**Installation and Configuration of FTPS on IIS 8.5**

Prepared by:

DCS-Midrange

**Statement of Property Information**

The information in this document is internal to APL. The document may not be disclosed, duplicated or used for any purpose, in whole or in part, outside APL without the prior written consent of APL.

**Document Status**

**Title: Installation and Configuration of FTPS on IIS 8.5 (For Windows Server 2012 R2)**

**Prepared by: DCS Midrange**

**Document Revision History**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Version #** | **Date** | **Modified By** | | | | | **Description** |
| **1.0** | 30-April-2013 | | | Hari | | Initial Document | |
| **2.0** | 25-Jan-2018 | | | Vijay Kumar Rapolu | | Updated Certificate request process | |
| **2.1** | 18-June-2018 | | | Sriram Yelisetty | | Updated data channel ports | |
| **2.2** | 03-Aug-2018 | | | Kranthi Sekhar Anupoju | | Updated versions and configuration process | |
|  |  | |  | |  |  | |
| **Peer Review/Approval** | | |  | |  | |  |
| **Version #** | **Date** | |  | | **Reviewer/Approver Name** | | **Position** |
| **1.0** | 16-May-2013 | |  | | Venkatesh Sethuraman | | Infra Mgr, Wintel Techlgy |
| **2.0** | 25-Jan-2018 | |  | | Venkatesh Sethuraman | | Infra Mgr, Wintel Techlgy |
| **2.1** | 18-Jun-2018 | |  | | Venkatesh Sethuraman | | Sr. Infra Mgr, Wintel Techlgy |
|  |  | |  | |  | |  |

Table of Contents

[1. Introduction 4](#_Toc520807886)

[1.1 Summary 4](#_Toc520807887)

[1.2 Audience 4](#_Toc520807888)

[1.3 Scope 4](#_Toc520807889)

[1.4 Terminology 4](#_Toc520807890)

[2. Installing FTP on 8.5 5](#_Toc520807891)

[2.1 Installing FTP for IIS 8.5 5](#_Toc520807892)

[3. How to setup a FTPS site 7](#_Toc520807898)

[3.1 Prerequisites 7](#_Toc520807899)

[3.2 Requesting for a CMA-CGM SSL Certificate 8](#_Toc520807900)

[3.3 Completing a Certificate request 11](#_Toc520807901)

[3.4 Creating an SSL-enabled FTP Site Using the IIS 8 Manager 13](#_Toc520807902)

[3.4.1: Use the FTP Site Wizard to Create an SSL-based FTP Site 13](#_Toc520807903)

[3.4.2 Configuring Additional FTP SSL Settings 17](#_Toc520807904)

[3.4.3 Configuring Additional FTP Settings 17](#_Toc520807905)

[4. How to configure the access to FTPS site for domain users 19](#_Toc520807906)

[4.1 Configuring the default domain for FTPS site 19](#_Toc520807907)

[4.2 Provide access to domain users to the FTPS site 20](#_Toc520807908)

[5. Contact details 25](#_Toc520807913)

[Appendix](#Appendix) I Setup access to FTPS site for users in DMZ Zone…………………………………26

# Introduction

FTPS in APL is used for secure file transfer with and between operating systems (Windows/Mainframe/Unix systems). FTPS Protocol (FTP over SSL/TLS, FTP+SSL) is a standard where connection between a client and server is encrypted using SSL/TLS. FTPS enables secure authentication and transfer of files through secure socket layer (SSL).

This document comprehensively outlines the process of setting up FTPS server with the required hardening configurations, firewall ports requirement and client to be used for FTPS access. This document can be used for complete end to end implementation of FTPS file transfer solution.

## Summary

This document will walk through the steps for Installing FTP on IIS 8.5, setting up a SSL enabled FTP site with the new FTP user interface in IIS 8.5 on Windows Server 2012 (R2).

This document also outlines the process for users to connect to the FTPS website including the authentication process in FTPS.

## Audience

This document is intended for Regional IT personnel, system integration vendors and service providers who want to create a FTPS 8.5 site using IIS 8.5.

## Scope

The content in the document is applicable to **Windows Server 2012 R2/2016** operating systems having IIS 8.5 or 10 installed.

## Terminology

|  |  |
| --- | --- |
| **Term or acronym** | **Description** |
| Domain users | All users in the domain D1.AD.APL.COM |
| DMZ | Demilitarized zone |
| FTP | File Transfer protocol |
| FTPS | FTP over SSL |
| FTP server or FTPS server | Server on which FTP or FTPS site is hosted |
| IIS | Internet Information Service |
| ICALCS, CALCS | Command line tool in windows server operating system to display or modify discretionary access controlled list (DACL) |
| PCT | Private Communication Technology protocol |
| SSL | Secure Socket Layer protocol |
| SFTP | SSH File Transfer Protocol |
| TLS | Transport Layer Security protocol |

# 

# Installing FTP on IIS 8.5

This section will walk you through the steps to install the new FTP service considering **Windows Server 2012 R2** Operating System (Configuration process and UI for Windows Server 2016 is the same)

**Overview of IIS Versions and Compatibility**

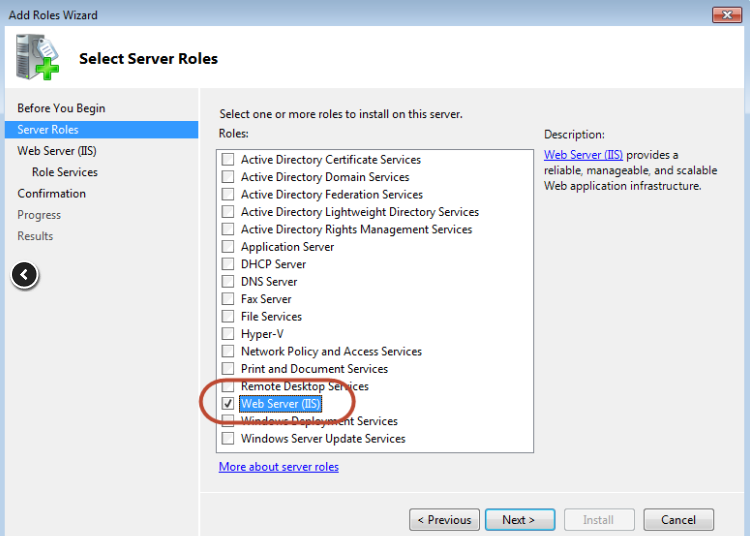
|  |  |
| --- | --- |
| **Version** | **Notes** |
| IIS 10 | The FTP 10 service ships as a feature for IIS 10 in Windows Server 2016 |
| IIS 8.5 | The FTP 8.5 service ships as a feature for IIS 8.5 in Windows Server 2012 R2. |

* IIS 8.5 is included in [Windows Server 2012 R2](https://en.wikipedia.org/wiki/Windows_Server_2012_R2) and [Windows 8.1](https://en.wikipedia.org/wiki/Windows_8.1). This version includes Idle Worker-Process page-out, Dynamic Site Activation, Enhanced Logging, ETW logging, and Automatic Certificate Rebind
* IIS 10 is included in [Windows Server 2016](https://en.wikipedia.org/wiki/Windows_Server_2016) and [Windows 10](https://en.wikipedia.org/wiki/Windows_10). This version includes support for [HTTP/2](https://en.wikipedia.org/wiki/HTTP/2)

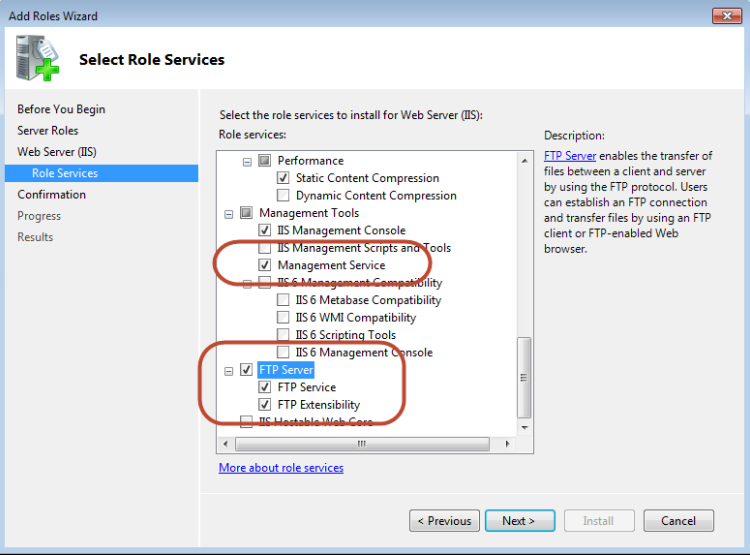
## Installing FTP for IIS 8.5

**IIS 8.5 for Windows Server 2012 R2**

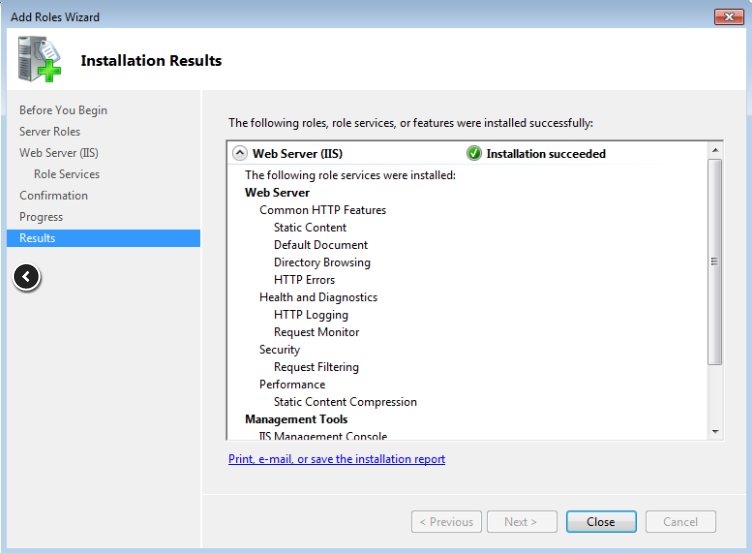
1. On the taskbar, click **Start**, point to **Administrative Tools**, and then click **Server Manager**
2. In the **Server Manager** Hierarchy pane, expand **Roles**, and then click **Web Server (IIS)**
3. In the **Web Server (IIS)** pane, scroll to the **Role Services** section, and then click **Add Role**



1. On the **Select Role Services** page of the **Add Role Services Wizard**, select **FTP Server and FTP Extensibility**.



