Internet Information Services (IIS)

Aidan Fetter

11/06/2023

1. What is ISS?

Internet Information Services (ISS) is a web server built for a Windows Server (such as Windows 2019 Server) meant to host just about anything on the internet. The service accepts HTTP(S) requests from remote clients and returns the appropriate response to create the web application. This allows anything from LANs (such as your home network) to WANs (such as the Internet) to both share and deliver information with each other either locally or globally. IIS supports a variety of services, including HTTP, HTTPS, FTP, FTPS, and SMTP.

- Newest IIS version (as of November 2023): IIS 10.0 version 1809, which is compatible with Windows 10 and Windows Server 2019

1.1. Inner workings of IIS

IIS servers produce responses based on the Active Server Page (ASP).net framework. When a request is sent to an IIS server, the server takes the request and sends it to the ASP application. The application then produces a response and sends it back to the IIS server and the client. Therefore, it can be said that the IIS works as a “middle-man” between the client and the ASP application.

2. IIS Installation and Configuration

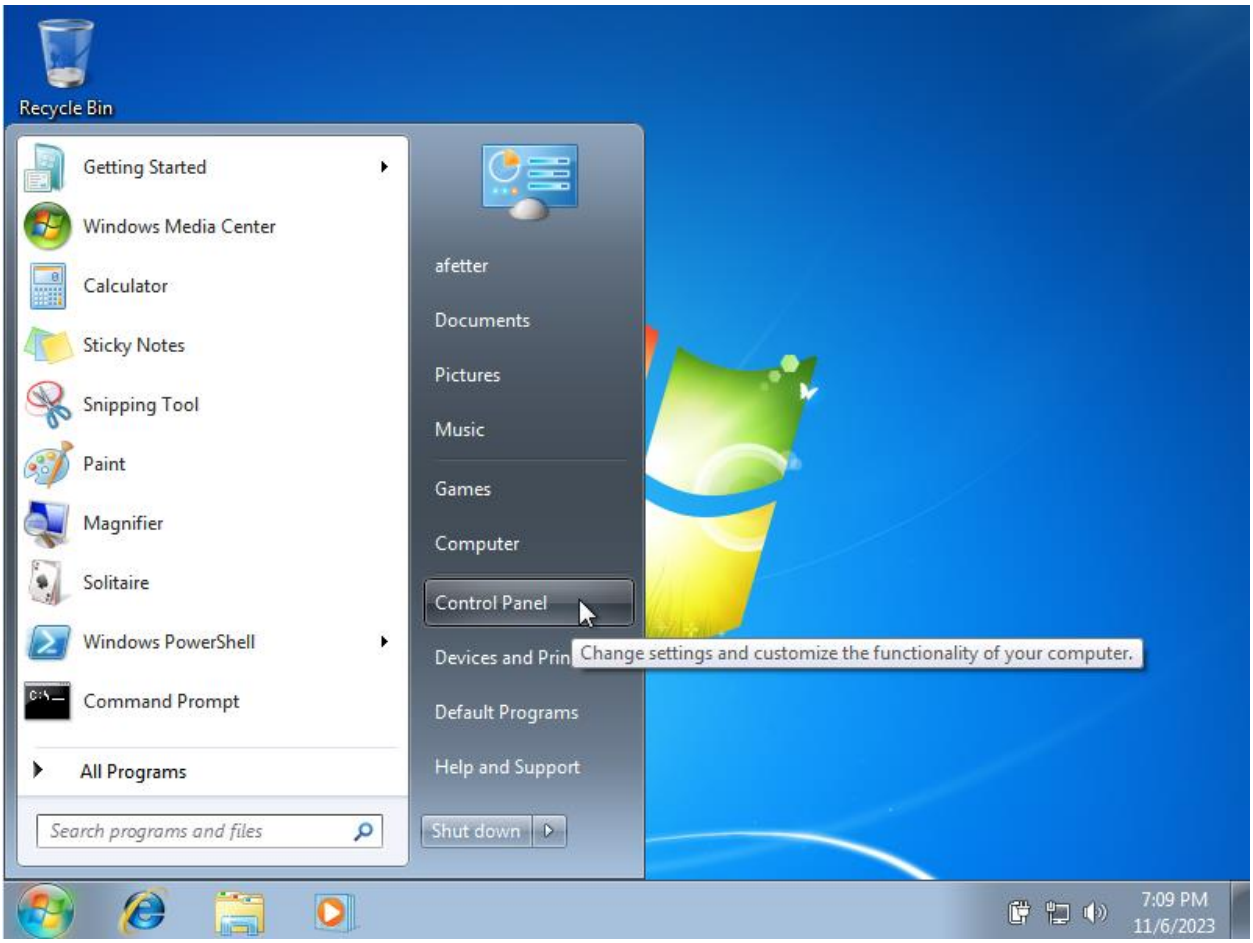
2.1. Open up a Windows Server system

A recommended Windows OS to use for this step is Windows server 2019 or Windows 10 as they are both compatible with the newest version of IIS. However, for demonstration purposes (and for purposes of the competition since we could be given any Windows system), we will be using Windows 2007 Home Professional to set up IIS 7.5

2.2. Navigate to the control panel and turn on IIS

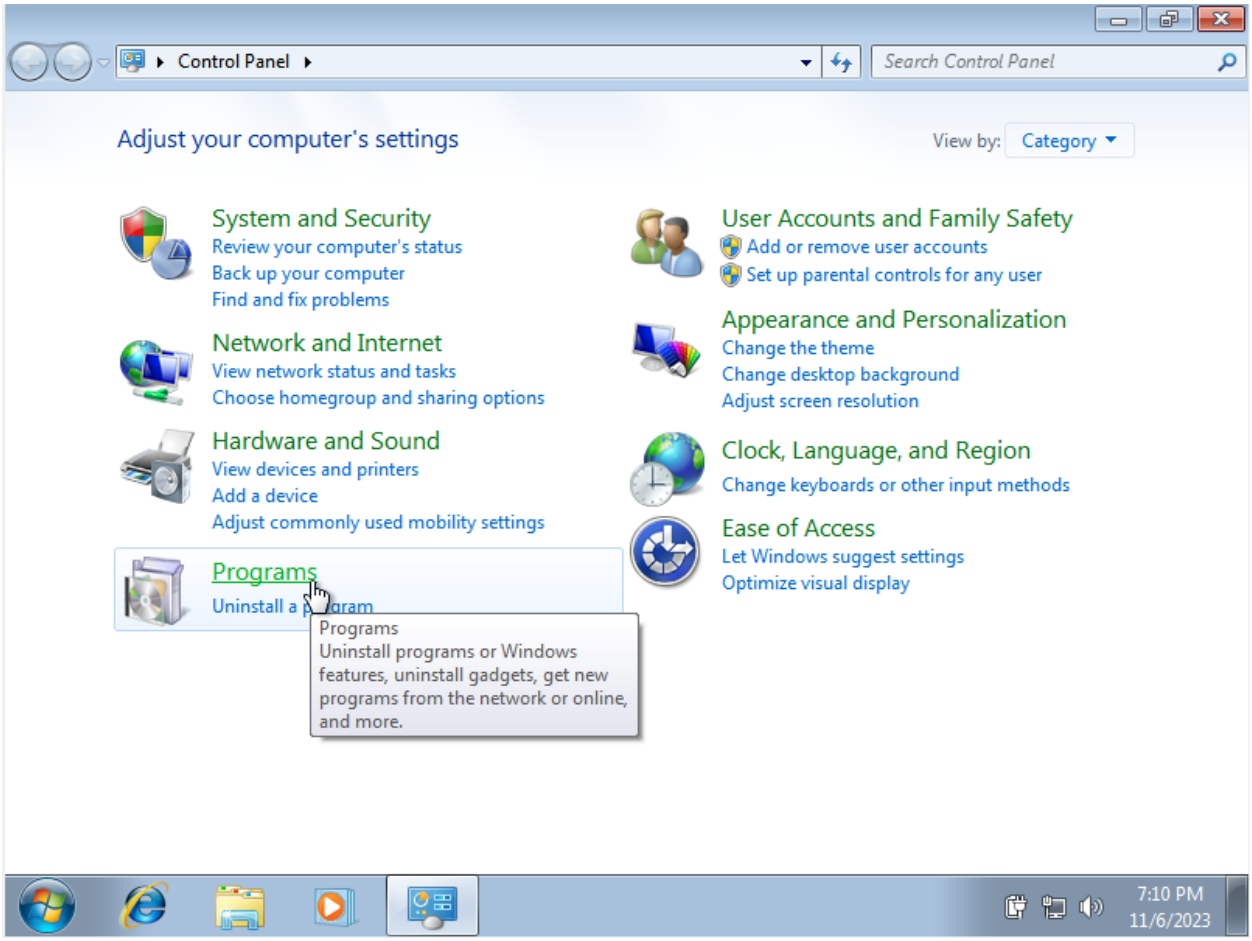
1. Upon logging in, click the Start menu at the bottom left corner and select “Control Panel”

