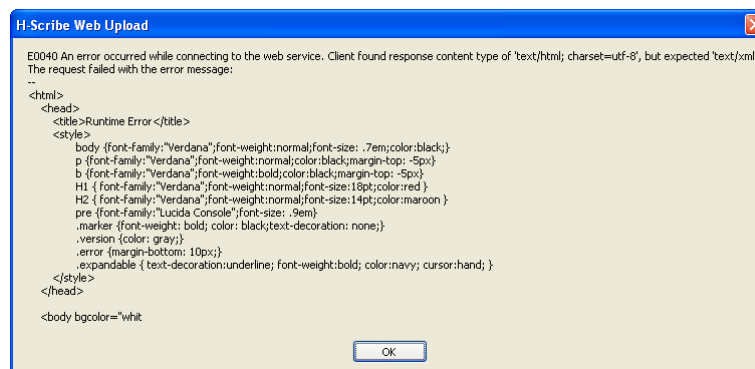
## Diagnostic Report Contents Description Table

Item	Description	File Name
Web.config	The configuration file for the web services	Web.config
Log Files	Several of the most recent log files will be included	Log_YYYY_MM_DD.xml YYYY = year, MM=month, DD=date
IIS Configuration	<b>Note: This file may contain passwords for alternate App Pools</b>	lisinfo.txt
Client Upload Application	A directory listing of all files in the inetpub\wwwroot directory	UploadClientFiles.txt
Data Storage Summary	A detailed summary of all uploaded recordings. The summary will not include any patient information.	DataStorageSummary.txt
Data Storage Summary (includes patient information)	A detailed summary of all uploaded recordings. The summary will contain patient names and ID numbers for recordings that have been completely uploaded.	DataStorageSummary.txt
Directory Permissions	A summary of directory permissions for the web service directory and the storage directory.	DirectoryPermissions.txt
Configuration files		DiaryAnnotations.txt, HookUpTechs.xml, Indications.xml, LogImage.jpg, LogoText.xml, Medications.xml, ReferringPhysicians.xml

## 8.3 Troubleshooting Symptoms

### Application Not Created / Incorrect ASP.NET version

The following error message will be displayed in the client application when either the web application was not created or the ASP.NET version was not set to 4.5 or later. See Section 6.

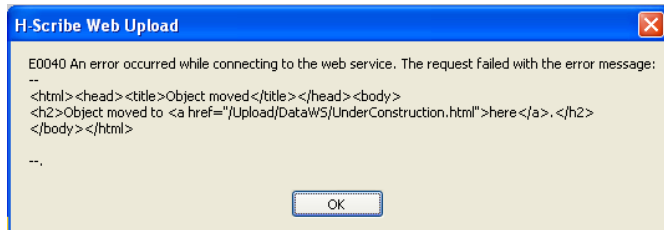


```

E0040 An error occurred while connecting to the web service. Client found response content type of 'text/html; charset=utf-8', but expected 'text/xml'.
The request failed with the error message:
--
<html>
<head>
<title>Runtime Error </title>
<style>
body {font-family:"Verdana";font-weight:normal;font-size:.7em;color:black;}
p {font-family:"Verdana";font-weight:normal;color:black;margin-top:-5px}
b {font-family:"Verdana";font-weight:bold;color:black;margin-top:-5px}
H1 {font-family:"Verdana";font-weight:normal;font-size:1.8pt;color:red }
H2 {font-family:"Verdana";font-weight:normal;font-size:1.4pt;color:maroon }
pre {font-family:"Lucida Console";font-size:.9em}
.marker {font-weight:bold;color:black;text-decoration:none;}
.version {color:gray;}
.error {margin-bottom:10px;}
.expandable { text-decoration:underline;font-weight:bold;color:navy;cursor:hand;}
</style>
</head>
<body bgcolor="whit
  
```

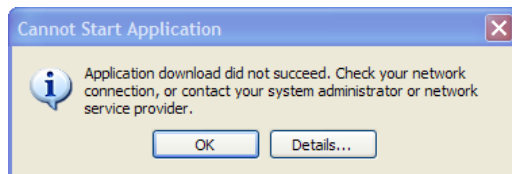
## Data Storage Directory Not Set

The following error message will occur if the data storage directory has not been configured. See Section 7.1.4.



## ProviderURL is incorrect

The following messages will appear during the installation of the application on the client machine if the domain name (or IP address) of the web server was incorrectly entered during installation.



Click on the Details button to display a message similar to:

### PLATFORM VERSION INFO

Windows	: 5.1.2600.131072 (Win32NT)
Common Language Runtime	: 2.0.50727.1433
System.Deployment.dll	: 2.0.50727.1433 (REDBITS.050727-1400)
mscorwks.dll	: 2.0.50727.1433 (REDBITS.050727-1400)
dfdll.dll	: 2.0.50727.1433 (REDBITS.050727-1400)
dfshim.dll	: 2.0.50727.1433 (REDBITS.050727-1400)

### SOURCES

Deployment url	:	
<i>http://holterwebupload.com/upload/WebUploadApplication.application</i>		
Server	:	Microsoft-IIS/6.0
X-Powered-By	:	ASP.NET
Deployment Provider url	:	
<i>http://holterwebuploa.com/Upload/WebUploadApplication.application</i>		

### ERROR SUMMARY

Below is a summary of the errors, details of these errors are listed later in the log.

