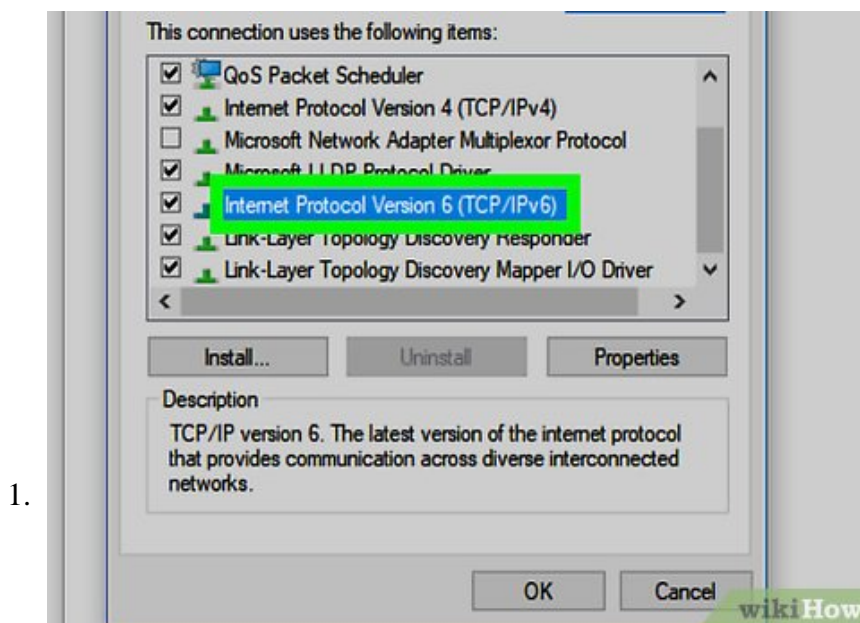


How to Install, Configure, and Test Certificate Services in a Windows Server 2012 R2 Domain

An organization can use certificates for several reasons, such as ensuring that only the intended recipients can read the transmitted data. In a Windows Server 2012 R2 domain, this document demonstrates viewing Web pages that are protected...

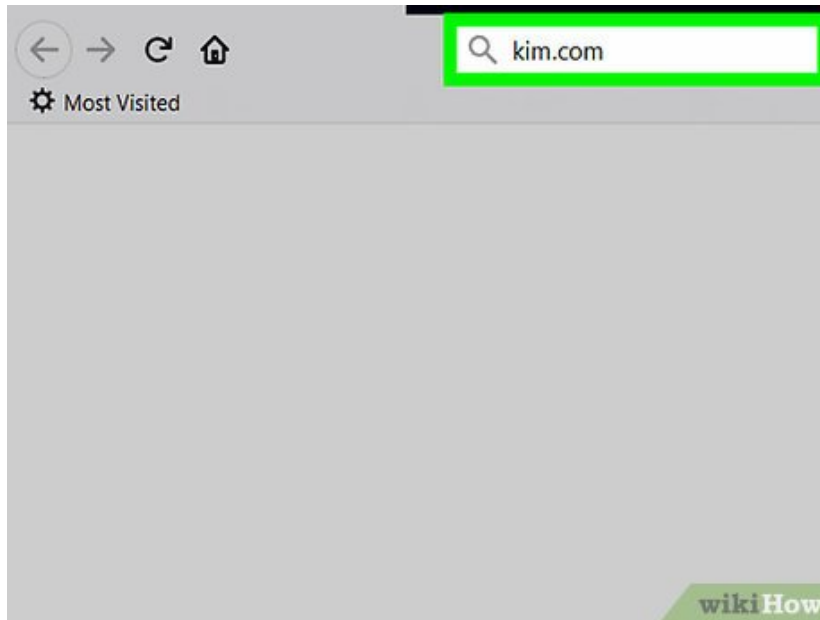
Part 1 of 5:

Reviewing the Configuration



Review network configuration.

1. Verify IP address, subnet mask, Preferred DNS, and name of the Windows Server 2012 R2 computer: 172.16.150.10, 255.255.255.0, 172.16.150.10, w12r2a10
2. Verify IP address, subnet mask, Preferred DNS, and name of the Windows 7 computer: 172.16.150.15, 255.255.255.0, 172.16.150.10, w715.



