Working with Verizon Connect Reveal in ArcGIS GeoEvent Server

Author: Morakot Pilouk (mpilouk@esri.com), Esri Inc.

Editor: Greg Tieman (gtieman@esri.com), Esri Inc.

Created: 3/5/2021

Last updated: 6/2/2021

Document version: 1.0.0

Introduction

Verizon Connect provides multiple fleet management solutions for tracking and managing your fleet of vehicles (*Figure 1*). This blog will focus specifically on Verizon Connect Reveal and how you can connect to the data feed and perform real-time ingestion and analysis with ArcGIS GeoEvent Server.

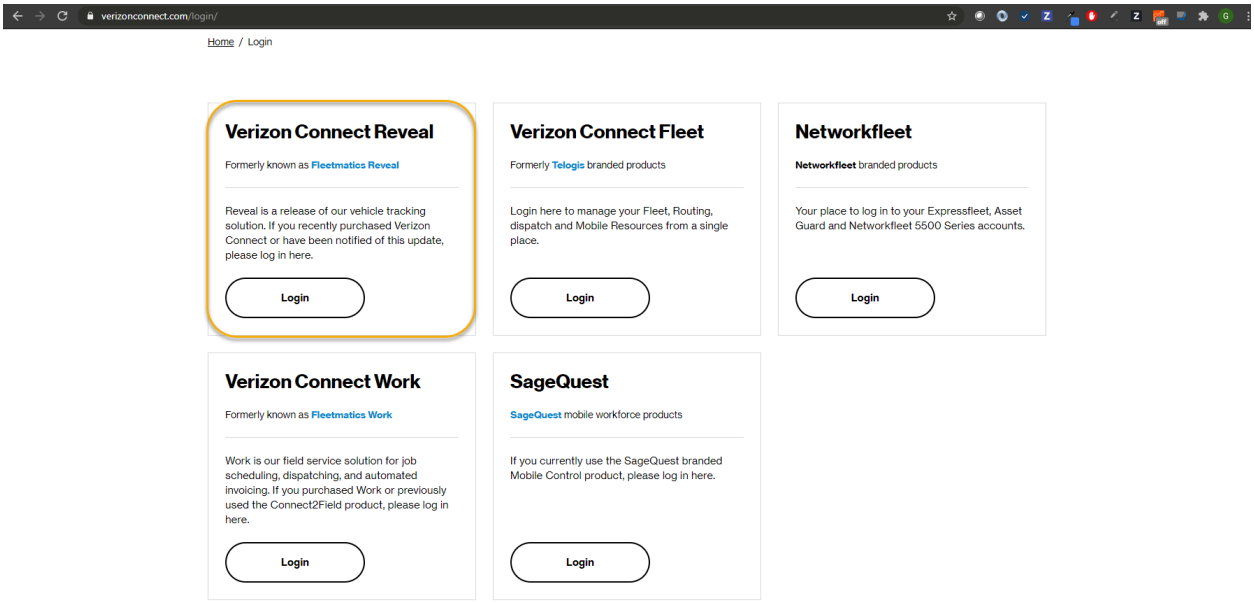


Figure 1: Verizon fleet management solutions

Verizon Connect Reveal provides an API to receive position data from your fleet of vehicles (*Figure 2*). A couple approaches are available for how you receive the data including polling a REST API endpoint on demand or having the data automatically pushed by a Verizon server to a client endpoint. This blog focuses on the *GPS Push Service* which based on the latter approach. This approach requires the client endpoint to be set up in such a way that a Verizon server can connect and send the data to it. The client endpoint needs to be protected using basic authentication. The Verizon server will authenticate with the client endpoint prior to sending data. This blog uses Windows IIS and the following steps highlight enabling basic authentication and routing from an IIS endpoint to an ArcGIS GeoEvent Server connector endpoint. An organization firewall or a load balancer can be used in place of IIS.

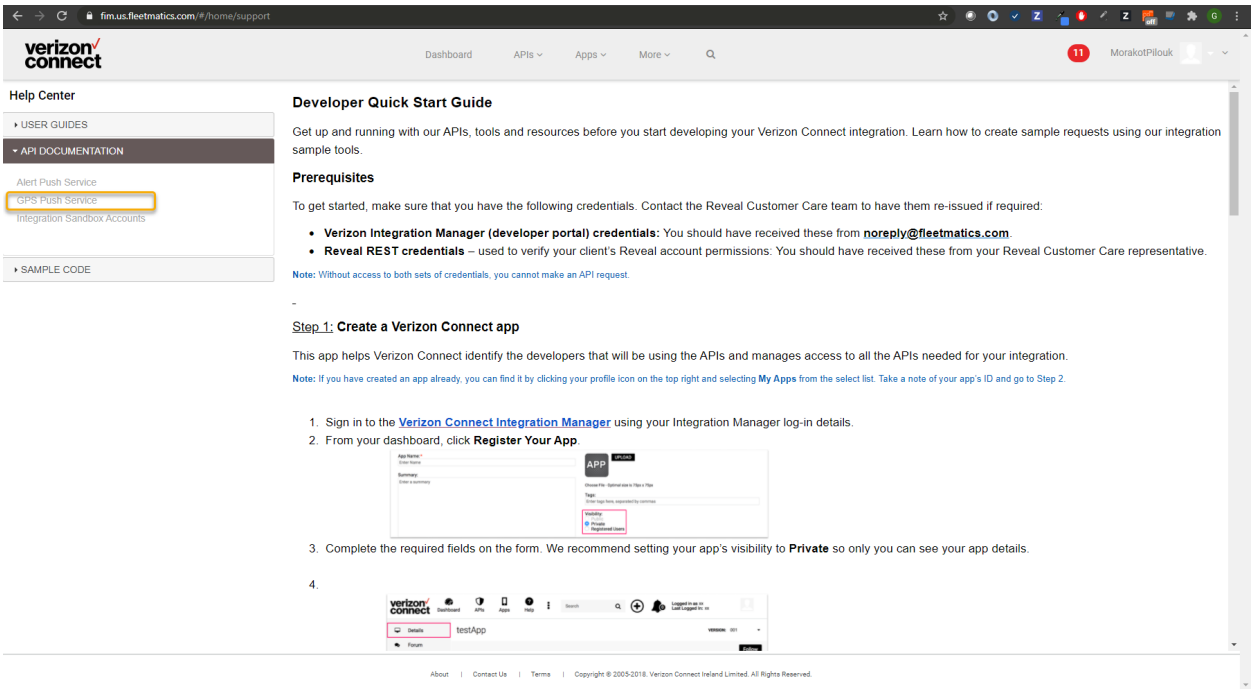


Figure 2: Verizon GPS Push Service

It is assumed you have GeoEvent Server installed and configured and are familiar with configuring inputs, GeoEvent Services, and outputs in GeoEvent Manager. If you're not, access the available quick start guide, documentation, and tutorials. This blog refers to GeoEvent Server 10.8.1.

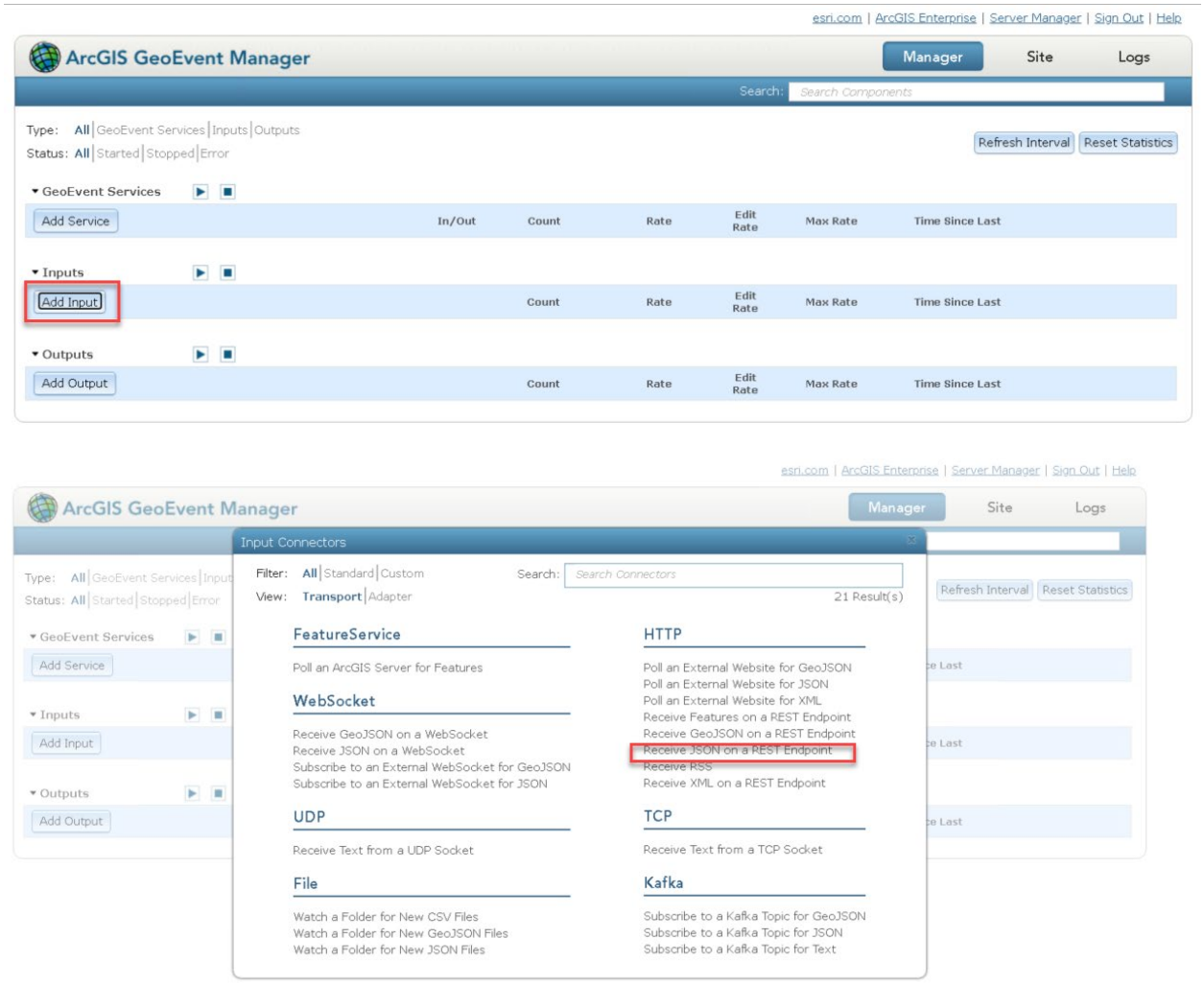
This blog is broken down into five sections. Follow the steps outlined in each section to properly configure, ingest, process, and disseminate the Verizon Connect Reveal data.

- Configure a GeoEvent Server connector endpoint to receive data from Verizon Connect Reveal
- Enable basic authentication on the machine
- Route traffic from an IIS endpoint to a GeoEvent Server connector endpoint
- Configure GeoEvent Server to process the Verizon Connect Reveal data
- Test the Verizon Connect Reveal data feed

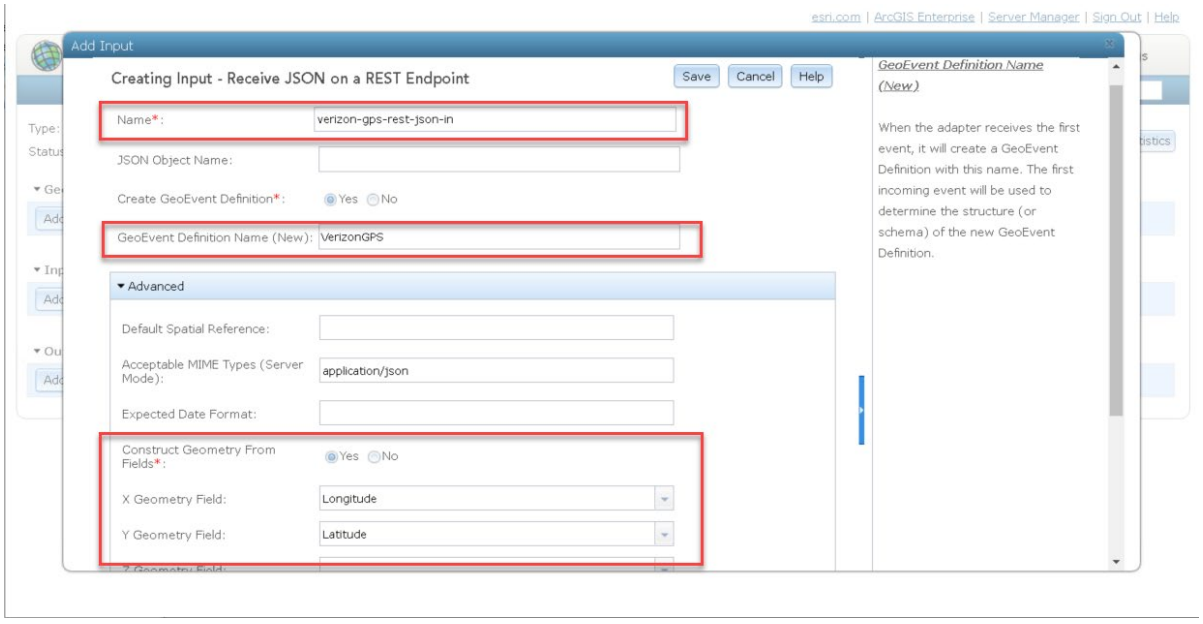
Configure a GeoEvent Server connector endpoint to receive data from Verizon Connect Reveal

First, configure a GeoEvent Server input connector to receive data from Verizon Connect Reveal.

1. Open a web browser and navigate to **ArcGIS GeoEvent Manager** (e.g., https://*<your_machine>*:6143/geoevent/manager).
2. Click **Add Input** and then click **Receive JSON on a REST Endpoint**.



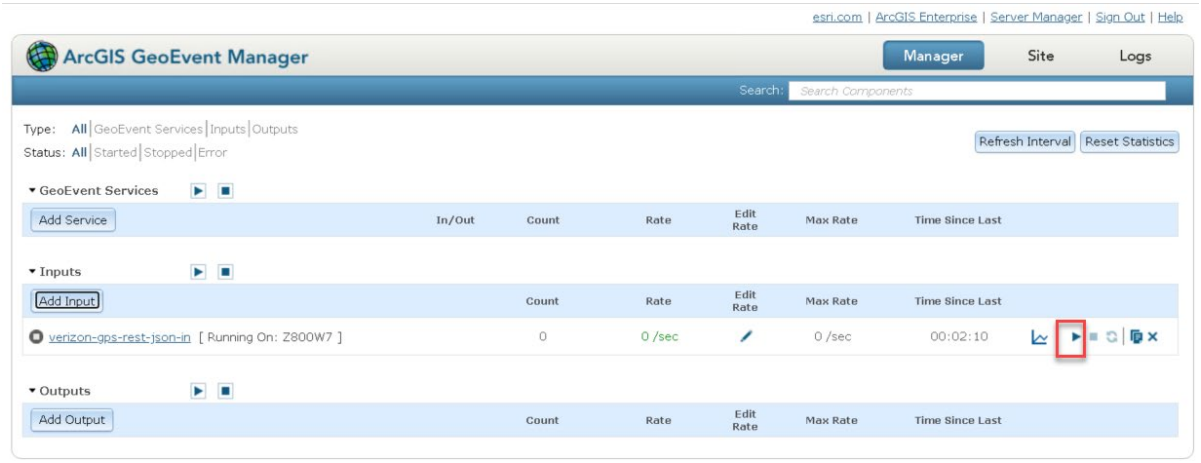
3. Configure the new input connector as illustrated below.



