

SSL/TLS - Signing Certificates With A Microsoft Certificate Authority

Article Number: 597 | Rating: 1/5 from 1 votes | Last Updated: Thu, Jun 15, 2017 at 1:05 AM

Overview

This KB article shows you how you can sign your SSL/TLS certificates with a Microsoft Certificate Authority (CA). This article compliments our product specific documentation for configuring SSL/TLS.

Why would you want to do this? When you create self-signed certificates they are not trusted by your web browser and produce warning messages. When a Windows computer is a member of an Active Directory (AD) domain, Internet Explorer will trust certificates signed by the CA(s) in that domain and hence will not produce warnings.

Requirements

This KB article assumes that you have been following the product specific documentation for configuring SSL/TLS and requires you to be in the root users home directory. If you are not in this directory execute the following command:

```
cd ~
```

Get Certificate Request

In the product specific documentation for configuring SSL/TLS you would have executed the following command:

```
openssl req -new -key keyfile.key -out certrequest.csr
```

You will have completed all of the fields and this will create the `certrequest.csr` file. Execute this command to display the contents of the request:

```
cat certrequest.csr
```

This will output something like this:

```
-----BEGIN CERTIFICATE REQUEST-----
MIICsDCAZgCAQAwazELMAkGA1UEBhMCQVUxDDAKBgNVBAMGA05TVzEPMA0GA1UE
BwwGU3lkbmV5MRswGQYDVQQKDBJNeSBDb2lwyW55IFB0eSBMdGQxIDAeBgNVBAMM
F3hpLXI2eC14ODYuYm94MjkzLmXvY2FsMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEAYmJrmOn5tea18eSBGby07hPMYbkwdMTrwq1DsrKBzQg+RrEjAmmN
s5ZvIsvFF1gVsx1IAASFFFG5M1UU2177bufNR/1D/6h4zwaVVz+8AzuuLy8oaD3r
WKSnlkT/td1XrBEKb5MUTp8KjxUjC8g/zpRimAzrIqIzzW913uLXkaf6DY9Q1uOJ
9ifNtWhe/7OYas08vykwYscZjWEGcxt14qYdh7X4BtOjXFMSrrHyCNgv8+TYJDnP
QIcjlurIrQTn+qH3U4nDWrym4Leu96vyHc0uO/kx+xtLb6svnYZganyAjmipa7cn
CFdVeC1EewSSTs1USGdecEYUearKLhc6XwIDAQABAAAwDQYJKoZIhvcNAQEFBQAD
ggEBAHIA5S2B88Iszn75iUosZQJvT74z/q6xiNQNiEMxzjgdMLoDumswHopFEoPd
fB0UQT614YZo1boqwy+YlNA7YizWt9vBJI6a3y1+Bi16mjdbdDBNqMuPkZjPtjqkh
AzNiSEWQL9LpOgmxDq33UKNi6kocffnUqIle28hTjWV6LNNy4gdmiYFrQAbAAIiJ
ubRbiEcrs1EiACTJgt3ucYD0tQvhlviSmk1j5xS0daGRAfntwyRe+0ZhLoRiykHk
cN/7NNzv5bSpGN8Lxe8H0spAaojg6t9JiFPsa8c0OW3Xj6CmiffG6Fwr5vySyTEv
HlprRyDQ1VV3LXZT9XeBJ+gAXJE=
-----END CERTIFICATE REQUEST-----
```

The following step will require you to provide this request.

Sign Using Web Interface

The Microsoft CA has a web interface available to use for signing certificate requests. This can be accessed by navigating to the following address in your web browser:

```
http://ca_server_address/certsrv
```

You will need to provide valid credentials to access the website.

You will be presented with the Welcome page. Click the **Request a certificate** link.

Microsoft Active Directory Certificate Services -- [Home](#)

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

Select a task:

- [Request a certificate](#)
- [View the status of a pending certificate request](#)
- [Download a CA certificate, certificate chain, or CRL](#)

Click the advanced certificate request link.

Microsoft Active Directory Certificate Services -- [Home](#)

Request a Certificate

Select the certificate type:

- [User Certificate](#)

Or, submit an [advanced certificate request](#).