1. Select **FTP Service**. (**Note**: To support ASP.NET Membership or IIS Manager Authentication for the FTP service, you will also need to select **FTP Extensibility**)
2. Click **Next**, On the **Confirm Installation Selections** page, click **Install**

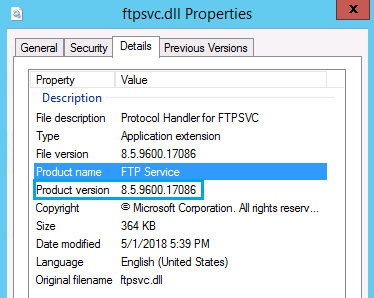


# How to setup a FTPS site

Before going through this section, it is strongly recommended to go through the above section “Installing FTP 8.5 and IIS 8.5 to make sure that all the correct components of FTP and IIS are installed.

**FTPS Version:**

Since FTP Server runs within svchost.exe, it can be determined by checking the property details of the following DLL: **C:\Windows\System32\inetsrv\ftpsvc.dll**



This section walks you through the steps for configuring an FTP site to use SSL with the new FTP user interface which includes

* Prerequisites
* Requesting for a CMA-CGM SSL certificate and complete the certificate request.
* Creating an SSL-enabled FTP site using the IIS 8.5 manager

**Note**: This walk-through contains a series of steps in which you log in to your FTP site using an account having local administrator rights. If you prefer to use a separate user account, you will need to create the appropriate folders and set the correct permissions for that user account when necessary.

## Prerequisites

The following items are required to be installed to complete the procedures in this section:

1. IIS 8.5 must be installed on your Windows 2012 R2 Server and IIS 10 if it is Windows 2016 Server, and the Internet Information Services Manager must be installed.
2. Make sure the new FTP 8.5 service is installed.
3. You will need to create a root folder for FTP publishing:
   * Create a root folder. In this case creating at “D:\FTPSROOT”, but the root folder can be created any drive as per the requirement.
   * Set the permissions to allow access for the administrators group:
     + Open a command prompt.
     + Type the following command:  
       ICACLS "D:\FTPSROOT" /Grant Administrators:F /T
     + Close the command prompt.

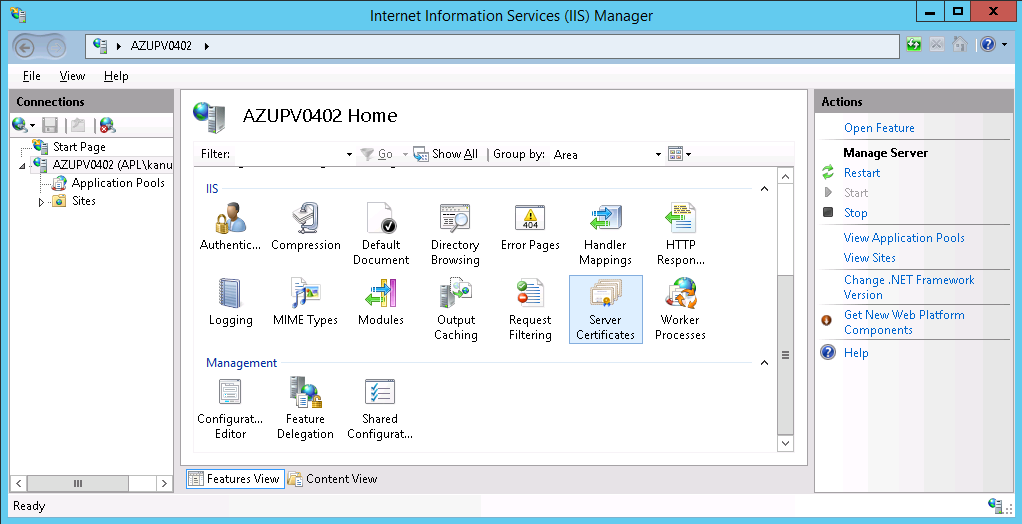
**Note**: The settings listed in this document specify “D:\FTPSROOT" as the path to your FTP site. You are not required to use this path; however, if you change the location for your site you will have to change the site-related paths that are used throughout this document.

## Requesting for a CMA-CGM SSL Certificate

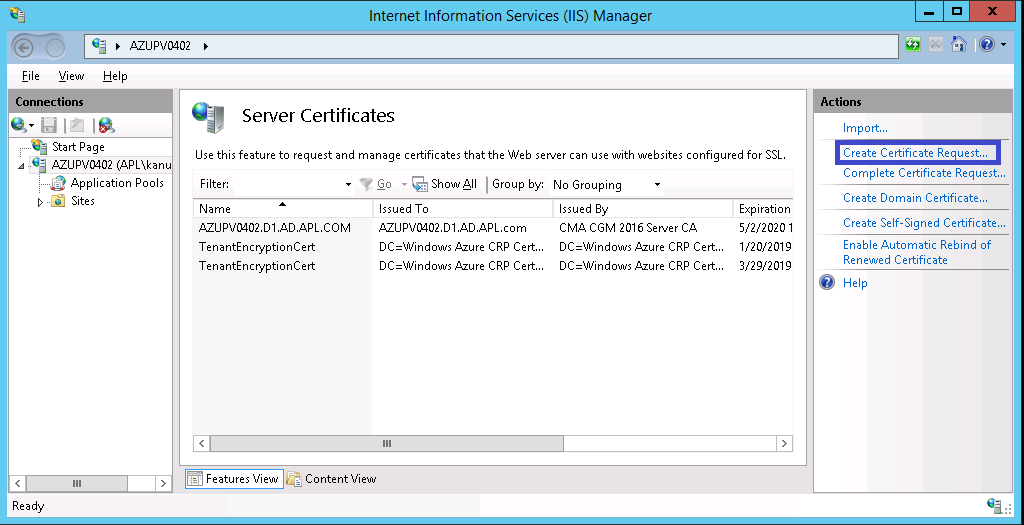
Before we create a SSL enabled FTP site, it is recommended to have a certificate created to enable SSL communication. In our APL environment, we use CMA-CGM internal certificate for Internal SSL communication.

Note: If you are setting up an FTP site for Internet-based activity, you would need to follow the process to obtain a third-party CA (Entrust, VeriSign etc.) certificate from GIO Security team.

1. Open the Internet Information Services (IIS 8.5) Manager.
2. Click your computer at the top node of the Connections tree, and then double-click the Server Certificates feature.



1. In the **Actions** menu (right pane), click **Create Certificate Request**.

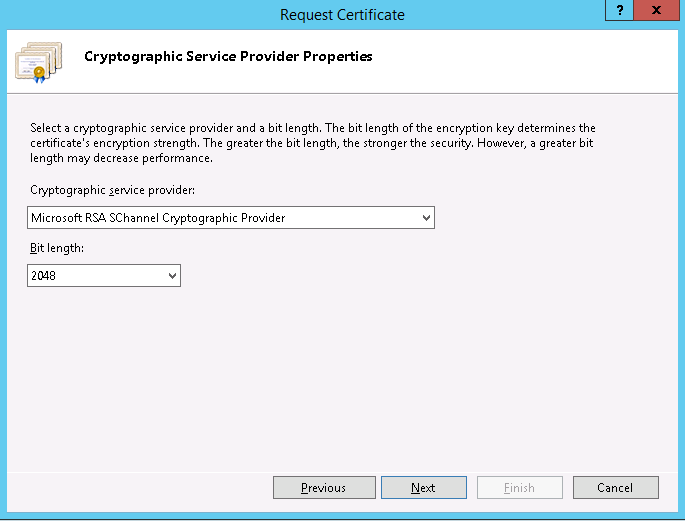


1. In the **Request Certificate** wizard, on the **Distinguished Name Properties** page, provide the information specified below and then click **Next**.

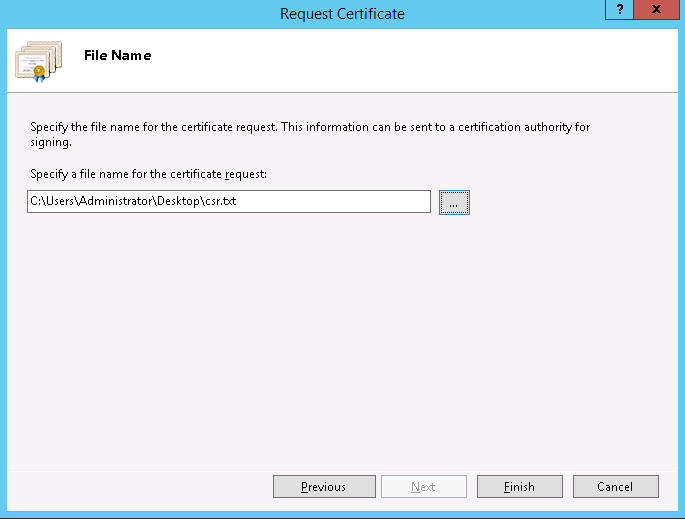
Among other information requested when generating a CSR, some of the data relating to Distinguished Name properties are:

* + Common Name (CN) – Provide the URL of the resource.
  + Organization (O) – Use **APL Limited** when submitting for “apl.com” and **CMA CGM** for “cma-cgm.com” domains.
  + Organizational Unit (OU) – Department of the organization like Messaging, GIO Middleware, Logistics IT, Remodel CRM etc.
  + City/Locality (L) – Location of the server where it is hosted like NOL Bldg, SG Non-prod DC, Plano DC, Singapore DC, etc.
  + Country/Region (C) – Location of the server where it is hosted like SG, US, etc.

1. On the **Cryptographic Service Provider Properties** page, provide the information specified below and then click **Next**.