2. IIS Installation and Configuration

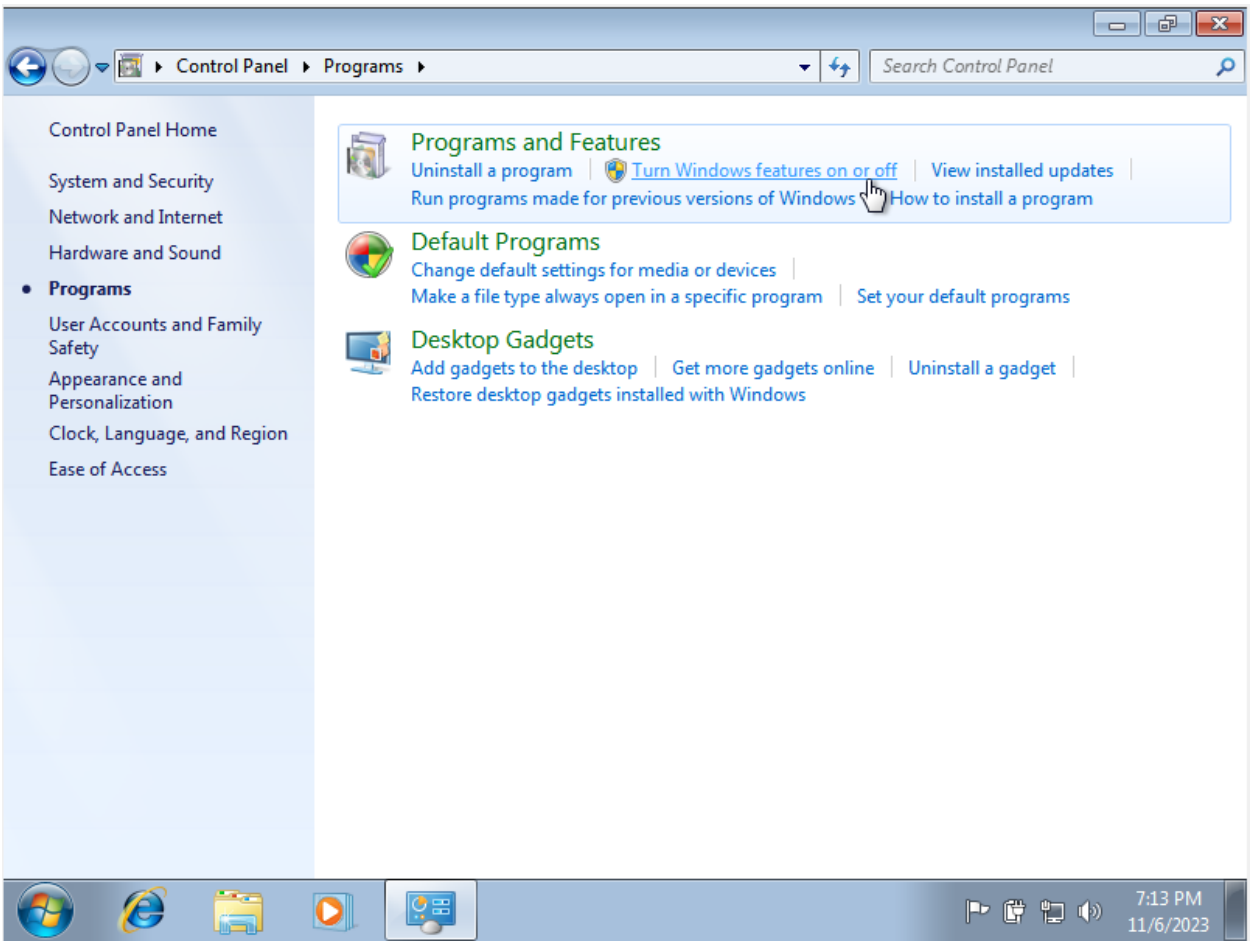


2. From here, click on “Programs” → “Turn Windows features on or off”

2. IIS Installation and Configuration



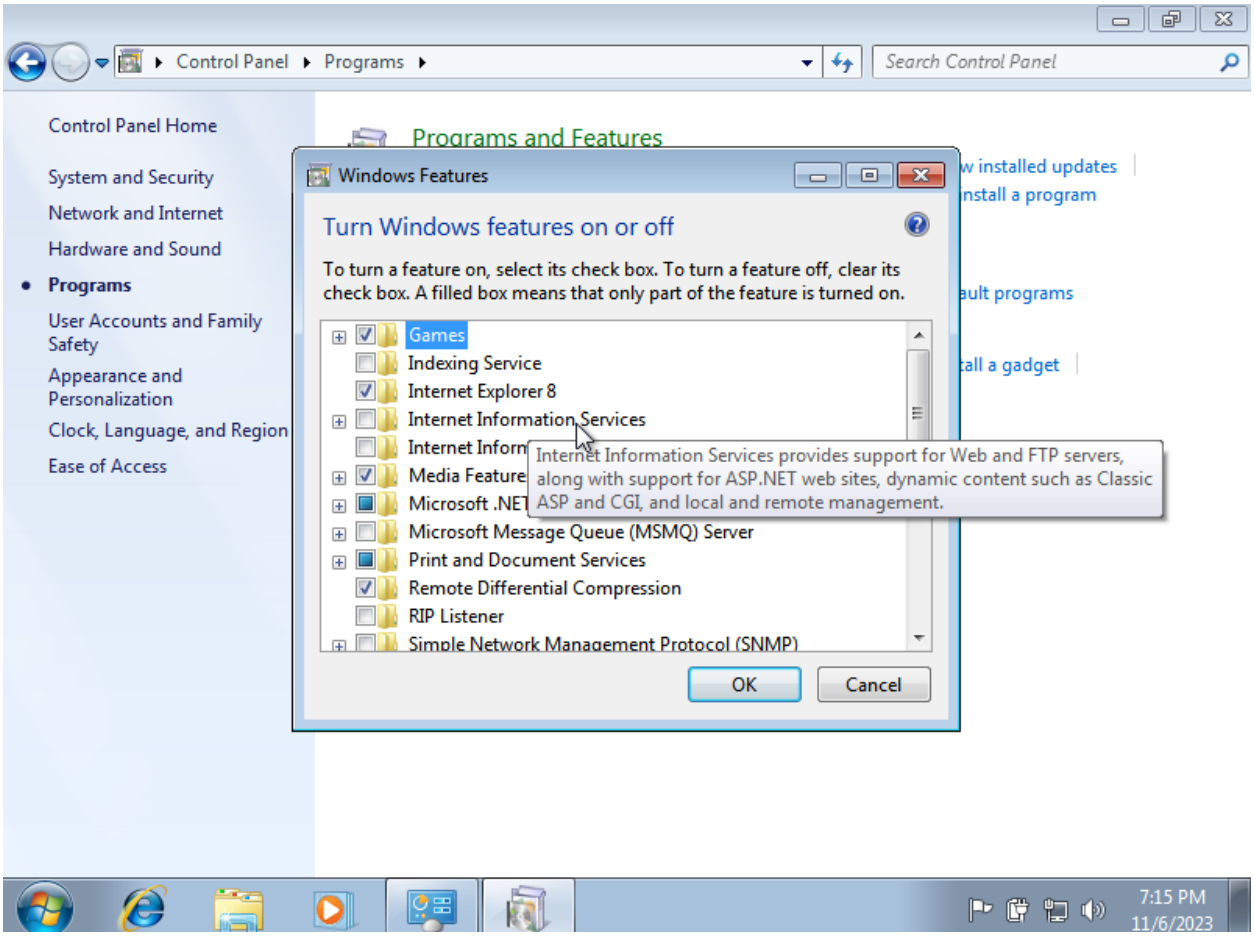
2. IIS Installation and Configuration



3. Press “Yes” to open the settings as an administrator

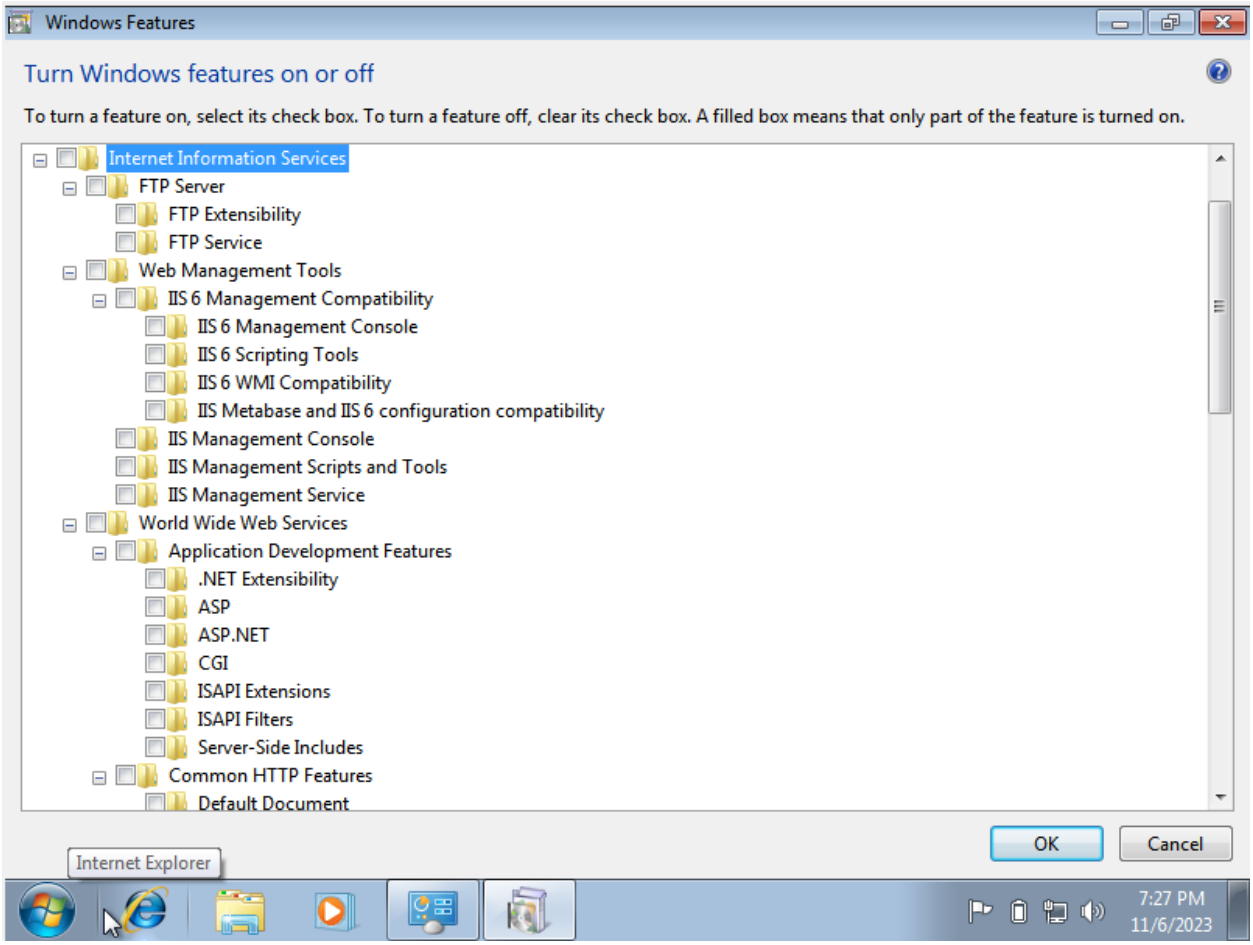
4. Locate the “Internet Information Services” feature

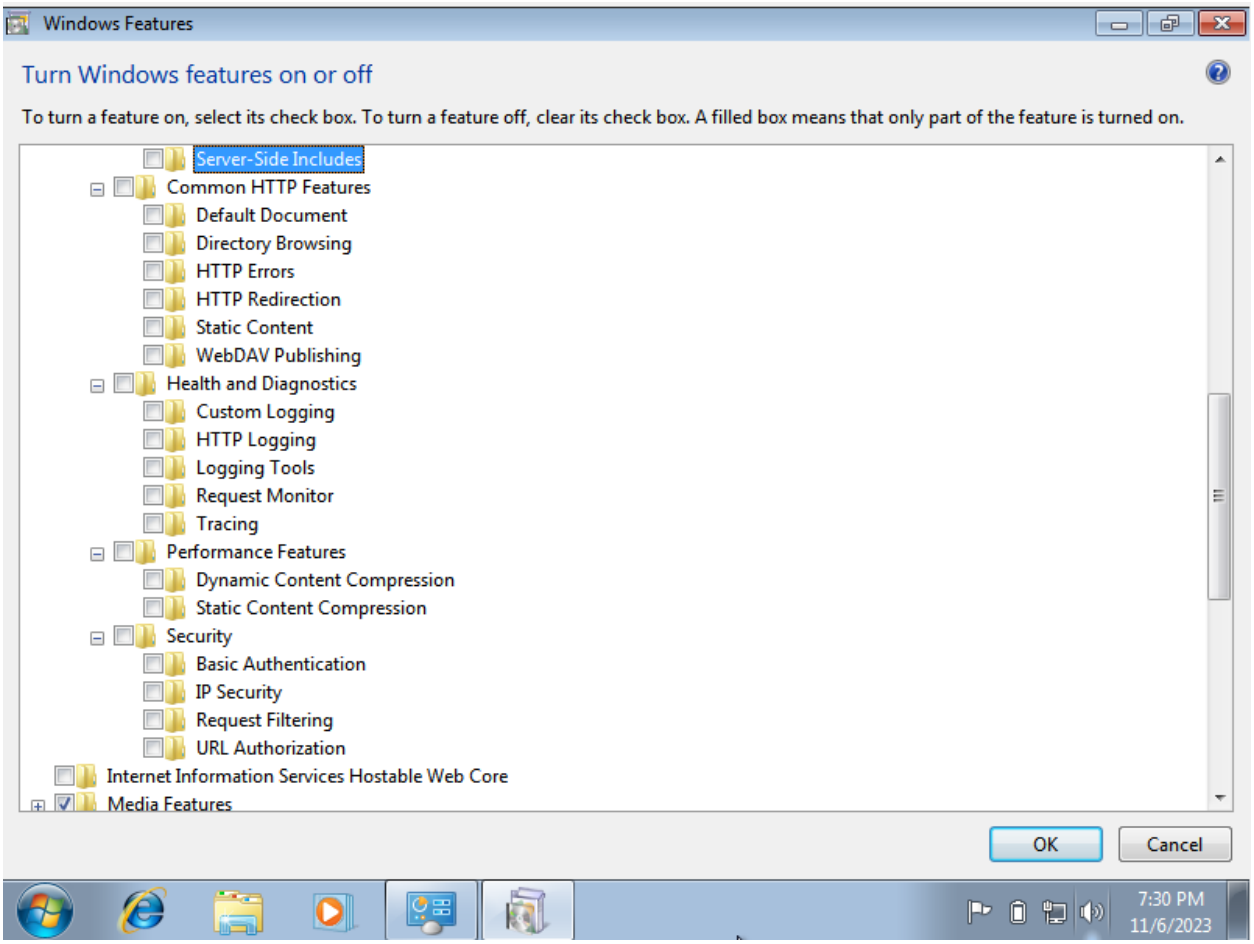
2. IIS Installation and Configuration



- Notice that there is another feature called “Internet Information Services Hostable Web Core”. This is because IIS by itself gives us the default installation of the service and only has the minimum set of features required to run it whereas the hostable web core allows us to use the ASP.net core framework to send HTTP requests and receive responses from the service
- Examining the IIS feature in further detail, we can see that there are several options we can choose from

2. IIS Installation and Configuration





- Each of these options allow for different IIS features to be turned on or off. Checking the box next to the "-" sign will turn only the default features on, meaning not all will check once you check the parent feature. You can hover over each of the different features in order to see what they do in further detail.

5. Enable the "Internet Information Services" feature

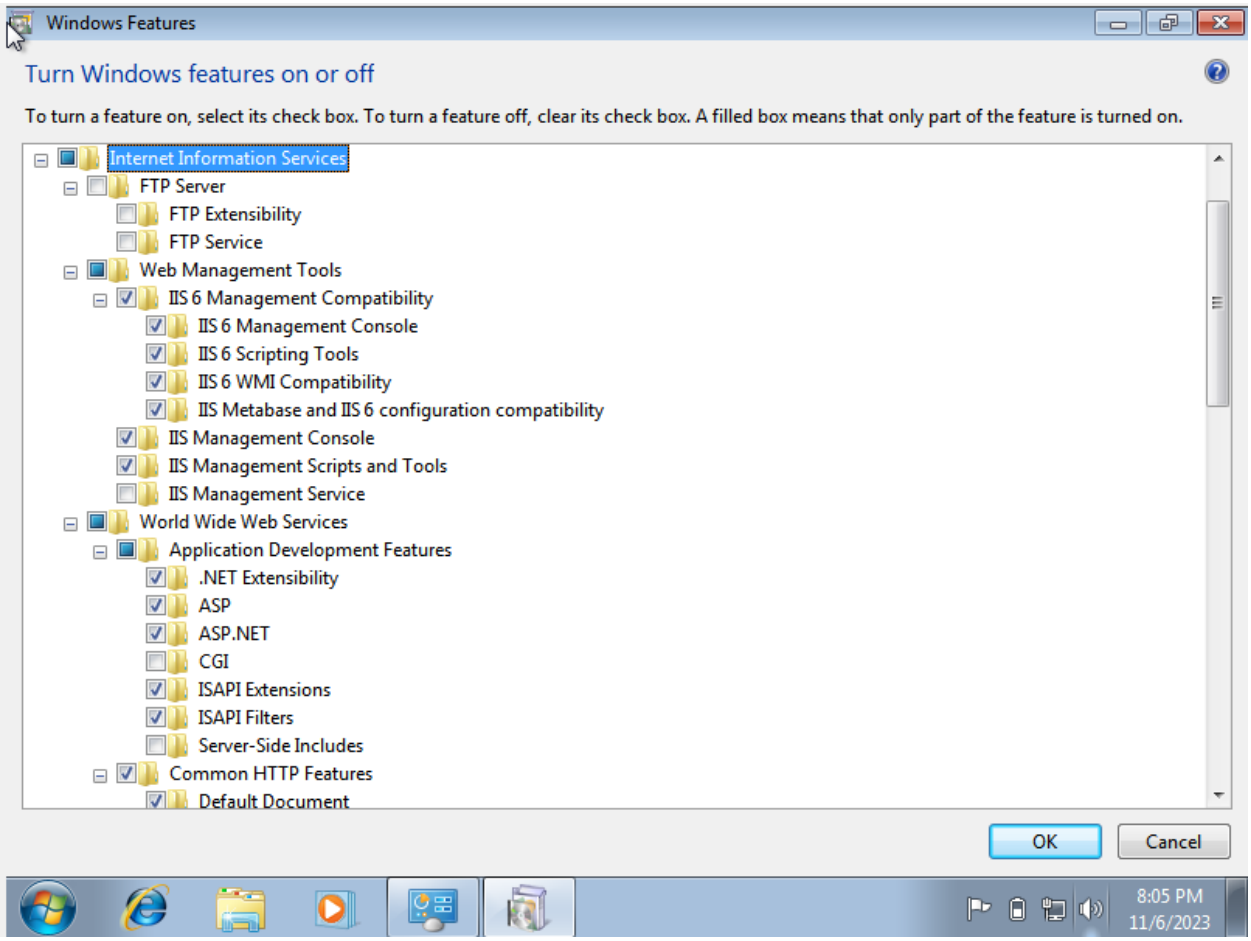
2.3. Enable features needed for your IIS server

For our purposes, we will be turning on all features in the "Security" dropdown as it pertains to mitigating the risk of the IIS service being attacked.

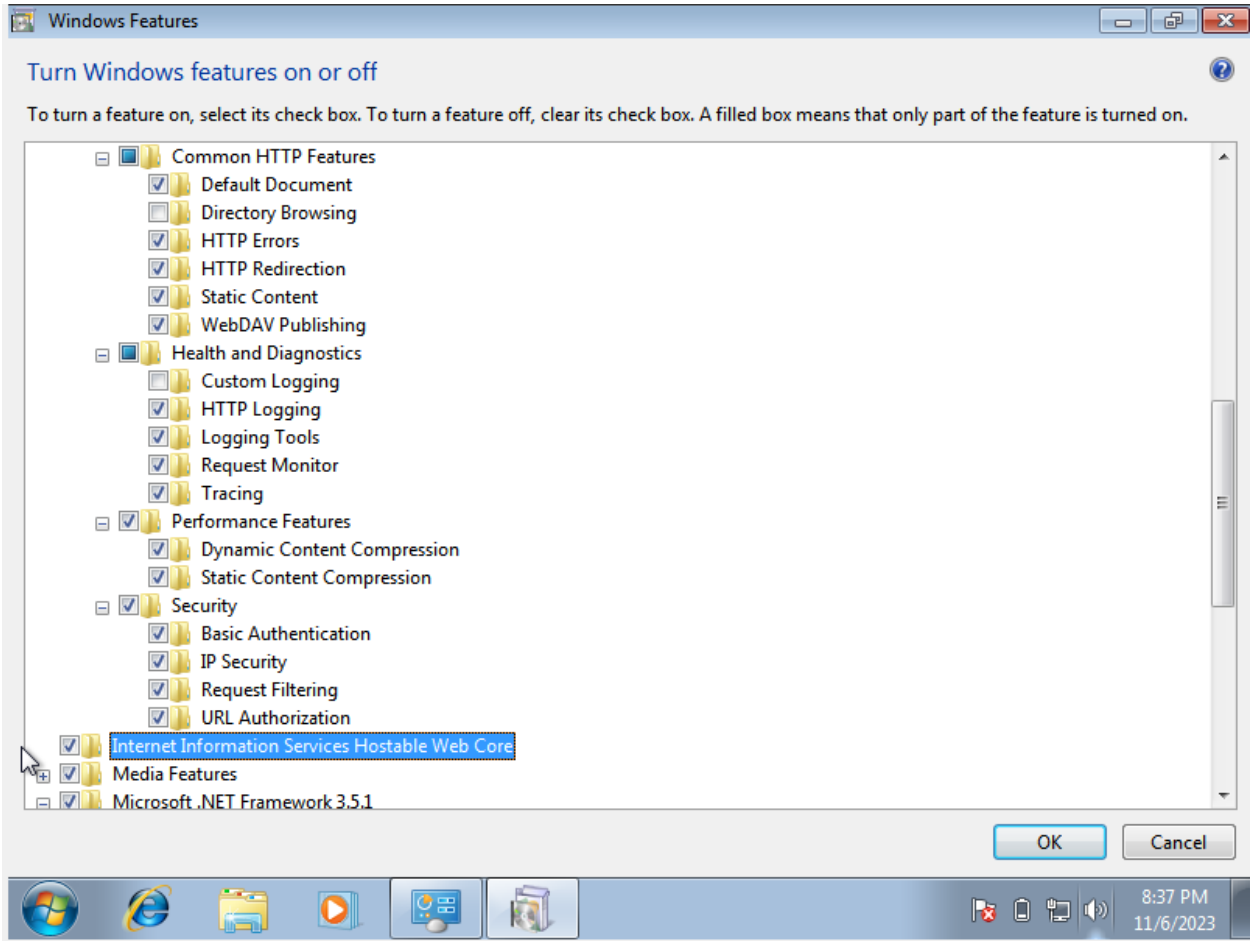
2. IIS Installation and Configuration

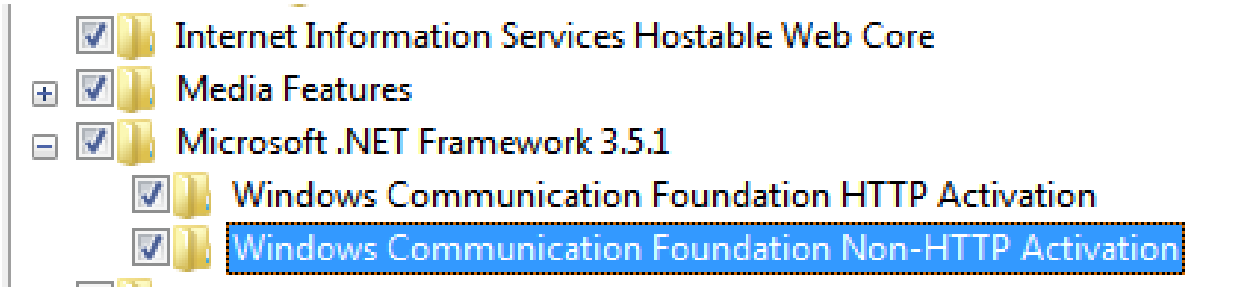
- Basic Authentication – Only valid Windows users can access the IIS server
- IP Security – Configure firewall rules for the server based on IP addresses/domain names
- Request Filtering – Configure firewalls rules to block requests from specific clients
- URL Authorization – Allows you to determine authorization levels for users accessing specific URLs on the server. For example, you don't want a user accessing an admin page, so you can determine what level of access they have here