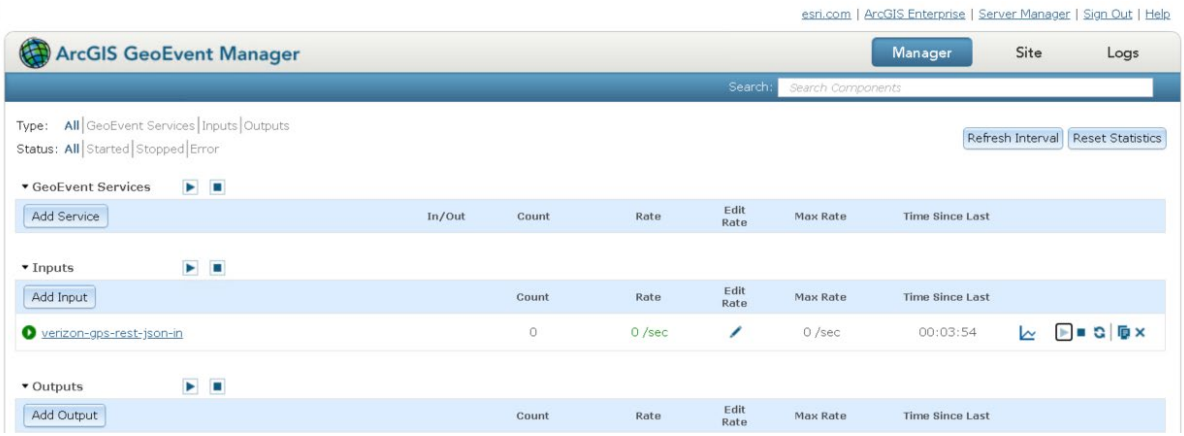
4. Click **Save** to save the new input.

   The new **verizon-gps-rest-json-in** input will be listed under **Inputs**.

5. Click play to start the input and make it ready to receive incoming data.

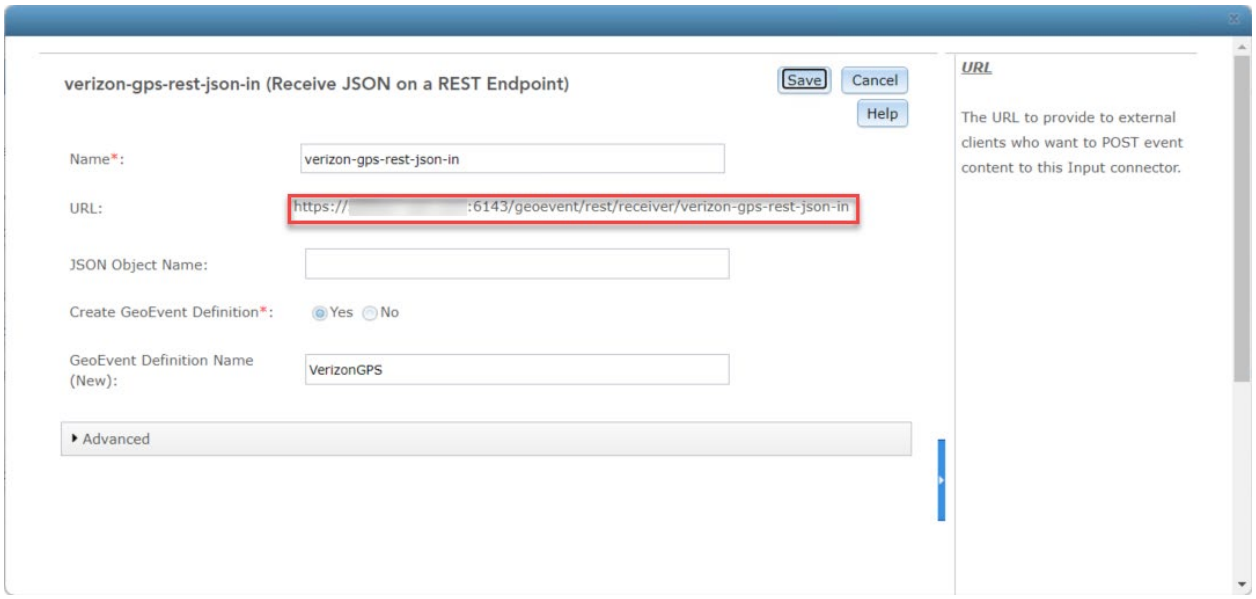


   Notice the input changes from a stopped state to started, indicated by the green icon to the left of the input.



6. Click the **verizon-gps-rest-json-in** input to open the properties.
7. Copy and paste the URL in the **URL** parameter to a text editor.

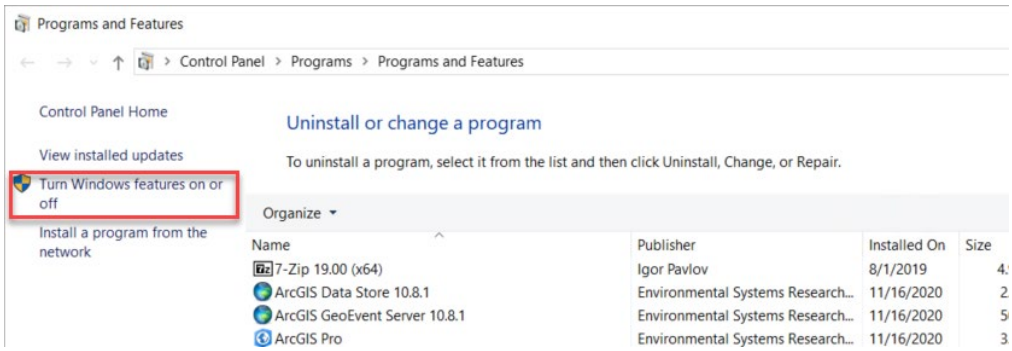
   You will use this later for a URL Rewrite rule.



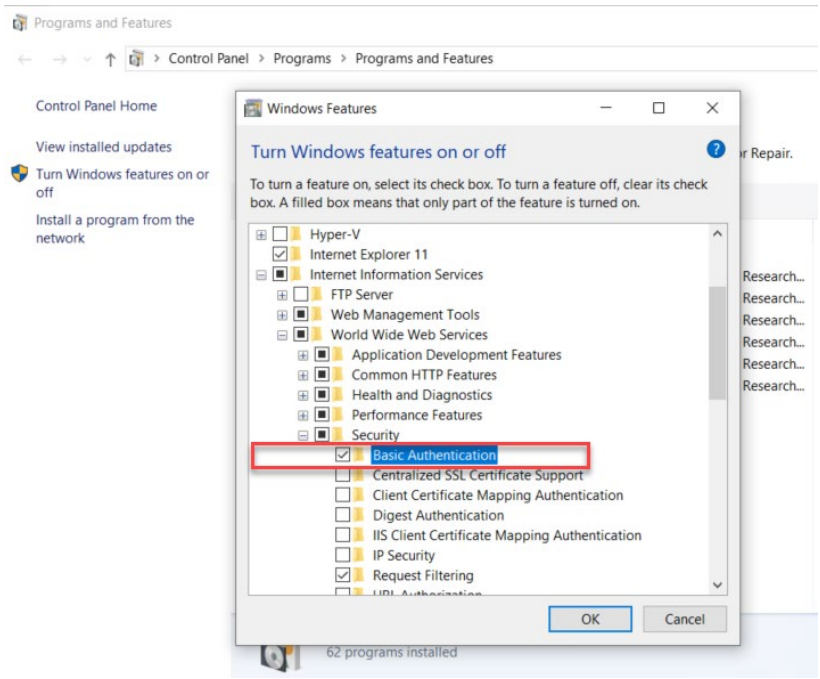
Enable basic authentication on the machine

To enable basic authentication, you will rely on a feature in the Windows operating system.

1. Open the **Control Panel** and navigate to **Programs** > **Programs and Features**.
2. Click **Turn Windows features on or off**.



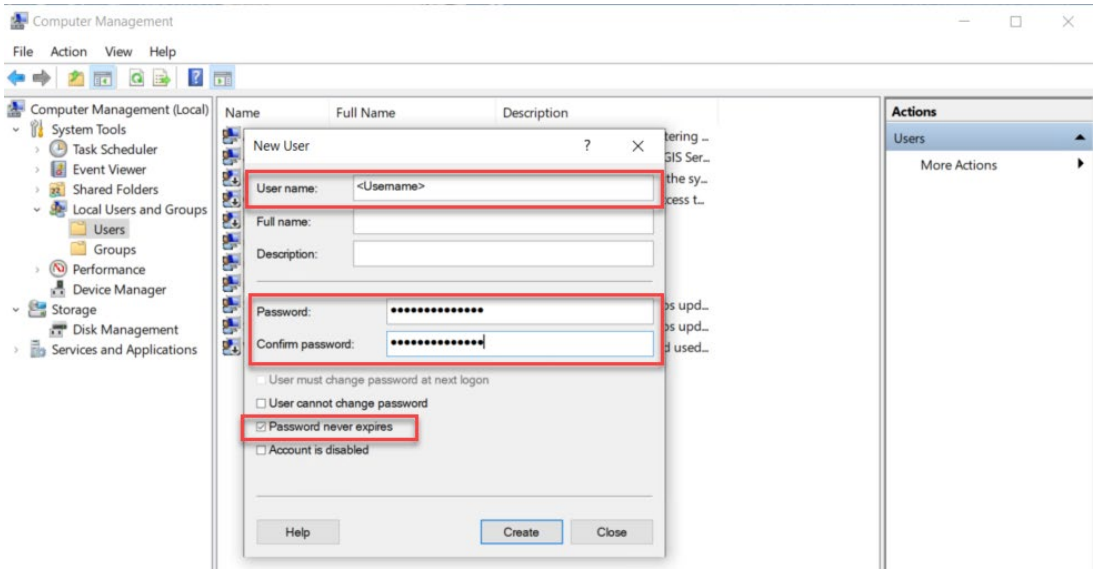
3. Navigate to **Internet Information Services** > **World Wide Web Services** > **Security** and check the **Basic Authentication** checkbox.



4. Click **OK** to apply the change and **Close** once the change is applied.

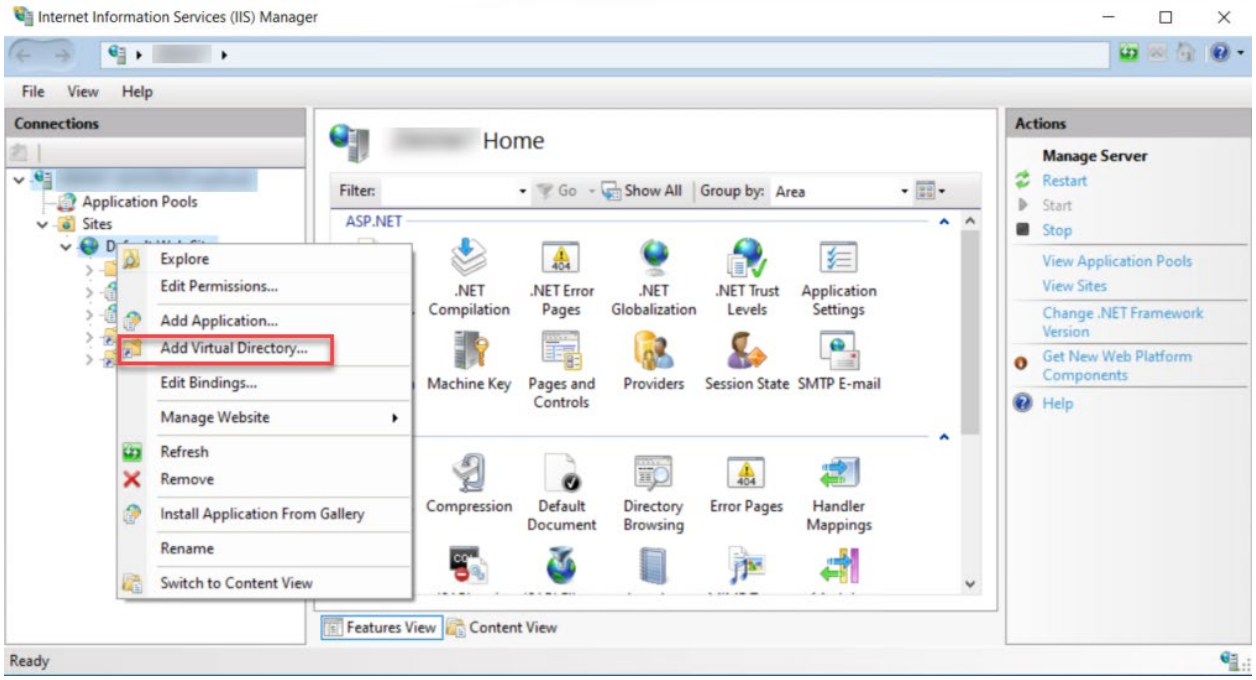
Next, you will create a local account on the machine that will provide the URL endpoint for the Verizon Connect Reveal server to authenticate, connect to, and send data to.

5. Open **Computer Management** and navigate to **Local Users and Groups** > **Users** and from **More Actions** click **New User**.
6. Enter your **User name** and **Password** then confirm.