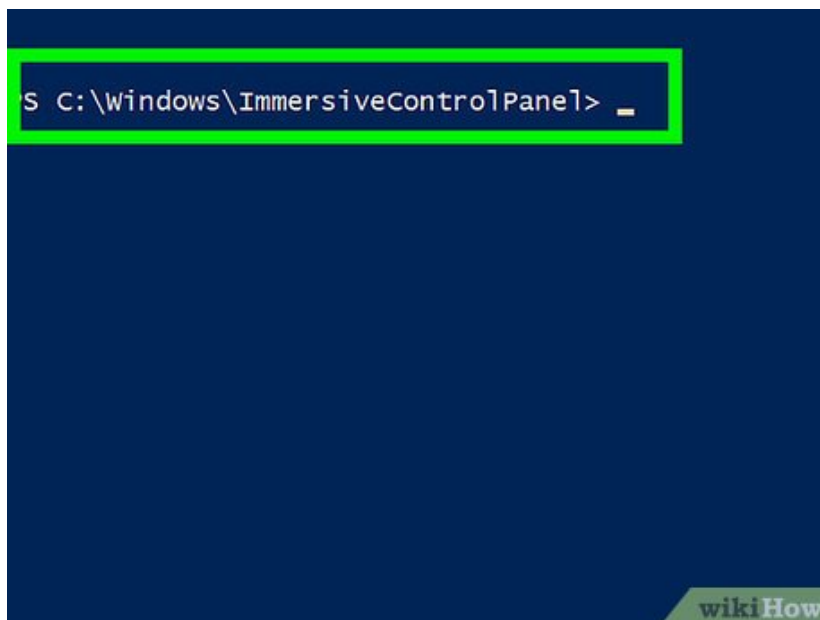
2.

Review domain configuration.

1. Verify the Windows Server 2012 R2 named w12r2a10, is configured to host the domain kim.com, Passworda10.
2. Verify the Windows 7 client, named w7a15, is configured as a kim.com domain member.
3. Verify that you have created a domain user named raja.

Part 2 of 5:

Installing, Configuring, and Verifying AD Certificate Services

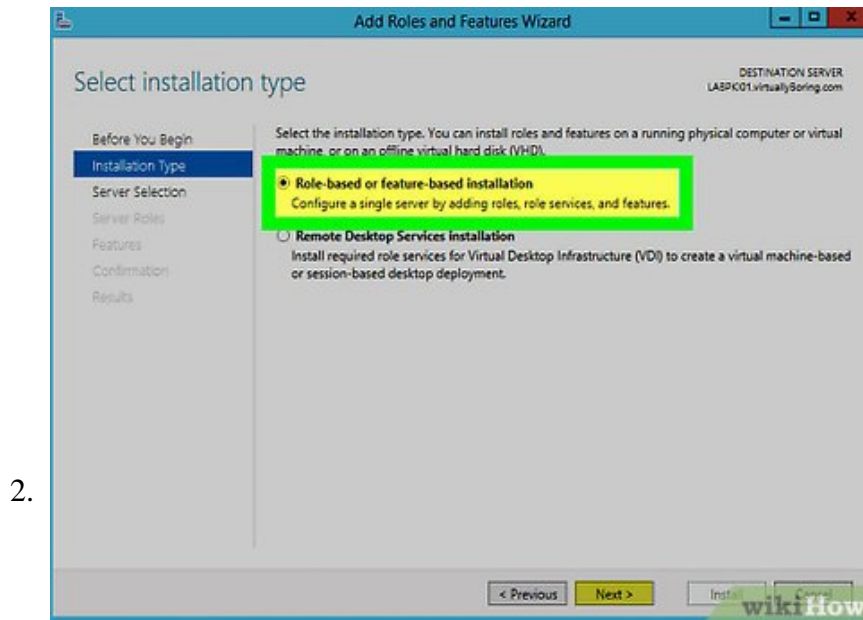


1.

Install Active Directory Certificate Services.

