

How to Configure CAWE in a Windows Server 2012 R2 Domain

This lab teaches you how to configure Certification Authority Web Enrollment (CAWE) in a Windows Server 2012 R2 domain. This process is useful in many situations, such as when a domain user wants to logon to a domain, but he or she does...

Part 1 of 3:

Installing and Configuring Computer, Domain, and Network Requirements

1. Install and configure computer requirements.

1. Install Windows 7 Virtual Machine.
2. Change the Windows 7 Virtual Machine name to `w7a15`.
3. Install Windows Server 2012 R2 Virtual Machine.
4. Change the server name to `w12r2a10` and set password to `Passworda10`.

2. Configure the network requirements.

1. Computer name, IP address, subnet mask, preferred DNS
2. `w12r2a10`, `172.16.150.10`, `255.255.255.0`, `172.16.150.10`
3. `w7a15`, `172.16.150.15`, `255.255.255.0`, `172.16.150.10`
4. Verify a successful ping of w12r2a10 and w7a15 in both directions.

3. Install and configure domain requirements.

1. Install AD DS and configure w12r2a10 to host domain `kim.com`.
2. Install and configure AD CS with certificate services with default settings.
3. Install and configure Web Server (IIS) role with default settings.
4. Display, on w7a15, kim.com homepage by FQDN, `http://w12r2a10.kim.com`.
5. Verify you cannot display securely, on w7a15, kim.com domain homepage by FQDN, `https://w12r2a10.kim.com`.

Part 2 of 3:

Configuring Webserver Requirements

1. Configure SSL properties.

1. Go to "Administrative Tools" and click "IIS Manager," on w12r2a10.
2. Expand "Sites."
3. Click "Default Web Site."
4. Double click SSL, in the center pane, to display the SSL Settings menu that has an SSL checkbox and three radio buttons labeled `Ignore`, `Accept`, and `Require`.
5. Notice that Require SSL is unchecked and Ignore is selected; these are the default settings after configuring SSL Bindings.

6. Verify you cannot display, on w7a15, kim.com domain homepage by FQDN, <https://w12r2a10.kim.com>.
 7. Verify that kim-W12R2A10-CA is not listed in "IE Trusted Root Certification Authority."
 8. Verify that Personal does not have a certificate issued by domain kim.com.
2. **Verify the webserver configuration.**
1. Note that for a domain user to request a certificate when using a client that is not a domain member, you must create a special CA site, which is placed in the Sites branch in IIS manager and is given the name certsrv.
 2. Go to "Administrative Tools" and click "IIS Manager," on w12r2a10.
 3. Expand w12r2a10 (KIM...).
 4. Expand "Sites."
 5. Click "Default Web Site."
 6. Notice that certsrv is not listed; therefore, you must add AD CS feature, (CAWE) Role Service.
3. **Install CAWE .**
1. Go to "Server Manager" on w12r2a10.
 2. Click "Add Roles" and features to display "Add Roles and Features Wizard," before you begin..
 3. Click to display "Select installation type."
 4. Notice that role-base or feature-base is selected.
 5. Click to display "Select destination server."
 6. Notice that there is only one server, so there is nothing to select.
 7. Click to display "Select server roles."
 8. Click the triangle next to ADCS to expand it.
 9. Click the checkbox next to Certification Authority Web Enrollment (CWE).
 10. Click "Add Required Role Services," when prompted.
 11. Click , until "Install" is shown.
 12. Click .
 13. Leave the Installation progress open.
 14. Hover the progress bar to see when the install completes, 100%.
4. **Configure CAWE installation.**
1. Click Configure ADCS on the destination server to configure the service and display "Credentials."
 2. Click to display "Role Services."
 3. Click the box next to "Certification Authority Web Enrollment."
 4. Click to display the confirmation page.
 5. Click .
 6. Click until you are returned to "Server Manager."
5. **Verify the webserver updated configuration.**
1. Expand "Sites" in IIS manager.
 2. Click "Default Web Site" and notice that certsrv is listed.
6. **Request and install certificate.**
1. Log on to w7a15 as maya.
 2. Go IE and on W7a15.
 3. Type <https://w12r2a10.kim.com/certsrv>.
 4. Click when prompted with "This CA is not trusted."
 5. Type at the Windows Security prompt.

6. Click Request a certificate at the "Microsoft Active Directory Certificate Services - kim-w12r2a10-CA" prompt.
7. Click "Advanced Certificate Request."
8. Click and submit a request to this CA.
9. When prompted with Web access confirmation, click Yes.
10. Click on "Advanced Certificate Request."
11. Click when prompted with Web access confirmation.
12. Click .
13. Click .
14. Click when prompted with "Do you want to open or save this file?"
15. Click when prompted with "A website wants to open web content..."
16. Click when prompted with "Certificate Information."
17. Click on "Welcome to the Certificate Import Wizard."
18. Click on **Certificate Store display**, the radio button next to "Place all certificates in the following store."
19. Click .
20. Click **Trusted Root Certification Authorities** on "Select Certificate Store."
21. Click .
22. Click on "Security Warning."
23. Click .
24. Click .
25. Click when prompted with "Security Warning. You are about to install a certificate..."
26. Click on "Certificate Import Wizard."
27. Click on "Certificate Information."
28. Click on "Certificate Issued."
29. Terminate IE when your new certificate has been successfully installed.

Part 3 of 3:

Verifying CAWE installation and Configuration

1. You'll now want to test homepage with HTTP and HTTPS.
 1. **Start IE on w7a15.**
 2. **Verify there is a Trusted Root Certification Authority for kim-W12R2A10-CA.**
 1. View Issued Certificates, on w12r2a10, and notice that the Requester Name for this newly acquired certificate is KIMmaya.
 3. **Log on to w7a15 as maya.**
 1. Change the IE homepage on w7a15 to point to <https://w12r2a10.kim.com>.
 2. Terminate IE.
 3. Start IE and be sure the displayed page is using https, not http.
 4. **Log on to w7a15 as andi.**

1. Change the home page to <https://w12r2a10.kim.com>.
 2. Verify that user andi cannot display https homepage.
 3. Log off as user andi.
5. **Log on as user maya.**
1. Verify that user maya can still display the https homepage.

You finished reading the article "**How to Configure CAWE 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.
