# How to modify listening ports of D-View 7

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Author | Description |
| *1.0* | *2017/6/20* | *Liu Li* | *First release* |

Content

[How to modify listening ports of D-View 7 1](#_Toc486955089)

[Abstract 3](#_Toc486955090)

[1. Modify the D-View 7 Web access port on IIS 3](#_Toc486955091)

[1.1 D-View 7 basic access configuration 3](#_Toc486955092)

[1.2 D-View 7 http access configuration 5](#_Toc486955093)

[1.3 D-View 7 https access configuration 6](#_Toc486955094)

[2. Modify the D-View 7 Core Server Listening Port 11](#_Toc486955095)

[2.1 Configuration file path 11](#_Toc486955096)

[2.2 Listening port nodes: https\_port, http\_port 12](#_Toc486955097)

[2.3 Running rules about “https\_port”, “http\_port” nodes 12](#_Toc486955098)

[2.4 Make the configuration effective immediately 12](#_Toc486955099)

[3. Configure the Firewall 13](#_Toc486955100)

[3.1 The Windows OS Firewall on Core Server 13](#_Toc486955101)

[3.2 Hardware Firewall 16](#_Toc486955102)

[4. Configure Probe 16](#_Toc486955103)

[4.1 Local Probe 16](#_Toc486955104)

[4.2 Install a remote Probe 17](#_Toc486955105)

[4.3 Remote Probe Settings 19](#_Toc486955106)

[Notes: 19](#_Toc486955107)

## Abstract

In current version of D-View 7, it will listen to 80/443 port at the runtime and the port cannot be modified by us. There is a potential problem: If another program needs to listen 80/443 port at the same time, then D-View 7 and this program can’t run at the same time. Therefore, D-View 7 has improved so that it can listen to the customized port number.

This document mainly described how to modified the related settings to let D-View 7 can work properly with customized port.

**Key work**: **Default Port,** **Modify Port.**

## Modify the D-View 7 Web access port on IIS

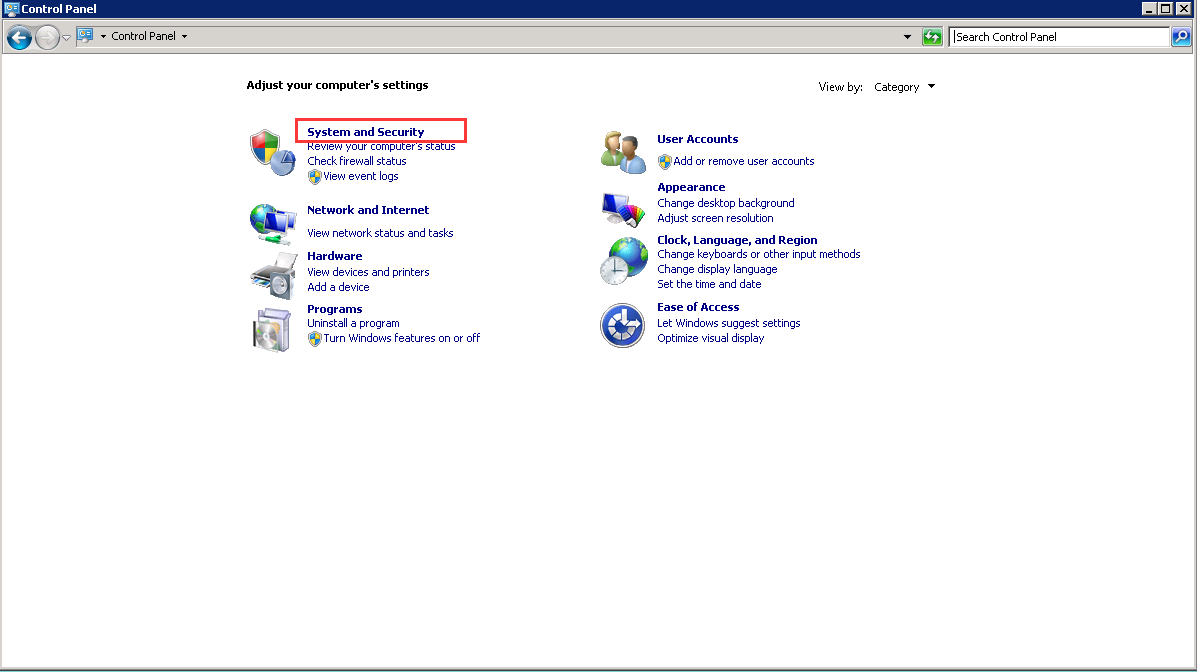
After the modification, we can access D-View 7 with customized port number. Moreover, we can also access the D-View 7 Web with http or https.

On IIS, if we want to access with http and customized port, we need to modified the “Default Web Site” binding port.

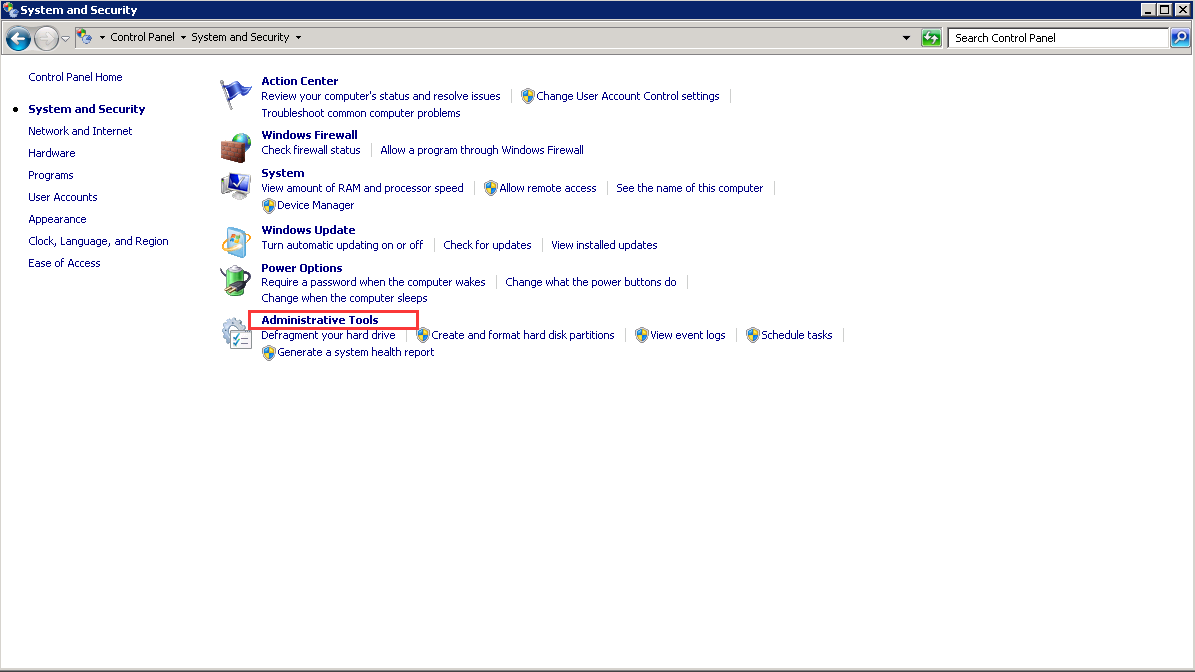
If we want to use the https and customized port to access D-View 7, we need to do more configuration such as install a certificate, modify the site binding port, set URL rewrite rules and so on.