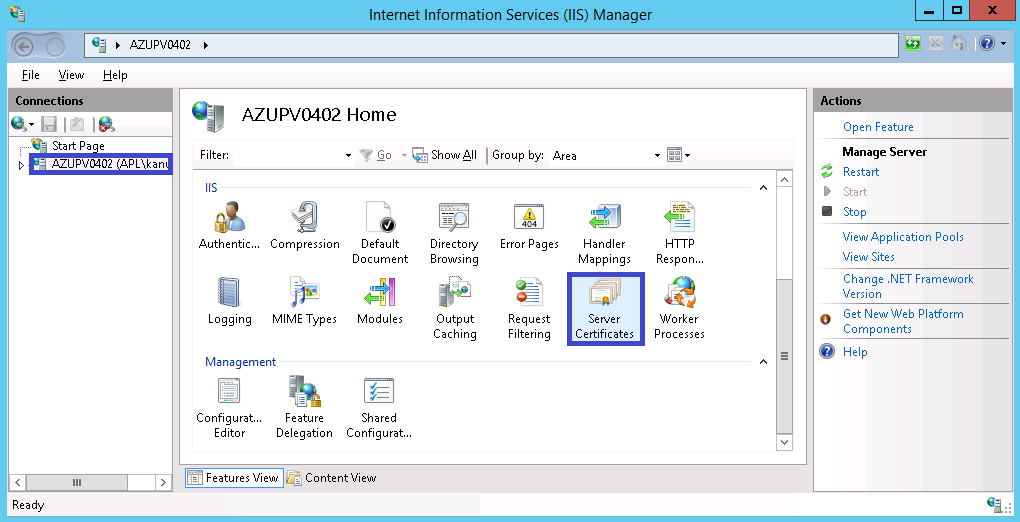
1. On the **File Name** page, under **Specify a file name for the certificate request**, click the **…** button to specify a save location for your CSR.



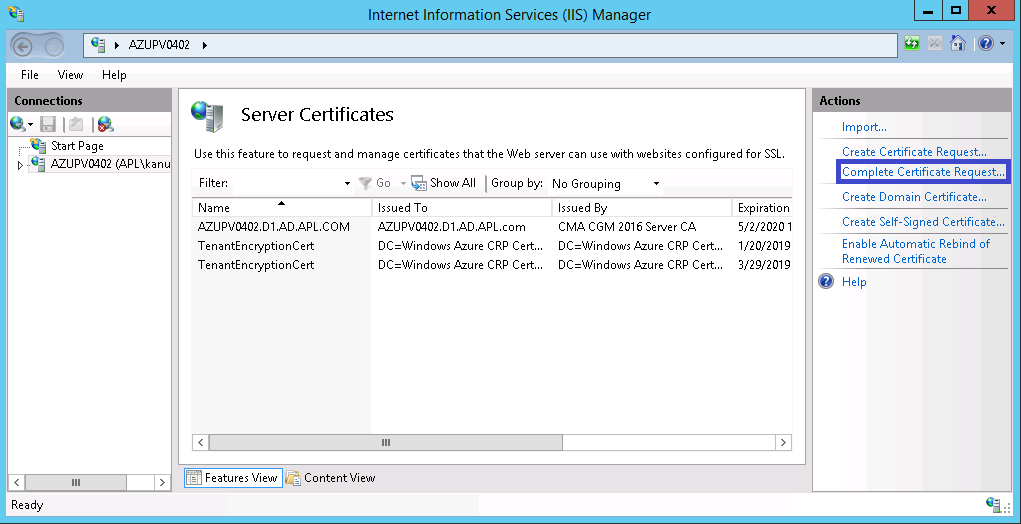
1. When you are done, click **Finish**.
2. Drop an Email to unipass Support team <[ho.SUPPORT\_UNIPASS@cma-cgm.com](mailto:ho.SUPPORT_UNIPASS@cma-cgm.com)> and APL security <[IT.security.operations@apl.com](mailto:IT.security.operations@apl.com)> attaching the CSR file requesting a certificate.

## Completing a Certificate request

1. On the server where you created the CSR, Open Internet Information Services (IIS) Manager (click **Start > Administrative Tools > Internet Information Services (IIS) Manager**).
2. In the **Connections** pane, locate and click the server.
3. In the server **Home** page (center pane) under the **IIS** section, double-click **Server Certificates**.



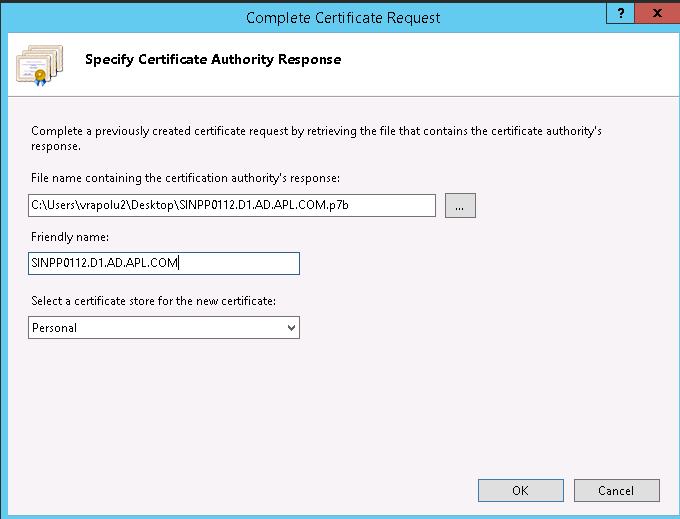
1. In the **Actions** menu (right pane), click **Complete Certificate Request**.



1. In the **Complete Certificate Request** wizard, on the **Specify Certificate Authority Response** page, provide the following information:
   1. **File name containing the certificate authority's response:**

Click the **…** button to locate the certificate file you received from CMA-CGM.

* 1. **Friendly name:** FQDN of the server hosting this certificate.



## Creating an SSL-enabled FTP Site Using the IIS 8.5 Manager

Creating an SSL-enabled FTP Site Using the IIS 8.5 Manager has two steps:

Step 1: Use the FTP Site Wizard to Create an SSL-based FTP Site

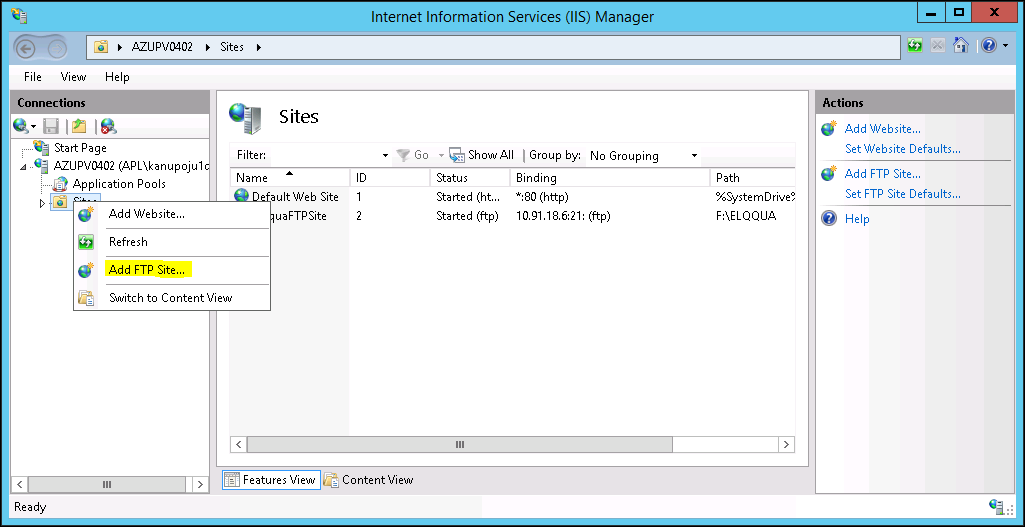
Step 2: Configuring Additional FTP SSL Settings

### 

### 3.4.1: Use the FTP Site Wizard to Create an SSL-based FTP Site

In this first step, you create a new FTP site that can only be opened using your administrator account.

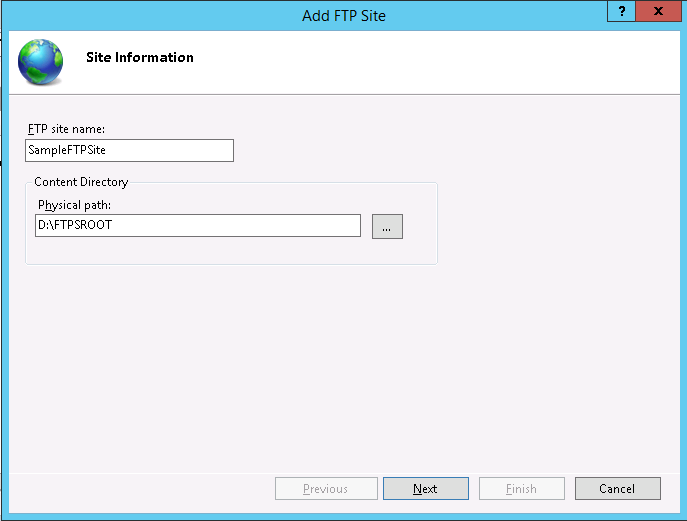
1. Go to IIS Manager. In the connections pane, click the Sites node in the tree.
2. Right-click the Sites node in the tree and click Add FTP Site, or click Add FTP Site in the Actions pane.



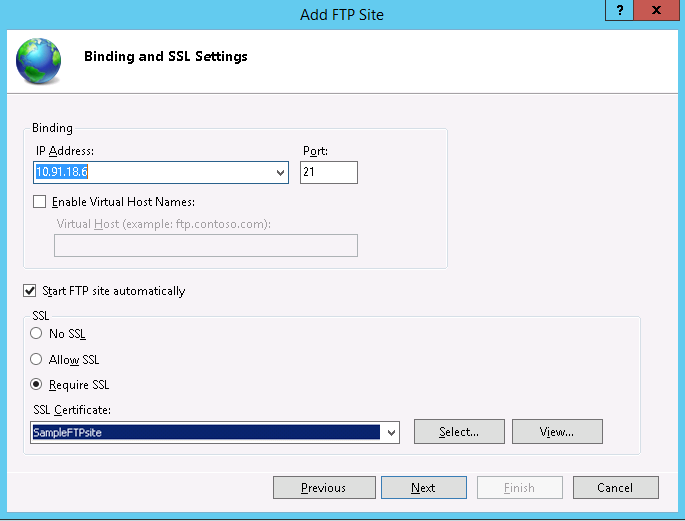
1. When the **Add FTP Site** wizard appears:

Now add a FTP site name and a file location for the public files.

