App Center Certificate Request Process

Using an Internal Microsoft CA

Abstract:

The intent of this document is to describe the high-level process for both requesting and adding an SSL certificate to App Center when using an internal Microsoft CA. The CA server is a Windows 2008 R2 Enterprise server running AD Certificate Services.

Step 1 - Generating the private key and certificate request

On your App Center server (RedHat or CentOS) run the following commands from a terminal. Please either be logged in as root or prefix each command with sudo.

openssl req -out CSR.csr -new -newkey rsa:2048 -nodes -keyout privateKey.key

During this process you will be prompted for some information. The most important item here is to make sure the "Common Name"/CN that you input will be the Fully Qualified Domain Name (FQDN) of the App Center server. If this does not make the FQDN of your App Center server you will have to repeat this process.

You should now have two files, "CSR.csr" and "privateKey.key" in the same directory that you ran the previous command. You will now need to take the contents of the CSR.csr file and provide them either to your CA admin, or if you have access to generate the certificate yourself take the following steps (or similar).

Example Screenshot of the CSR.csr file opened in gedit (notepad equivalent in linux).



Step 2 - Requesting the SSL certificate

Go to the following URL on your Server 2008 R2 system.

https://nameofyourCAserver/certsrv

Select "request a certificate"

| C Hicrosoft Active Directory Certificate Services - Windows Internet Explorer | | × |
|---|--|----------------------|
| C C k https://acahost/certary/ | 💌 😵 Certificate Error 💿 🍄 🗙 💽 Bing | <u>۹</u> - |
| 🏫 Favorites 🛛 🏤 🖉 Suppested Sites 🔹 🔊 😢 Web Sice Gallery 👻 🖉 Microsoft Active Directory C | | |
| Hicrosoft Active Directory Certificate Services | h + 🔊 - 🖻 🖶 - Page - 1 | Safety + Tools + 🔞 + |
| Microsoft Active Directory Certificate Services symcmobility-AD01-CA | | 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 pon the type of certificate you request, perform other security tasks. | ou communicate with over the Web, sign and encrypt messages, and | d, depending |
| 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 | f 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 | | |
| | | × |
| | Notected Mode: Off | - 100% · |
| 🖉 Start 🔜 🔽 🛄 💽 🕺 📖 😥 | 🖾 io 😫 🖓 🖻 👸 | 4:35 PM |

Select "advanced certificate request"

| Difference Control Active Directory Certificate Services - Windows Internet Explorer | | _ <u>_</u> × |
|---|--------------------------------------|-------------------------------------|
| S S = [2] https://localhest.jortpr.us.ap | 💌 😵 Certificate Error 🖹 🔄 🎸 🗙 🔁 Bing | P • |
| 🚰 Favorites 🛛 🙀 🙋 Suggested Sites 👻 🙋 Web Size Gallery 👻 🖉 Microsoft Active Directory C | | |
| Blarosoft Active Directory Certificate Services | 👌 • 🖾 - 🖾 | 🚔 🔹 Page 👻 Safety 👻 Tools 👻 😧 🕶 |
| Himmond Astron Directory Catilicate Services commonshifts ADM PA | | Homo |
| microsoft Active Directory Centincare Centres | | <u>nome</u> |
| Request a Certificate | | |
| Select the certificate type: | | |
| User Certificate | | |
| Or, submit an advanced certificate request. | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | * |
| https://localhost/certsrv/certraged.asp | 💦 🚱 Local intranet Protected M | ode: Off 🥢 🖓 🔹 🕅 100% 🔹 // |
| 🖉 Start 🔚 🖉 📜 🥵 🚱 | 📼 🎨 | 🔒 🔇 🏱 📆 🅼 🝪 4:36 PM 10/26/2012 🎞 |

Select "Submit a certificate request by using a base-64-encoded CMC..."

