HIFIS

HOMELESS INDIVIDUALS AND FAMILIES INFORMATION SYSTEM

INSTALLATION GUIDE

VERSION 1.0

REACHING HOME | VERS UN CHEZ-SOI

Employment and Social Development Canada | Emploi et Développement social Canada

Canada

This publication is available for download at canada.ca/publicentre-ESDC. It is also available upon request in multiple formats (large print, Braille, MP3, audio CD, e-text CD, DAISY, or Accessible PDF), by contacting 1-800-O-Canada (1-800-622-6232). By teletypewriter (TTY), call 1-800-926-9105.

PDF
Cat. No.: Em12-56/3-2019E-PDF
ISBN/ISSN: 978-0-660-29936-5

ESDC
Cat. No. : SSD-221-03-19E

TABLE OF CONTENTS

GLOSSARY OF TERMS

Term	Definition
Admissions	The process of admitting an individual or family that is homeless or at-risk of homelessness into a service provider.
At-risk of Homelessness	Individuals or families who are not homeless, but whose current economic and/or housing situation is precarious or does not meet public health and safety standards.
Bed Selection	A graphical display of a shelter's rooms and beds.
Bulletin	A message that can be read by users who are logged in to HIFIS.
Case Management	Refers to intentional and collaborative service planning between service providers and their clients. The "intent" of the interactions differentiates various forms of case management. For example, case managers can specialize in the following: ■ **Service Navigation:** Connecting clients to appropriate services using information gathered through triage and assessment. Includes completing paperwork for various waiting lists and following up on referrals. ■ **Housing-Based Case Management**: Helping clients to reduce acuity in the areas of life that present risks to a tenancy. Includes arranging and coordinating a range of services to meet client needs.

Term	Definition
Chronic Homelessness	People who are currently experiencing homelessness and meet at least one of the following criteria: ■ have a total of at least six months (180 days) of homelessness over the past year; or ■ have recurrent experiences of homelessness over the past three years, with a cumulative duration of at least 18 months (546 days).
Client	An individual or family that is experiencing homelessness or at-risk of homelessness who has accessed or is currently accessing services provided by a service provider.
Client Consent Form	An agreement between the client and the service provider that provides the service provider consent on the collection, retention, and sharing of an individual's data.
Cluster	A functionality in HIFIS allowing the data of clients from specific service providers to be isolated. Service providers in clusters can only view data within their designated cluster.
Community Advisory Board (CAB)	Local organizing committee responsible for approving the Community Plan and recommending projects for funding to the Community Entity.
Community Data- Sharing Agreement (CDSA)	An agreement signed by service providers that governs data-sharing within a community. The CDSA outlines a common understanding of what information is to be shared and why, detailing privacy and security protocol decisions, the quality of data to be provided, data entry protocols and relevant data management practices.

Term	Definition
Contributing Factors	Life events that have played a role in leading the client to requiring assistance from a service provider.
Coordinated Access	A way for communities to bring consistency to the process by which people experiencing or at risk of homelessness access housing and related services within a geographic area. Core components of a strong Coordinated Access system include a Housing First approach; real-time data about the supply of and demand for housing resources; and a streamlined service-delivery approach with access points to service, a standardized workflow for triage and assessment; prioritization and vacancy matching and referral.
Custom Tables	HIFIS module that is used to create customized records for service providers whose needs exceed the defaults of the application. Custom tables are used to gather information on clients with user-created fields.
Data Provision Agreement (DPA)	An agreement between ESDC and a HIFIS Lead organization that authorizes ESDC's quarterly collection of the non-directly identifiable data-fields in exchange for HIFIS.
Family Head	Where individuals are part of a family, the Family Head is the person who has been identified as the lead for the family as a whole (e.g., the primary parent or guardian responsible for dependents).

Term	Definition
HIFIS Administrator	The role that is responsible for the administrative functions within HIFIS (e.g., configuration, data integrity, backups).
Homeless Individuals and Families Information System (HIFIS)	Developed by ESDC in collaboration with communities, HIFIS is a comprehensive data collection, reporting and case management system that supports the day-to-day operations of housing and homelessness response service providers. HIFIS is designed to support the implementation of Coordinated Access by allowing multiple service providers from the same community to access real-time data and refer clients to the appropriate services at the right time.
HIFIS Host	Organization that has the servers on which HIFIS is installed and where client information is stored.
HIFIS Lead	Depending on the context, refers to the organization or dedicated staff responsible for the initial set-up, implementation and ongoing maintenance of HIFIS.
HIFIS Program	A label or tag created by the community to group client transactions by category. For example, *HIFIS Programs* can be used to track similar kinds of services (e.g., shelter stays, youth programming or assistance provided during a natural disaster) or goods and services funded by the same source (e.g., certain supportive housing units in a building). Reports can be generated using *HIFIS programs*, summarizing service transactions either within or across HIFIS service providers.

Term	Definition
HIFIS Service Provider	Organized and logical "set of services" that is available to individuals and families. HIFIS Service Providers share client information based on their individualized access rights, which are assigned to specific staff roles in the housing and homelessness response system.
Homelessness Management Information System (HMIS)	A tool that captures records client-level data and manages service provider information over time within a housing and homelessness response system. The Homeless Individuals and Families Information System (HIFIS) is one type of HMIS.
Housing First	An approach that involves moving people experiencing homelessness — particularly people experiencing chronic homelessness —rapidly from the street or emergency shelters into stable and long-term housing, with supports.
Housing and Homelessness Response System	Refers to all the service providers within a geographic boundary that help individuals and families with their housing challenges. In an integrated system with Coordinated Access, service providers most often use the same Homeless Individuals and Families Information System (HIFIS) installation.
Life Events	Life Events are defined as discrete experiences that disrupt an individual's usual activities causing a substantial change and readjustment.
Local Help Desk	A service established by a community that supports HIFIS users to manage the system and resolve technical issues, including incident management, service requests, problem management, advance support, and release management.

Term	Definition
Look-up Tables	A functionality that is used to add, edit, or remove values that appear in the drop-down menus throughout HIFIS.
Modules	Key components of HIFIS organized by functions or similar types of service transactions (e.g., Case Management, Housing Placement, Directory of Services, Food Bank).
Person(s) with Lived Experience	Individual or family that has experienced homelessness.
Primary Service Provider	A service provider with the ability to modify the mandatory fields and look-up table values of service providers placed underneath it.
Privacy Assessment	Process used to determine how service delivery could affect the privacy of an individual or family, with the goal of ensuring that privacy issues are identified and resolved or mitigated.
Rights Templates	Functionality that allows an administrator to apply the same user rights to multiple HIFIS users depending upon their roles and/or responsibilities.
Service Provider	Organization in the housing and homelessness response system that has staff who directly interact with clients to help them address their housing challenges.
Service Prioritization Decision Assistance Tool (SPDAT)	An assessment tool for frontline workers developed by OrgCode Consulting to inform prioritization in a Coordinated Access system and also support case management.

Term	Definition
Super-user	A service provider's HIFIS specialist with special privileges needed to administer and maintain the system as well as train HIFIS users.
User Rights	Govern ways by which a user can access HIFIS modules and view information. Rights specify if a user can see, edit, and/or delete data.
Violence Against Women shelter (VAW)	A service provider that caters specifically to women and their children who are fleeing violence, or the threat of violence.
Vulnerability Index Assessment (VAT)	An assessment tool for frontline workers developed by Downtown Emergency Service Centre to measure a person's vulnerability, which could be used to prioritize who should receive service first.
Vulnerability Index – Service Prioritization Decision Assistance Tool (VI-SPDAT)	Self-reported survey used to quickly determine a client's acuity. This triage tool is not designed to provide extensive detail about a client's vulnerability. Results can be confirmed or refined through a full SPDAT assessment.

THE HIFIS TOOLKIT

Over the last two decades, the ways to measure the extent of homelessness have significantly evolved in Canada. The dedication of service providers and municipal and provincial governments to collect and share data through the Homeless Individuals and Families Information System (HIFIS) and Point-in-Time counts is at the centre of this success. When used jointly, these data collection efforts provide a comprehensive local and national picture of homelessness. For the first time in history, Canadians have quality data that supports policy and program development, as well as strategic planning in the homelessness sector.

As Canada is moving forward with the National Housing Strategy and Reaching Home: Canada's Homelessness Strategy, collecting, managing and sharing data becomes more important than ever to advance the collective understanding of homelessness and to support decision-making. In particular, Reaching Home emphasizes coordinated access and introduces a data-driven, client-centred approach to serve individuals and families experiencing or at risk of homelessness.

In this context, the Government of Canada is committed to continuously enhance HIFIS in order to support communities in their data collection and efforts to eliminate homelessness. Recognizing that HIFIS modernization is driven by the homelessness sector's needs, a National HIFIS working group was created in 2018 to leverage the expertise of communities and experts and help guide HIFIS enhancements.

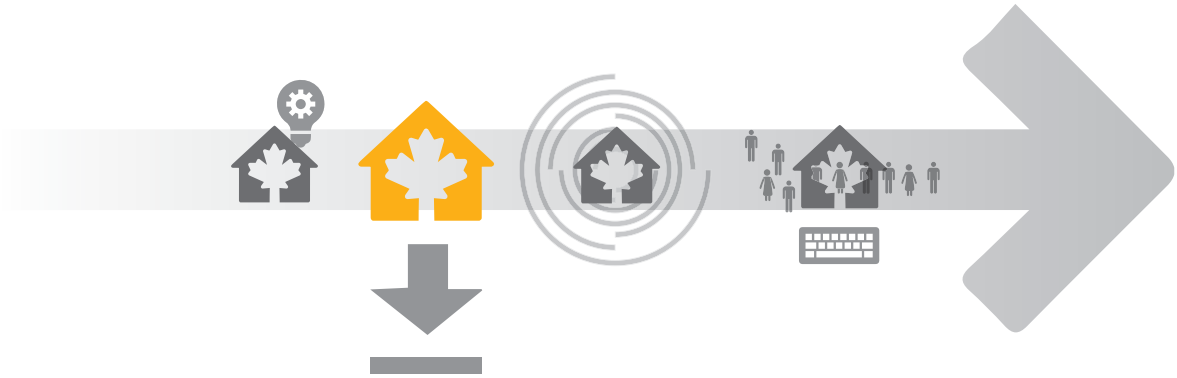
HIFIS is designed to support coordinated access by allowing multiple service providers from the same community to access real-time homelessness data through a community-wide system available via web-enabled devices, such as laptops, smartphones and tablets. HIFIS also allows communities to document the number, characteristics, and needs of homeless individuals and families, as well as the number of people receiving services.

To meet Reaching Home requirements and implement coordinated access systems, communities have to adapt their business model, which encompasses developing and adopting new governance frameworks and data management strategies. Doing so requires planning, committing resources and training to promote data literacy and instill a data-driven culture.

To assist communities in this transformation, ESDC has developed a HIFIS Toolkit composed of four guides. These guides cover the following topics:

1. ***Implementation*** – Provides guidance from planning to the deployment and maintenance of HIFIS.
2. ***Installation*** – Describes the technical requirements, architecture and installation procedures.
3. ***Configuration*** – Explains the configuration procedures to align with community's business needs.
4. ***User instruction*** – Gives a description of each function and how to use it.

Communities using HIFIS become part of a pan-Canadian movement that is building a data-driven culture to advance the understanding of homelessness in Canada. By working together, we can support the most vulnerable Canadians in providing access to safe, stable and affordable housing and reduce chronic homelessness nationally by 50% by 2027–2028.



ABOUT THE HIFIS INSTALLATION GUIDE

This *Installation Guide* is for the individual(s) responsible for the installation of HIFIS. The *Installation Guide* covers the minimum technical requirements for installation; the overall HIFIS system architecture; and the steps needed to install and configure HIFIS on a server.

The guide is divided into two parts: the first with the installation steps and explanation, and the second with complementary screenshots.

The *Installation Guide* can be used with the *Implementation Guide*, which covers the activities leading and following the installation of HIFIS, and the *Configuration Guide*, which provides the steps to configure HIFIS.

For more information to support the implementation and management of HIFIS, you can visit the Homelessness Learning Hub.

To stay connected and get the latest updates on HIFIS, please confirm your interest by sending your consent at support@hifis.ca.

For any questions or enquiries, you can contact the HIFIS Clients Support Centre at **1-866-324-2375** or support@HIFIS.ca

1.0 TECHNICAL REQUIREMENTS

This section of the guide covers the technical specifications that are required for an organization to host HIFIS.

The following table outlines the minimum technical requirements to install HIFIS.

Components	Software Requirements	Hardware Requirements	Hard Disk Space Requirements
Application	**Software** ■ Crystal Reports Runtime version 13.03500*; ■ SQL Server Native Client**	**Operating System** Windows Server 2012 or later*** **Processor** 2 GHz or faster **Memory** 2 GB RAM or more	**Hard Disk Space** 2 GB or more****
Server	**Software** See table on following page for required server roles and features	**Operating System** Windows Server 2012 or later*** **Processor** 2 GHz or faster **Memory:** 2 GB RAM or more	**Hard Disk Space:** 50 GB or more*****
Database	**Software**: ■ SQL Server Express 2012 or later with Advanced Services and Full-Text Search enabled; ■ Crystal Reports Runtime version 13.0.3500*; ■ SQL Server Native Client**; ■ Net Framework 3.5 SP1; ■ Windows Installer 4.5; ■ Windows PowerShell 1.0	**Operating System** Windows Server 2012 R2 or later*** **Processor** 2 GHz or faster **Memory** 2 GB RAM or more	**Hard Disk Space:** 10 GB hard disk space or more*****

Disclaimer Notes:

** The SQL Server Native Client version depends on the version of SQL Server installed.

*** As the OS version changes, the rest of the requirements and recommendations will increase.

**** Use of multiple HIFIS4 modules may require additional storage requirements and active storage availability should be review routinely.

***** Microsoft online documentation for minimum requirements must be evaluated depending on the software installed.

SERVER SOFTWARE

The following roles and features are based on a Windows Server 2016 installation, required roles/ features remain consistent but versions may differ.

Required Server Roles	Required Server Features
■ File and Storage Services Storage Services ■ Web Server (IIS) ■ Web Server ■ Common HTTP Features ■ Default Document ■ Directory Browsing ■ HTTP Errors ■ Static Content ■ Health and Diagnostics ■ HTTP Logging ■ Performance ■ Static Content Compression ■ Security ■ Request Filtering ■ Application Development ■ NET Extensibility 4.6 ■ ASP.NET 4.6 ■ ISAPI Extensions ■ ISAPI Filters ■ Management Tools ■ IIS Management Console	■ NET Framework 4.6 Features ■ NET Framework 4.6 ■ ASP.NET 4.6 ■ WCF Services ■ HTTP Activation ■ TCP Port Sharing ■ SMB 1.0/CIFS File Sharing Support ■ Windows Defender Features ■ Windows Defender ■ GUI for Windows Defender ■ Windows PowerShell ■ Windows PowerShell 5.1 ■ Windows PowerShell ISE ■ Windows Process Activation Service ■ Process Model ■ Configuration APIs ■ WoW64 Support

2.0 HIFIS SYSTEM ARCHITECTURE

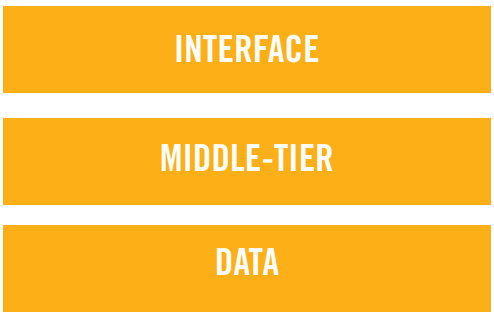
This section explains the architecture, the design and deployment scenarios. The first scenario outlined in this guide is the recommended deployment option. Section 3 provides the step-by-step procedure required for the recommended deployment scenario.

While other deployment options are outlined in this guide, there are no step-by-step installation procedures for those scenarios.

2.1 SYSTEM DESIGN

HIFIS 4 is comprised of several distinct components with a design that can accommodate a variety of deployment configurations and implementation scenarios. The core components are representative of those common to a typical multi-tiered enterprise system and consist of a presentation layer, a business middle-tier and an underlying data store.

Figure 1 – HIFIS 4 System Design Layers



2.1.1. Presentation Interface

The Presentation Interface consists of a web application which users see and with which they interact on a web browser. This allows users to access HIFIS from any web-enabled device with a compatible web browser and network access to the HIFIS web-application server.