We will also be enabling the following features:



2. IIS Installation and Configuration





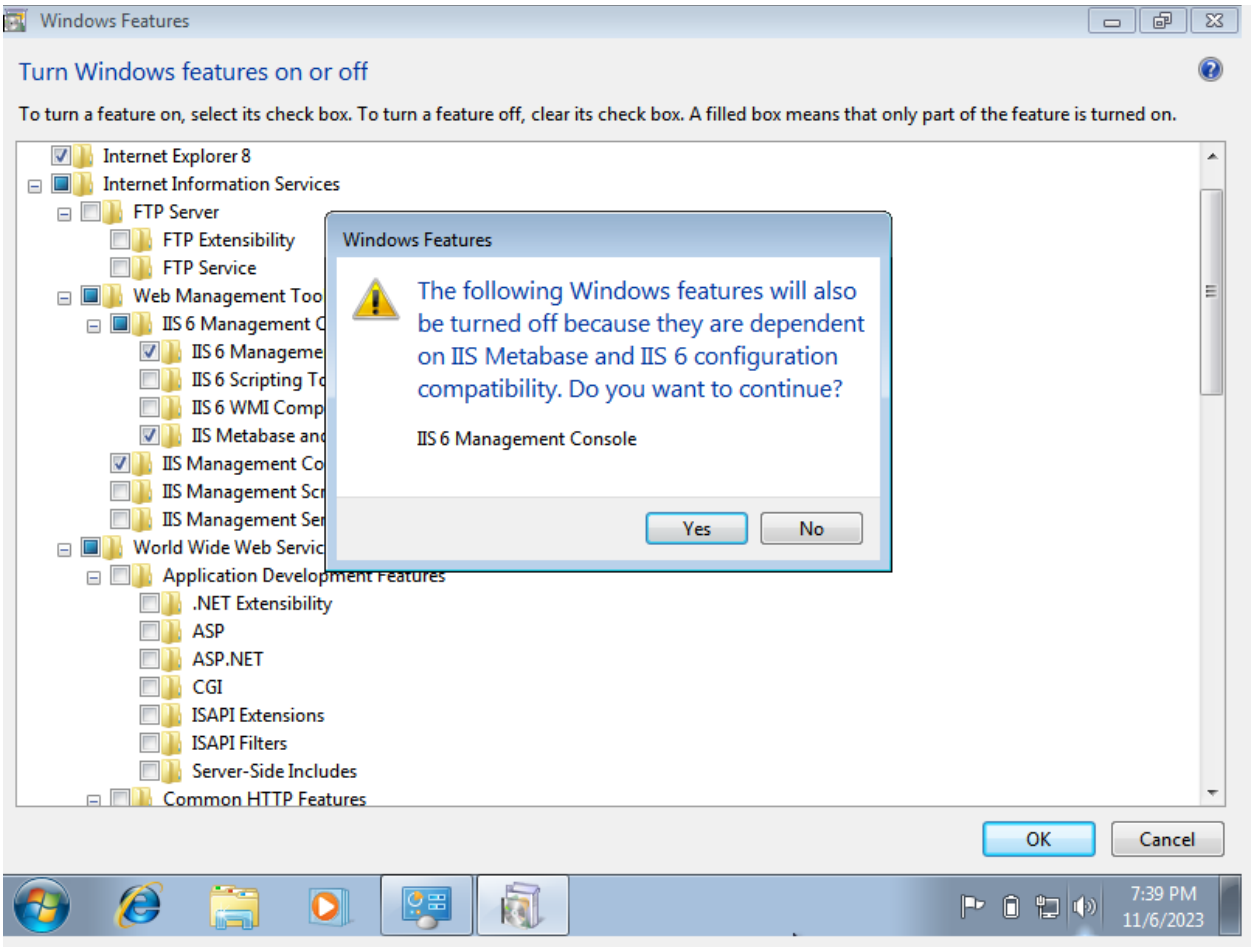
- IIS 6 Management Compatibility – While IIS 6 is an older version of IIS, this feature allows you to download existing, working scripts to easily manage the IIS 7 server
    - IIS 6 Management Console - Installs the IIS 6 management console so you can administer an IIS server
    - IIS Scripting Tools – Installs scripts needed to configure the IIS server
    - IIS 6 WMI compatibility – Installs Windows Management Instrumentation (WMI) in order to give you access to server monitoring tools
    - IIS Metabase and IIS 6 configuration compatibility – Allows configuration data from the IIS 6 application to interact with the configuration data from IIS 7; Allows for the above features to run properly

2. IIS Installation and Configuration

- IIS Management Console – Installs the IIS 7 management console to manage the current version of IIS for the VM
- IIS Management Scripts and Tools – Installs configuration scripts for the server
- IIS Management Service - Allows for remote management of the IIS server
    - We will NOT enable this one for our purposes as we will be running the server locally and will have no need to run it remotely
- .NET Extensibility – Allows for the server to host .NET framework applications
    - A .NET framework allows you to build applications for Windows systems
- ASP – Allows the server to host Classic ASP applications
- ASP.NET – Allows the server to host ASP.NET applications
    - You can read about the differences between Classic ASP and ASP.NET here
- ISAPI Extensions – Installs the Internet Server Application Programming Interface (ISAPI) to handle client requests
- ISAPI Filters – Enables ISAPI filters to enhance functionality of the ISAPI, making it easier to filter requests
- Default Document – Allows you to set a default file if a user does not specify a file to locate in the URL (ex: index.html)
- Directory Browsing – Allows users to view the contents directories on the web server
    - This should NOT be enabled for our purposes as it can lead to directory traversal and/or other attacks if not handled properly
- HTTP Errors – Allows you to set custom error messages
- HTTP Redirection – Allows you to redirect customers to a specific direction if needed (ex: if they click on a link and don't have authorization to view its contents
- Static Content – Allows .htm, .html, and static images to be hosted from the server
- WebDAV Publishing – Allows you to use HTTP on the server
- HTTP Logging – Enables logging of website activity when users access the server
- Logging Tools – Installs logging tools and scripts for the server to use when hosting applications to monitor traffic
- Request Monitor – Enables the monitoring of the "health" of the sever and any applications associated with it
- Tracing – Allows the server to trace ASP.NET applications and any failed requests from clients
- Dynamic Content Compression – Compresses dynamic content before sending it back to the client, allowing web pages to render faster and reducing the time to First Contentful Paint (FCP)
    - FCP is the loading time of content useful to the user (such as text or graphics). First Paint (FP) is also measured in some instances that defines the time it takes for the very first pixels to load in the user's browser
- Static Content Compression – Compresses static content before sending it back the client, resulting in faster transmission times between the server and the client
- Internet Information Services Hostable Web Core – Enables core IIS functionality to properly handle HTTP requests

- Windows Communication Foundation HTTP Activation – Allows you to build service-oriented applications that use HTTP requests to obtain data
- Windows Communication Foundation Non-HTTP Activation – Allows you to build service-oriented application that do not use HTTP requests to obtain data
    - The two features above regarding Windows Communication Foundation (WCF) have been deprecated as of .NET version 5.0 (The newest version of .NET is version 7.0). However, since IIS 7 still uses .NET 5.0

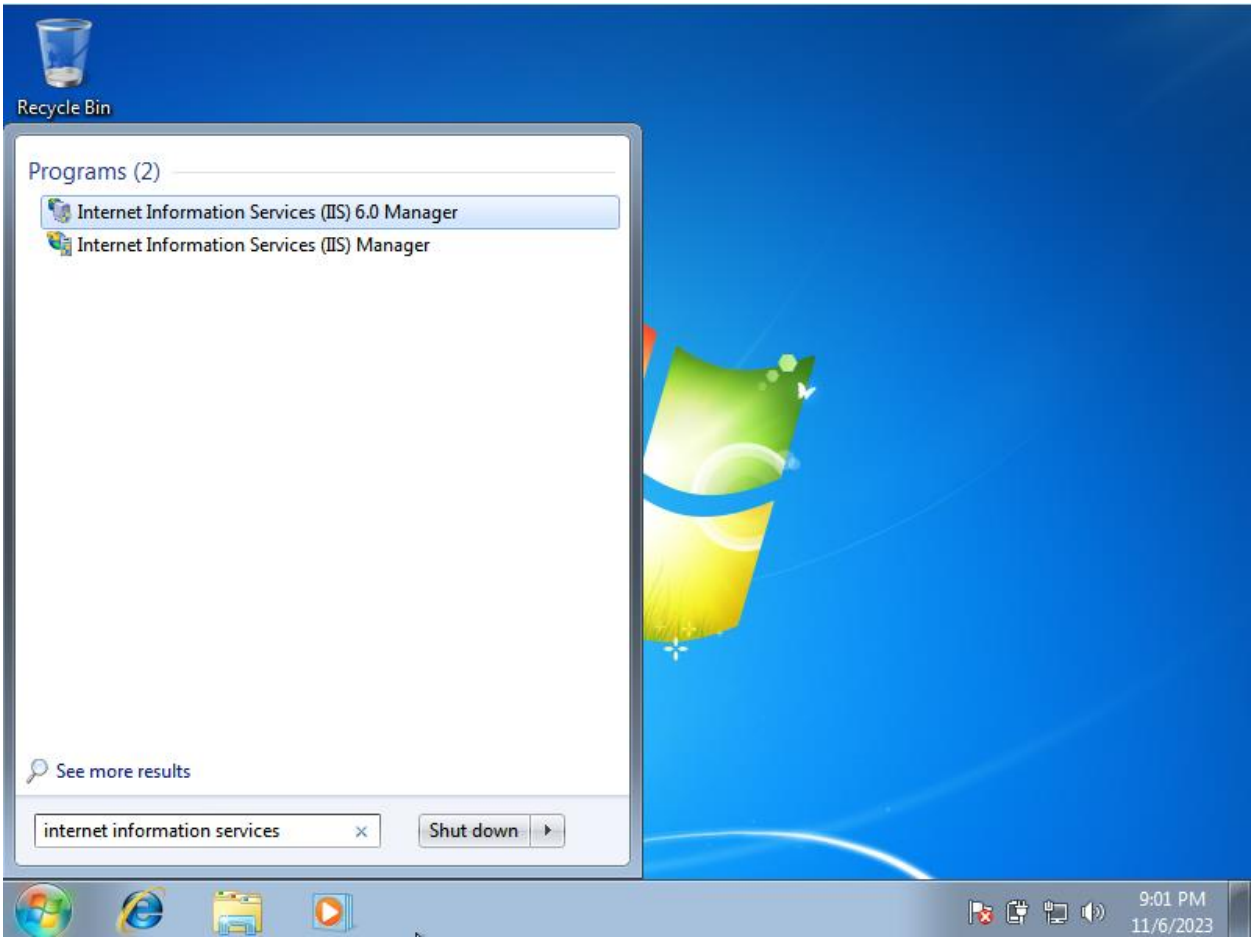
Side note: When enabling and disabling features, ensure that all other features related to the one you are enabling/disabling are in the same state. If there are features that rely on the one you are enabling, they will enable automatically. However, if there are features that are enabled but rely on the one you are disabling, the following pop-up will appear:



2.4. Install IIS and its related features

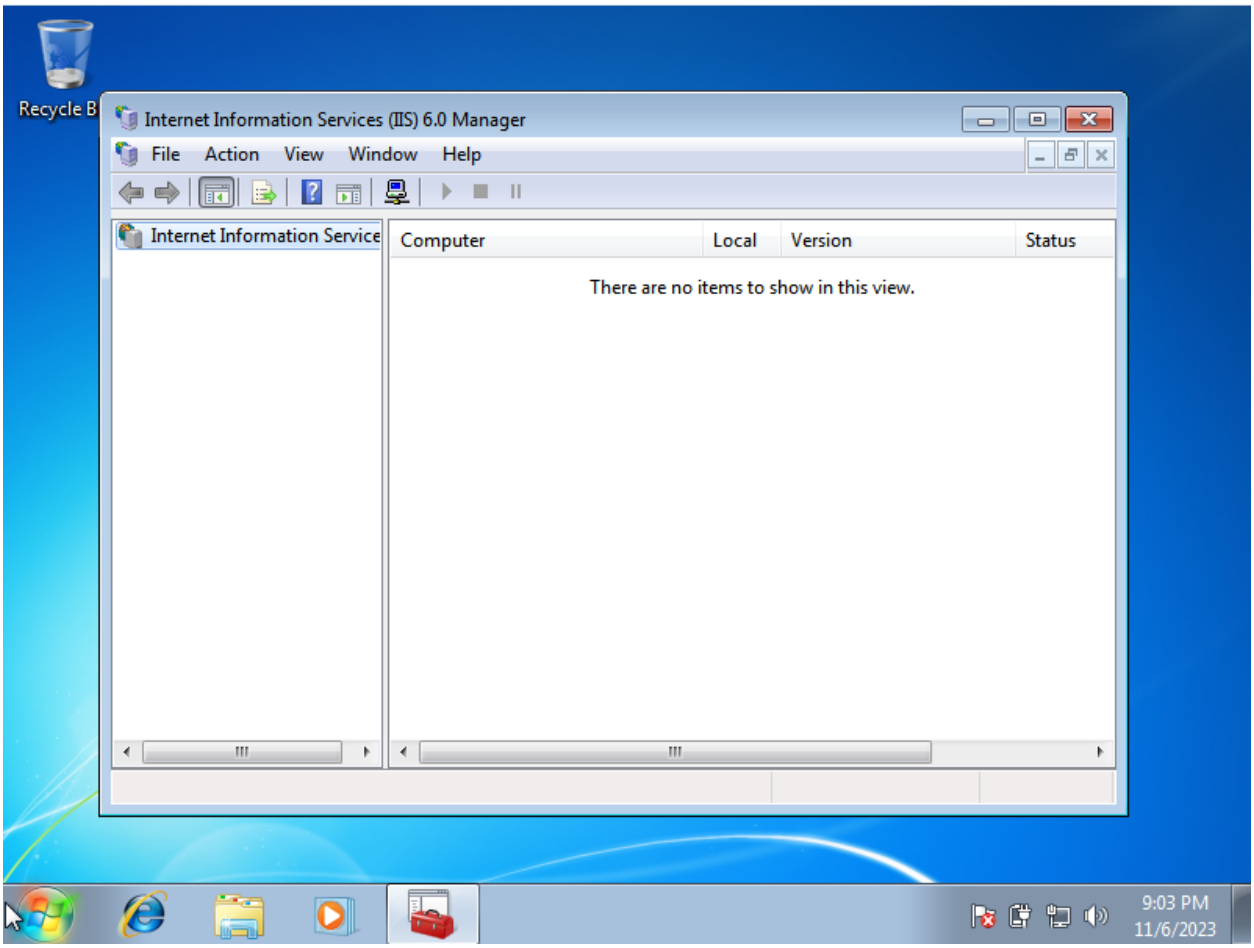
1. Once you have all features you would like to install checked, press “OK” to move on to the installation process and wait for Windows to add the features to your VM. When finished, you will be sent back to the “Programs” page in the Control Panel
2. To verify the installation, go to the Start menu at the bottom-left corner and type either “Internet Information Services” or “IIS” to display the management software