### D-View 7 basic access configuration

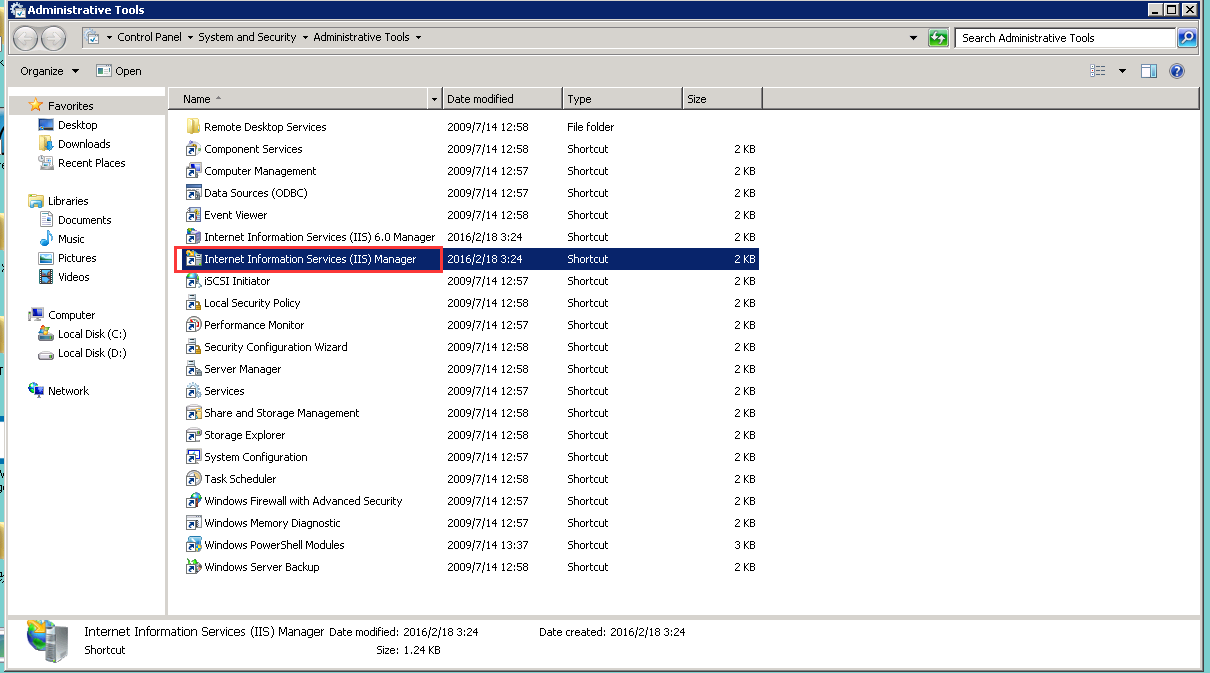
Open the control panel, click “System and Security”.



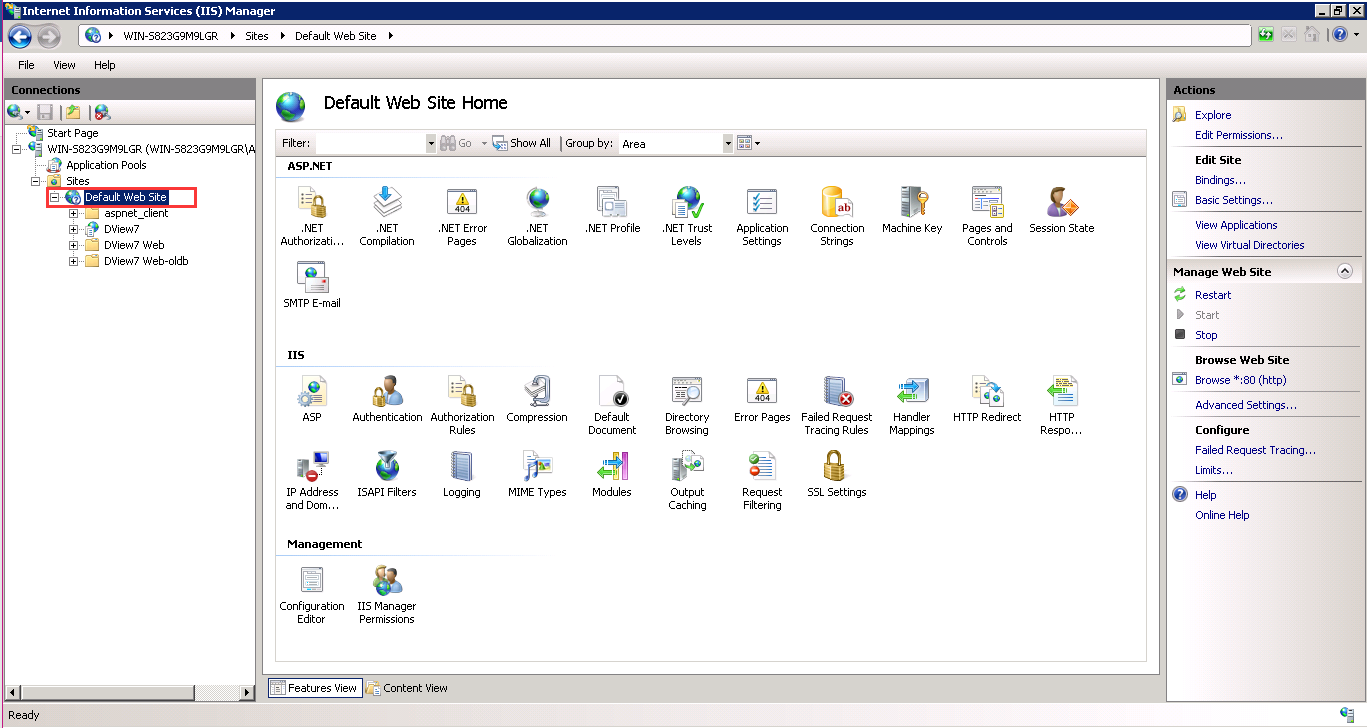
Click “Administrative Tools”.

