eServer

SETUP AND SITE INSTALLATION INSTRUCTIONS

INNOTECH®

Proprietary

Trademark

The term ‘Innotech’ used in this manual is a trademark of Mass Electronics Pty Ltd trading as Innotech Control Systems Australia.

'Microsoft' and 'Windows' are registered trademarks of the Microsoft Corporation in the United States and other countries.

Disclaimer

While great efforts have been made to assure the accuracy and clarity of this document, Mass Electronics Pty Ltd assumes no liability resulting from any omissions in this document, or from misuse of the information obtained herein. The information in this document has been carefully checked and is believed to be entirely reliable with all of the necessary information included. Mass Electronics Pty Ltd reserves the right to make changes to any products described herein to improve reliability, function and design, and reserves the right to revise this document and make changes from time to time in content hereof with no obligation to notify any persons of revisions or changes. Mass Electronics Pty Ltd does not assume any liability arising out of the application or any use of any product or circuit described herein; neither does it convey licence under its patent rights or the rights of others.

Document Management

Document Title: eServer Setup & Site Installation Instructions

Revision History

Version Number	Date	Summary of Changes
1.0	2009	Draft release of document, for comment.
2.0	July 2009	Full Release.
3.0	December 2010	Updates to guide for changed eServer Setup workflow. Addition of information for the use of eServer with SQL Server 2008 R2 Express Edition databases. Added relevant setup information for eServer on a Windows Server 2008 R2 computer.
4.0	December 2011	Updated draft document including changes in setup due to new release of eServer. Added General Troubleshooting Tips section.
5.0	January 2014	Contact Details update, Style update, Internet Explorer 10 and 11 compatibility troubleshooting added, other minor information added and errors fixed.
6.0	May 2016	Supported operating systems updated. Added IIS installation and configuration information for Windows 8.1/10 & Server 2012.
7.0	May 2018	Added https information for the IIS Manager. Added information about Automatic Restarting of eServer. Removed MIME Type information. Minor edits.

This page has been left intentionally blank.

Contents

Contents (Continued)

Configuring Internet Information Services (IIS)

Configuring eServer Communications

Contents (Continued)

List of Illustrations

List of Illustrations (Continued)

List of Illustrations (Continued)

List of Illustrations (Continued)

List of Tables

eServer

SETUP AND SITE INSTALLATION INSTRUCTIONS

1 Preliminary Information

INNOTECH®

1-1 Introduction

This manual is intended to provide the customer with complete and comprehensive documentation to set up and configure the Innotech eServer software for a site computer. eServer enables local and remote client computers access to a Magellan Explorer interface from within their web browser, enabling direct access to information on the site computer.

Although the intent of this manual is to simplify the installation task, instructions contained in this manual are based on the assumption that the typical installer is familiar with the operation of the Microsoft Windows 7 or 10 Professional or Windows Server 2008/2012 R2 operating systems.

Customers should familiarise themselves with the content of this manual before attempting installation and setup of eServer on their computer.

Throughout this manual there are icons to illustrate general notes and important notes, as illustrated below:

These notices indicate a piece of useful information which should be read.

IMPORTANT

*These notices contain information about the software that **must be done** before proceeding further to ensure success.*

1-1.1 Systems Covered by this Manual

The manual covers the preparation and configuration of a remote computer to access and display a Magellan Explorer interface from within a web browser, while accessing information on a remote computer. This is facilitated through the Innotech eServer software when using an Microsoft Internet Explorer web browser.

1-1.2 Terminology used in this Manual

In order to simplify the instructions, common terminology and references to other Innotech products are used throughout this manual. A brief description of some of the terminology is provided in this section.

eServer Client computer: any computer which is connecting to the eServer Host computer. In common scenarios, an eServer Client computer will be a laptop computer, a computer on the site's local area network or an external computer connecting to the eServer Host computer via a secure Internet connection. The eServer Client computer requires both a supported Windows operating system and Internet Explorer software.

eServer Host computer: the computer which is running the Innotech eServer software and has the Magellan project loaded. In common scenarios, this will be a computer on site, and accessible from computers on the local area network and computers on external networks if required. The eServer Host computer requires a supported Windows operating system.

DNS: Domain Name System, a naming system for computers, services or any resources on a private network.

eServer: a web-based Magellan Explorer solution that allows a remote computer to display a Magellan Explorer interface from within their web browser while accessing information on a remote computer.

iComm: Innotech's communications server used by applications software.

IIS: Microsoft Internet Information Services software. This software enables your eServer Host computer running capability to interact securely with connecting eServer Client computers.

IP address: a numerical label that is assigned to any device participating in a computer network that uses the Internet Protocol for communication between its nodes.

Magellan Builder: an event driven, object oriented real-time Supervisory Control and Data Acquisition package. Magellan Builder is used to create or modify a Magellan Project, which is run by Magellan Explorer or eServer software.

1-1.3 Scope of this Technical Manual

This technical manual contains:

Table 1-1: Document Chapters

Chapter Number	Chapter Name	Description
1	Preliminary Information	Contains initialisation related information of a general nature such as computer requirements and pre-installation materials.
2	Installation of eServer Software	Contains instructions for the installation and basic configuration of the eServer software onto a computer, and installation of the additional ATOM Reports Component if required.
3	Configuring Internet Information Services (IIS)	Contains instructions for configuring IIS on supported Windows operating systems.
4	Configuring eServer Communications	Contains instructions for the configuration of security and access control on eServer software. Additionally, steps are provided to enable eServer to communicate with an SQL Server database.
5	General Troubleshooting Tips	Contains instructions for troubleshooting and resolving general issues that may arise during the installation and configuration of eServer software.

1-2 System Requirements

Both the eServer Host computer and any connecting eServer Client computers must meet the minimum computer requirements to ensure correct operation.

1-2.1 Minimum Computer Requirements

Supported Operating Systems:

- Windows® Server 2012 R2
- Windows® Server 2008 R2 with Service Pack 1
- Windows® 10 Professional 64-bit & 32-bit
- Windows® 7 Professional 64-bit & 32-bit with Service Pack 1

Minimum System Requirements:

- Intel Pentium Dual-Core 2.8GHz processor or equivalent
- 4GB of RAM
- 350MB Hard Disk Drive required
- 1024 x 768 display with 16-bit video card (1920 x 1080 recommended)
- CD-ROM or DVD-Drive
- Keyboard and mouse of compatible pointing device
- Requires a computer with iComm installed

1-3 Special Considerations

The following installation considerations must be observed to ensure the proper installation and configuration of eServer, Magellan Web-Based graphics, ATOM Reports Component and Internet Information Services. The eServer software allows ten concurrent connections to the Magellan project, and the following items are required for proper operation:

- eServer v1.50 or greater installation package and required security dongle
- Magellan Builder v1.50 or greater installation package and the appropriate security dongle for installation. Magellan Builder is required for site setup only.
- Completed Magellan project
- Windows Internet Information Services (IIS) must be installed on the computer running the eServer software according to the operating system. This is enabled on Windows 7 & 10 from the Windows Features Setup. For Windows Server 2008/2012 R2, IIS is an additional configuration option.
- A static IP address from the ISP and proper Firewall / Router configuration if using internet access

1-4 Advanced Site Considerations

The following installation considerations must be observed for sites with advanced data logging requirements, such as connection to an SQL Server database:

- Both the eServer Host computer and any connecting eServer Client computers must meet the minimum computer requirements to ensure correct operation. Depending on the site requirements, more advanced computer specifications may be required for the eServer Host computer, such as RAID-based redundancy systems, and a higher-end computer processor. Refer to 1-2 - System Requirements for more information.
- Consult with the site IT Manager to ensure that connecting eServer Client computers can access the eSever Host computer and the SQL Server database in a safe and secure way.
- Be aware that installing SQL Server 2008/2016 R2 Standard Edition may take up to 60 minutes to complete. SQL Server Express 2008 R2 can take up to 20 minutes.

1-5 Installation Plans

The following installation data should be gathered and made available to the installation team in the event that a connection to an SQL Server is required:

- This technical manual.
- Ensure you are logged into the computer as a System Administrator when installing software and commissioning the eServer Host and eServer Client computers
- Site Information Technology security and installation requirements
- Magellan Builder security dongle to configure project settings. Magellan Builder is required for site setup and project modifications only. You may remove the dongle once the site is commissioned.
- eServer security dongle for the eServer Host computer. This must remain connected to the eServer Host computer in order for eServer to run.
- For the setup of eServer Client computers that require access to eServer generated Crystal Reports, you may choose to download the Crystal Reports for Web Components package from the Innotech website and install it manually as it is a 100MB file download.
- DNS name or static IP address of the SQL Server computer.
- Name of the SQL Server Database being used for point logging.
- Any other data source as it becomes known

1-5.1 Required Software on Site Computer

The following software needs to be installed on the site computer.

- Magellan Builder v1.50 or greater with security dongle. You may remove the Magellan Builder security dongle once setup is completed.
- eServer v1.50 or greater with security dongle. The eServer security dongle must remain connected to the eServer Host computer in order for eServer to run.
- ATOM Reports Component
- iComm Communication Server
- Windows Internet Information Services (IIS)

The eServer software may be used on an intranet (internal Ethernet), externally via the internet or both.

This page has been left intentionally blank.

eServer

SETUP AND SITE INSTALLATION INSTRUCTIONS

2 Installation and Configuration of eServer Software

INNOTECH®

2-1 Overview

This section provides an overview of the steps required for the installation and basic configuration of the eServer software onto a computer, and installation of the additional Magellan Crystal Report additions if required.

*The installation program for eServer v1.50 or greater **automatically** creates and configures the necessary web page files on your computer in the location c:\MyWebPages. Once eServer and the ATOM Reports Component (if required) have been installed, you will have to check the security settings for c:\MyWebPages and your computer's Internet Information Services Settings.*

See the following for more information:

- *2-5 Security Access to the c:\MyWebPages Directory*
- *Chapter 3 - Configuring Internet Information Services (IIS)*

2-2 Pre-installation Tasks

2-2.1 Overview

Prior to installing eServer v1.50 or greater there are a series of pre-installation tasks to undertake. This includes gathering all the required information to make the installation process easier, and preparing site computer security settings to facilitate an easy setup process.

IMPORTANT

Many of the processes within the Pre-installation Tasks assume a moderate to high degree of technical IT expertise. It is recommended to consult with the site IT Manager for assistance and site specific security settings where required.

2-2.2 Remote Access, Ports and Security Information

2-2.2.1 Internet Access

You may use an existing and available Broadband Cable/ADSL Internet Connection, however in this scenario the site will need to have a **DNS name or static IP address setup through the Internet Service Provider (ISP)**, and also allow the opening of Ports through their Firewall / Router.

*If the site IT Staff deny the setup of required ports, a separate ADSL internet connection will need to be provided to a dedicated computer. This computer can be configured with a **Static External IP address** and configured to have **Port Forwarding**. In this instance, IT Staff will only need to enable Port 80 for internet connection and accept outgoing connections on 443, 20000 and 20001, not incoming through their own Firewalls. Regardless, the computer running eServer and iComm needs to have the full incoming and outgoing connections to the Ports setup.*

2-2.2.2 Port Forwarding and Firewalls

The following Ports are required to be opened through the Firewall to allow incoming and outgoing connections to specific parts of the Innotech System.

Table 2-1: Required Ports for an Innotech System

Required Ports	Usage
Port 443	Secure Communications Port (HTTPS)
Port 20000	Innotech Communications Server (iComm)
Port 20001	Secure Communications Port (eServer)
Recommended Additional Ports [1]	
Port 5900	For VNC (Virtual Network Computing)
Port 21	For FTP (File Transfer Protocol)
Port 1723	For VPN (Virtual Private Network)
Optional Ports	**Usage**
Port 8227, 8228, 8230 [2]	Innotech Chronicle Manager remote communications with the Chronicle Server (if required)
Port 3389 [3]	For Remote Desktop (mstsc)

[1] Enabling VNC, FTP or VPN assists with remote site access to the computer for management and file transfers. This is optional but highly recommended as it allows remote diagnostics, analysis and troubleshooting of site problems if they occur.

[2] Enabling Ports 8227, 8228 and 8230 is only necessary for remote access using Chronicle Manager to configure the site Chronicle Server.

[3] The HASP security dongles used by eServer and Magellan do not fully support Remote Desktop. You will not be able to launch eServer or Magellan through Remote Desktop.

At a minimum ensure to enable the Required Ports as listed above.

2-2.2.3 Security Information

Both iComm and eServer are resistant to denial of service attacks from unauthenticated clients, and both support 32-bit encryption with initial login challenge/response authentication. If a client's login name and password is not authenticated immediately by eServer or iComm, the connection is terminated.

Both servers have been tested for buffer overrun attacks, and both servers have an audit trail of connection attempts. It is not possible, even with a custom-written rogue program that manages proper authentication, for any program to connect to either of these servers and execute a file or download unauthorised data from the server. Neither of these programs currently contains functionality to allow file downloads, server-side execution, or any kind of interactive login.

To setup access over the internet, you will need to open 443, 20000 and 20001 through the Firewall to transmit and receive data. Then accept incoming connections, and Port Forward from the external static IP address, to the internal static IP address of the computer running the iComm Server and eServer software. You will be able to see who has logged in via the audit trails, even from an eServer Client computer.

From the eServer Client computer, only ports 443, 20000 and 20001 need to be open for an outgoing connection.

2-2.3 Setup of a Dedicated Site Computer with ADSL Connection

2-2.3.1 Overview

This section provides detailed information for configuring a site computer with a dedicated ADSL connection for running the eServer software. Refer to Figure 2-1 for an example eServer setup network topology.

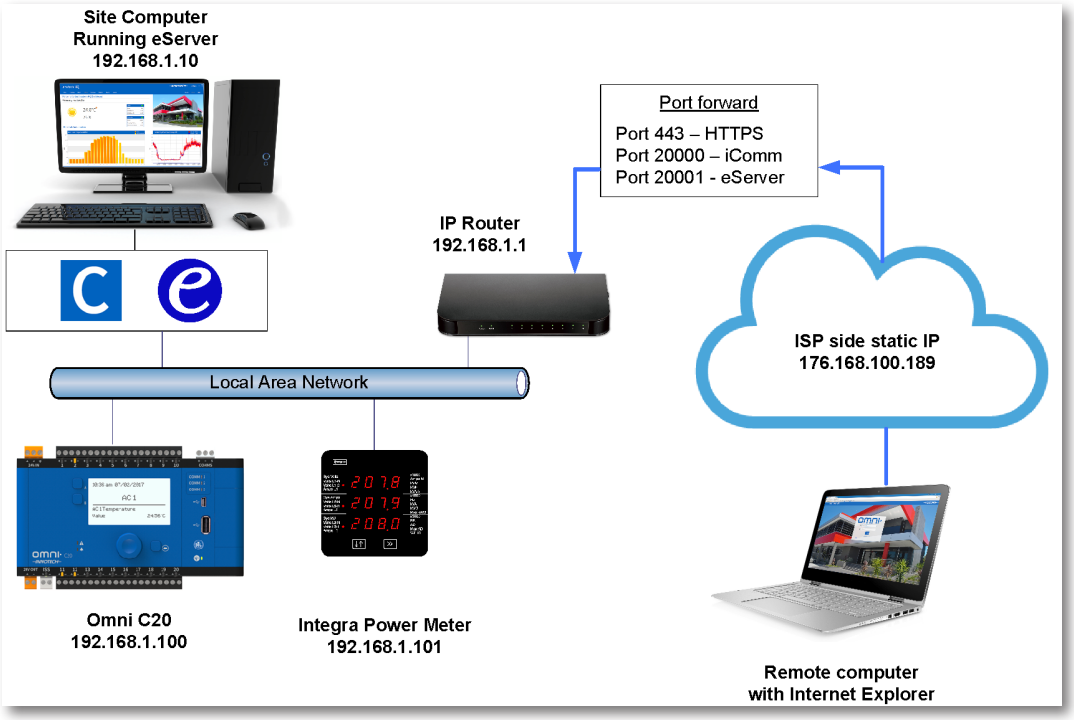

Figure 2-1: Example of eServer Setup Network Topology

2-2.3.2 Computer Setup

Once the ADSL connection to the eServer Host computer is completed, the computer must be protected. The following is required to complete this step:

- Antivirus software from a reputable provider. Some antivirus and security software will block eServer communication and port traffic by default. If this occurs, allow the required communications on the computer. Refer to the specific antivirus or security software help manual for more details on how to do this.
- Firewall enabled and configured - either Windows firewall or third party software. Ensure to enable the required ports for eServer communications.
- Administration rights on the computer with a valid username and password
- Static IP address for the ADSL connection
- Static IP address on the local computer

2-2.3.3 Router Setup

1. Set up the computer with a temporary IP address and make it the same as the default IP range of the ADSL router being used.
2. Log onto the router and set a new username and password. Go to the Port Settings (generally found in Security) and allow the ports described previously in 2-2.2.2 Port Forwarding and Firewalls.
3. You will need to forward the requests for each Port to the static IP address of the computer running iComm and/or eServer as shown below in Figure 2-2 (Please note that this screenshot is for software that is specific to this router, and may vary depending on the brand and model of the router).

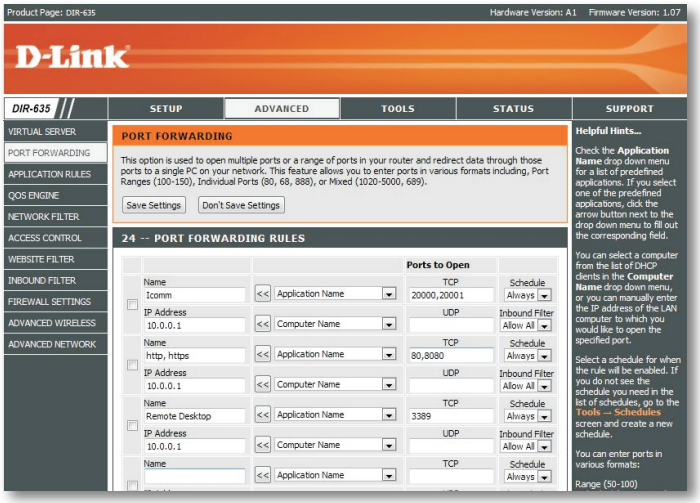

Figure 2-2: Example of Forwarding Requests for Ports to Static Ip Addresses

2-2.4 Domain Name System (DNS) Setup

To use eServer with an SQL Server on the dedicated site computer and remotely you will both need internal and external access to iComm. To do this, you will need to use an actual DNS name that is accessible from the External and Internal Addresses. In most projects with stand-alone computers accessing the internet the router is basic and is not a DNS server.

Use the following site to set one up.

Go to http://dyn.com and create a DNS account (these are not expensive and are very reliable).
Eg: sitename.dyndns.org

Download the Dynamic DNS Updater and install it on your Site computer. This will ensure the External Address is always linked to the DNS name.

2-3 Installation of eServer Software

2-3.1 Overview

The installation program for eServer v1.50 or greater automatically installs all web page files on your computer to work with minimal user intervention.

The following steps describe the process to install the eServer software onto a site eServer Host computer.

IMPORTANT

Ensure that the eServer Host computer meets the minimum specifications outlined in 1-2 System Requirements before installing the eServer software. Ensure that you have configured and DNS and Port Security settings prior to installation, as during installation you will be asked to enter this information.

There are common installation steps for all supported Operating Systems. Any specific differences are described at the relevant section in the document.

2-3.2 Installation Steps

Launch the eServer Installation Program. From the Setup window, select Next to commence installation, as illustrated below in Figure 2-3.

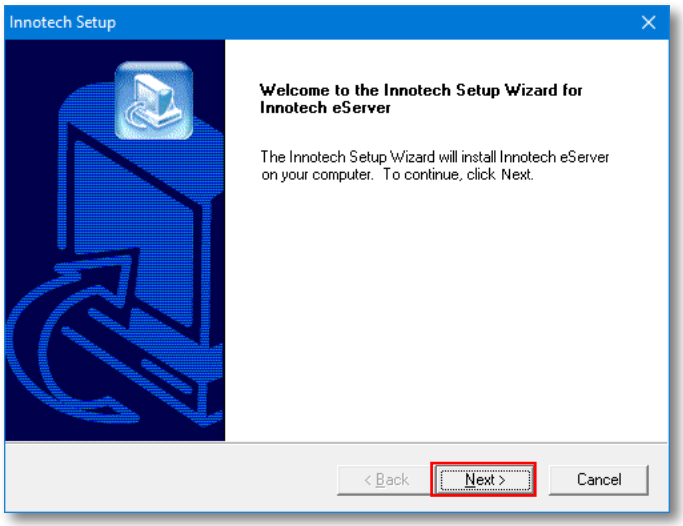

Figure 2-3: Commence Installation of the eServer Software

Read and acknowledge the eServer **Software Licence Agreement,** as illustrated below in Figure 2-4. Click **Yes** to continue.

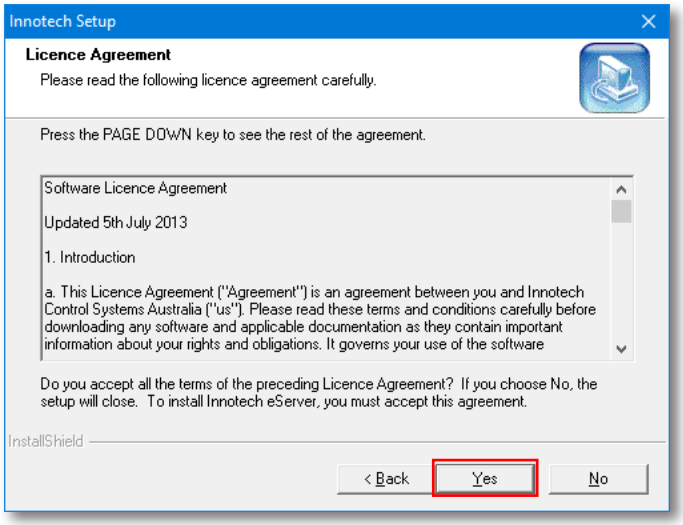

Figure 2-4: eServer Software Licence Agreement

Enter the **Customer Information** for your eServer software installation, as illustrated below in Figure 2-5. Click **Next** to continue.

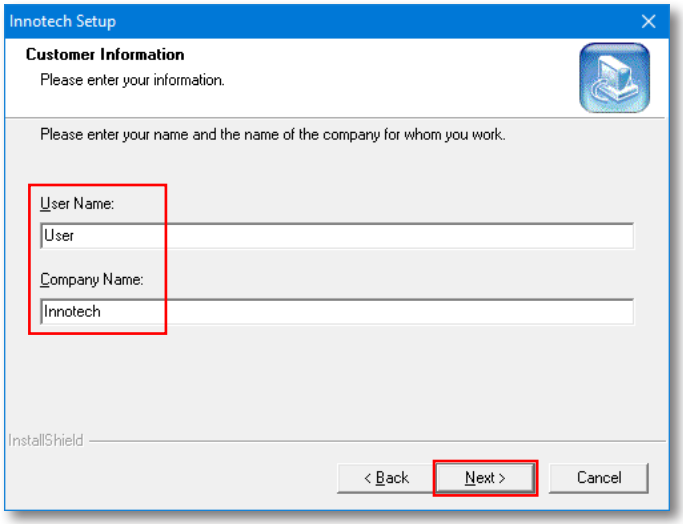

Figure 2-5: eServer Software Customer Information

Confirm the eServer software **installation location**, as illustrated below in Figure 2-6. Click **Next** to continue.

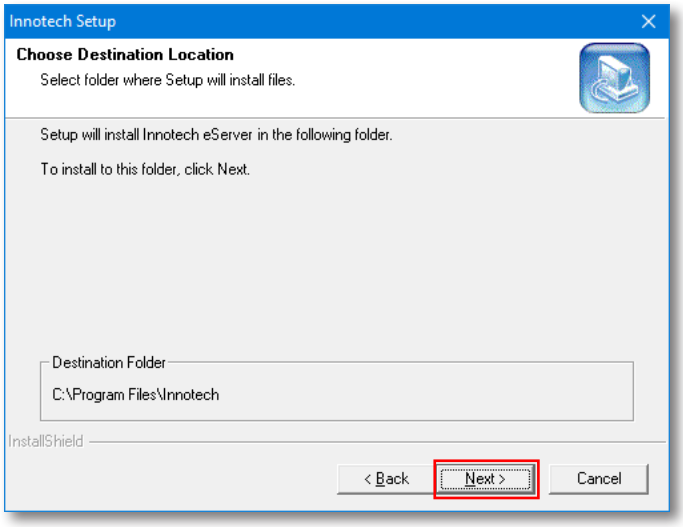

Figure 2-6: eServer Software Installation Location

Wait wait a few minutes as the eServer software is installed on your computer, as illustrated below in Figure 2-7.

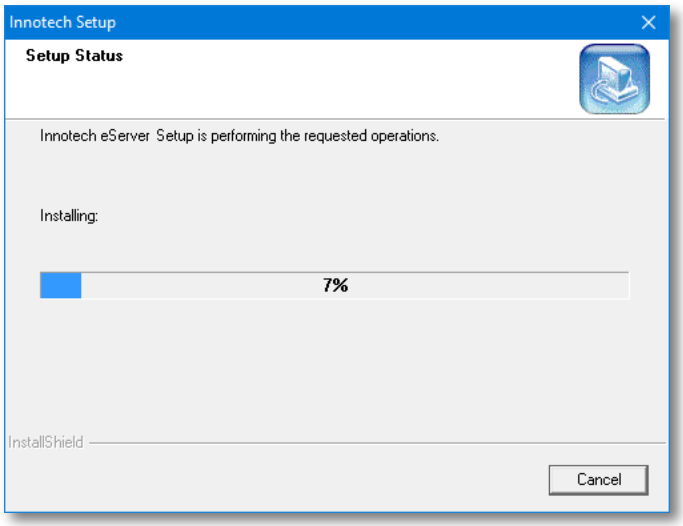

Figure 2-7: eServer Software File Installation

When the eServer software installation process is completed, click **Finish** to close and exit.

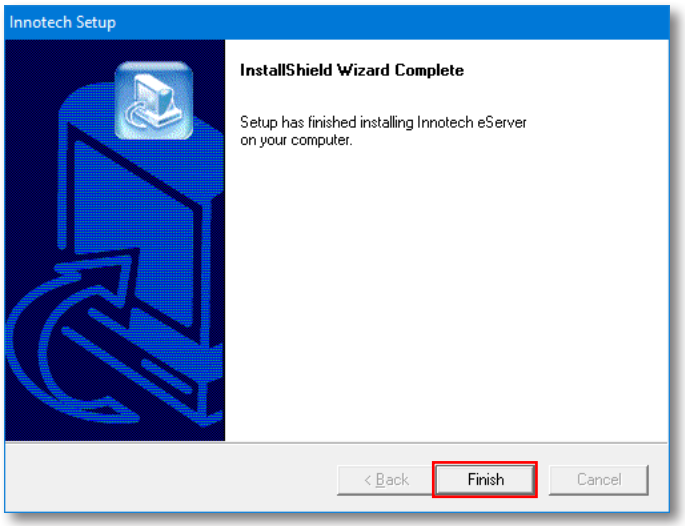

Figure 2-8: eServer Software File Installation Finished

2-4 Installation of ATOM Reports Component

2-4.1 Overview

The ATOM Reports Component allows for advanced report generation from Magellan or eServer software using the Innotech ATOM software. This is a separate optional install which is required for the generation of ATOM Reports.