2. IIS Installation and Configuration



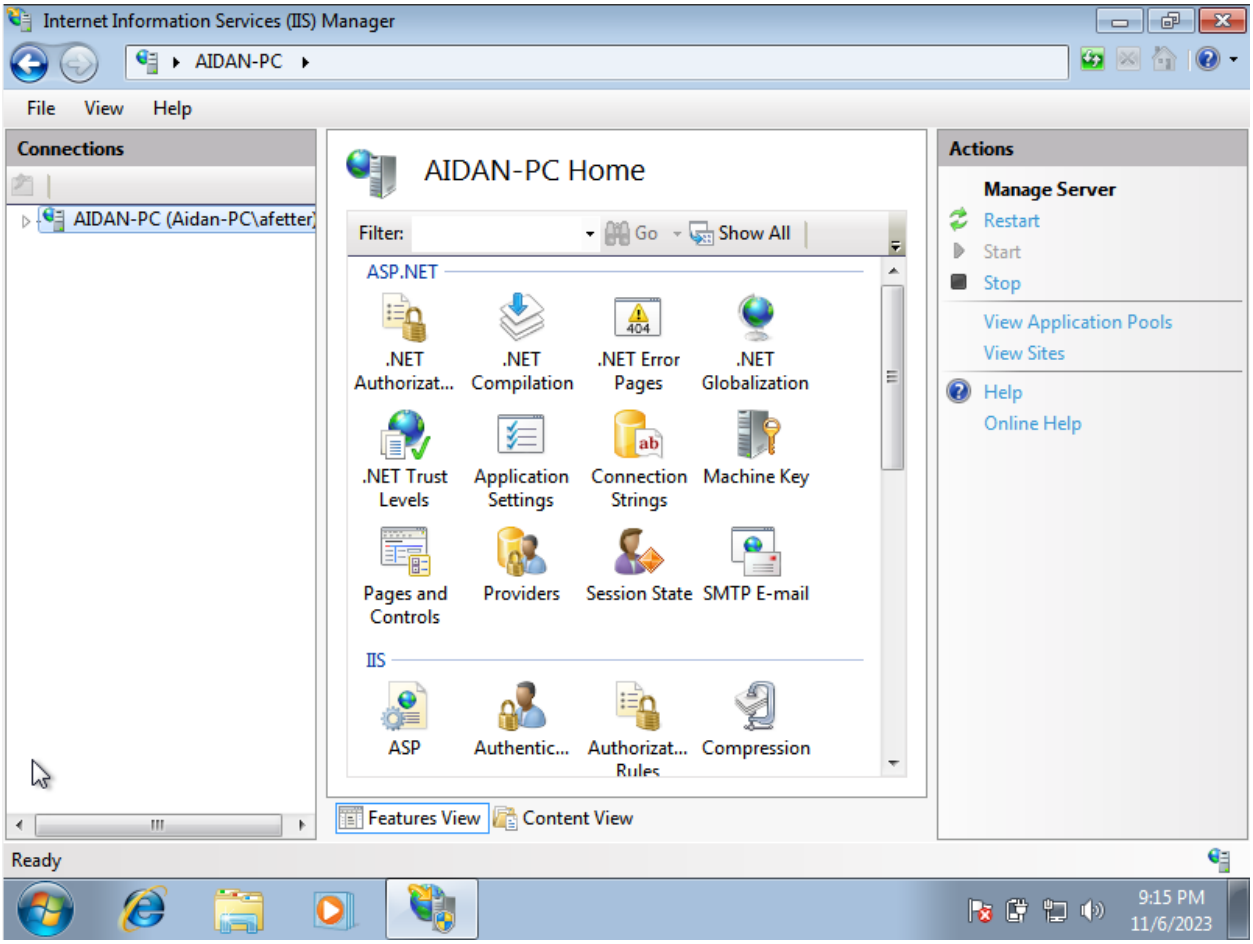
- Since we enabled the IIS 6.0 Manager, we have two management softwares. When viewing the IIS 6.0 manager, it will look like this:

2. IIS Installation and Configuration



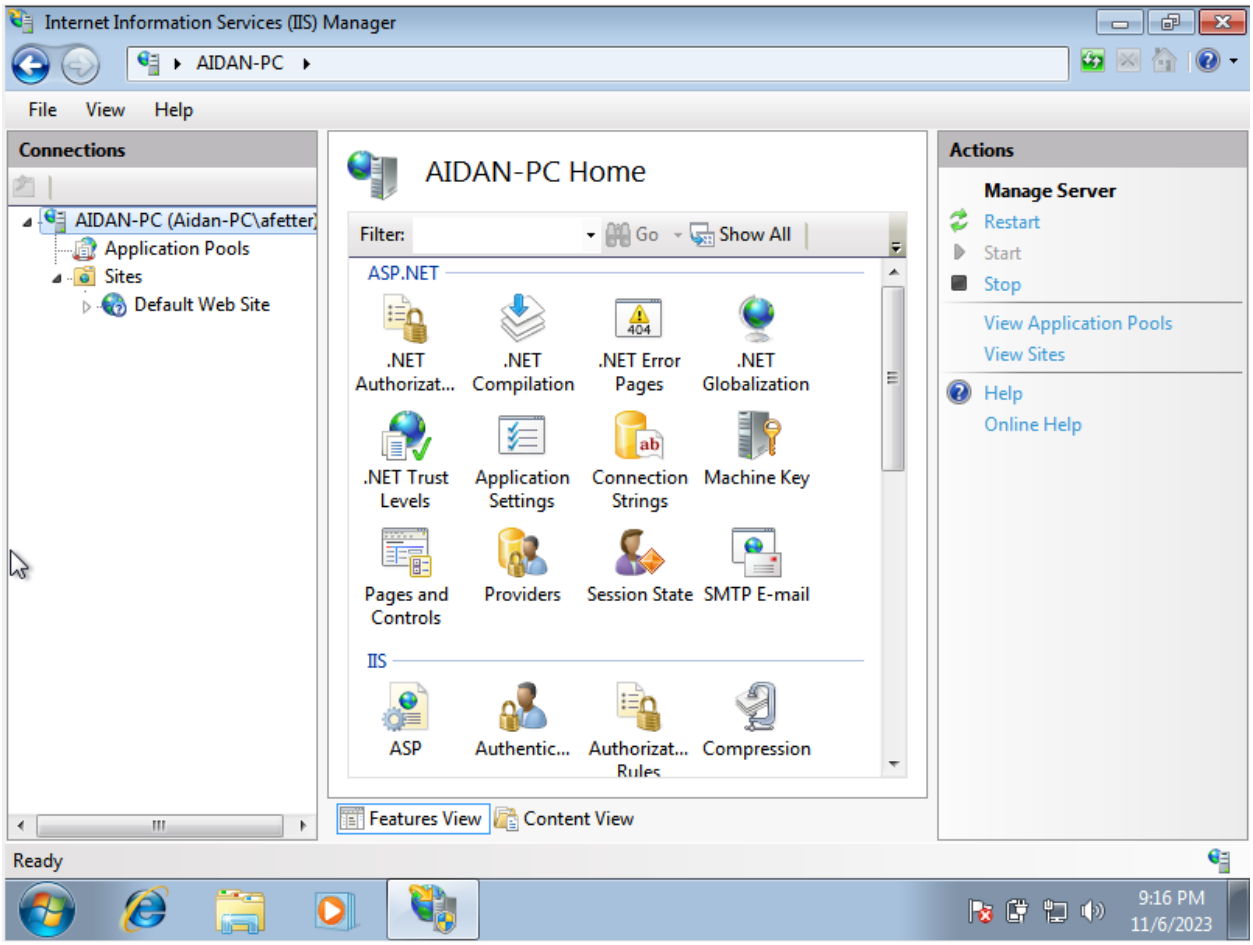
- Since this allows for older, secure scripts from IIS 6 to be used in IIS 7, we will not pay any attention to this management software
- We will be working with the 7.0 Manager in the following steps as it should like this upon opening:

2. IIS Installation and Configuration

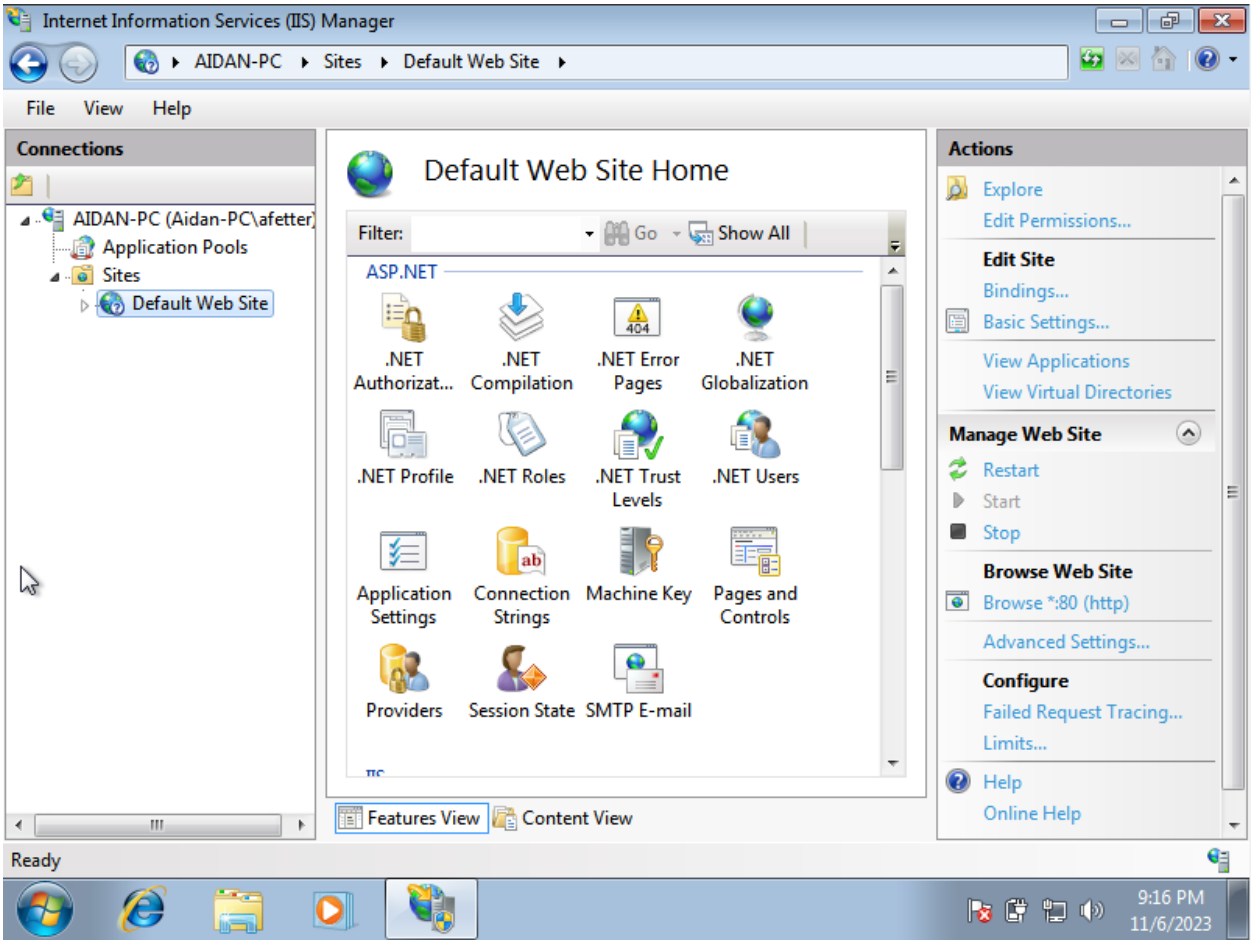


3. Now that IIS has been installed, we can now view the default website provided to us by the IIS service as well as its location showing where the page is stored on the server. Click the arrow next to the PC name as well as the arrow next to “Sites” to view the default site

2. IIS Installation and Configuration



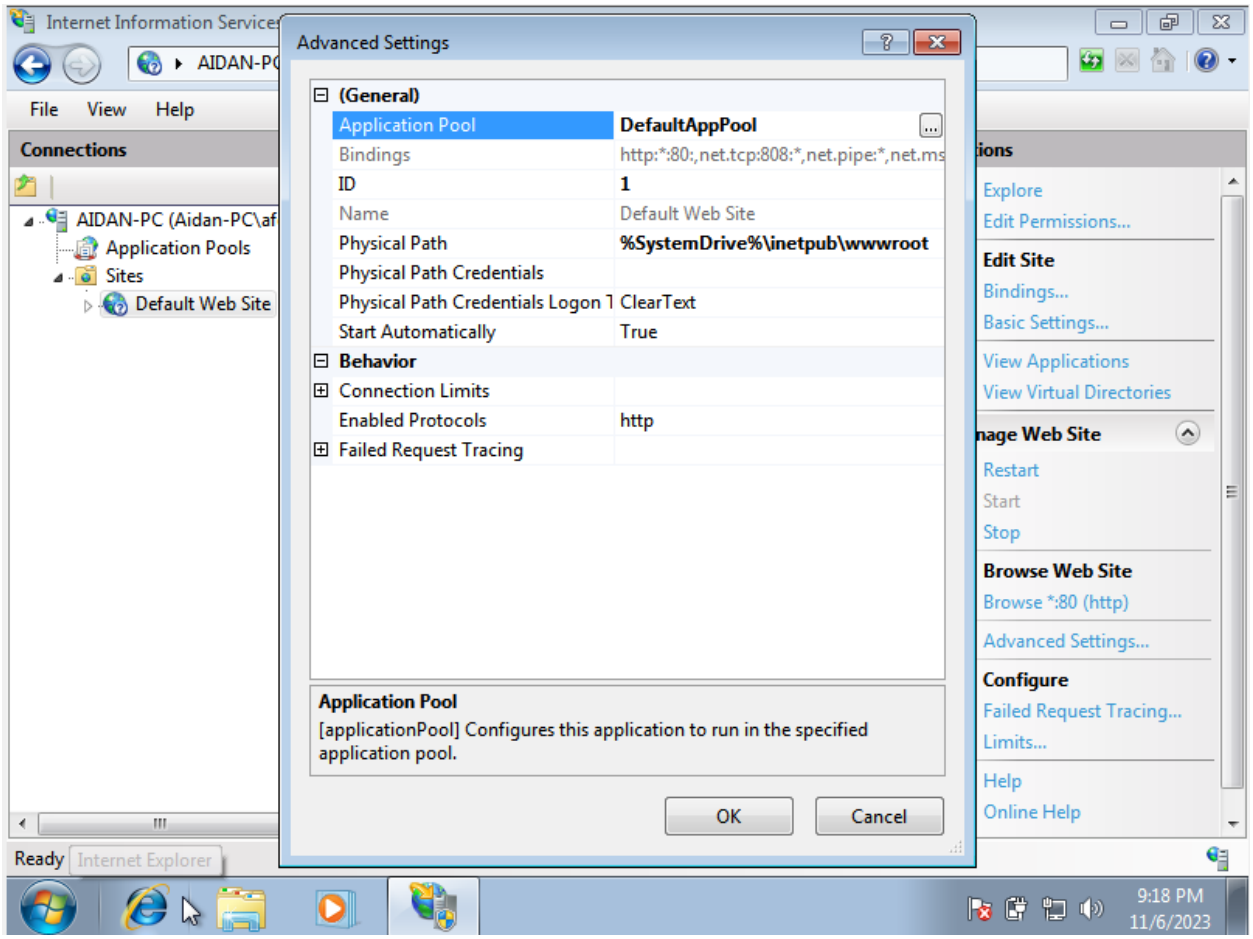
4. Click the “Default Web Site” tab to view the actions that can be taken



- When looking at the “Actions” section, we can see that the website is currently running and gives us the option to stop it if needed.