The web application uses a user interface framework called the Web Experience Toolkit[1] (WET) and a default theme that can be modified or replaced to customize the look and feel of HIFIS.

The web application also includes a web-based Crystal Reports runtime engine to generate and display reports created with Crystal Reports. HIFIS ships with a series of reports included, but with Crystal Reports you can also create new reports or edit existing reports and upload them directly into HIFIS.

The Presentation layer does not contain any application logic except that which is required for correctly displaying information for the user. It depends on the Middle-Tier component to handle application logic and information.

2.1.2 Middle-Tier

The HIFIS 4 Middle-Tier is a service-oriented business component. It consists of a series of hosted web services that implement all of the HIFIS business logic and handle authentication. Because HIFIS 4 is service-oriented with

[1] Web Experience Toolkit. http://wet-boew.github.io/

web services that encapsulate the rules and behaviours of the application. It is adaptable to complex operational environments. Access to the web services is also configurable at the hosting level and within the HIFIS application itself to control and monitor what systems are accessing services, and what activities are taking place. Since the HIFIS web application is built on these same services, the behaviour of the HIFIS web application and a third-party system using the same services will be the same.

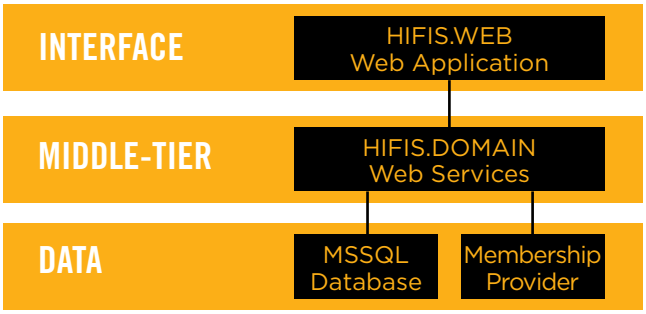
2.1.3. Database

The Database layer of the system represents the lowest level component and contains the actual data for HIFIS. While the initial release of HIFIS uses a Microsoft SQL database, it can also be deployed with alternative database vendors.

2.2. TECHNICAL SYSTEM ARCHITECTURE

HIFIS is organized in a hierarchical structure, ranging from the user interface to the underlying database. Each of these layers has one or more software components that must be deployed and configured. Here, we will examine each layer's components and the information necessary for deployment planning.

Figure 2 – HIFIS 4 System Design Layers with Technical Components



2.2.1. HIFIS.WEB

The front facing web application in the presentation layer is represented by the HIFIS.WEB component. HIFIS.WEB is a Microsoft .NET Framework 4.0 MVC 4 web application that must be hosted in Internet Information Services (IIS) 7 or above. As per the system's design, HIFIS.WEB does not include any of the formal HIFIS business logic, it is simply a user interface for interacting with the web services hosted in the middle-tier to perform the system operations and display the results. Consequently, much of the configuration effort of setting up the HIFIS.WEB application in IIS is configuring the service references and bindings in the web.config file.

Since it is a Microsoft MVC 4[2] web application, when deploying the HIFIS.WEB web application, you may choose to install MVC 4 in the Global Assembly Cache (GAC) of the IIS server, or deploy the MVC 4 libraries in the HIFIS.WEB Bin folder. All other libraries and dependencies are included in the application deployment folders except Crystal Reports.

[2] ASP.NET MVC 4, http://www.asp.net/mvc/mvc4

Crystal Reports is used as the runtime report engine in HIFIS.WEB and can only be installed in the GAC. If Crystal Reports is not already installed on the server, the HIFIS.WEB installation package provides an installer for the required Crystal Reports runtime engine library files.

Customizing the user interface can be achieved through several means. Since HIFIS.WEB is an MVC 4 application, each of the web views is represented by .cshtml files in the View folder of the deployment location. These files contain a combination of html, JavaScript and a special view syntax called Razor, and each can be modified to alter the way HIFIS.WEB displays information in the web browser. Be aware that modifying these files could break your HIFIS.WEB application and should only be attempted by those with explicit knowledge of the .NET MVC framework and the Razor syntax. You can learn about MVC and Razor from the Microsoft website.

HIFIS.WEB also uses an interface toolkit called WET. It can be found in the content folder of the HIFIS.WEB web application deployment folder. WET consists of a series of CSS and JavaScript files to provide a suite of interface components that are used throughout the HIFIS.WEB. As with modifying the .cshtml files in the View folder, changes to most of the files in WET could break the HIFIS.WEB web application without a solid understanding of WET in general, CSS, and JavaScript. The best way to implement your own look and feel for HIFIS.WEB is to use one of the provided WET themes and modify it to meet your requirements, then deploy it in the content folder of your HIFIS.WEB installation. You can learn about WET by visiting its documentation website[3].

2.2.2. HIFIS.DOMAIN

The middle-tier component, called HIFIS.DOMAIN, consist of a series of Microsoft .NET Windows Communication Foundation (WCF) web services that provide application logic functionality and data access to the HIFIS data for applications, like the HIFIS.WEB web application. HIFIS.DOMAIN deploys similarly to HIFIS.WEB, into an IIS application folder and is configured in much the same way through an app.config file. As with HIFIS.WEB, the bulk of the configuration is related to properly setting up the service endpoints and bindings. Because HIFIS.DOMAIN deploys as a separate component, it can be deployed to a different physical server instance than was used for HIFIS.WEB. HIFIS.DOMAIN also handles authentication, which does require that you also configure a membership provider[4] in the app.config file.

HIFIS.DOMAIN must also include an installation of a Crystal Reports Runtime Engine in order to respond to report requests from HIFIS.WEB. A key strategy in the design of HIFIS 4 was to eliminate direct access to the HIFIS database by any components outside of the middle-tier web services. Crystal Reports, however, does require direct access to the underlying database in order to generate report results. To resolve this dependency on direct database access, HIFIS.DOMAIN was designed with the ability to run Crystal Reports in the middle-tier environment with managed access to the database. The report results are then packaged and provided through the reporting web services to HIFIS.WEB to be displayed in a browser. Since the report is generated in the middle-tier, but

[3] Web Experience Toolkit, http://wet-boew.github.io/wet-boew/index.html

[3] Managing Users by Using Membership, http://msdn.microsoft.com/en-us/library/tw292whz(v=vs.100).aspx

displayed in the presentation level, the runtime engine is required in both places.

An existing or alternate installation of Crystal Reports can be used in either HIFIS.WEB or HIFIS.DOMAIN as long as they both support Crystal Reports 2008 report format or better.

2.2.3. Database

As it has been indicated already, HIFIS deploys with a Microsoft SQL Server database by default for both the HIFIS database and the membership provider. Like HIFIS.DOMAIN, because the database itself is a separate component, it can also be deployed on a different physical server from HIFIS.WEB and HIFIS.DOMAIN.

By default, HIFIS uses Microsoft SQL Server 2008 R2 (with Advanced Services if using the Express edition). If a compatible SQL server already exists on the infrastructure being used for HIFIS, you could configure your deployment to utilize the existing instance and simply create a new database for the deployment. HIFIS includes the necessary scripts in the installer to create both the initial HIFIS database and a membership provider database in a Microsoft SQL environment.

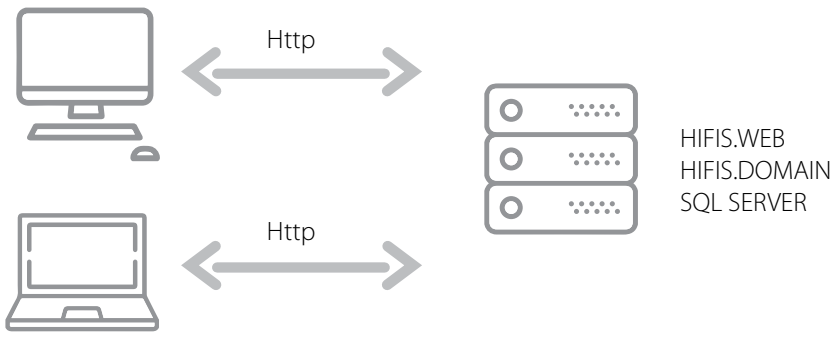
.

2.3. DEPLOYMENT SCENARIOS

2.3.1. Single Server

The HIFIS web application follows a service-oriented architecture (SOA) and therefore provides freedom with respect to how the components deploy. The most common deployment scenario is to place everything on a single server in a private network. This means that HIFIS.WEB and HIFIS.DOMAIN are installed on a single instance of IIS on a Windows server, along with the database.

Figure 3 – Single Server Deployment



[5] A service-oriented architecture (SOA) refers to the design of software functions that can be deployed and accessed remotely by an independent system. This separation allows for flexibility in the deployment of HIFIS and provides non-HIFIS systems access to the underlying HIFIS system separate from the HIFIS web application.

The interactions between the web application, services, and database are all occurring on the same physical server with no information being shared across a network, which, in turn, mitigates any security risks with information being transmitted over a network. Users accessing the web application however, would be transmitting information between the server and their device with a web browser. Your own circumstances and risk tolerance and/or security practices will determine whether you need to take steps to ensure secure communications between clients and the server on a private, secure network.

2.3.2. Distributed Instances

In a distributed configuration, HIFIS.WEB and HIFIS.DOMAIN can be separated and installed on separate instances of IIS on different physical servers.

Separating the components on a network may introduce a potential performance penalty since data now has to travel across the network twice: once between HIFIS.DOMAIN and the HIFIS.WEB web application, and again to the user's web browser. To minimize any delays, the components have been designed to perform operations simultaneously, where possible, and to ensure that only data necessary to satisfy a user's request travels between the HIFIS.DOMAIN web services and the HIFIS.WEB application.

This configuration can also be leveraged to minimize the exposure of the core HIFIS.DOMAIN web services and data to end users, while simultaneously enhancing the end user's experience. Consider the following scenario:

Figure 4 – Distributed Server Deployment

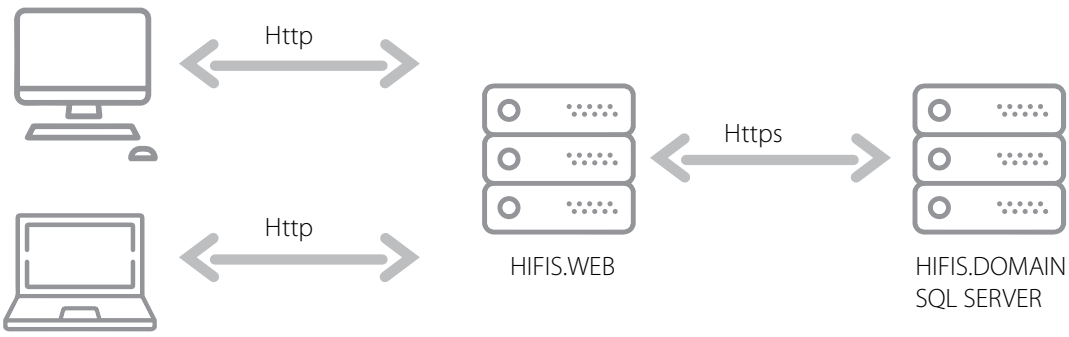
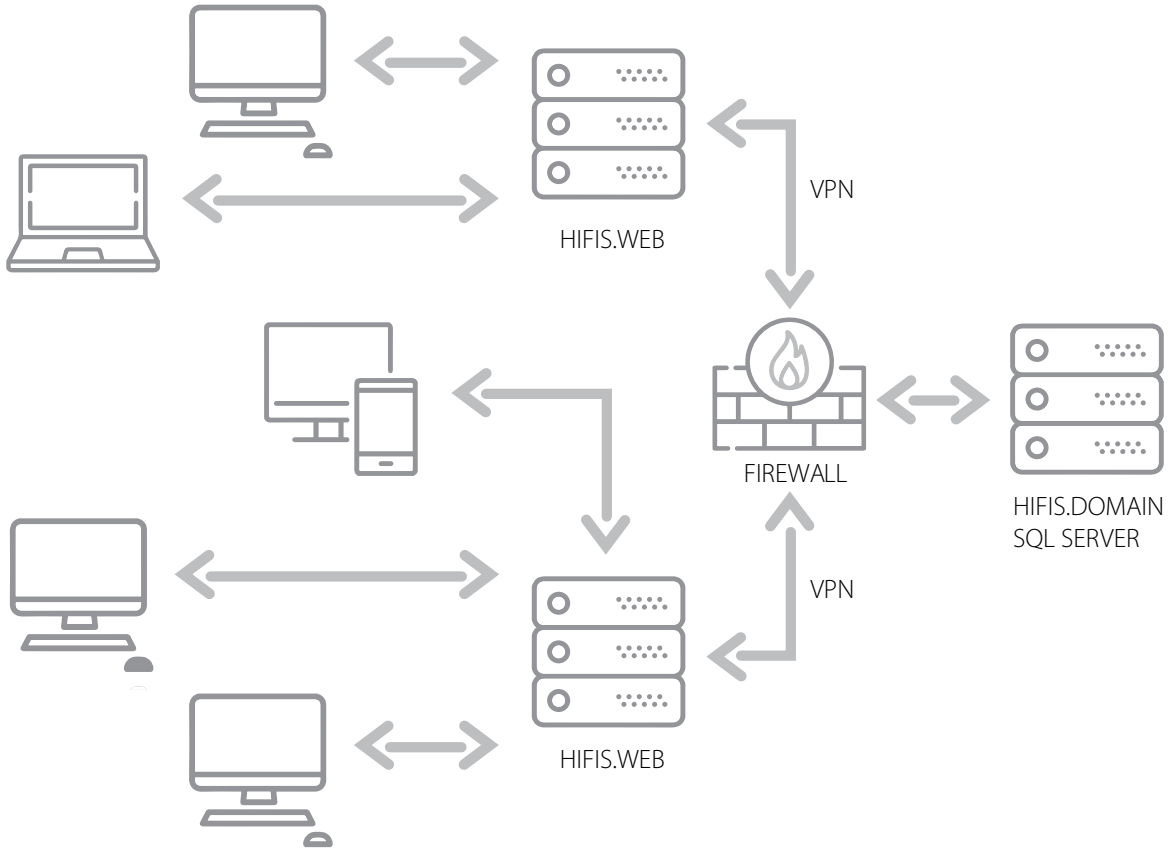


Figure 5 – Distributed Server Deployment with Multiple Instances



In this case, a central authority is hosting the HIFIS.DOMAIN web services with the users of the HIFIS.WEB web application on external private networks. The central authority minimizes exposure of its infrastructure by providing access for HIFIS.DOMAIN to the external servers hosting HIFIS.WEB over a secure connection, such as a virtual private network (VPN). In turn, the HIFIS.WEB servers provide local access to the HIFIS.WEB web application for clients on their private networks.

Also, the HIFIS.WEB web application component can be customized so users on each of the networks are presented with a version of HIFIS that is themed and customized according to their needs and operating environment, all while remaining part of the same integrated system.

2.4. AUTHENTICATION, AUTHORIZATION AND SECURITY

The default installation and deployment of HIFIS 4 includes everything needed for authentication, but there are many ways this can be configured to meet your environment and operational requirements.

Before considering these concepts, here is a standard workflow for HIFIS 4:

- A user navigates to the login URL of the HIFIS.WEB web application.
- HIFIS.WEB returns a login web form requesting the username and password.
- The user enters a username and password and submits the web form.
- HIFIS.WEB passes the login credentials to the HIFIS.DOMAIN authentication service for authentication.
- HIFIS.DOMAIN uses the configured membership provider to authenticate the credentials. If they are valid, the service constructs an encrypted security token and passes it back to HIFIS.WEB.

(If the credentials failed to authenticate, HIFIS.DOMAIN will respond to HIFIS.WEB with a validation error.)

- HIFIS.WEB receives the security token and can now use this to access other services in HIFIS.DOMAIN.
- The user navigates to a web page in HIFIS.WEB that requires information from HIFIS.DOMAIN.
- HIFIS.WEB passes the security token to HIFIS.DOMAIN through the desired service as a parameter in the service operation requesting data.
- HIFIS.DOMAIN uses the security token to determine if this is a valid request from an authenticated user. If it is, it proceeds to handle the service request and responds to HIFIS.WEB with the requested data from the database (if the security token is not valid it will respond with a validation error).

2.4.1. Authentication

Authentication refers to verifying that the login credentials provided in order to access the system are valid. In HIFIS.DOMAIN, there is a membership provider configured to handle user authentication. The process for authentication in HIFIS is the same for both a user and a system — a username and a password are passed to an authentication web service that will access the configured membership provider to validate the credentials. If they are valid, a special security token is created by the authentication web service and returned to the caller. This security token is then passed by the caller in subsequent service calls to interact with the HIFIS services. This token is valid until it either times out or the application revokes its authorization.