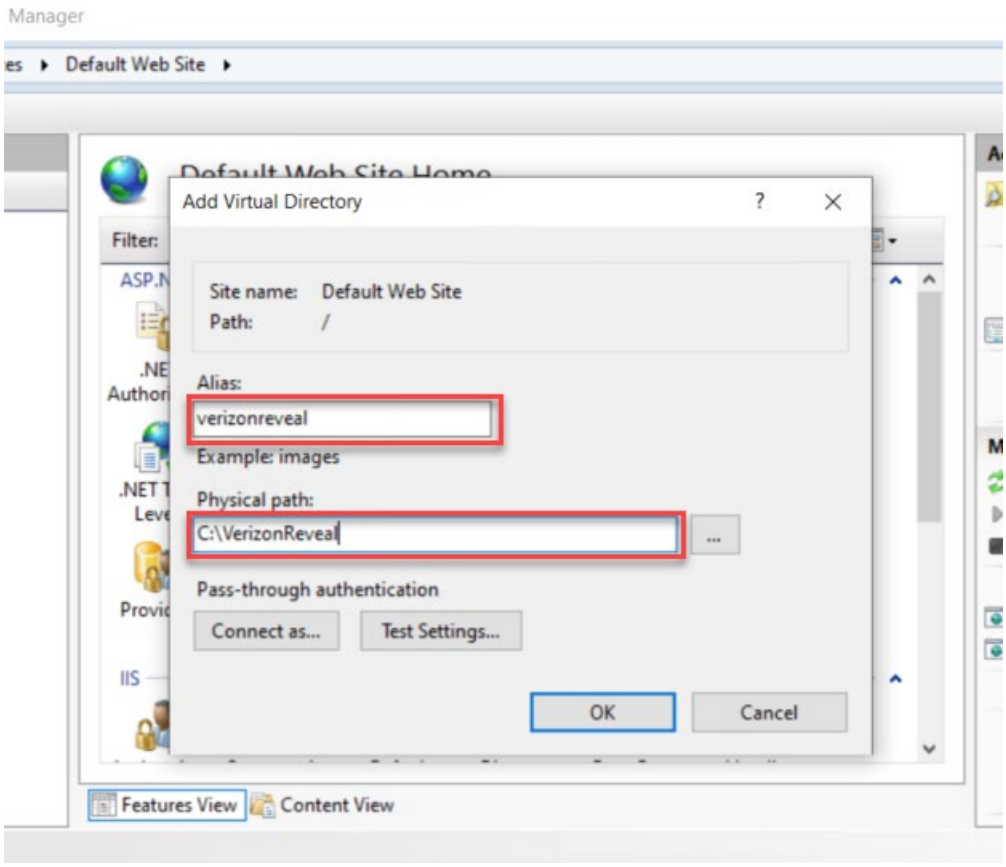


7. Click **Create** to create the new user.
8. In **File Explorer**, create a new folder at **C:\VerizonReveal**.

9. Open **Internet Information Services (IIS) Manager** and navigate to **Sites** and right-click **Default Web Site** and choose **Add Virtual Directory**.

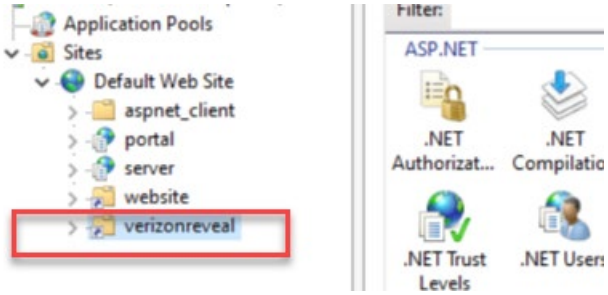


10. Enter the **Alias** and **Physical path** as illustrated below. then click the OK button to dismiss the dialog.



11. Click **OK** to add the new virtual directory.

    The new virtual directory should now appear under **Default Web Site**.



12. To test the virtual directory, create a new **index.html** file in the folder **C:\VerizonReveal**.
13. Open **index.html** in a text editor and copy and paste the content below.

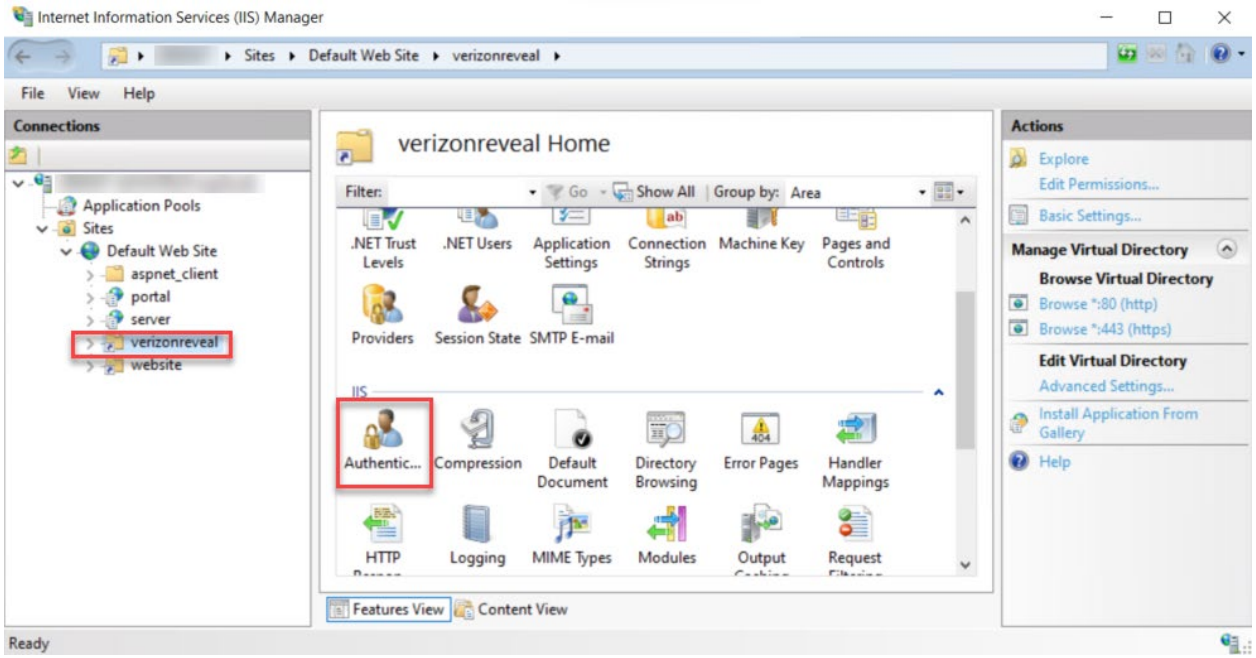
```
<!DOCTYPE html>
<html>
<body>
Hello Verizon
</body>
</html>
```

14. Save the text file.
15. In a browser, enter **http://localhost/verizonreveal**.

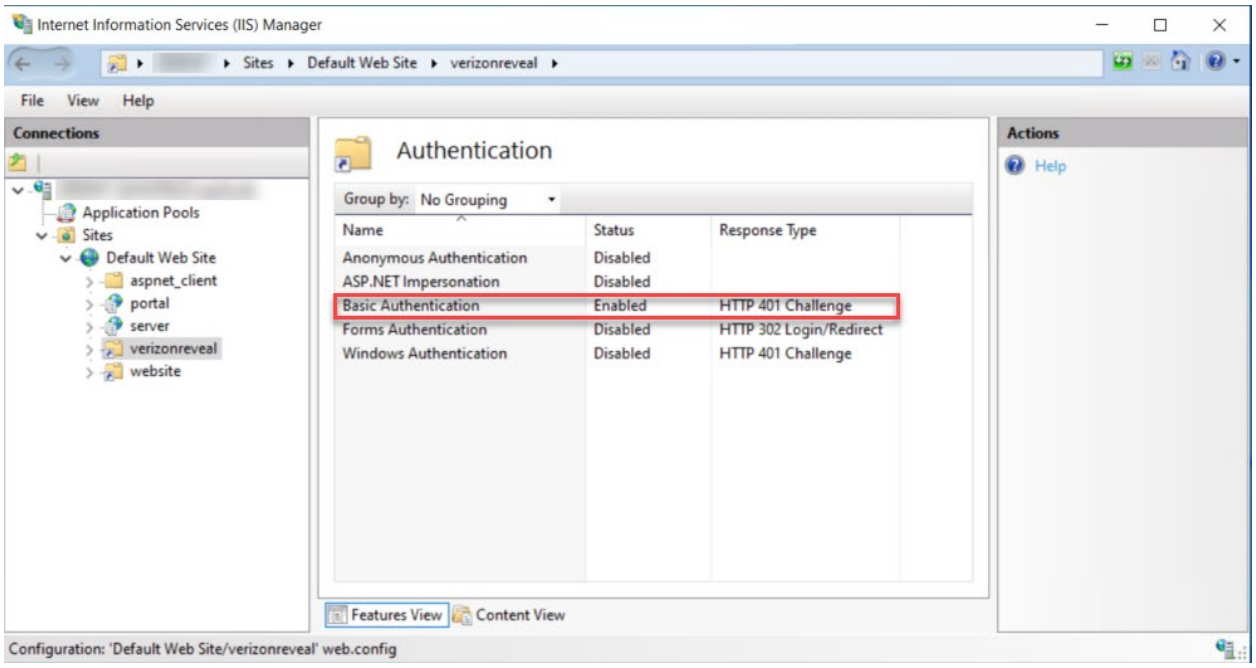
    The text **Hello Verizon** should display on the page.

Next, it is necessary that basic authentication be enabled for the virtual directory in IIS Manager.

16. Open **Internet Information Services (IIS) Manager** and navigate to **Sites** > **Default Web Site** and select the **verizonreveal** virtual directory.
17. Double-click **Authentication** or click **Open Feature** from the **Actions** panel on the right.

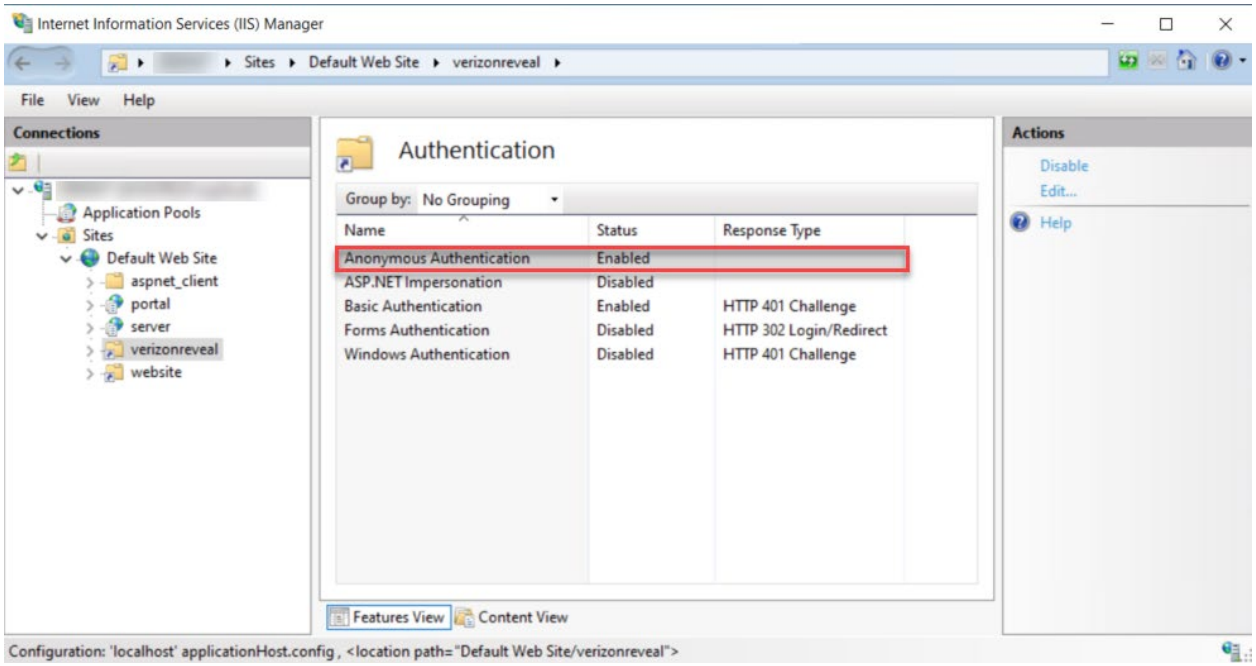


18. Select **Basic Authentication** then choose **Enable** under **Actions** on the right panel.



Notice the **Status** column for the **Basic Authentication** changed from **Disabled** to **Enabled**.

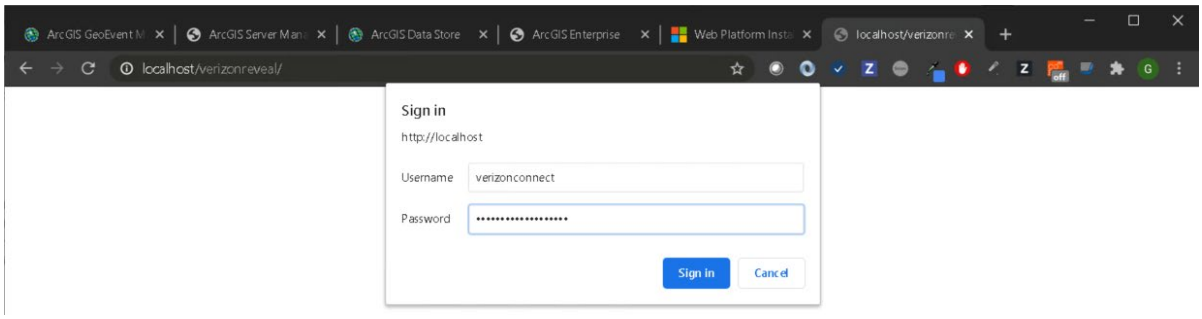
19. The **Anonymous Authentication** status is **Enabled** by default, select it and then choose **Disable** from **Actions** panel on the right.



The status of the **Anonymous Authentication** changes to **Disabled**.

20. To test the basic authentication, open the browser and navigate to http://localhost/verzionreveal/.

    A **Sign in** dialog will pop up.



21. Enter your **Username** and **Password** for the **verizonconnect** user and click **Sign in**.

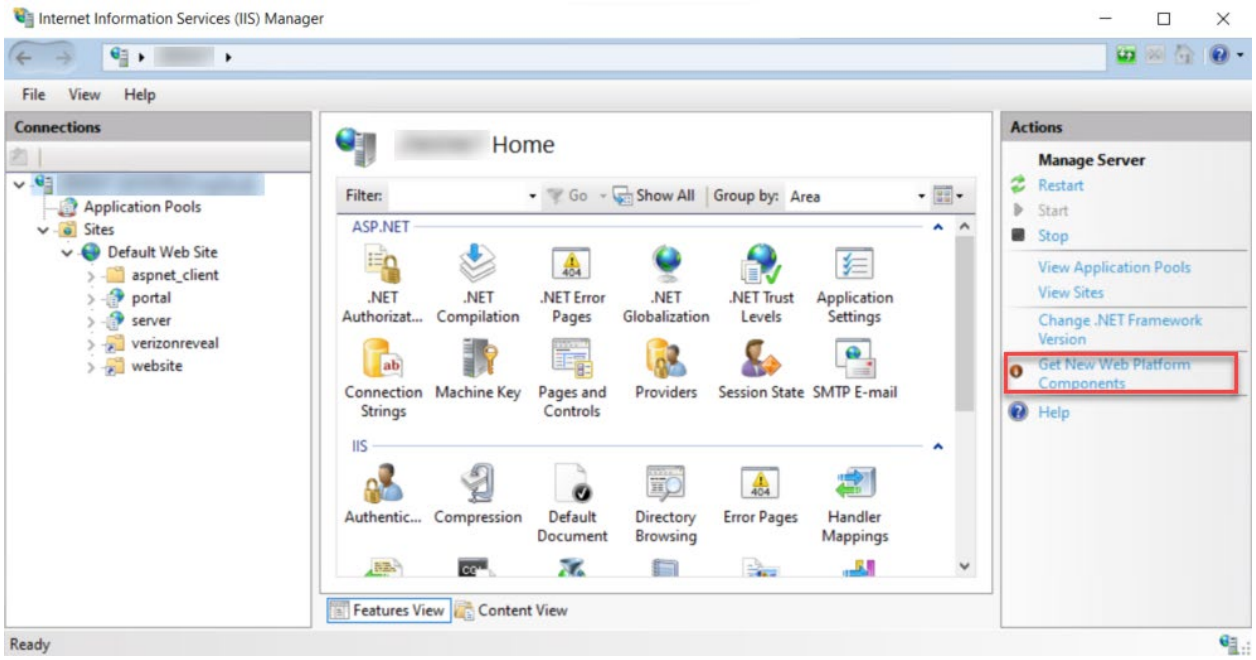
    If authentication is successful, the webpage will display **Hello Verizon**, indicating basic authentication is working properly.