| C Hicrosoft Active Directory Certificate Services - Windows Internet Explorer | | _ 8 × |
|--|--------------------------------------|---------------------------------|
| 🚱 🕑 💌 👔 https://boahost/certrojd.asp | 💌 😵 Certificate Error 🛛 🗟 🐓 🗙 💽 Bing | P • |
| 🔆 Favorites 🛛 🎪 🖻 Suggested Step 👻 🕑 Web Sice Gallery 👻 🖉 Microsoft Active Directory C | | |
| Blacosoft Active Directory Certificate Services | 🛅 • 🗟 · 🖻 🖷 | 🕴 🔹 Page 🔹 Safety 👻 Tools 👻 🔞 👻 |
| Microsoft Active Directory Certificate Services - symcmobility-AD01-CA | | Home |
| | | |
| Advanced Certificate Request | | |
| The policy of the CA determines the types of certificates you can request. Click one of the following options to: | | |
| Create and submit a request to this CA. | | |
| Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file. | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | <u> </u> |
| | Local intranet Protected Mode | : Off 🛛 🖓 🔹 🔍 100% 🔹 // |
| Astart 📇 🛛 📜 🧐 🧟 | 📼 🍖 😫 | OP 10/26/2012 |

Paste in the contents from the CSR.csr file into the "Base-64-encoded certificate request" box and from the "Certificate Template" drop-down select "Web Server" and click submit.

| C Microsoft Active Directory Certificate Services - Windows Internet Explorer | | <u>_8×</u> |
|---|---|-----------------------|
| C . v R https://dcahost/cetrsv/certsyt.asp | 💌 😵 Certificate Error 🛛 😂 🔸 🔁 Bing | P - |
| 🙀 Favorites 🛛 🎪 🖻 Suggested Stes 🔻 🖉 Web Sice Gallery 👻 🖉 Microsoft Active Directory C | | |
| 6 Microsoft Active Directory Certificate Services | 🏠 • 🔂 - 🗅 🚔 • Page • Safe | ety + Tools + 🔞 + |
| | | A |
| Microsoft Active Directory Certificate Services symcmobility-AD01-CA | | 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 sector and the 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 sector and the 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 sector and the 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 sector and the 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 sector and the saved request to the saved request | ernal source (such as a Web server) in the Saved Request box. | |
| Saved Request: | | |
| Base-64-encoded Labov071_s01abc11451ac/2abg1atliCTL/n4 Base-64-encoded Labov07174-0G0E10alsEVCK1254cCH1310gg2/be4 centification request Labov07174-0G0E10alsEVCK1254cCH1310gg2/be4 CMC or LEBusch-C25evC340382CGayr2amt54sQ01acK1020F0C PKCS #10 or END CERTIFICATE REQUEST | | |
| Certificate Template: | | |
| Web Server | | |
| Additional Attributes: | | |
| Attributes: | | |
| Submit > | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | Cocal Intranet Protected Mode: Off | • • 100% • |
| Afstart 🛃 🛛 🥞 🕵 👺 🥭 | 🔤 🍖 😫 🗭 陀 🏭 🕼 | 4:37 PM 10/26/2012 |

You should now have an option to download the issued certificate either "DER encoded" or "Base 64 encoded". SELECT BASE 64 ENCODED for both the "Download Certificate" and "Download Certificate Chain"

| Ø Microsoft Active Directory Certificate Services - Windows Internet Explorer |
|--|
| Co Co v 🖉 https://localhost/certsrv/certfnsh.asp |
| 🔆 Favorites 🙀 🙋 Suggested Sites 🔹 🙋 Web Slice Gallery 🔹 🙋 Microsoft Active Directory C |
| Microsoft Active Directory Certificate Services |
| Microsoft Active Directory Certificate Services symcmobility-AD01-CA |
| Certificate Issued |
| The certificate you requested was issued to you. |
| O DER encoded or O Base 64 encoded O Base 64 encoded |
| Download certificate Download certificate chain |
| |
| |
| |

As a second to final step you will need to convert the "Certificate Chain" file you just downloaded from P7B to PEM format. First make sure you copy both those the aforementioned files to your App Center server. Now, you can do this by running the following command, where certificatechain.p7b is the "certificate chain" you downloaded from the CA server and certificatechain.cer will be the name of the converted certificate.p7b file.

openssl pkcs7 -print_certs -in certificatechain.p7b -out certificatechain.cer

You should now have the following files

- privateKey.key
- certnew.cer (this is the default name of the SSL certificate that is issued from the Microsoft CA server).
- certificatechain.cer (the certificate chain file we just converted in the last step)