The .NET framework provides two membership providers, one for SQL and one for Active Directory. HIFIS uses the SQL provider by default so that user account information is stored in an SQL database. The SQL membership provider is also specifically designed for use with a Microsoft SQL database, which is also the default database platform for HIFIS. By default, HIFIS is configured to use the same database for both the HIFIS data and the membership provider data. If you want your HIFIS users to log in with their credentials from Active Directory, you can edit the app.config file to use the Active Directory membership provider and configure its settings according to your information.

If you have other requirements not met by these configuration options, you can choose to create a custom membership provider. This requires writing .NET code to implement the .NET System.Web.Security.Membership interface for a custom provider, deploying your custom library to the HIFIS.DOMAIN bin folder in your IIS deployment, and editing the app.config file to use your custom implementation. In this way you can create an authentication component for your HIFIS deployment that uses whatever you require, such as a database from another vendor, or some other mechanism altogether.

2.4.2. Two-Factor Authentication

In addition to the configurable membership provider, HIFIS also supports the integration of two-factor authentication. Two-factor authentication, when enabled, requires the user logging in to provide an additional piece of security information. Normally, this information will only be accessible by the user through an external mechanism such as a security key fob or a cell phone. HIFIS includes hooks to trigger the two-factor security infrastructure to generate the additional security information in real-time when the user is on the HIFIS login page.

Utilizing two-factor authentication in HIFIS requires that you provide a custom two-factor authentication library for the HIFIS implementation that wraps your specific security infrastructure to make it accessible to HIFIS. The HIFIS Team has a working demonstration version using the Twilio SMS text messaging system that can be implemented for live use or used as a starter project to implement your own custom two-factor solution.

2.4.3. Authorization

Aside from the credentials that users provide when logging in to access HIFIS, there are other features that can be configured to provide further authorization and to secure the information being exchanged between components of the system. Built into Windows and IIS are tools that you can enable that will provide greater control of who or what can access HIFIS. For example, you can use IP address or domain restrictions to prevent unauthorized devices from connecting to the web application or the web services. You can also edit the binding configuration for the WCF web services to define the access parameters for your clients, including requiring them to use a secure connection and provide other user credentials.

It is important to note that this is in addition to the user authentication that is done by HIFIS. Consider the workflow described above, where the HIFIS.WEB web application must already have access to the HIFIS.DOMAIN authentication web service before it can even pass in the HIFIS user credentials. This implies there is a wraparound authorization and security context that can be configured and managed separately from the internal authorization features of HIFIS itself. These wraparound features are part of IIS and use a completely separate validation system such as a domain account or a security certificate.

2.4.4. Security

Thus far, we have mostly been concerned with ways to authenticate and authorize access to HIFIS and its components. This simply ensures that those interacting with HIFIS are allowed to do so. However, authenticated or authorized access does not mean it is also secure.

While the security token returned from HIFIS.DOMAIN is encrypted, the user credentials initially passed in for authentication are not. HIFIS does not encrypt data that is being transferred between the web services and the web application or another third-party application on its own. In order for that information to be encrypted and secured, you must also configure IIS to use Secure Sockets Layer (SSL) encryption. If you enabled SSL for HIFIS.WEB, then users will access the HIFIS.WEB web application with the prefix https:// in the address bar of their internet browser denoting a secure connection. You can also enable SSL for HIFIS.DOMAIN so the exchange of information between HIFIS.WEB and the HIFIS.DOMAIN web services is encrypted and secure.

Since the most common deployment configuration is to host both HIFIS.WEB and HIFIS.DOMAIN on the same IIS server instance, the HIFIS web application is set up to use non-secure HTTP bindings and message-based security with Windows as the default client credential type when communicating with the HIFIS.DOMAIN web services. If you are deploying HIFIS.WEB to a different server than HIFIS.DOMAIN and the connection between the servers is not secure, you will want to consider using SSL.

When configuring SSL security you have the option of installing a purchased SSL certificate from a trusted Certificate Authority or installing a self-signed certificate you create yourself. If you elect to use a self-signed certificate, be aware that modern web browsers may display visible warnings to the user, alerting them that the web site they are visiting does not have a certificate issued by a trusted authority. This can be mitigated, however, by sharing the certificate with the client machines and installing it on the local certificate store.

3.0 INSTALLATION PROCEDURES

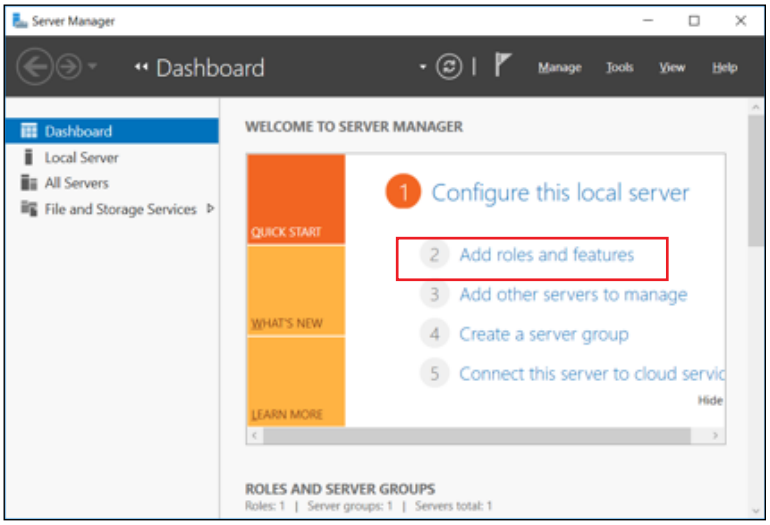
This section provides instruction on the steps for installing HIFIS on a Windows Server. It also includes steps for installing SQL Express and covers Crystal Reports in HIFIS..

3.1. INSTALLATION AND CONFIGURATION ON WINDOWS SERVER 2016

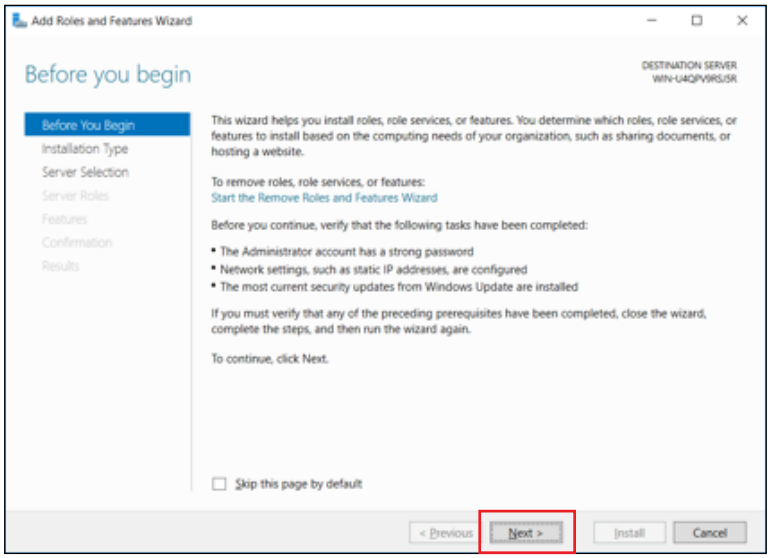
This guide will walk you through the necessary steps to install and configure HIFIS 4 on a clean install of Windows Server 2016.

Step 1 Launch *Server Manager*.

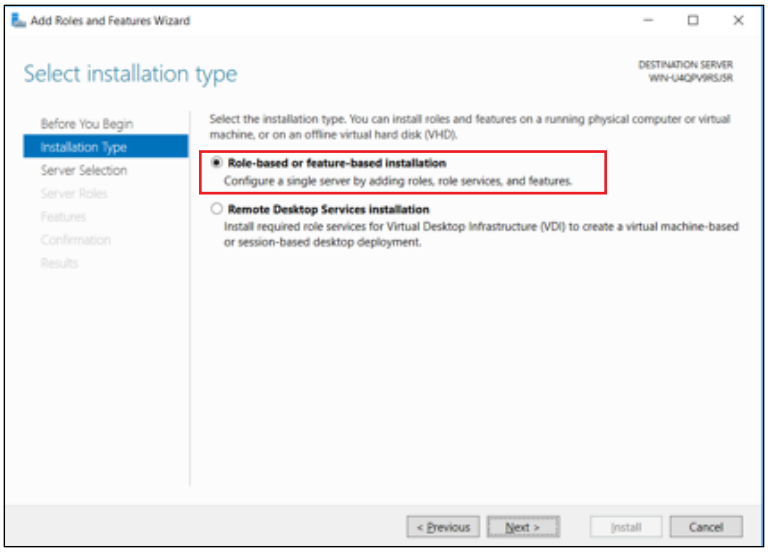
Step 2 Select *Add roles and features* from the Dashboard quick start menu:



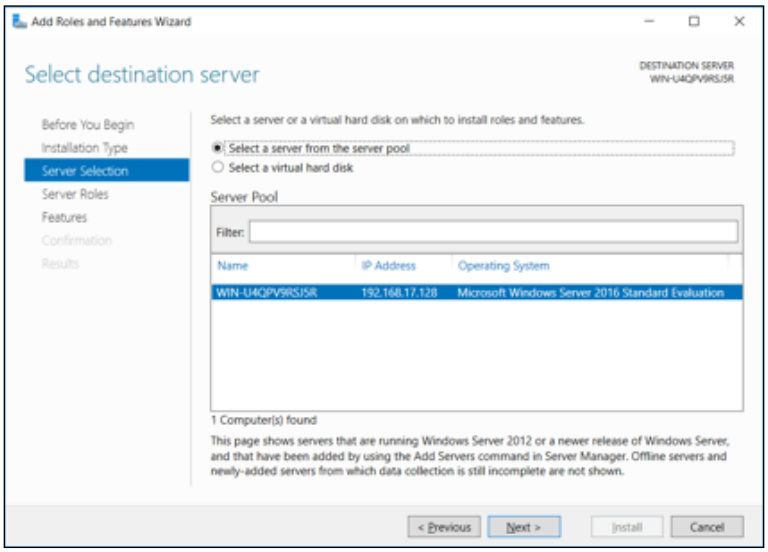
Step 3 Click *Next*:



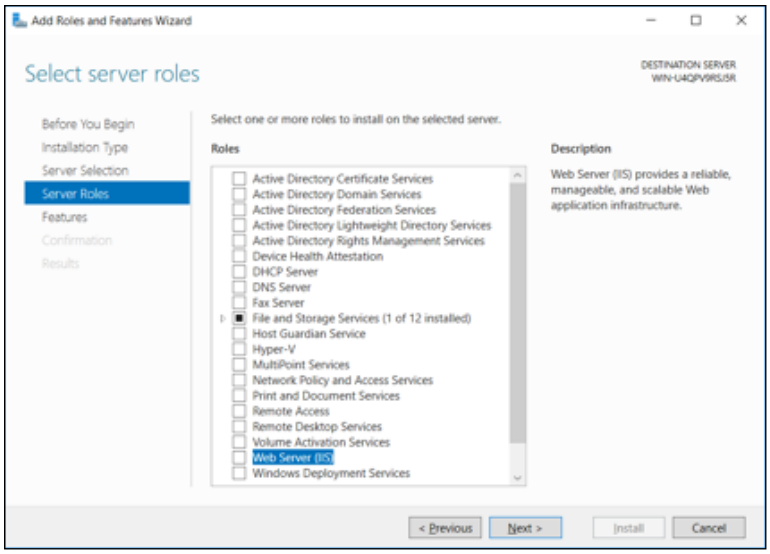
Step 4 Select *Role-based* or *feature-based installation* and then click *Next*:



Step 5 Select the server you wish to configure and click *Next*:



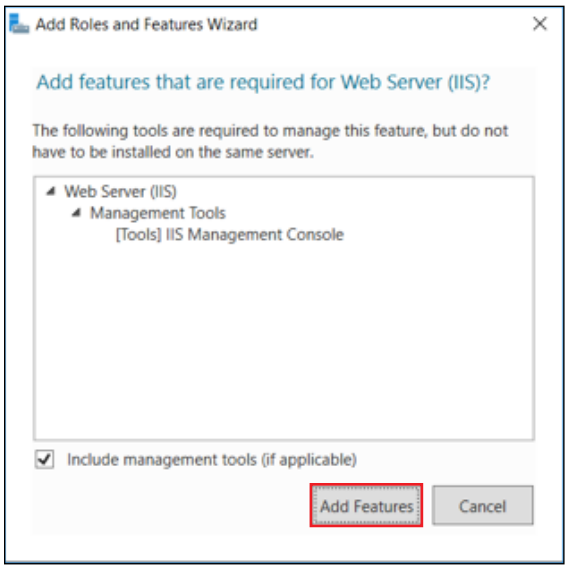
Step 6 Select the required roles and click *Next* (refer to *Table 1*):



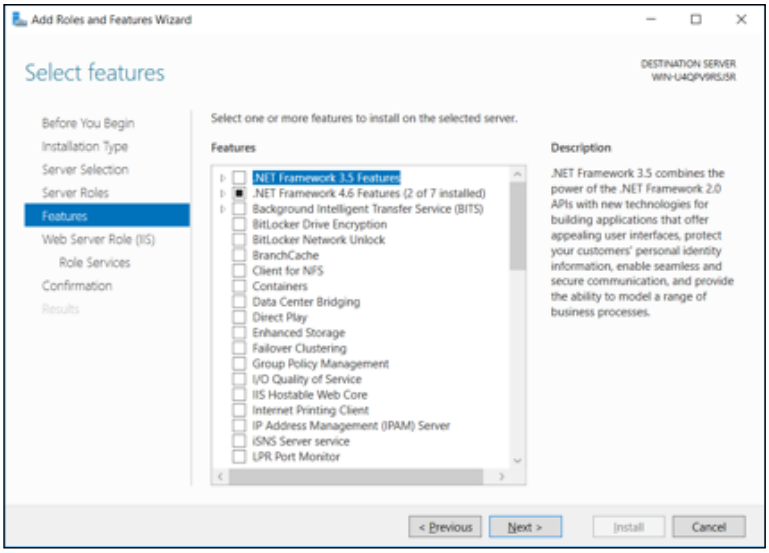
Required Server Roles

File and Storage Services
Storage Services
Web Server (IIS)
Web Server
Common HTTP Features
Default Document
Directory Browsing
HTTP Errors
Static Content
Health and Diagnostics
HTTP Logging
Performance
Static Content Compression
Security
Request Filtering
Application Development
.NET Extensibility 4.6
ASP.NET 4.6
ISAPI Extensions

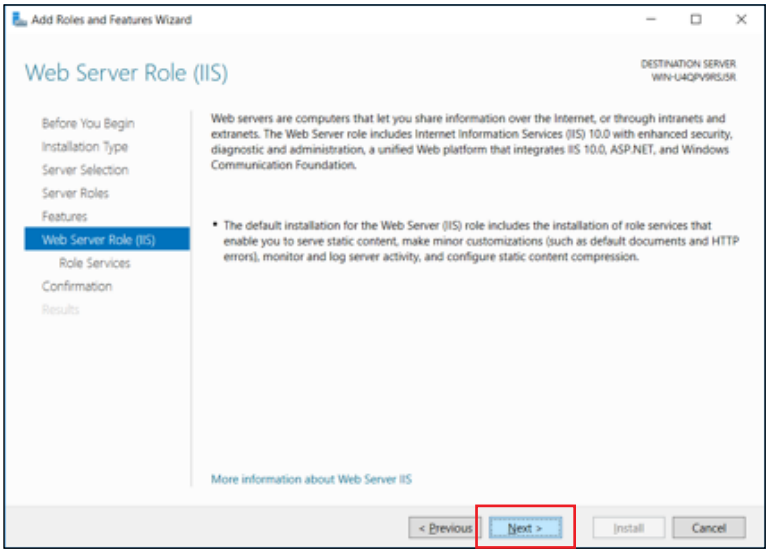
Note: You may be prompted to add additional dependant features. Click *Add Features* to continue:



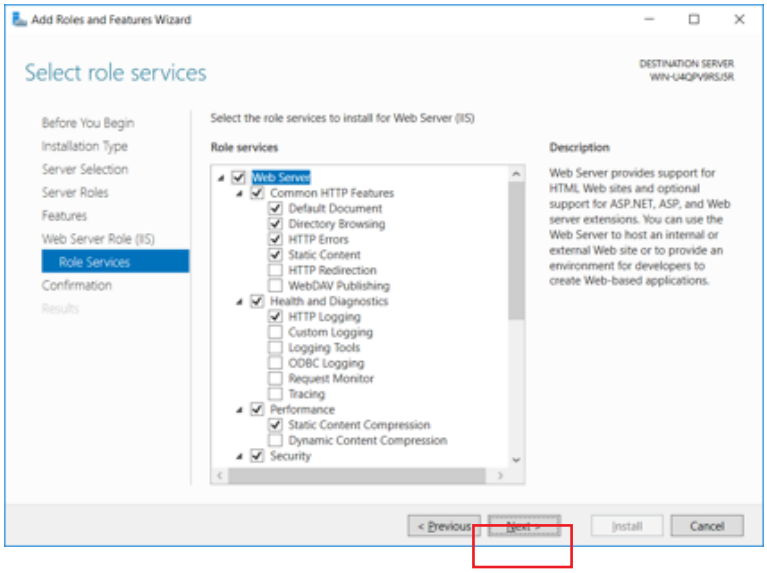
Step 7 Select the required features and click *Next* (refer to Table 2):



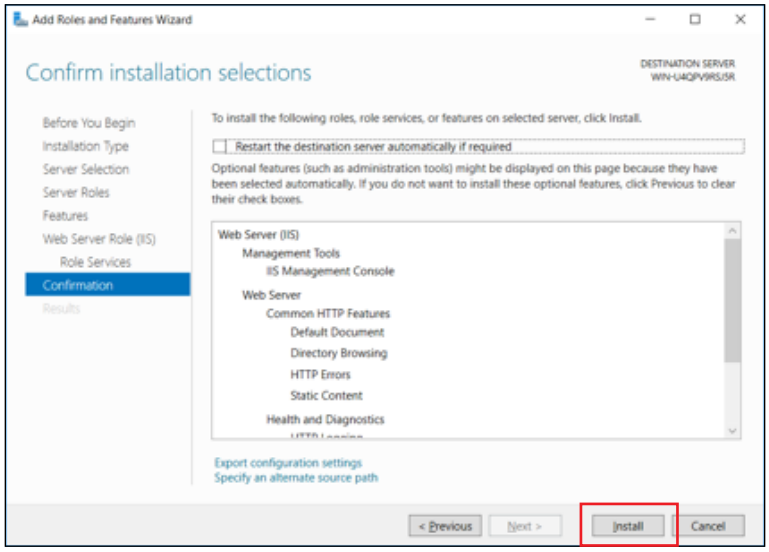
Step 8 At the Web Server Role (IIS) screen, click *Next*:



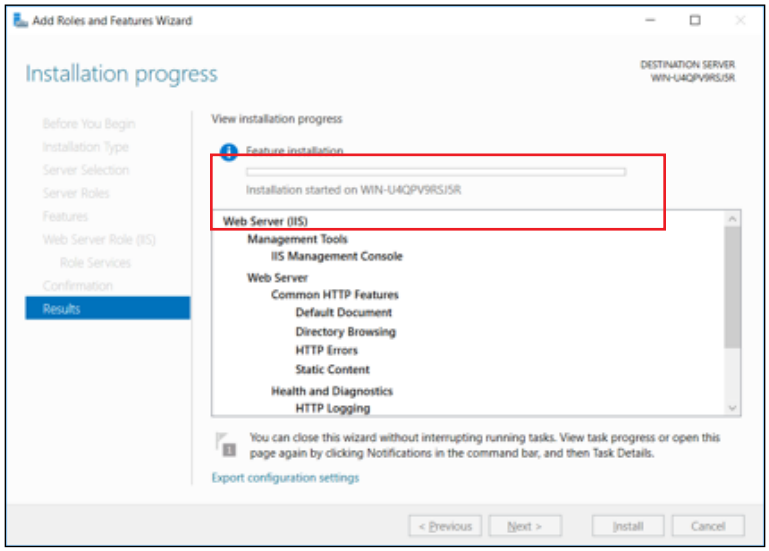
Step 9 At the Select role services screen, click *Next*:



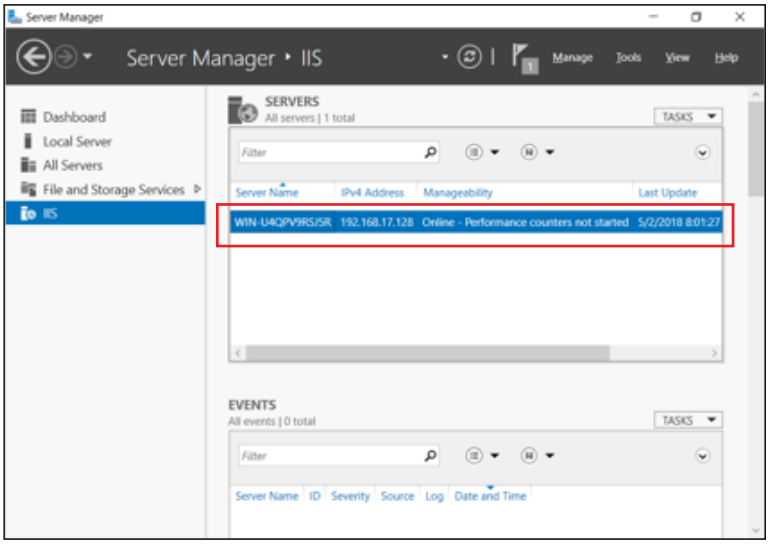
Step 10 At the Confirm installation selections screen, click *Install*:



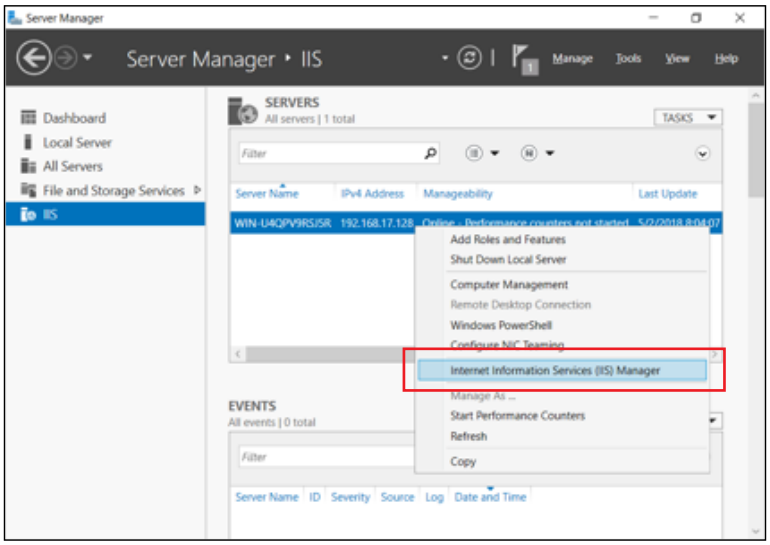
Step 11 Windows Server will now install the selected roles and features. When the installation is complete, click *Close*:



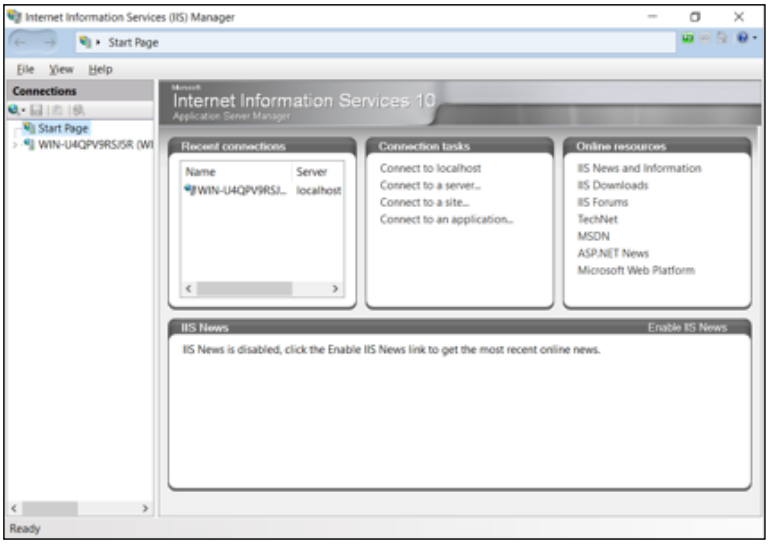
Step 12 You will return to the Server Manager. *IIS* (Internet Information Services*)* will now appear in the menu on the left hand side. Click on *IIS* and locate your server, which will be listed in the Servers area. If there is more than one server displayed, select the one you wish to configure for HIFIS 4.



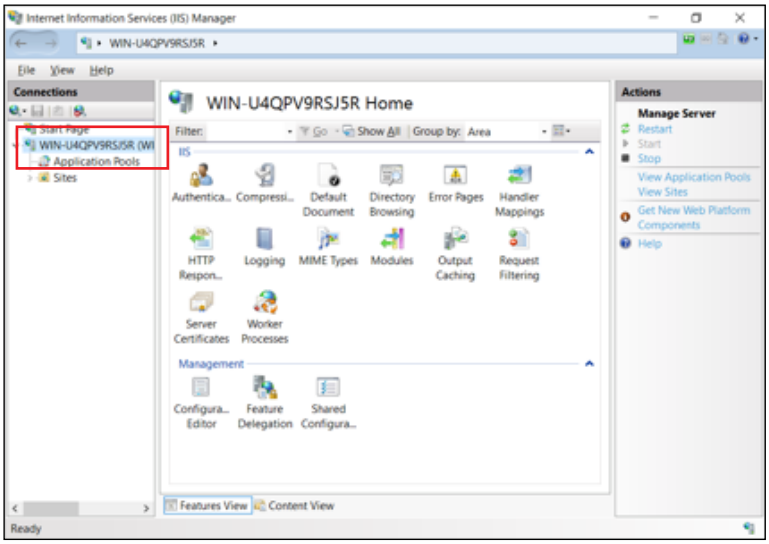
Step 13 Right-click on the server name and select *Internet Information Services* (IIS) *Manager*:



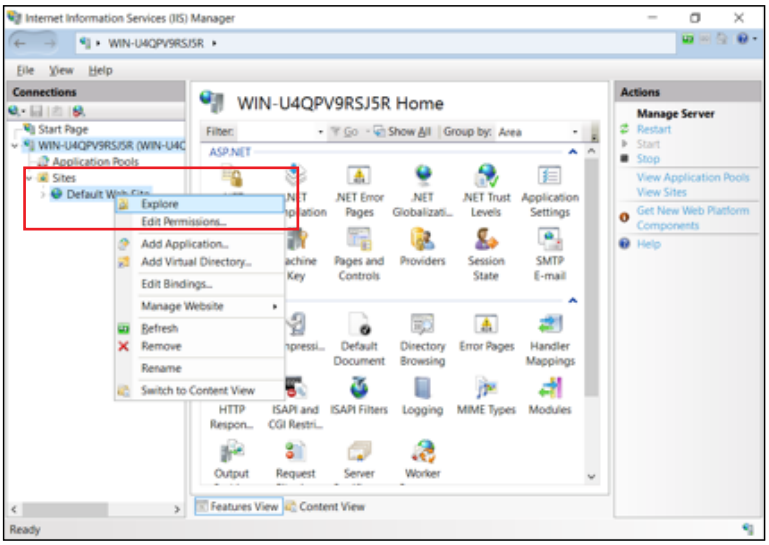
Step 14 You will now see the *Internet Information Services (IIS) Manager*.



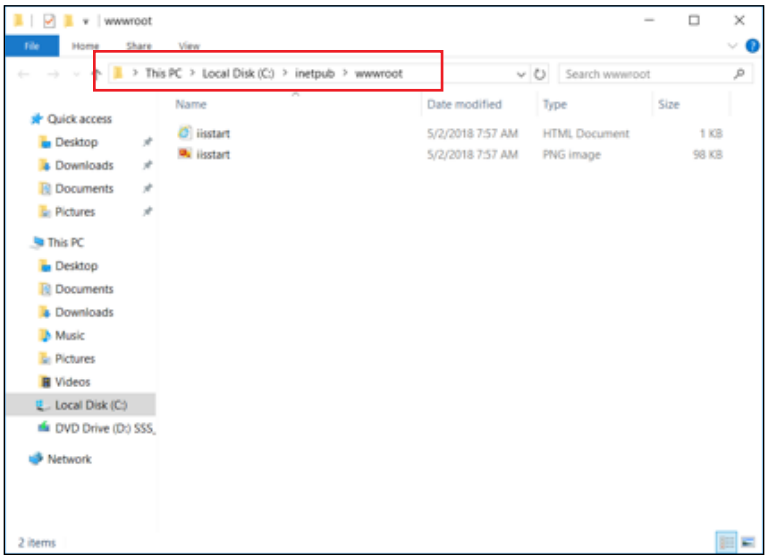
Step 15 Select your server in the *Connections* area on the left side:



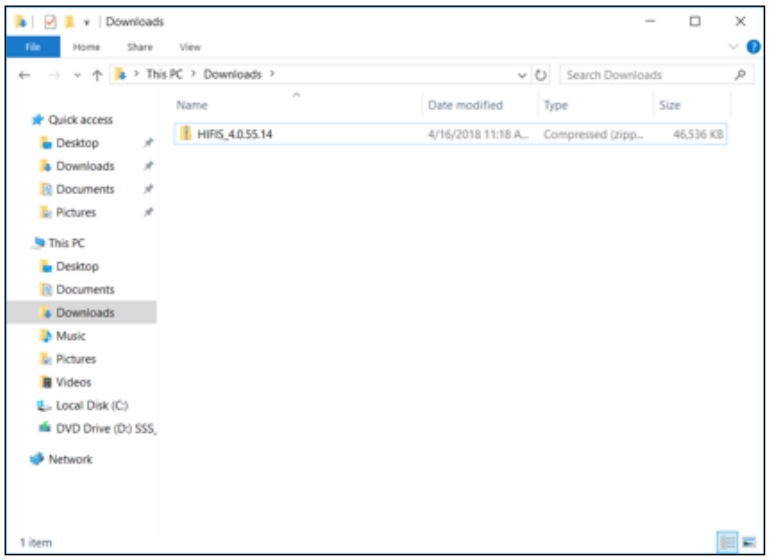
Step 16 Expand the *Sites* node and right-click on the *Default Web Site* node. Select *Explore* from the menu that appears:



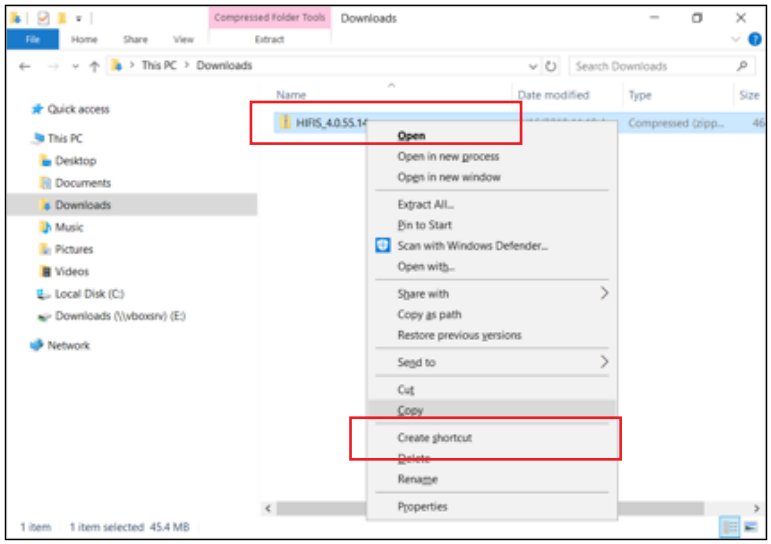
Step 17 You are now ready to install the HIFIS 4 application. Take note of the default web site file location (usually C:\inetpub\wwwroot):



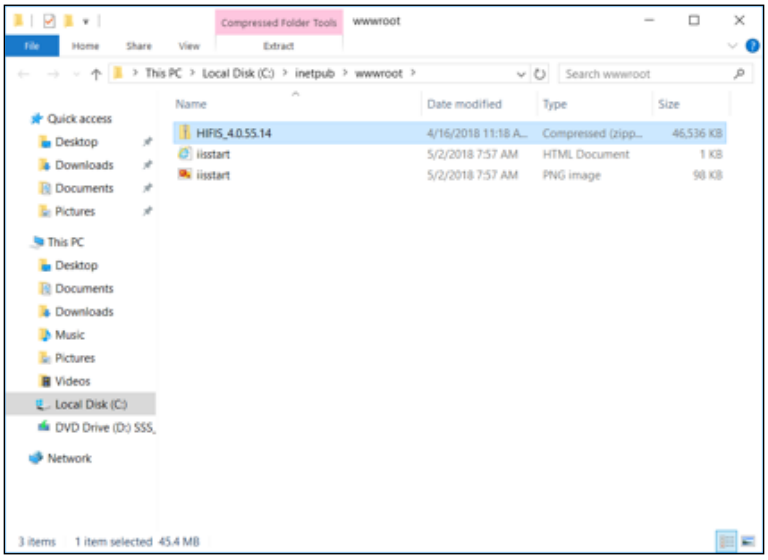
Step 18 Navigate to the *Downloads* folder (or to the location where you have downloaded the HIFIS 4 application files):



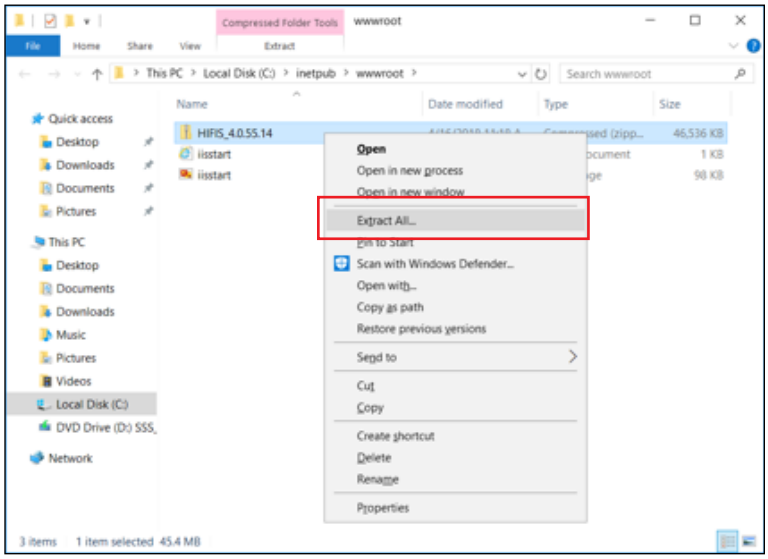
Step 19 Right-click on the HIFIS 4 application zip file and select *Copy*.