*The ATOM Reports Component is intended to work in a system where the Magellan or eServer Software is accessing data stored in a **SQL Server database**. This is part of a system utilising the **Innotech ATOM software**.*

See the following for more information:
- *Chapter 4 - Configuring eServer Communications*

2-4.2 Installation Steps

Launch the ATOM Reports Component Installation Program. The program will detect your system configuration to install the required files, as illustrated below in Figure 2-9.

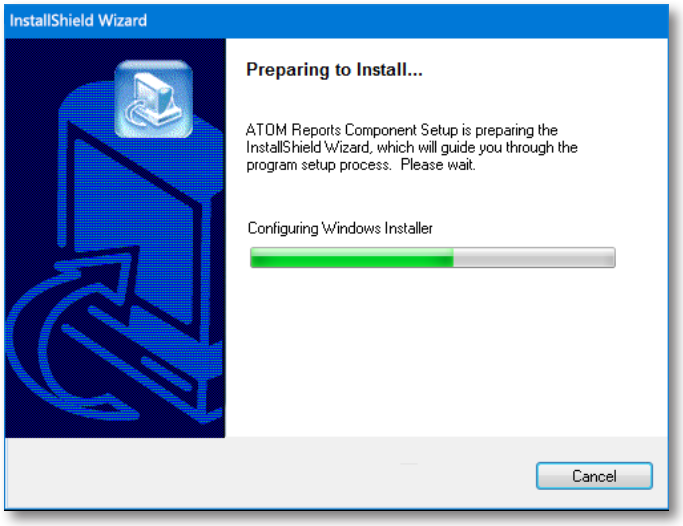

Figure 2-9: ATOM Reports Component Installation Preparation

Click **Next** to commence installation, as illustrated below in Figure 2-10.

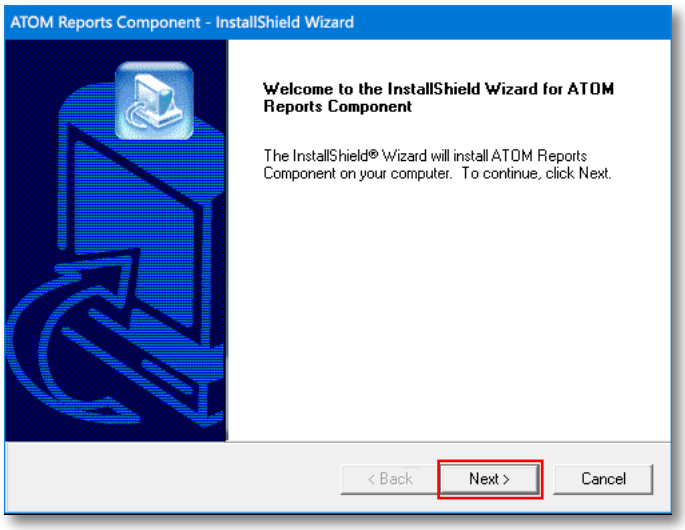

Figure 2-10: Commence ATOM Reports Component Installation

Select the specific ATOM Reports Component items to install. The **default is to install the files required for both the Magellan and eServer software**, as illustrated below in Figure 2-11. Click **Next** to continue.

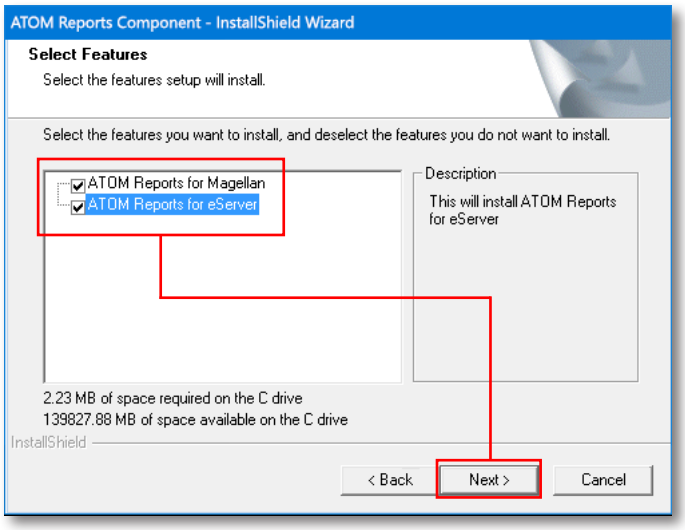

Figure 2-11: Select the Specific ATOM Reports Components to Install

When the ATOM Reports Component installation process is completed, click **Finish** to close and exit.

2-5 Security Access to the c:\MyWebPages Directory

2-5.1 Overview

To enable eServer Client computers connection and access to the contents of the c:\MyWebPages directory, you will need to configure folder security settings. This allows eServer Client computers to access to necessary files of the eServer project.

*You will need to enable security access to a user called "**Everyone**", and then customise the security settings for "Everyone". If the user "Everyone" already exists for this directory, check that the suitable security and access settings have been enabled for this directory.*

2-5.2 Create Special User "Everyone" for c:\MyWebPages

Navigate to **c:\MyWebPages** on your computer. Right-click on the MyWebPages folder and select **Properties** from the popup menu. Select the **Security** tab and click **Edit** to change permissions, as illustrated below in Figure 2-12.

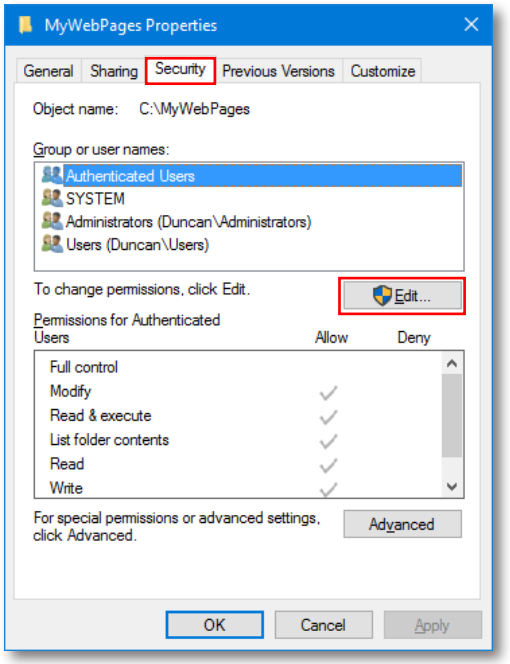

Figure 2-12: Edit Security Groups for c:\MyWebPages

Click **Add** to create the new Security Group "Everyone", as illustrated below in Figure 2-13

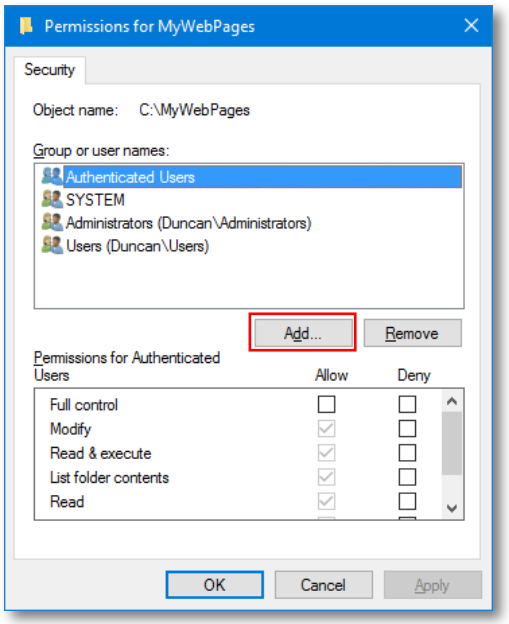

Figure 2-13: Add the new Security Group "Everyone"

Type **Everyone** into the Object Name field and click OK to apply, as illustrated below in Figure 2-14.

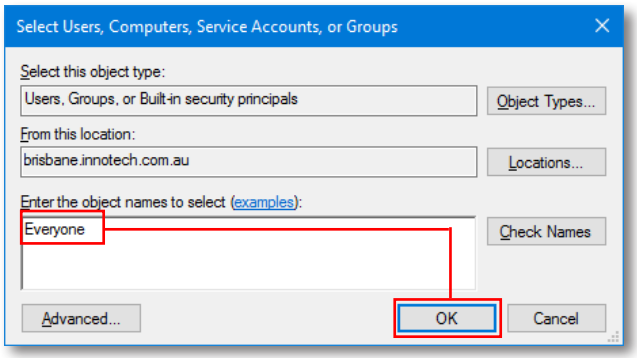

Figure 2-14: Enter the new Security Group "Everyone"

Click **OK** to close the Security Properties settings for c:\MyWebPages, exiting to the main window.

2-5.3 Configure Security Settings for Special User "Everyone"

Navigate to **c:\MyWebPages** on your computer. Right-click on the MyWebPages folder and select **Properties** from the popup menu. Select the **Security** tab. Ensure that the user "Everyone" is present in the Groups and User Names list. Click **Edit** to configure properties for Security Group "Everyone", as illustrated below in Figure 2-15.

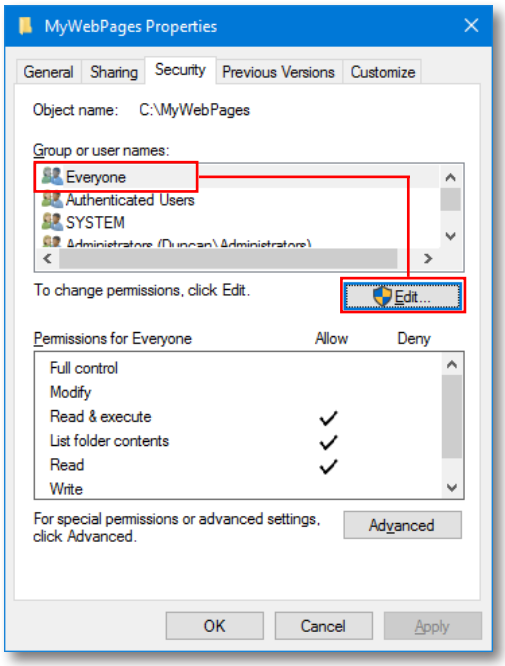

Figure 2-15: Edit properties for Security Group "Everyone"

Select **Everyone** in the Groups or User Names List. In the Permissions List, ensure that **Full Control** is enabled, as illustrated below in Figure 2-16. Click **OK** to return to the previous window.

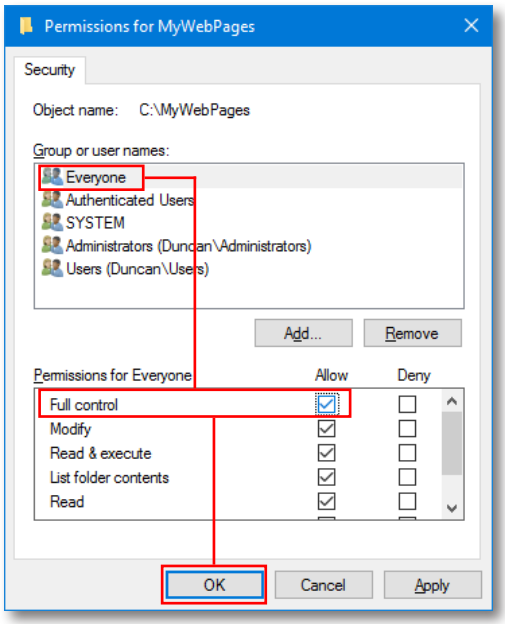

Figure 2-16: Select Full Control for Security Group "Everyone"

With Full Control Enabled for "Everyone", click Advanced to configure Special Permissions for Security Group "Everyone", as illustrated below in Figure 2-17.

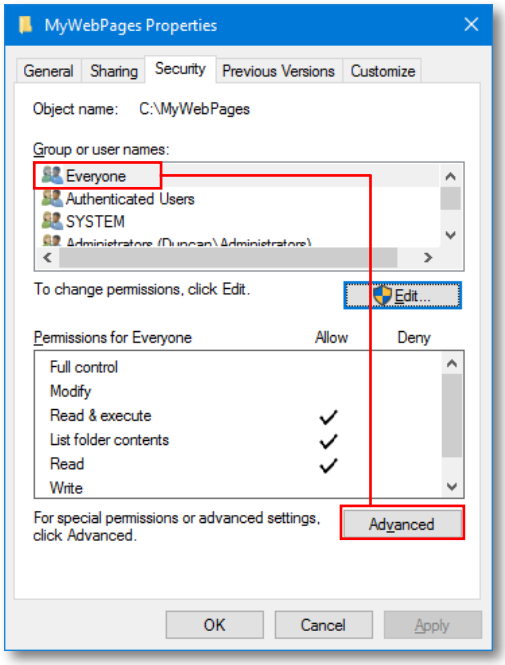

Figure 2-17: Open Advanced Security Settings for Security Group "Everyone"

Select **Everyone** into the Object Name field and click **Change Permissions...**, as illustrated below in Figure 2-18.

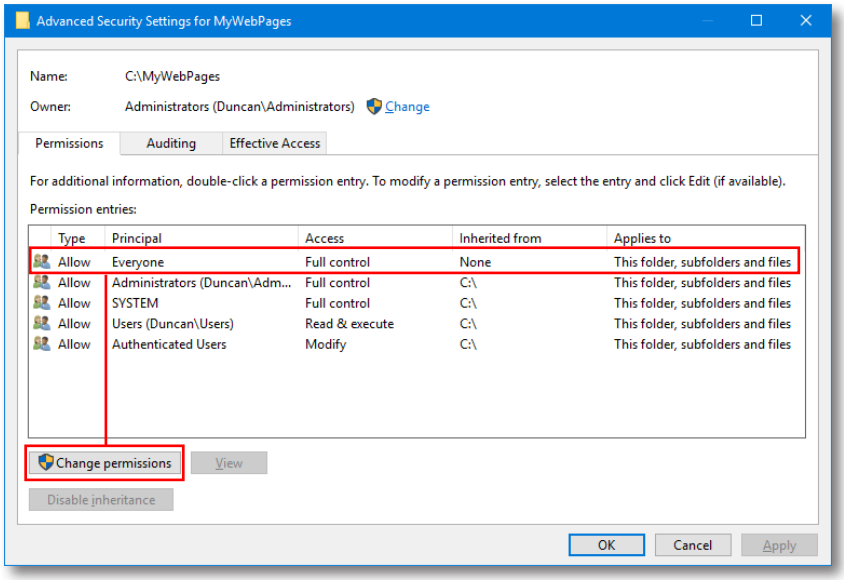

Figure 2-18: Edit Advanced Security Settings for Security Group "Everyone"

Ensure that the security option for the "Everyone" Security Group are selected, as illustrated below in Figure 2-19. Click **OK** to confirm your settings.

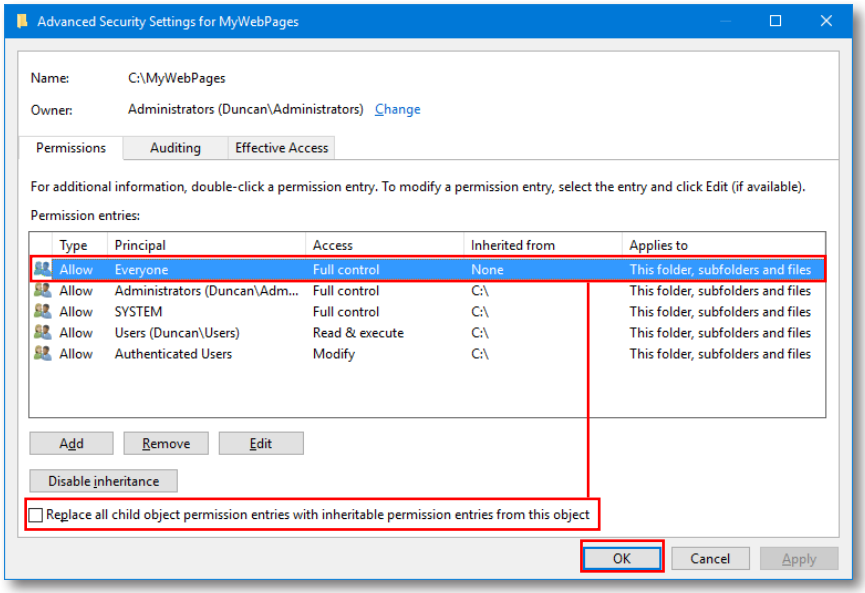

Figure 2-19: Set Advanced Security Settings for Security Group "Everyone"

Changing security settings for "Everyone" will launch a Windows Security warning. Click **Yes** to confirm the security settings for the "Everyone" Security Group, as illustrated below in Figure 2-20.

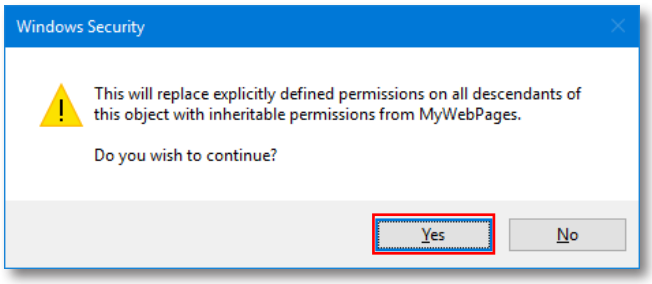

Figure 2-20: Confirm Advanced Security Settings for Security Group "Everyone"

Click **OK** to exit all the way out of the c:\MyWebPages Properties Window.

eServer

SETUP AND SITE INSTALLATION INSTRUCTIONS

3 Configuring Internet Information Services (IIS)

INNOTECH®

3-1 Overview

This section provides an overview of the steps required to install and configure Windows Internet Information Services (IIS) settings.

*IIS enables your **eServer Host computer** (the computer running the eServer software) the capability to interact securely with connecting eServer Client computers. IIS is not enabled by default on a fresh install of Windows.*

3-2 Installing Internet Information Services (IIS)

3-2.1 Overview

This section provides an overview of the steps required to install Windows Internet Information Services (IIS) on supported operating systems. If the computer already has IIS Installed, you may skip this section.

*IIS enables your eServer Host computer the capability to interact securely with connecting eServer Client computers. Once IIS has been installed, **you will need to configure it** to correctly to enable eServer to operate.*

3-2.2 Installing IIS on Windows Server 2008 R2

These instructions detail the process for installing IIS on a Windows Server 2008 R2 (SP1) computer. For a computer with a fresh install of Windows Server 2008 R2, there will be an interface presented on the screen to setup initial configuration options for your server computer.

It is recommended to have the server computer's initial configuration settings set by the site IT Manager.

Once your server computer's initial settings are correct, you can use the Initial Configuration Tasks window to commence setup of IIS functionality. Select **Add Roles** from the Customise this Server options, as illustrated below in Figure 3-1.

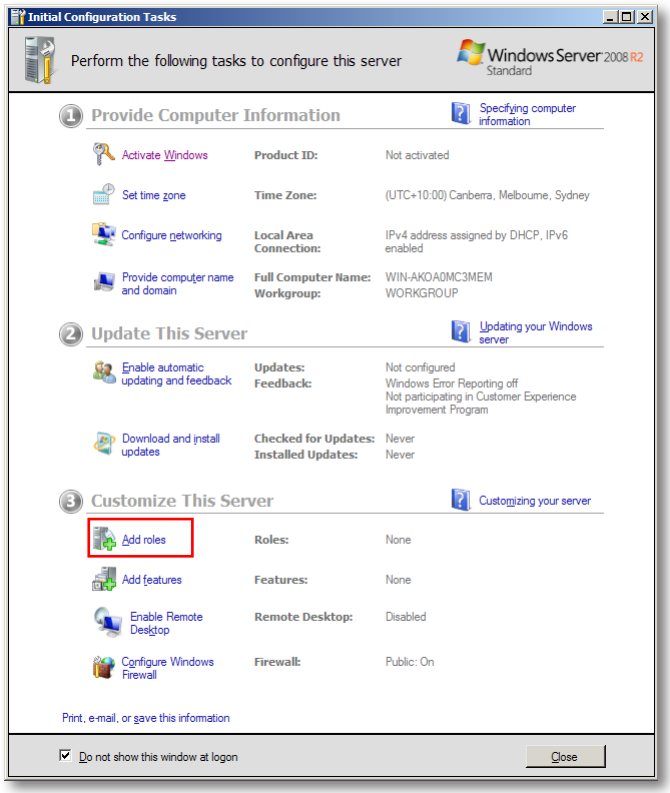

Figure 3-1: Initial Configuration Tasks on Windows Server 2008 R2

If your server computer has had the initial settings configured, and a restart has occurred, you can select to add the IIS role to the server through the Server Homepage window, which will appear on the desktop by default. Select **Roles** in the left menu, and click **Add Roles**, as illustrated below in Figure 3-2.

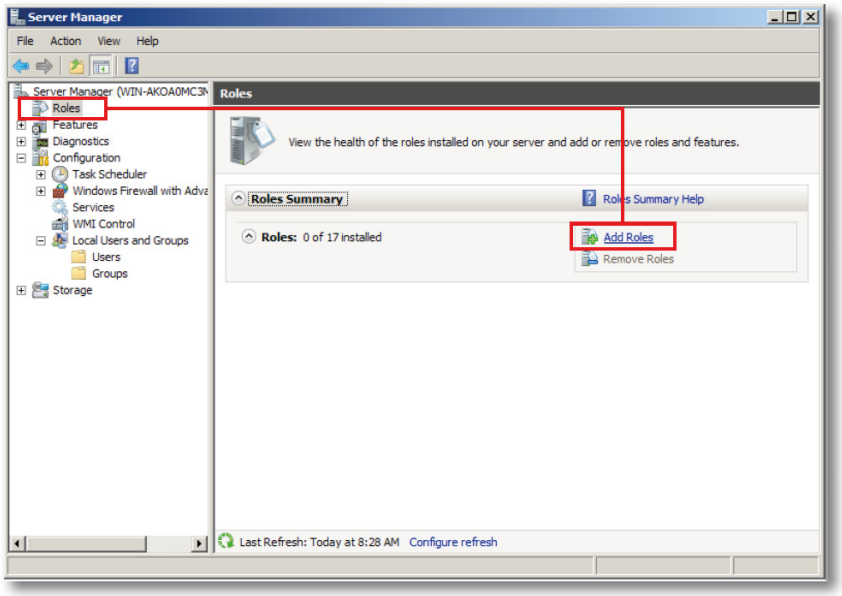

Figure 3-2: Server Manager Window on Windows Server 2008 R2

Check the initial information, and follow any steps which have been missed before you continue to setup IIS on the server computer. Once prepared, click **Next** to continue, as illustrated below in Figure 3-3.

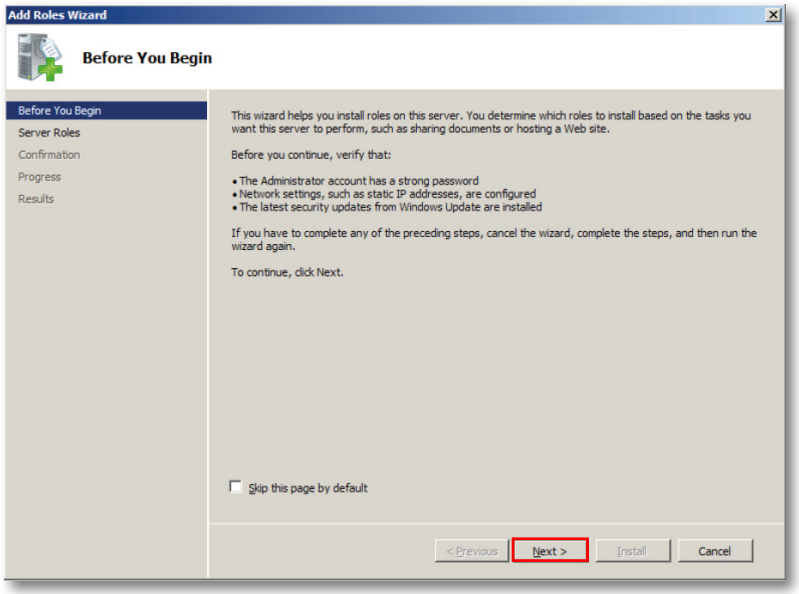

Figure 3-3: Confirm that initial setup of your server computer is correct

From the list of Server Roles, select Web Server (IIS) and click Next to continue, as illustrated below in Figure 3-4.

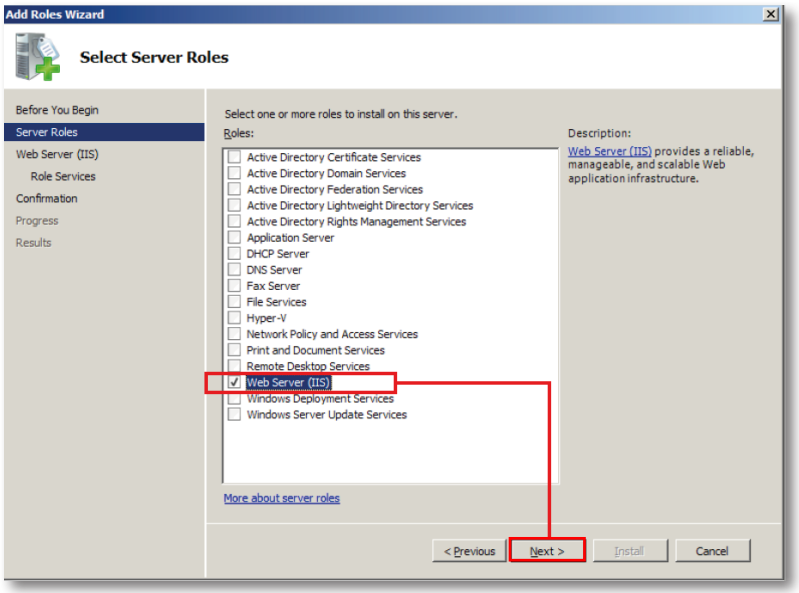

Figure 3-4: Select Web Server (IIS) from available Server Roles

Read through the Web Server (IIS) information. Click **Next** to continue, as illustrated below in Figure 3-5.

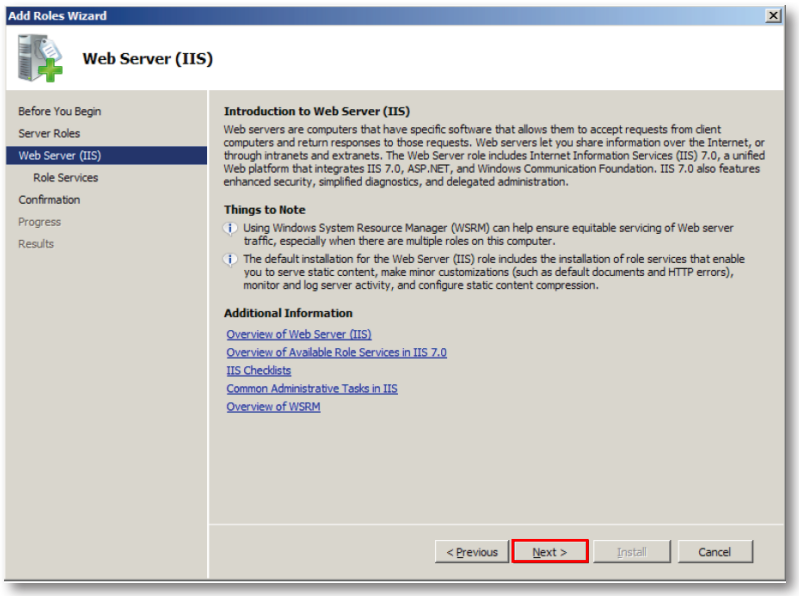

Figure 3-5: Read the Introduction to Web Server (IIS)

Scroll down the list of available options for IIS and select **Basic Authentication**, as illustrated below in Figure 3-6. Click **Next** to continue.