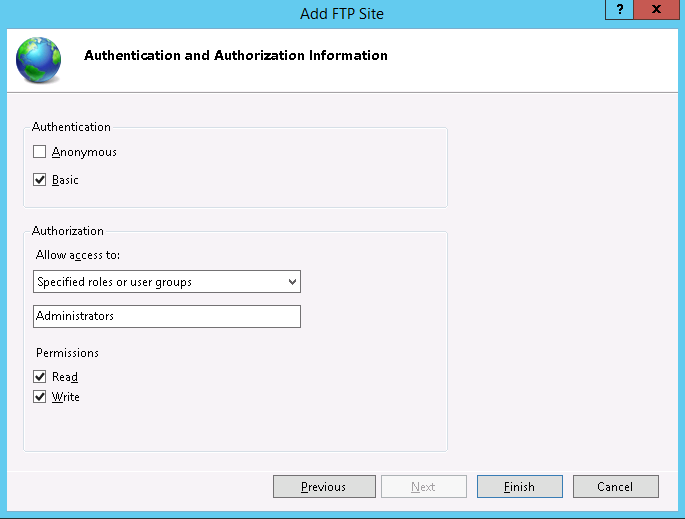
* 1. Enter the name of the FTPsite in the **FTP site name** box, and then for physical path navigate to the folder that you created in the Prerequisites section. In this case “SampleFTPsite” is the name of the FTPsite and “D:\FTPSROOT” is the physical path.
  2. Click **Next**.



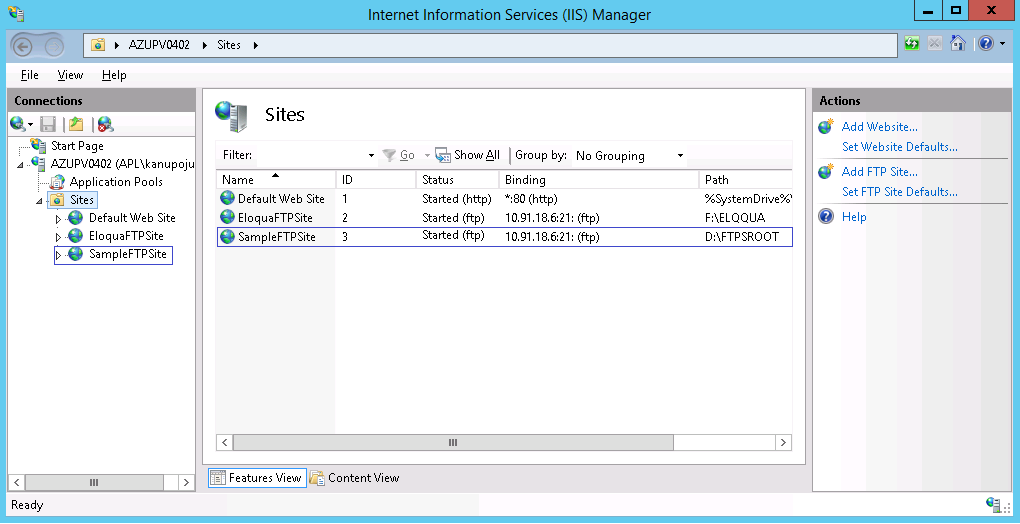
1. On the next page of the wizard:
   1. Choose an IP address for your FTP site from the **IP Address** drop-down. (In this case 10.91.18.6)
   2. You would normally enter the TCP/IP port for the FTP site in the **Port** box. In this case, choosing the default port of 21
   3. For this walk- through, host name is not used, so the **Virtual Host** box is blank
   4. Make sure that the **Certificates** drop-down is set to your SSL certificate. For example, if you followed the optional step to create a self-signed certificate, the drop-down box should say “SampleFTPsite"
   5. Make sure that the **Require SSL** option is selected. Both control channel and data channel are encrypted by selecting this option
   6. Click **Next**.



1. On the next page of the wizard:
   1. Select **Basic** for the **Authentication** settings
   2. For the **Authorization** settings:
      1. Choose "Specified roles or user groups" from the **Allow access to** drop-down. Or you can choose specified users for giving access to specified user.
      2. Type "administrators" in the next box. (in this case administrators group will be given access to ftp site)
      3. Select **Read** and **Write** for the **Permissions** option
   3. When you have completed these items, click **Finish**.



1. You will see the below screen after you click finish.



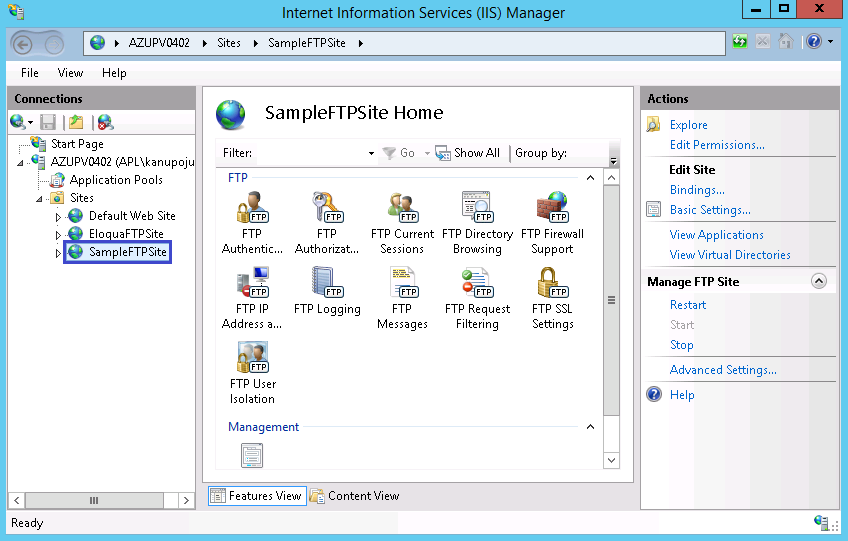
1. Now a new SSL-based FTP site has been created.

### 

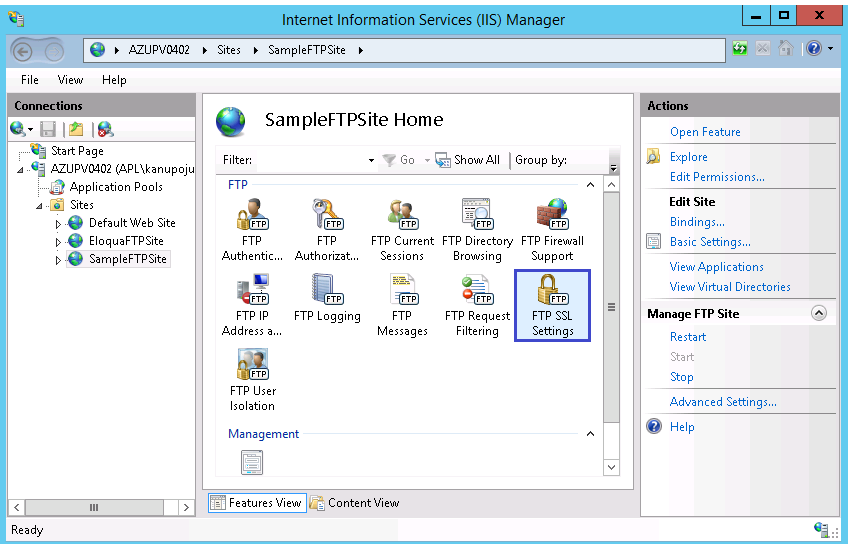
### 3.4.2 Configuring Additional FTP SSL Settings

The SSL policy for FTP is customizable on a site-by-site basis. In this step, you configure additional SSL settings for your FTP site to use 128-bit encryption. We will also configure SSL policy for internal FTP sites.

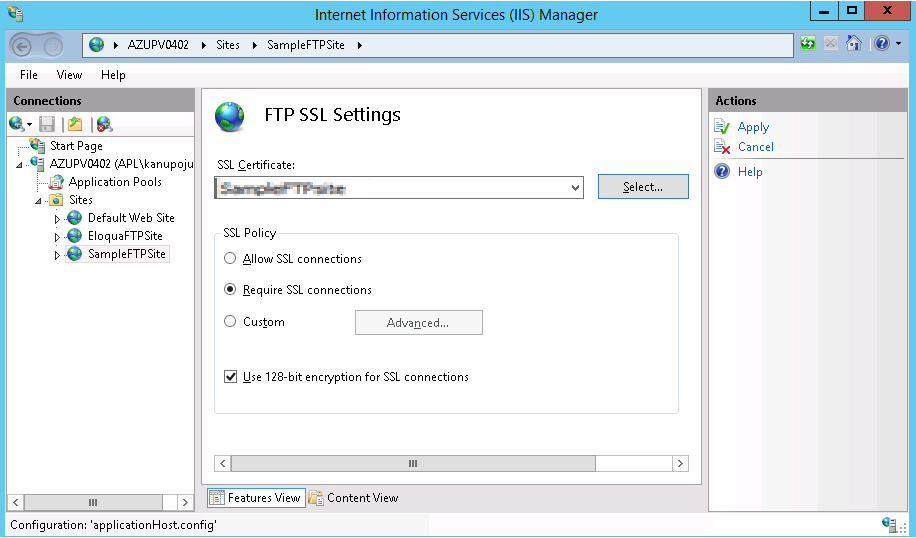
1. Go to the IIS 8.5 Manager. Click the node for the FTP site that you created in Step 1. The icons for the entire FTP configuration options will display



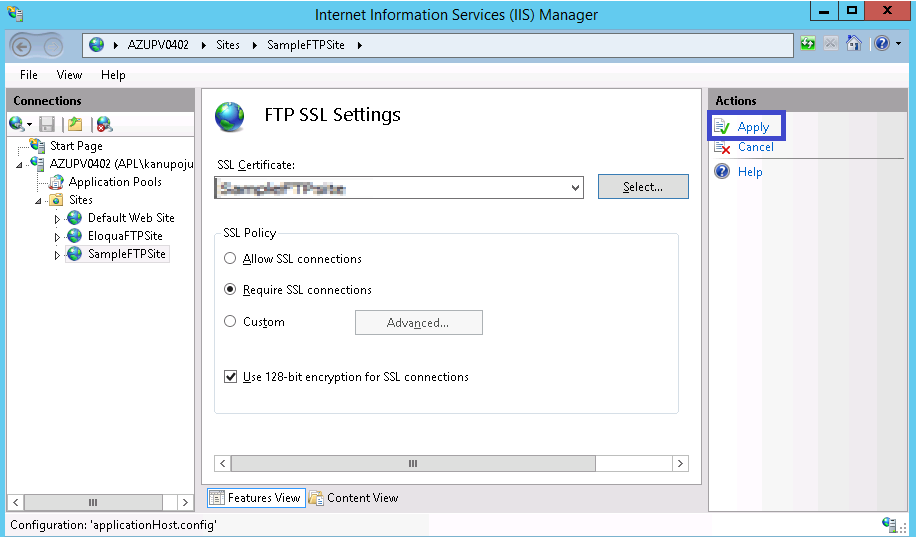
1. In order to configure the SSL options, double-click the **FTP SSL Settings** icon to open the SSL settings feature page.