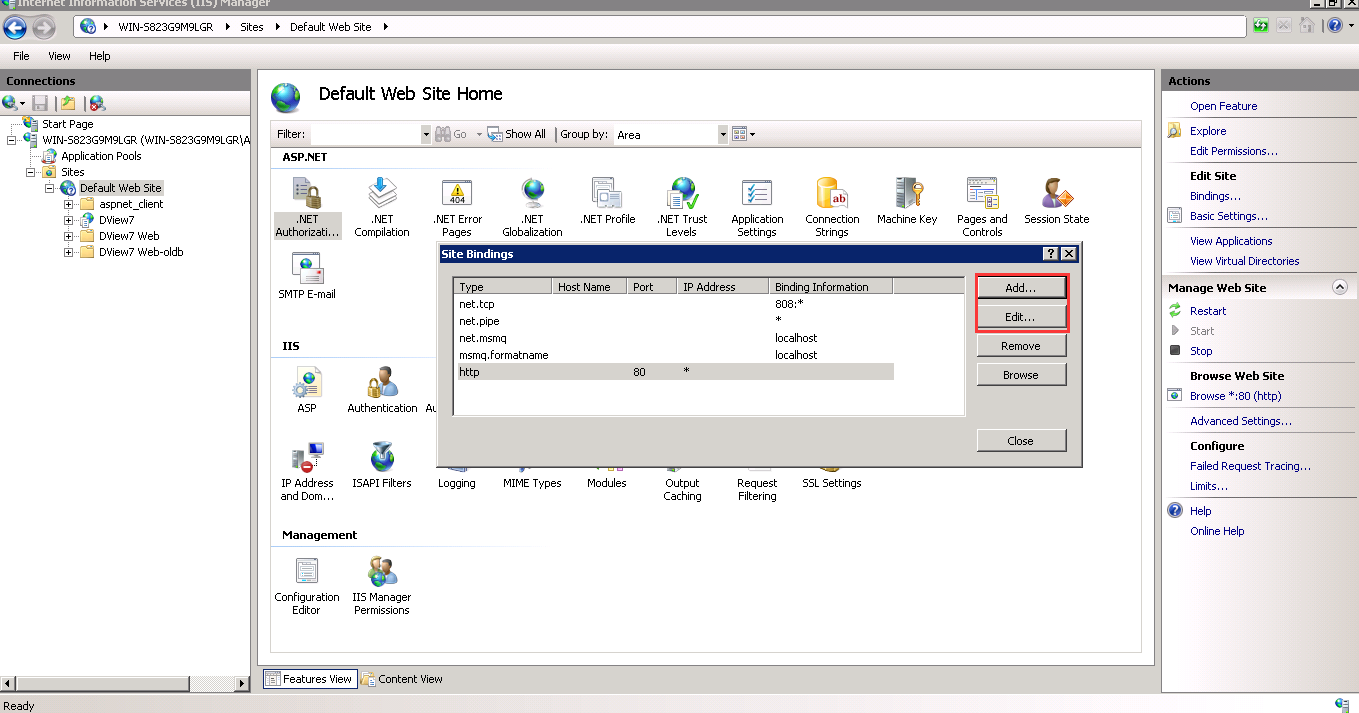


Open IIS Manager.



Right-click “Default Web Site” and select “Edit Bindings”.

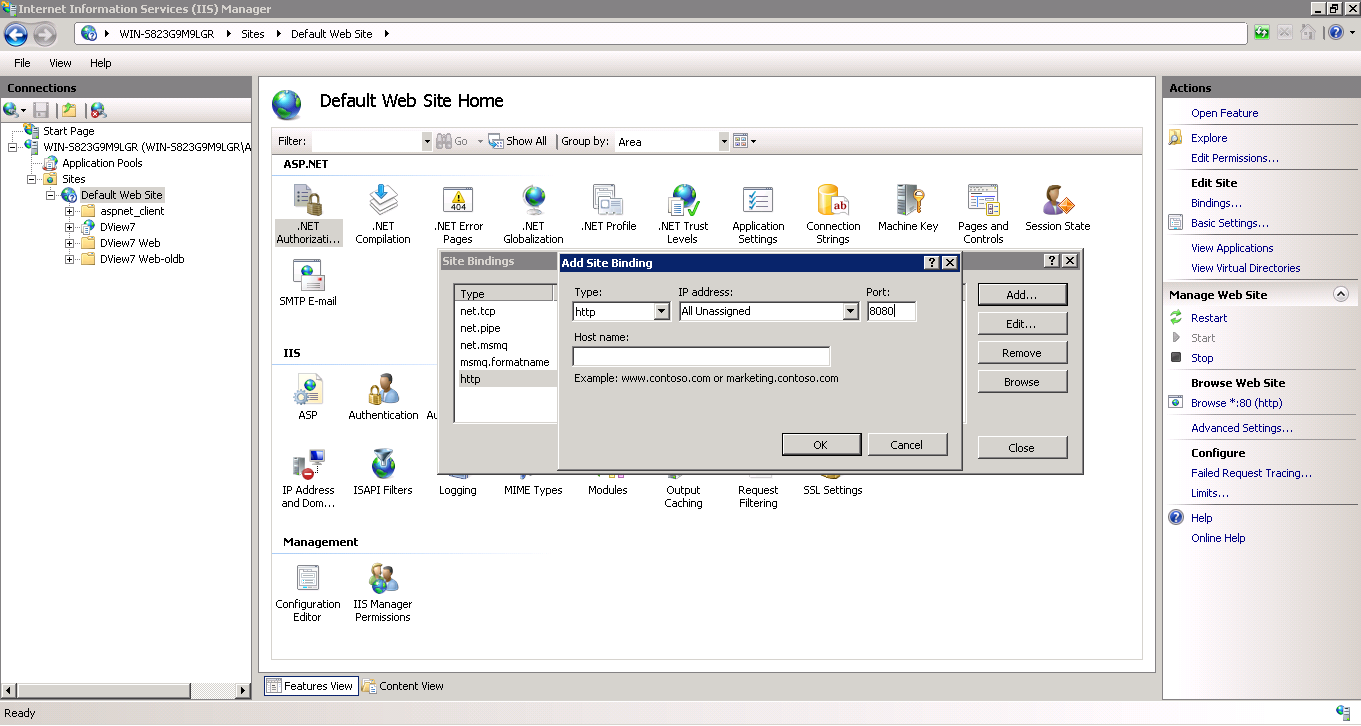
****

****

### D-View 7 http access configuration

Input the required port(e.g.:8080). After setting up, click the “OK” button to save.

Now, we can access D-View 7 by http.