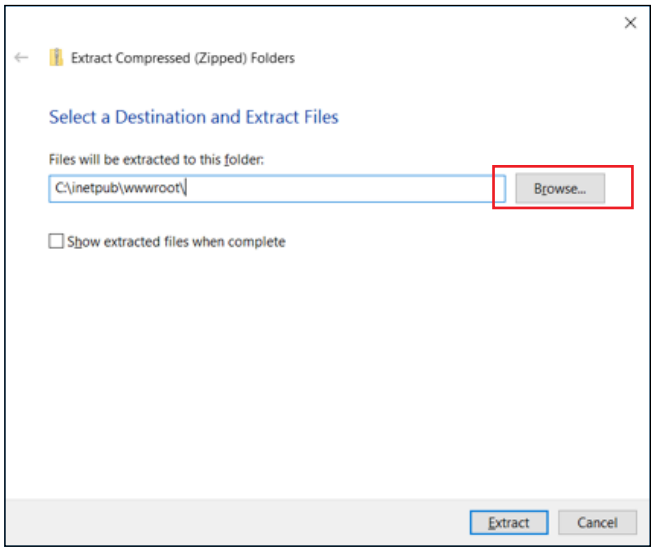
Step 20 Navigate to the default web site location you noted earlier and paste the HIFIS 4 zip file by pressing CTRL+V or right-click and select *Paste*:



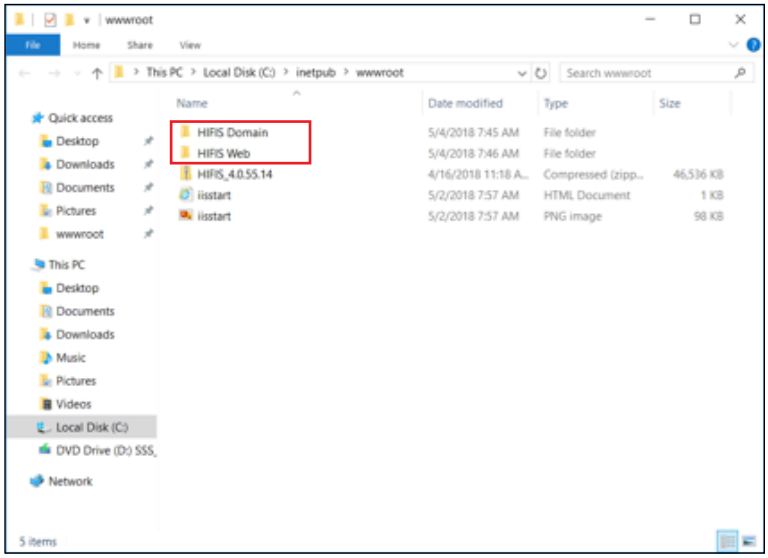
Step 21 Once the HIFIS 4 application zip file has finished copying, right-click on it and select *Extract All*:



Step 22 You will be prompted to select a destination, enter or browse to the default web site location and click *Extract*:

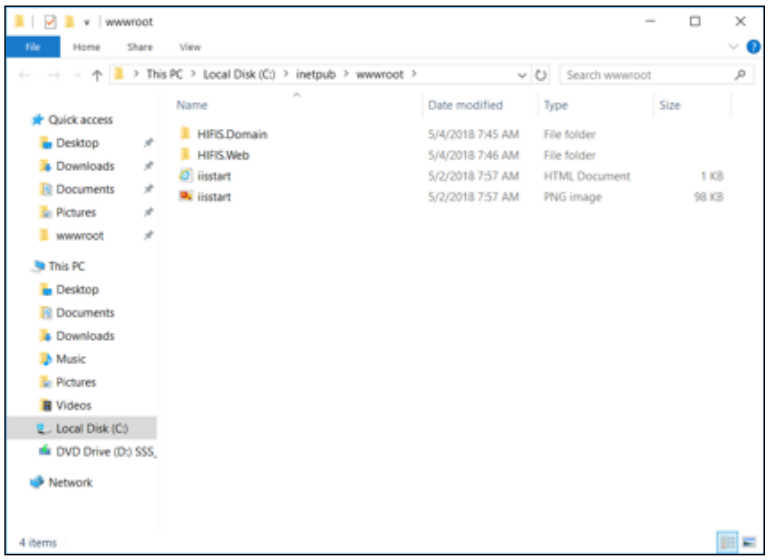


Step 23 When completed, there will be two new folders, “HIFIS Web” and “HIFIS Domain”. Rename the folders to “HIFIS.Web” and “HIFIS.Domain”*:

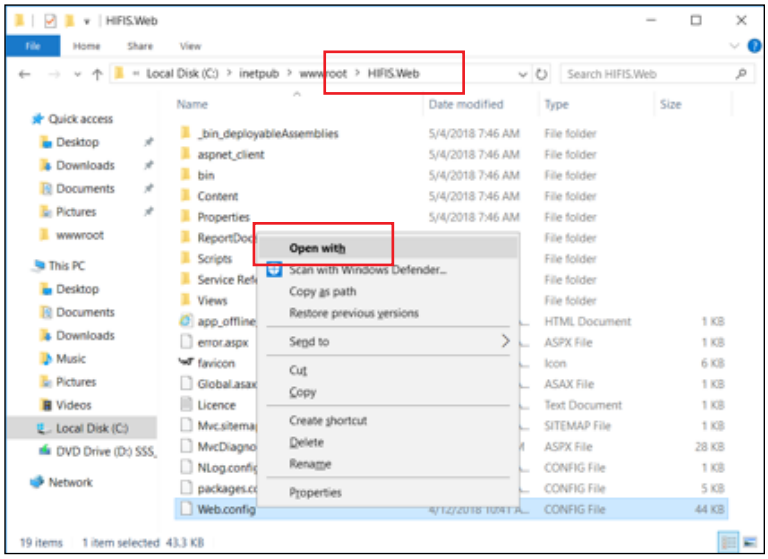


*You may choose an alternative naming convention if you wish, however you will need to remember these folder names in the steps that follow.

Step 24 You may now delete the HIFIS 4 application zip file that was copied earlier:

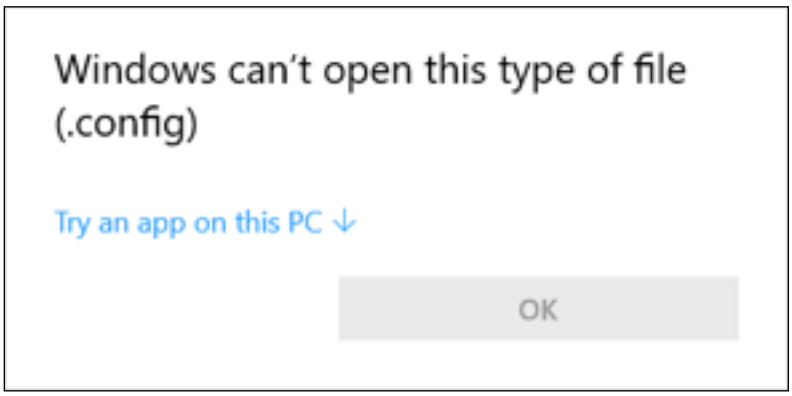


Step 25 Next, we will configure the HIFIS 4 application. Open the HIFIS.Web folder and right-click the file named “Web.config”. From the menu that appears, select *Open with*:

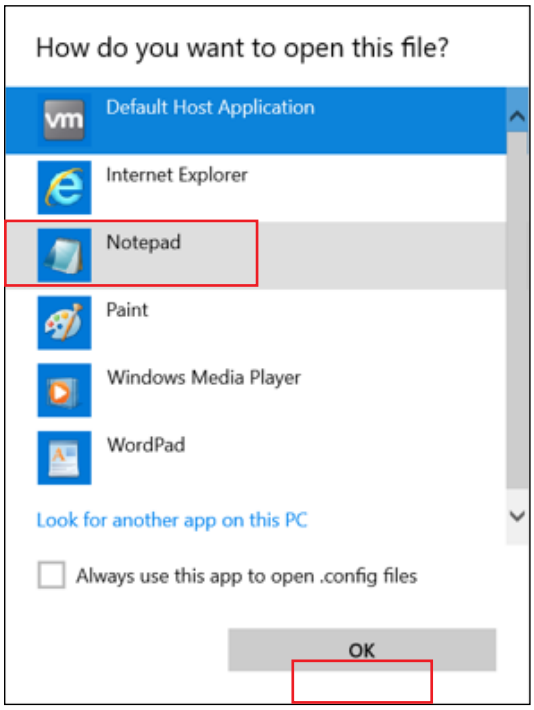


Note: If you cannot find the file, look for a template version of the configuration called “WebTemplate.config” and rename the file to “Web.config” (or make a copy of it and rename the copied version).

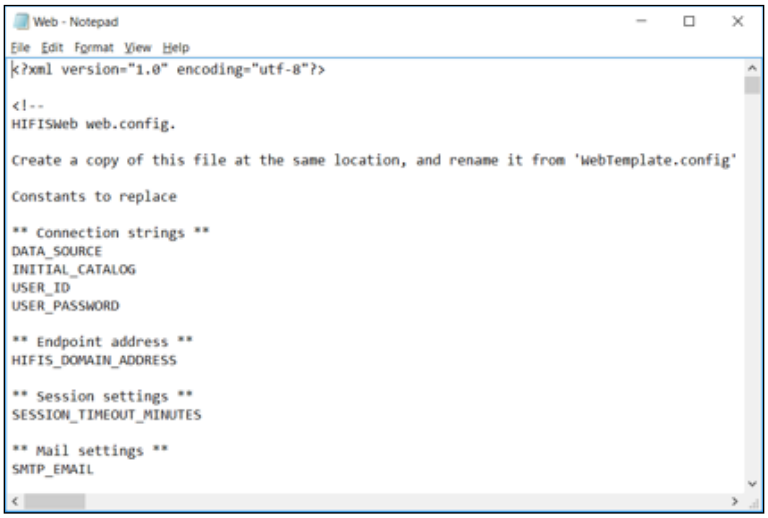
Step 26 By default, Windows Server 2016 does not know how to open files of this type. Select *Try an app on this PC*:



Step 27 Select Notepad from the list of available applications and then click *OK*:

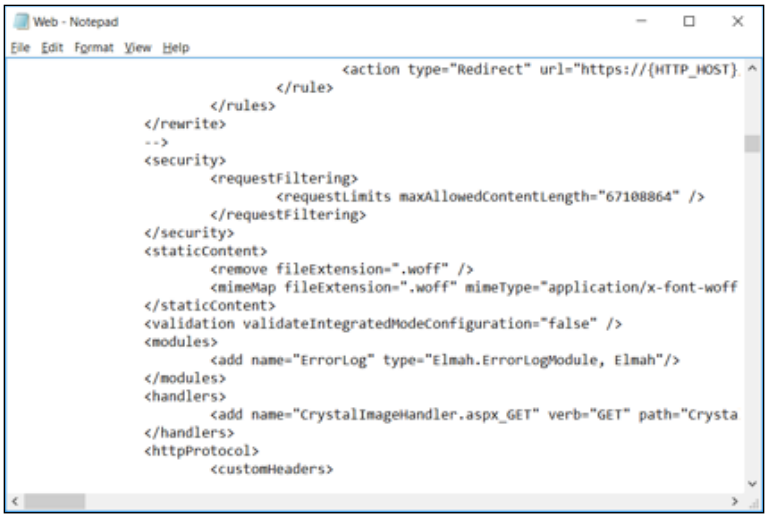


Step 28 The file will now open using Notepad:



Step 29 Because we are installing on Windows Server 2016, we must disable a mimeMap setting that is not required. Scroll through the file until you reach the <staticContent> section as in the image below. Delete the lines highlighted in blue:

Step 30 The <staticContent> section should now look like this:



Step 31 Scroll down to the setting named <sessionState> and replace the SESSION_TIMEOUT_MINUTES text with a suitable numeric value. This will determine how long a session remains active before automatically timing out.

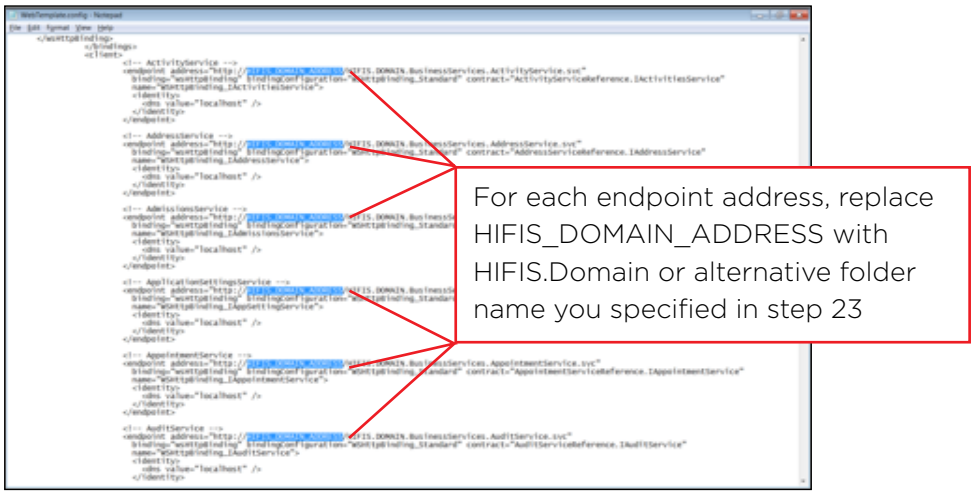
Step 32 Your configuration file should now look similar to this:

Step 33 Scroll to bottom of the configuration file to the section called <connectionStrings>.