Route traffic from an IIS endpoint to a GeoEvent Server connector endpoint

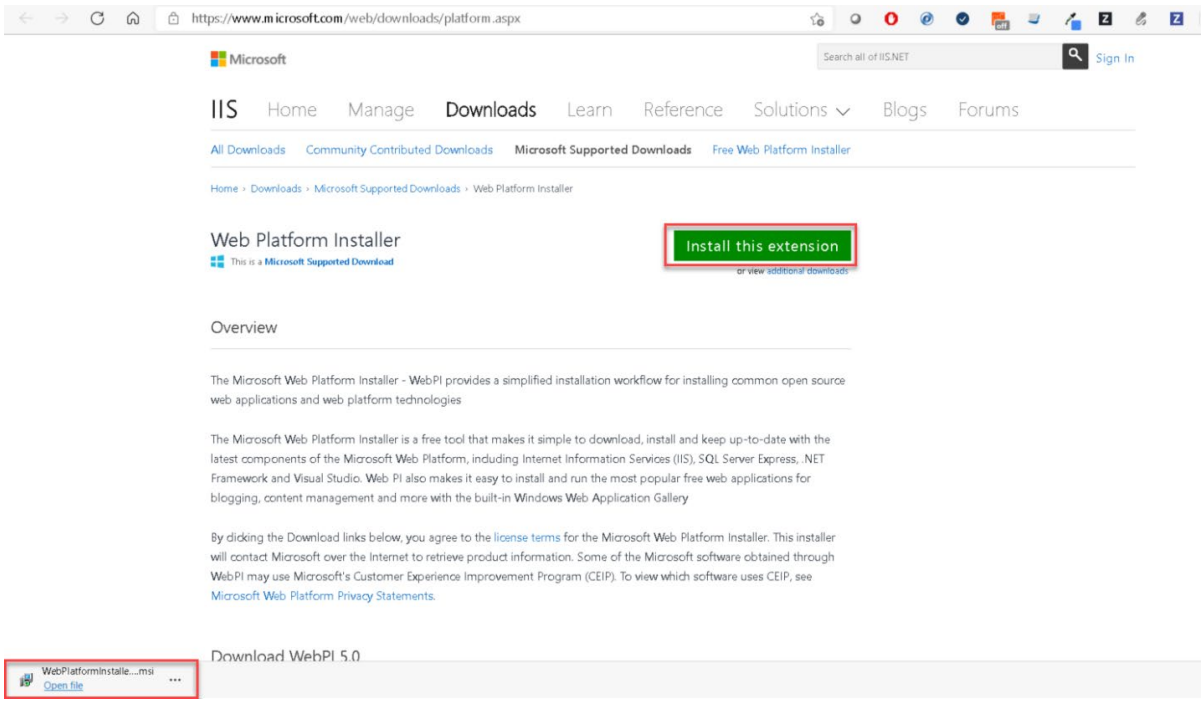
IIS provides the **URL Rewrite** extension that can be used to redirect HTTP traffic. The URL Rewrite module should be installed first.

1. In a browser, navigate to the Web Platform Installer on the Microsoft IIS site.

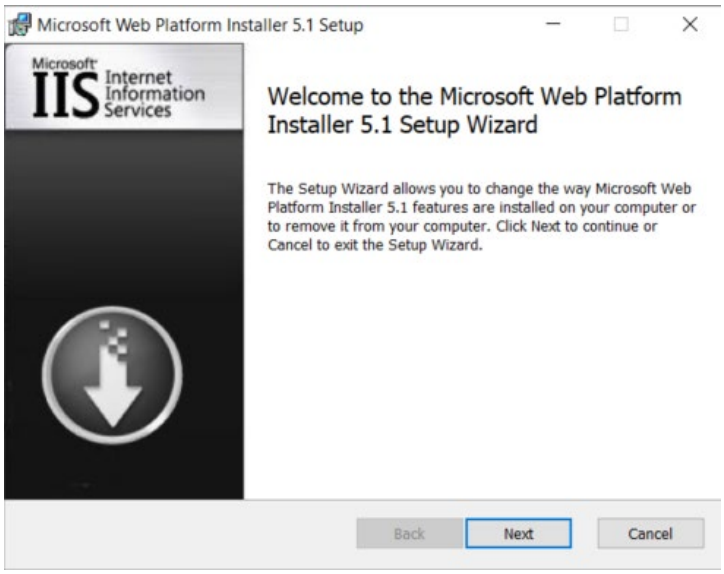
   Optionally, in **IIS Manager**, click **Get New Web Platform Components** to access the same webpage.



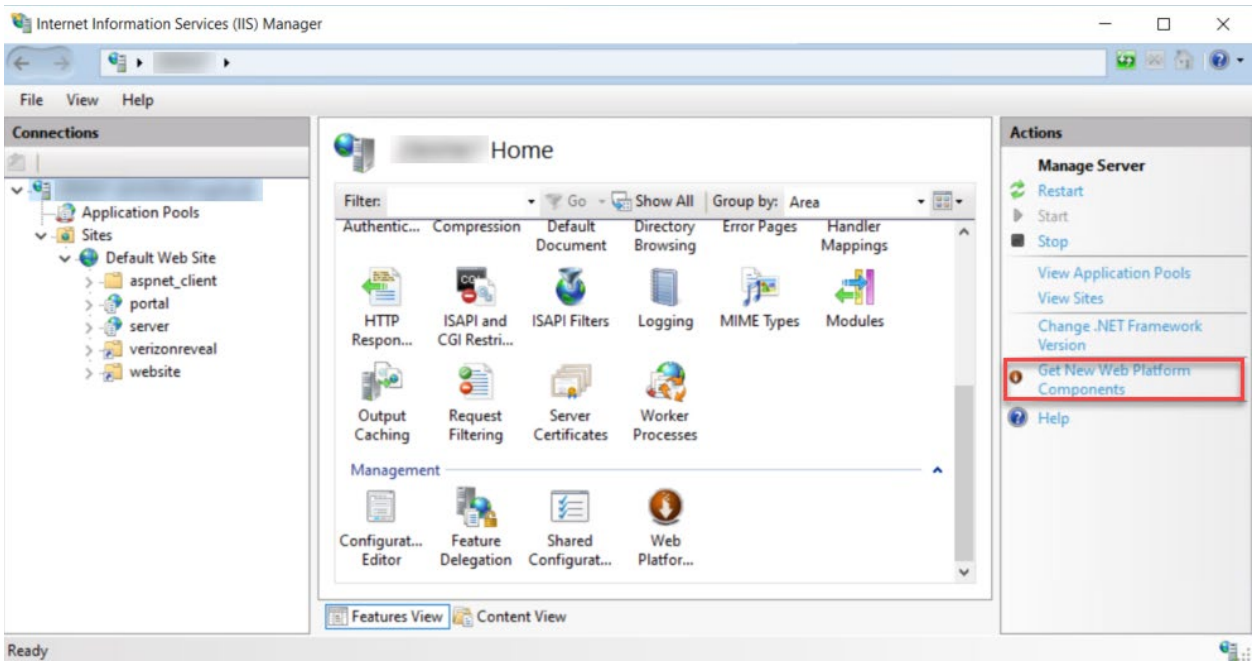
2. Click **Install this extension** to download the installer.



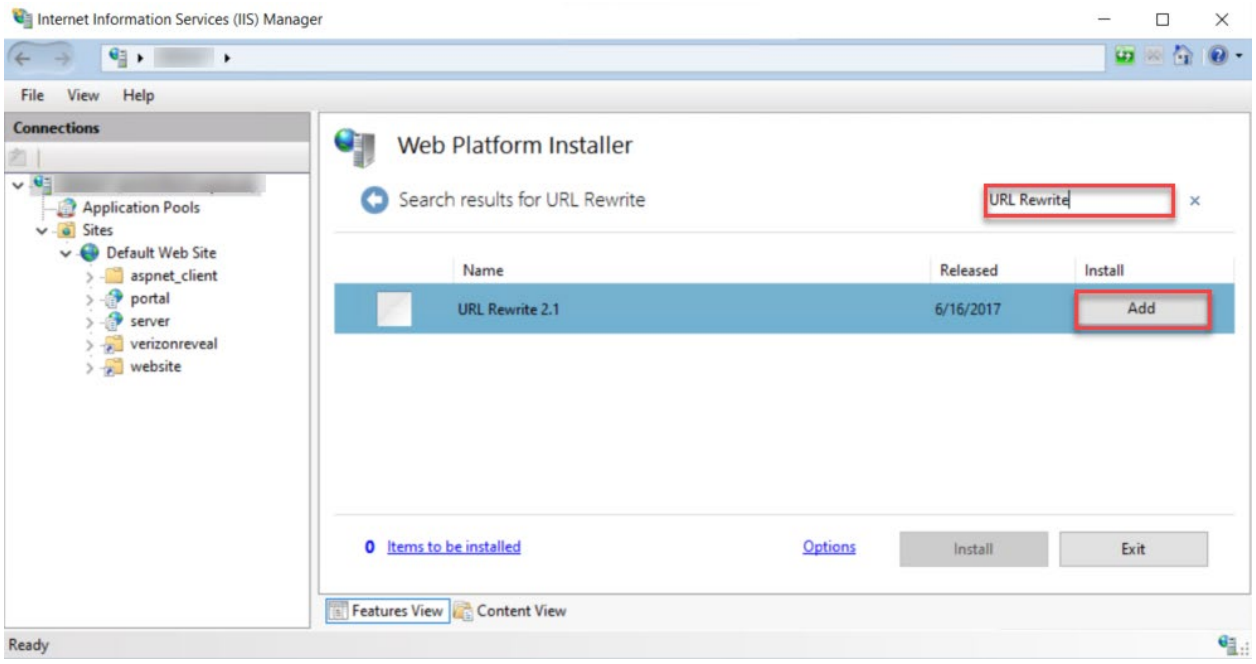
3. Open the **WebPlatformInstaller.msi** installer after it downloads.



4. After the installation completes, relaunch **IIS Manager** to refresh its content.
5. Select your machine, scroll to bottom of the middle panel, and double-click **Web Platform Installer**.

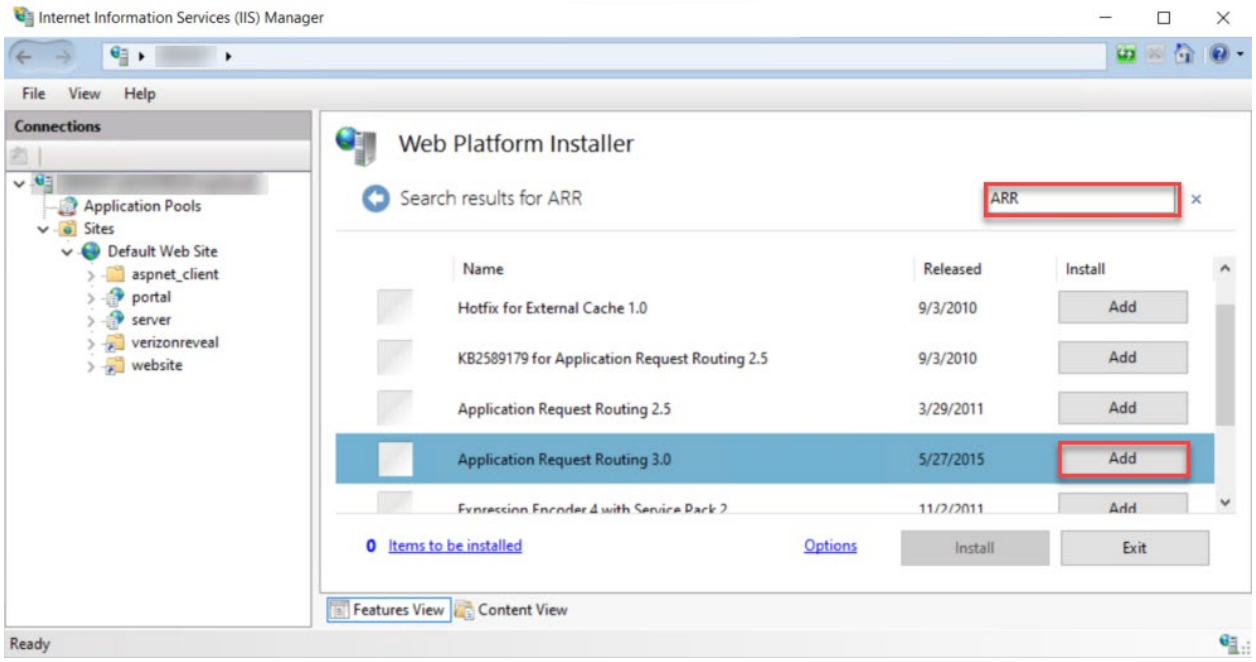


6. In the search box, search for **URL Rewrite**.
7. Click **Add** to add it to add **URL Rewrite 2.1** to the installation list.