In the **Saved Request** field paste the certificate request, including the -----BEGIN CERTIFICATE REQUEST----- and -----END CERTIFICATE REQUEST----- lines.

In the **Certificate Template** drop down list select **Web Server**.

Click the **Submit** button.

Microsoft Active Directory Certificate Services -- [Home](#)

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
fB0UQT6l4YZo1boqw+yLNA7YizWt9vBJI6a3y1+B
AzNiSEWQL9Lp0gmxDq33UKNi6kocffnUqIle28hT
ubRbiEcrsIEIaCTJgt3ucYD0tQvhlviSmk1j5xS0
cN/7NNzv5bSpGN8Lxe8H0spAaojg6t9JiFPsa8c0
HlprRyDQ1VV3LXZT9XeBJ+gAXJE=
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

Web Server

Additional Attributes:

Attributes:

The certificate will be signed and issued. Select **Base 64 encoded** and then click the **Download certificate** link.

Your web browser will prompt you to download a file called certnew.cer which you can save. You will need to open this file in a text editor such as Notepad and will appear something like:

```
-----BEGIN CERTIFICATE-----
MIIEszCCA5ugAwIBAgITbwAAAA/Kbjz1BRf/EQAAAAAADzANBgkqhkiG9w0BAQsF
ADAeMRwwGgYDVQQDExNCT1gyOTMtV1NFLVdTRTAyLUNBMB4XDTE3MDYxNDYmDEz
Ml0xNDTE5MDYxNDYmDEzMlowazELMAkGA1UEBhMCQVUxODAKBgNVBAGTA05TVzEP
MA0GA1UEBxMGU31kbmV5M5RcwsdfsdQQKEw5Cb3gyOTMgUHR5IEx0ZDEkMCIgA1UE
AxMbeGktcjZ4LXg4Ni5ib3gyOTMtd3N1LmxxvY2FsMIIBIjANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEAymjrmOn5tea18eSBGy07hPMYbkwDMTrwq1DsrbKzQg+
RrEjAmmNs5ZvIsvFF1gVSX1IAASFFFG5M1UU2177bufNR/1D/6h4zwaVVz+8Azuu
Ly8oaD3rWKSnlkT/td1XrBEKb5MUTp8KjxUjC8g/zpRimAzrIgzIzzW913uLXkaf6
DY9Q1uOJ9ifNtWhe/7OYas08vykwYscZjWEGcxt14qYdh7X4BtOjXFMSrrHyCNgv
8+TYJdnPQIcjlurIqTn+qH3U4nDWrym4Leu96vyHc0uO/kx+xtLb6svnYZganyA
jmiipa7cnCFdVeC1EewSaaaUSGdecEYUeaRKLhc6XwIDAQABo4IBmzCCAzcwHQYD
VR0OBBYEFNMHCBBpPsVSM7fFv/FGJbB6+zFMB8GA1UdIwQYMBaAFM2vfjWY14mA
xcc5obdaQubEkoj5MEAGA1UddddQ5MDcwNaAzodGGL2h0dHA6Ly9XU0UwMi9DZXJ0
RW5yb2xsL0JPWDI5My1XU0UtV1NFMDItQ0EuY3JSMIHKBggrBgEFBQcBAQSBvTCB
ujCBtwYIKwYBBQUHMAKGgagggGFwOi8vL0NOPUJPDWI5My1XU0UtV1NFMDItQ0Es
Q049QU1BLENOPVB1YmxxpYyUyMEtleSUyMFN1cnZpY2VzLENOPVN1cnZpY2VzLENO
PUNvbmZpZ3VYXRpb24sREM9Qk9YMjKzLVdTRScEQz1sb2NhbD9jQUN1cnRpb2mlj
YXRlP2Jhc2U/b2JqZWN0Q2xhc3M9Y2VydG1maWNhdG1vbKf1dGhvcml0eTAhBgkr
BgEABYI3FAIEFB4SAFcaZQBiaFMAZQBByAHYAZQBByMA4GA1UdDwEB/wQEAwIFODAT
BgNVHSUEDDAAKBgggrBgEFBQcDATANBgkqhkiG9w0BAQsFAAOCQAQEAqJdgvH30WjYA
eYcqCCK5MgjC69GctV3uv/zFMjPwezJegJ+BaC6QzQmC+BP+c5QoHnaJTxeRkZ
qVy+FKUMqssrOpTFcuoKX8IKTrg7YcXIhycZi1t3k/zQyShAy36QLz18pU0Uga
DMBH+wqLg3r7M8p7oFYE/lzh6+xtFnqFo2juJTXICkeFuX9JwhhtjUIhMvXXMtU+
1PelhLQtgU0jo9cmDYOA4OcqAn9z48ZOLmc3oXAYxKLbk1deigzRqj+nv0LEAt6M
VqYke4frWLnZXNH95AvwXEnV4ctJEW2a1hDFelrfcSKvXs+cJnMbawQ+/kAhjK6
TrMfb3j6sQ==
-----END CERTIFICATE-----
```