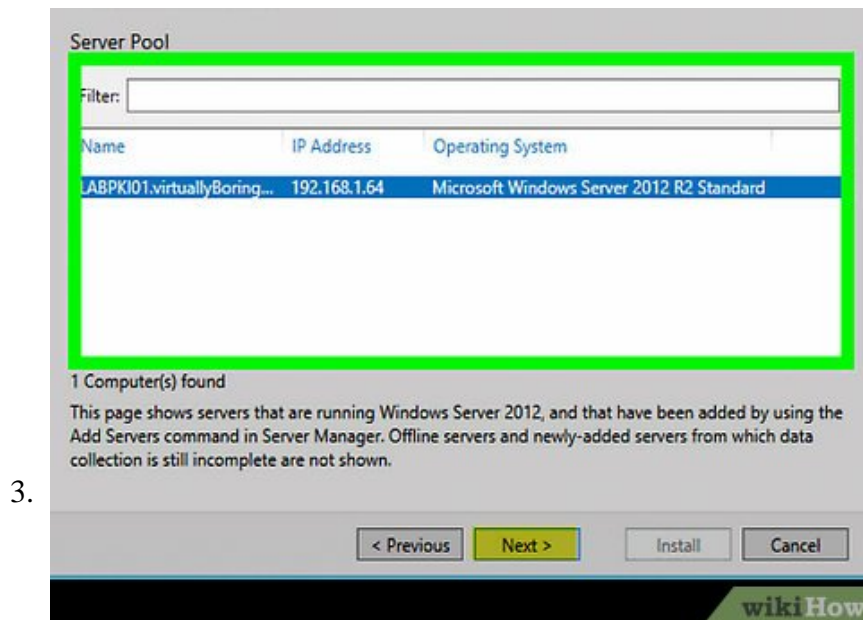
1. Use the default settings on the machine named w12r2a10, which is hosting domain kim.com.

2. Keep the Installation progress window open.



Configure active directory certificate services.

1. Click Configure Active Directory Certificate Services on the destination server when the blue installation progress bar is 100%; this action displays the Credentials window.
2. Click Next to display Role Services.
3. Click the checkbox next to Certification Authority and click Next.
4. Click Next several more times to accept all defaults and display Confirmation.
5. Click Configure to display results and verify there is a green circle with a white check mark, and click Close twice.



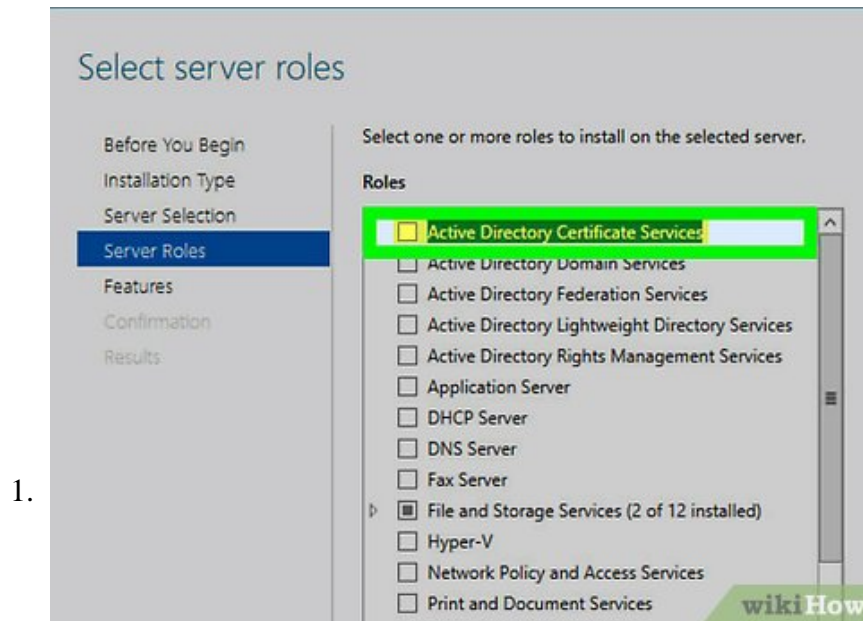
Verify Active Directory Certificate Services.

1. Open Administrative Tools and double click Certification Authority.
2. Expand kim-W12R2A10-CA and click Issued Certificates.