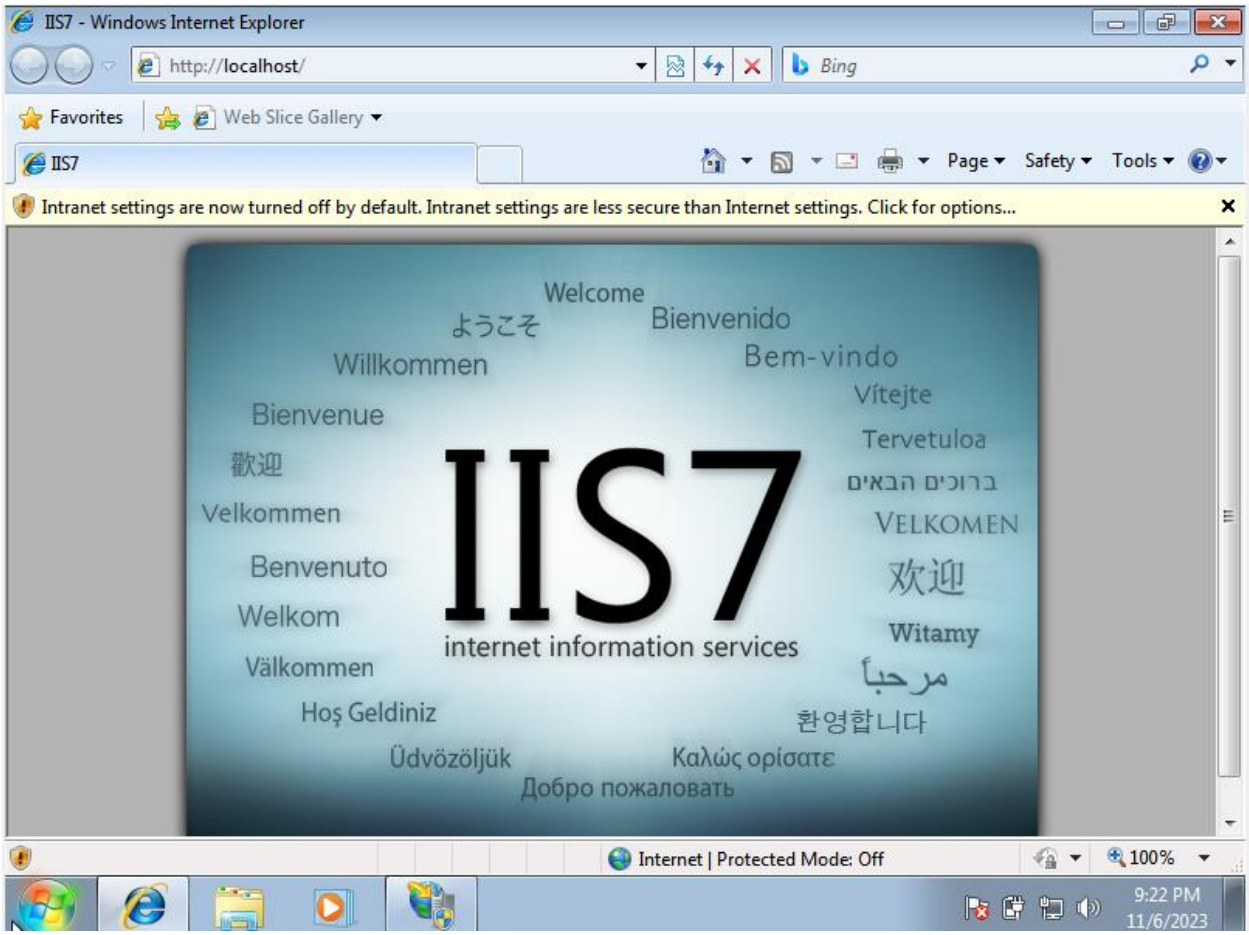
5. Click the “Advanced Settings…” option to view more detailed information about the website

2. IIS Installation and Configuration



- Based on the screenshot above, we can see the ports the website is connected to, the website ID, the name of the website, and the file path in which the website is stored. The path is important when hosting a web server because it tells the administrator where the file configuration for that particular website is stored. This path is also where new websites can be added to tell the server for others to see.

6. Click “OK” to exit out of the advanced settings tab. Press “Browse *.80 (http)” to open the default website for your IIS server



- Based on the URL, we can tell that the server is hosting this website on the localhost address

7. You have successfully configured and installed IIS features!

3. Security Configuration for an IIS Server

3.1. Update to latest version

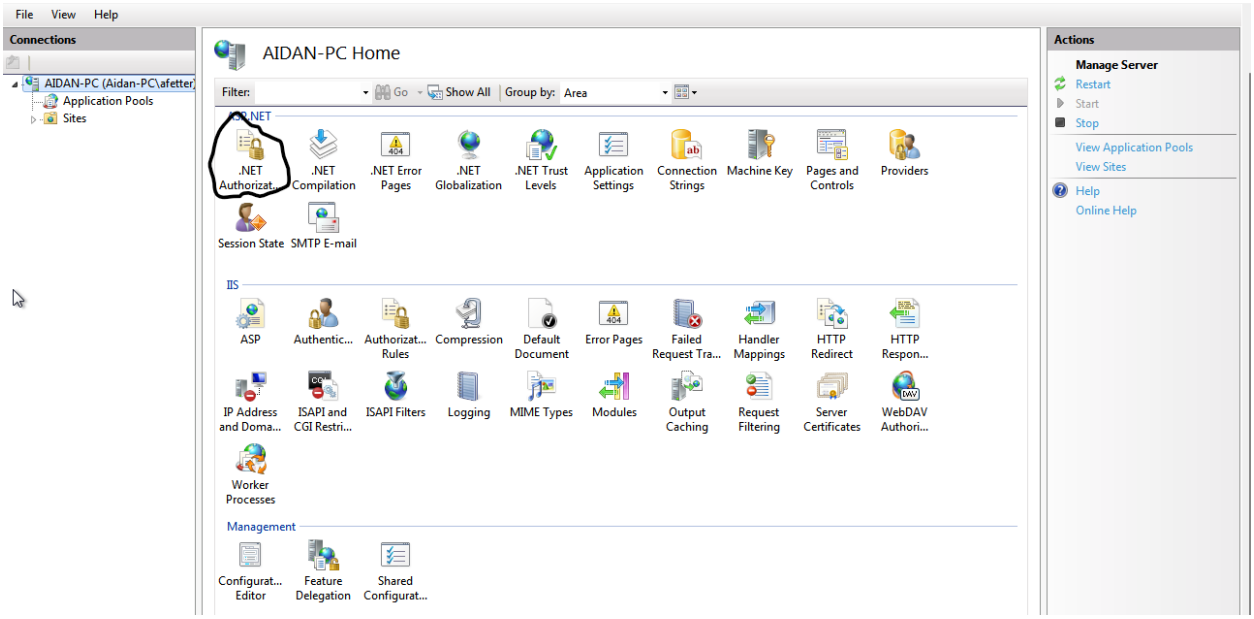
When configuring an IIS server, ensure that you are using the most up-to-date version of the service in order to avoid any recorded Common Vulnerability Exposures (CVEs) from being used on the service.

3.2. Ensure that only the modules needed are installed on the server

If unnecessary modules are installed during configuration, attackers could use these unused resources as potential attack vectors to exploit your IIS server. Make sure that when you install and administer the service, keep an eye out for which features are used while the server is running.

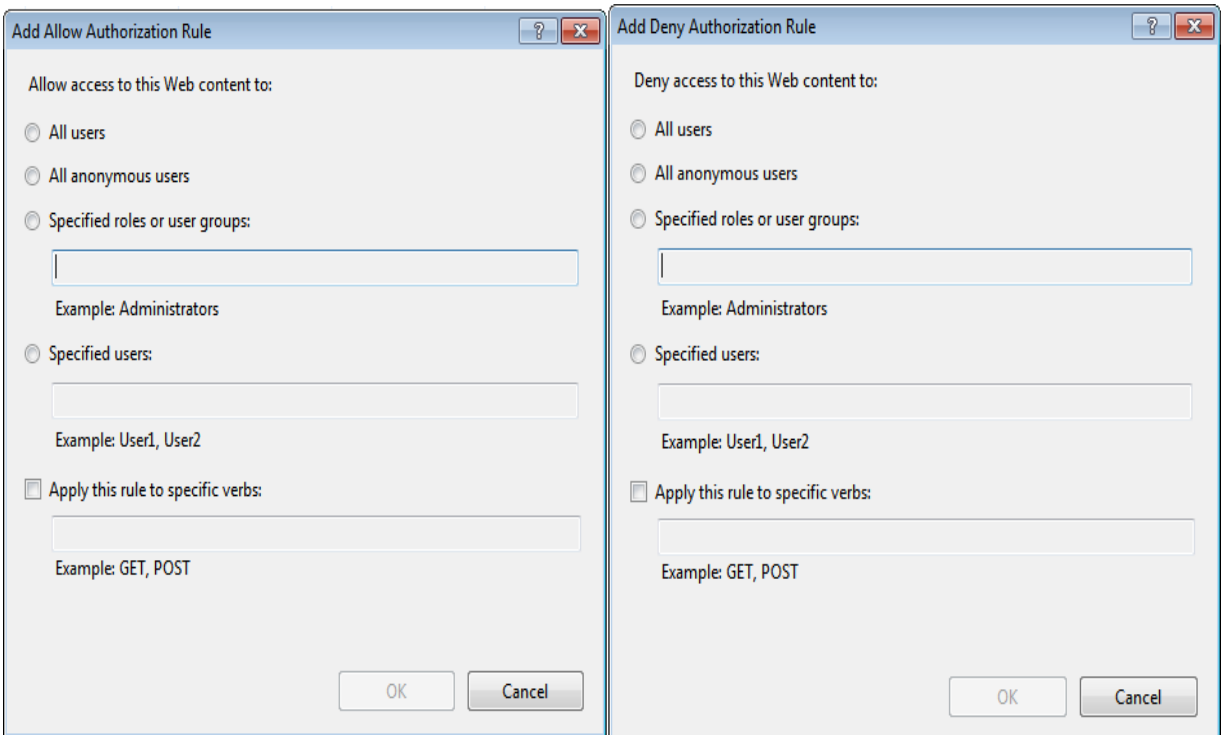
3.3. Limit user accessibility

1. Locate the ".NET Authorization Rules" in the IIS manager to authorize which users have access to the websites and applications hosted by the server.



- Note: This setting is available to both specific websites and the web server itself. For this step, we will be changing the web server settings; however, the same setting should be configured by clicking on the "Default Web Site" button under "Sites". There is also an "Authorization Rules" button under the "IIS" section. The difference between this button and the one we are currently looking at is that the former has to do with the users accessing the service in general while the latter deals with the specific methods the user can use when browsing (such as "GET", "POST", or "PUT"). Both buttons should be examined and configured to match your service and maximize security.

2. After clicking this, you will be able to add, remove, edit, or view authorization rules for the server itself. This is useful if you only want a specific number of people to have access to the services provided by the IIS server.

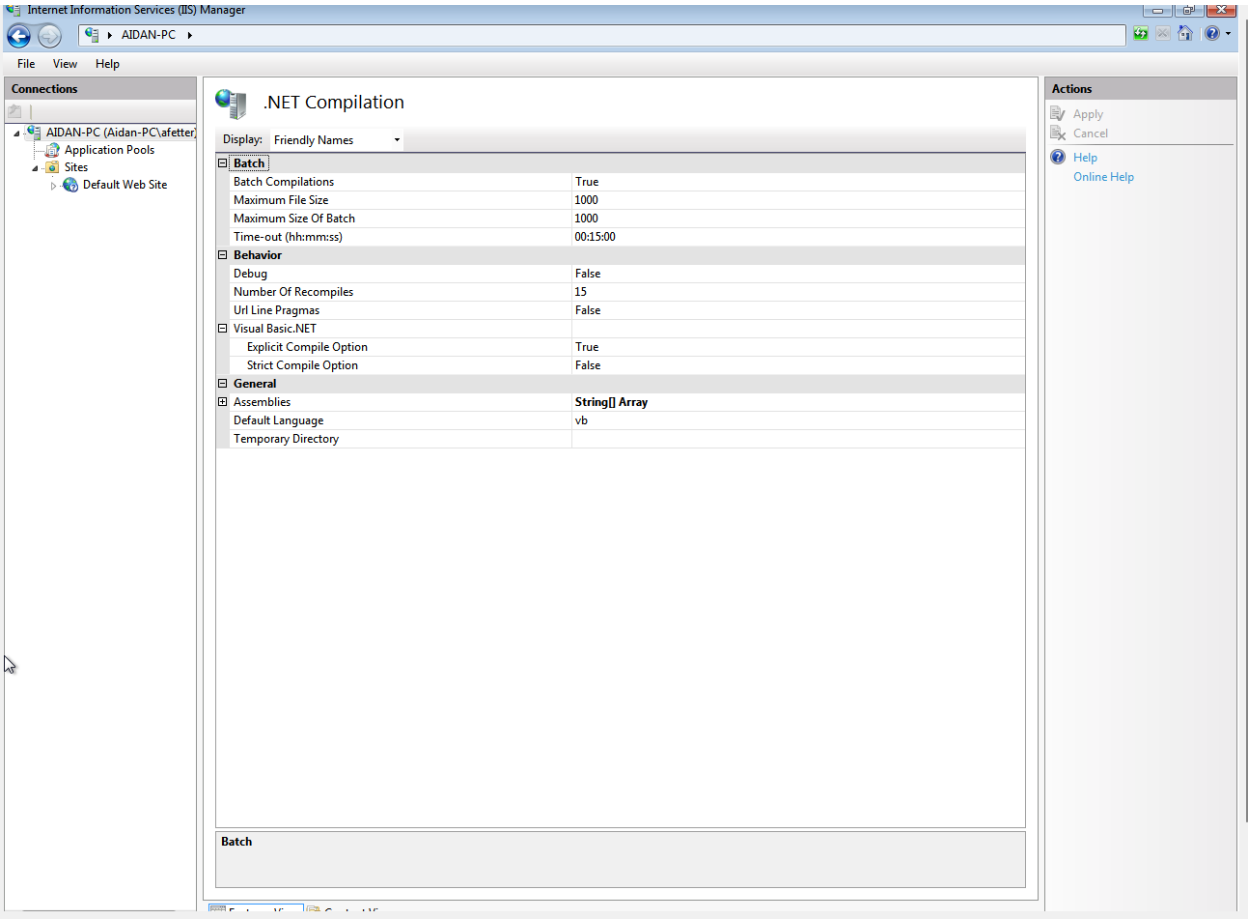


Optional Team activity: Edit the already configured authorization rule to include only the usernames on your VM and apply the rule to the HTTP verbs GET, POST, and HEAD and deny access of IIS services to all anonymous users along with the verbs OPTION, PUT, CONNECT, TRACE, and PATCH