Step 3 - Selecting the certs to upload

These files will be uploaded to the App Center during the configuration process. Per the screenshot below, the signed certificate (certnew.cer) should be pointed to by the "SSL Certificate File". the privateKey.key (from step 1) should be pointed to by the "SSL Key File", and the certificatechain.cer (that we converted previously from p7b), should be pointed to by "SSL CA Certificate Bundle".

| 🔍 Applications Places System 河 🛞 | | | | | 1 | 9:28 PM 🔇 |
|--|-----------------------------|---------------------------------------|--------------------------------|---------------------------------|---|-----------|
| 8 | 2 | Nukona App | Center Configurate | or - Mozilla Firefox | Security Undates Available | > |
| <u>File Edit View Terminal Tabs Help</u> | File Edit View History Boo | okmarks <u>T</u> ools <u>H</u> elp | | | The second | |
| Removing s3syncvoll task in /etc/cron.d/nukona.sh (unneeded in ISOs) | Connecting | × 🛛 openssi gen | erate certificate r × | • | There are Z package updates availa | able. |
| Removing local YUM ISO repository - /etc/yum.repos.d/nuk.repo | | 1 cm - 1 | | | View Updates | |
| Checking symbolic links. | | config | | ☆ - L | | |
| Lnanging "owner:group" of folders to "apache:apache" | Most Visited T Ded Hat | Red Hat Magazine | Bod Hat Natwork | Red Hat Support | | |
| /sbin/chkconfig monit off | Most visited · | A Reu Hat Magazine | Red Hat Network | Red Hat Support | | |
| Disabling httpd until configuration complete. | NURCONA | | Configure Nuls | ana Ann Cantar | • | |
| /sbin/chkconfig httpd off | NORGINA | | Configure Nuki | ona App Center | | <u> </u> |
| Configuring service startup - postfix | Beenword | | | | | |
| Configuring service startup - nukconfig | Fassword. | | | | | |
| /sbin/chkconfiglevel 235 nukconfig on | Use External Database: | | | | | |
| Please configure 🞾 certs 💷 🗙 | | | | | | |
| Installation can Ele Edit View Places Help | CCI Information | | | | | |
| (usr/local/hu | SSL mormation | | | | | |
| 126/0ct/2012 20: arcs | | | | | | |
| 26/0ct/2012 20: | Set up Apache with SSL?: | | | | | |
| (26/0ct/2012 20: CA_Chain.p7b) CertRequestChain. CertRequestSigned. | SSI Cartificata Eila | /root/Deskton/certs/Ce | artBerry Browse Mu | et have a common-name (CN) w | ith the hortname and domain | |
| [26/0ct/2012 20: Cer Cer | SSL Centificate File. | Лоористине | stated browsen. Int | at have a common hame (on) w | an me nostrane and domain | |
| 26/0ct/2012 20: | SSL Key File: | /root/Desktop/certs/pri | ivateKi Browse Mu | st NOT have a password on the f | file! | |
| 26/Oct/2012 20: CrA2E 0 19/F | SSL CA Certificate Bundle | /root/Desktop/certs/Ce | ertRegi Browse | | | |
| (26/Oct/2012 20: CSR.csr privateKey.key | | | | | | |
| [26/0ct/2012 20: | | | | | | |
| 26/0ct/2012 20: (26/0ct/2012 20: | Email Information | | | | | |
| [26/0ct/2012 20: | | | | | | |
| 26/0ct/2012 20: | Please enter your email ser | ver information here | If you are using a pro | xy, you probably need to | enter a username and password. If | 3 |
| (26/0ct/2012 20: | unauth anticated mail cases | · · · · · · · · · · · · · · · · · · · | | | weed | |
| [26/0ct/2012 20: Certis - CA_chain.p/b selected (50 kb) | unaumenticated mail serve | r on port 25 (for examp | pie), you may not nee | ed a usemame and passi | word. | |
| [26/0ct/2012 20:50:00] "GET /static/images/ul-og_gtass_05_tttttt_1X400.png HTTP [26/0ct/2012 20:50:07] "POST /seekey HTTP/1 1" 200 56 | - | | an ait as une ann a billte a a | | | |
| [26/0ct/2012 20:51:29] "POST /config HTTP/1.1" 500 81275 | Email Proxy Host: | | Inall.symemobility.co | | | |
| [26/Oct/2012 20:54:24] "POST /config HTTP/1.1" 500 81275 | E-mail Dearer Banto | | 25 | | examples: 25: SMTP, 587: SMTP-TLS, 465: SM | |
| [26/0ct/2012 20:55:02] "GET /config HTTP/1.1" 200 14086 | Email Proxy Port: | | (legacy) | | | |
| [26/0ct/2012 20:55:02] "GET /static/jquery.min.js HTTP/1.1" 304 0 [26/0ct/2012 20:55:02] "GET /static/iguery.ui 1 8 14 custom min is HTTP/1 1" 30 | Email Broxy Lloor (optional | \- | | | = | |
| [26/0ct/2012 20:55:02] "GET /static/jquery-ui-1.8.14.custom.min.js HTTP/1.1" 304 0 | Email Floxy Oser (optional | <i>j</i> . | | | | |
| [26/0ct/2012 20:55:02] "GET /static/site.css HTTP/1.1" 304 0 | Email Proxy Password (rec | quired if username | | | | |
| [26/0ct/2012 20:55:02] "GET /static/nukona_white.png HTTP/1.1" 304 0 | given): | | L | | | |
| [26/Oct/2012 20:55:02] "GET /static/page_bg.jpg HTTP/1.1" 304 0 | Email Provy Password (co | nfirm): | | | | |
| [26/0ct/2012 20:55:02] OET /static/top_bar_bg.png HTP/1.1" 304 0 | Email Floxy Password (con | ining. | L | | | |
| [26/Oct/2012 21:12:46] "POST /config HTTP/1.1" 200 14279 | Submit | | | | | |
| | 3 | | III | Wai | iting for localhost | |
| 😸 🛛 🕼 [root@myappcenter:] 🔳 root@myappcenter: 🧕 🕲 Nukona App Center 🧐 Dov | nloads 🛛 🙀 root |) 🎾 D | esktop | 📁 certs | 🔳 root@myappcenter: 📃 | 6 |