****

### D-View 7 https access configuration

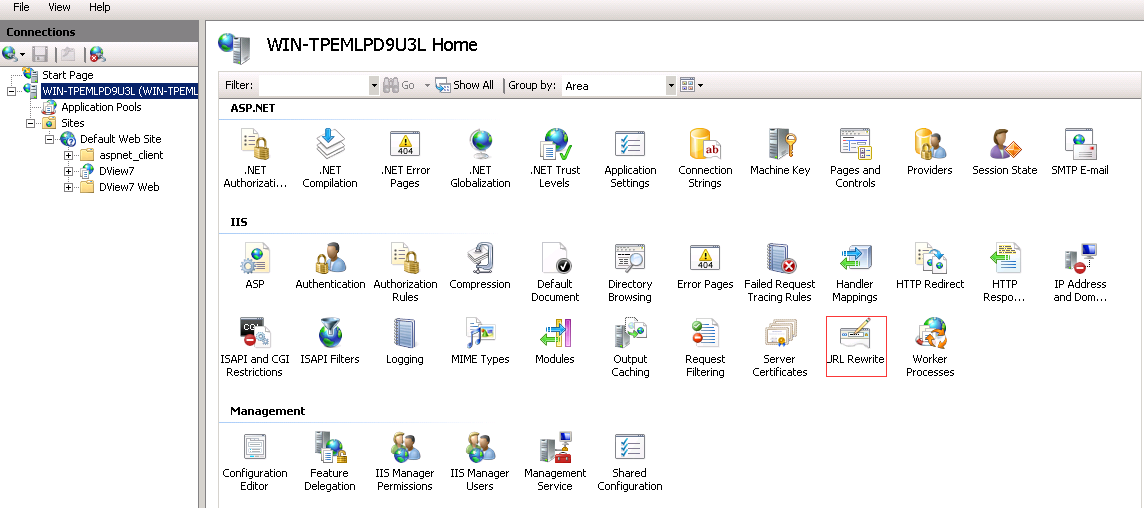
If we use https to access DV7, we need to install a certificate first. We can request a certificate from the web, or import an existing certificate by IIS. There, we use Self-Signed Certificate, take IIS 7 for example.

#### Download and install URL Rewrite:

First, we should download “Microsoft URL Rewrite Module 2.0 for IIS 7(x64)” from this link:

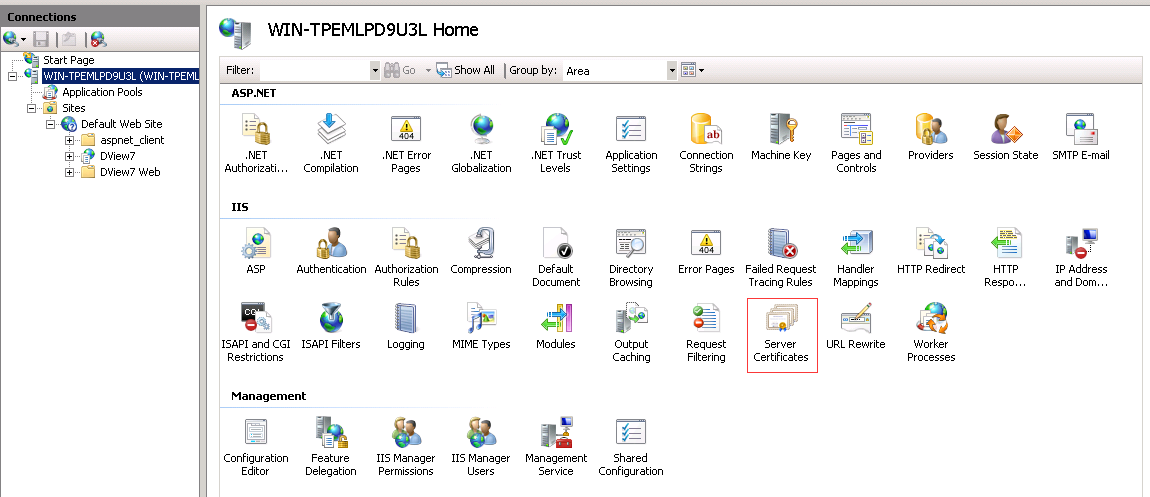
https://www.microsoft.com/en-US/download/details.aspx?id=7435

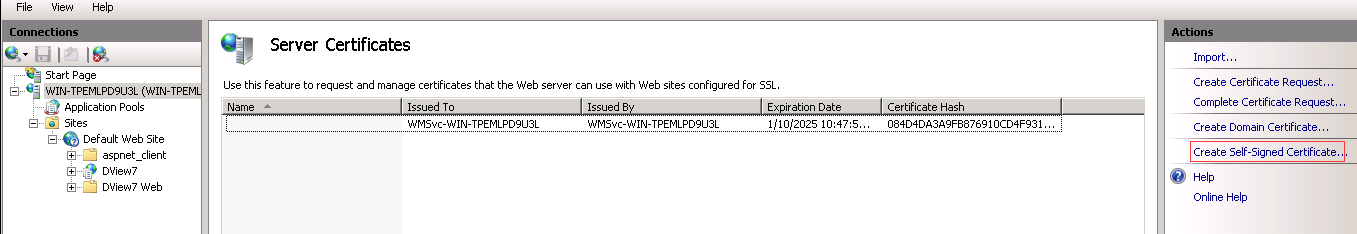
The download file name like “rewrite\_2.0\_rtw\_x64.msi”, directly double click to run. After install and restart IIS, we can see “URL Rewrite” added.



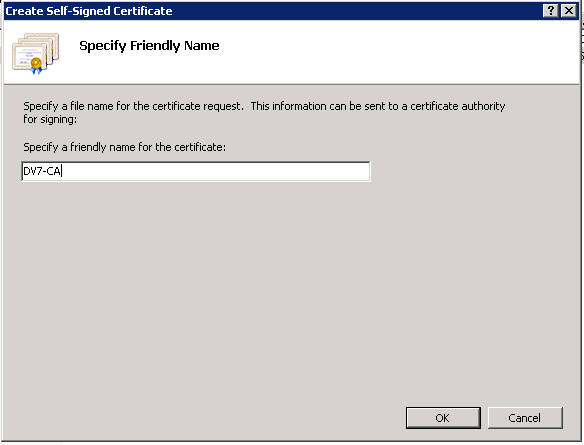
#### Install server certificate:

Double click “Server Certificates” to enter the Server Certificates set page.

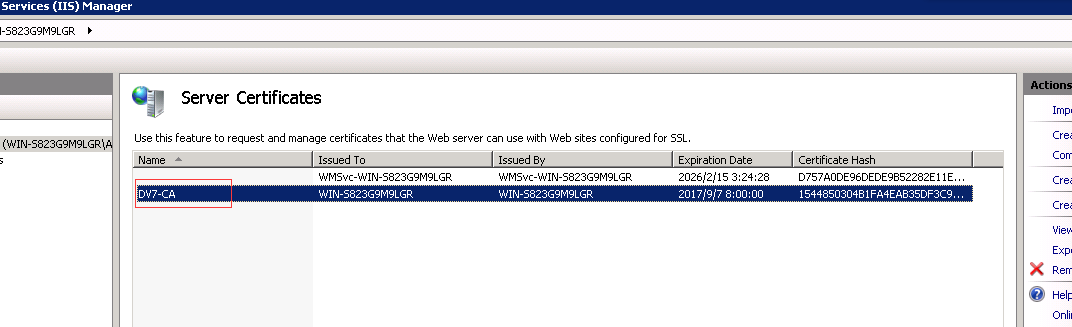




Click “Create Self-Signed Certificate” and then input a friendly name.