3.4. Ensure that ASP.net application code is configured as intended

1. Click the ".NET Compilation" button from the IIS manager located directly next to the ".NET Authorization" button

3. Security Configuration for an IIS Server

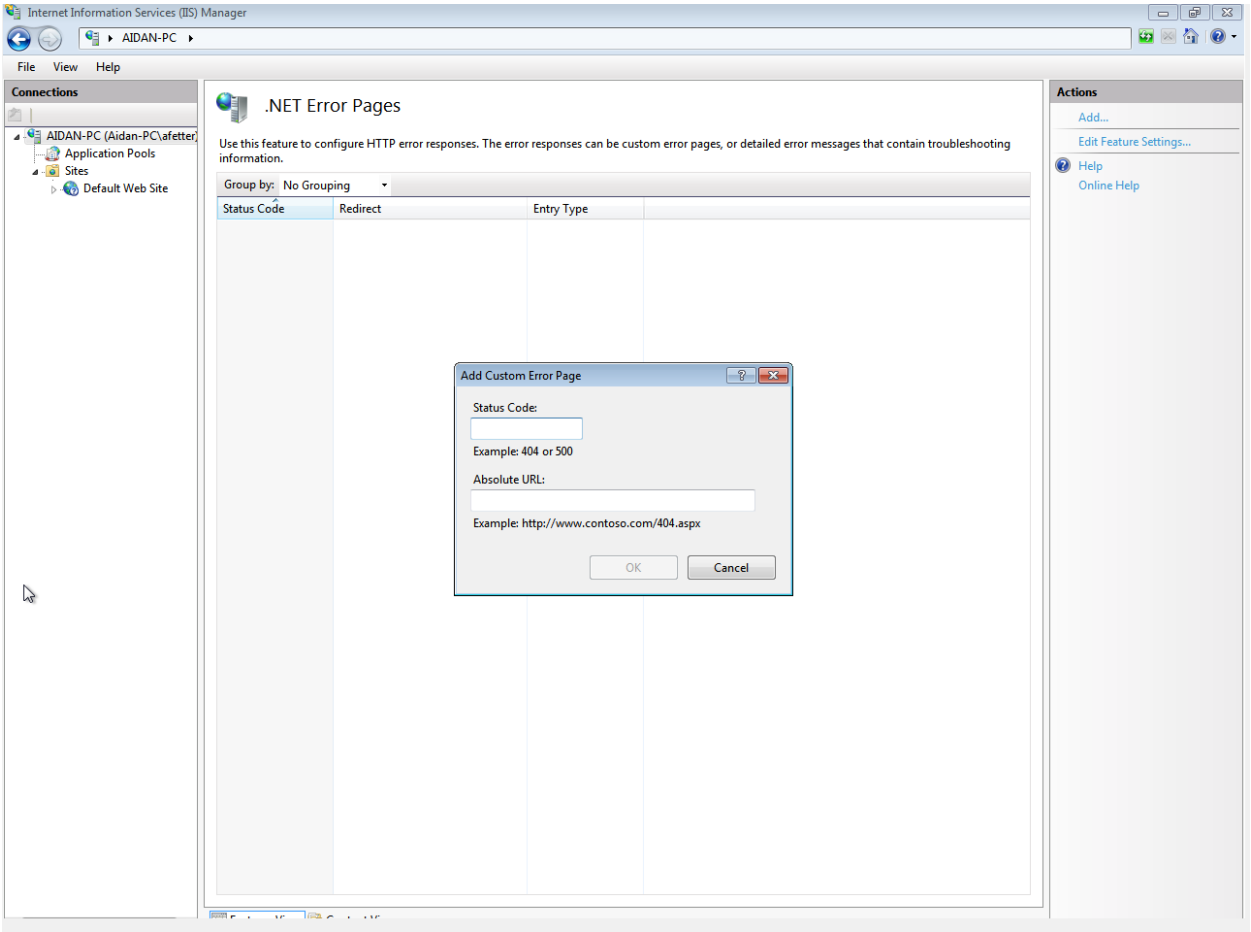


- Batch Compilations – Allow various programs to run in batches automatically while the server is running
- Maximum File Size – Max size (in kilobytes) of generated source files per batch
- Maximum Size of Batch – Max number of pages per batch compilation
- Time-out (hh:mm:ss) – Timeout Period of batch compilation
- Debug – Indicates whether or not debug binaries are used during compilation
- Number of Recompiles – If the number of recompiles is exceeded, the system will restart
- URL Line Pragmas – Indicates whether or not compiler instructions use physical paths or URLs (True → Use URLs)
- Explicit Compile Option – Sets the Microsoft Visual Basic explicit compile option. This means that all variables must be declared using a Dim (Declare in memory), Private, Public, or ReDim (used to resize a dynamic array that has already been declared as one of the other three options with empty parentheses)
    - Learn more about this section here
- Strict Compile Option – Sets the Microsoft Visual Basic script compile option. This means that upon compilation, data-type conversions that would result in data loss is explicitly denied along with any conversion between numeric types and strings

- Assemblies – Defines the set of assemblies from the \bin folder or the Global Assembly Cache (GAC)
    - The GAC stores .NET assemblies designed to be shared across several applications
- Default Language – Defined the default compilation language used. By default, the language is Visual Basic
- Temporary Directory – Specifies a directory (if needed) to store temporary files during compilation. The default is a location under the Temporary ASP.NET Files directory

3.5. Add a custom error page

1. Click the ".NET Error Pages" button located next to the ".NET Compilation" button
    - This page allows you to add custom error pages to the server. This is important because if errors are not handled properly and the user finds a way to break the code, that could potentially expose some of the internal workings of the server
2. Click "Add…" to add a new error page location

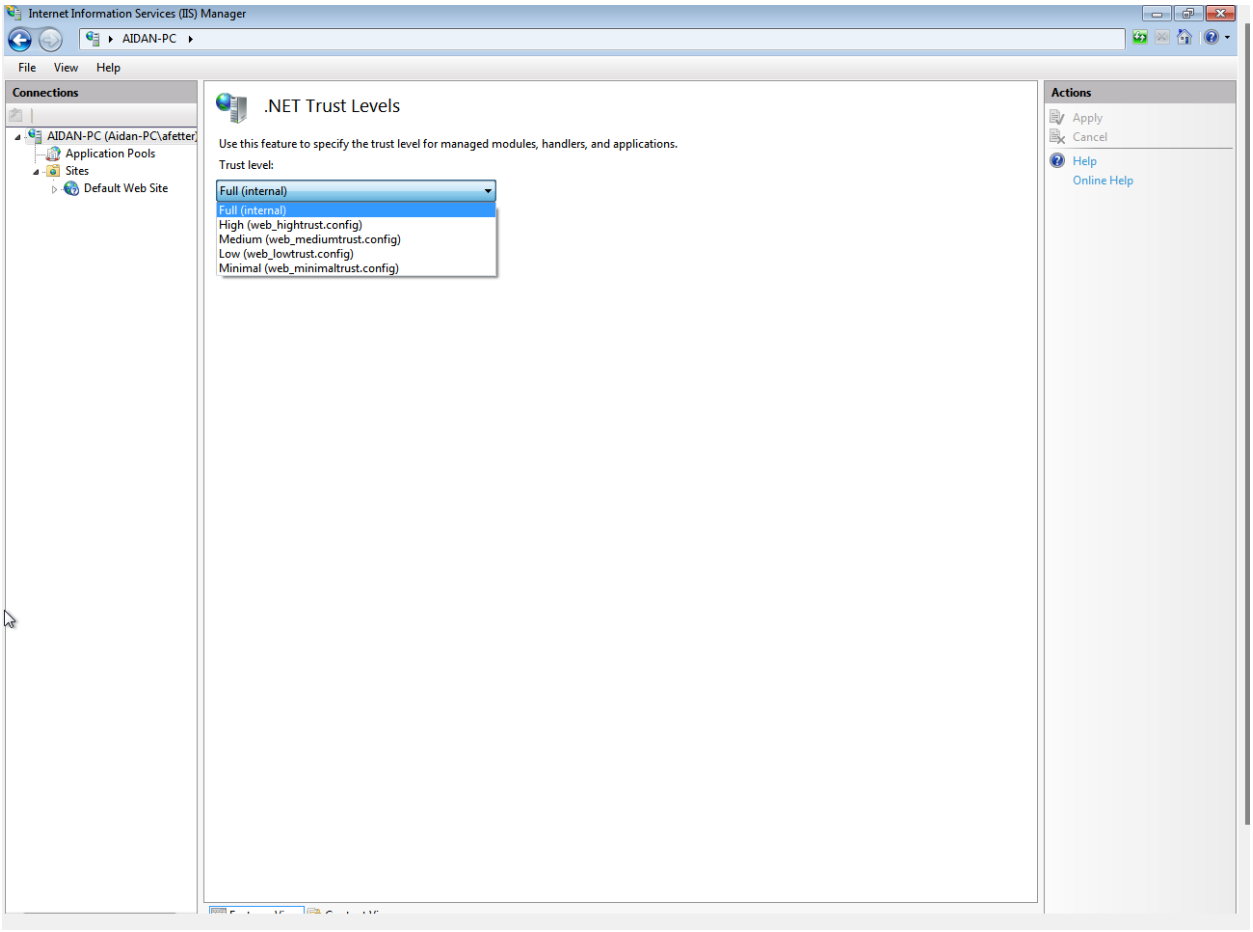


- In order for this to work, you need to already have an error page customized and uploaded as a valid URL. This is to ensure that users are properly being sent to your page.

Optional Team activity: Create an error page and add it to the default website in the IIS server. Be sure to include the URL when adding the page to the server manager so it is processed properly.

3.6. .NET Trust Levels

1. Click the ".NET Trust Levels" button next to the ".NET Error Pages" button
   - This page allows you to specify the level of code access security (CAS) that is applied to an application

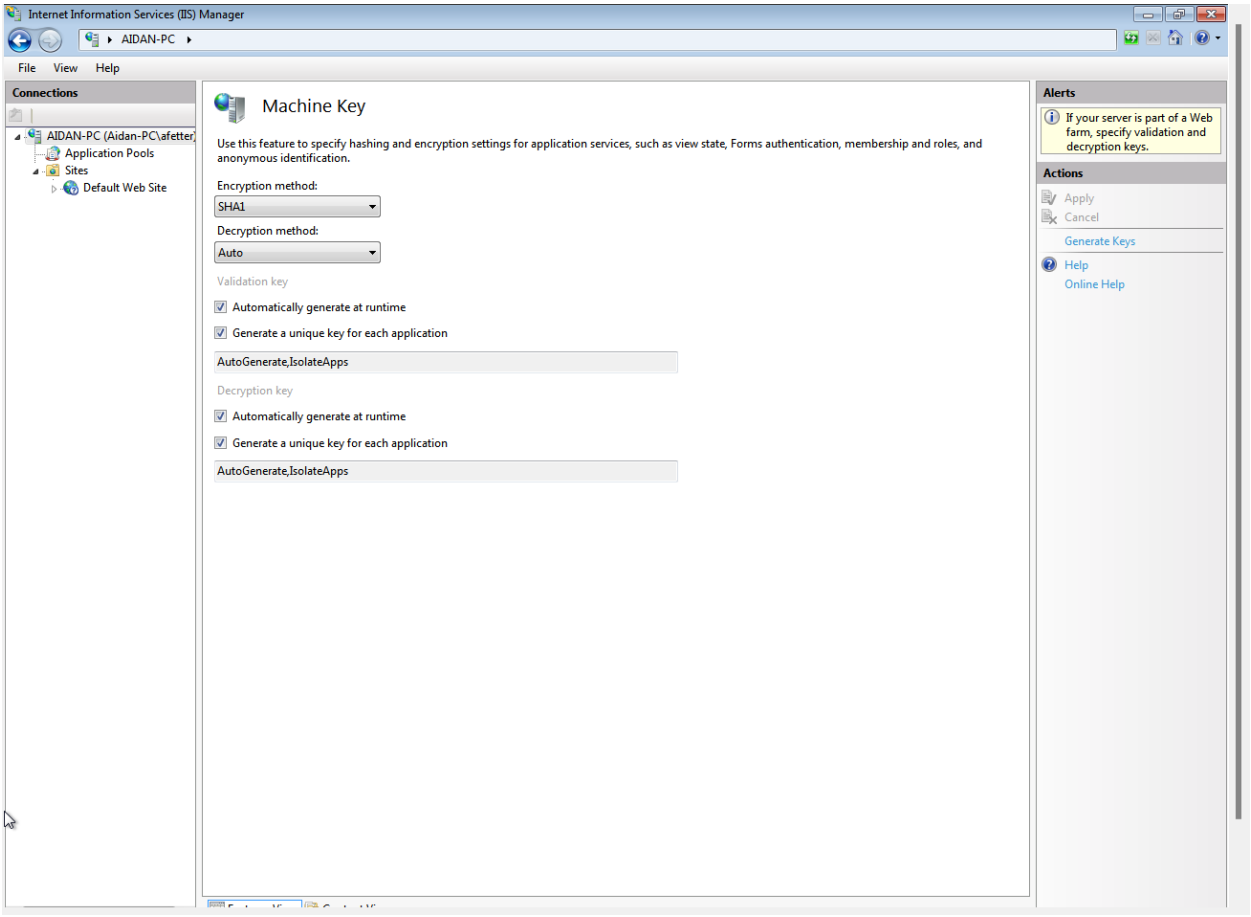


   - Trust Levels:
     - Full (internal) – Unrestricted permissions; All privileged operations are supported
     - High (web_hightrust.config) – The application cannot:
       - Call unmanaged code
       - Call service components
       - Write to the event log
       - Access message queuing service queues
       - Access ODBC, OleDb, or Oracle data sources
     - Medium (web_mediumtrust.config) – On top of high level restrictions, the ASP.NET application cannot:

        - Access files outside of the application directory
        - Access the registry
        - Make network or web service calls
    - Low (web_lowtrust.config) – On top of medium level restrictions, the application cannot:
        - Write to the file system
        - Call the Assert method to test if an expression is true or false
    - Minimal (web_minimaltrust.config) – The application has only executable permissions
2. Change the trust level to “Minimal (web_minimaltrust.config) to ensure that applications can only run for those accessing it

3.7. Configure hashing and encryption settings for application services

1. Click the “Machine Key” button next to the “Connection Strings” button



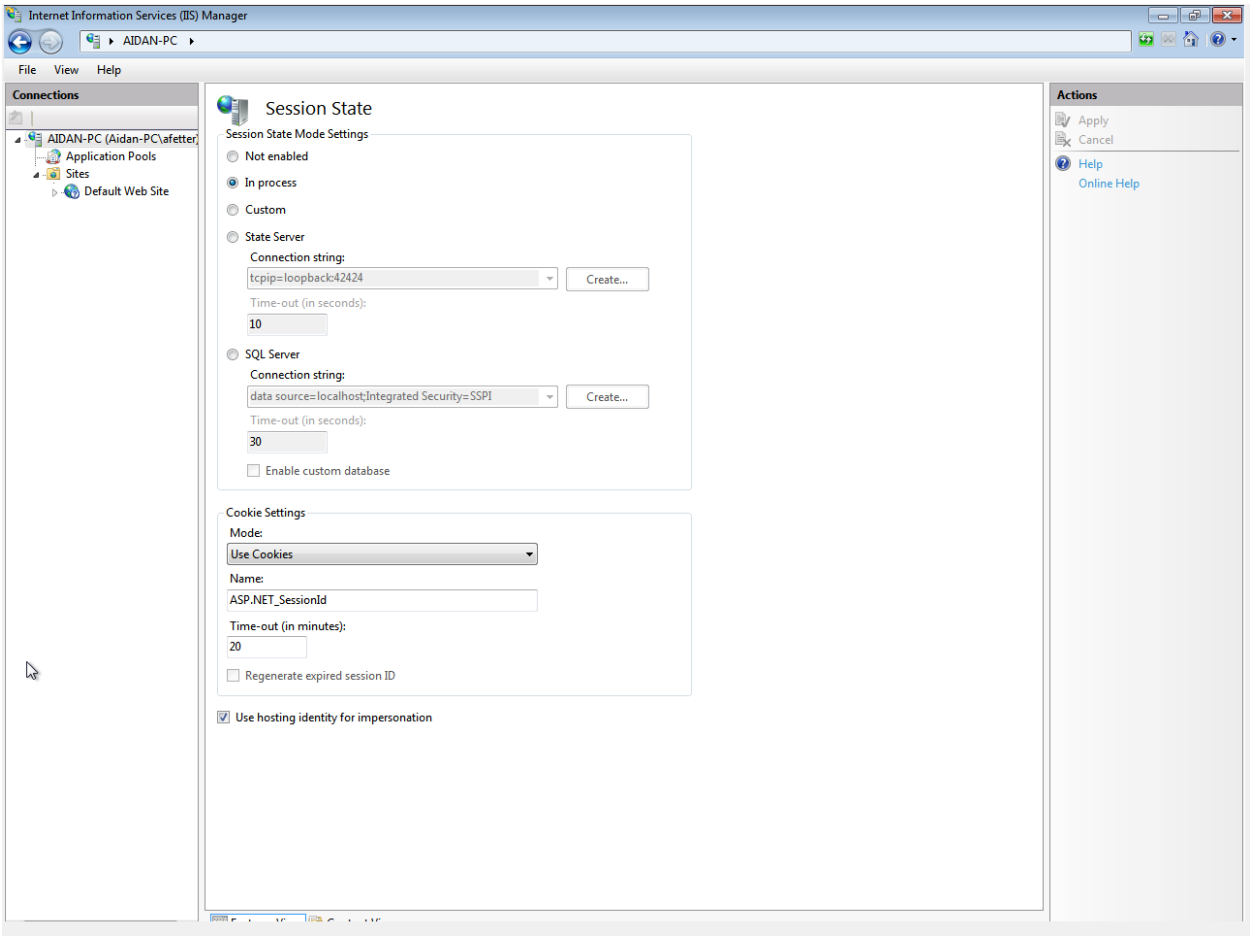
- This page lets you choose hashing and encryption settings for applications and authentication, membership and roles, and anonymous identification
- By default, the encryption method used is SHA1. This algorithm is insecure as various collisions have occurred, making this a very insecure method to use. For this section, the best method to use is either AES or TripleDES as both are very secure

algorithms still used today. However, it is recommended to use AES as it is much faster than TripleDES when encrypting and uses less memory.

