Exchange 2016: Create CSR and Install SSL Certificate

Creating a CSR and installing your SSL certificate on your Microsoft Exchange Server 2016

Use the instructions on this page to use the Exchange Admin Center to create your certificate signing request (CSR) and then to install your SSL certificate on your Exchange 2016 server.

1. To create your certificate signing request (CSR), see Exchange 2016: How to Create Your CSR.
2. To install your SSL certificate, see Exchange 2016: How to Install and Configure Your SSL Certificate.

If you are looking for a simpler way to create CSRs, and install and manage your SSL Certificates, we recommend the DigiCert® Certificate Utility for Windows. With the DigiCert Utility, you can generate a CSR and install an SSL certificate, plus more. See Exchange 2016: Create CSR & Install SSL Certificate with DigiCert Utility.

1. Exchange 2016: How to Create Your CSR

Using the Exchange Admin Center (EAC) to Create Your CSR

1. Access the EAC by opening a browser and browsing to the URL of your server (e.g., *https://localhost/ecp*).
2. On the **Exchange Admin Center** credentials page, type your **Domain/user name** and **Password** and then click **sign in**.
3. In the **EAC**, in the sidebar menu on the left, click **Servers** and then in the menu at the top of the page, click **Certificates**.
4. On the **Certificates** page, in the **Select server** drop-down list, select your Exchange 2016 server and then click the + symbol.
5. In the **new Exchange certificate** wizard, select **Create a request for a certificate from a certification authority** and then click **Next**.

6. In the ***Friendly name for this certificate:** box, type a friendly name for the certificate and then click **Next**.

   The friendly name isn't part of the certificate; instead, it's used to identify the certificate.

   We recommend that you add DigiCert and the expiration date to the end of your friendly name, for example: *yoursite-DigiCert-expirationDate*. This information helps identify the issuer and expiration date for each certificate. It also helps distinguish multiple certificates with the same domain name.

7. **Wildcard Plus Certificate**

   Note: If your *are not creating a csr for a wildcard certificate*, click **Next**.

   To create a CSR for a wildcard certificate, do the following:

   1. Check **Request a wild-card certificate**.
   2. In the ***Root domain:** box, type the root domain for all the subdomains (e.g., **.example.com*).
   3. Click **Next**.

8. In the ***Store certificate request on this server** box, click **Browse…**, select the server you want to store the certificate request on, and then click **Next**.

9. **Select Domain(s) to Include on the SSL Certificate**

   Note: If you *are creating a csr for a wildcard certificate*, skip this step by clicking **Next** and **Next**. Proceed to step 10.

   To select the domain(s) that you want included on your SSL certificate, do the following:

   1. Click **Next**.

      The wizard populates the list with domains that Exchange 2016 suggest you include in your certificate request.

      Although you can edit the list of domains on this page of the wizard, we recommend doing it on the next page.

   2. On the next page, review the list of names/domains and use the +, ✏, -, and ✓ symbols to add, edit, remove, and select the domains you want included on your SSL certificate.
   3. When you are finished, click **Next**.

10. Under **Specify information about your organization**, provide the following information and then click **Next**:

*Organization name:	Type your company's legally registered name (e.g., *YourCompany, Inc.*).
*Department name:	Type the name of your department within the organization. Frequently this entry will be listed as "IT" or "Web Security".
*City/Locality:	Type the city/locality where your company is legally located.
*State/Province:	Type the state/province where your company is legally located.
*Country/Region name:	In the drop-down list, select the country/region where your company is legally located.

11. Under ***Save the certificate request to the following file**, enter a UNC path to save your CSR to.

    Note: Select a location that you can access. You must be able to access the location so that you can use the CSR to order your SSL certificate.

12. Click **Finish** to generate the CSR and save it to the specified UNC path.

13. Use a text editor (such as Notepad) to open the file. Then, copy the text, including the **-----BEGIN NEW CERTIFICATE REQUEST-----** and **-----END NEW CERTIFICATE REQUEST-----** tags, and paste it into the DigiCert order form.

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIICvDCCAaQCAQAwdzELMAkGA1UEBhMCVVMxEjAQBgNVBAgTCVlvdXJTdGF0ZTER
MA8GA1UEBxMIWW91ckNpdHkxCzAJBgNVBAsTAklUMRowGAYDVQQKExFZb3VyQ29t
cGFueSwgSW5jLjEYMBYGA1UEAxMPd3d3LmV4YW1wbGUuY29tMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA379BFFxfACdXsUk2wrQka/nAlKbo+I9DAW32
+/SRxj/KtXVddscKW1obHGpMKPw4meJqOpQwJkIChYjSUQSpPKzdGpccDMf/eoF0
J7EaQ2szLv9AqdRQw2Aaek8SmocVmd3LxEOX4VvALBOMLHVrB5/vhYfGECLJbc31
RdEbdXyHDtHklRAoIVQCfjTwBWGNAD337vmHW7Q0R6FYUoa4fcJh7Rv6jHSywqwx
7pVfaDbZPuTgUhw7wksKNFxccG0xcTMr/+GrciHEuZ0chq86CBP9RIyLpp2+RMSf
m6rMEYm9o65j7vEYaKEJUOJtA5MIs/ZjaXfS1LjXurLU0nCOQQIDAQABoAAwDQYJ
KoZIhvcNAQEFBQADggEBAK159goyAYOpcnrQ2EvCGlizrK1kS3D8JjnAiP1NHrjB
/qdTYR+/8Dr/hMcwwU5ThGAVf68eMkk6tUNwAdpZ9C904Js2z+ENEbO8GA0Fc4rw
ix7vb15vSXe3shGijRGIzzHVGRoR3r7xQtIuMaDAr3xlV8jHbcvZTcpX0Kbq6H1G
NLA4CXsOI4KGwu4FXfSzJEGb3gEJD8HaMP8V8er5G0owv/g/9Z/1/b0g97kAcUwk
M2eDsvPhMx/pENGbnLPe4XMy7NPiEdzFnaYtUy2BDcXj3ZQEWxRWklERgg9/YcWI
obf5ziuNm1Df24NBt5tpCNzfGviKT6/RYfWg3dMaKxc=
-----END NEW CERTIFICATE REQUEST-----
```