- \* Activation of *http://holterwebupload.com/upload/WebUploadApplication.application* resulted in exception. Following failure messages were detected:
  - + Downloading *http://holterwebuploa.com/Upload/WebUploadApplication.application* did not succeed.
  - + The remote name could not be resolved: 'holterwebuploa.com'

See Section 7.2 for steps on changing the deployment provider URL.

## 9. CONFIGURING PROGRAMS THAT USE WEB UPLOAD DATA

---

### 9.1 H-Scribe Version 4.xx

The following configuration must be performed to allow an H-Scribe system with version 4.3x software to access and acquire uploaded Holter recordings. On the web server, the directory created within the Data Storage Directory (see Section 7.1.4 using the example named UploadedData) must be made accessible to the H-Scribe system. Create a file share for this directory and grant H-Scribe users full control; adjust the security settings to give H-Scribe users full control. At the H-Scribe system you must create the file **c:\usr\WebUploadPath.txt**. This file must contain a mapped or UNC path to the shared Data Storage Directory (see Section 7.1.4 using the example named UploadedData) on the web server.

### 9.2 H-Scribe Version 5.xx

The following configuration must be performed to allow an H-Scribe system with version 5 or later software to access and acquire uploaded Holter recordings.

1. The Windows user with IT Administrator permissions running H-Scribe must have read/write access to the Web server directories. Select the **System Configuration** icon and then **WU/Surv Folders** button to enter the Web Upload path.



2. Select the Path field and select **Browse** to navigate to the appropriate directory, or enter the path manually. Click **Add** to include the path for the selected group.
3. The Web upload data path can be removed by highlighting the path and selecting **Delete**.
4. The Web upload path can be authenticated using **Validate**. When the path is not valid a red exclamation mark is displayed next to the path field.
5. Select the **Save Changes** button before exiting this window.

### 9.3 Hypertension Diagnostic Suite (HDS)

The following configuration must be performed to allow a Hypertension Diagnostic Suite (HDS) system at version 2.60 software or later to access and acquire uploaded ambulatory blood pressure (ABP) recordings.

1. Configure the HDS Import Base directory
2. Run HDS.
  - Double-click the **Hypertension Diagnostics Suite** program icon on the computer desktop. Or,
  - From the Windows Start menu, select **Programs → Mortara Instrument Inc → Hypertension Diagnostics Suite**.
3. Click the Software Configuration button in the lower right corner of the HDS main screen.

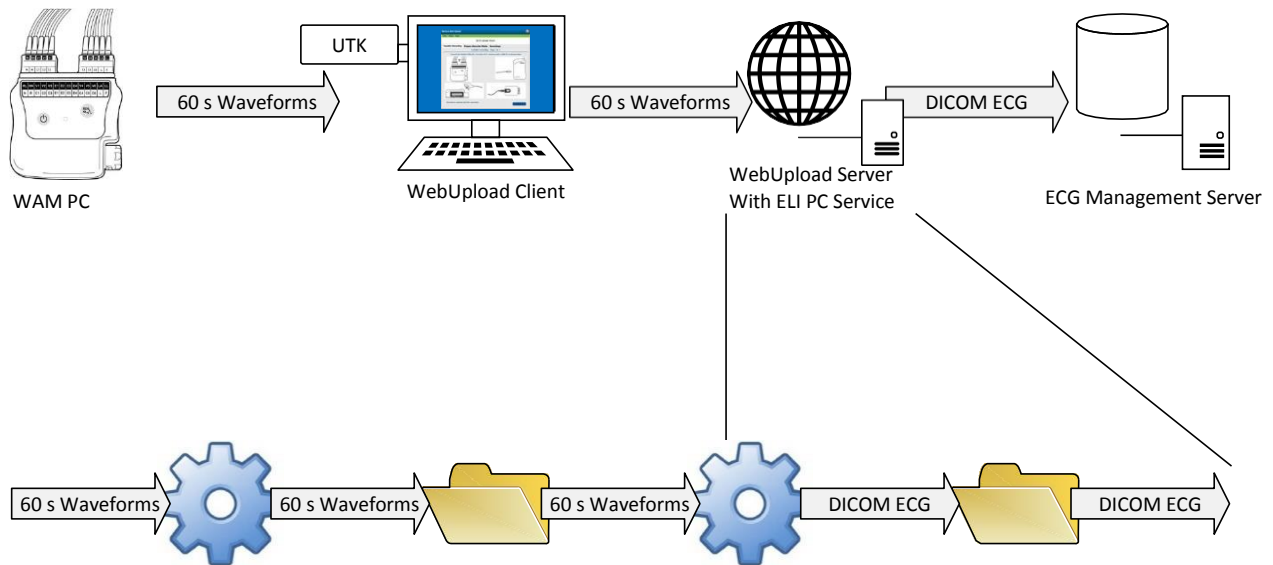


4. On the left side of the Software Configuration screen, choose System Properties.
5. On the right side of the Software Configuration screen, note the Import Base directory box. Click the Browse button in this box. In the displayed prompt, navigate to the directory selected during Welch Allyn Web Upload 3 installation as the server data storage location, and choose the UploadedData subdirectory.
6. Click OK.