Saving or transferring this certificate to your Nagios server is covered in the [Save Certificate On Nagios Server](#) section of this KB article.

Sign Using certreq.exe

If you are unable to use the web interface to sign the certificate, you can use the `certreq.exe` program instead. Login to the Windows server that has the Certification Authority role installed.

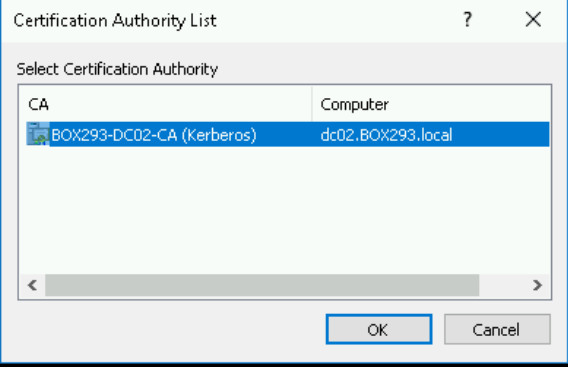
The `certrequest.csr` file from the Nagios server will need to be transferred to this server, you will not be able to paste the request into a form. You can however simply paste the contents into a Notepad file and save it somewhere (the desktop perhaps) with the name of `certrequest.csr`.

Open a command prompt as an administrator and execute the following commands:

```
cd %HOMEPATH%\Desktop
certreq.exe -submit -attrib "CertificateTemplate: WebServer" certrequest.csr certfile.crt
```

This will prompt you which Certification Authority server you want to submit the request to. Select the appropriate one and click **OK**.

```
C:\Users\Administrator.BOX293\Desktop>certreq.exe -submit -attrib "CertificateTemplate: WebServer" certrequest.csr certfile.crt
Active Directory Enrollment Policy
{5B0159C9-27FF-4456-9A4A-C9AAD76214AF}
ldap:
```