2. Choose either AES or TripleDES as the encryption method
3. Leave the decryption method as "Auto" as it will autodetect which encryption algorithm was used (if you would like to specify the specific algorithm, you may do so too)
4. Ensure that both boxes for "Validation key" and "Decryption key" are checked
    - Validation Key – Confirms the integrity of data
    - Decryption Key – Used to encrypt and decrypt forms authentication tickets and view states

3.8. Configure session state and cookie settings

1. Click the "Session State" button next to the "SMTP E-mail" button



- This page allows you to control the state of user information maintained across browser sessions
    - <u>Session State Mode Settings:</u>
        - Not enabled – No session state
        - In process (default) – Stores session data in the worker process where the application runs

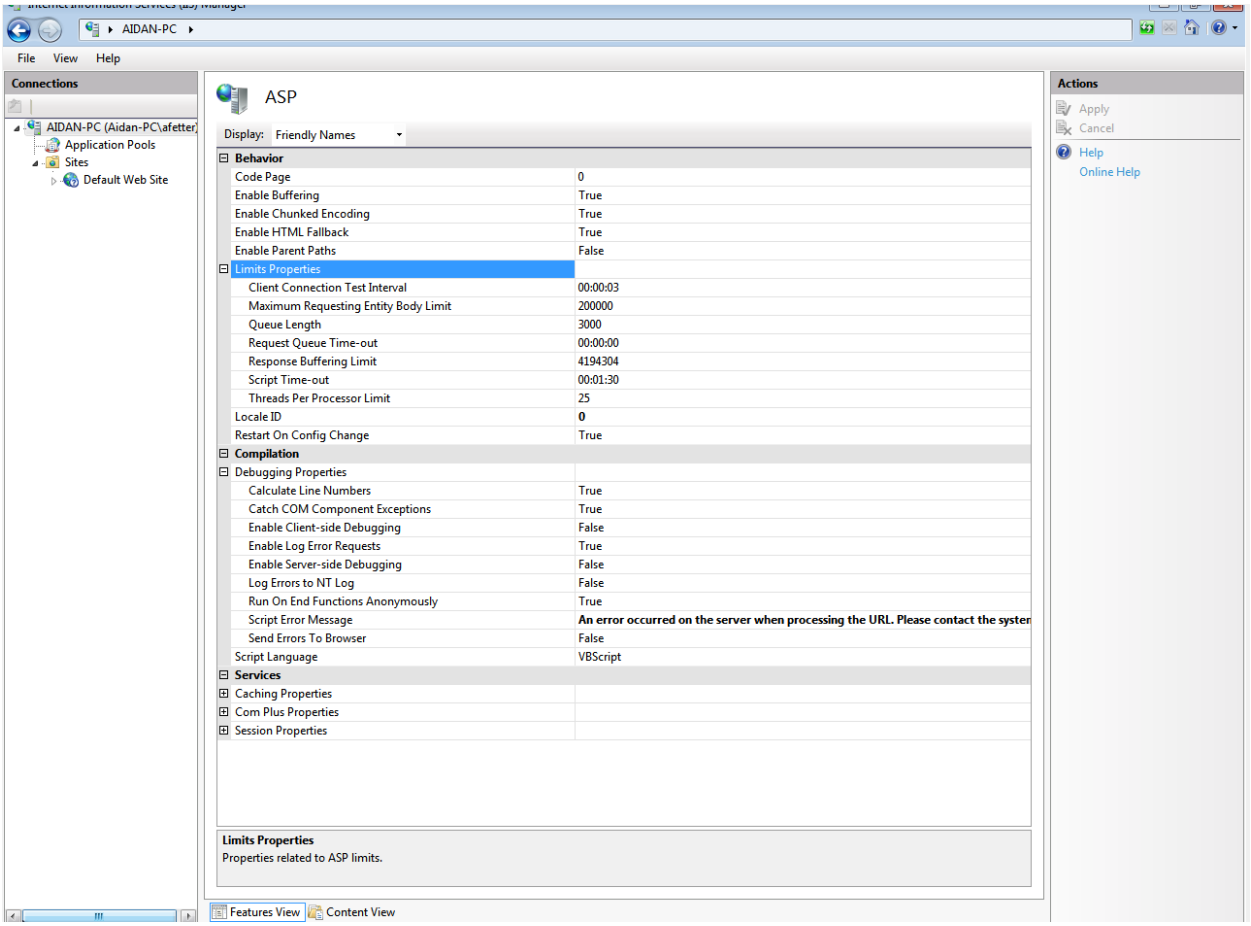
- Custom – Use a custom provider to handle session state
- State Server – Stores session data outside the worker process where the application runs. The session state is preserved when the worker process ends
- SQL Server – Stores session data on an SQL server instead of the worker process. Along with preserving the session state externally, it is also preserved if either the Windows state service or the web server goes down

2. Choose the session state mode that fits best with your IIS server. However, it is not recommended to choose "Not enabled" as session states are very important in maintaining user data on the server
3. Ensure that the "Cookie Settings" mode is set to "Use Cookies" in order to maintain user state on the server as they are accessing the hosted applications

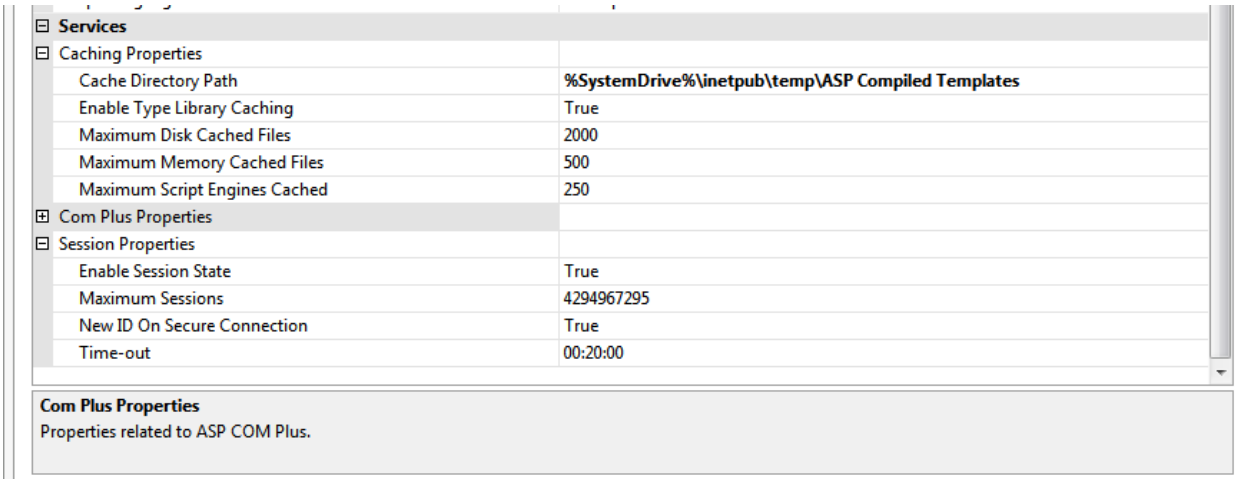
- Use hosting identity for impersonation – Enables Windows authentication to allow authorized hosts to remotely connect to the IIS server

3.9. Ensure that ASP application properties are configured properly

1. Click the "ASP" button under the "IIS" section



3. Security Configuration for an IIS Server



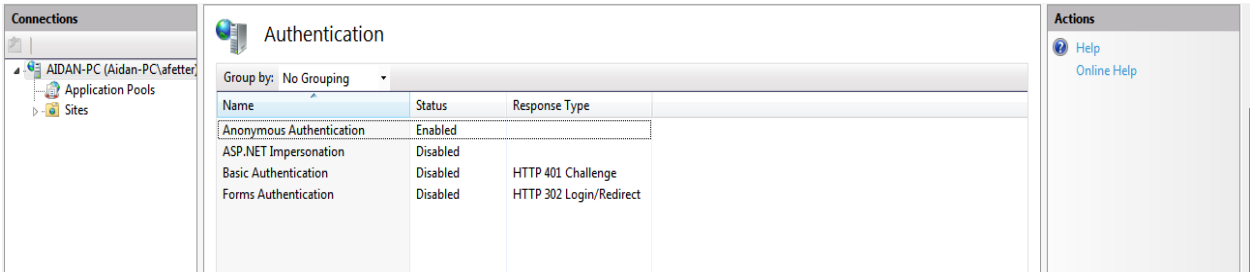
2. Go through each field and determine what properties need to be changed for your IIS sever

- Important ones to look at:
    - Enable Chunked Encoding – True
    - Enable HTML Fallback – True
    - Enable Parent Paths – False
        - This field, if set to true, can lead to a directory traversal attack as the ASP page would allow paths relative to the current directory to be displayed.
    - Restart On Config Change – True
        - This field should be set to true because, for example, if an attacker gets into the IIS Server Manager and changes a setting, the server administrator(s) would be notified and the attacker would be exposed.
    - Enable Client-side Debugging / Enable Server-side Debugging – False
        - The client should not have access to server-side coding issues as this can give them an insight as to how the server is configured. If this field is set to false, the line where the error is occurring would not be displayed and instead the message within the “Script Error Message” would appear.
    - Enable Log Error Request – True
        - Writes ASP error reports to the client browser and to the IIS log files when set to true.
    - Send Errors to Browser – False
        - When this option is set to true, error messages will be send to the client’s browser along with the Window’s Event Log. This should be set to false because if a user has access to these error logs, they can get a glimpse into the backend configuration of the web page, allowing them to find potential exploits.
    - Enable Session State – True

        - When this option is set to true, users maintain a persistent session state when accessing an ASP connection. This allows data to persist while the user browses the application and sends requests to the server.
    - Maximum Sessions – This option can be set as needed depending on how much your IIS server can handle. If you allow too many sessions, an attacker can exploit this and perform a DDoS attack on the server by initiating as many sessions as possible
    - New ID On Secure Connection – True
        - When this option is set to true, the user's sessionID is sent to the server as a secure cookie value if it is assigned over a secure channel
    - Time-out – This option tells the server how long to keep a session active starting from the last request. Make sure you're not setting this value too high or you could risk attacks such as session hijacking or replay attacks.

3.10. Configure authentication settings for users

1. Click the "Authentication" button next to the "ASP" button



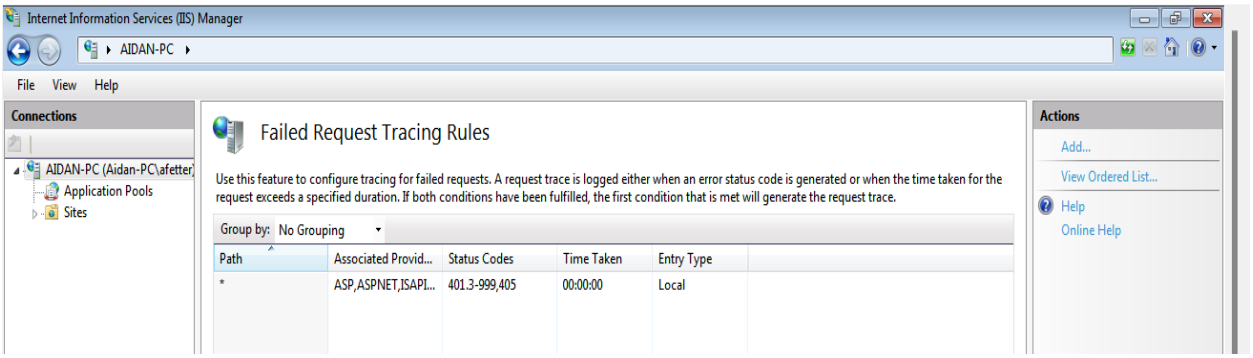
- This page allows you to determine how you want users to be authenticated when accessing the services provided by the IIS server

2. Configure the settings as needed

- The settings are as follows:
    - Anonymous Authentication - Allows any user to access any public content without authorization (use it when you want everyone that visits the website to view its contents
    - ASP.NET Impersonation - Allows you to run ASP.NET applications under a context other than the default ASPNET account (for example, an arbitrary user account)
    - Basic Authorization - Requires user to enter a valid username and password to gain access to services provided by the IIS
    - Forms Authentication - Uses client-side redirection to forward users to an HTML form in which they can enter credentials
- Note: To enable maximum security on the server, only enable either basic authentication or forms authentication as they both require users to enter valid credentials to see the web content

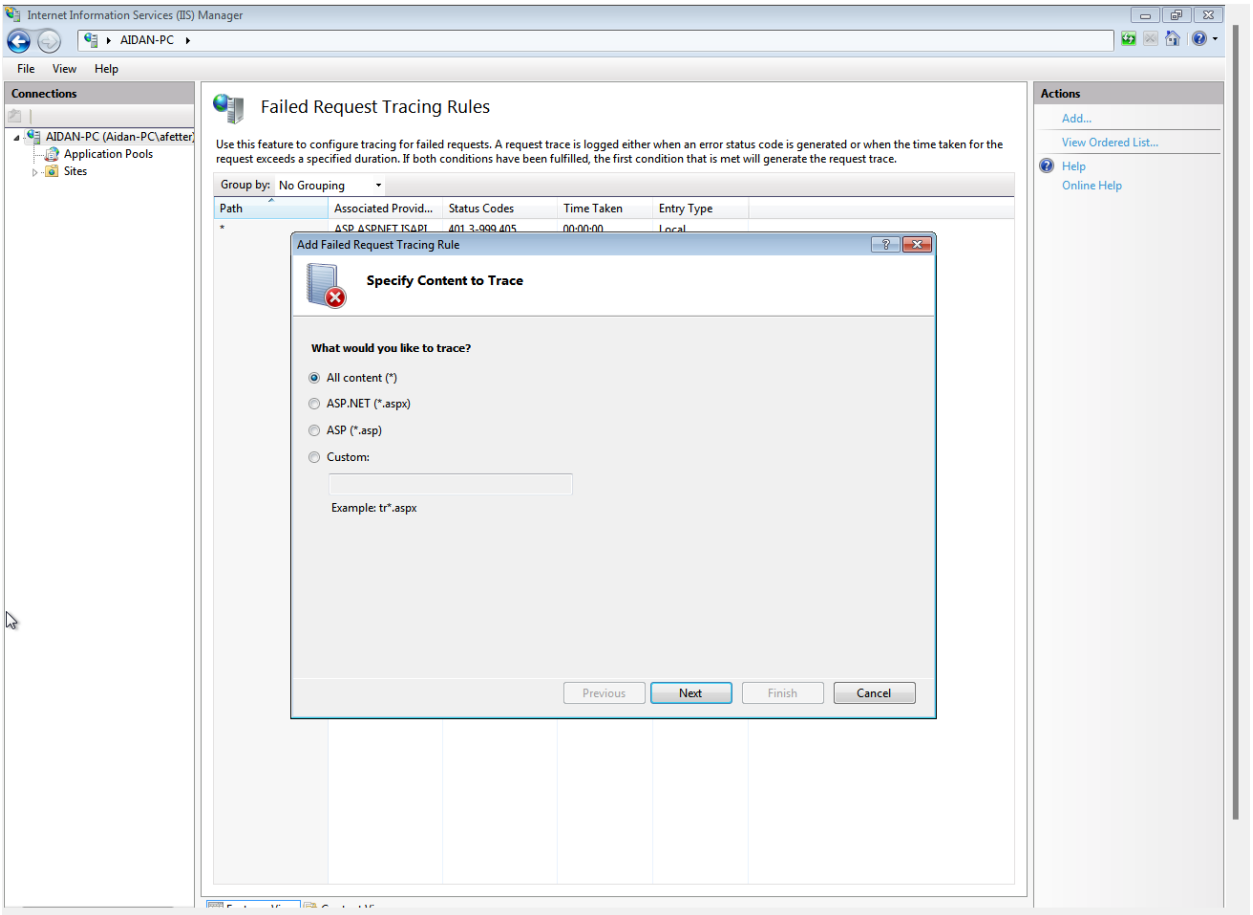
3.11. Trace failed requests

1. Click the “Failed Request Tracing Rules” button next to the “Error Pages” button



- This page allows you to choose which content should be traced upon failure.