1. When the **FTP SSL Settings** page displays, check the box adjacent to “Use 128-bit encryption for SSL connection.



1. On the **FTP SSL Settings** page, click **Apply** in the **Actions** pane to save the SSL settings.



**Note**: If 128-bit encryption is configured, then users must use FTP clients that support 128-bit encryption to access the FTPS site.

1. **FTP SSL Policy for both internal FTP site and external FTP site is set to** Require SSL Connections policy.

### 

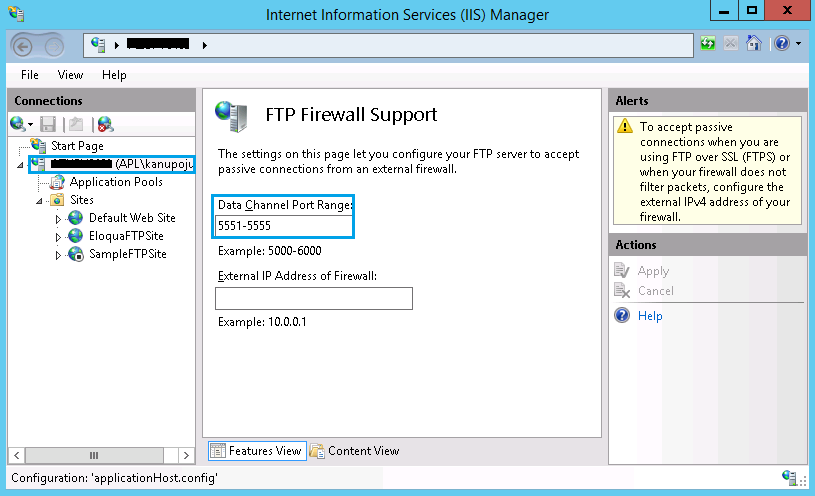
### 3.4.3 Configuring Additional FTPS Settings

This step is required to control data ports through which the FTPS site will accept the passive connections.

Set the Data channel port range on the FTPS site.

For this goto run -> inetmgr.msc -> click on the server name -> FTP Firewall Support ->set the required Data channel port range -> click Apply

**(Note: - Please try to use the Data channel port range 5551-5555)**

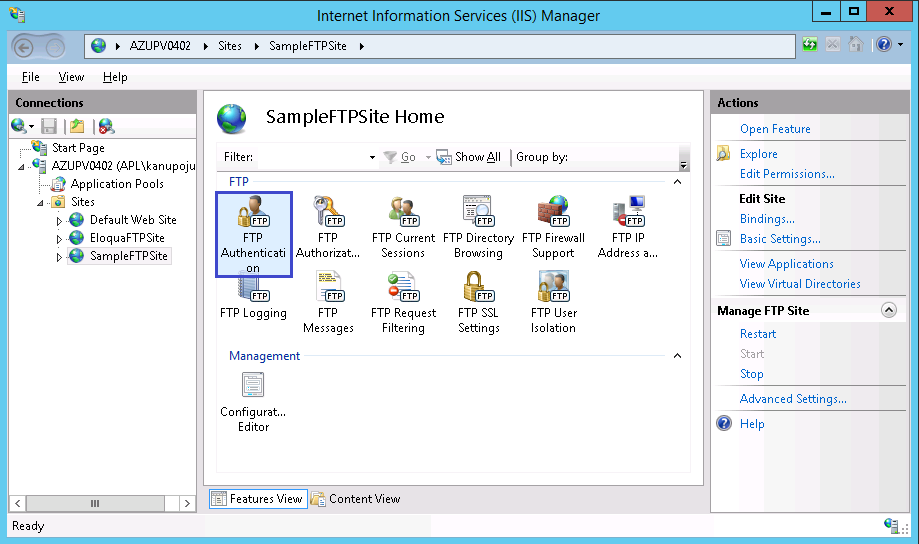
****

# How to configure the access to FTPS site for domain users?

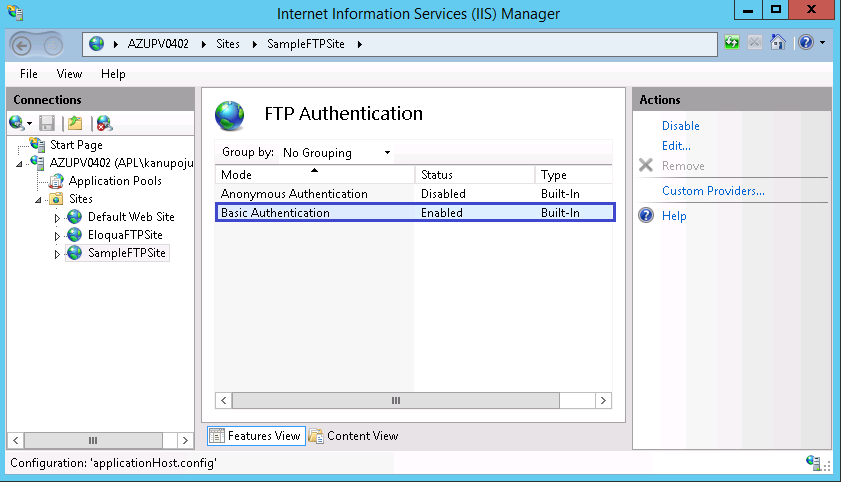
This section walks you through steps to configure Default domain in a FTP site and how-to setup access to FTP site for the domain users.

## Configuring the default domain for FTPS site

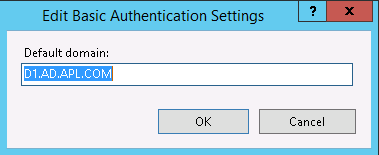
1. Open the IIS console. Go to the FTP website for which the default domain must be configured. Click on the website (In this case SampleFTPsite). Click on FTP Authentication as shown in the below picture.



1. Double click on FTP Authentication. A console will open as shown in the below picture. Select Basic Authentication in the central pane and select Edit in the Actions pane.



1. A new window will open. Enter the domain name for which you want to allow the authentication. Click OK.



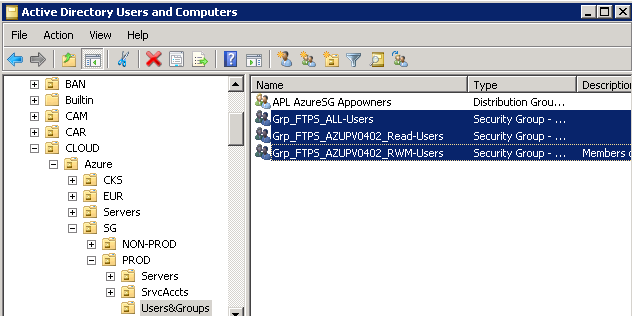
Now we have configured the default domain. But it doesn’t guarantee all the domain users can authenticate to the FTP site.

## Provide access to domain users to the FTPS site

1. Create groups to access FTPS server. Go to ADDS: D1.AD.APL.COM > Cloud > Azure > SG > Prod > Users&Groups (**In this case**)

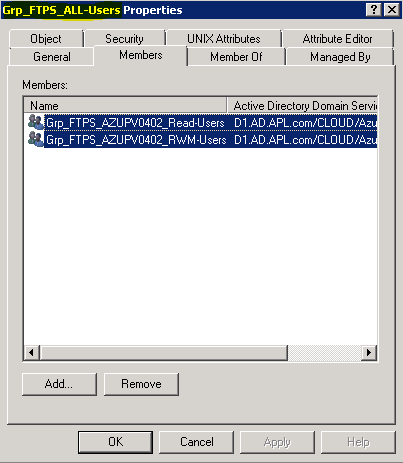
Grp\_FTPS\_ServerName\_Read-Users (this is the naming convention followed while creating groups)

Grp\_FTPS\_ServerName\_RWM-Users

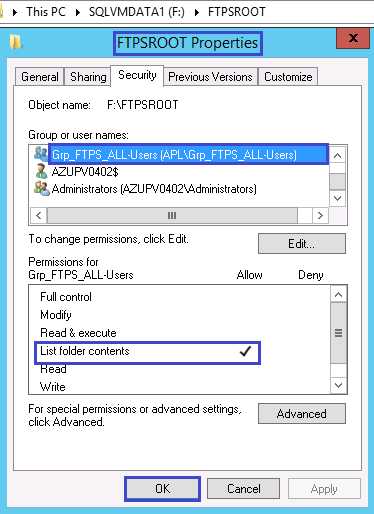


1. The groups **Grp\_FTPS\_AZUPV0402\_Read-Users** and **Grp\_FTPS\_AZUPV0402\_RWM-Users** should be added to **Grp\_FTPS\_All\_Users**, which is part of **FTPS Authorization rules** for access.