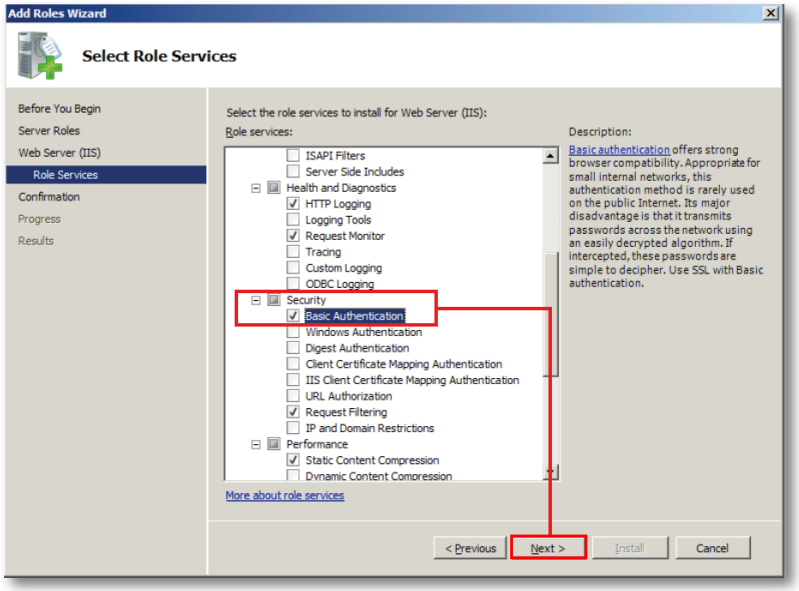

Figure 3-6: Setup IIS options for a Windows Server 2008 R2 computer

Confirm your installation settings. Click **Install** to commence setup of IIS, as illustrated below in Figure 3-7.

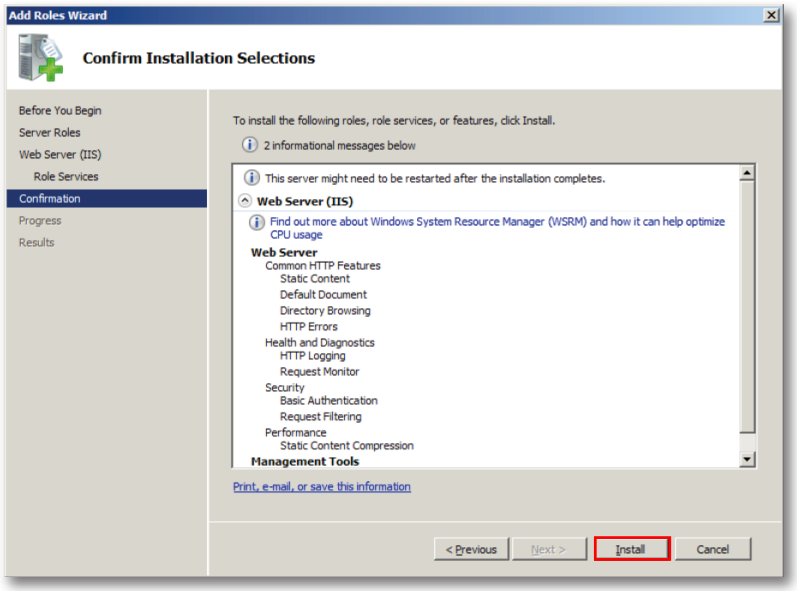

Figure 3-7: Confirm IIS installation options for a Windows Server 2008 R2 computer

Wait a few minutes whilst IIS is installed, as illustrated below in Figure 3-8.

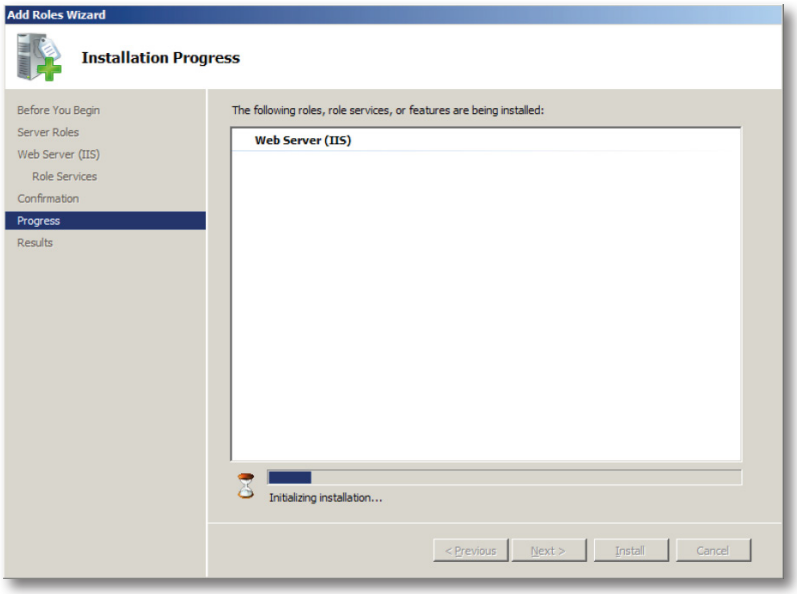

Figure 3-8: IIS installation in progress on a Windows Server 2008 R2 computer

Review the results and any warnings post-install. Consult with the site IT Manager for any site-specific or computer-specific warnings which may occur. Click **Close** to exit, as illustrated below in Figure 3-9.

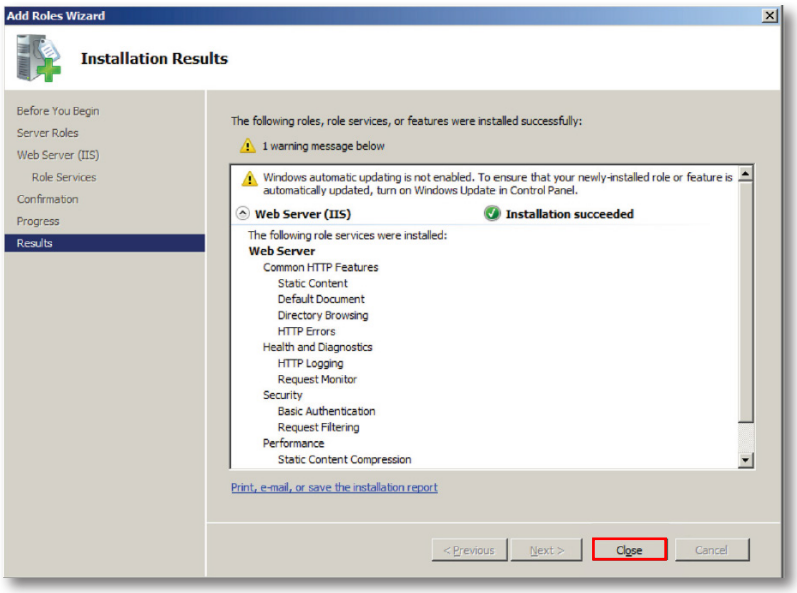

Figure 3-9: Review IIS installation results on Windows Server 2008 R2

Once your server computer has been setup with the new role as a Web Server (IIS) you are ready to configure IIS to work with the eServer software

Firstly, confirm that the role Web Server (IIS) has been initialised on your server computer. From the Server Manager window, select **Roles** and validate that the **role is present in the Roles Summary list**, as illustrated below in Figure 3-10.

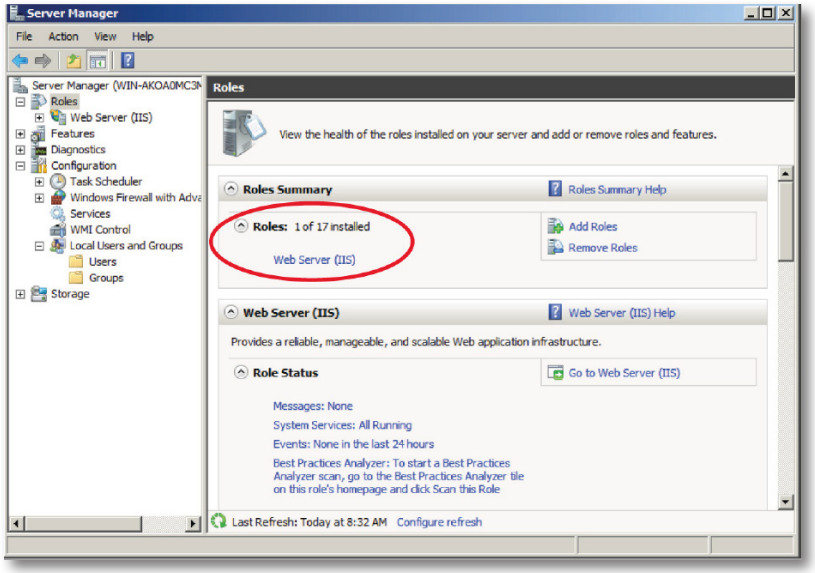

Figure 3-10: Validate the role Web Server (IIS) in the Server Manager window

3-2.3 Installing IIS on Windows Server 2012 R2

These instructions detail the process for installing IIS on a Windows Server 2012 R2 computer.

1. Open Server Manager. The Dashboard will show if the IIS role is installed.

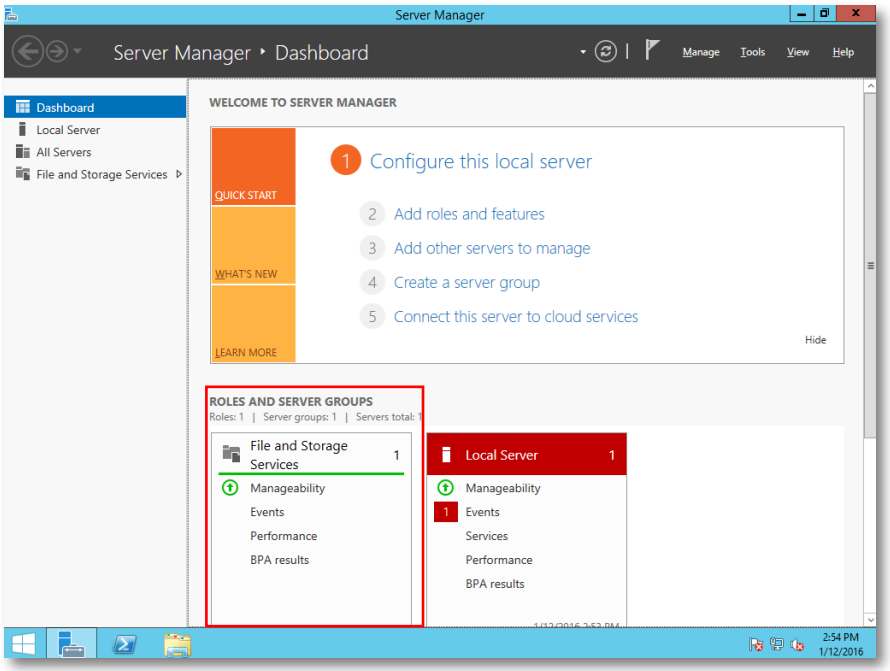

Figure 3-11: Server Manager Dashboard

2. Click Add roles and features.

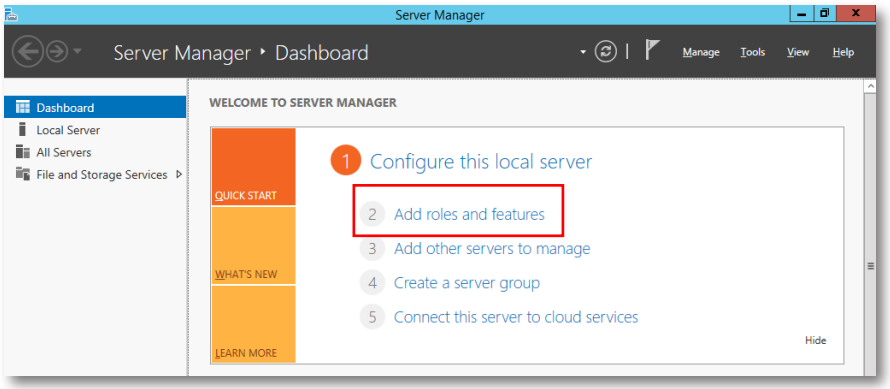

Figure 3-12: Server Manager Dashboard - Add roles and features

3. Click Next

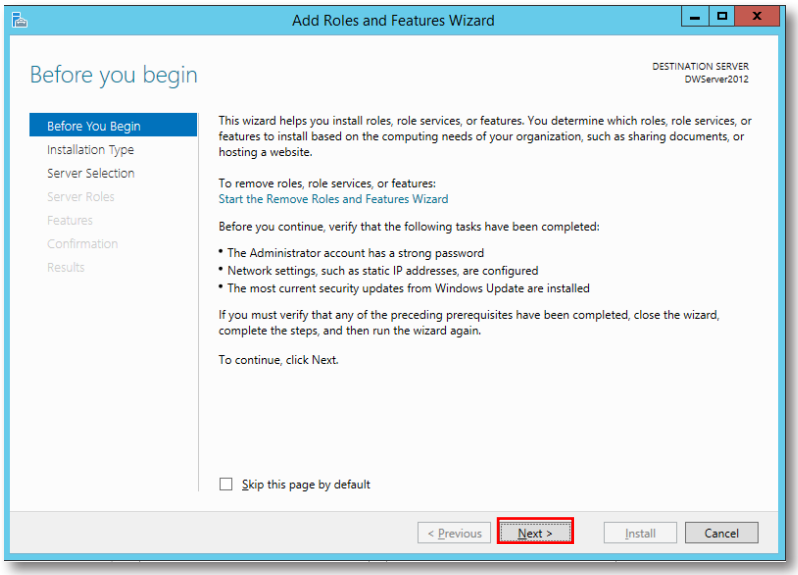

Figure 3-13: Wizard information screen

4. Select installation type and click next.

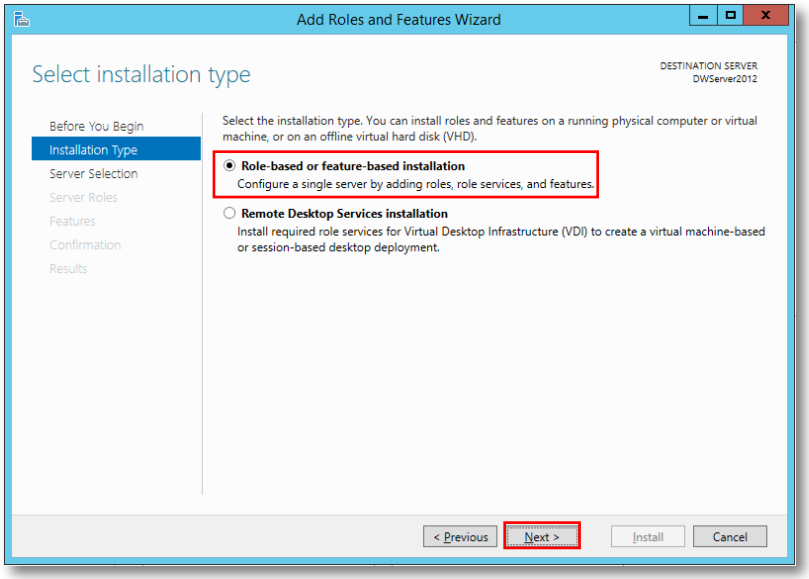

Figure 3-14: Select Installation Type

5. Select destination server and then click Next.

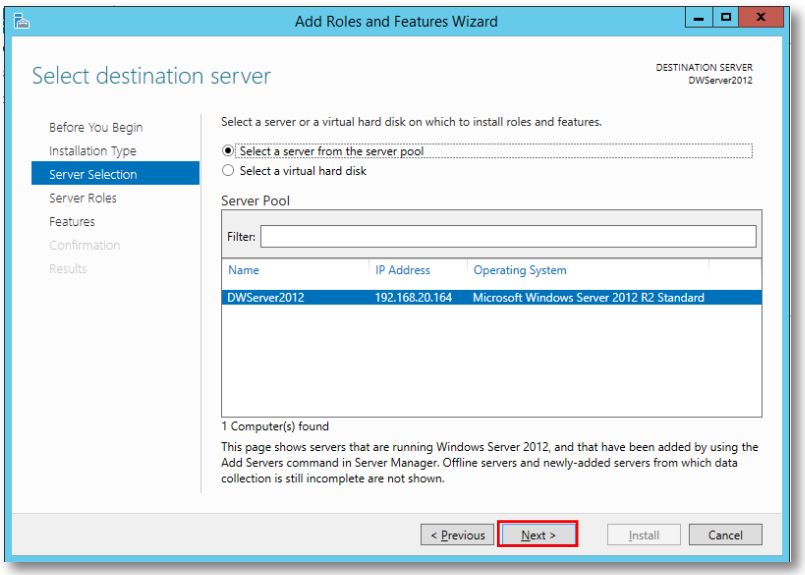

Figure 3-15: Select Destination Server

6. Scroll down and click the Web Server (IIS) checkbox.

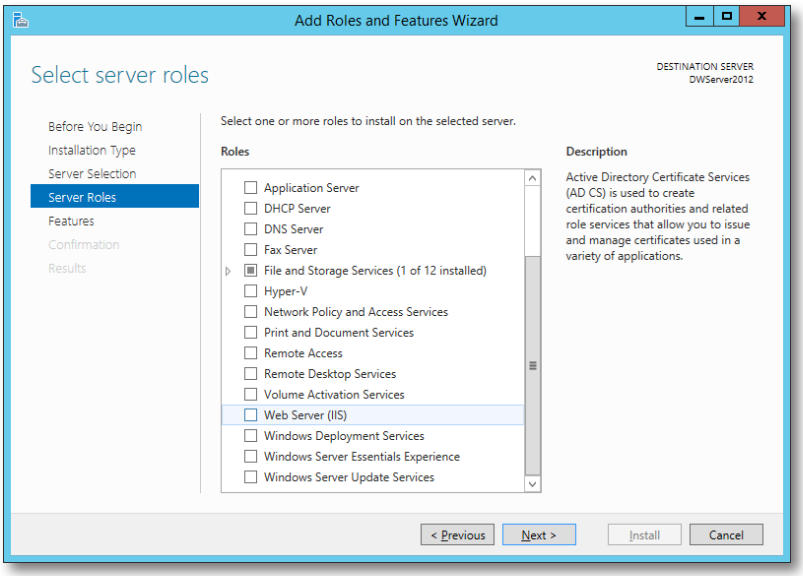

Figure 3-16: Select the Web Server (IIS) Role

7. Click Add Features.

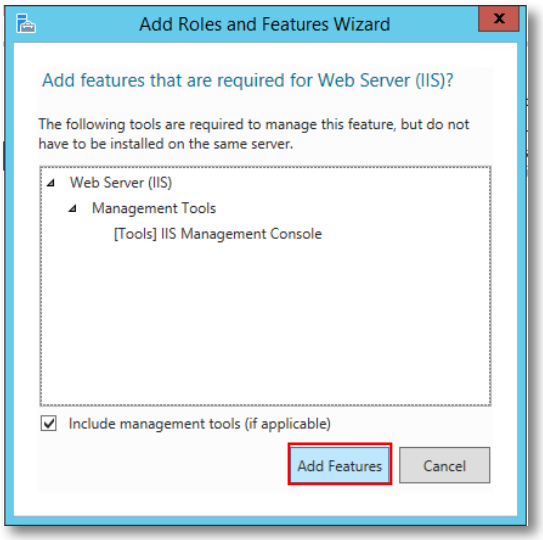

Figure 3-17: Add Required Features

8. Click Next at the next few screens and then click the Install button.

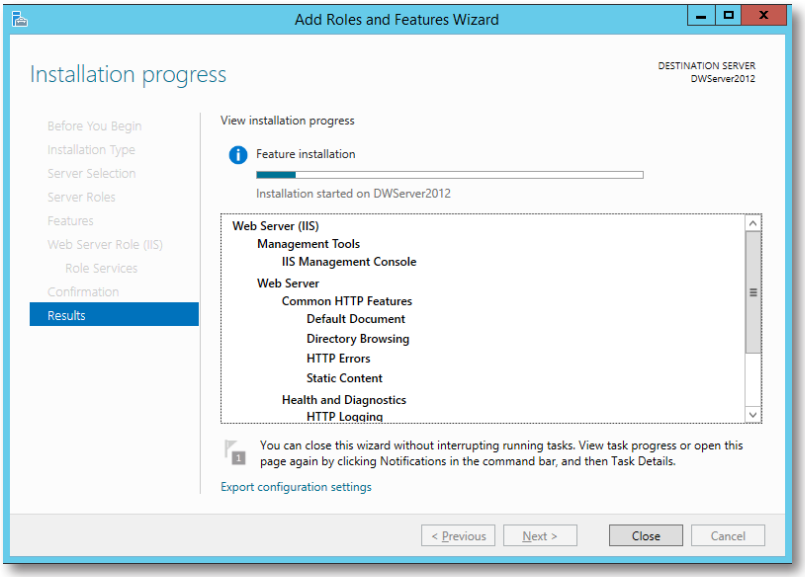

Figure 3-18: Installation in Progress

9. After installation, the IIS Role will now be visible on the Dashboard.

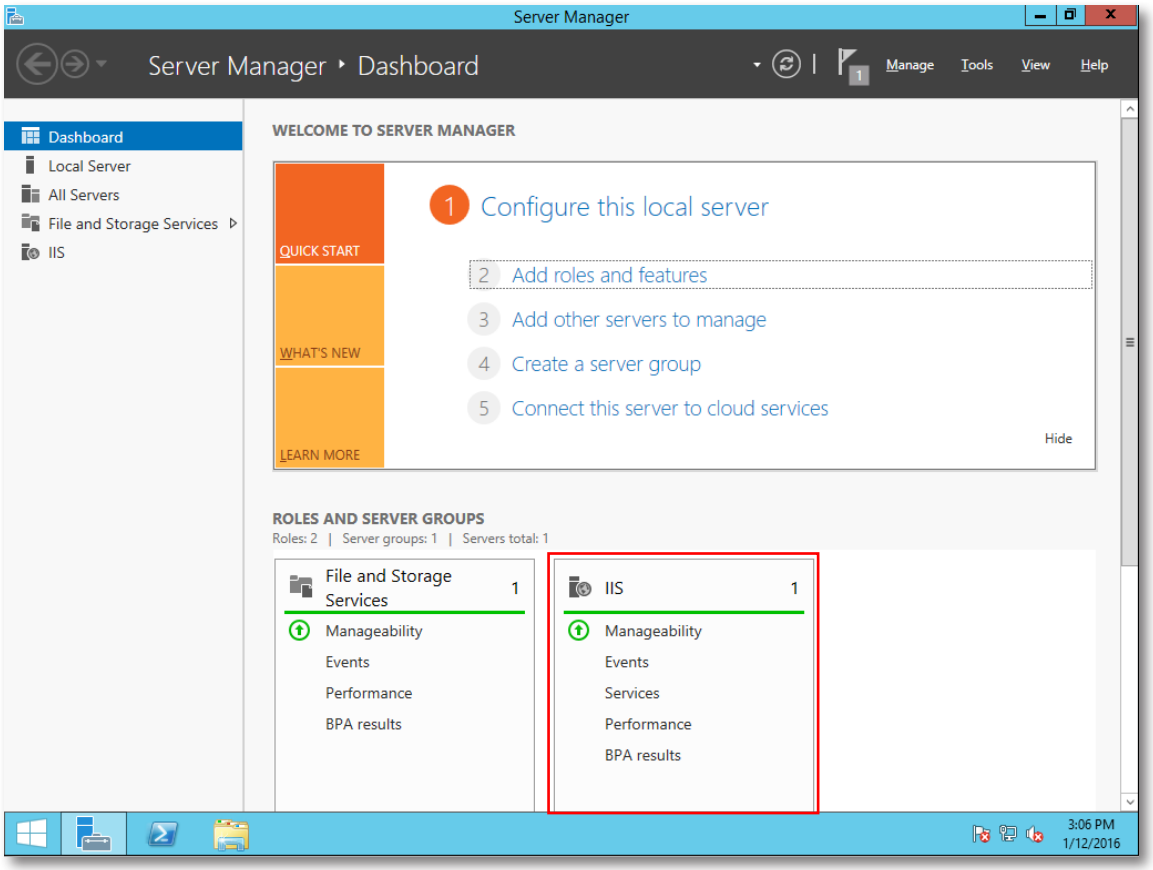

Figure 3-19: Installation Complete

3-2.4 Installing IIS on Windows 7

These instructions detail the process for installing IIS on a Windows 7 (SP1) computer.

It is recommended to have the server computer's initial configuration settings set by the site IT Manager.

Verify if IIS has previously been installed on the Windows 7 computer by opening **Control Panel** from the Windows **Start** menu, as illustrated below in Figure 3-20.

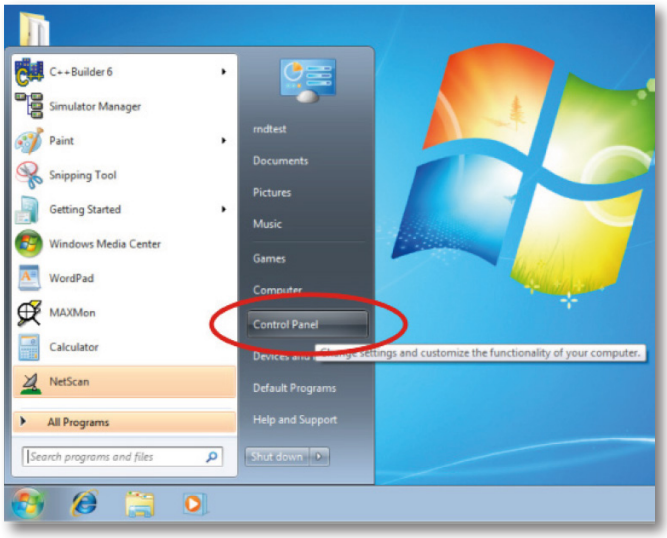

Figure 3-20: Opening Control Panel on Windows 7

Select **Small Icons** on the top right to open up the complete list of **Control Panel** options. Select **Programs and Features** from the Control Panel list, as illustrated below in Figure 3-21.