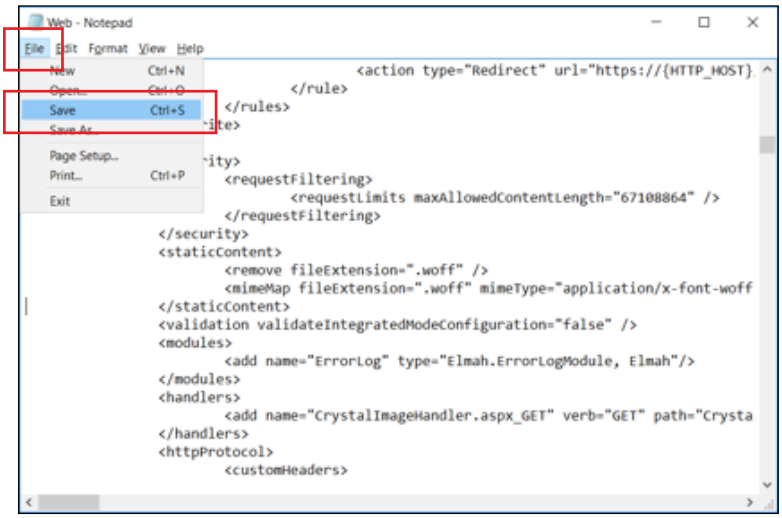
Step 34 In the configuration file for the HIFIS Web application component, there is only one database connection string to configure called HIFIS_HelpEntities. This database connection provides access to the integrated help and training content in HIFIS 4. Adjust the connection string as necessary to connect to the HIFIS 4 database that will provide this information. It does not have to be the same database that contains HIFIS 4 client data.

Step 35 At the end of the configuration file, there is a setting called <errorLog>. Replace the text ELMAH_LOG_DIR with a folder location used for error logging.

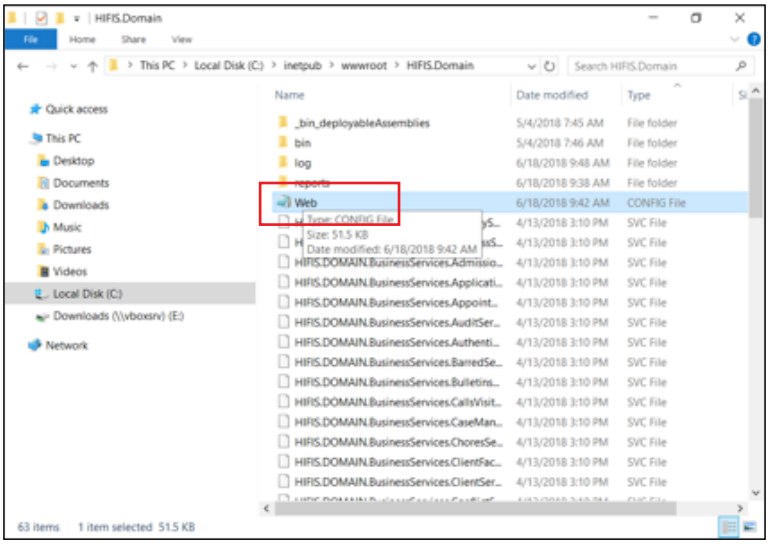
Step 36 The HIFIS 4 web application, called HIFIS.Web, uses Windows Communication Foundation (WCF) to interact with the business tier called HIFIS.Domain. In the HIFIS.Web configuration file, there is an endpoint configuration for each business service available in the business tier. They can be found in the <client> section (see image). For each endpoint, you must update the address to point to the correct location. The template configuration file has place holder text, “HIFIS_DOMAIN_ADDRESS”, which you can replace with the text “HIFIS.Domain” for each endpoint if you are confirming to the configuration provided in this document. If you have customized the name of the folder (step 23) where the HIFIS.Domain component is installed you will need to use that same folder name here.



Step 37 Save the changes to the configuration file by clicking *File* and selecting *Save*. You may close the configuration file.



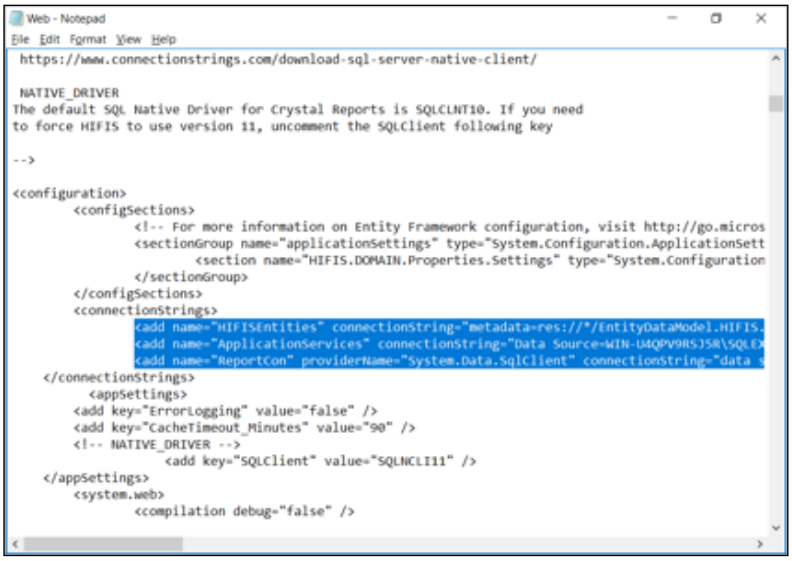
Step 38 Navigate to the *HIFIS.Domain* folder and find the *web.config* file. Double-click to open it.



Note: If you cannot find the file, look for a template version of the configuration called "WebTemplate.config" and rename the file to "Web.config" (or make a copy of it and rename the copied version).

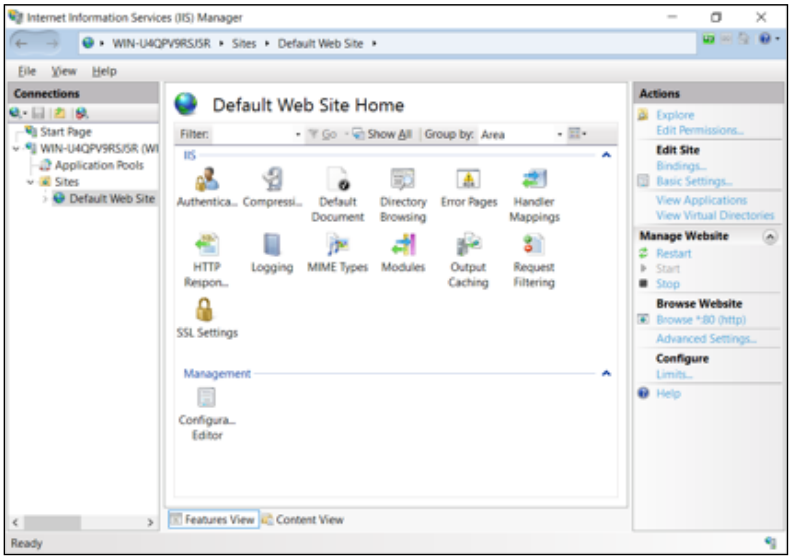
Step 39 As with the previous configuration file, you will need to update the database connection information in the <connectionStrings> section. There are three connection strings to update:

- *HIFISEntities* (database containing the live HIFIS data)
- *ApplicationServices* (database containing the user account information)
- *ReportCon* (database used for reporting)

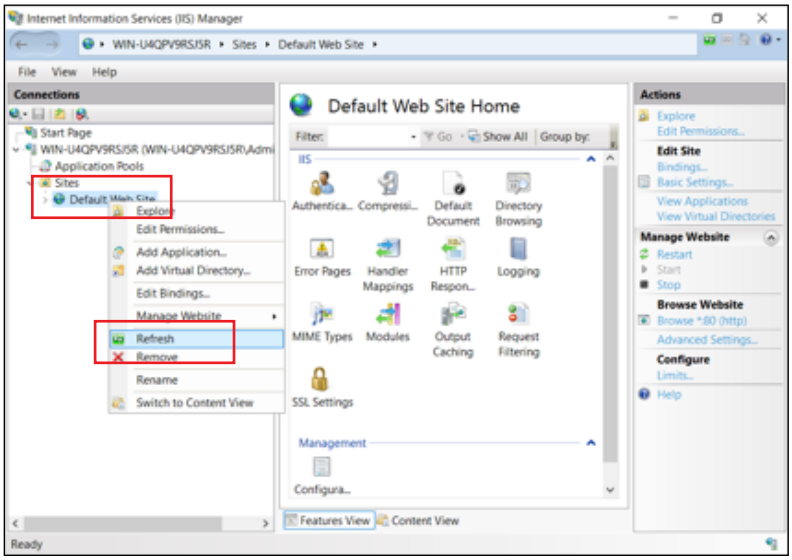


Note: Unless you have a specific business requirement, normally all three of these are configured to use the same database. Adjust the connection strings as necessary to connect to the HIFIS 4 database. When you are finished, save and close this file.

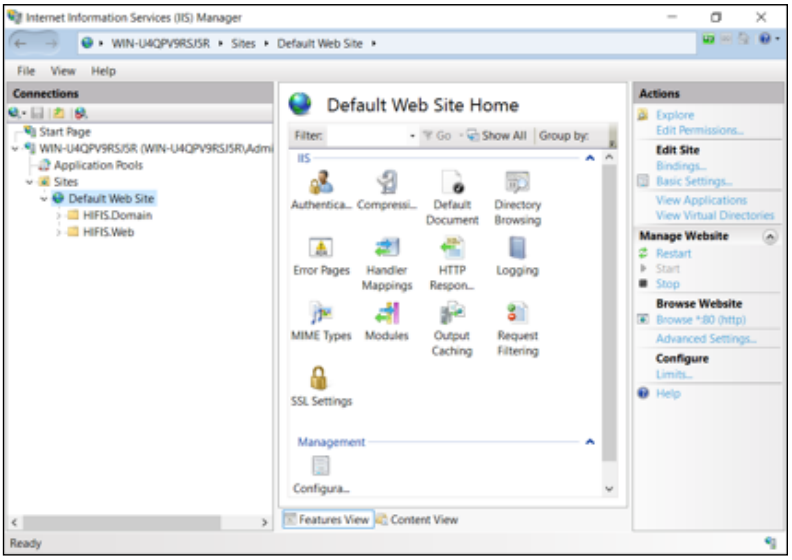
Step 40 Return to the *Internet Information Services (IIS) Manager*.



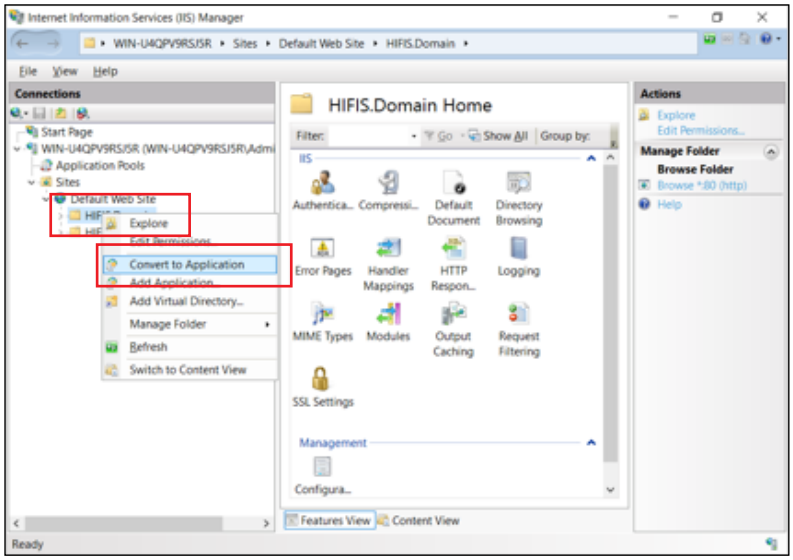
Step 41 Right-click on the *Default Web Site* node under Sites and select *Refresh*.



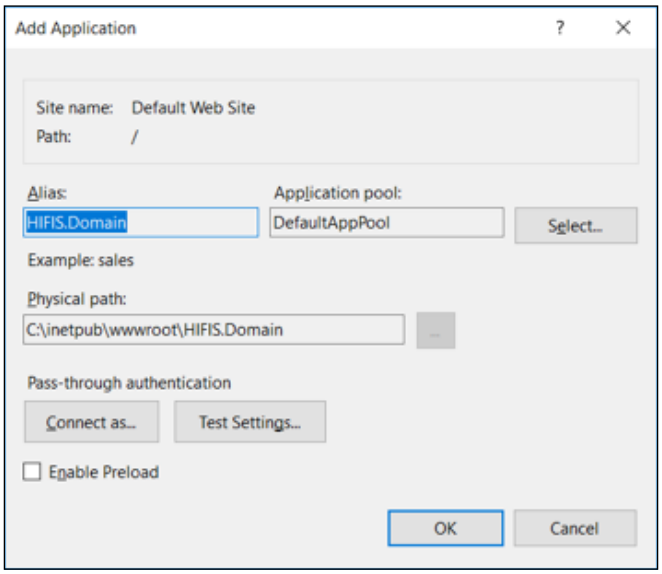
Step 42 You will now see the two HIFIS folders that we extracted previously.



Step 43 Right-click on *HIFIS.Domain* and select *Convert to Application*.

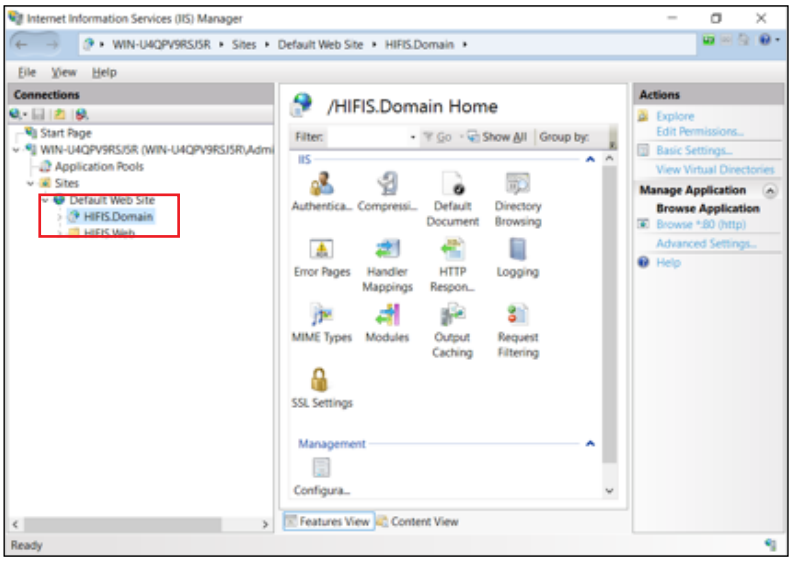


Step 44 In the *Add Application* dialogue box, click *OK*.

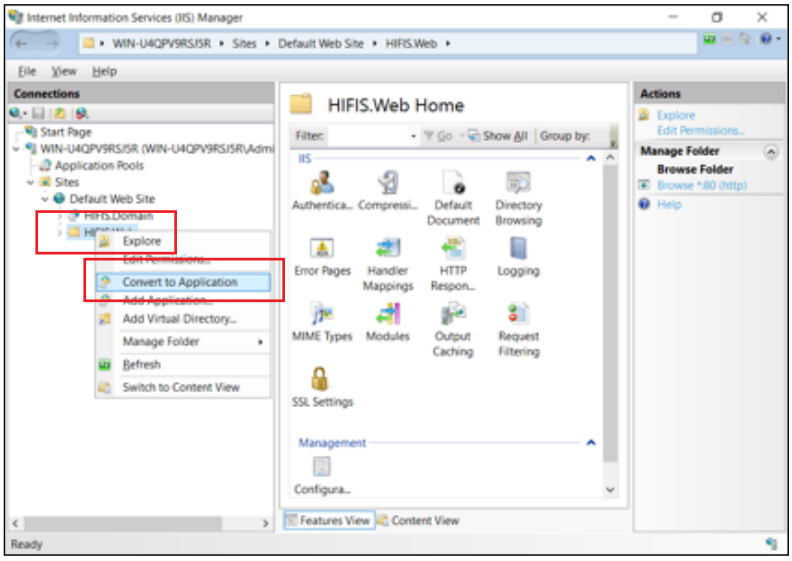


Important: The Alias defaults to the same name as the selected folder. The alias is the text that will be used to form the web address of this application. Previously, when we configured the endpoint addresses for the web services in the HIFIS.Web configuration file. If you are using an alternative name for this alias, the endpoint addresses must be configured to use the same alias in the address (e.g. if you set the alias to "HIFISWebServices" the endpoint addresses would all follow the pattern: http://localhost/HIFISWebServices/HIFIS.Domain.BusinessService...)