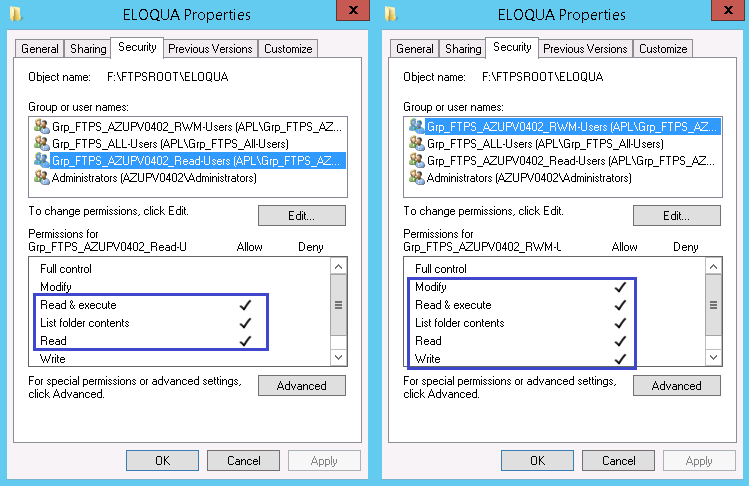
**Note:** Every sub-folder under FTPSROOT folder should have specific Read and RWM groups created on AD and users be added to respective groups ONLY for access accordingly



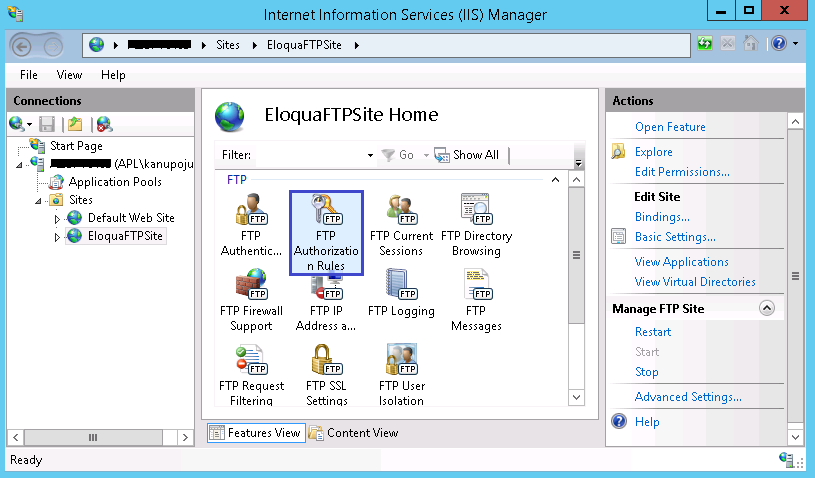
1. Now, on the root folder (D:\FTPSROOT), set ONLY list permission for this group.



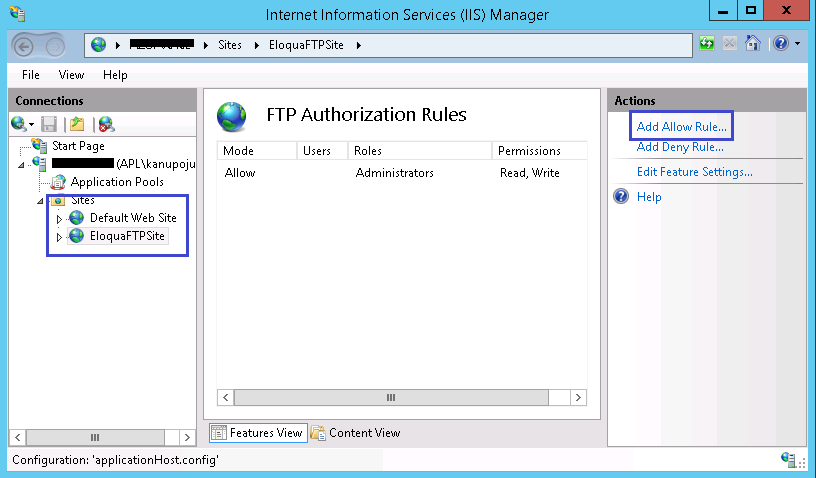
1. On Eloqua (F:\FTPSROOT\ELOQUA), Set permissions with Read and RWM groups respectively



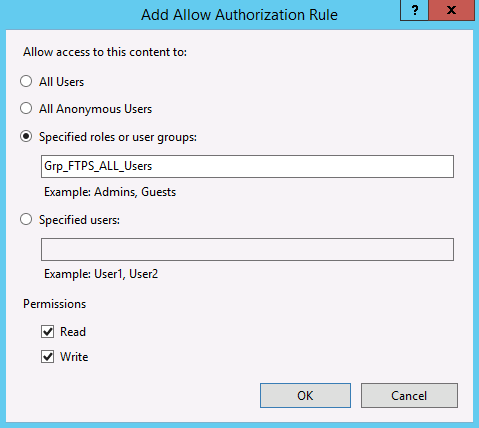
1. Now we have to allow the group to have read and write access to the FTP site. For that, go to IIS manager console -> FTP Authorization rules.



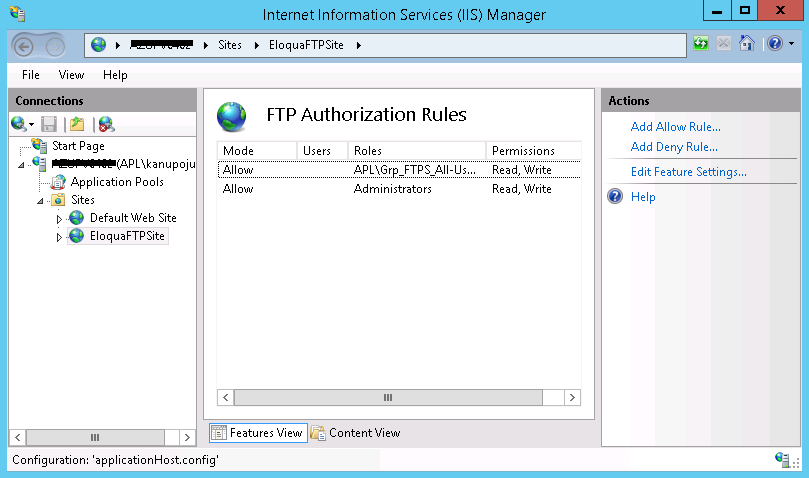
1. After you double click the FTP authorization rules. A console will open. Select Add allow rule



1. A new window will open. Add the group name (APL\Grp\_FTPS\_All-Users) under “specified roles or user groups”. Give read and write access. Click OK



1. The group Grp\_FTPS\_All\_Users (in this case) has read and write access on the FTP Site as show below.



Now if any domain user wants to have access to FTPS site, add the user to the local groups created for FTPS users on the FTPS server and grant necessary Read/Write permission to the respective subfolder.

Please go through Appendix I to setup access to FTPS site for users in DMZ zone.

# Contact details

For any suggestions and queries on this document please email us at [**AMS.msinfra@apl.com**](mailto:AMS.msinfra@apl.com)

**Appendix I:**

**How to Setup Access to FTPS site for users in DMZ zone**

This section walks you through steps to setup access to FTP site for the users in the DMZ zone.

There are two types of user authentication, one using windows users (Windows users FTP authentication) and another using IIS 8.5 Manager accounts (IIS authentication). We will use IIS authentication in order to setup access to FTPS site for users in DMZ zone. For users who will need to access the external hosted FTPS site from DMZ zone, IIS 8.5 manager accounts will be created with required privileges.

The following are some of the things to consider while using the IIS authentication in a FTP site.

1) You cannot restrict access to individual IIS 8.5 manager users to a specific folder inside the root folder.

2) IIS 8.5 manger users will either have read or write permission on the root folder and on all the files and folders inside the root folder.

3) If a FTP site is created exclusively for domain users, then don’t use IIS 8.5 authentication. Its preferable to create different sites one for domain users and other for IIS 8.5 manager users if required. However, if it’s necessary to access the same site by domain users and IIS 8.5 manager users, then grant the permissions on the root folder and subfolder as necessary (Please make a note of point 1 and point 2).

For the ease of use, the FTP site created earlier is used here. It is assumed that a new site has been created with basic authentication enabled (domain has been set) and ONLY Local Administrators group on the server have been granted full read and write access to the site. The following section explains the steps how to configure FTP authentication for IIS 8.5 manager accounts.

1. We have to grant special permissions to the Network Service to be able to use the IIS 8.5 management service. (The "Network Service" account is used by the COM process that handles authentication extensibility; therefore, you must grant the account specific permissions to certain folders to enable this form of authentication. We will grant the "Network Service" account "read" permissions to the IIS "config" folder)
2. Open the command prompt. Type the following:

ICACLS "%SystemDrive%\Windows\System32\inetsrv\config" /Grant "Network Service":R /T

ICACLS "%SystemDrive%\Windows\System32\inetsrv\config\administration.config" /Grant "Network Service":R

ICACLS "%SystemDrive%\Windows\System32\inetsrv\config\redirection.config" /Grant "Network Service":R

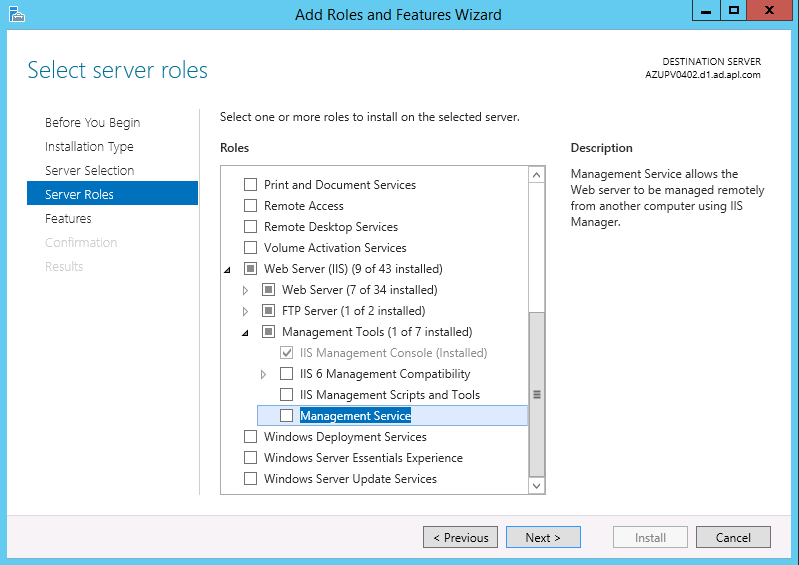
1. Now we have to give rights to the Network Service to the root FTPS folder, in our instance this is D:\FTPSROOT. When you run this command replace the directory with your own. Open the command prompt. Type the following:

ICACLS "D:\FTPSROOT" /Grant "Network Service":M /T

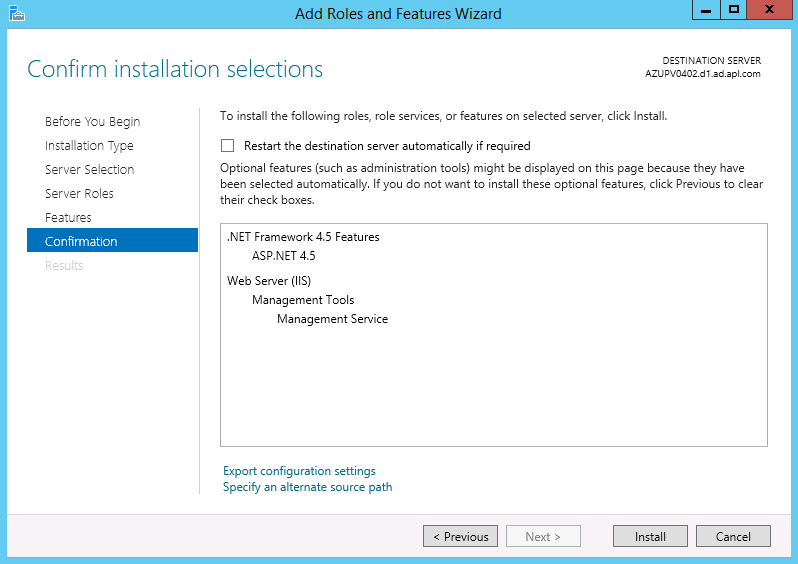
**Note**: The settings listed in this walkthrough specify “D:\FTPSROOT" as the path to your FTPS site. You are not required to use this path; however, if you change the location for your site you will have to change the site-related paths that are used throughout this walkthrough

Next we need to install the IIS 8.5 management service on the server.