A certificate will be issued and saved to the desktop with the name `certfile.crt`. You will need to open this file in a text editor such as Notepad and will appear something like:

```
-----BEGIN CERTIFICATE-----
MIIEszCCA5ugAwIBAgITbwAAAA/Kbjz1BRf/EQAAAAAADzANBgkqhkiG9w0BAQsF
ADAeMRwwGgYDVOQDExNCT1gyOTMtV1NFLVdTRTAyLUNBMB4XDTE3MDYxNDYmDEz
Ml0XDTE3MDYxNDYmDEzMLowazELMAKGA1UEBhMCQVUxDDAKBgNVBAgTA05TVzEP
MA0GA1UEBxMGU31kbmV5MRcwsdfsdQKQew5Cb3gyOTMgUHR5IEEx0ZDEkMCIGA1UE
AxMbeGktcjZ4LXg4Ni5ib3gyOTMtd3NlLmxvY2FzMIIBIjANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEAymjrmOn5tea18eSBGbY07hPMYbkwDMTrwq1DsrKBzQg+
RrEjAmmNs5ZvIsvFF1gVsx1IAASFFFG5M1UU2177buFNR/1D/6h4zwaVVz+8Azuu
Ly8oaD3rWKSnlkT/td1XrBEKb5MUTp8KjxUjC8g/zpRimAzrIgzIzzW913uLXkaf6
DY9QluOJ9ifNtWhE/7OYas08vykwYscZjWEGcxt14qYdh7X4BtOjXFMSrrHyCNgv
8+TYJDnPQIcj1uRiRqTn+qH3U4nDwrym4Leu96vyHc0uO/kx+xtLb6svnYZganyA
jmipa7cnCFdVeClEewSaaaUSGdecEYUeaRKLhc6XwIDAQABO4IBmzCCAzcwHQYD
VR0OBBYEFNMHCbbBpPsVSM7fFv/FGJbB6+zFMB8GA1UdIwQYMBaAFM2vfjWY14mA
xcc5obdaQUbEkOj5MEAGA1UddddQ5MDcwNaAzoDGG2h0dHA6Ly9XU0UwMi9DZXJX
RW5yb2xsL0JPWDI5My1XU0UtV1NFMDItQ0EuY3JsMIHKBggrBgEFBQcBAQSBvTCB
ujCBtwYIKwYBBQUHMAKGgagggGFw0i8vLONOPUJPWDI5My1XU0UtV1NFMDItQ0Es
Q049QUlBLENOPVB1YmXpYyUyMETleSUyMFN1cnZpY2VzLENOPVN1cnZpY2VzLENO
PUNvbmZpZ3VyYXRpb24sREM9Qk9YmjkzLVdTRsxEQz1sb2NhD9jQUN1cnRpZmlj
YXR1P2Jhc2U/b2JqZWNOQ2xhc3M9Y2VydG1maWNhdG1vbkl1dGhvcml0eTAhBgkr
BgEAYI3FAIEFB4SAFcaZQBIAFMAZQByAHYAZQByMA4GA1UdDwEB/wQEAwIFoDAT
BgNVHSUEDDAKBggrBgEFBQcDATANBgkqhkiG9w0BAQsFAAOCQAQEAJdgvH30WjYA
eYcqCCK5Mgjc69GctV3uv/zFMjPWezJegJ+BaC6QzQmC+BP+c5QoHnaJTxeRkZ
qVy+FQKUMqssrOpTfCuOKX8IKTrg7YcXIhycZilT3k/zQySuhAy36QLz18pU0uGa
DMBH+wqLg3r7M8p7oFYE/lzH6+xtFnqFo2juJTXICkeFuX9JwhhtjUIhMvXMxtU+
1PelhLQtgU0jo9CmDYOA40cQaN9z48ZOLmc3oXAYxKLbk1deigzRqj+nv01EA6M
VqYke4frWLnZXNH95AvwXEnV4ctJEw2alhdFelfrcSKvXs+cJnMbawQ+/kAhjK6
TrMfb3j6sQ==
-----END CERTIFICATE-----
```

Saving or transferring this certificate to your Nagios server is covered in the [Save Certificate On Nagios Server](#) section of this KB article.


Save Certificate On Nagios Server

The signed certificate needs to be saved to the Nagios server into the root users home directory with the filename of `certfile.crt`. Execute the following command on your Nagios server to create a new file on your Nagios server:

```
vi certfile.crt
```

When using the `vi` editor, to make changes press `i` on the keyboard first to enter insert mode. Press `Esc` to exit insert mode.

Paste the certificate text into the new file, including the `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` lines.

 When you paste the certificate into `vi`, it's possible that blank lines are added between each line. You will need to **remove** these blank lines as they will cause the certificate file to break.

Save the changes in vi by typing:

```
:wq
```

and press **Enter**.

This completes the steps for signing a certificate with a Microsoft CA. You should now return to the product specific documentation for configuring SSL/TLS to complete the steps to implement this signed certificate.

Final Thoughts

For any support related questions please visit the [Nagios Support Forums](#) at:

<http://support.nagios.com/forum/>

Posted by: **tlea** - Wed, Jun 14, 2017 at 5:28 PM. This article has been viewed 3989 times.

Online URL: <https://support.nagios.com/kb/article/ssl-tls-signing-certificates-with-a-microsoft-certificate-authority-597.html>