HDS is now configured to find data received by the Welch Allyn Web Upload server via its Import Preview selection. The HDS Import Preview window is available in the Browse Database view, by right-clicking a patient folder, or in the File menu when a patient folder is selected.

## 9.4 ELI PC Service

ELI PC Service (v1.0.0) runs in the background and continually scans an input folder tree for new WAM PC recordings. When it finds a new recording, it automatically converts it to a 10-second resting ECG. It exports the ECG as a DICOM 12-lead ECG Waveform file into the output folder and then deletes the original recording. ELI PC Service's Input Directory is configured to be the same as WebUpload's Storage Directory. Follow the installation and configuration instructions in the ELI PC Service administrator manual. Below is a diagram showing where ELI PC Service fits into WebUpload's overall dataflow.





## Appendix A: Configuring Silent Installs

---

This is a sample WebUploadInstallConfig.xml file that is used to initialize the configuration of the client application when installed with the silent installer. Most of the settings are optional and commented out. There are however, two settings that absolutely must be entered in order for the client to find the server and data.

DirectoryPath – This is the path of the folder on the client where the data and settings are stored.

DataWebServices – This is the URL of the server that the client uses to upload and download data.

```
<?xml version="1.0" encoding="utf-8" ?>
<ConfigurationSettings>
  <RegistrySettings>
    <!-- DirectoryPath: Required path to local data -->
    <DirectoryPath>c:\Web Upload Files for xxx.xxx.xxx.xxx upload\</DirectoryPath>
    <!-- UpdateLocation: Used by Click-Once installs, not used by stand-alone installer -->
    <!-- <UpdateLocation>http://xxx.xxx.xxx.xxx/upload/WebUploadApplication.application</UpdateLocation> -->
  </RegistrySettings>
  <ConfigInfo>
    <!-- UseMetricUnits: true or false -->
    <!-- <UseMetricUnits>false</UseMetricUnits> -->
    <!-- UseNetworkCredentials: true or false -->
    <!-- <UseNetworkCredentials>true</UseNetworkCredentials> -->
    <!-- UseSSL: true or false -->
    <!-- <UseSSL>true</UseSSL> -->
    <!-- CustomerName: site name -->
    <!-- <CustomerName>Site Name</CustomerName> -->
    <!-- AutoTransmit: true or false -->
    <!-- <AutoTransmit>true</AutoTransmit> -->
    <!-- AutoErase: true or false -->
    <!-- <AutoErase>true</AutoErase> -->
    <!-- Zip: true or false -->
    <!-- <Zip>true</Zip> -->
    <!-- DaysToDelete: number of days -->
    <!-- <DaysToDelete>7</DaysToDelete> -->
    <!-- ReferringPhysicians: list of physicians -->
    <!-- <ReferringPhysicians>
      <string>Physician 1</string>
      <string>Physician 2</string>
    </ReferringPhysicians> -->
    <!-- Symptoms: list of annotations -->
    <!-- <Symptoms>
      <string>Annotation 1</string>
      <string>Annotation 2</string>
    </Symptoms> -->
    <!-- Indications: list of indications -->
    <!-- <Indications> -->
      <!-- <string>Indication 1</string> -->
      <!-- <string>Indication 2</string> -->
    <!-- </Indications> -->
    <!-- Medications: list of medications -->
    <!-- <Medications> -->
      <!-- <string>Medication 1</string> -->
      <!-- <string>Medication 2</string> -->
    <!-- </Medications> -->
    <!-- HookUpTechs: list of technicians -->
    <!-- <HookUpTechs> -->
      <!-- <string>Technician 1</string> -->
      <!-- <string>Technician 2</string> -->
    <!-- </HookUpTechs> -->
    <!-- OrdersDirectory: Local path to orders -->
    <!-- <OrdersDirectory>c:\Web Upload Files for xxx.xxx.xxx.xxx upload\Orders\</OrdersDirectory> -->
    <!-- AutoURL: must be false to use DataWebServices URL -->
    <AutoURL>false</AutoURL>
    <!-- DataWebServices: Required URL of the upload service -->
    <DataWebServices>http://xxx.xxx.xxx.xxx/upload/DataWS/DataServices.asmx</DataWebServices>
  </ConfigInfo>
</ConfigurationSettings>
```