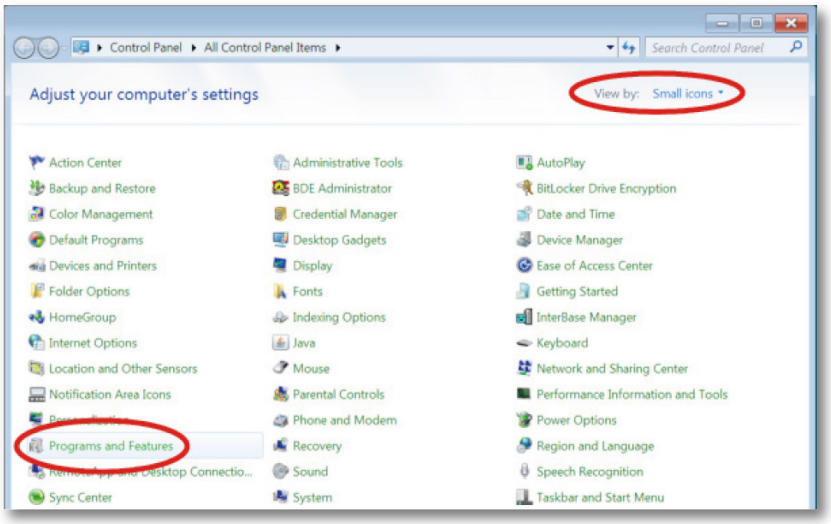

Figure 3-21: Open Programs and Features from the Control Panel on Windows 7

Click **Turn Windows features on or off** from the left pane of the Programs and Features window, as illustrated below in Figure 3-22.

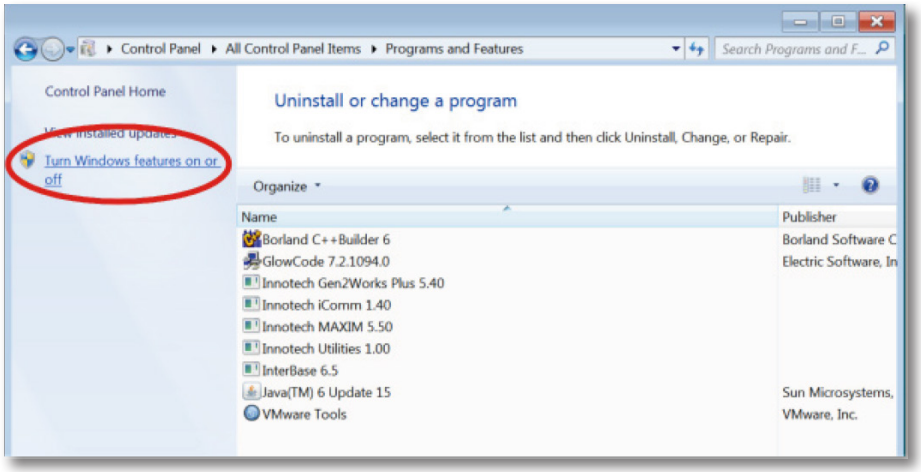

Figure 3-22: Selecting "Turn Windows Features On or Off" on Windows 7

From the Windows Features menu, do the following:

- Scroll down the list of Windows Features, and expand the Internet Information Services tree list. Underneath that, expand the Web Management Tools list. Ensure that IIS Management Console is selected, as illustrated below in Figure 3-23.
- Immediately underneath, ensure that World Wide Web Services is selected with a blue square, as illustrated below in Figure 3-23.
- The IIS Management Console is NOT activated by default on Windows 7. This feature can be enabled from Windows Features.

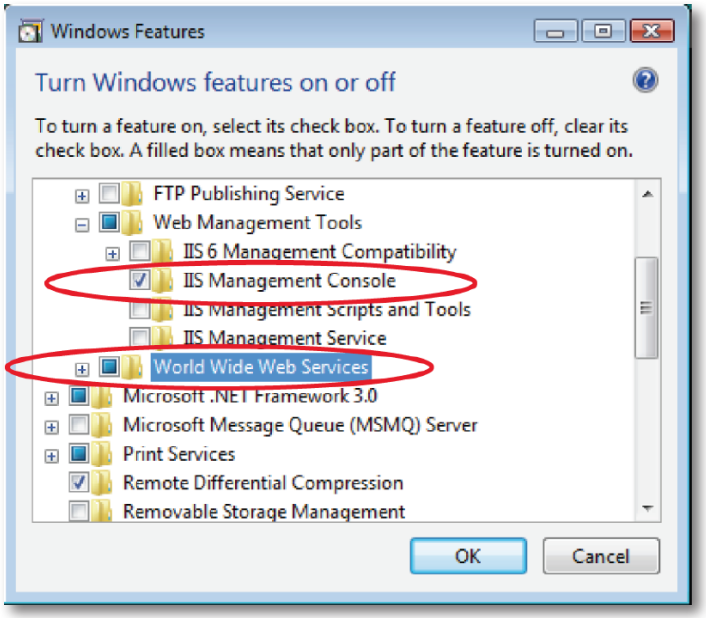

Figure 3-23: Setup IIS Features on Windows 7

*If the IIS Management Console box is not checked, click on the box and then click on **OK** to install the IIS Management Console. Follow the on-screen prompts to complete this process. If required, this process may be completed by the site IT department.*

3-2.5 Installing IIS on Windows 10

These instructions detail the process for installing IIS on a Windows 10 computer.

Verify if IIS has previously been installed on the Windows 10 computer by opening **Programs and Features** by right clicking the Windows **Start Button** and left clicking Programs and Features, as illustrated below in Figure 3-24.

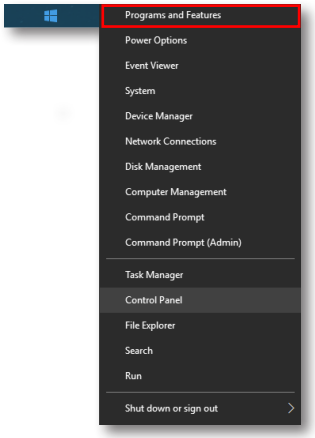

Figure 3-24: Opening Programs and Features on Windows 10

Click on **Turn Windows features on or off**, located on the left pane of the Programs and Features window and illustrated below in Figure 3-25.

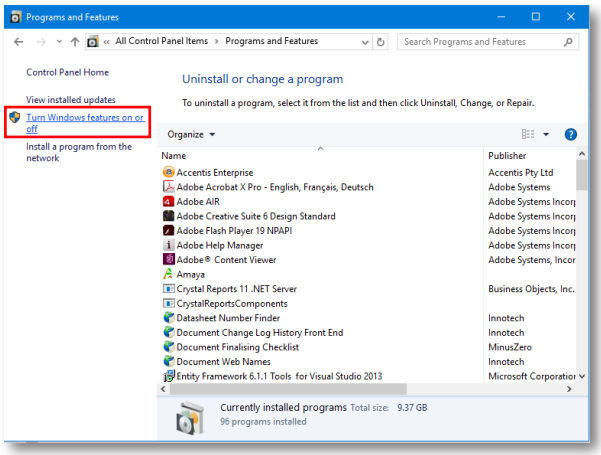

Figure 3-25: Opening Windows Features Menu on Windows 10

From the Windows Features menu, do the following:

- Scroll down the list of Windows Features, and expand the **Internet Information Services** tree list. Underneath that, expand the **Web Management Tools** list. Ensure that **IIS Management Console** is selected, as illustrated below in Figure 3-26.
- Immediately underneath, ensure that **World Wide Web Services** is selected with a blue square, as illustrated below in Figure 3-26.
- The IIS Management Console is **NOT installed by default on Windows 10**.

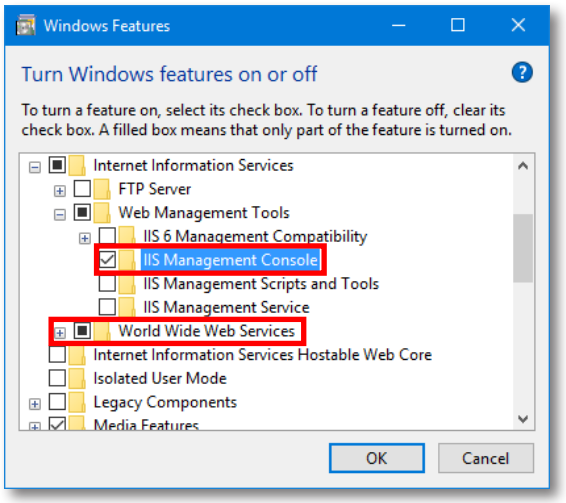

Figure 3-26: Setup IIS Features on Windows 10

If the IIS Management Console box is not checked, click on the box and then click on **OK** *to install the IIS Management Console. Follow the on-screen prompts to complete this process. If required, this process may be completed by the site IT department.*

3-3 Launching Internet Information Services (IIS)

3-3.1 Overview

There are different ways to launch the IIS Manager window on different Operating Systems. This section provides steps to open IIS on supported Operating Systems.

3-3.2 Launching IIS on Windows Server 2008

Open the IIS Manager from the Windows Start Menu. Select Administrative Tools and click **Internet Information Services (IIS) Manager**, as illustrated below in Figure 3-27.

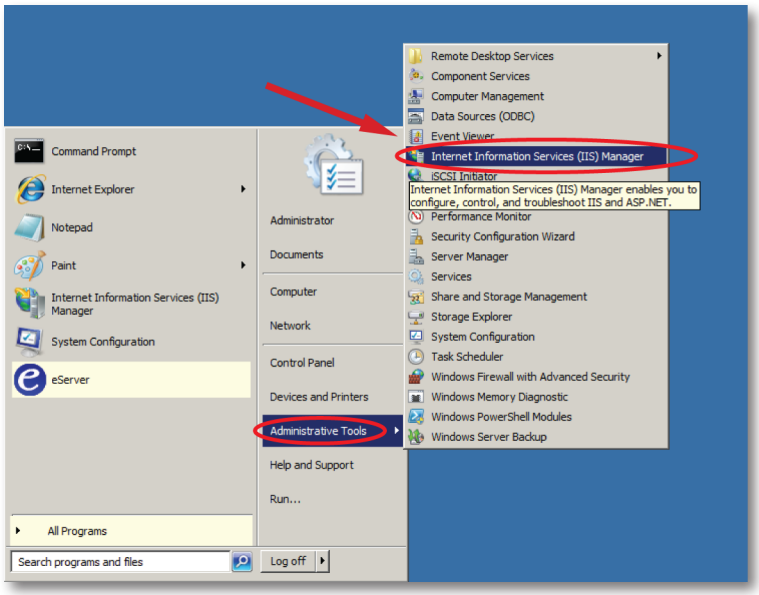

Figure 3-27: Launch the IIS Manager on Windows Server 2008 R2

This will launch the home screen of the IIS Manager, as illustrated below in Figure 3-28.

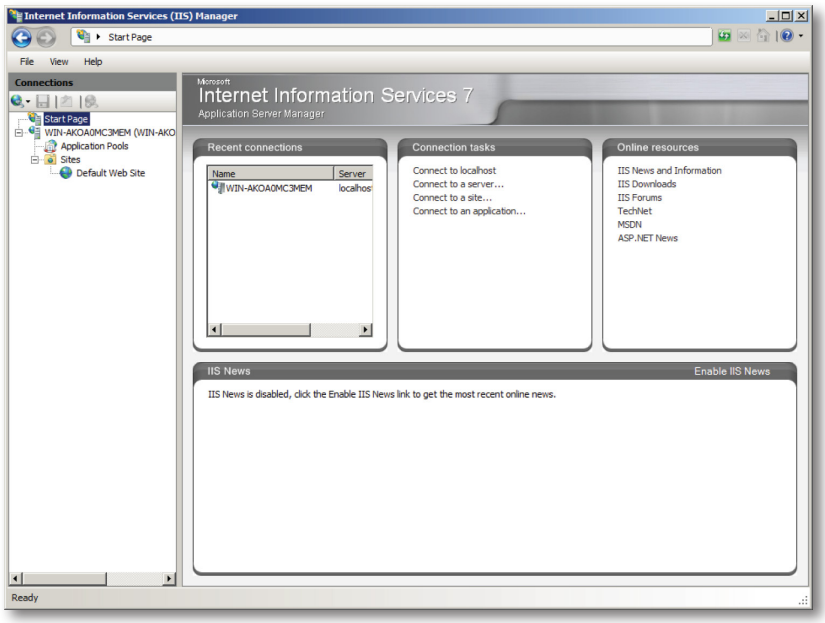

Figure 3-28: Home screen of the IIS Manager on Windows Server 2008 R2

3-3.3 Launching IIS on Windows Server 2012 R2

Click the Windows button to show the tile screen if not already visible and immediately type IIS, as illustrated below in Figure 3-29.

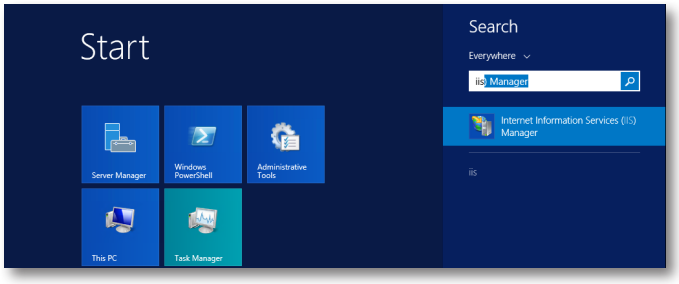

Figure 3-29: Windows Server 2012 R2 Tile Screen

Click Internet Information Services (IIS) Manager to launch IIS.

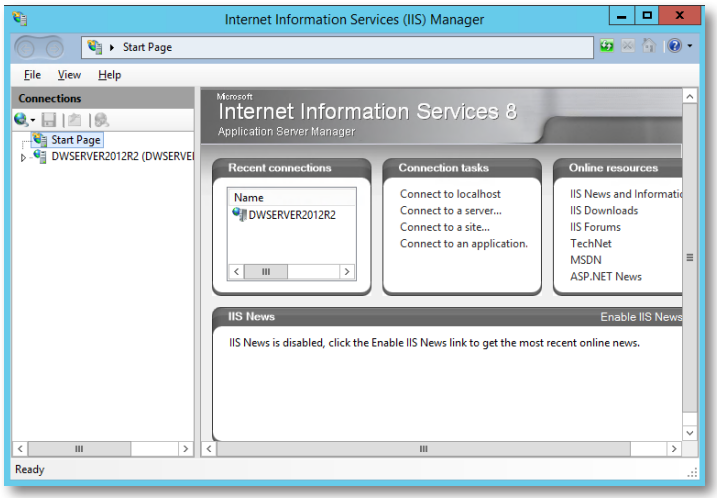

Figure 3-30: IIS Manager on Windows Server 2012 R2

3-3.4 Launching IIS on Windows 7

Open the Control Panel from the Windows Start Menu, as illustrated below in Figure 3-31.

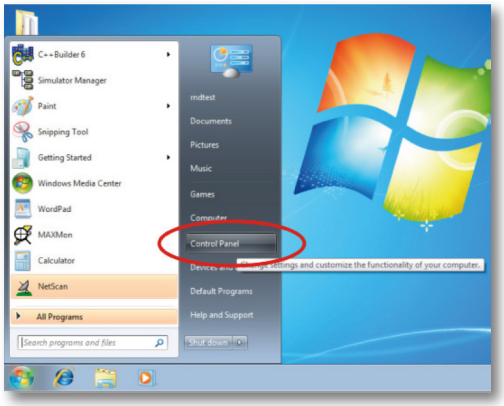

Figure 3-31: Opening Control Panel in Windows 7

Select **Small Icons** view from the top right panel, which will open the complete list of Control Panel options. Select **Administrative Tools** from the Control Panel list, as illustrated below in Figure 3-32.

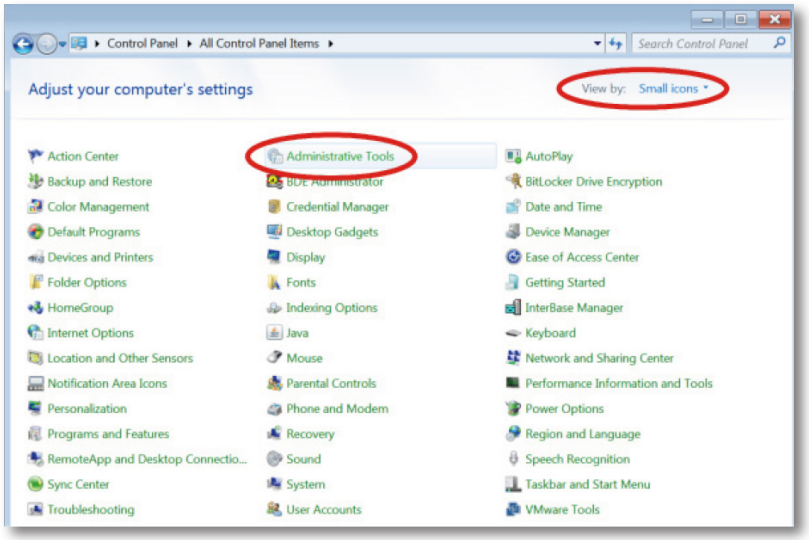

Figure 3-32: Open Administrative Tools on Windows 7

Select **Internet Information Services (IIS) Manager** from the Administrative Tools menu, as illustrated below in Figure 3-33.

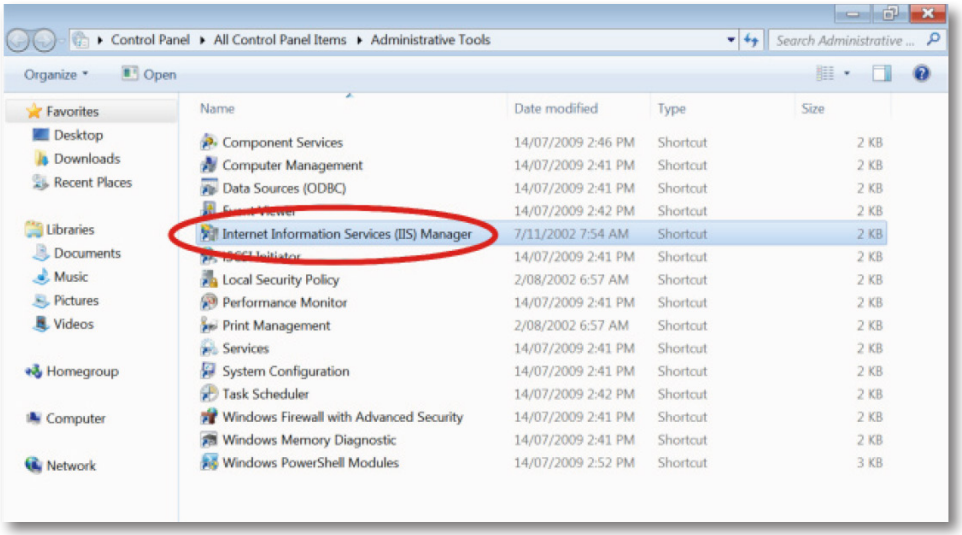

Figure 3-33: Launch IIS on Windows 7

3-3.5 Launching IIS on Windows 10

Click the Windows button and immediately type IIS, as illustrated below in Figure 3-34.

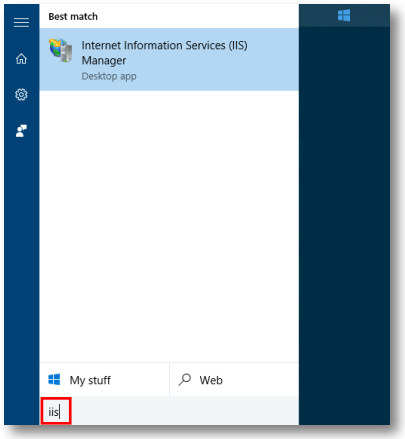

Figure 3-34: Windows 10 Start Menu

Click Internet Information Services (IIS) Manager to launch IIS, as illustrated below in Figure 3-35.

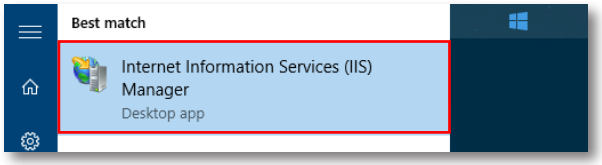

Figure 3-35: IIS Search Result

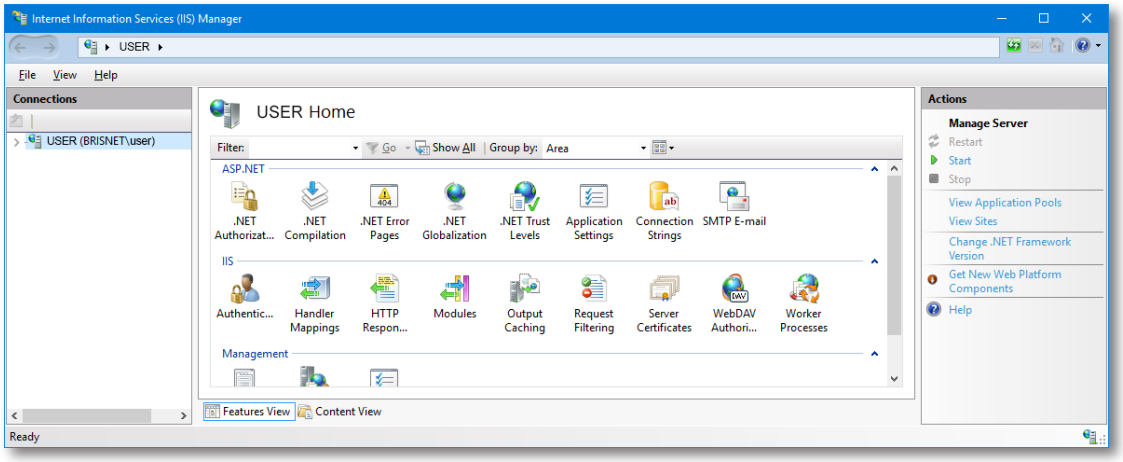

Figure 3-36: IIS Manager on Windows 10

3-4 Configuring Internet Information Services (IIS)

3-4.1 Overview

This section provides the steps to configure Internet Information Services to work as part of an Innotech system using eServer.

There are common steps to setup IIS on Windows Server 2008 / 2012 R2, Windows 7 and Windows 10, which are outlined in 3-2.2 to 3-2.5.

3-4.2 Configure IIS on Windows Server 2008 /2012 R2, 7 and 10

From the IIS Manager window, select expand the Connections list to view the **Default Web Site**. This will display menu options for the Default Web Site. Select **Basic Settings...** from the Actions menu, as illustrated below in Figure 3-37.

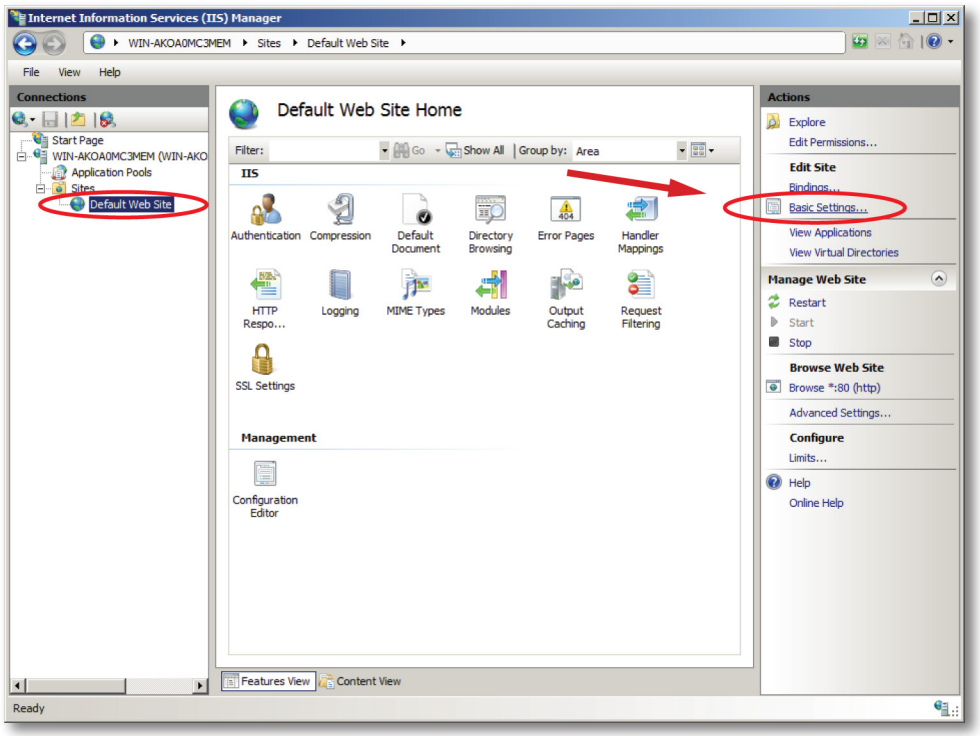

Figure 3-37: Open Basic Settings for Default Web Site

Set physical location path for Default Web Site to be **c:\MyWebPages**, as illustrated below in Figure 3-38. Click **OK** to save and exit.

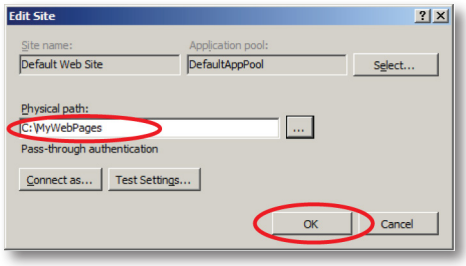

Figure 3-38: Configure Physical Path for c:\MyWebPages

Set the Authentication properties for the Default Web Site. Select **Default Web Site** and double click on the **Authentication** icon, as illustrated below in Figure 3-39.

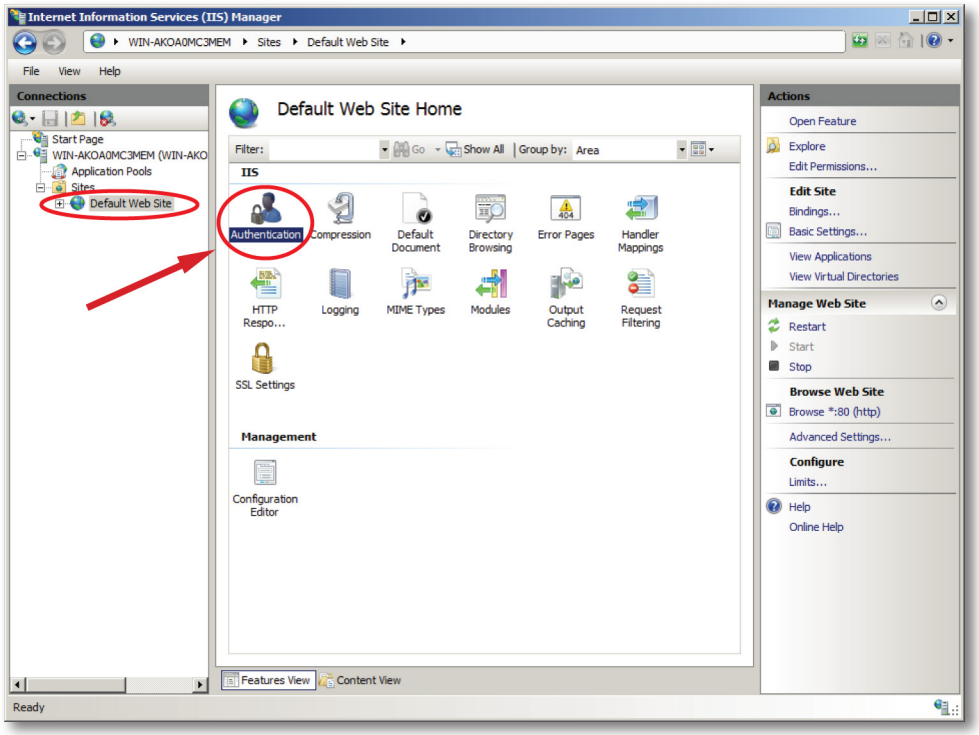

Figure 3-39: Set Authentication properties for Default Web Site

In the Authentication list, click on **Anonymous Authentication** and click on **Edit...** in the Actions Pane on the right, as illustrated below in Figure 3-40.