3. Right click the white area and click Refresh, if it is empty.
4. Reboot the domain controller, if it is still empty after a few refreshes.
5. Display Issued Certificates after reboot and scroll the right pane, to review it.
6. Notice that w12r2a10.kim.com is listed under Issued Common Name.

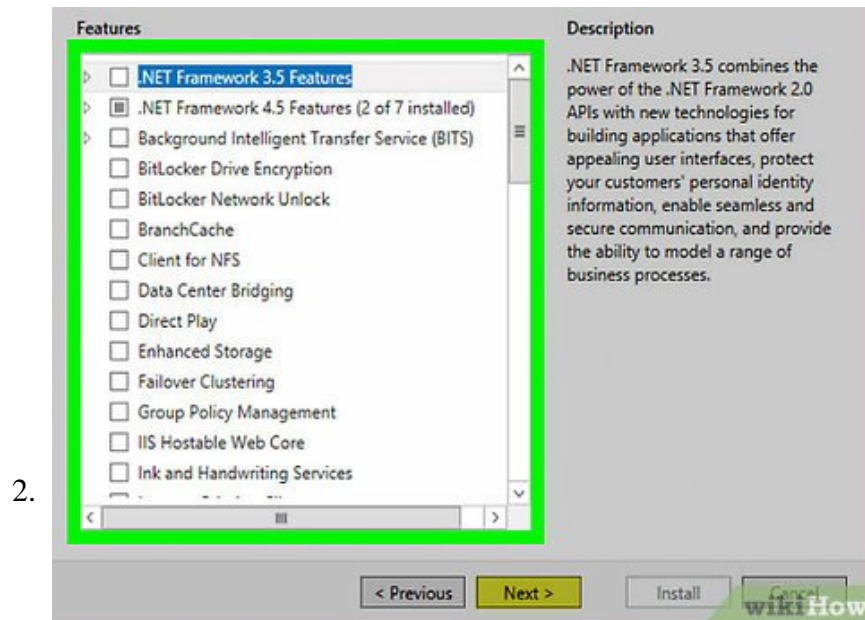
Part 3 of 5:

Installing and Browsing Web Server (IIS)



Install Web server (IIS).

1. Configure the default settings, while installing IIS on the machine named w12r2a10, which is hosting domain kim.com.
2. Keep the Installation progress windows open.
3. Click Close when the blue installation progress bar is 100%.

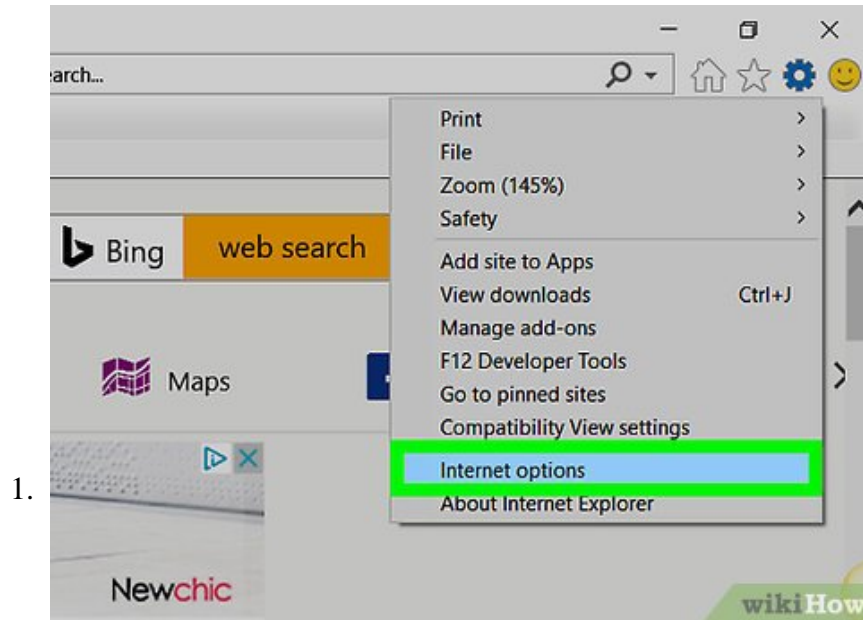


Browse Web server (IIS).