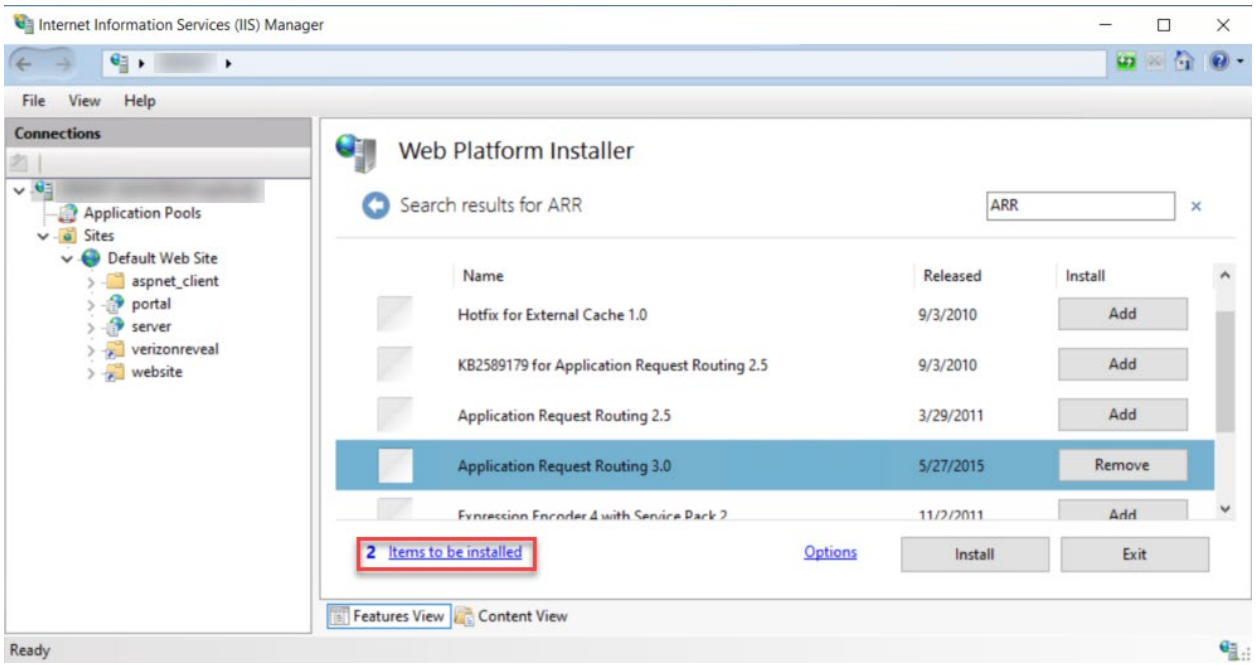


In addition to the **URL Rewrite** module, the **Application Request Routing** module also needs to be installed.

8. In the search box, search for **ARR** and click **Add** to add **Application Request Routing 3.0**.

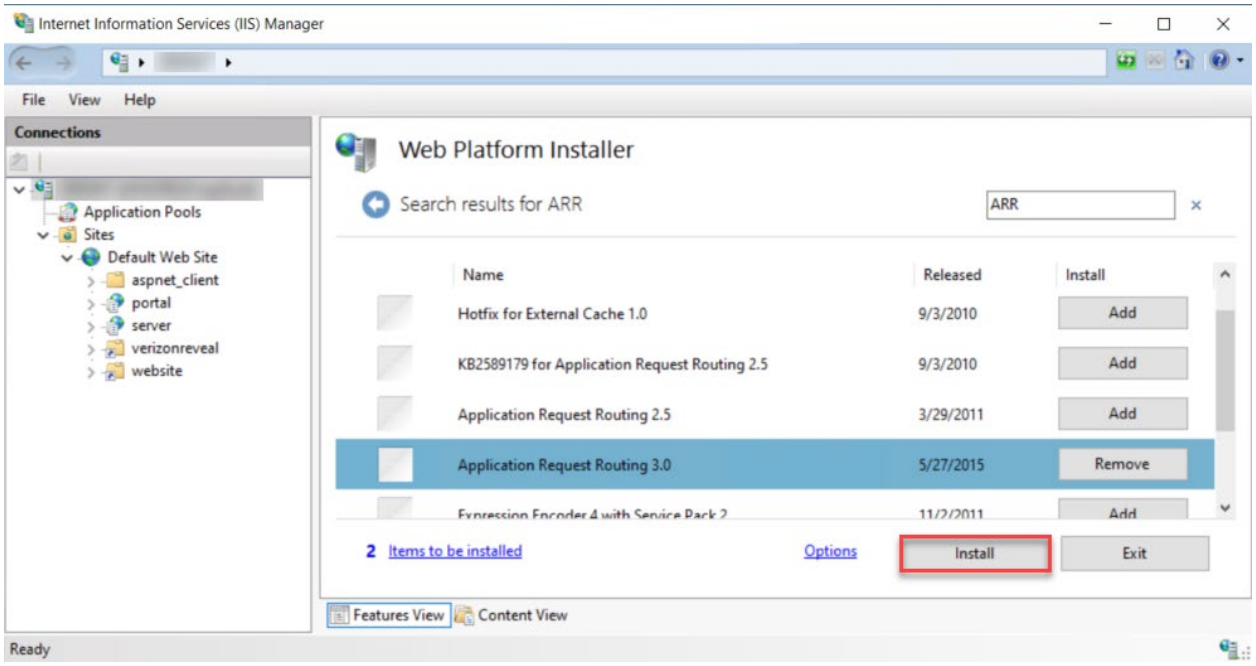


9. Click **2 Items to be installed** to show the items to install.

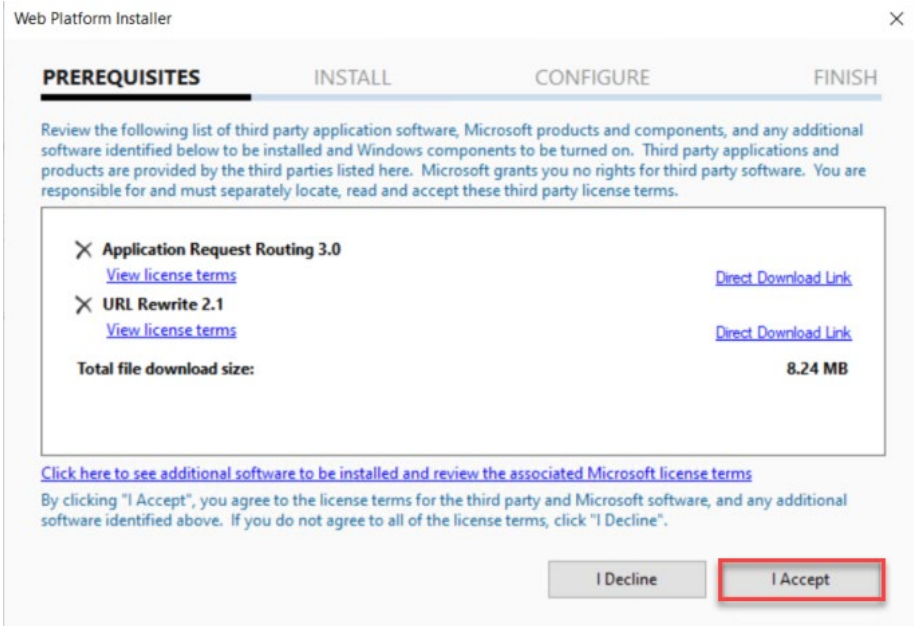


10. Verify **Application Request Routing 3.0** and **URL Rewrite 2.1** are listed.

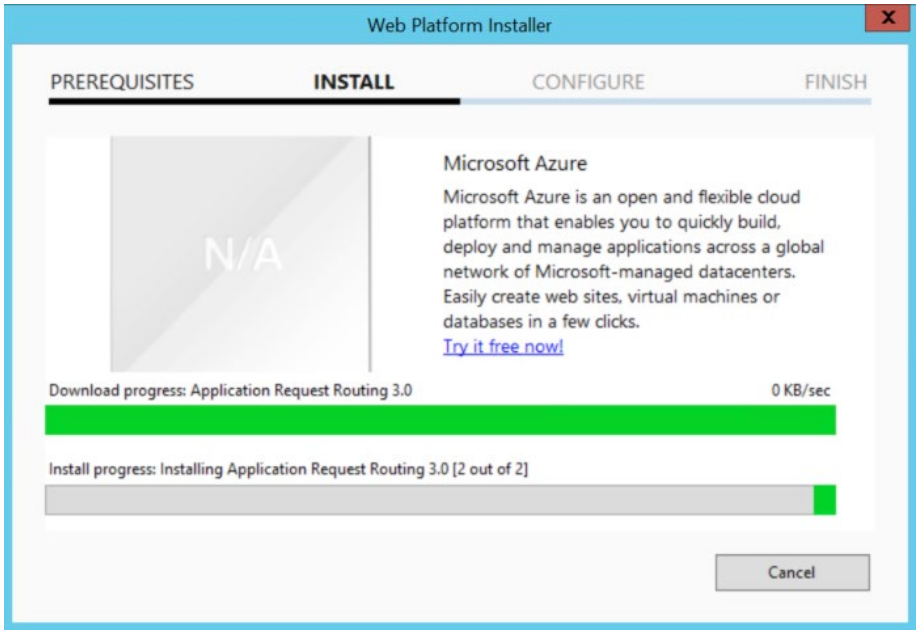
11. Click **Close** to dismiss the dialog.
12. Click **Install** to install the two items.



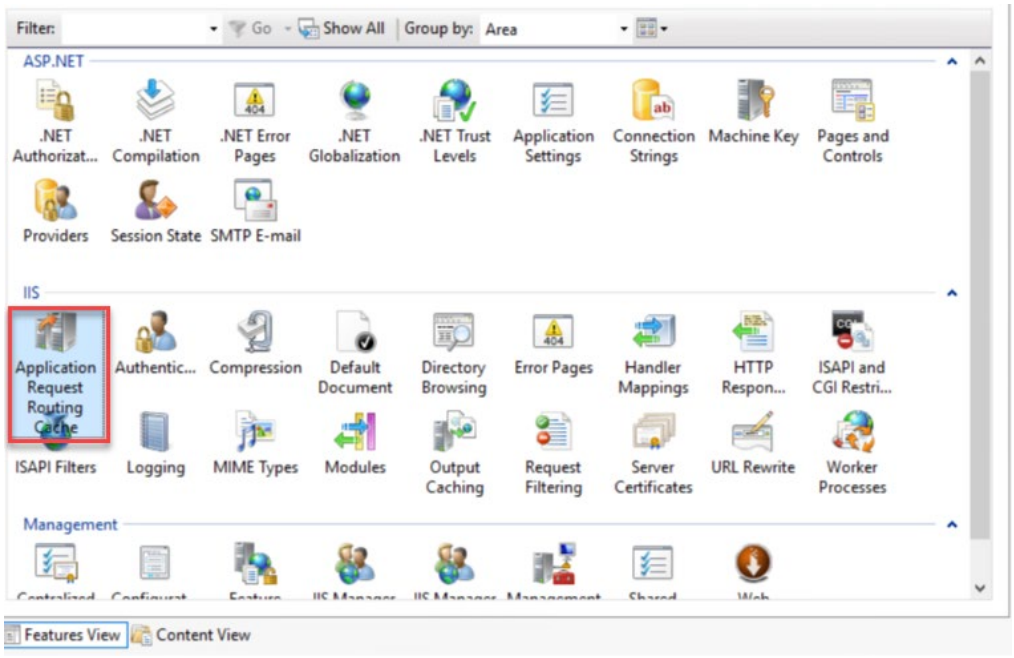
13. Click **I Accept** to continue with the installation.



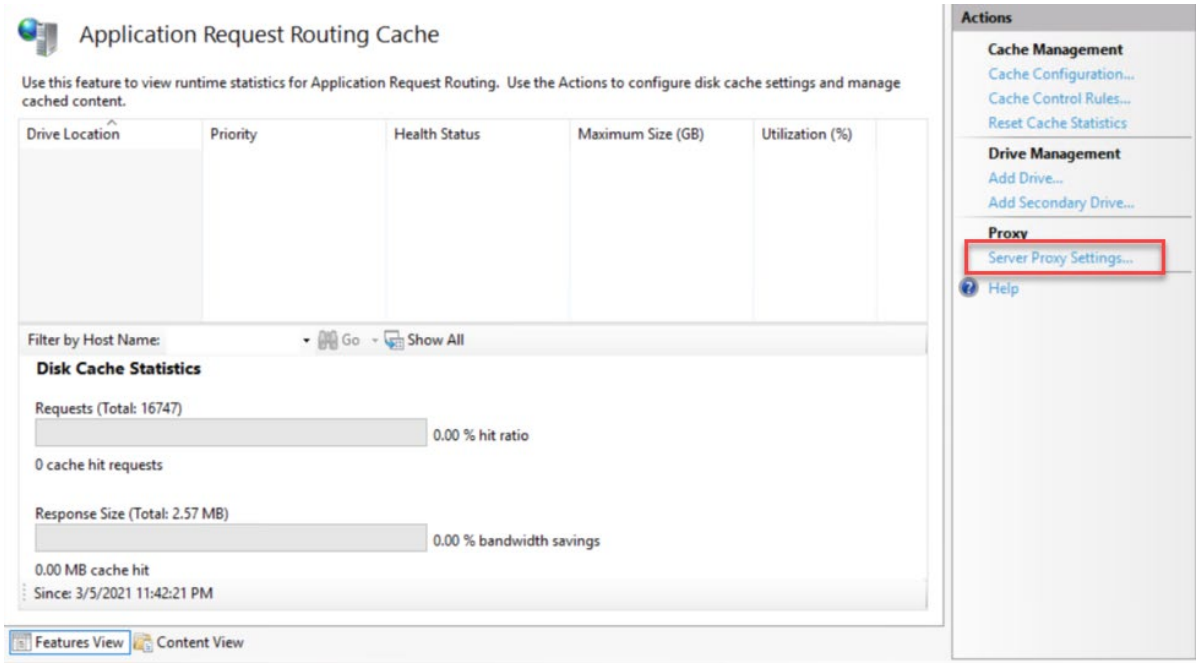
The two items will be installed.



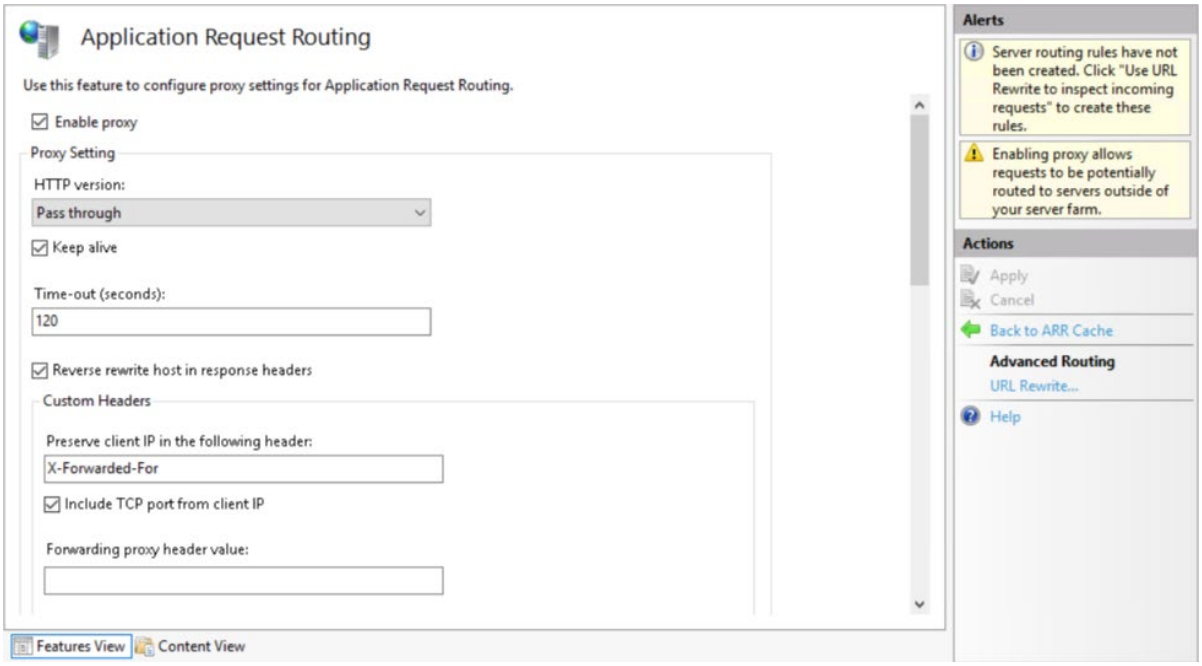
14. After the installation completes, relaunch **IIS Manager** to refresh its content.
15. In the IIS group, double-click **Application Request Routing Cache** to open it.