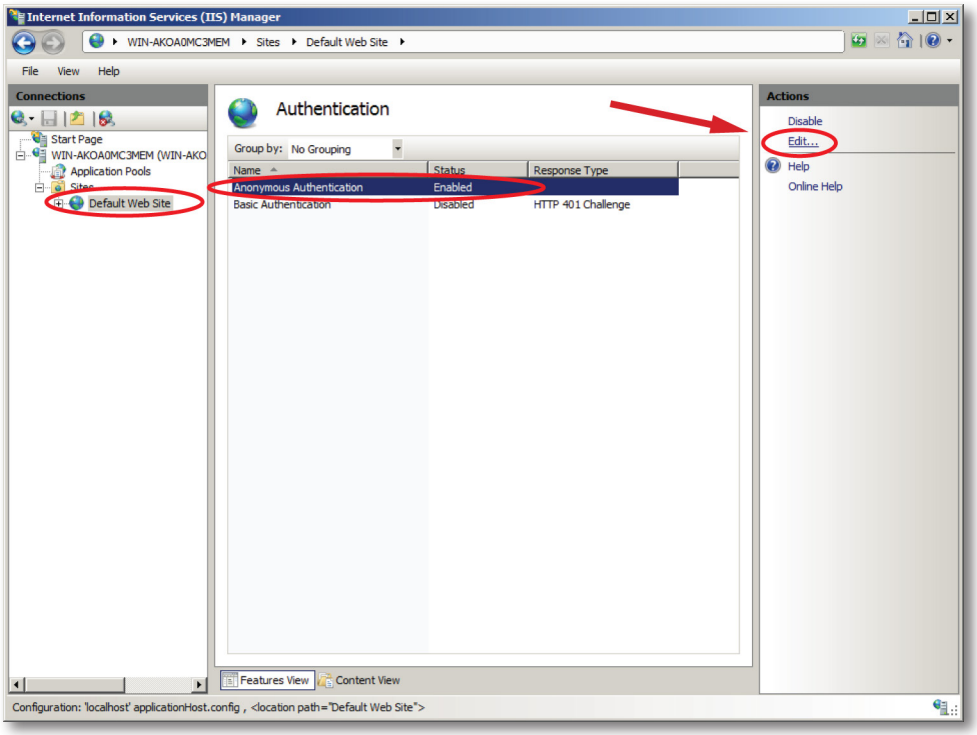

Figure 3-40: Edit Anonymous Authentication properties

Ensure that **Specific User** is selected, and click on the **Set...** button, as illustrated below in Figure 3-41.

Figure 3-41: Set Anonymous user identity

Enter **IUSR** as the Username. Leave all other fields blank and click OK to apply, as illustrated below in Figure 3-42.

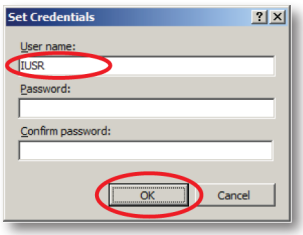

Figure 3-42: Set IUSR credentials

Click OK to save and exit Anonymous Authentication setup, as illustrated below in Figure 3-43.

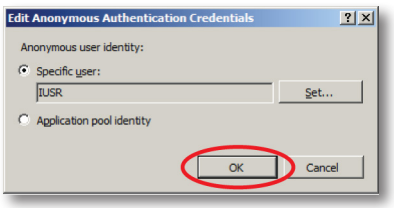

Figure 3-43: Save and Exit Anonymous Authentication Setup

Return to the main window as illustrated below and open **Default Document** as illustrated below in Figure 3-44.

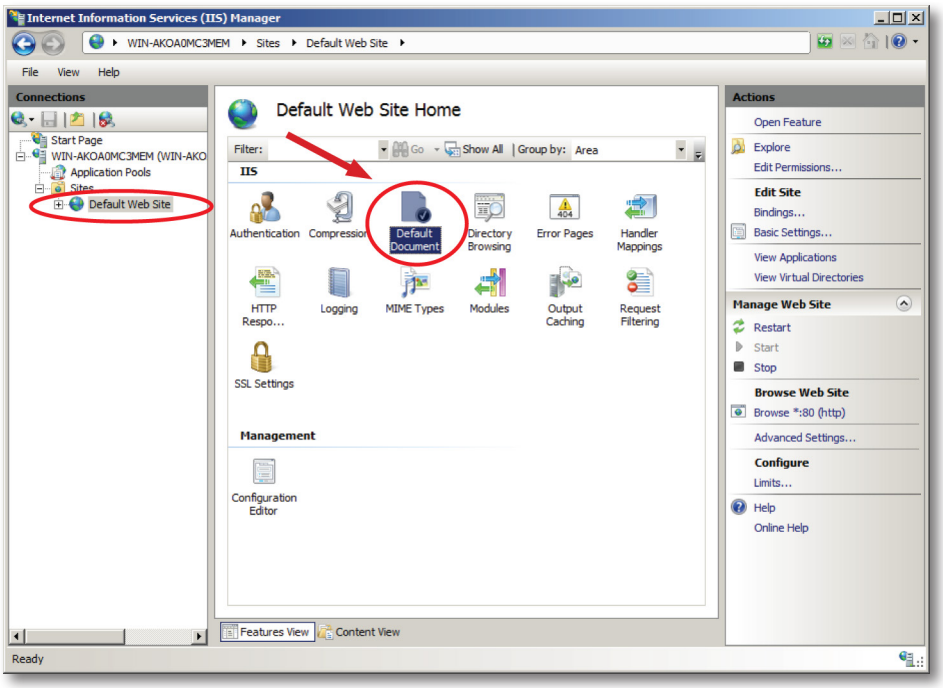

Figure 3-44: Open Default Document Menu for Default Website

Select **index.htm** in the Default Document list. If it does not exist, click the **Add...** button to add the document index.htm. Use the **Move Up** button to move index.htm to the top of the Default Document list, as illustrated below in Figure 3-45.

IMPORTANT

There may be both a Index.html and Index.htm files in this list. ***Ensure to use the file Index.htm.***

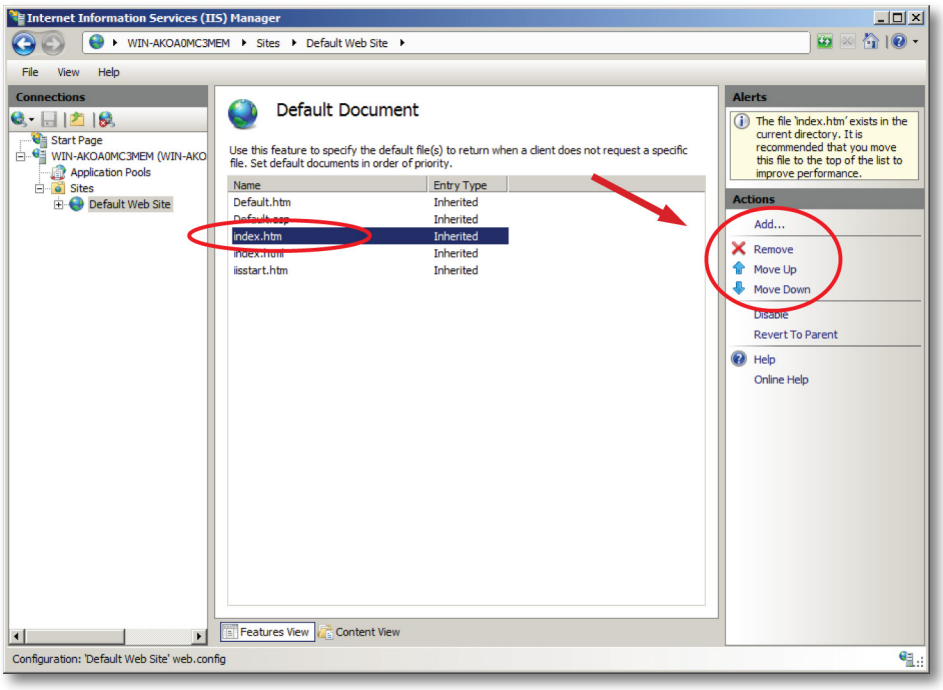

Figure 3-45: Select Default Document index.htm

If an information window appears, read the dialogue and click **Yes** to accept, as illustrated below in Figure 3-46. The default settings for Default Document are suitable for eServer implementation.

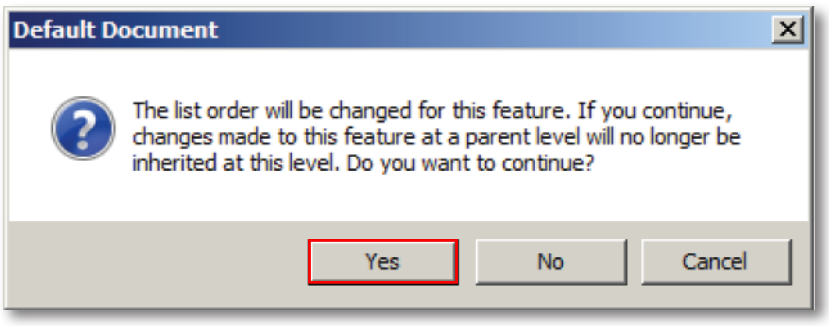

Figure 3-46: Confirm Selection of Default Document index.htm

Validate that **index.htm** is at the top of the Default Document list (not index.html), as illustrated below in Figure 3-47.

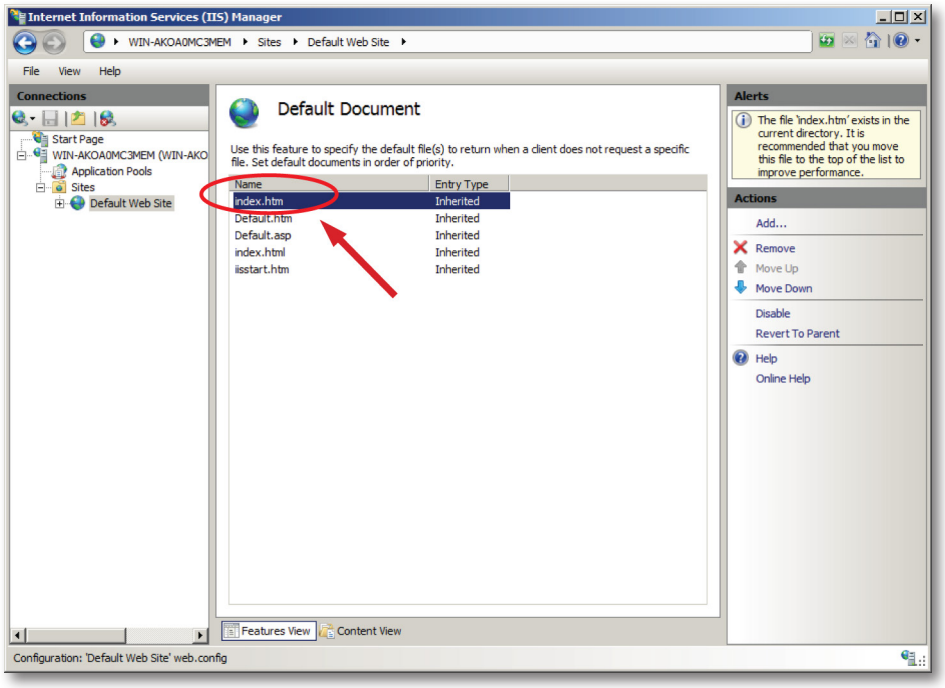

Figure 3-47: Locate the Default Document index.htm

Close and exit all IIS menu windows. IIS setup for eServer is complete for the Windows Server 2008 / 2012 R2, Windows 7 and Windows 10 Operating Systems.

3-5 Set up an Self Signed SSL Certificate

3-5.1 Overview

This section provides the steps to set up a self signed SSL Certificate and https for eServer.

The series of images over the next few pages show how to complete the set up.

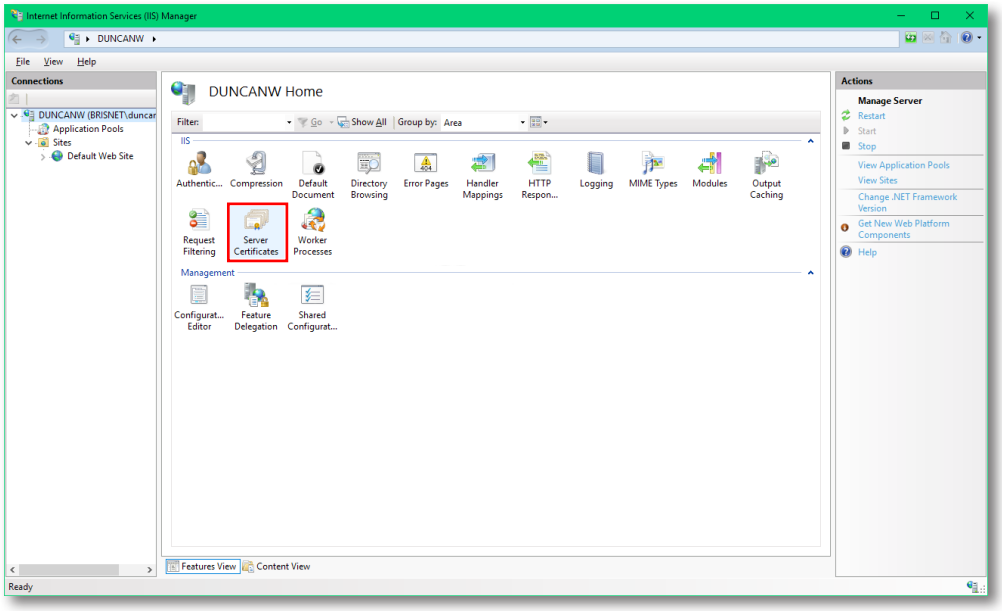

Figure 3-48: Double Click Server Certificates

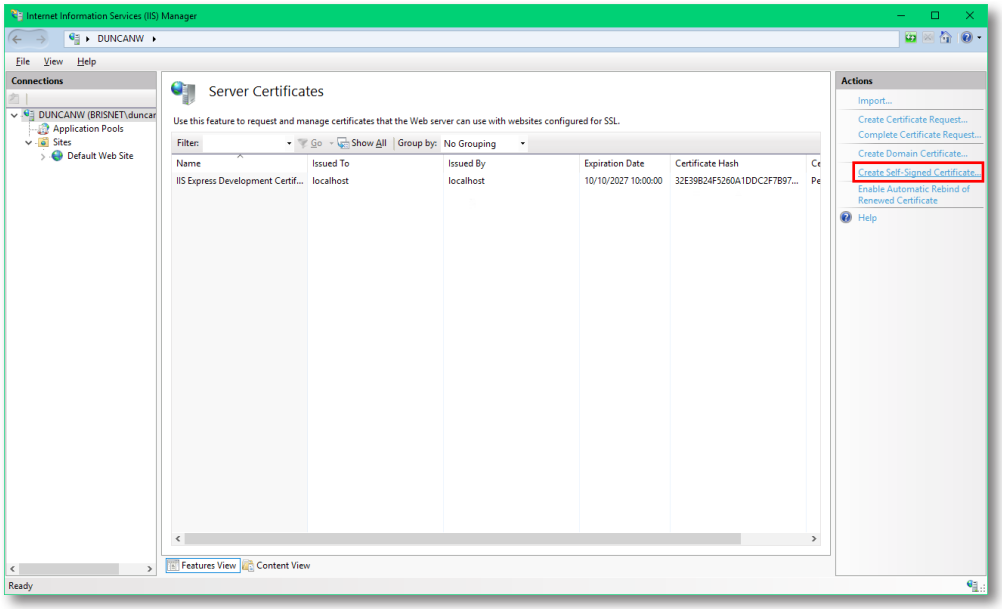

Figure 3-49: Click Self Signed Certificates

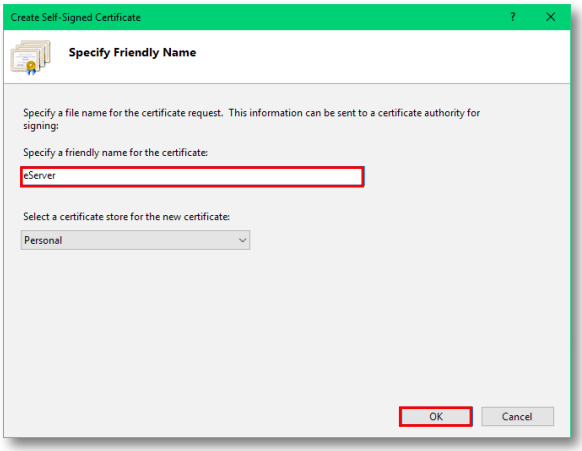

Figure 3-50: Enter a name for the certificate and click OK

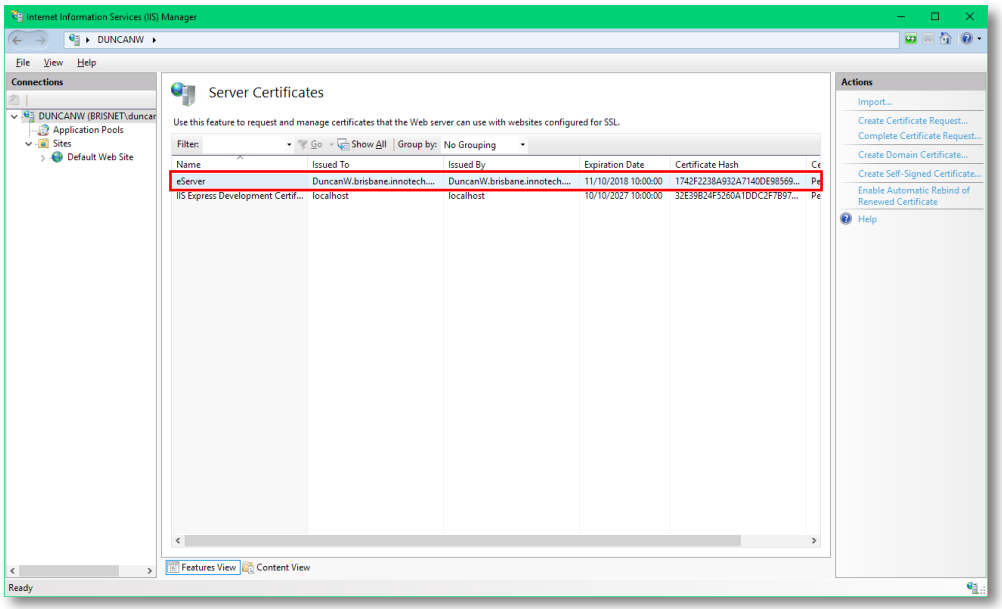

Figure 3-51: Self Signed Certificate Created

After your certificate has been created in IIS, you need to set up the Bindings to enable certificate usage with https. Click here for information on editing the IIS Bindings.

3-6 Set up a 3rd Party SSL Certificate

3-6.1 Overview

This section provides the steps to set up a 3rd Party SSL Certificate for eServer.

The series of images over the next few pages show how to complete the set up.

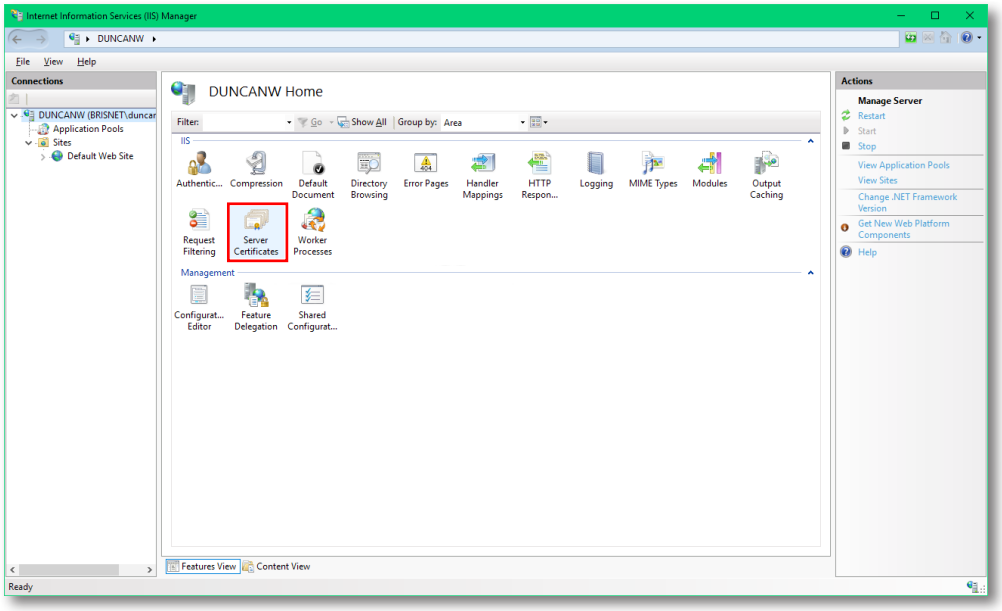

Figure 3-52: Double Click Server Certificates

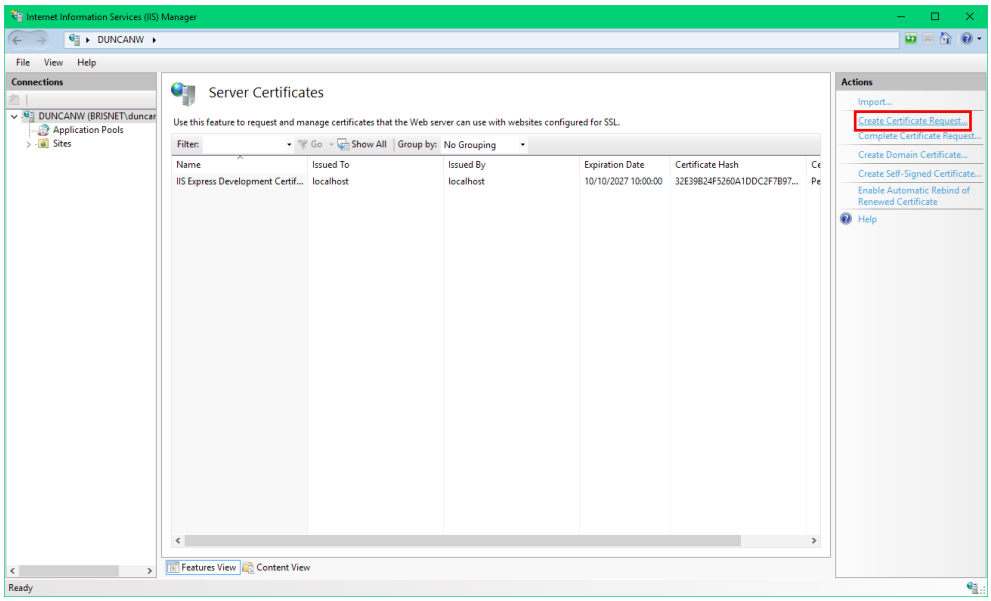

Figure 3-53: Click Create Certificate Request

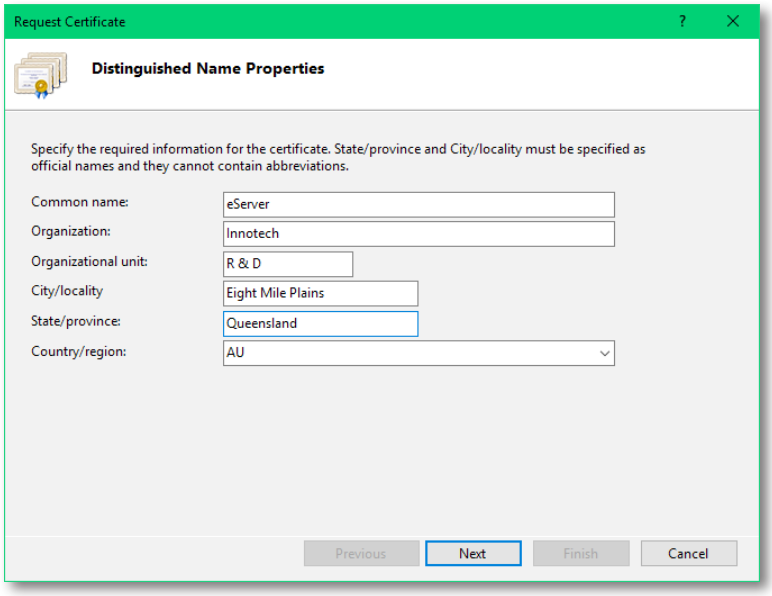

Figure 3-54: Fill in details for the CSR

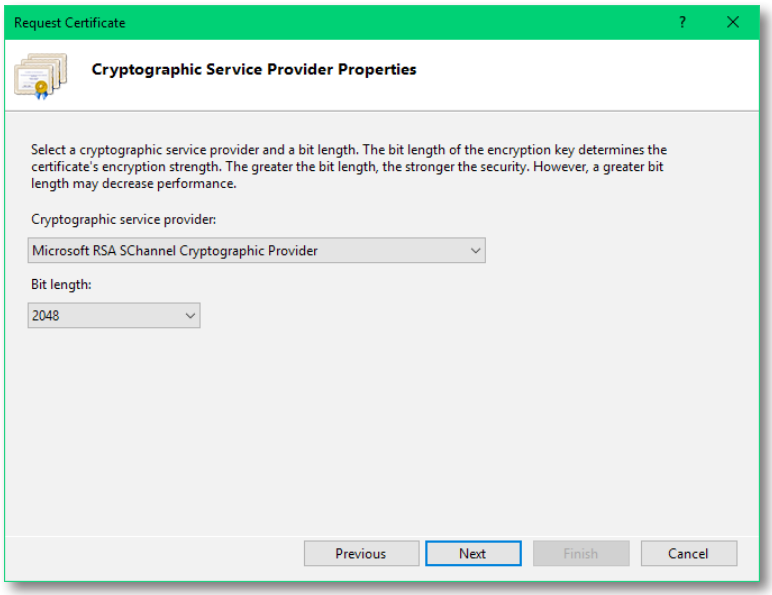

Figure 3-55: Select a Bit Length of 2048 or more

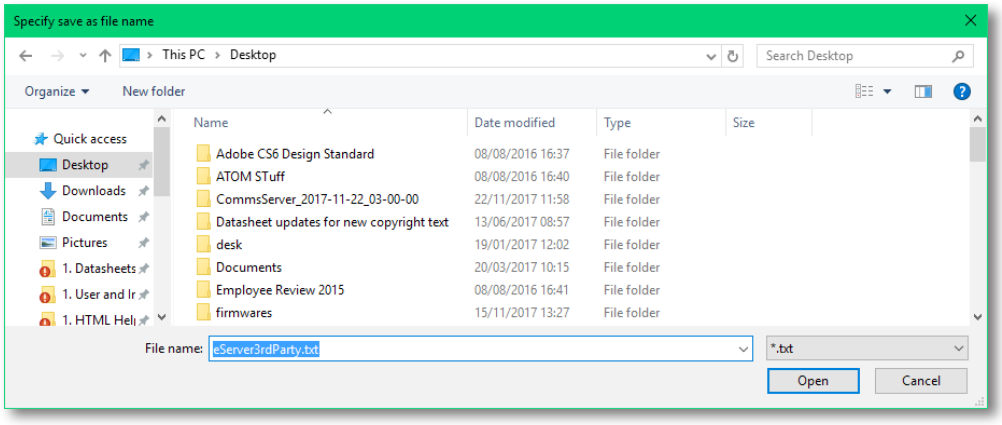

Figure 3-56: Save your CSR File

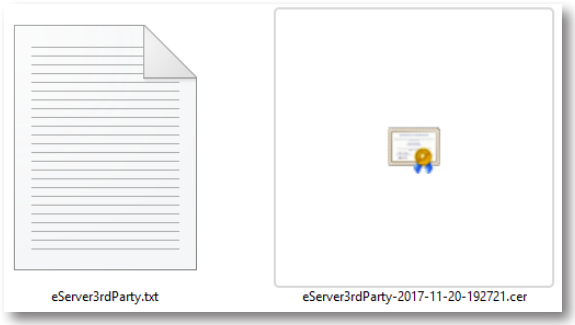

Figure 3-57: Submit file to your 3rd Party Certificate Provider to receive your certificate