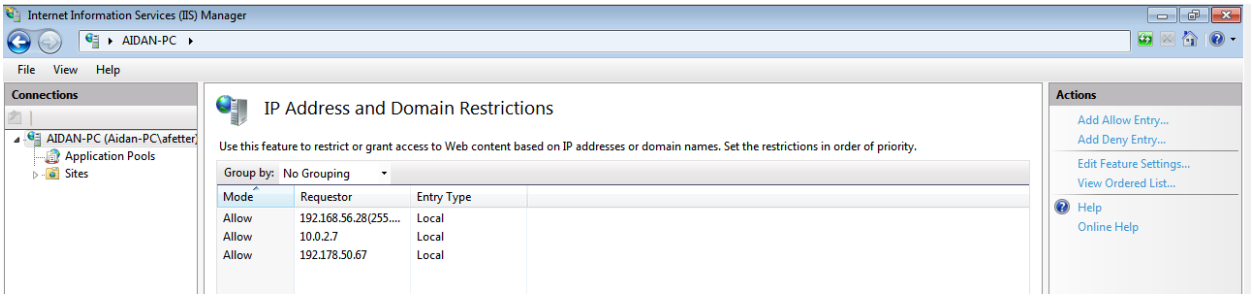
2. Press the “Add…” button to add a new trace rule



3. To maximize security, you should track all content to ensure that the server keeps track of every failure that may occur while hosting. By default, all failed content will be traced. If this is not the case on your server, press “Next” and specify that all status codes should be monitored

3.12. Restrict access to specific IP addresses and domains

1. Press the “IP Address and Domain Restrictions” button next to the “ISAPI and CGI Restrictions" button

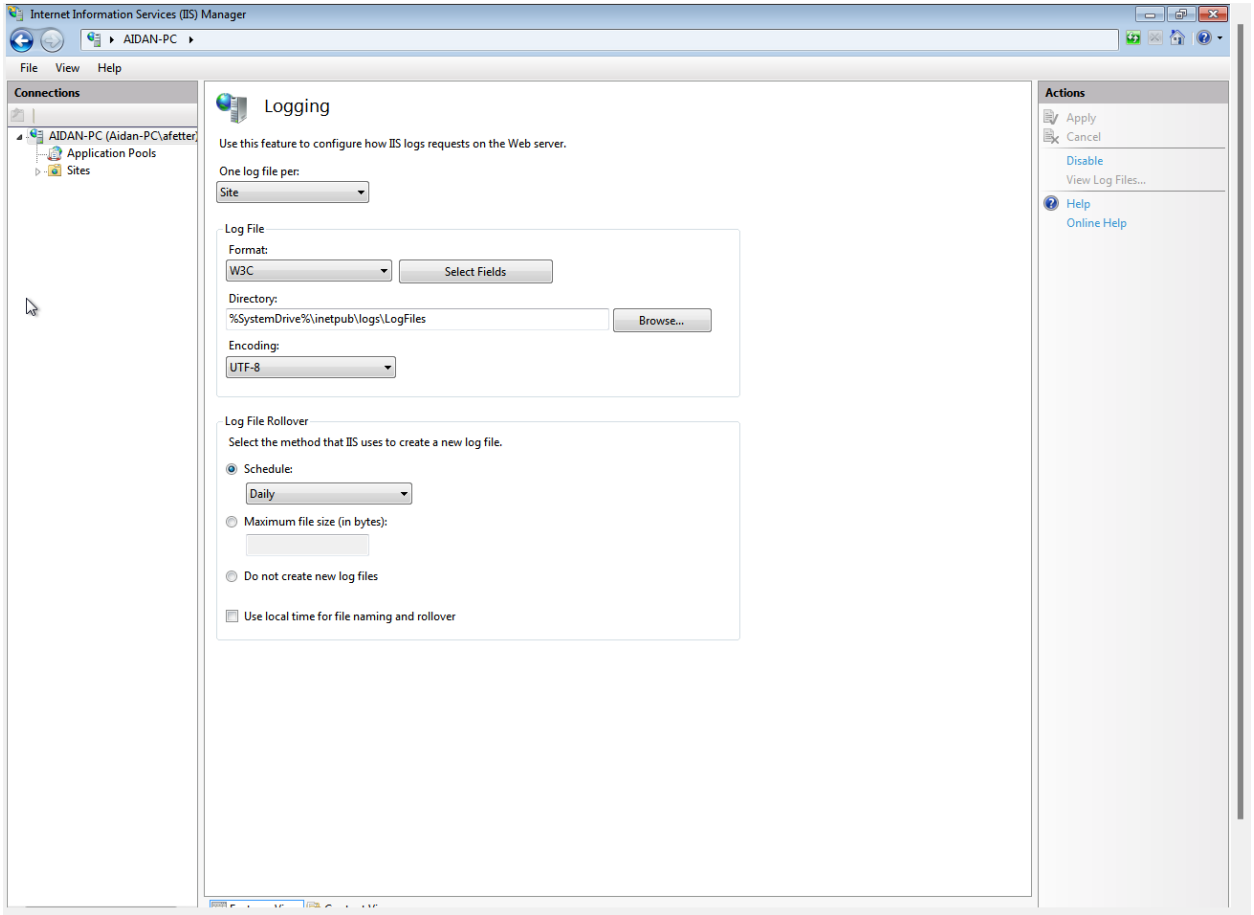


- This page allows you to choose which IP addresses and domains are allowed and denied access to the IIS server’s resources (similar to a packet-filtering firewall)

2. Configure the settings to match your IIS audience

3.13. Ensure that logging is enabled

1. Press the “Logging” button next to the “ISAPI Filters” button

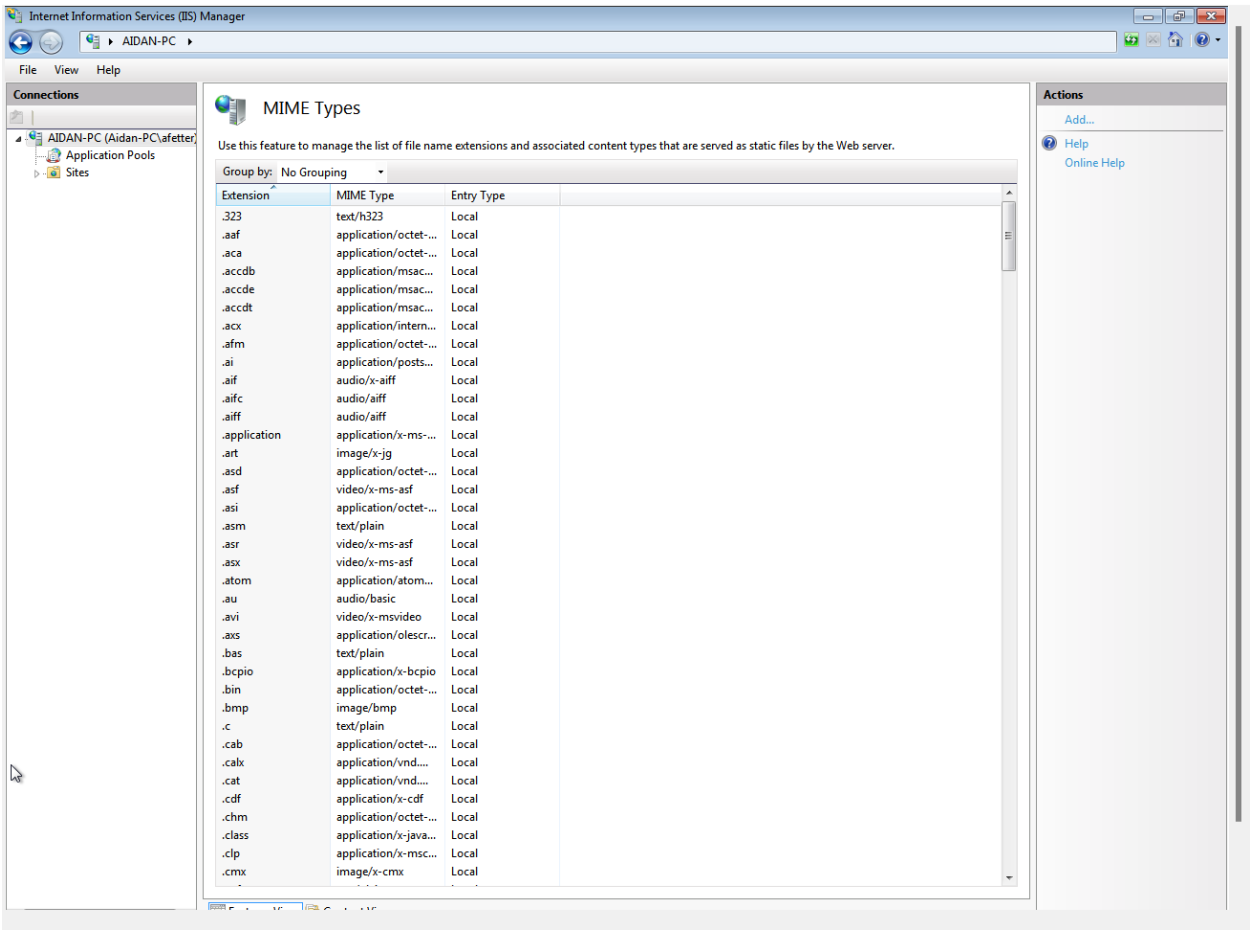


- This page allows you to choose how often you want the IIS server to create a log, the encoding method for each log, and the format the log is stored in. This page is also important because it shows the directory the logs are stored in. This is crucial for security because it allows a server administrator to locate the logs and understand what happened in case of an attack, failed configuration, etc.

2. Configure the settings to match with how/where you want logs to be kept

3.14. Choose the types of files that can be sent to a browser from the server

1. Click the “MIME Types” button next to the “Logging” button



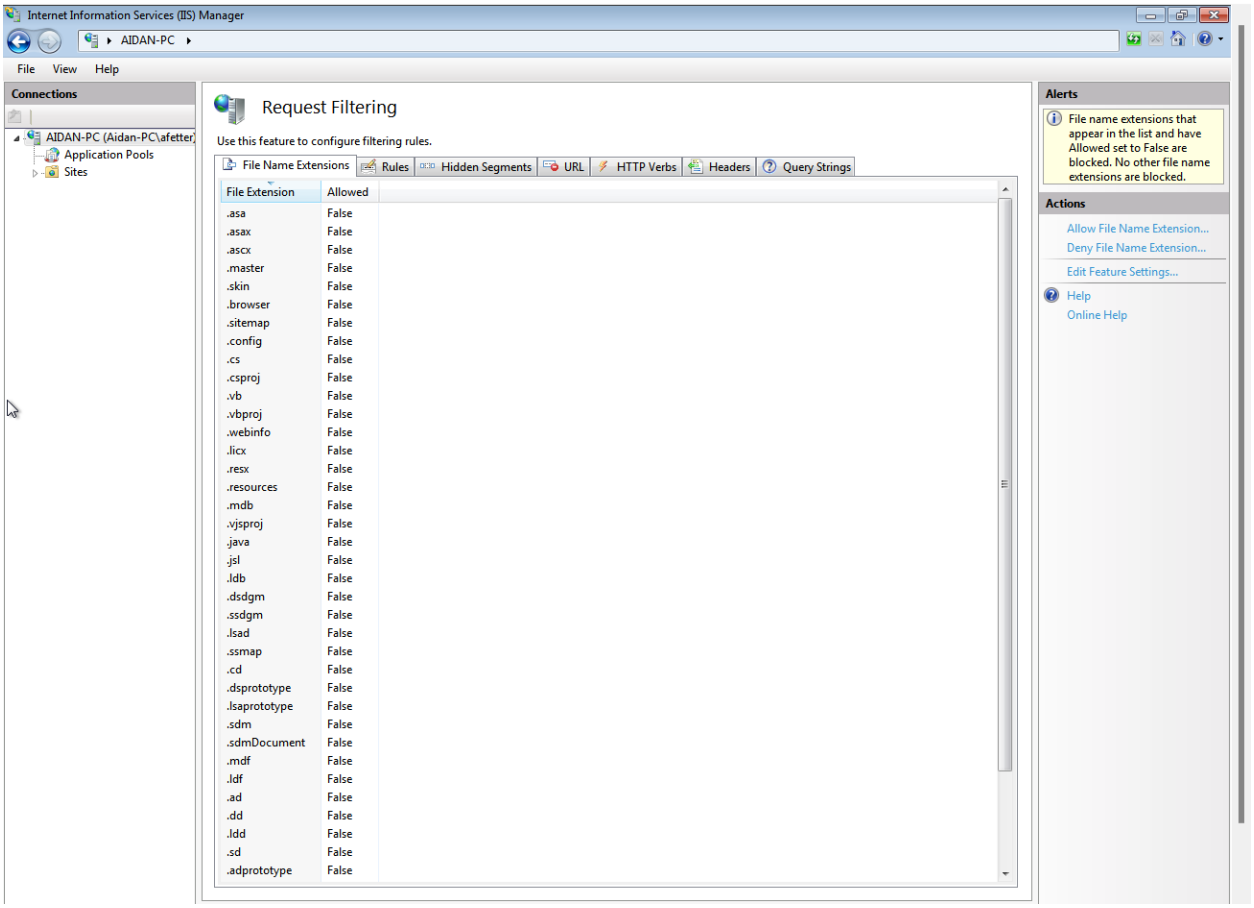
- This page allows you to specify the specific MIME types allowed to be sent by the server to a user accessing the IIS services. This page is important because it allows you to filter out MIME types you don’t need or add more if needed.

2. Add/Remove the appropriate MIME types for your IIS server

3.15. Filter Requests

1. Click the “Request Filtering” next to the “Output Caching” button

3. Security Configuration for an IIS Server



- This page allows you to filter requests sent to the IIS server based on the following attributes:
    - File Name Extensions (such as .dd and .java)
    - Rules (such as headers, file extensions, and strings)
    - Hidden segments (such as bin and App_data)
    - URLs (such as www.google.com)
    - HTTP verbs (such as “POST”, “GET”, and “HEAD”)
    - Headers and the header size held within an HTTP request
    - Query Strings (such as

```
‘ OR ‘1’=’1
```

      in an attempt to perform an SQLi attack)

- This filter is very important because it can prevent your IIS server from potential attacks that may occur due to faulty sanitization.

2. Ensure that all filtering rules are put in place and take as many potential exploits into account as possible

4. Team Activity During Meeting

During the meeting, everyone will be working on the below tasks together as this will be the case during the actual competition. As the team captain/co-captain, ensure that everyone on the team understands how a task was completed before moving on so everyone is on the same page. Also be sure to look over who is doing what and how well they adapt to the team so you can understand how to improve the team as a whole before the competition.

1. Edit the default authorizarion rules (both IIS and .NET) to include only the usernames on your VM and apply the rule to the HTTP verbs GET, POST, and HEAD and deny access of IIS services to all anonymous users along with the verbs OPTION, PUT, CONNECT, TRACE, and PATCH.

2. Assume you want the customers accessing your web services to be limited to a max file size of 50000 KB (5 MB). Implement this change in your IIS settings page.

3. Create a custom error page and add the path as an entry so the server outputs that page upon returning the error code.

4. Limit the trust level of the server so it only has executable permissions and configure hashing and encryption settings for application services.

5. Ensure that all failed requests to the server are traced and allow only the following IP addresses to access server content:
   - 192.168.56.28 – 192.168.56.40
   - The IP address of your VM
   - The IP address of **www.google.com**

After about 20-30 minutes, ask different members of the team to present how they did one of the problems to ensure that the all members were collaborating with each other effectively and understood how to complete the tasks.

5. References and Additional Resources:

- IIS Official Website
- IIS In-Depth Explanation With Security Configuration - Microsoft
- IIS Overview
- Internet Information Services - Wikipedia
- What Is IIS Server? - SolarWinds

5. References and Additional Resources:

- What is IIS? - Stackify
- IIS Configuration and Setup
- IIS Web Server Installation & Website Configuration | Introduction to Windows Server 2016 Course
- Enabling IIS and required IIS components on Windows 7
- Improving IIS Security - UpGuard