1. Go to Administrative Tools.
2. Double click Internet Information Services Manager.
3. Expand w12r2a10 (KIM...) and expand sites.
4. Click Default Web Site and then click Bindings under Actions.
5. Click Add.
6. Click the dropdown menu under Type and select https.
7. Click the dropdown under SSL certificate, where you will see the certificates for the certification server, kim-w12r2a01-CA, and the Domain (Web server), w12r2a10.kim.com.
8. Click Cancel followed by Close.

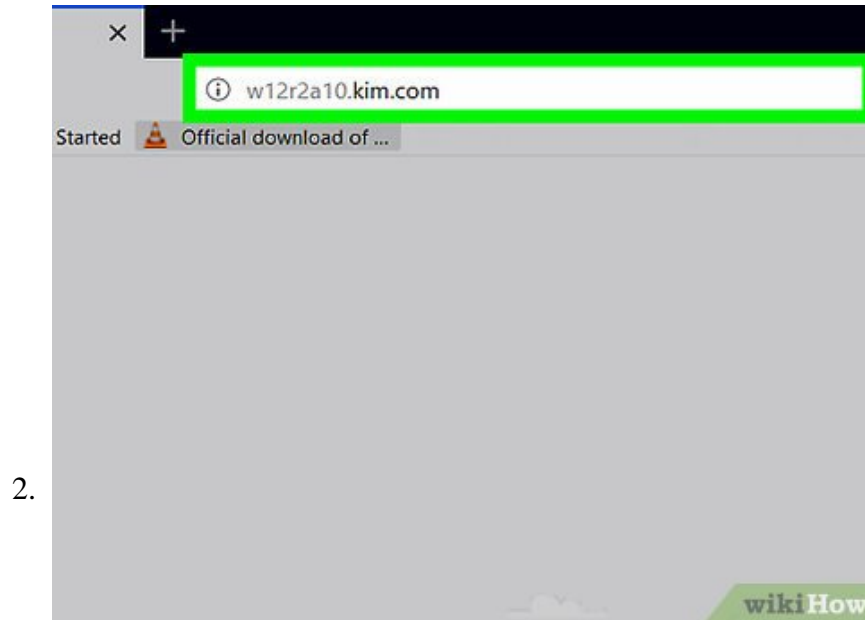
Part 4 of 5:

Displaying Domain Member Certificate Configuration



View certificate on domain member.

1. Log on to the domain from w7a15 as user raja. Configure IE to point to your homepage, <http://w12r2a10.kim.com>.
2. Terminate and restart IE to display your homepage.
3. Go to IE, Tools, Internet Options, Content, Certificates and click all tabs to view their listings.
4. Notice that Intermediate Certification Authorities and Trusted Root Certification Authorities have an entry for Certification Authority server, kim-w12r2a10-CA.
5. Notice that Personal is empty; why? Because domain user raja has not requested one.
6. Go to IE, Tools, Internet Options, Content, Publishers and click all tabs.
7. Notice that Intermediate Certification Authorities and Trusted Root Certification Authorities have an entry for Certification Authority server, kim-w12r2a10-CA.
8. Notice that this Personal is also empty.
9. Why is a certificate entry in Trusted Root Certification Authorities has an entry, kim-w12r2a01-CA, important? It means that the server is trusted by the member client; specifically, the client can display the https page if the Web server is configured to serve it.