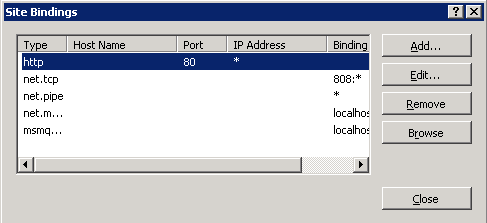


Click “OK” button, the certificate is ok.

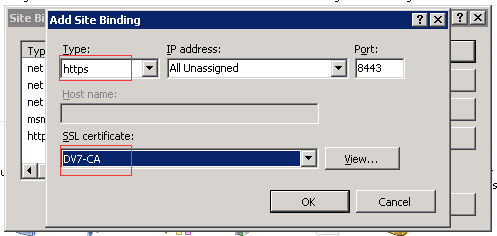


#### Set site binding:

Then, we set site binding. Right-click “Default Web Site” and select “Edit Bindings”.



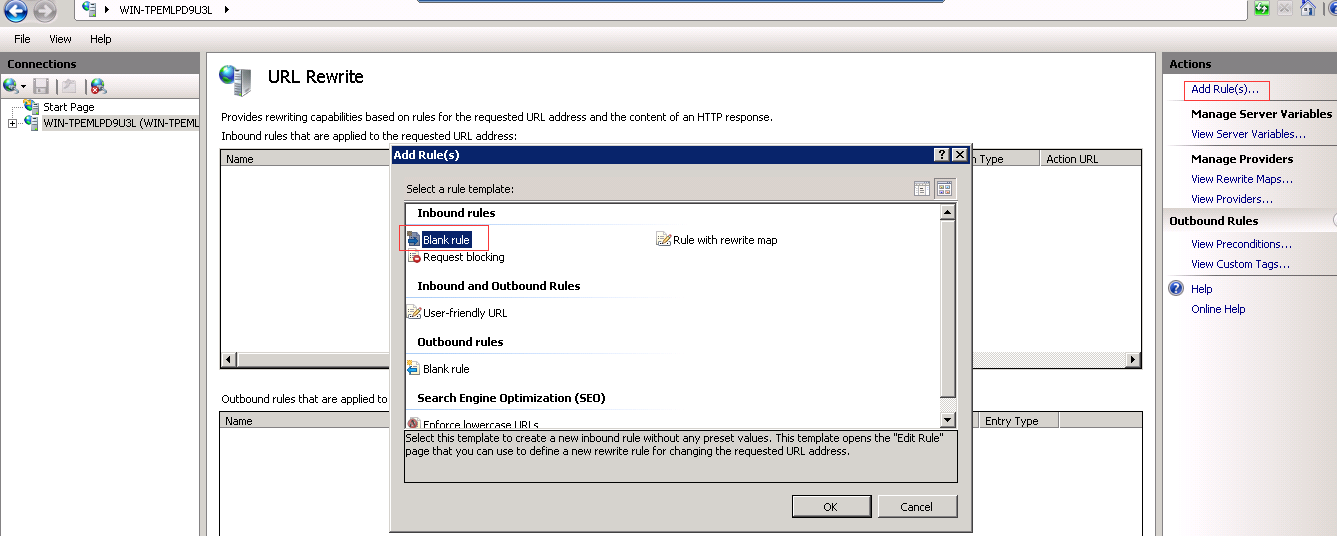
Click “Add” button and set listening port(e.g.:8443).



After click “OK” button, the site binding is ok.

#### Set URL Rewrite Rules:

Finally, we set “URL Rewrite”. Click “Add Rule(s)” and select “Blank rule”.

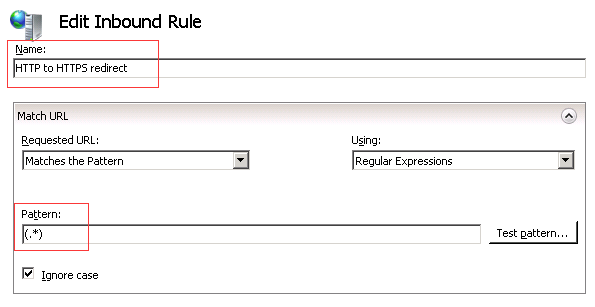


Click “OK” button and set the parameter like below.

Match URL:

Name: “HTTP to HTTPS redirect”;

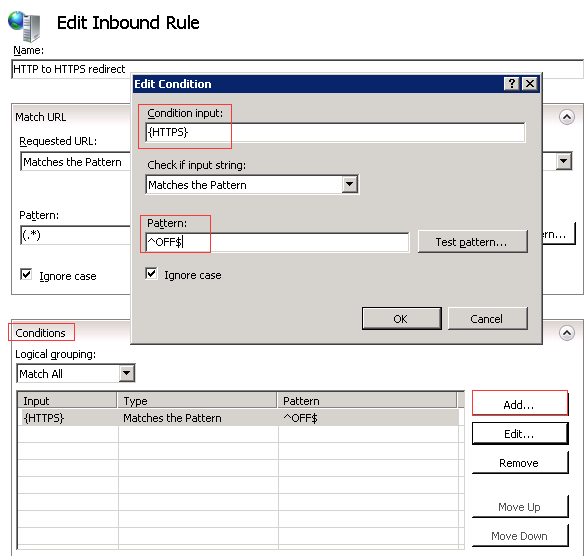
Pattern: “(.\*)”



Conditions:

Condition input: {HTTPS}

Pattern: ^OFF$

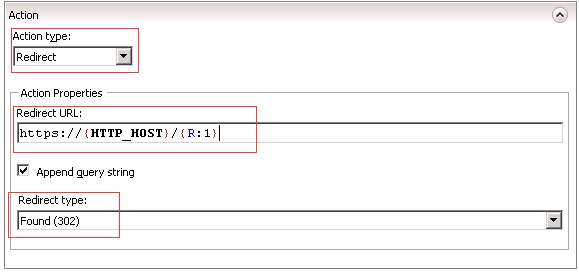


Action:

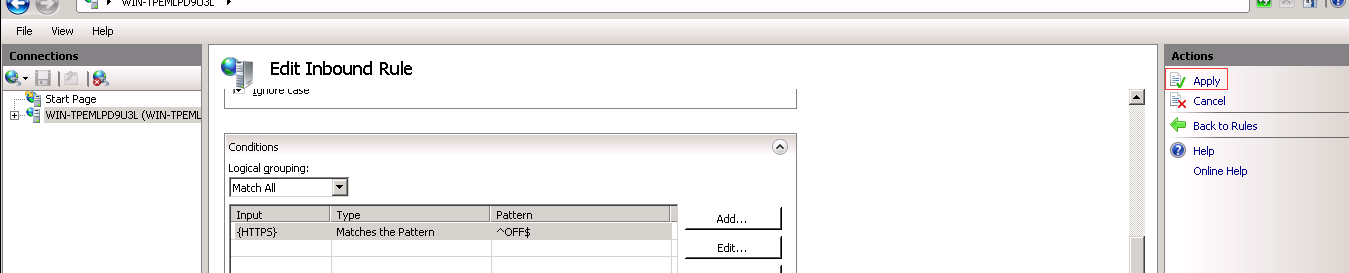
Action type: Redirect

Redirect URL: https://{HTTP\_HOST}/{R:1}

Redirect type: Found (302)



All of the configuration is ok, click “Apply” to take effect.