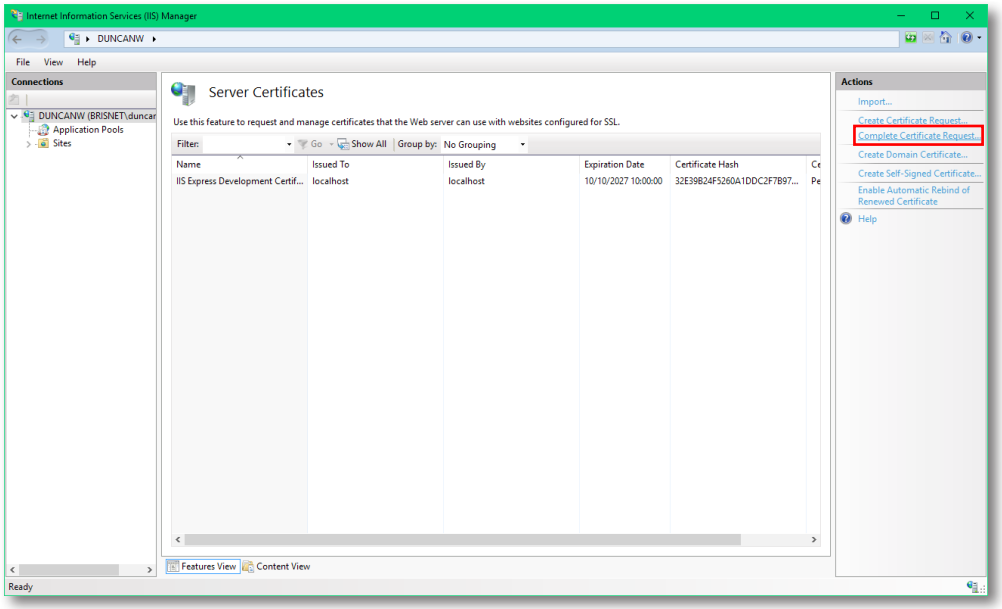

Figure 3-58: Click Complete Certificate Request

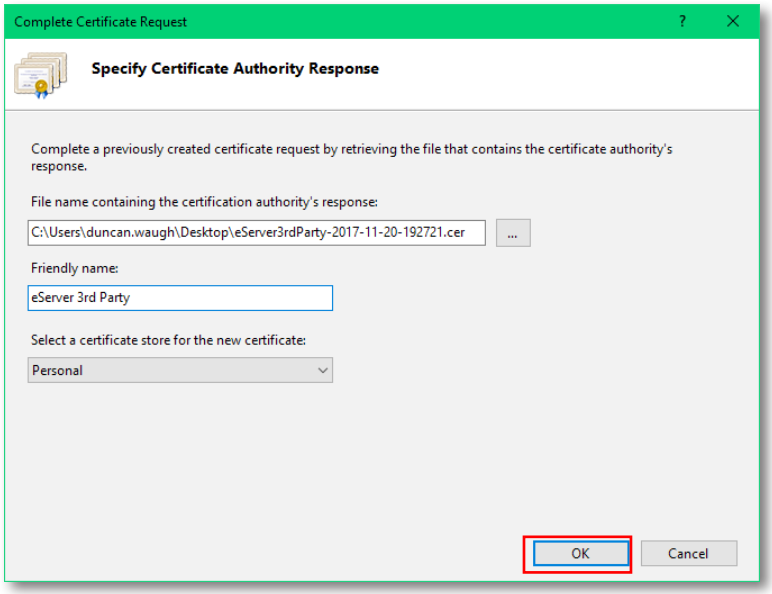

Figure 3-59: Select your .cer file, enter a friendly name and click OK

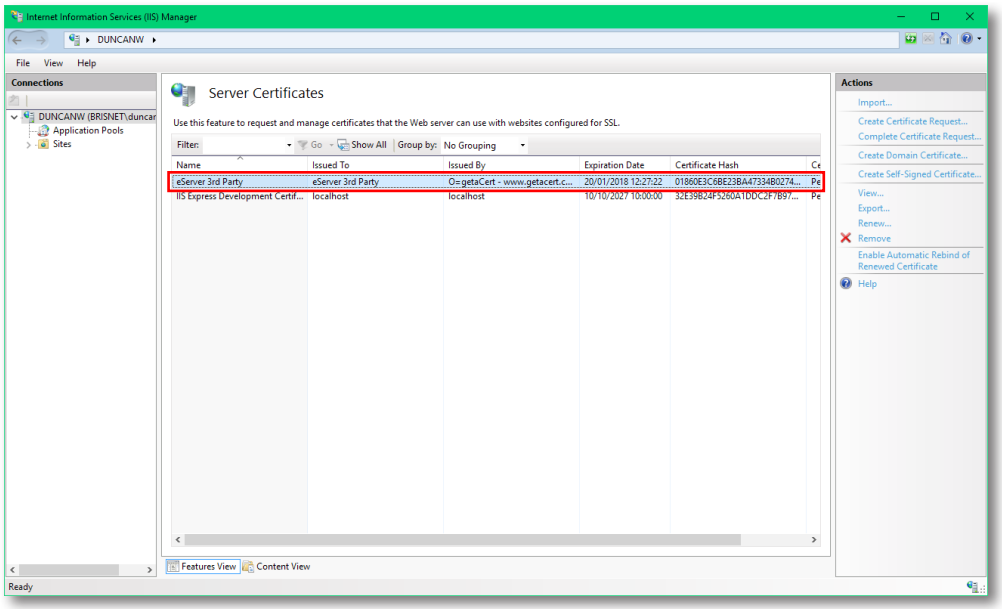

Figure 3-60: 3rd Party Certificate Listed

After your certificate has been created in IIS, you need to set up the Bindings to enable certificate usage with https. Click here for information on editing the IIS Bindings.

3-7 Set up Certificate Bindings and https

3-7.1 Overview

This section provides the steps to set up a self signed SSL Certificate and https for eServer.

The series of images over the next few pages show how to complete the set up.

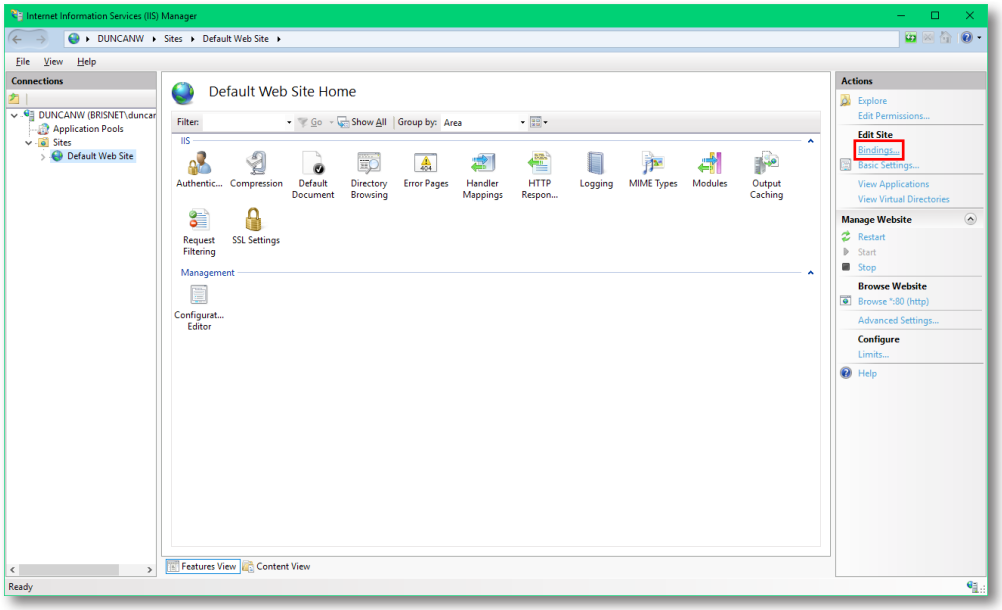

Figure 3-61: Click Bindings

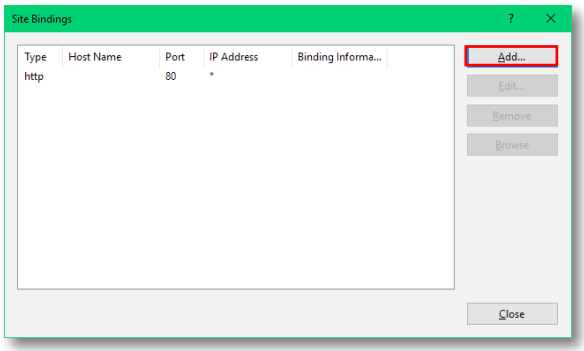

Figure 3-62: Click Add

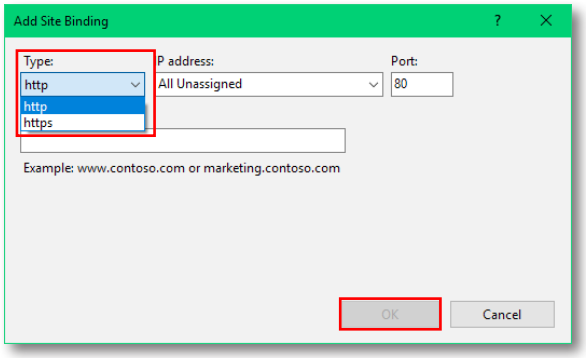

Figure 3-63: Select the https Type

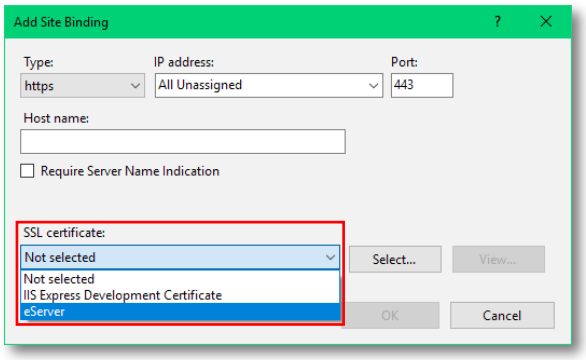

Figure 3-64: Select the SSL Certificate you created

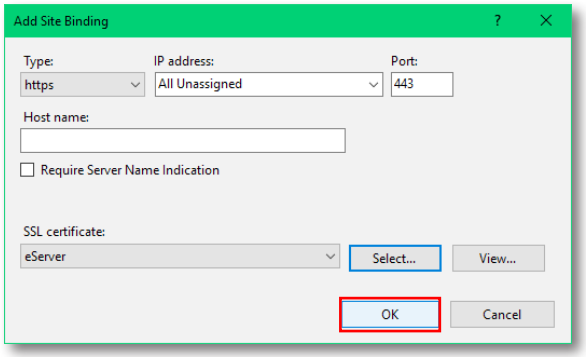

Figure 3-65: Click OK

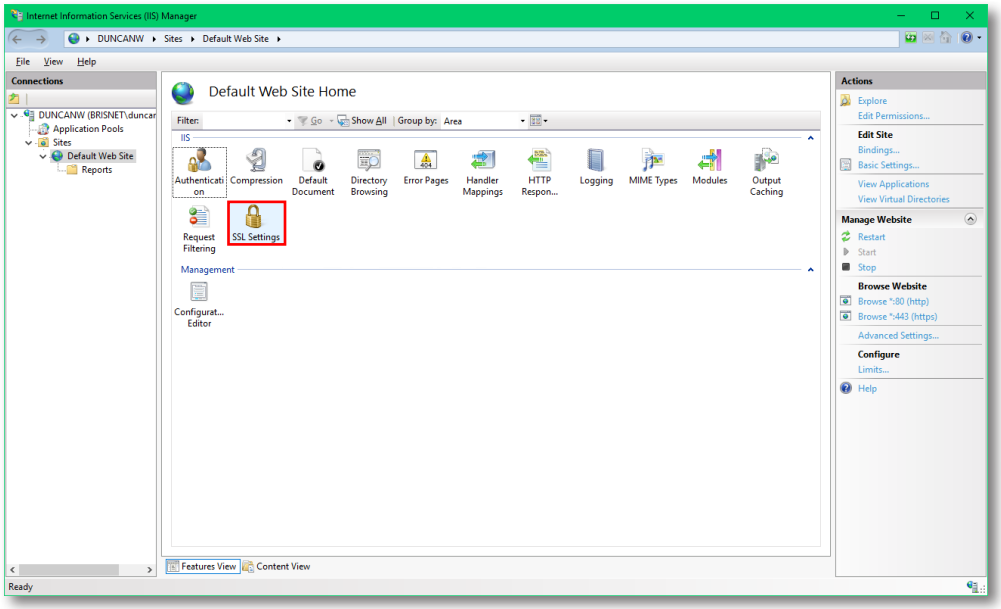

Figure 3-66: Click SSL Settings

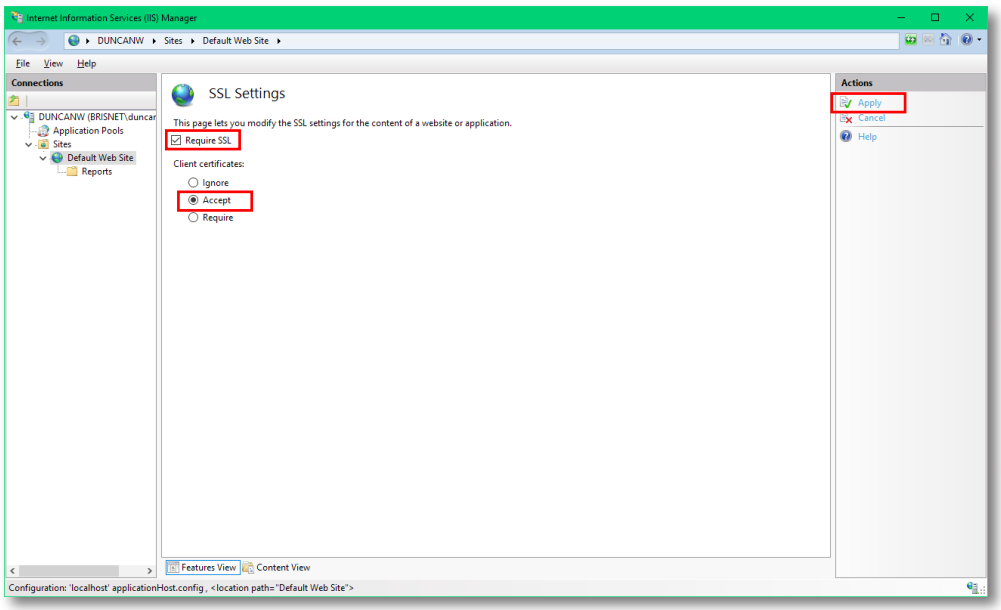

Figure 3-67: Check Require SSL, Click Accept and then Apply

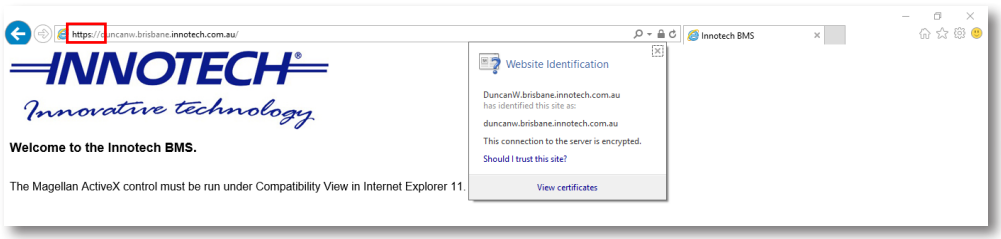

Figure 3-68: You can now browse to the website using https://

eServer

SETUP AND SITE INSTALLATION INSTRUCTIONS

4 Configuring eServer Communications

INNOTECH®

4-1 Overview

This section provides an overview of the steps required to configure security and access control on eServer software to allow remote computers to access Magellan projects via the eServer software. Additionally, steps are provided to enable eServer to communicate with an SQL Server database.

4-2 Configure eServer Project Settings

4-2.1 Overview

This section provides instructions on how to configure your eServer Project Settings to work as part of a system including Innotech eServer 1.50 or greater. Specifically, this section provides information on how to open your project and set project connection properties for a database, iComm server and connected devices.

*Ensure you are logged into the computer as a **System Administrator**. You will need to use **Magellan Builder v1.50 or greater** to configure the project settings, so ensure you have a Magellan Builder security dongle in addition to the eServer security dongle. Once you have setup the eServer Host computer, you may **remove the Magellan Builder security dongle, leaving just the eServer security dongle installed**.*

4-2.2 Launch Project for Configuration

Shutdown eServer and open **Magellan Builder v1.50** or greater. From the menu bar, open the Magellan Package, as illustrate below in Figure 4-1.

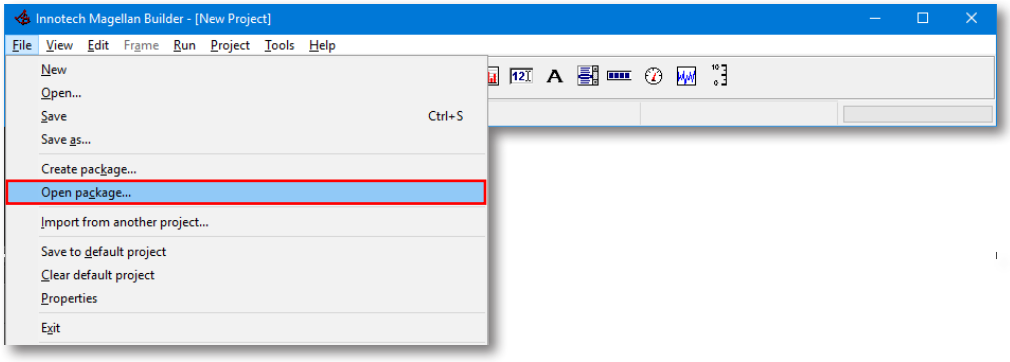

Figure 4-1: Open the Magellan project

4-2.3 Set Project Properties for the Access Database

Select Project from the menu bar, and open the Project **Properties** as illustrated below in Figure 4-2.

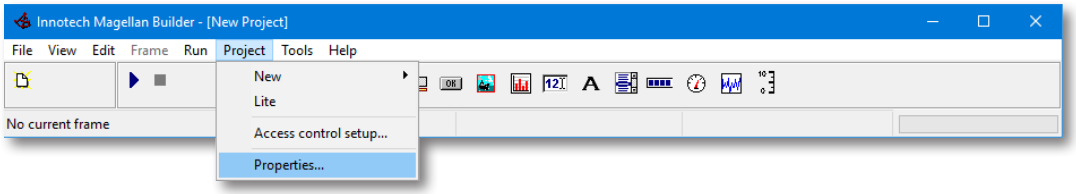

Figure 4-2: Open Project Properties to enter the Access database settings

In the Project Properties menu, select the Database Server type. The default is No Database. Use the dropdown list to select the Access database as illustrated below in Figure 4-3.

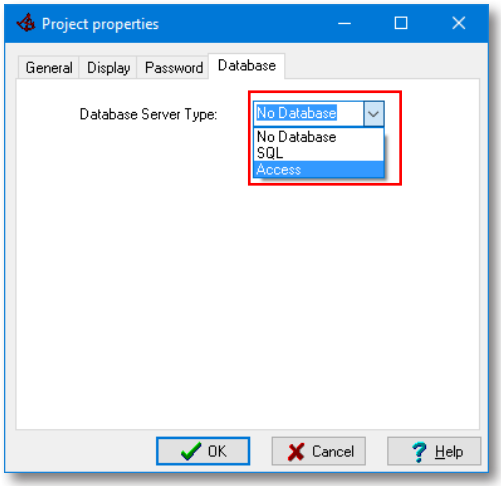

Figure 4-3: Selecting Access database in Magellan Project Properties

Enter the Access Database settings as described below, and illustrated below in Figure 4-4.

Access Driver: Select the appropriate Access Driver to use for the Access Database. For an Innotech iComm Access Database, use version 2000-2003.

Access Database File: Navigate to and select the Access Database to use with Magellan. For an Innotech iComm Access Database, the default path is:
c:\Program Files\Innotech\iComm\iCommDatabase

Automatically Connect on Startup: Select this option to enable automatic connection to the Access Database at project launch (*Recommended*). Alternatively, use Magellan commands to connect / disconnect as required during runtime.

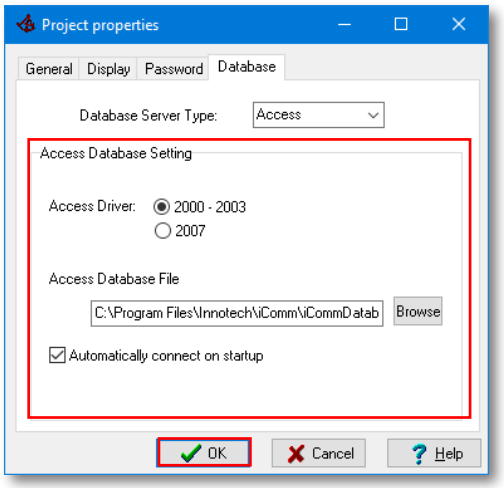

Figure 4-4: Selecting Access database Type in Magellan Project Properties

Click OK to save and apply your Magellan Project Properties changes.

4-2.4 Set Project Properties for the SQL Database

Select **Project** from the menu bar, and open the **Project Properties** as illustrated below in Figure 4-5.

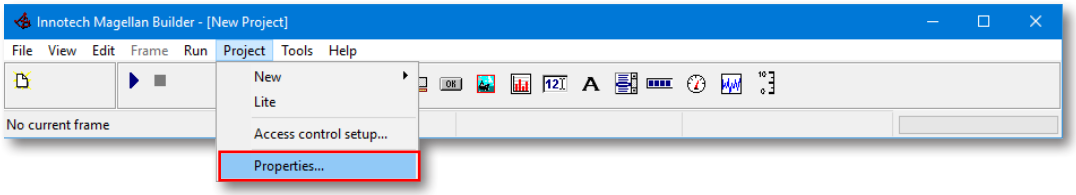

Figure 4-5: Open Magellan Project Properties

In the Project Properties menu, select the Database Server type. The default is No Database. Use the dropdown list to select a SQL database, as illustrated below in Figure 4-6.

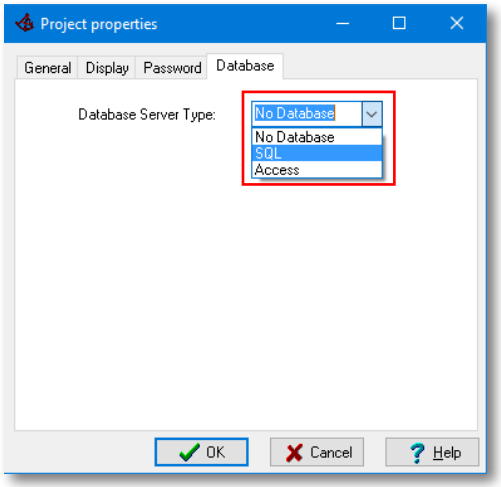

Figure 4-6: Selecting SQL database in Magellan Project Properties

Selecting a SQL Database will automatically open the Connection Settings window, allowing you to enter the details for the SQL Database connection, as illustrated on the next page in Figure 4-7.

In the Connection Settings window, enter the required SQL Database connection settings within each available field. The example below is suited for when connecting to the Innotech Chronicle database.

If using the default Chronicle Server or ATOM Package installation processes, the SQL Database will have been allocated the Database Name: ***GreenstarLogging*** *by default.*

For connection to the Innotech Chronicle database, enter the following:

Connection Name: Enter a name for the connection. **This is used only within Magellan but must be a single word with no spaces.**

Server Address: Enter the valid internal network DNS name or static IP address for the computer running the SQL Server; **for example** "**Computername\SQLExpress**".

External Address: Enter the valid external DNS name or external static IP address for the computer running the SQL Server; **for example** "**DNSName.domain.com**".

Database type (selection buttons): Select SQL Server Express to use eServer in collaboration with the Innotech Chronicle database (*recommended*). Select Access to use a legacy iComm database.

Database Name: Ensure this is set to **GreenstarLogging** in order to use the Innotech Chronicle database.

Requires Log-in: Enter the valid username and password for the SQL Server.

IMPORTANT

It is ***critical*** *that the settings entered in the Magellan Project and the Chronicle Server (which writes to the SQL Server database) exactly correspond. Refer to the representation below at Figure 4-7 for a guide on which fields relate directly.*

The use of the term localhost, or address 127.0.0.1 for any fields or settings is ***not recommended. Please use a valid DNS name or static IP address for all connection details****.*

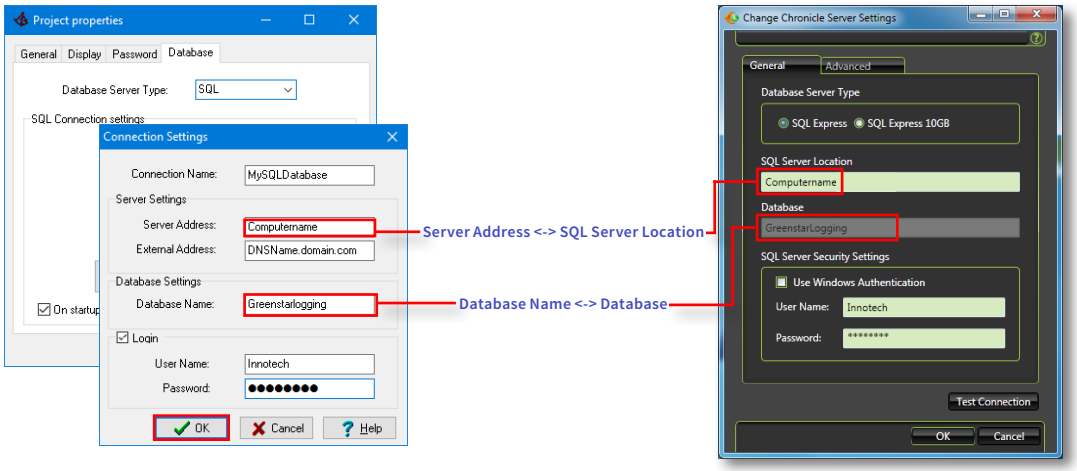

Figure 4-7: eServer and Chronicle Server Settings for the SQL Server

IMPORTANT

The internal and external Server address is to be the same when using v1.5

Click OK to save and apply your new SQL Server connection.