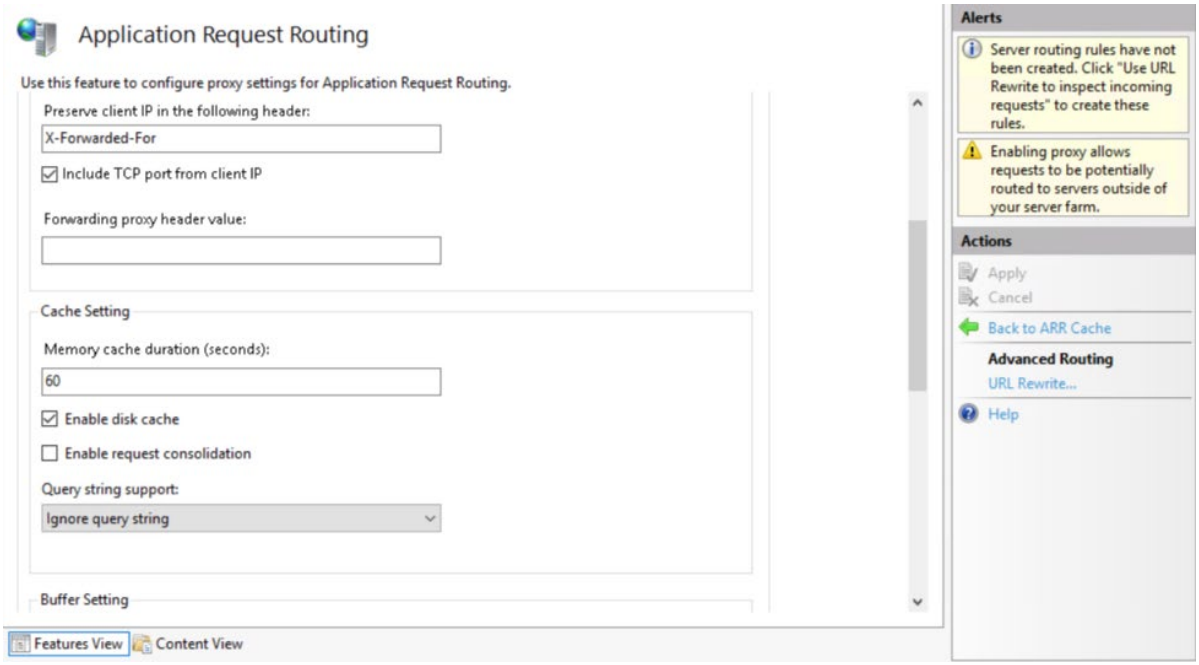


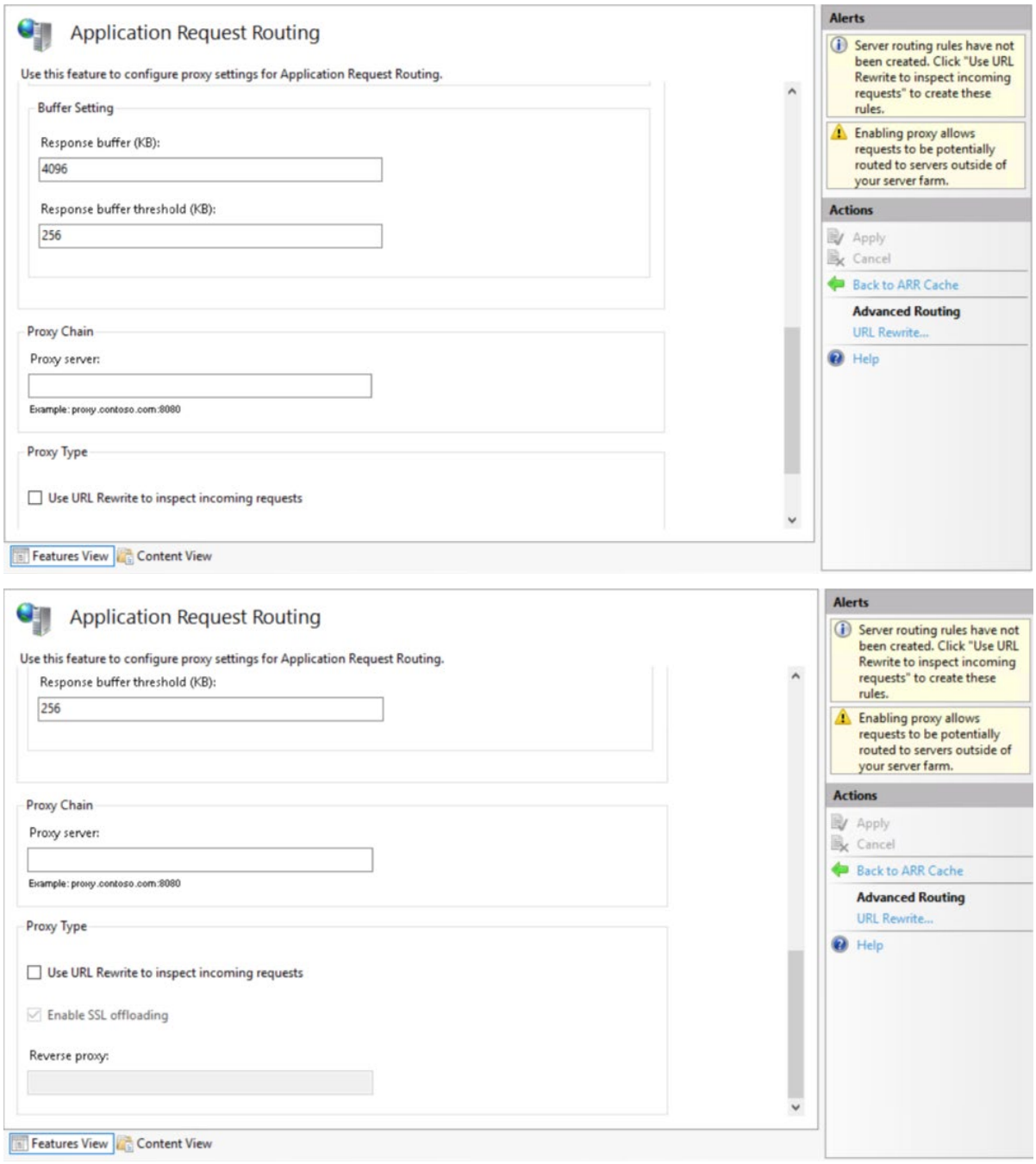
16. In the **Actions** panel, in the **Proxy** subgroup, click **Server Proxy Settings**.



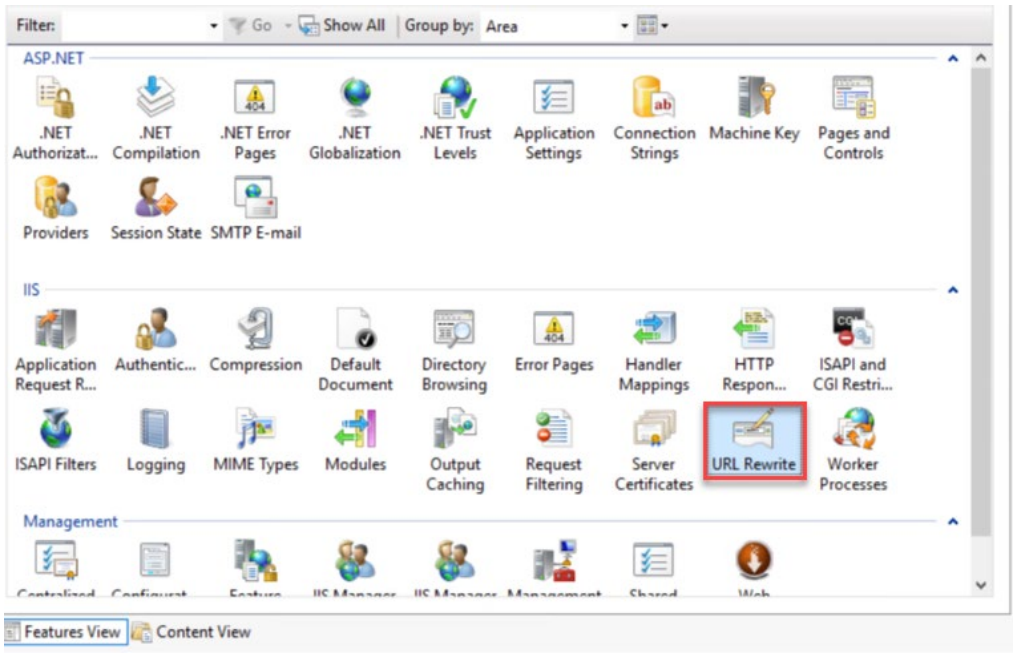
17. Review the **Application Request Routing** settings and ensure they match the illustrations below.


Application Request Routing
Use this feature to configure proxy settings for Application Request Routing.
Enable proxy
Proxy Setting
HTTP version:
Pass through
Keep alive
Time-out (seconds):
120
Reverse rewrite host in response headers
Custom Headers
Preserve client IP in the following header:
X-Forwarded-For
Include TCP port from client IP
Forwarding proxy header value:
Features View
Content View
Alerts
Server routing rules have not been created. Click "Use URL Rewrite to inspect incoming requests" to create these rules.
Enabling proxy allows requests to be potentially routed to servers outside of your server farm.
Actions
Apply
Cancel
Back to ARR Cache
Advanced Routing
URL Rewrite...
Help

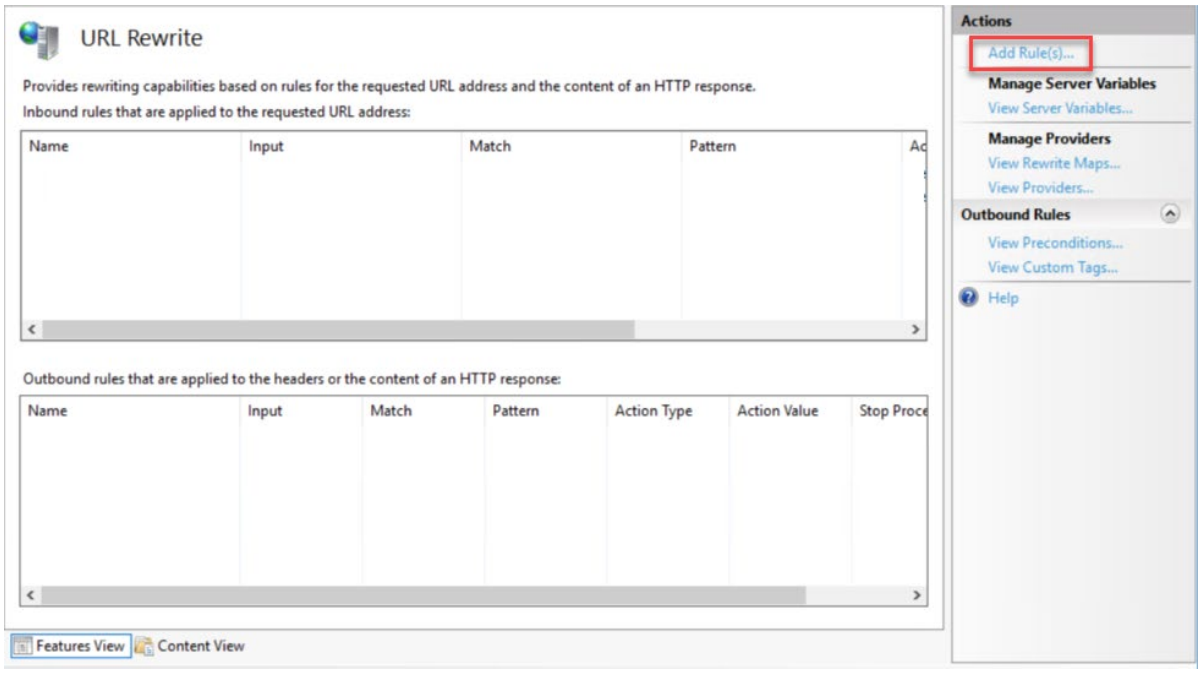

Application Request Routing
Use this feature to configure proxy settings for Application Request Routing.
Preserve client IP in the following header:
X-Forwarded-For
Include TCP port from client IP
Forwarding proxy header value:
Cache Setting
Memory cache duration (seconds):
60
Enable disk cache
Enable request consolidation
Query string support:
Ignore query string
Buffer Setting
Features View
Content View
Alerts
Server routing rules have not been created. Click "Use URL Rewrite to inspect incoming requests" to create these rules.
Enabling proxy allows requests to be potentially routed to servers outside of your server farm.
Actions
Apply
Cancel
Back to ARR Cache
Advanced Routing
URL Rewrite...
Help



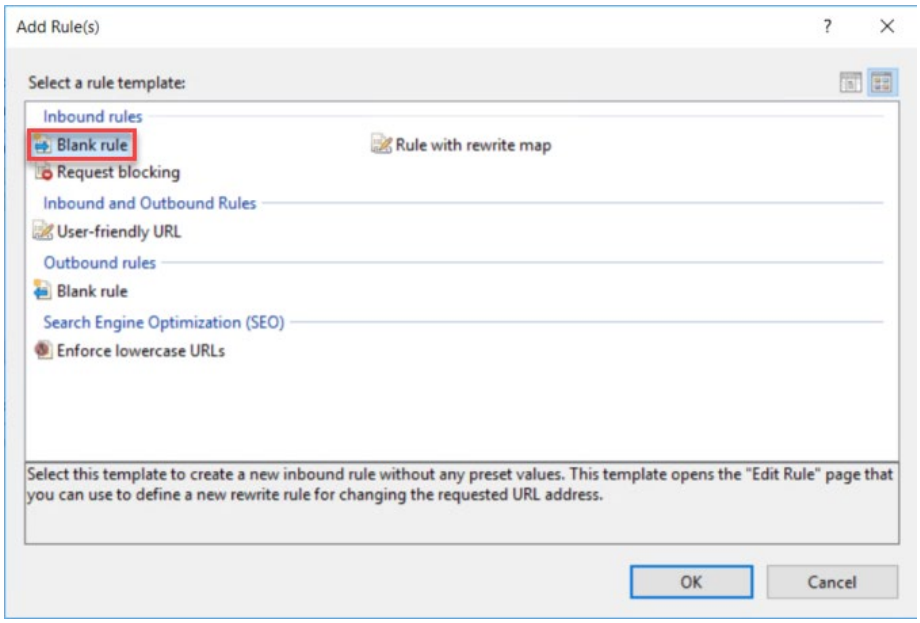
18. Navigate back to **Home** in **IIS Manager** by clicking the machine name in the tree view.
19. Double-click on the **URL Rewrite** to open it.