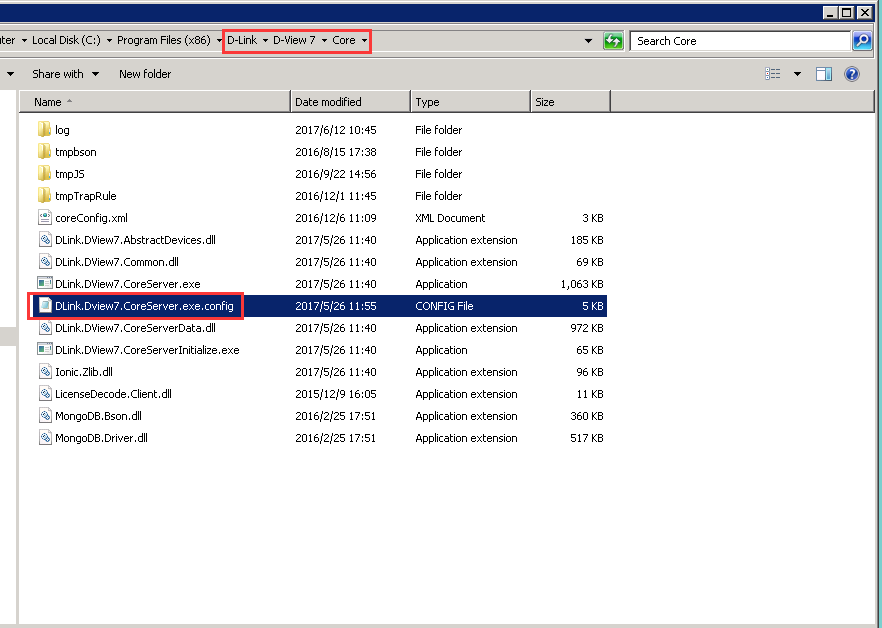
Now, we can access DV7 by https.

## Modify the D-View 7 Core Server Listening Port

In the D-View 7 core server configuration file, D-Link will provide an interface that allows us to modify the default listening port.

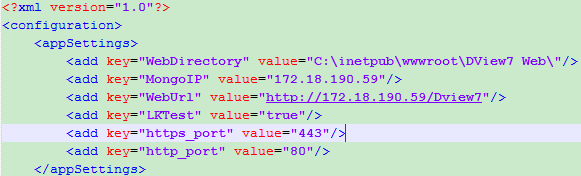
### Configuration file path

“…\D-Link\D-View 7\Core\ DLink.Dview7.CoreServer.exe.config”.



### Listening port nodes: https\_port, http\_port

We can modify the default values of https\_port and http\_port to the specified port here.

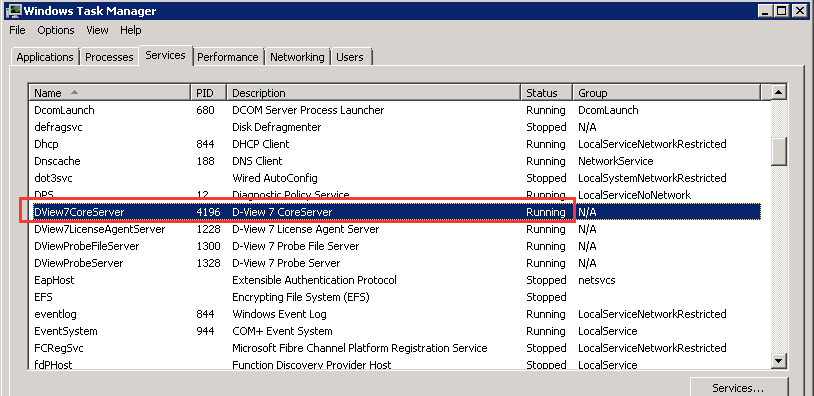


### Running rules about “https\_port”, “http\_port” nodes

* If there are no “https\_port”, “http\_port” nodes in the configuration file, core server will listen 443 & 80 port by default when it is running.
* If there are “https\_port”, “http\_port” nodes been configured in the configuration file, core server will read and valid the value.
* If the value is a legal port number, core server will run and listen it. Otherwise, core server will use default value (http\_port:80, https\_port:443) as the listening port.

### Make the configuration effective immediately

Open Windows Task Manager, restart core server service. So far, the listening port of core server has been modified successfully.