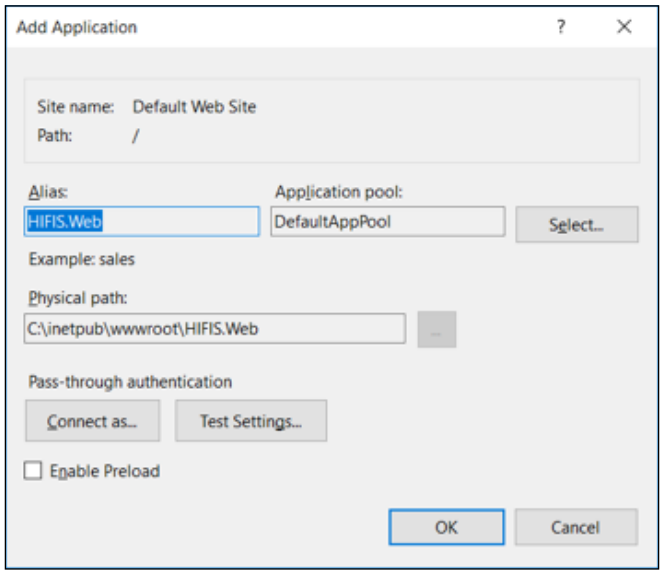
Step 45 Notice that the icon for *HIFIS.Domain* has changed to indicate that it is now an application in IIS.



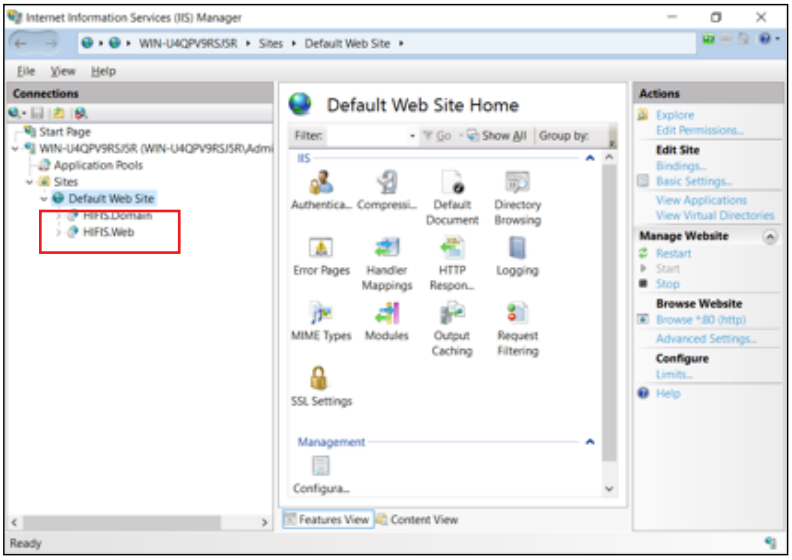
Step 46 Right-click on *HIFIS.Web* and select Convert to Application.



Step 47 In the *Add Application* dialogue box, click *OK*.



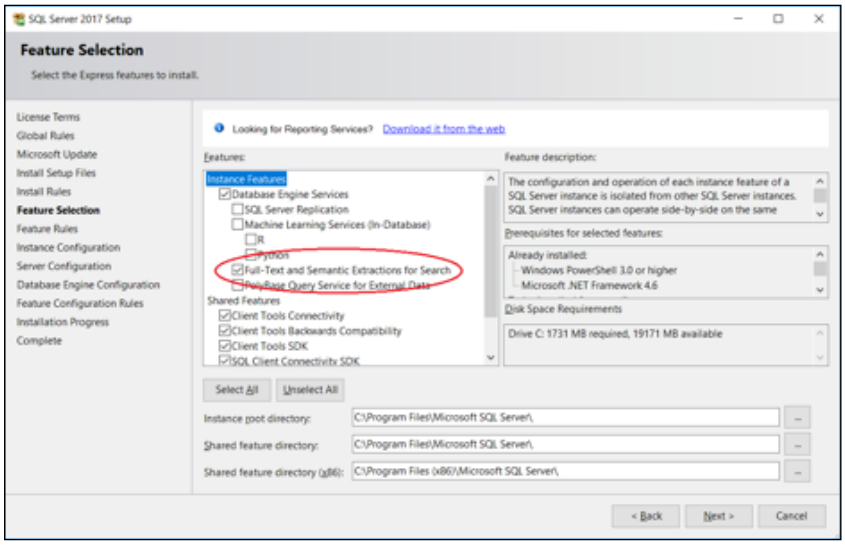
Step 48 Notice that the icon for *HIFIS.Web* has also changed to indicate that it is now an application in IIS.



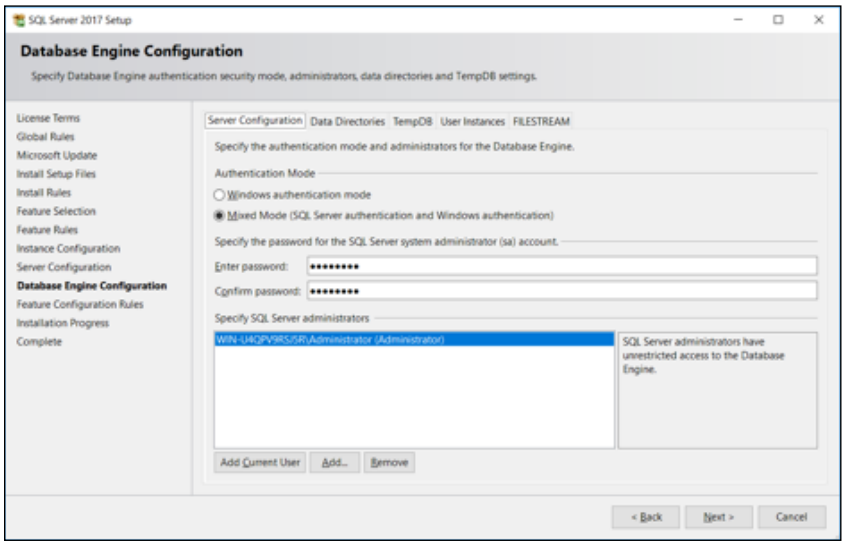
3.2. INSTALLING SQL EXPRESS 2017 WITH ADVANCED DATA SERVICES

Follow the documentation for the version of SQL Server that you wish to install. HIFIS is compatible with SQL Server 2008 R2 or better. For all versions, you must include the full-text search feature.

Note: If you are installing an Express version of SQL Server, ensure you download a specific version that includes the full-text search feature, normally called "SQL Server Express with Advanced Tools".



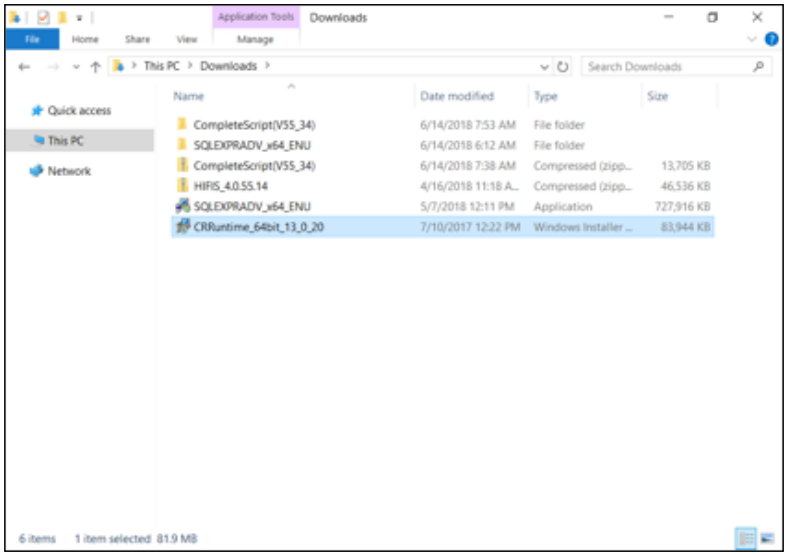
This guide assumes the use of Mixed Mode authentication and describes using SQL Server authentication. If you have a business requirement to use Windows Authentication Mode, you will need to adjust your configuration as per the information found here: https://msdn.microsoft.com/en-us/library/bsz5788z.aspx.



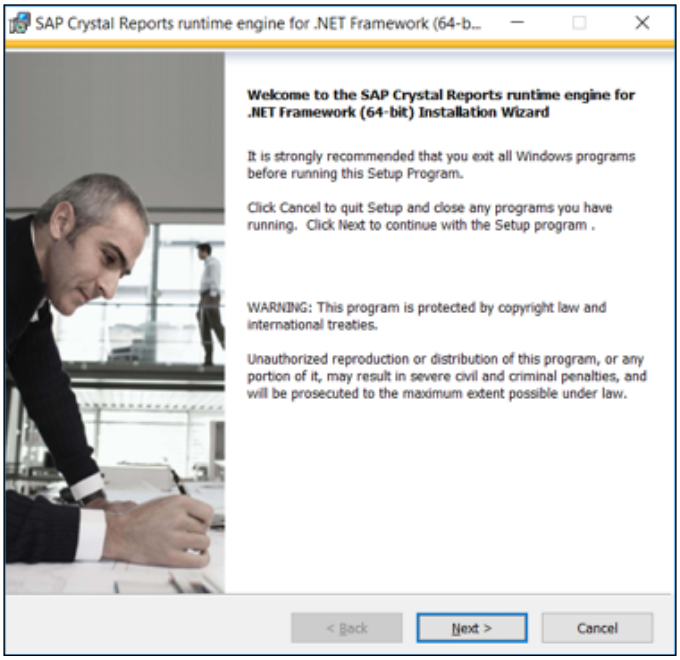
3.3. CRYSTAL REPORTS

HIFIS 4 uses SAP Crystal Reports to provide real-time integrated reporting. In order to enable reporting, you must install the Crystal Reports runtime engine from a link provided by the HIFIS team.

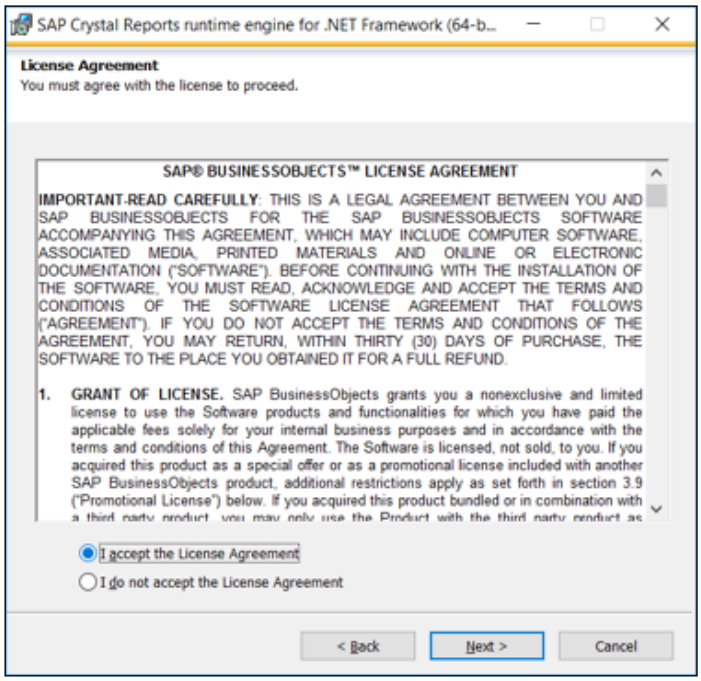
Step 1 Double-click the SAP Crystal Reports installation file that you downloaded.



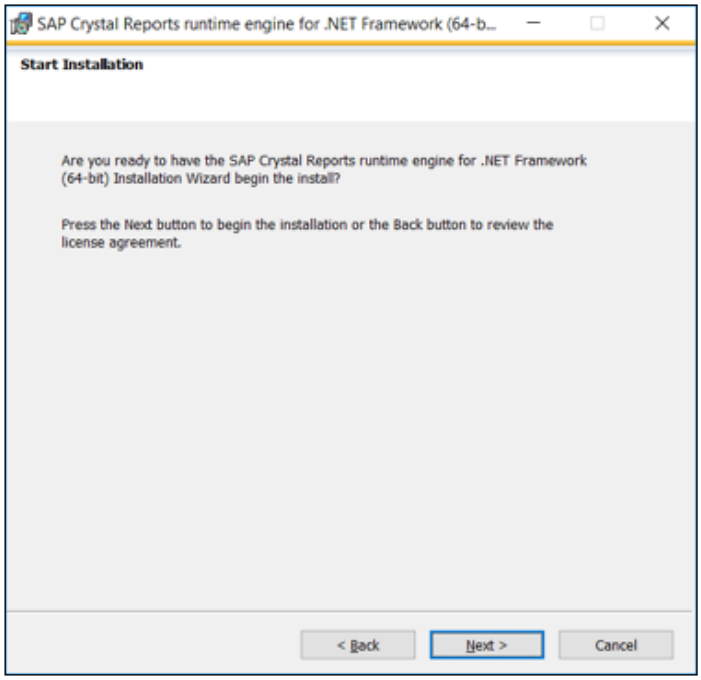
Step 2 Click *Next*.



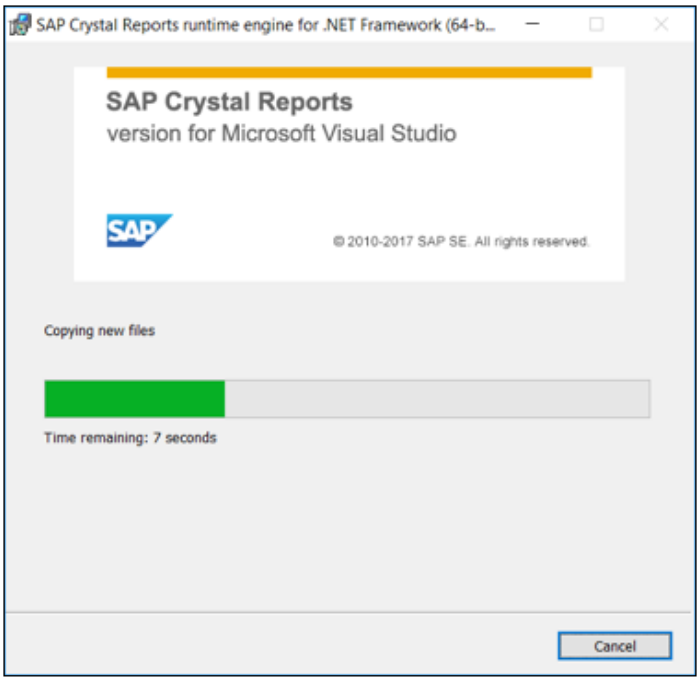
Step 3 Review and accept the *License Agreement*.



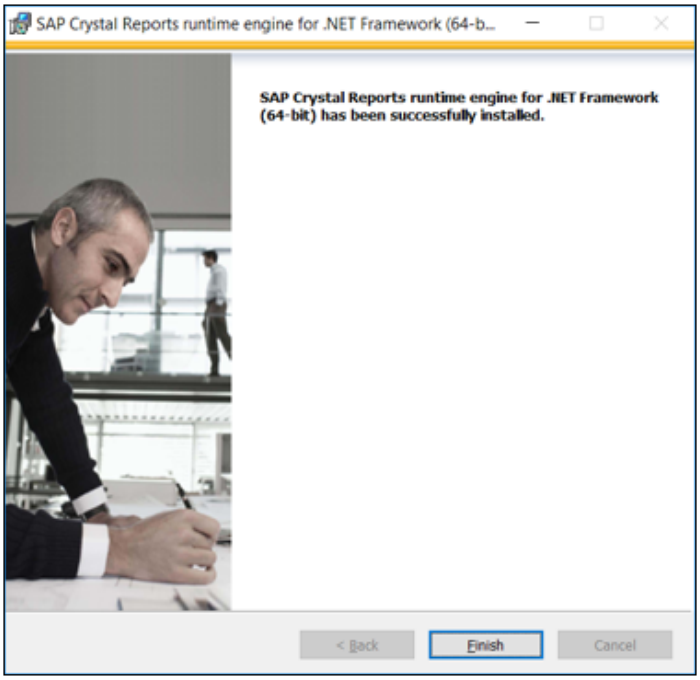
Step 4 Ensure you are installing the correct version (normally the 64-bit version). Click *Next*.



Step 5 Allow the installation to complete.



Step 6 Click *Finish*.