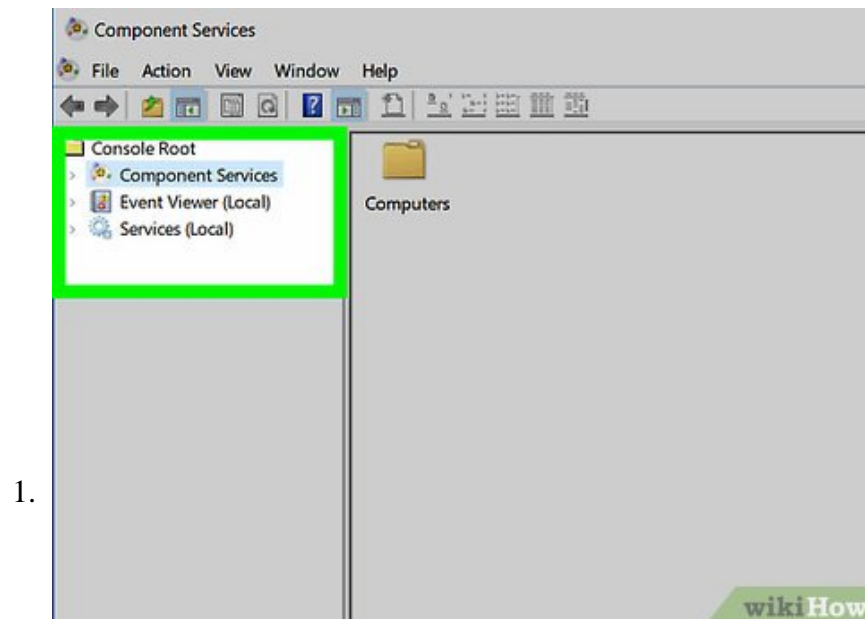


Display your homepage on w7a15 using https.

1. Note that even though the server and client have certificates, https does not work.
2. Observe that the reason it does not work is because port 443 is not configured.

Part 5 of 5:

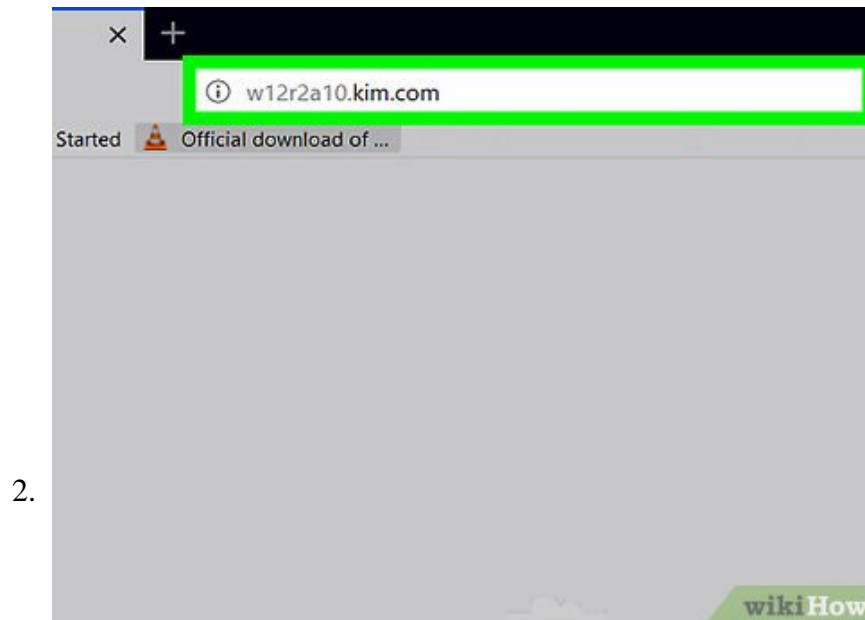
Applying and Verifying Secure Socket Layer (SSL)



Configure SSL.

1. Go to Administrative Tools on the domain controller.
2. Double click Internet Information Services Manager and expand w12r2a10 (KIM...)
3. Expand sites.

4. Click no, if you are prompted about Microsoft Web Platform.
5. Click Default Web Site and click Bindings under Actions.
6. Click Add.
7. Click the dropdown menu under Type and select https.
8. Click the dropdown menu under SSL certificate, where you will see the certificate for the certificate server, kim-w12r2a10-CA, and the Domain (Web server), w12r2a10.kim.com.
9. Click OK. .
10. Notice that https is now listed in Site Bindings.
11. Click Close.
12. Note that the server is now configured for https access



Verify SSL.

1. Logon to the domain from w7a15 as user raja.
2. Display your homepage on w7a15 using https.
3. Note that it works, since the server is configured to server https pages.
4. Note also that, even though raja does not have a certificate, the https page displayed, because of these reasons.
 1. w7a15, which raja is using, has a certificate issued by the enterprise CA.
 2. kim-w12r2a01-CA; specifically, there is now a trust between the domain controller and w7a15
 3. SSL is configured, but it is not being enforced

You finished reading the article "**How to Install, Configure, and Test Certificate Services in a Windows Server 2012 R2 Domain**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.