Caveats:

Because I was using my own internal CA, none of my iOS or really any other devices outside my AD infrastructure, will trust this SSL certificate. Therefore, you must download the CA's root certificate and import it into each devices trusted certificate store. THis can be done a number of ways, on Windows systems simply use the Certificates MMC snap in, for iOS devices you can use the iPCU. In either case, the same site I browsed to to request my certificate from (https://nameofyourcaserver/certsrv) will have a download link/area similar to the screenshot below. Use that to import into your devices OS. Again, Base 64 is the encoding option that should be used.

| C Hicrosoft Active Directory Certificate Services - Windows Internet Explorer | | X |
|--|--|-----------------------------|
| 🚱 🕙 💌 😰 https://bcahost/cetsrv/cetsarc.asp | 👻 😵 Certificate Error 🛛 🗟 🖘 🗙 🗔 Bing | <u>۹</u> - |
| 🖕 Favorites 🛛 🎪 🙋 Supposed Sites 🔹 🔊 Web Sice Gallery 👻 🖉 Microsoft Active Directory C | | |
| 🛞 🔹 🍘 Karosoft Active Directory C 🧭 Marosoft Active Director 🗴 | 🟠 • 🗔 - 🗆 🖶 • | Page • Safety • Tools • 😧 • |
| Microsoft Active Directory Certificate Services symcmobility-AD01-CA | | Home |
| Download a CA Certificate, Certificate Chain, or CRL | | |
| To trust certificates issued from this certification authority, install this CA certificate chain. | | |
| To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method. | | |
| CA certificate: Current [symcmobility-AD01-CA] | | |
| Encoding method: | | |
| C DER C Base 64 | | |
| Download CA certificate Download CA certificate chain Download Latest base CRL Download latest date CRL | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | 💦 🚱 Local intranet Protected Mode: Off | √ + 100% + |
| Afstart 🐰 🛛 🎇 🧔 🚊 👰 😥 | | P 🗐 🕼 🖏 10:19 PM 10/29/2012 |