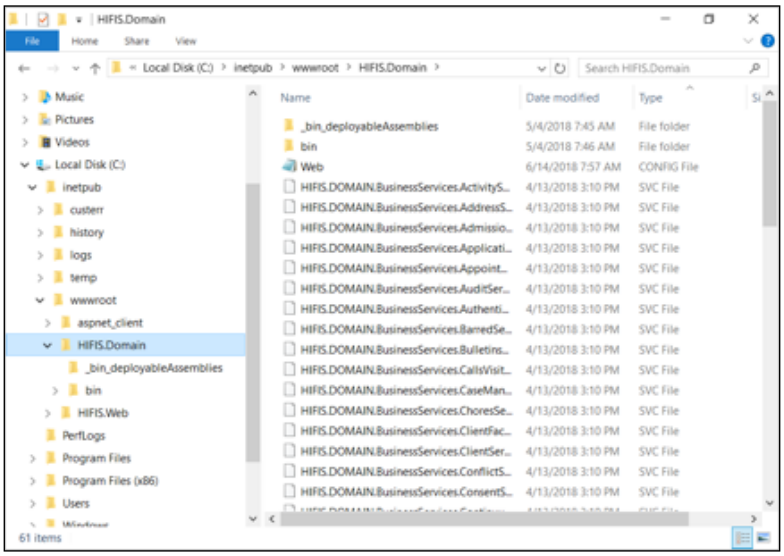
CRYSTAL REPORTS – COMMON ISSUES

These are some common issues and fixes related to the configuration of Crystal Reports. If you receive the following error, you will need to create a folder required for Crystal Reports to function properly.

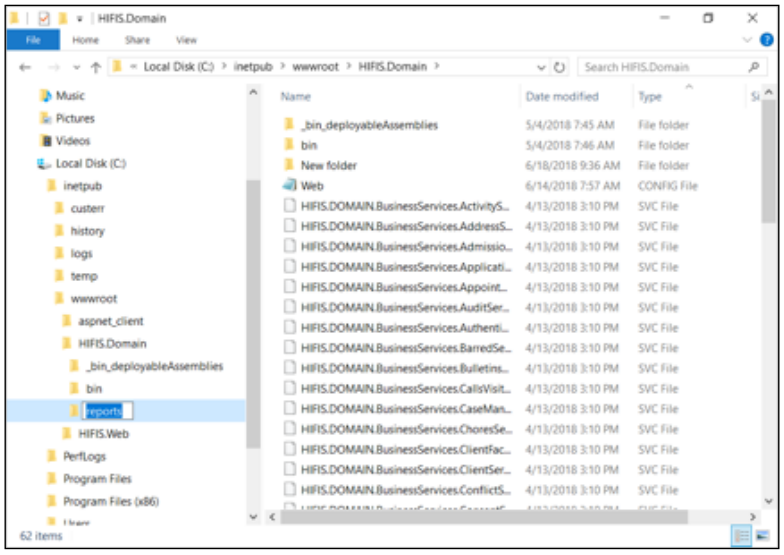
Error: "The required folder [...] does not exist and HIFIS was unable to create it for the following reason: Access to the path [...] is denied."

Solution: Create the folder required for Crystal Reports to function properly (see steps below).

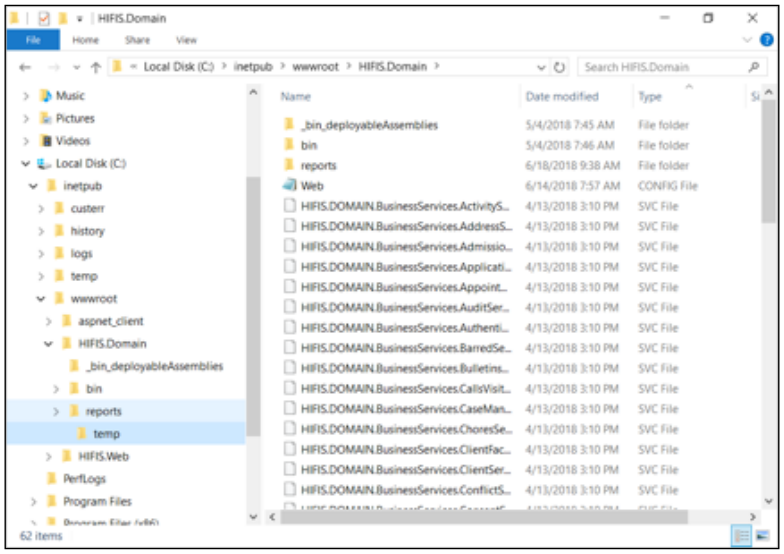
Step 1 Navigate to the *HIFIS.Domain* folder in Windows Explorer. Right-click on *HIFIS.Domain* and select New -> Folder.



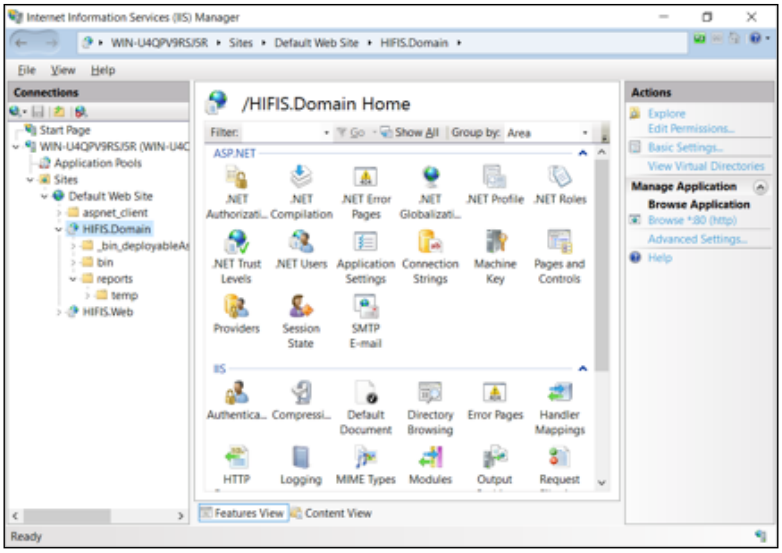
Step 2 Name the new folder *reports*.



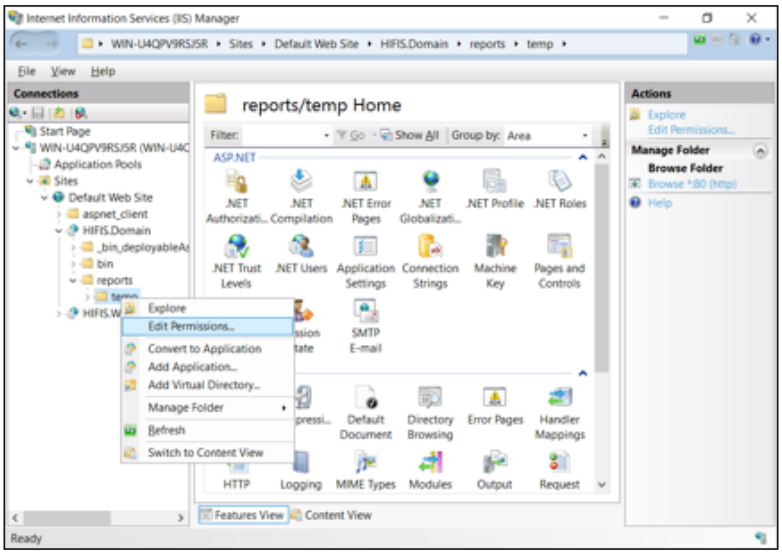
Step 3 Create a second folder, inside the *reports* folder you just created, called *temp*.



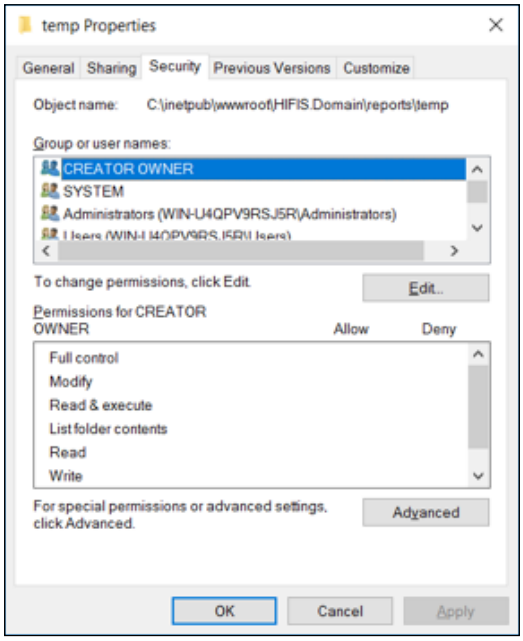
Step 4 In *Internet Information Services* (IIS) Manager, refresh the folders under *HIFIS.Domain*.



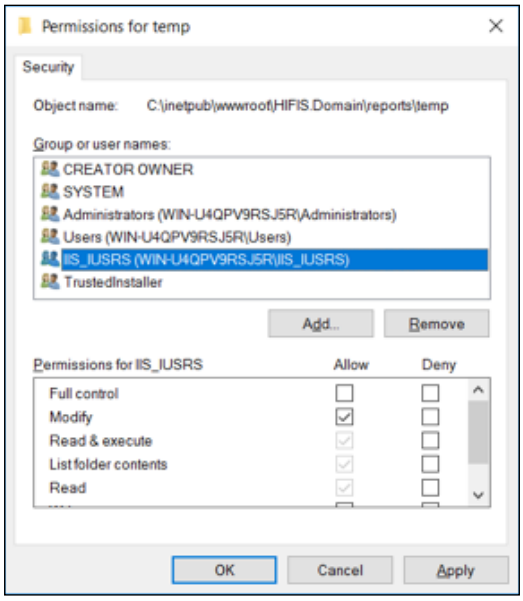
Step 5 Right click on the newly created temp folder and select *Edit Permissions.*



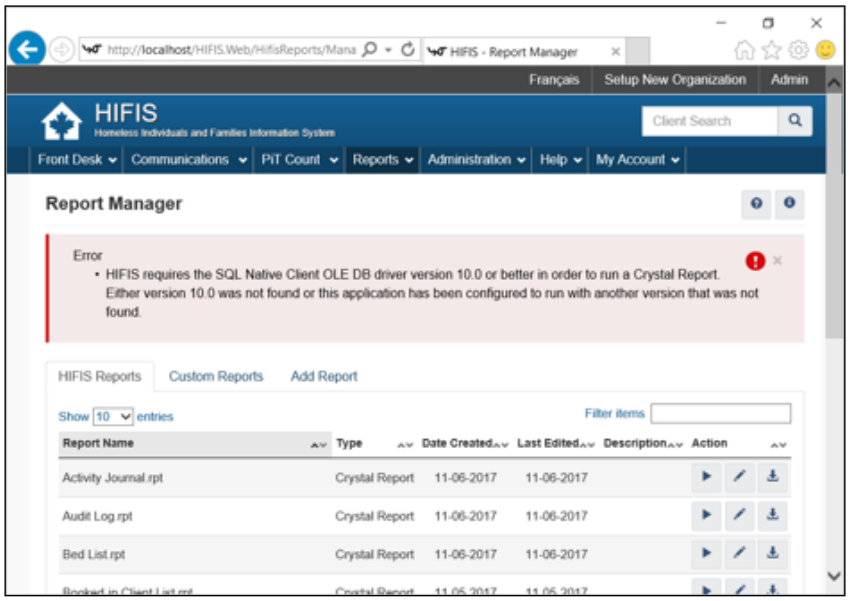
Step 6 Click *Edit*.



Step 7 On the list, scroll down to find the group called *IIS_IUSRS* and select it. With the group selected, place a check-mark in the *Allow* column for the Modify permission as per the image below and click OK. This will resolve the error.



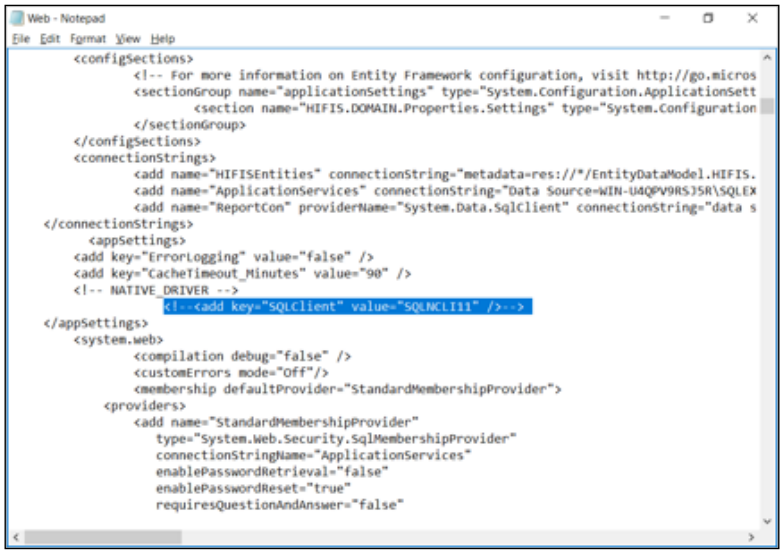
Error: ***"HIFIS requires the SQL Native Client OLE DB driver version 10.0 or better [...]"***



Solution: Modify the *HIFIS.Domain* configuration file and possibly install an additional component (by default, HIFIS will attempt to the SQL Native Client 10.0 for reporting connections to the SQL database). If you have version 11.0 installed, follow the steps below to adjust the configuration.

Step 1 Navigate to the *HIFIS.Domain* folder in Windows Explorer and open the *web.config* file for editing. Find the section called <appSettings> and identify the line highlighted in blue.

Step 2 Remove the comment tags surrounding this line until it looks like the line highlighted in blue:

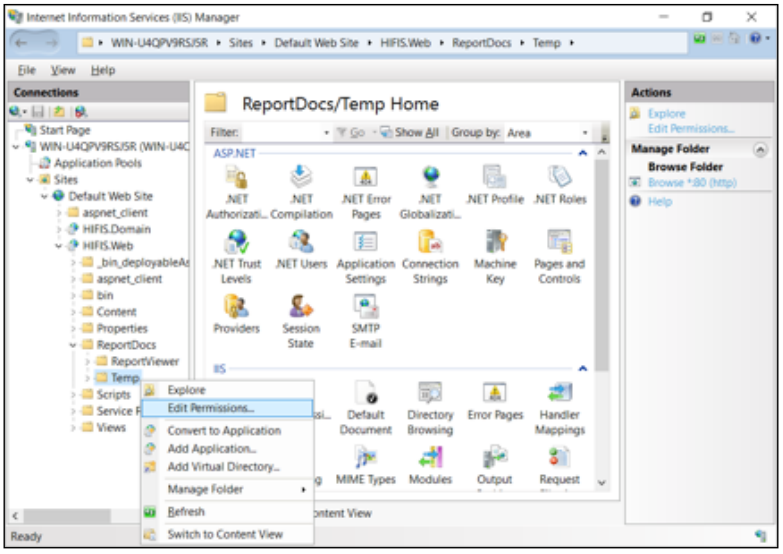


Step 3 Save your changes. If you continue to receive the error, ensure you have installed the SQL Native Driver version 10.0 or version 11.0.

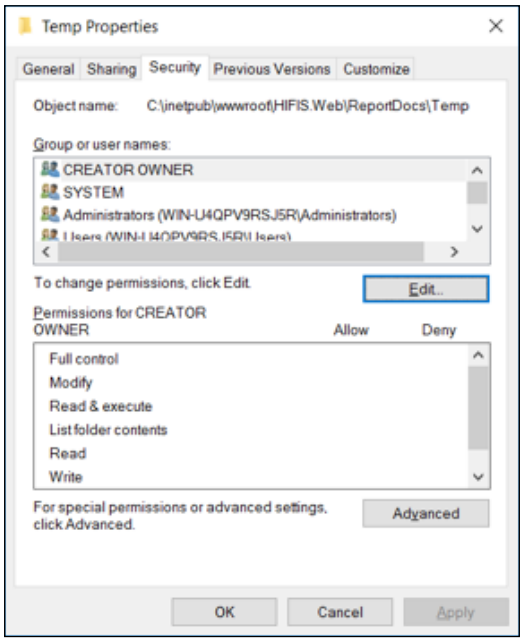
Error: ***"Access to the path C [...] is denied"***

Solution: Create a folder required for Crystal Reports to function properly.

Step 1 From Internet Information Services (IIS) Manager, navigate to the *HIFIS.Web -> ReportDocs -> Temp folder*. Right-click on the Temp folder and select *Edit Permissions*.



Step 2 Select the *Security* tab and then click *Edit*.



Step 3 On the list, scroll down to find the group called *IIS_IUSRS* and select it. With the group selected, place a check-mark in the *Allow* column for the *Modify* permission as per the image below and click OK. This will resolve the error.