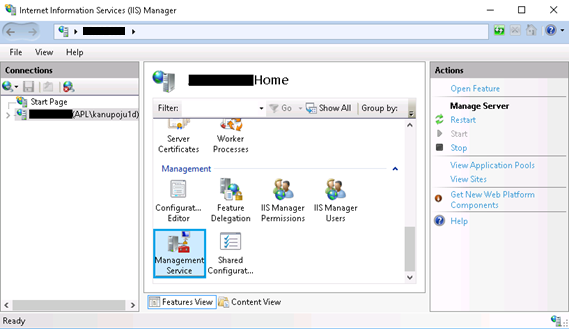
1. Open the Server Manager
2. Open the **Roles**, find the **Web Server (IIS)** role, and click on **Add Role Services**.



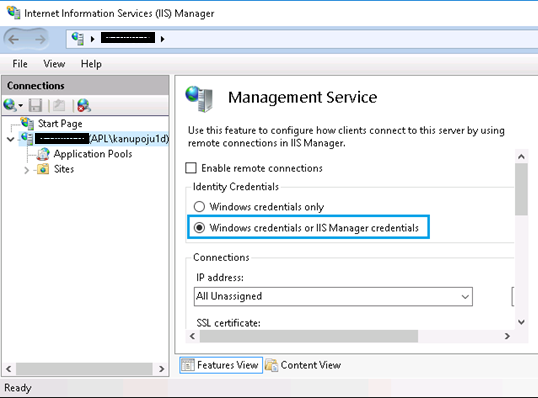
1. In the **Select Role Services** window scroll down till you find **Management Service**, if it is unchecked then place a check mark next to it and click **Next**. If there are any other required features that also need to be installed, you will be prompted to install those
2. Next you will have a summary screen of everything that is going to be installed, click **Install** to start the process.



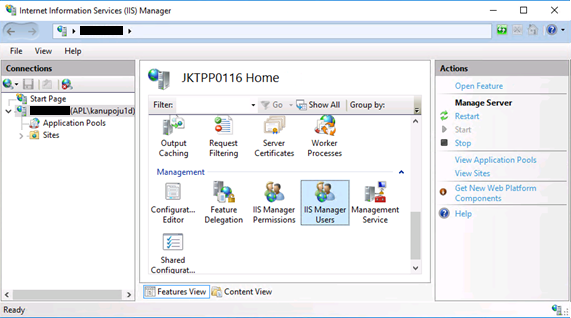
1. The next window will show you the progress of the installation process
2. Installation Results window will appear when the installation is finished, click on **Close** when done.
3. Open IIS Manager. Select the server in IIS Manager; scroll down in the center pane to **Management Service** and click on it



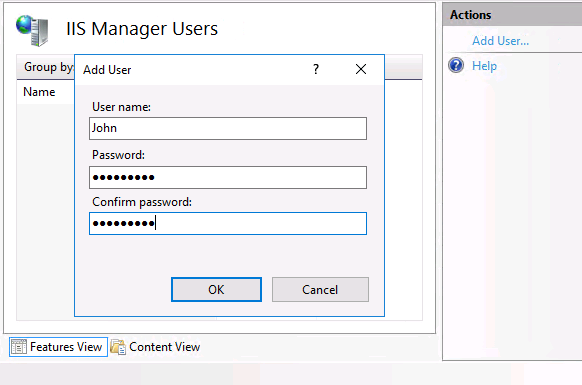
1. In the Management Service pane, look for the **Identity Credentials** box and select **Windows credentials or IIS Manager Credentials**, then click **Apply**.



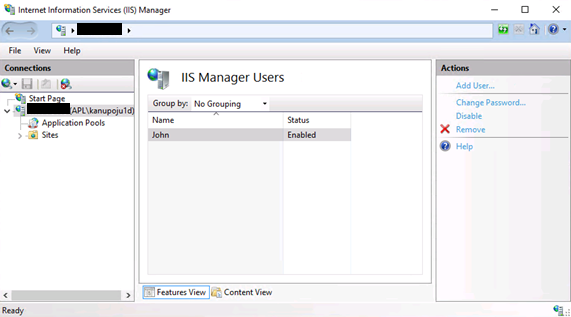
1. In the connections pane select the server you are working on, and double click on **IIS Manager Users**.



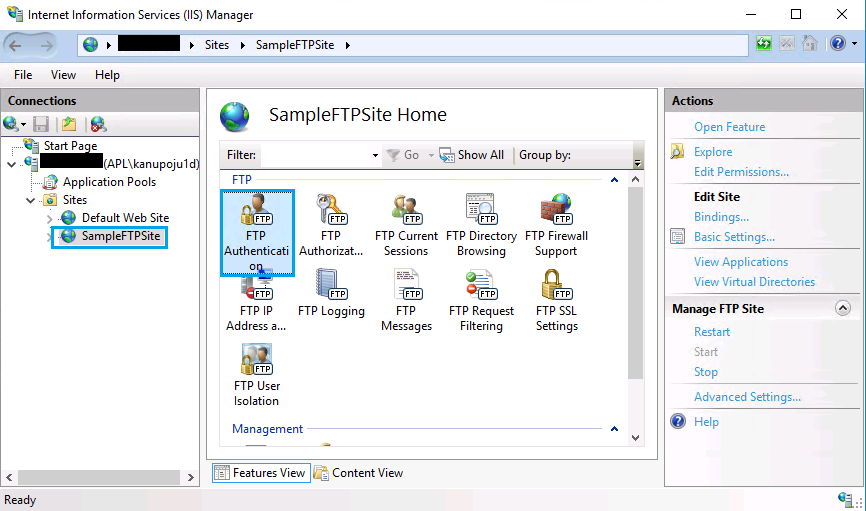
1. Click on **Add User …** in the Actions pane.
2. Now you will create a user account that can be used, in our case we will add **John** and enter a password for that user.



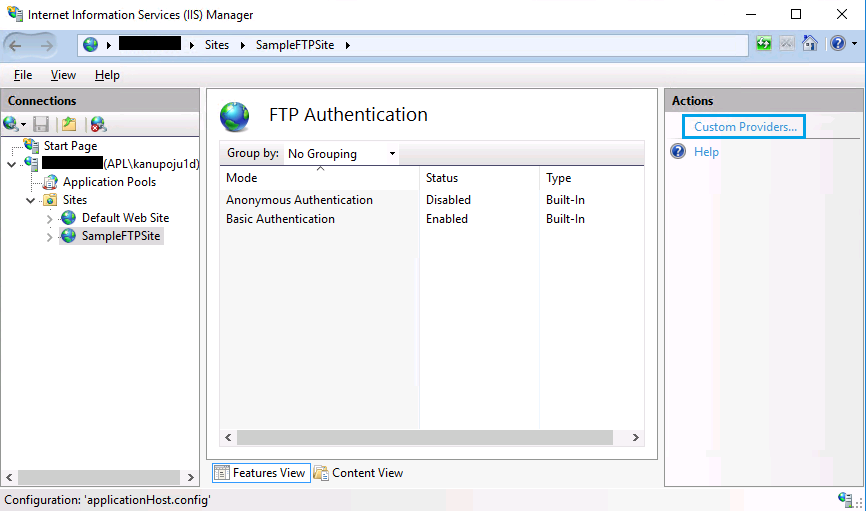
1. You will now see that the user is created and you can do some limited administration in this panel for this user, including Disable User and Change Password.



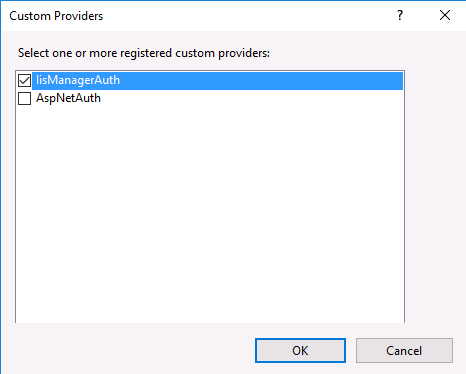
1. Now click the site you want to configure to use IIS 8.5 Manager Authentication in the connections pane, choose **FTP Authentication** in the center pane.