20. Click **Add Rule(s)** from the **Actions** panel.

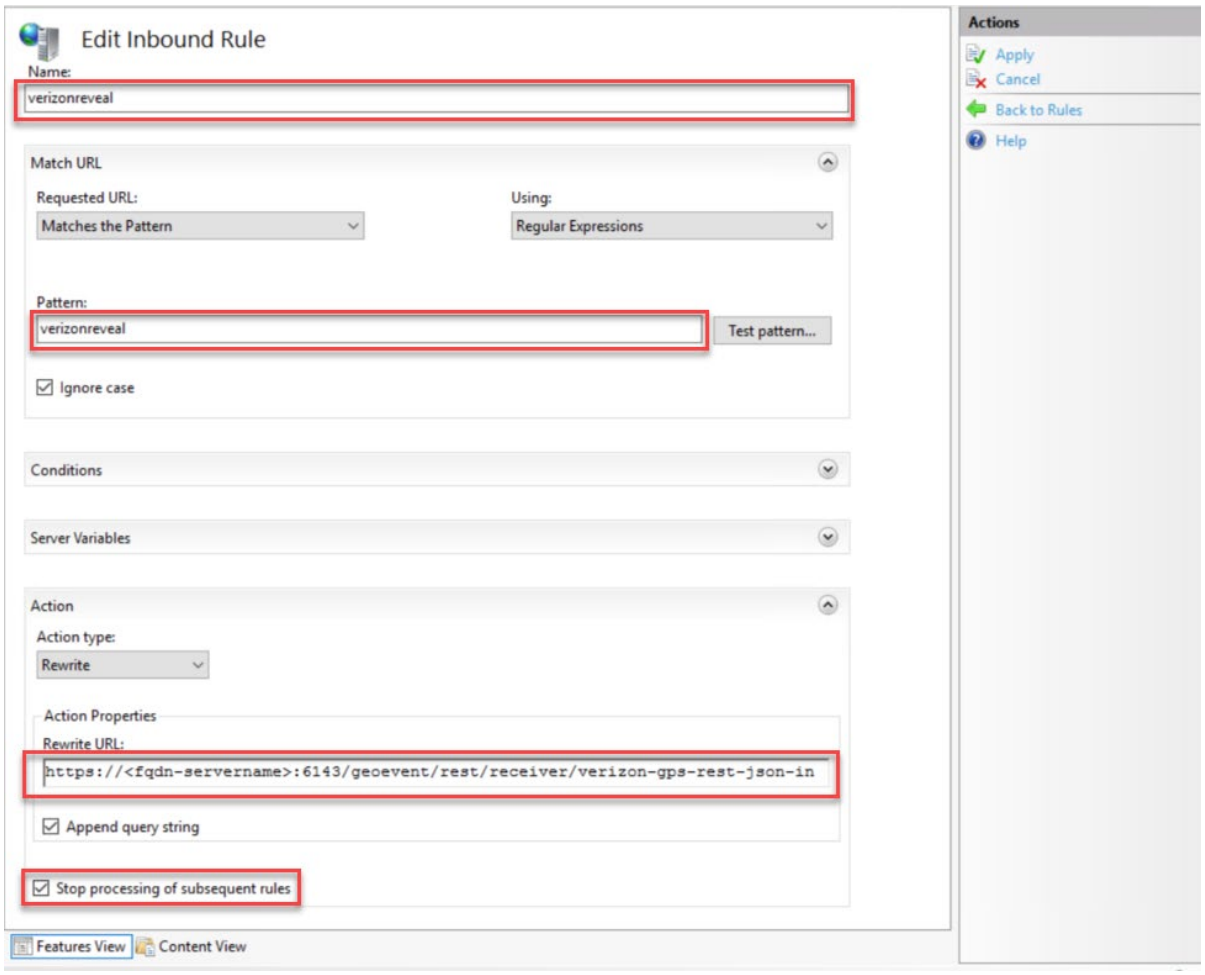


21. On the **Add Rule(s)** dialog, select **Blank rule** and click **OK**.



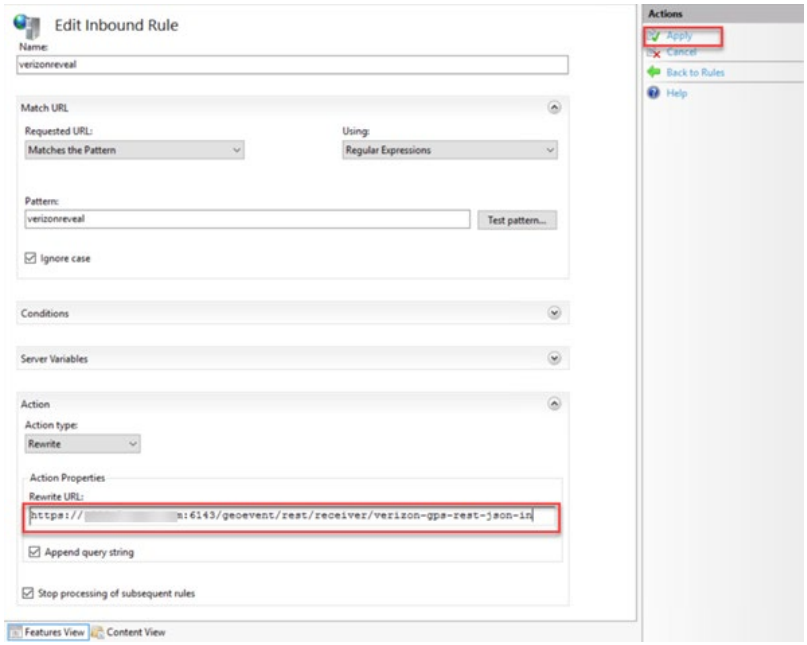
22. Enter the rule configuration as illustrated in the example below.

    NOTE: The **Rewrite URL** you enter should be the same URL as the GeoEvent Server input connector you created in the Configure a GeoEvent Server connector endpoint to receive data from Verizon Connect Reveal section above.

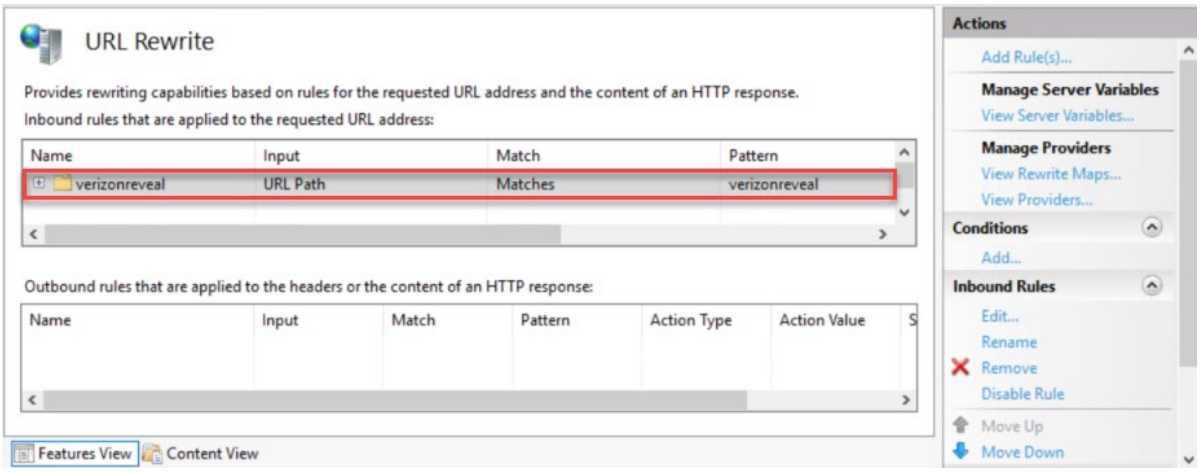


For this example, the **Rewrite URL** is

`https://<your_server>:6143/geoevent/rest/receiver/verizon-gps-rest-json-in`



23. Click **Apply** to create the rule.
24. Click **Back to Rules** to navigate back, the newly created rule will be listed.



With everything configured, GeoEvent Server is now ready to receive data from the Verizon Connect Reveal server.

Configure GeoEvent Server to process the Verizon Connect Reveal data

The Verizon Connect Reveal GPS Push Service data contains sub-hierarchies in its data structure. This data is not easily translated to a feature schema that can be used in ArcGIS applications. So, in this case, the GPS Push Service data needs to be mapped to a flattened schema first. You can accomplish this using the real-time processing capabilities of GeoEvent Server.

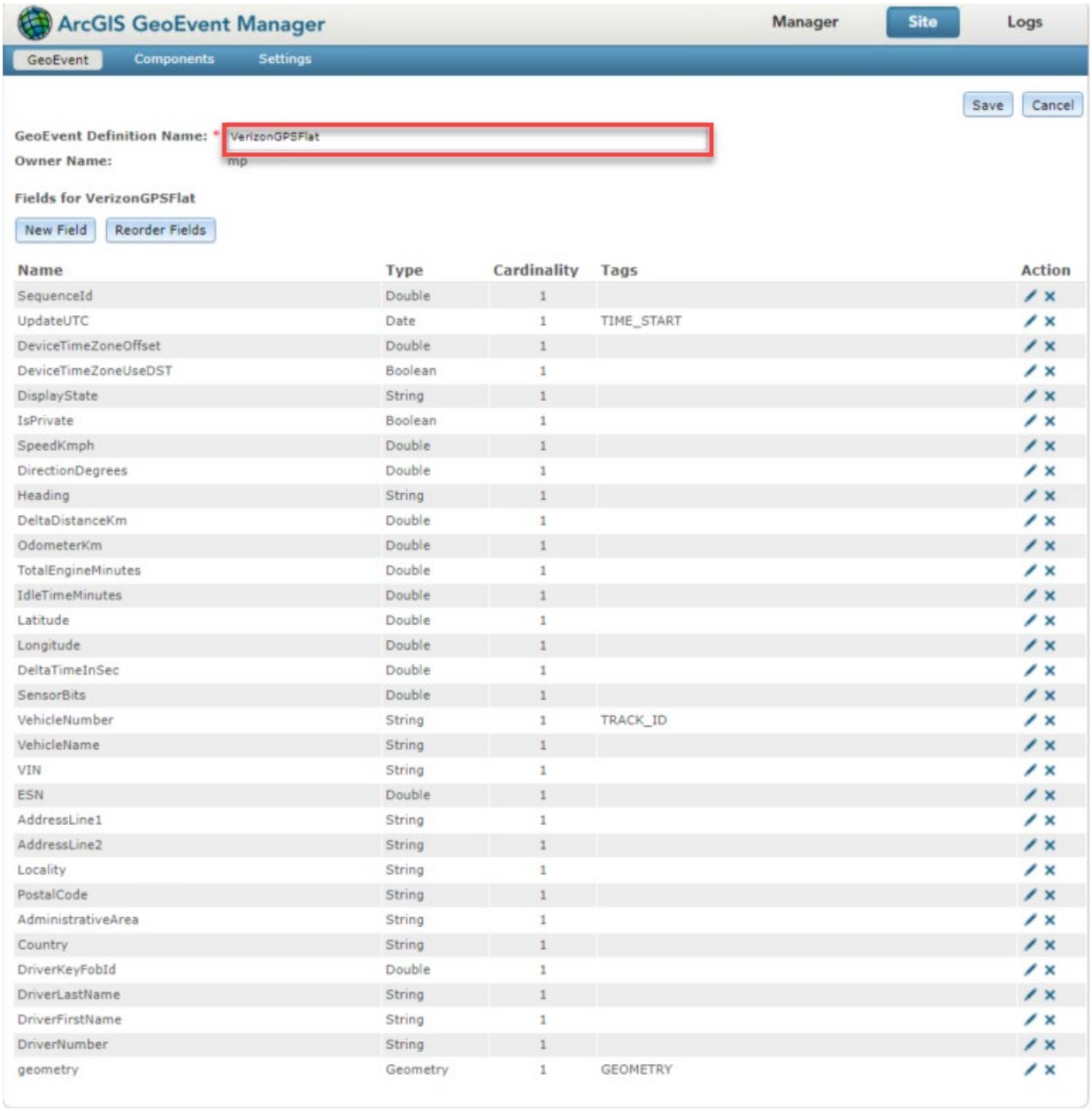
Below is the hierarchical data directly from the GPS Push Service:

Fields for VerizonGPS

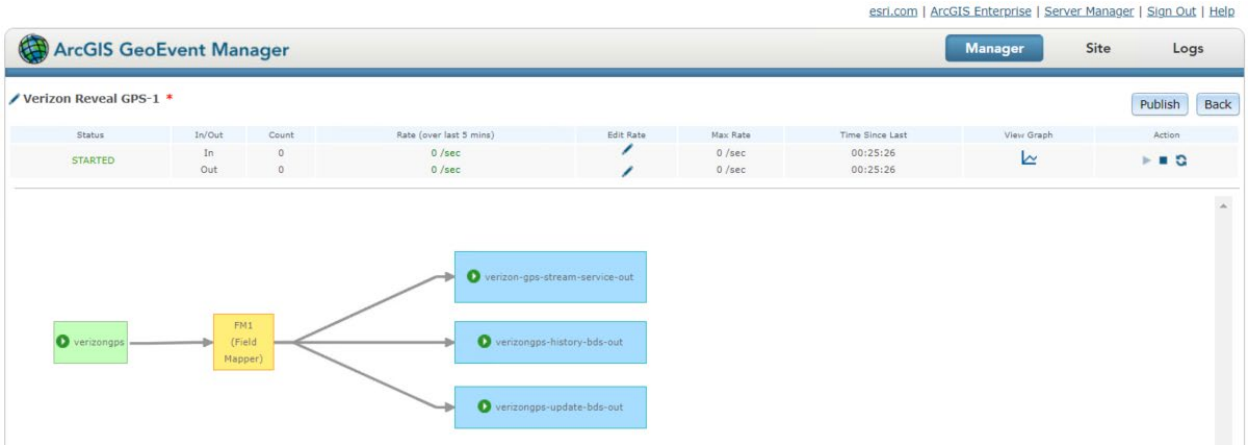
New Field | Reorder Fields

Name	Type	Cardinality	Tags	Action
SequenceId	Double	1		
UpdateUTC	Date	1	TIME_START	
DeviceTimeZoneOffset	Double	1		
DeviceTimeZoneUseDST	Boolean	1		
DisplayState	String	1		
IsPrivate	Boolean	1		
SpeedKmph	Double	1		
DirectionDegrees	Double	1		
Heading	String	1		
DeltaDistanceKm	Double	1		
OdometerKm	Double	1		
TotalEngineMinutes	Double	1		
IdleTimeMinutes	Double	1		
Latitude	Double	1		
Longitude	Double	1		
DeltaTimeInSec	Double	1		
SensorBits	Double	1		
geometry	Geometry	1	GEOMETRY	
f	String	1		
token	String	1		
SensorValues	String	1		
Vehicle	Group	1		
Number	String	1		
Name	String	1		
VIN	String	1		
ESN	Double	1		
Address	Group	1		
AddressLine1	String	1		
AddressLine2	String	1		
Locality	String	1		
PostalCode	String	1		
AdministrativeArea	String	1		
Country	String	1		
Driver	Group	1		
DriverKeyFobId	Double	1		
DriverLastName	String	1		
DriverFirstName	String	1		
DriverNumber	String	1		

And here is the flattened schema required by ArcGIS applications:



The steps for flattening the data structure will not be outlined in this blog. The Field Mapper Processor illustrated in the yellow box below) should be used to map the GPS Push Service data from the original hierarchical schema to the flattened schema. Additional guidance on the real-time processing workflows of GeoEvent Services can be found in the GeoEvent Server tutorials.