Upon creating the new SQL Server connection, the Project Properties window will list the connection. Up to 100 SQL database connections can be configured. Choose the default SQL Server connection as illustrated below in Figure 4-8.

Before applying, choose the enable automatic connection (recommended):

Automatically connect on startup: Select this option to automatically connect to the SQL Server database at startup of eServer (*recommended*). Alternatively, you can program a particular frame in your Magellan Project to launch the "*dbopen*" command to connect when the frame is launched. Refer to the Magellan Online Help for more information on the use of the "*dbopen*" command.

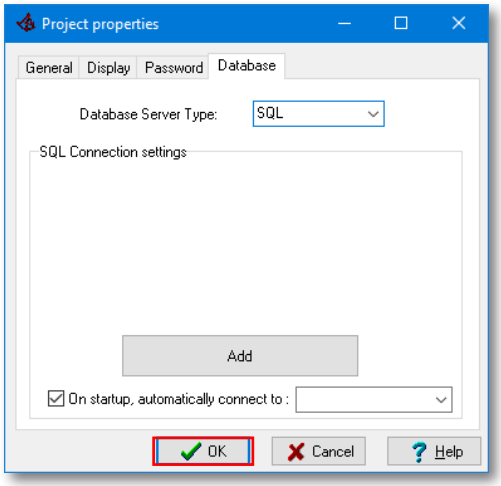

Figure 4-8: Open iComm Server Properties in the Magellan project

Click OK to save and apply your new Project Properties.

4-2.5 Set iComm Connection Properties

In the Magellan Project, navigate to the Points Manager and check all connection settings. Open the Properties of the site iComm Server, as illustrated below in Figure 4-9.

You may need to create a new iComm Server if none are visible in the project. From the drop down menu illustrated below in Figure 4-9, select New IO Server.

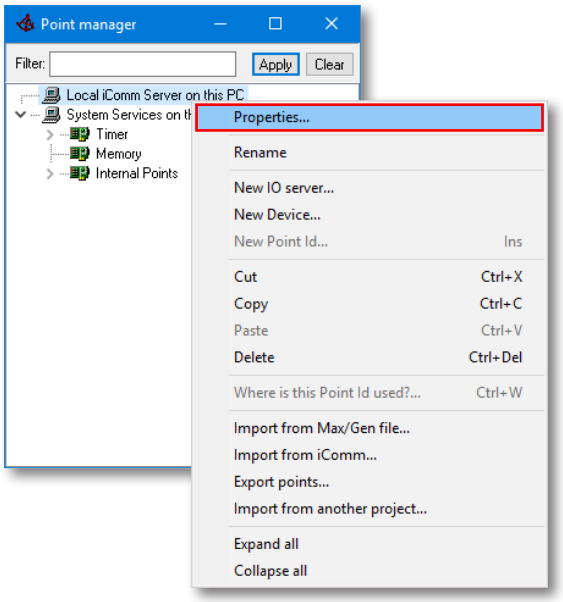

Figure 4-9: Point Properties

From the IO Server Properties General Tab, enter site specific IO Server Properties and connection information, as illustrated below in Figure 4-10. For example, enter the following:

IO Server Name: enter a name for your IO Server (for your reference)

Type of IO Server: Select the type of IO Server (iComm Server, or other)

Host Computer:- Enter the internal network DNS name or internal static IP address for the computer running the IO Server; for example "**iComm on Computername**".

External Address: Enter the valid external DNS name or external static IP address for the computer running the IO Server; for example "**DNSName.domain.com**".

IMPORTANT

*It is **critical** that the settings entered for Host Computer and IO Server Security exactly match settings in the Innotech Chronicle software (which writes to the SQL Server database). Refer to the representation at Figure 4-10 below for a guide on which fields relate directly.*

*The use of the term localhost, or address 127.0.0.1 for any fields or settings is **not recommended. Please use a valid DNS name or static IP address for all connection details.***

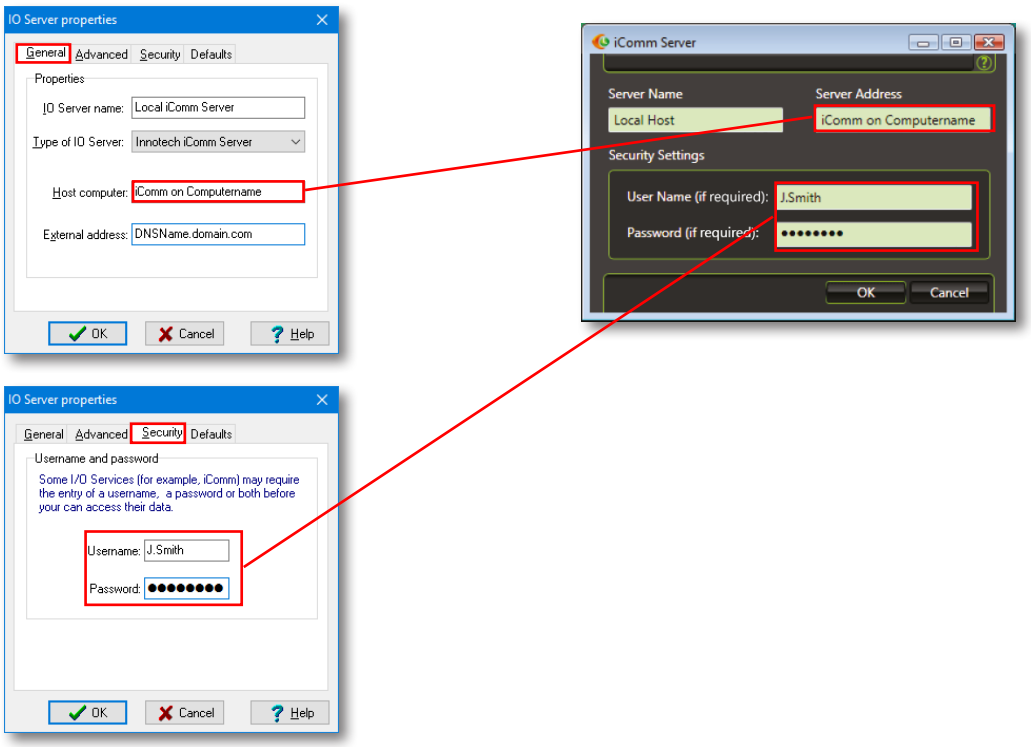

Figure 4-10: Check the eServer and Chronicle Server settings for the iComm Server

4-2.6 Set iComm Connection Properties

Once your iComm Server Settings are correct, select each Device and check the internal Device Settings correspond correctly with the iComm Server, as illustrated below in Figure 4-11, Figure 4-12 and Figure 4-13.

You can import devices and points via an iComm Server in the Points Manager. Right click on the iComm Server and select Import Points from iComm or import from a valid Genesis or MAXIM configuration file.

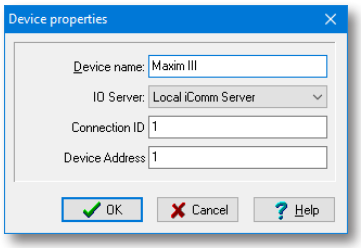

Figure 4-11: Example Device Properties for Connection 1, Device 1

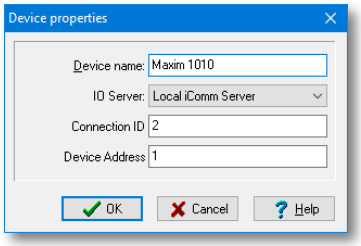

Figure 4-12: Example Device Properties for Connection 2, Device 1

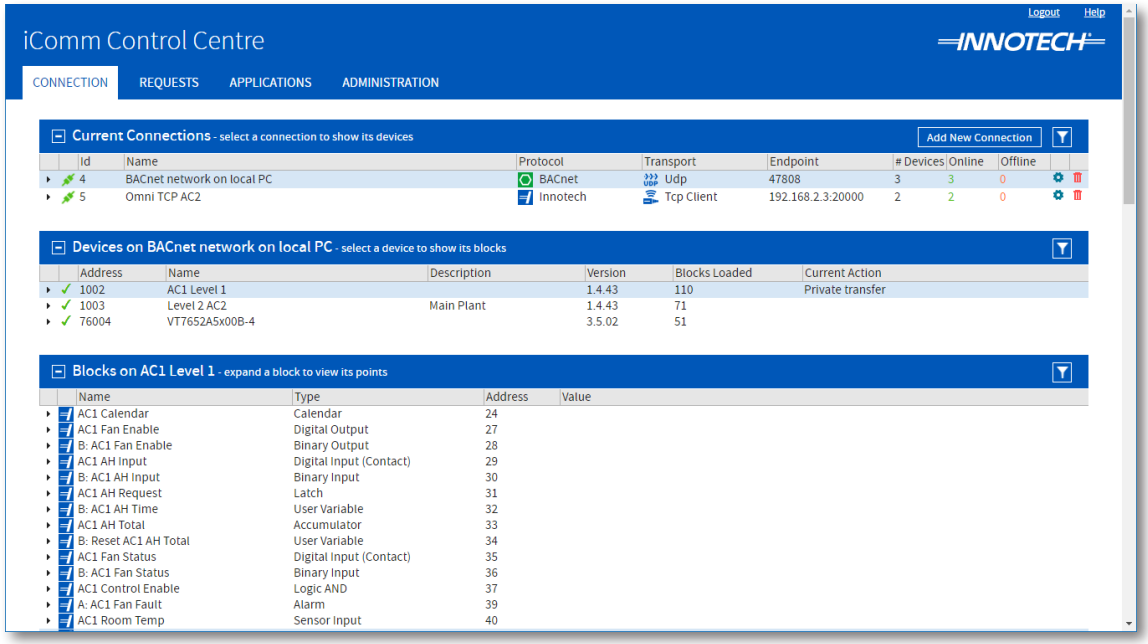

Figure 4-13: Validate your Device Settings with the iComm Server

4-2.7 Save Project Settings

Once all project settings have been updated, ensure to use Save As to save a new revision of the Magellan project file, as illustrated below in Figure 4-14.

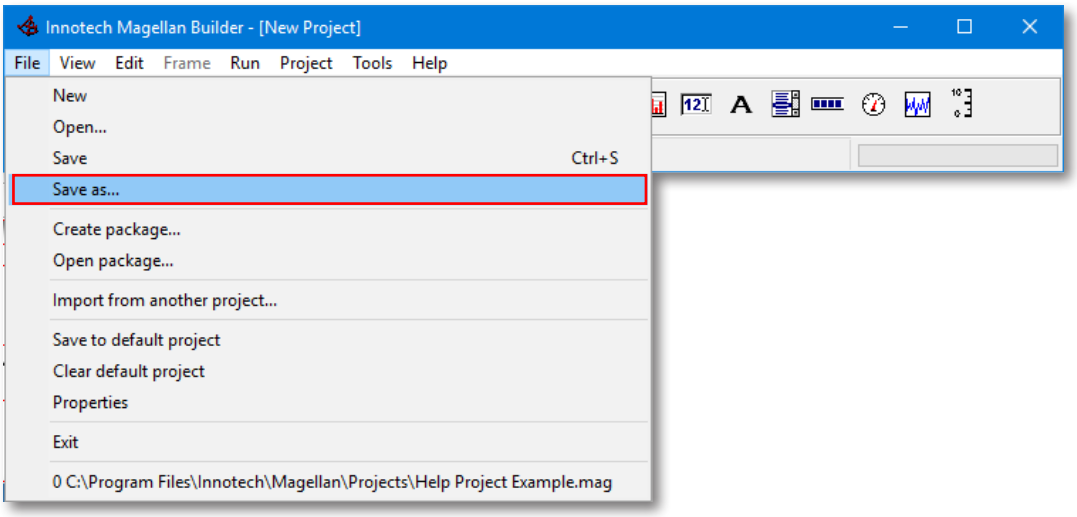

Figure 4-14: Save updated Magellan project settings

Relaunch eServer. Check that it is using the updated Magellan project. Ensure to create a new Magellan Package file for use with eServer, as illustrated below in Figure 4-15.

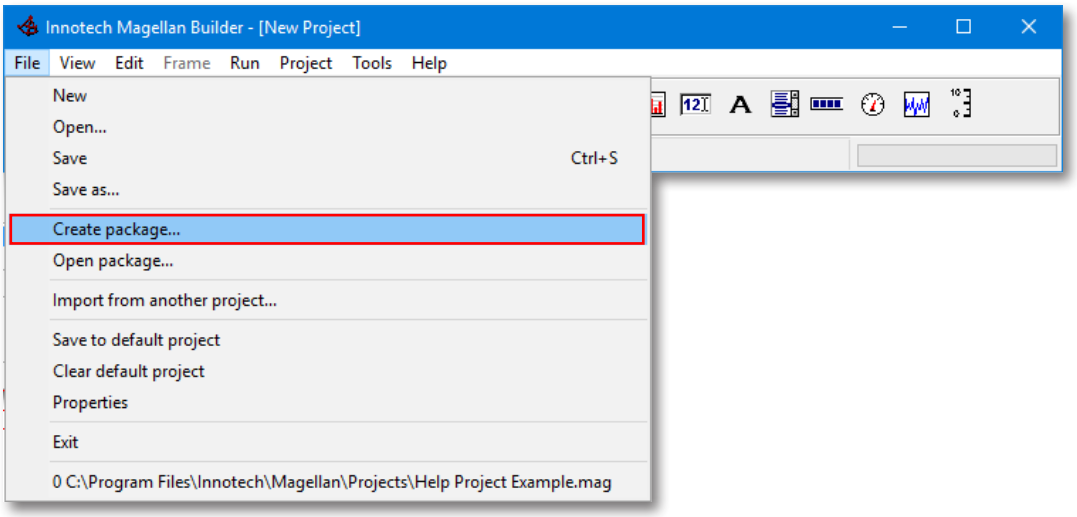

Figure 4-15: Create new Magellan package

IMPORTANT

*Before finishing, **ensure to remove the Magellan Builder security dongle**, leaving just the eServer security dongle to enable operation of the eServer software.*

4-3 Setup SQL Server Communications

4-3.1 Overview

The following information is intended to provide qualified technical personnel with the required settings for a manual setup of a Microsoft SQL Server 2016/2008 R2 Express Edition database.

SQL Server 2016/2008 R2 Express Edition is required for site which are using historic Trends or ATOM Reporting functionality.
Innotech recommends where possible to use the Innotech Chronicle Server Installation Package which ***automates the installation and configuration of SQL Server*** *to operate correctly with eServer. Contact Innotech Sales for more information on Chronicle, ATOM and other BMS solutions.* ***Note that this requires a computer which has not had any version of SQL Server installed previously.***

IMPORTANT

To integrate with an existing SQL Server, or upgrade to SQL Server 2016/2008 R2 Express Edition, consult with the Site IT Manager to ensure that the SQL Server settings are correctly configured as listed below in 4-3.2 Default SQL Server 2008 R2 Express Edition Settings*.*

4-3.2 Default SQL Server 2016/2008 R2 Express Edition Settings

IMPORTANT

Recommended for advanced users only!

Table 4-1: Default SQL Server 2016/2008 R2 Express Edition connection settings

Parameter	Recommended Setting	Notes
Default Instance	MSSQLSERVER	
Instance ID	MSSQLSERVER	
Authentication Mode	Mixed Mode	Required for remote access to SQL Server.
SQL Server Authentication	Enabled	
Communication Protocol Configuration ⓘ		
Shared Memory Protocol	Enabled	
Named Pipes Protocol	Enabled	
TCP/IP Protocol	Enabled	
UDP/IP Protocol Default Port	1434	Ensure no other applications are using port 1434. Ensure a firewall is not blocking incoming or outgoing traffic on port 1434.
VIA Protocol	Disabled	

ⓘ Use the SQL Server Configuration Manager to manage Communication Protocol settings. This tool is accessible from the Windows Start Menu once SQL Server Express Edition is installed.

4-4 Setup eServer Security, Access Control & Restarting

4-4.1 Overview

Information contained in this section includes configuration settings for security and access control allowing eServer to facilitate secure connection with connecting eServer Client computers.

4-4.2 Configure eServer Security

Start the **eServer** program (*it will minimize on the bottom right of your toolbar*). Double-click on the eServer icon on the toolbar to open the window. From the File Menu, select **Load Configuration** to select and load your eServer Project, as illustrated below in Figure 4-16.

Magellan saves the project by default as a .mag project. Use Magellan to export the project as a .mpk file, which is a packaged version for delivery, including all the project's graphical objects. ***The .mpk file is the file to open using eServer****.*

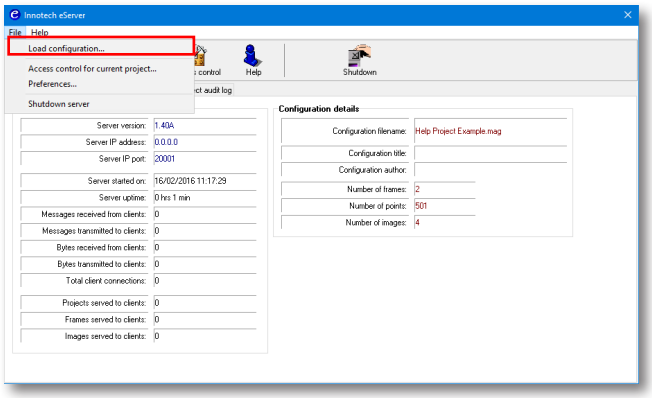

Figure 4-16: Load the Magellan project into eServer

To enable security for incoming connections, open the **Preferences** Menu, as illustrated below in Figure 4-17.

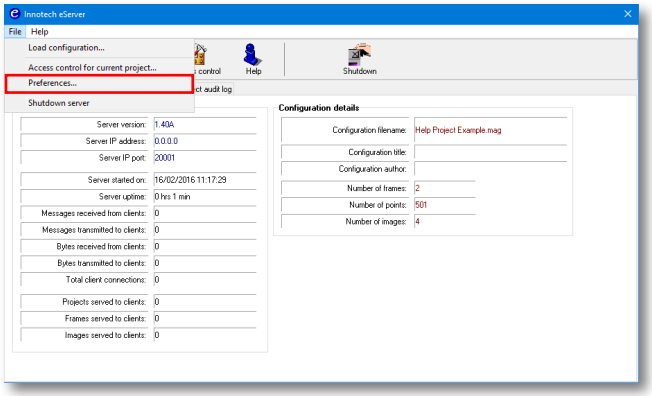

Figure 4-17: Open eServer Project Preferences

From the Preferences Menu, tick the **Enable security for connection to eServer** box and enter the required Username and Password, as illustrated below in Figure 4-18 (if you don't want extra eServer Connection security, leave it blank).

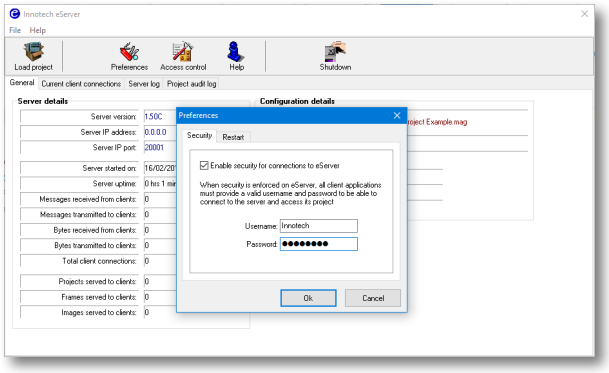

Figure 4-18: Configure eServer Connection Security

4-4.3 Setup eServer Automatic Restart

In eServer's Preferences, check the box on the Restart tab to automatically restart eServer at a specified time. Restarting eServer will refresh all the connections.

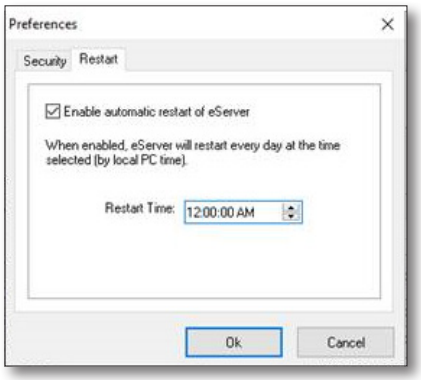

Figure 4-19: Preferences - Restart Tab

If using this feature, it is not compatible with RDP and it is recommended to disable RDP if being used. You can generally disable RDP by going into Control Panel -> System -> Remote Settings -> Don't Allow remote connections to this computer. Please note that machines joined to a Domain may have these settings overridden by group policy. In that case liaise with your IT department.

4-4.4 Enabling eServer Access Control

If you want **Access Control** on your project, go to **Access Control**. Tick the **Enable access control for this project** box, and enter the information, as illustrated below in Figure 4-21. If you don't want Access Control, leave it blank.

If your Magellan Project has access control setup already, simply check the box and this information will be added automatically.

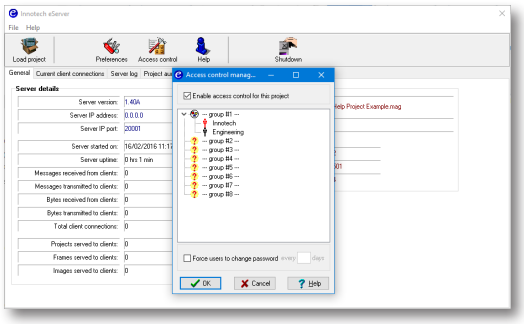

Figure 4-21: Enable eServer Access Control

4-4.5 Test eServer Connectivity

Open **Internet Explorer** and in the Address Bar, enter your computer name or IP Address and the HTML page name:

Example 1: **http://[Computer Name]/index.htm** Example 2: **http://[IP Address]/index.htm**

If Security is set up on the project, you will be required to enter the authentication details, as illustrated below in Figure 4-20.

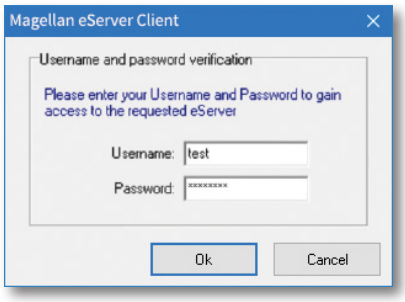

Figure 4-20: Entering Connection Authentication Details

You will need to allow downloading of the **Magellan ActiveX Control** if prompted. Follow all onscreen instructions to complete the test connection, and follow the steps outlined next in 4-5 - Setup of eServer Client Computer.

There is a an online troubleshooting guide included for any connecting eServer Client computers. This will help to resolve common connection problems such as Internet Explorer Security Settings which may block the installation of the Magellan ActiveX Control.

When you **exit** the project, Internet Explorer will still be open. Add the address to your Favourites so you don't need to enter it manually each time.

IMPORTANT

If a PC has previously connected to a v1.40 eServer the IE cache needs to be cleared before connecting to the v1.50 eServer so that the latest ActiveX files can be downloaded.

4-5 Setup of eServer Client Computer

4-5.1 Overview

eServer 1.50 or greater enables automatic configuration of eServer Client computers. Upon connection of an eServer Client Computer, eServer will automatically download and install the necessary ancillary files to complete the setup.

*Ensure that you are logged into the eServer Client computer as a **System Administrator**, and have a functional network connection to download and install necessary ancillary files from the eServer Host computer. Otherwise refer to Section 5 - General Troubleshooting Tips.*

These instructions detail the first connection of an eServer Client computer to a eServer Host computer running eServer 1.50 or greater. This will require the download and installation of the eServer Native Client and Magellan ActiveX Control. You will only be required to download and install these components the first time a Client computer connects to an eServer Host computer running eServer 1.50 or greater, unless a new version is installed on the eServer Host Computer.

4-5.2 Connection Steps

Follow all onscreen instructions during setup of connecting eServer Client computers. The most common issue faced with initial connection of eServer Client computers is ensuring that security settings are correct and that Internet Explorer is correctly shutdown and restarted when advised by onscreen instructions.

Launch Internet Explorer. In the **address bar**, enter the **specific DNS name or static IP address** or computer name of the eServer computer you are connecting to, as illustrated below in Figure 4-22.

Figure 4-22: Launch Internet Explorer and Connect to eServer Computer

From the Magellan ActiveX Control Setup page, click **Install** to install the updated Magellan ActiveX control on the computer, as illustrated below in Figure 4-23.

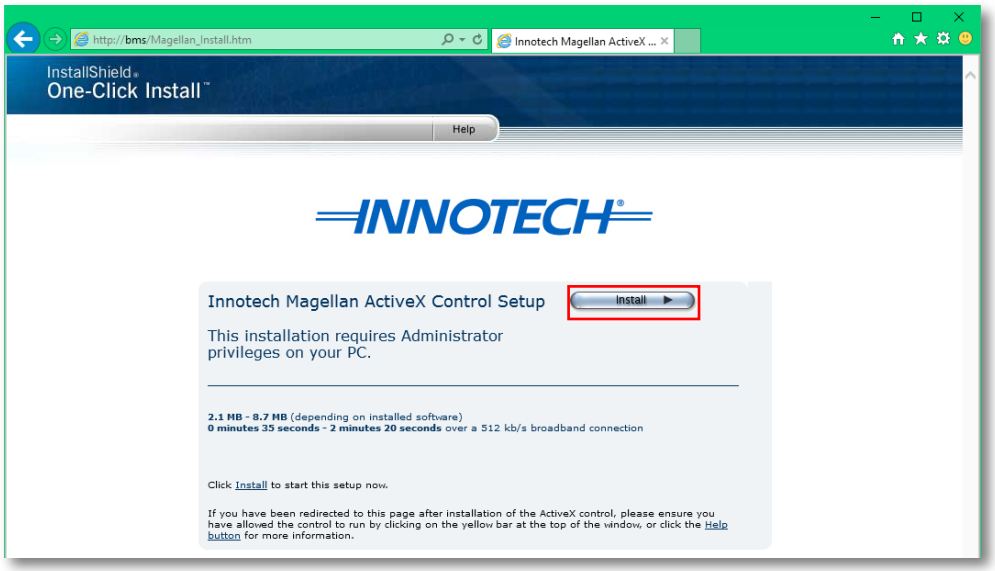

Figure 4-23: Install Magellan ActiveX Control

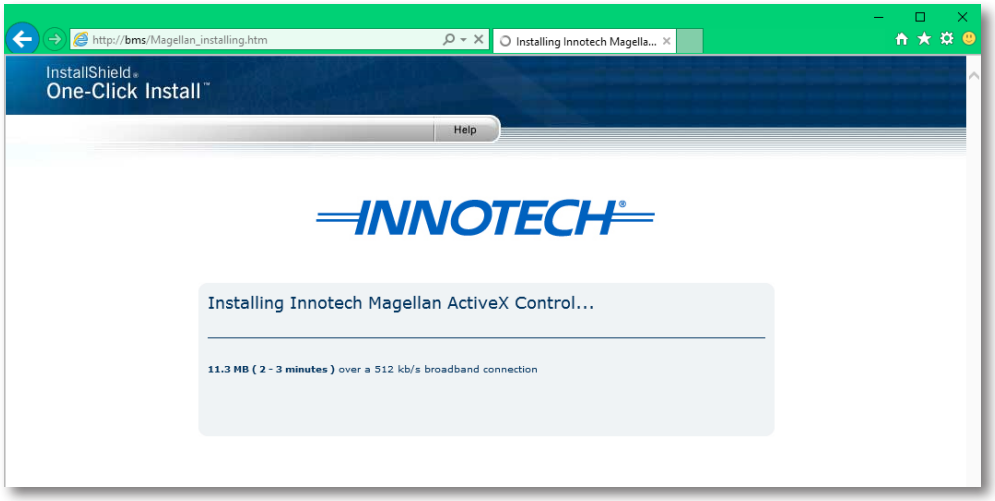

Figure 4-24: Installing Magellan ActiveX Control

Once installation has finished, click Finish and then navigate to the eServer computer to connect.