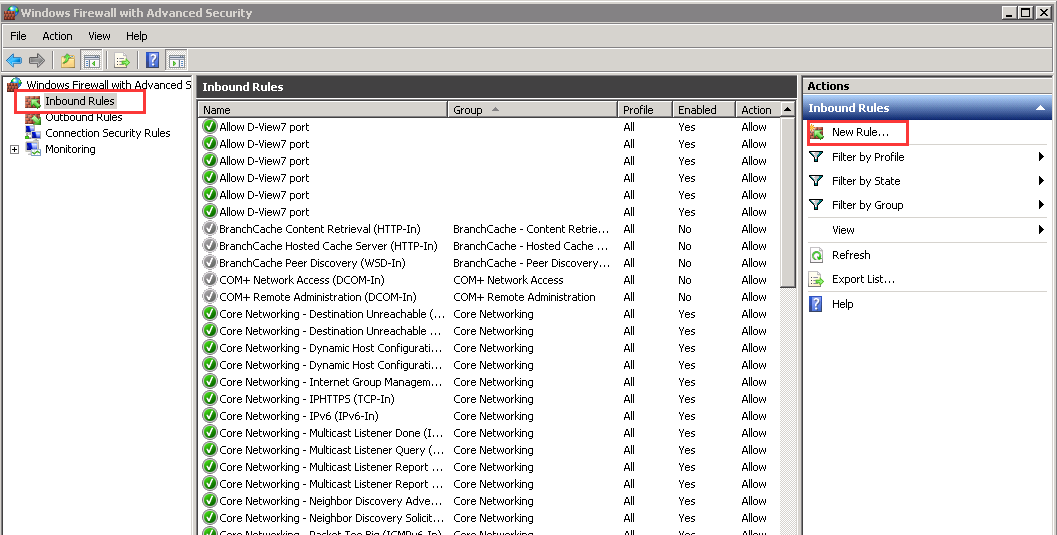


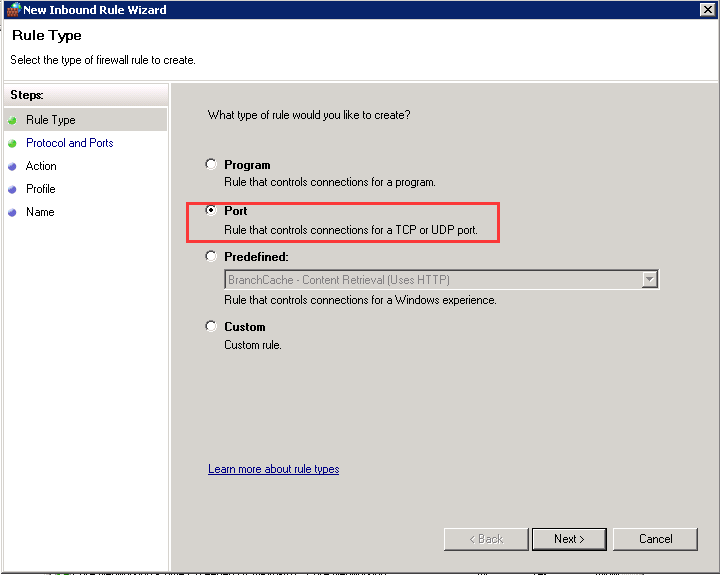
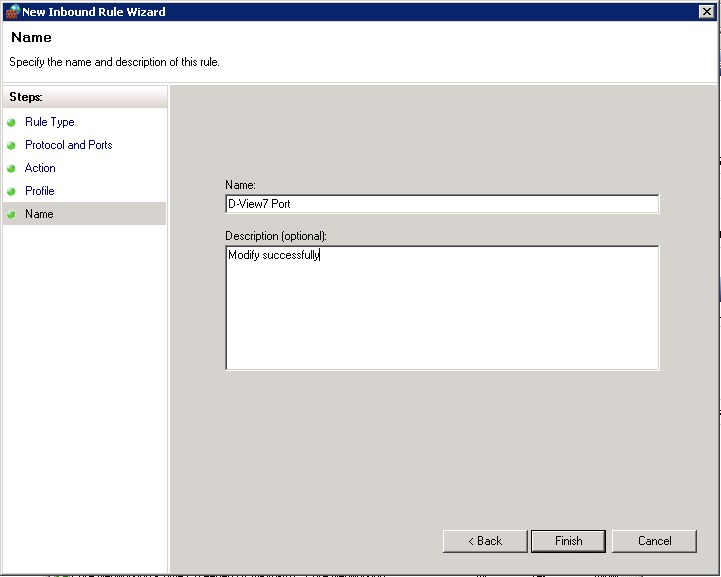
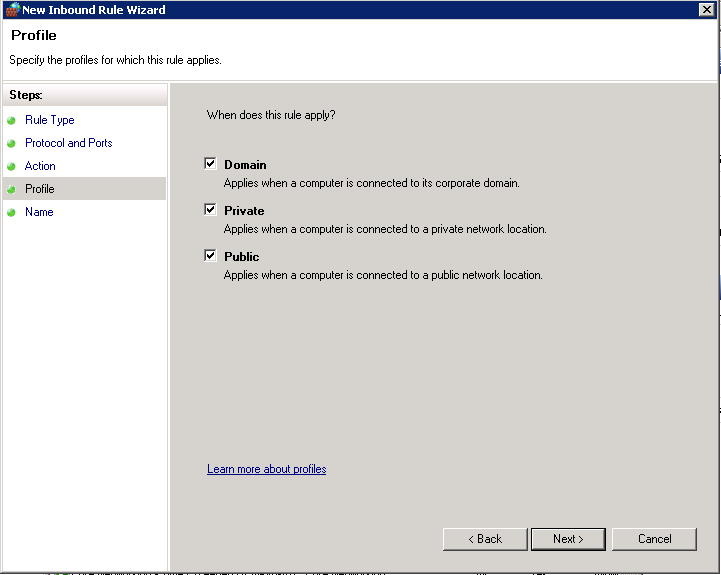
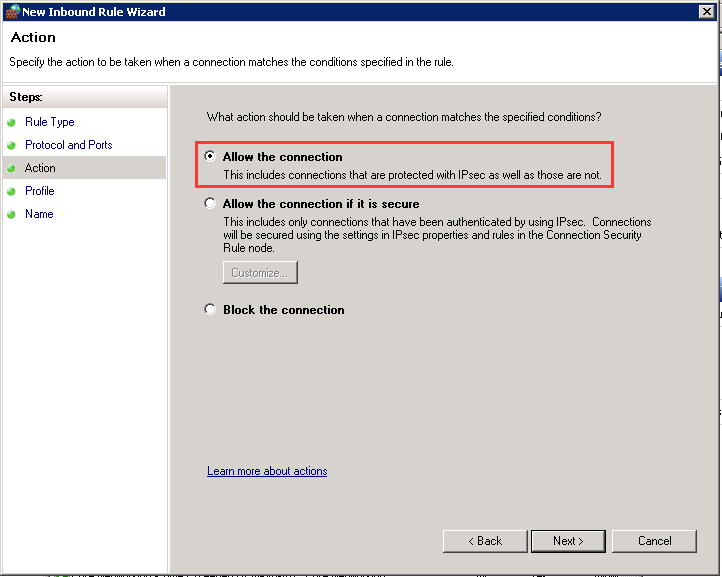
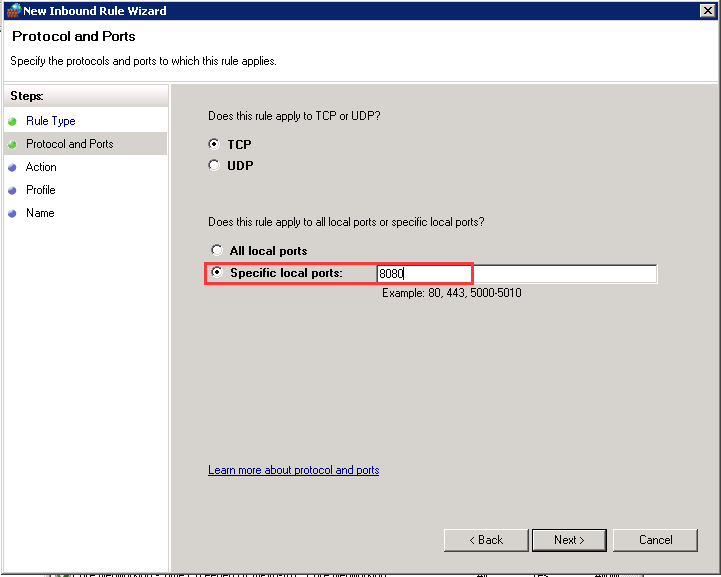
## Configure the Firewall

We should configure the firewall rules to allow the customized port to access freely. There may be two parts that need to be configured:

### The Windows OS Firewall on Core Server

We need to configure the windows OS firewall on the core server and add Inbound Rules to allow the connections with customized port through (e.g.:8080) .