Processor Properties

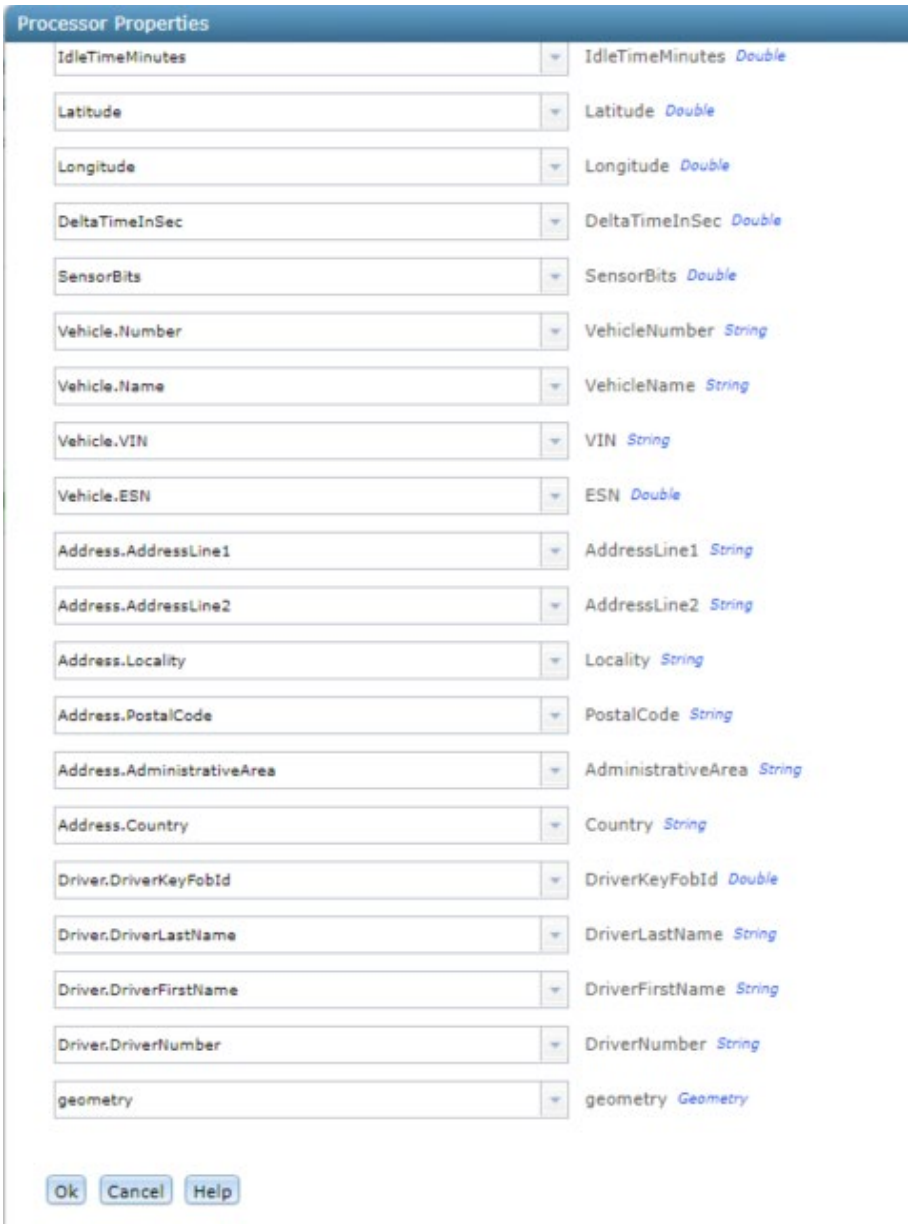
Name:* FM1

Processor: Field Mapper

Source GeoEvent Definition*: VerizonGPS

Target GeoEvent Definition*: VerizonGPSFlat

Source Fields	Target Fields
SequenceId	SequenceId *Double*
UpdateUTC	UpdateUTC *Date*
DeviceTimeZoneOffset	DeviceTimeZoneOffset *Double*
DeviceTimeZoneUseDST	DeviceTimeZoneUseDST *Boolean*
DisplayState	DisplayState *String*
IsPrivate	IsPrivate *Boolean*
SpeedKmph	SpeedKmph *Double*
DirectionDegrees	DirectionDegrees *Double*
Heading	Heading *String*
DeltaDistanceKm	DeltaDistanceKm *Double*
OdometerKm	OdometerKm *Double*
TotalEngineMinutes	TotalEngineMinutes *Double*
IdleTimeMinutes	IdleTimeMinutes *Double*
Latitude	Latitude *Double*
Longitude	Longitude *Double*
DeltaTimeInSec	DeltaTimeInSec *Double*
SensorBits	SensorBits *Double*
Vehicle.Number	VehicleNumber *String*



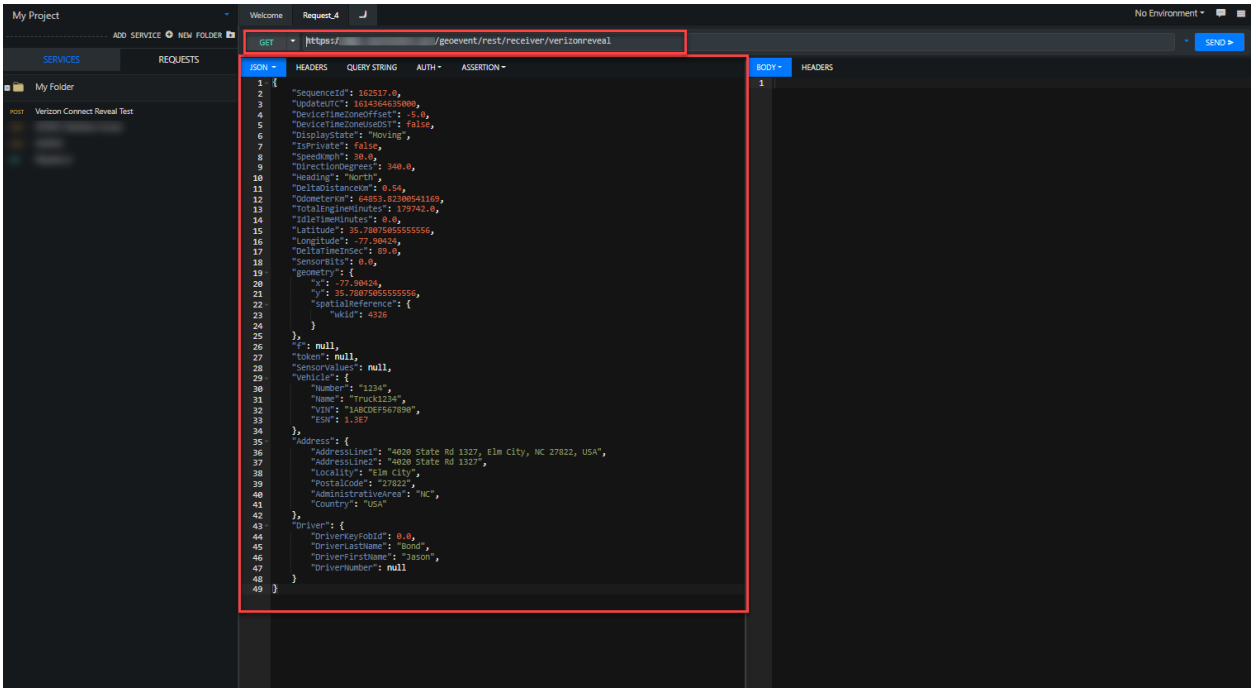
Test the Verizon Connect Reveal data feed

Prior to requesting Verizon Connect Reveal start sending data to the IIS endpoint, additional tests should be conducted first. Apps such as *Boomerang* can be used to post the data to the IIS URL for testing.

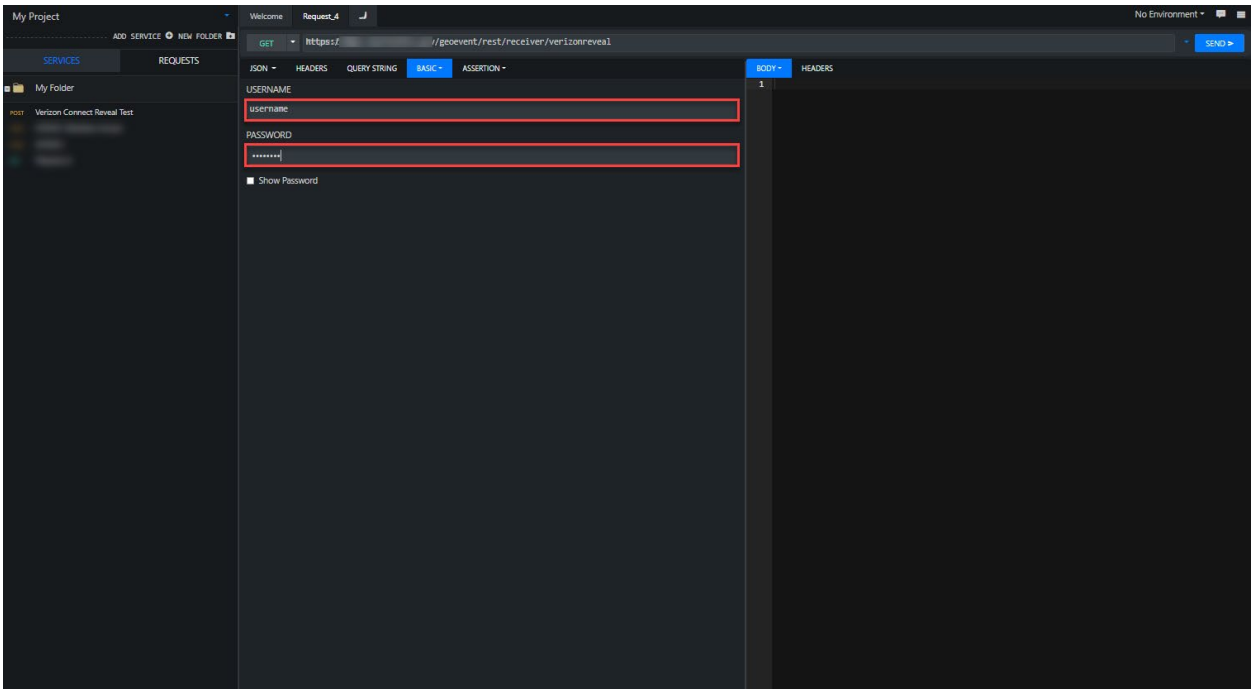
1. Open a browser and navigate to **Boomerang**.
2. Click **Quick Request**.
3. Change **GET** to **POST**.
4. Enter the IIS URL (in this example, https://<your_server>/verizonreveal/).
5. Copy the sample JSON data below and paste into JSON body panel.

```
{
	"SequenceId": 162517.0,
	"UpdateUTC": 1614364635000,
	"DeviceTimeZoneOffset": -5.0,
	"DeviceTimeZoneUseDST": false,
	"DisplayState": "Moving",
	"IsPrivate": false,
	"SpeedKmph": 30.0,
	"DirectionDegrees": 340.0,
	"Heading": "North",
	"DeltaDistanceKm": 0.54,
	"OdometerKm": 64853.82300541169,
	"TotalEngineMinutes": 179742.0,
	"IdleTimeMinutes": 0.0,
	"Latitude": 35.78075055555556,
	"Longitude": -77.90424,
	"DeltaTimeInSec": 89.0,
	"SensorBits": 0.0,
	"geometry": {
		"x": -77.90424,
		"y": 35.78075055555556,
		"spatialReference": {
			"wkid": 4326
		}
	},
	"f": null,
	"token": null,
	"SensorValues": null,
	"Vehicle": {
		"Number": "1234",
		"Name": "Truck1234",
		"VIN": "1ABCDEF567890",
		"ESN": 1.3E7
	},
	"Address": {
```

```
            "AddressLine1": "4020 State Rd 1327, Elm City, NC 27822, USA",
            "AddressLine2": "4020 State Rd 1327",
            "Locality": "Elm City",
            "PostalCode": "27822",
            "AdministrativeArea": "NC",
            "Country": "USA"
        },
        "Driver": {
            "DriverKeyFobId": 0.0,
            "DriverLastName": "Bond",
            "DriverFirstName": "Jason",
            "DriverNumber": null
        }
    }
```

6. Click the **AUTH** tab and click the **BASIC** auth type.
7. Enter the **USERNAME** and **PASSWORD** for the **Verizonconnect** user you created earlier.



8. Click **SEND**.

   Boomerang displays a 

response code if the transmission is successful. In GeoEvent Manager, the Verizon Connect Reveal input's count will also increase once the data is received.

Upon successfully testing the data stream, GeoEvent Server is now ready to receive data from the Verizon Connect Reveal server. The IIS URL and the basic authentication information should be communicated to Verizon Connect Reveal. It is also recommended you encrypt the traffic using an HTTPS URL to avoid exposing the basic authentication information in the HTTP header. Since the HTTP traffic is being sent over a public network, it is also recommended you obtain a CA-signed certificate for your server from a trusted certificate provider (e.g., Verisign, DigiCert, etc.) and apply it to your server.