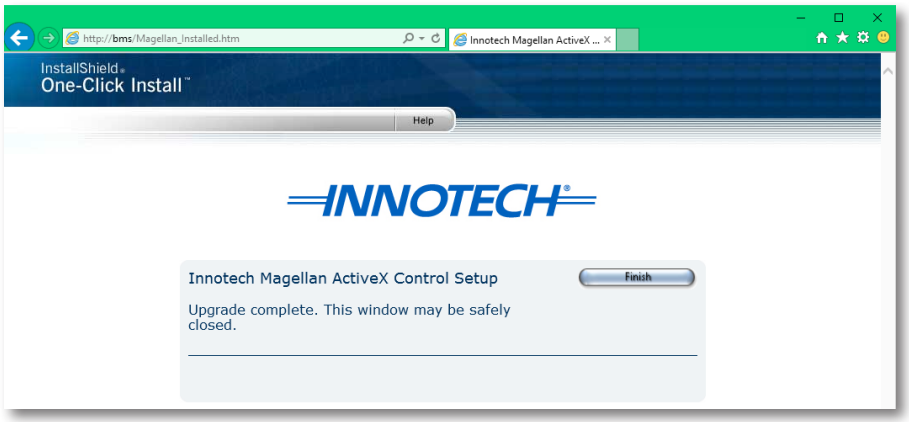

Figure 4-25: Finish Installation

4-5.2.1 How to disable the Project Loading Confirmation

Follow the steps below to disable the loading confirmation window shown in Figure 4-26.

1. Open the index.htm file located in the MyWebPages folder of the eServer Computer in a text editor such as Notepad.
2. Below the Control.DisplayHeight line add a new line with the text **control.Silent = 1** as shown below.
3. Save the file and when you load the project from the client computer, the confirmation should no longer be displayed.

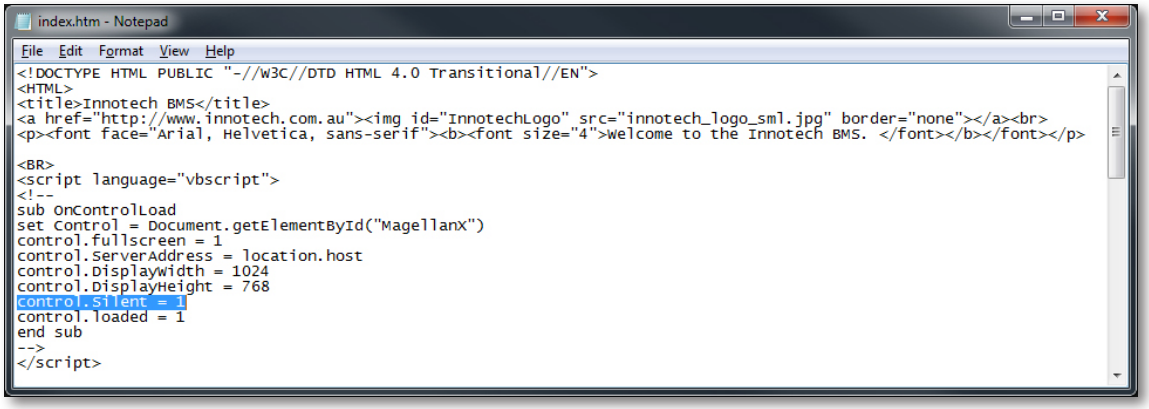

Figure 4-26: Index.htm file contents

4-5.3 Setup Crystal Reports Software on eServer Client Computer

4-5.3.1 Overview

eServer 1.50 or greater supports the generation of Crystal Reports. This requires the installation of the Crystal Reports Web Components software on the eServer Client computer.

The Crystal Reports Web Components software is only required for eServer Client computers which are connecting to an eServer 1.50 or greater and are requesting the generation of Crystal Reports. Note that the Crystal Reports Web Components are necessary for the generation of Crystal Reports using the Innotech ATOM software.

Installation of the Crystal Reports Web Components can be done during site commissioning; alternatively for computers which do not have the Crystal Reports Web Components installed, if required by eServer the user will be guided through the download and installation process.

IMPORTANT

*The Crystal Reports Web Components bundle is a **100MB file download**. Installing this software will require being logged in as a **System Administrator**.*

4-5.3.2 Manual Installation of Crystal Reports Web Components

Ensure to be logged into the computer as a System Administrator to install the Crystal Reports Web Components.

Select the Crystal Reports Web Components installation program, and double-click to launch. From the welcome screen, click **Next** to commence installation, as illustrated below in Figure 4-27.

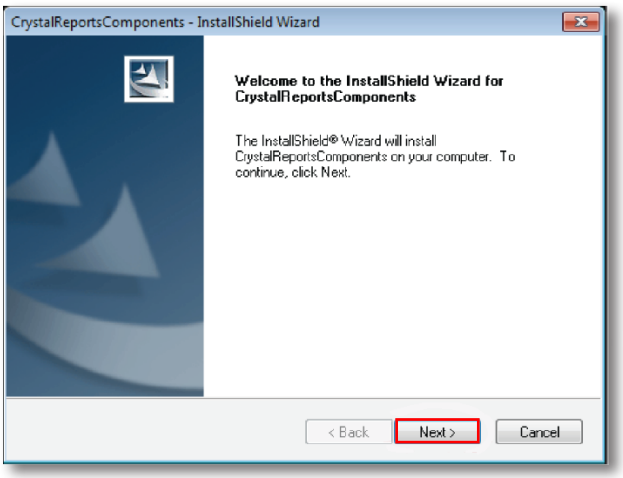

Figure 4-27: Launch the Crystal Reports Web Components installer

Choose the patch on the computer to install the Crystal Reports Web Components. It is recommended to install to the default location. Click **Next** to confirm installation path, as illustrated below in Figure 4-28.

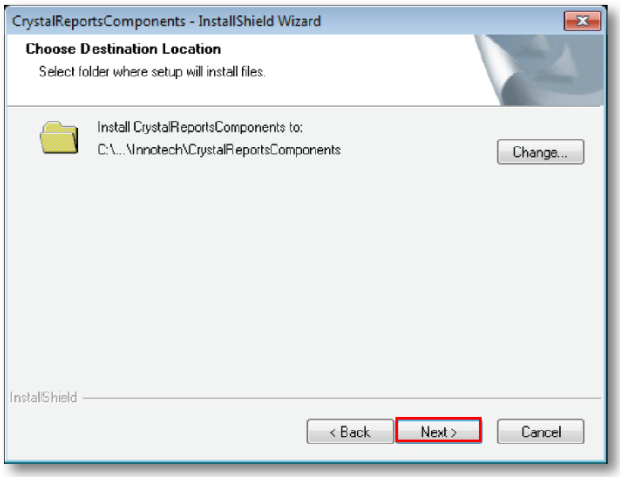

Figure 4-28: Confirm Installation Location for Crystal Reports Web Components

Click **Install** to install Crystal Reports Web Components, as illustrated below in Figure 4-29.

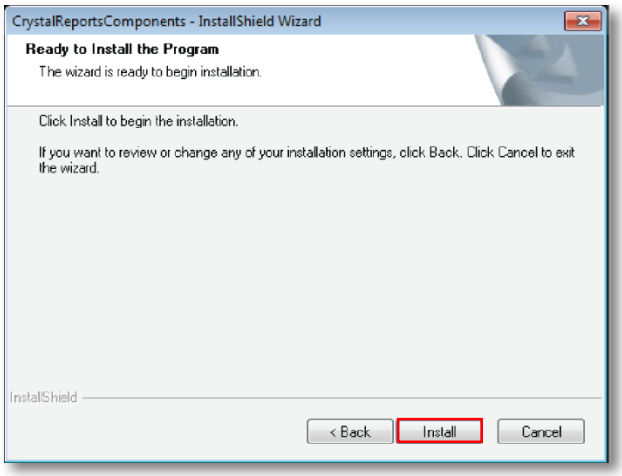

Figure 4-29: Commence Installation of Crystal Reports Web Components

Wait a few minutes while the software is installed, as illustrated below at Figure 4-30 and Figure 4-31.

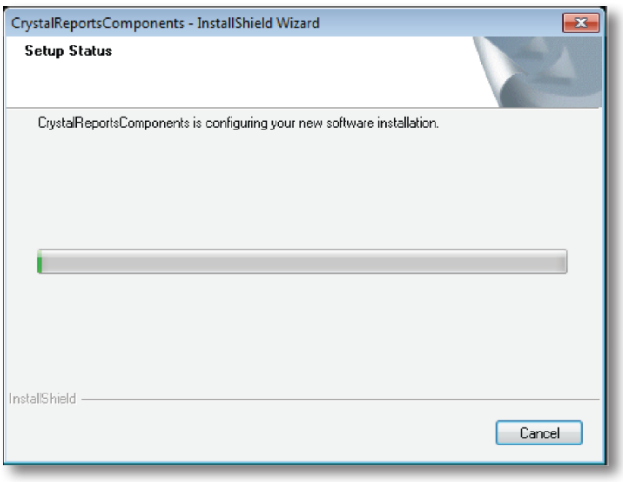

Figure 4-30: Crystal Reports Web Components Commencing Installation

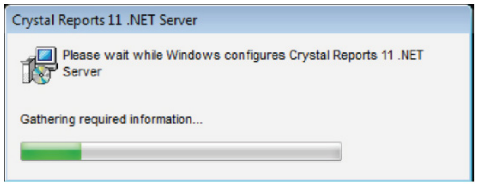

Figure 4-31: Crystal Reports Web Components Continuing Installation

Once installation is complete, click **Finish** to exit the Crystal Reports Web Components installation program, as illustrated below at Figure 4-32

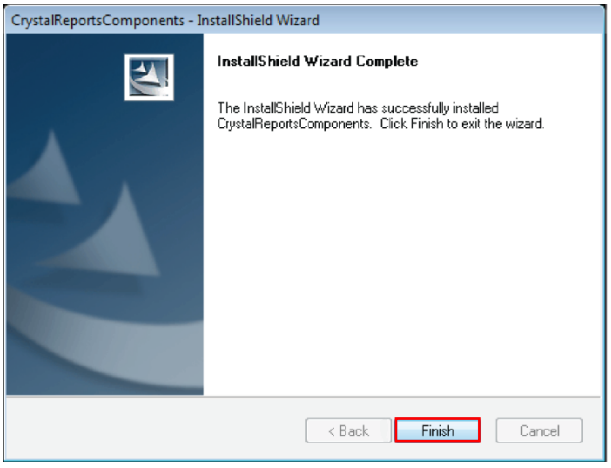

Figure 4-32: Crystal Reports Web Components Installation Complete

4-5.3.3 Automated Installation of Crystal Reports Web Components

An eServer Client computer that does not have the Crystal Reports Web Component installed is still able to connect and interact with an eServer Host computer. However, if a request if made by the client to generate a Crystal Report, the eServer Client computer will be required to download and install the required components from the Innotech website.

Ensure to be logged into the computer as a System Administrator to install the Crystal Reports Web Components.

If an eServer client proceeds to generate a Crystal Report, the client is guided through the process as described in this section. When the eServer Client requests the generation of a Crystal Report, an information window appears on the screen advising that additional components must be installed, as illustrated below at Figure 4-33.

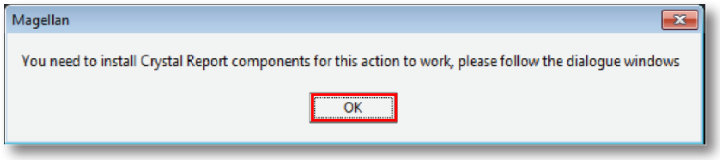

Figure 4-33: Message Advising that Crystal Reports Web Components are needed

From the File Download window, select **Run** to download and run the software, as illustrated below at Figure 4-34. Alternatively, you may want to save to file to use the downloaded installer on another eServer Client computer.

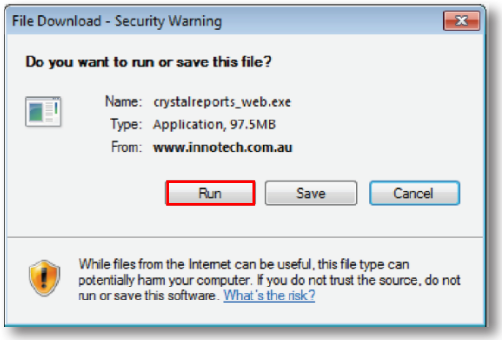

Figure 4-34: Select to Download the Crystal Reports Web Component

Wait a few minutes for the file to download, as illustrated below at Figure 4-35. Once complete, follow the steps outlined previously in 4-5.3.2 Manual Installation of Crystal Reports Web Components to implement the software setup.

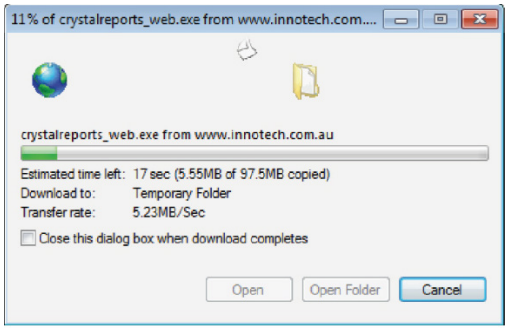

Figure 4-35: Downloading the Crystal Reports Web Component

Once the Crystal Reports Web Components has been installed, relaunch Internet Explorer and connect to the eServer Host computer to continue.

This page has been left intentionally blank.

eServer

SETUP AND SITE INSTALLATION INSTRUCTIONS

5 General Troubleshooting Tips

INNOTECH®

5-1 Introduction

This section provides general troubleshooting tips for some of the common problems that may be encountered during the eServer setup and configuration process. Please contact your IT department, or nearest Innotech office for further information.

IMPORTANT

Always consult with the Site IT Administrator for any special requirements needed for a particular IT network configuration.

5-1.1 Download and Install Unsigned ActiveX Controls

If the host computer running the eServer software and the client computer are on an isolated intranet without internet access, the eServer client computer will not be able to download and install the eServerNativeClient and ActiveX control from the host computer. Therefore you will have to configure Internet Explorer so that it can download and install unsigned ActiveX controls. You can do this by following the steps below.

Open Internet Options in Internet Explorer and click on Tools → Internet Options. From the *Security* tab in the Internet Options window, click on **Local intranet** and then click on **Custom level...** as illustrated below in Figure 5-1.

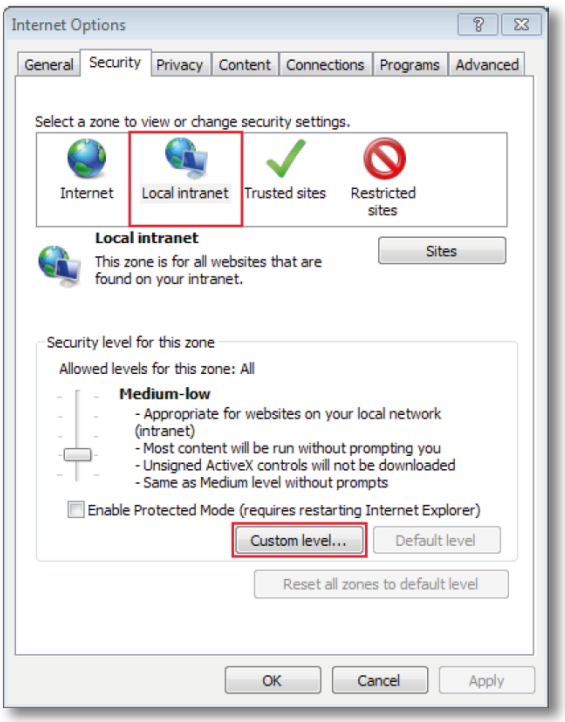

Figure 5-1: Local Intranet Settings in Internet Explorer

In the *Security Settings* window, scroll down to *Download unsigned ActiveX controls* and click on the radio button next to *Prompt* to select it, as illustrated in Figure 5-2.

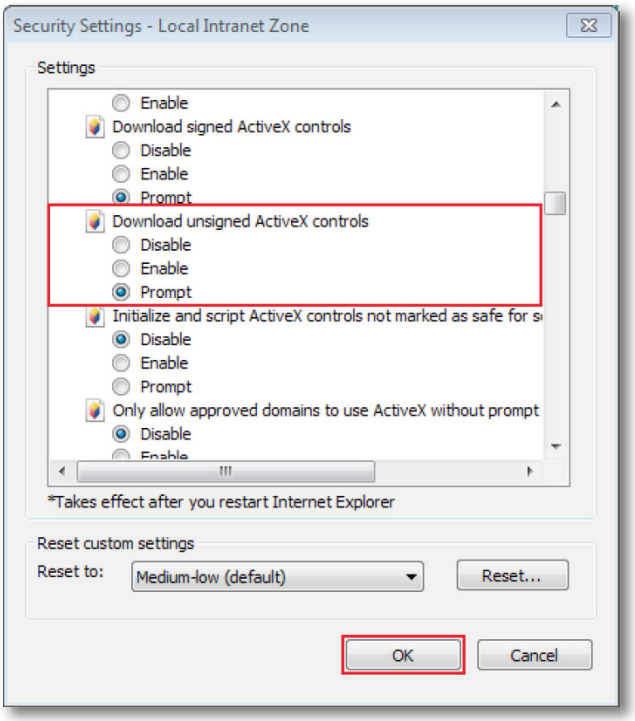

Figure 5-2: Configure IE to Download Unsigned ActiveX Controls

Click on **OK** to save your settings. Click **OK** again on the *Internet Options* window to exit and apply your settings.

5-1.2 Bypass Proxy Server Settings

If a site has a proxy server, and the local network is not set to bypass it, client computers attempting to access the eServer project on the host computer may not be able to download the latest ActiveX control. They will instead be redirected to the proxy server to download whatever version that is cached on the proxy server. This may be an older version than what is required for the client computer in order to access the eServer project correctly.

The workaround to this problem is to bypass the proxy server if the IP address requested by the client computer is on the local network. Follow the steps below to configure Internet Explorer to bypass the proxy server.

Open Internet Options in Internet Explorer and click on Tools → Internet Options. From the *Connections* tab in the Internet Options window, click on **LAN settings**, as illustrated in Figure 5-3.

IMPORTANT

Ensure to check with the Site IT Administrator before bypassing Proxy Settings, as this may cause ancillary connection issues for the computer.

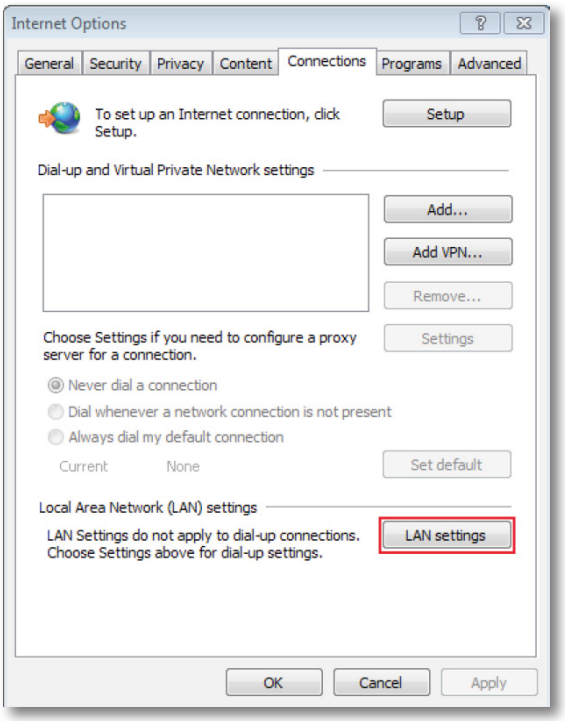

Figure 5-3: Configure LAN Settings in Internet Explorer

In the Local Area Network (LAN) Settings window, verify that the *Bypass proxy server for local addresses* box is checked and click on **Advanced**, as illustrated in Figure 5-4.

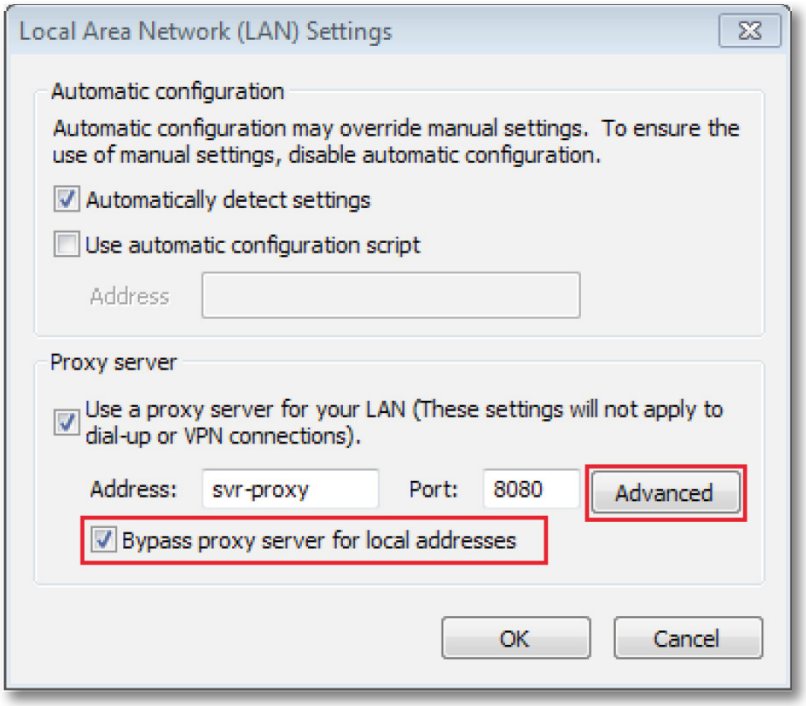

Figure 5-4: Bypass Proxy Server Settings in Internet Explorer

In the Proxy Settings window under *Exceptions*, add the desired IP range for which you want to bypass the proxy server, as illustrated in Figure 5-5. For example you can enter *http://192.168.1.** to bypass all IP addresses in this range.

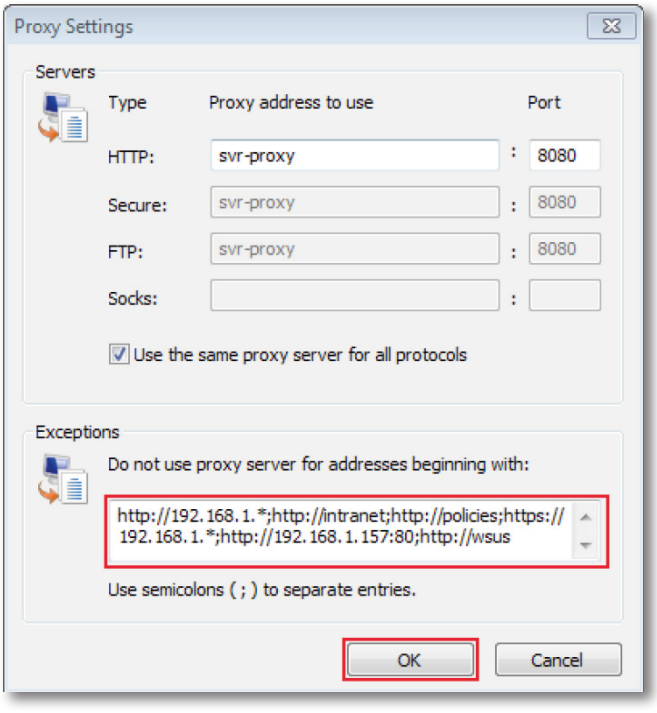

Figure 5-5: Enter Proxy Server Exceptions in Internet Explorer

Once you have entered the IP range into the *Exceptions* box, click **OK** to save your settings, and click **OK** on all subsequent windows to close them and apply your changes.

5-2 Internet Explorer Compatibility with eServer

5-2.1 Internet Explorer 11

- Type in your address in the address bar as per usual, if you see the “Internet Explorer 6 or above” screen click the Internet Explorer settings button (located under the close button, it looks like a cog) and select Compatibility View Settings. The address you are currently at, your eServer address, should be there ready to add. Click Add to add the address to the list.
- You can alternatively press ALT to show the menu bar. In the Tools menu, select Compatibility View Settings and add the address to the settings window.

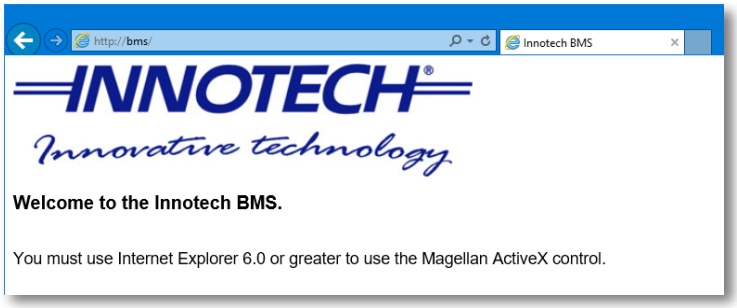

Figure 5-6: Internet Explorer 11 Before Settings Change

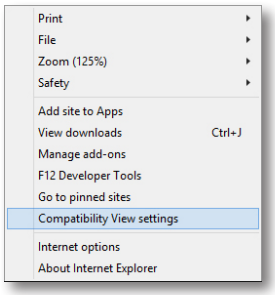

Figure 5-7: Internet Explorer 11 "Cog" Settings Menu

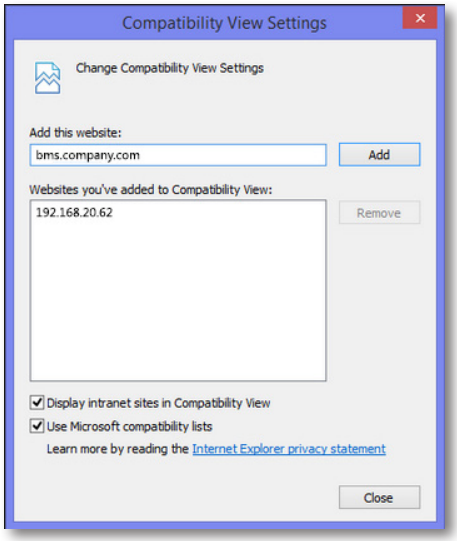

Figure 5-8: Internet Explorer 11 Compatibility View Settings

This page has been left intentionally blank.

Innotech Support

Innotech provides technical information on the Web to assist you with using its products.
At www.innotech.com, you can find technical manuals, user instructions, and data sheets for all our products.

For direct product support or product information, contact your local distributor, or an Innotech representative.

You can contact us via email, phone, or postal mail:

Website: www.innotech.com
Email: sales@innotech.com
Phone: +61 7 3421 9100
Mail: Innotech Control Systems
P.O. Box 292
Sunnybank
QLD 4109
Australia