1. Click on **Custom Providers** in the action pane.

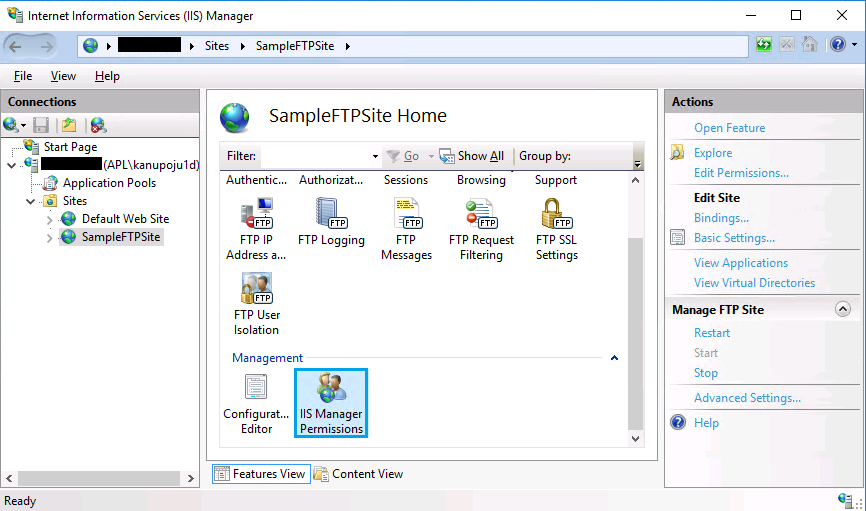


1. In the Custom Providers dialog window place a check next to **IisManagerAuth**, and then click **OK**.

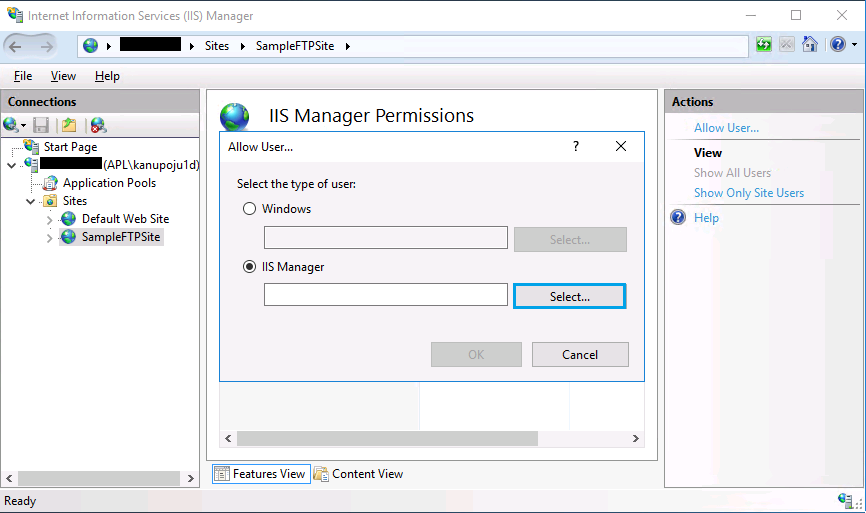


Your **FTP Authentication** page should now show both **Basic Authentication** and **IIS Manager Authentication** enabled.

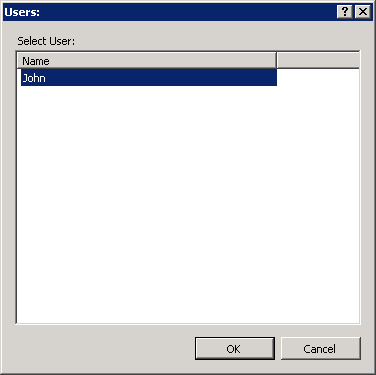
1. Now let’s add the user we created earlier by selecting the FTP site in the connections pane and then select **IIS Manager Permissions** in the center panel.



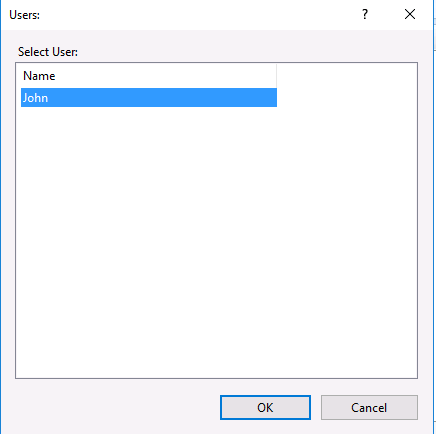
1. Click on **Allow User …** in the Actions pane
2. The **Allow User …** dialog box now shows both types of users, **Windows & IIS Manager**. In our case we are going to click the **Select …** button.



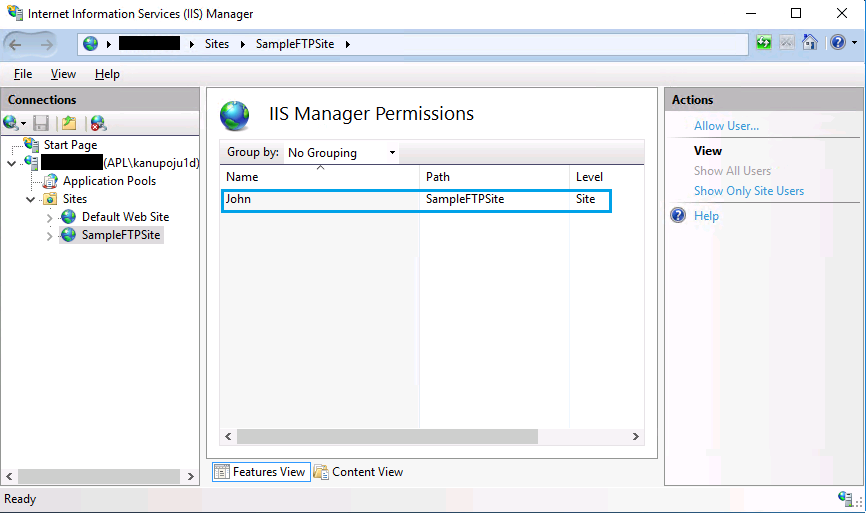
1. In the **Users** dialog select the user, (John in our case) and click **OK**.



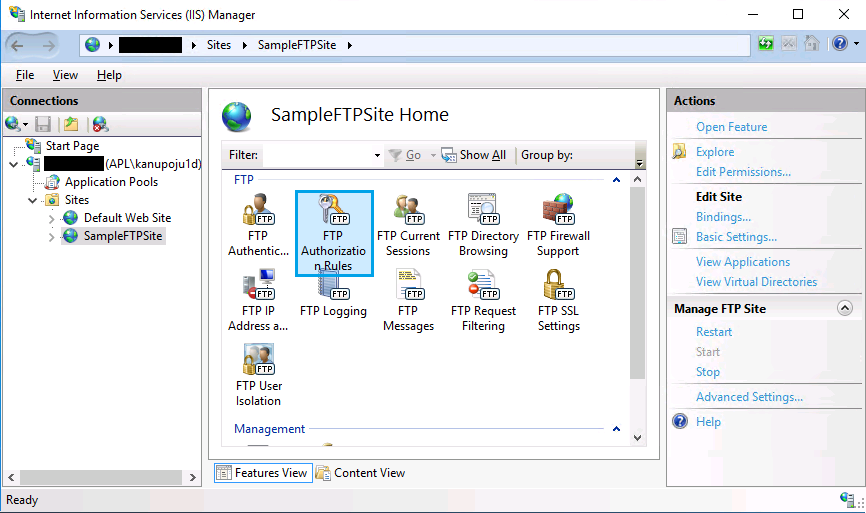
1. Click **OK** to continue and add the user to IIS Manager Permissions.



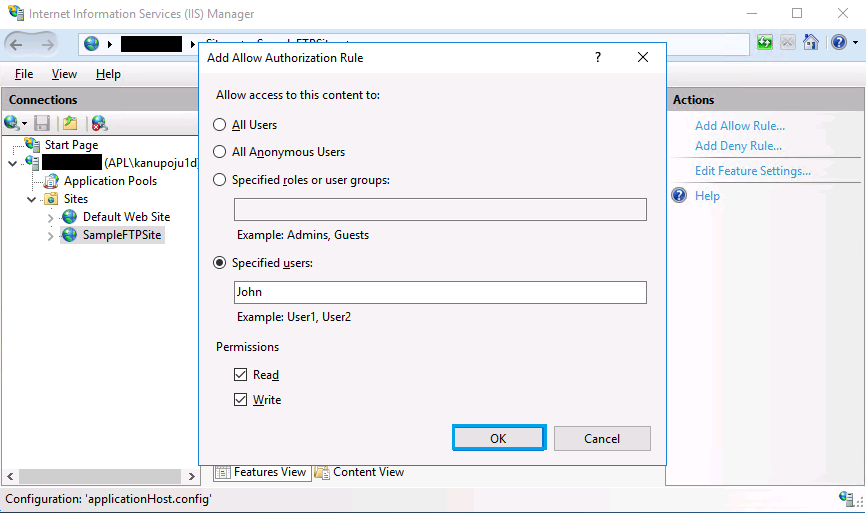
After you click OK. The below screen appears.



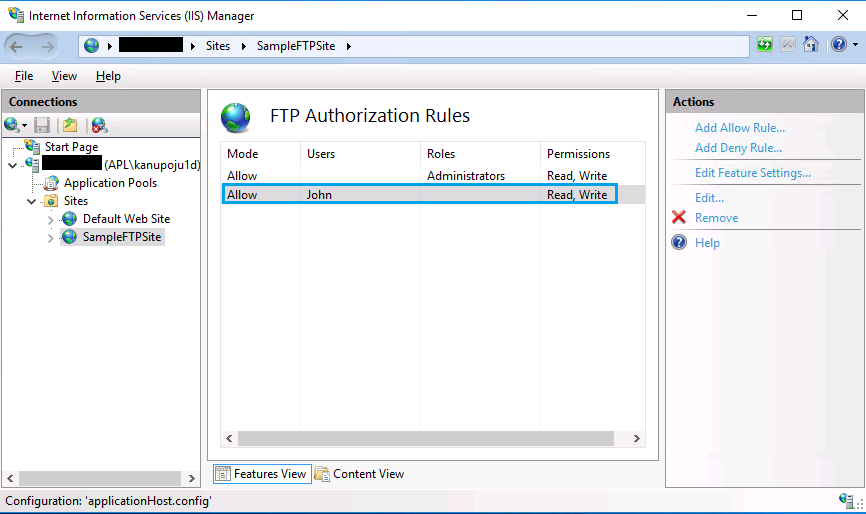
1. Now we’ve to add an authorization rule, so let’s choose the site again in the connection pane, then **FTP Authorization Rules**, in the central pane.



1. Select **Add Allow Rule …** in the actions pane.
2. **Add Allow Authorization Rule** dialog box is next, so select **Specified users** and type the users’ names in, separated by commas. Select the checkbox next to either or both **Read/Write** permissions, and click **OK**. (You can give the access based on your requirements)



1. Click Ok. The below screen appears. You can see John added over there.



This completes the setup and configuration of FTP authentication for IIS 8.5 manager accounts.