### Hardware Firewall

We also need to configure the NAT or the network firewall to allow the connections with customized port through.

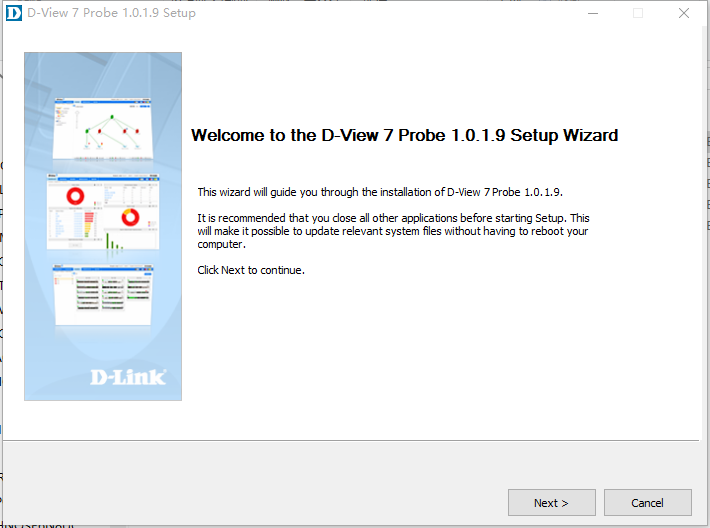
## Configure Probe

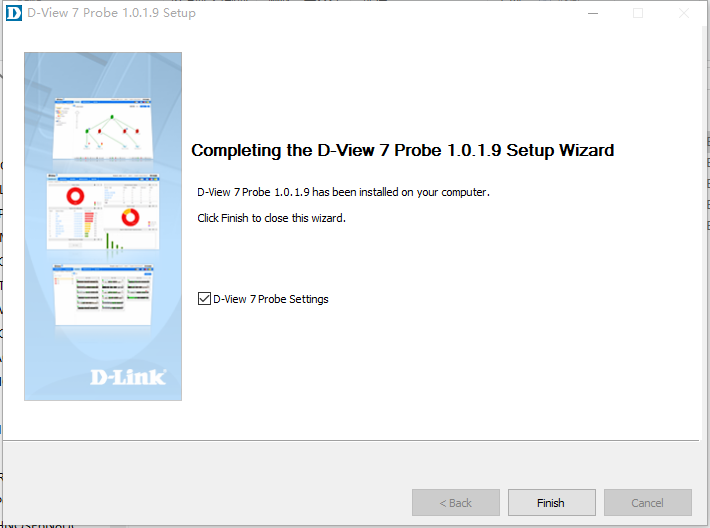
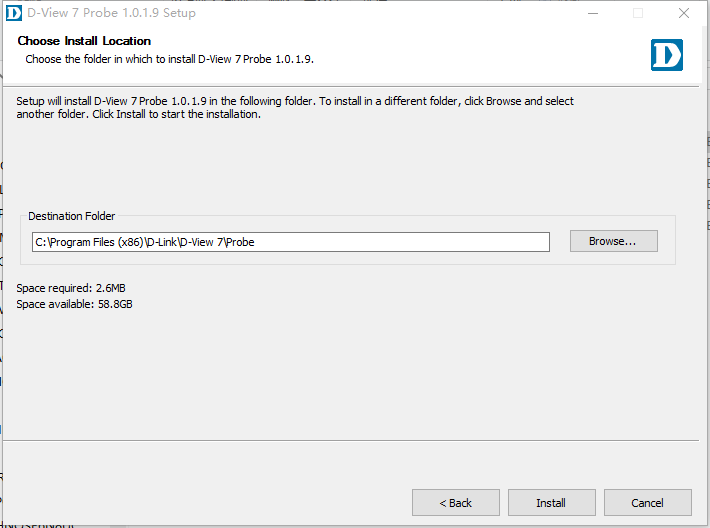
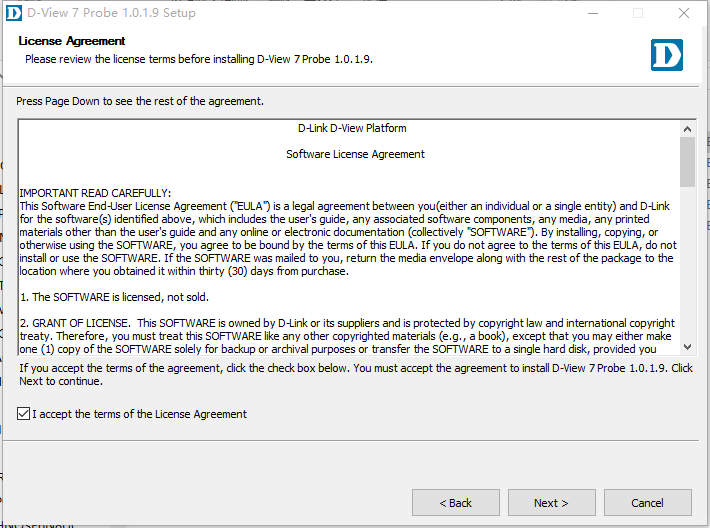
### Local Probe

Local Probe will read the port from the D-View 7 core server configuration file, it will get a valid value of "http\_port".

If the port value is an integer 0<Port<65535, probe will use this port to connect to core server. Otherwise, it will use 80 to login to core.

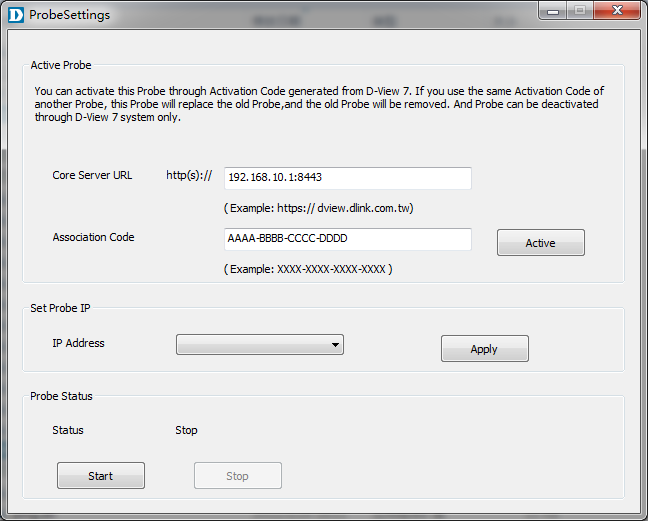
### Install a remote Probe





### Remote Probe Settings

After installing remote Probe, run “Probe Settings” tool will ask us to input the “Core Server URL”. We can input the URL with the customized port to let probe login and connect to core server. The format should be “IP:Port”(e.g.:192.168.10.1:8443).



Notes: If we want to modify the port of the remote Probe that has been deployed, we must uninstall this Probe, and then follow the steps above to install it again.