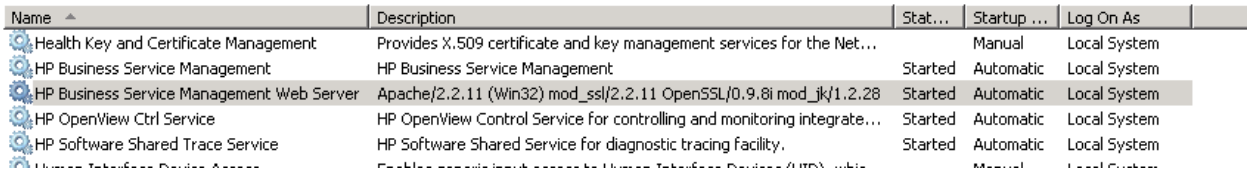
Enabling SSL on Apache for BSM 9.x

The steps involved in enabling SSL on the out-of-the-box Apache web server installed with BSM 9.x on windows are as follows:

1. Confirm you can access BSM via Apache without SSL enabled
2. Generate a server key (server.key) and obtain or generate a server certificate (server.crt)
3. Modify httpd.conf and httpd-ssl.conf to support SSL
4. Modify BSM Infrastructure settings to notify BSM of the changes
5. Import the certificate into cacerts
6. Test the SSL connection

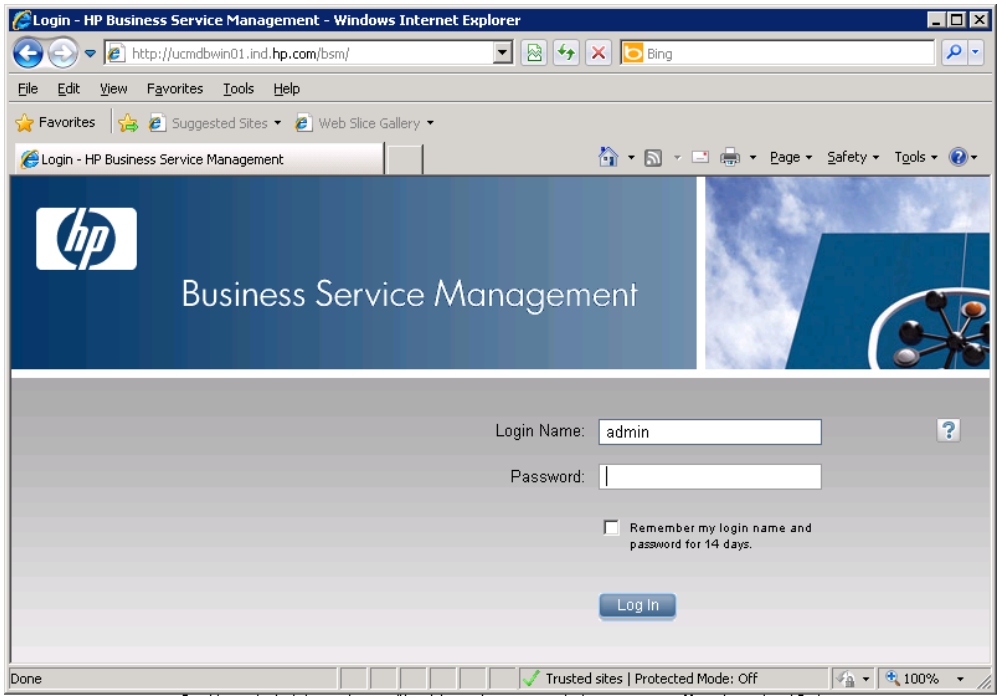
1. Confirm you can access BSM via Apache without SSL enabled

1. First, we start from the basics and confirm that we are indeed dealing with a BSM instance that is using Apache. For this:
   a. On the BSM Gateway server, open <drive>:\HPBSM_postinstall\userInputs.user in notepad
   b. Confirm that the entry "WebServerType=" has the value "Apache" and not "IIS". If it IIS, then the Apache related configuration within this document will not apply.
2. Make sure Apache (named "HP Business Service Management Web Server") has been installed on the Gateway server and is running as a service



Name	Description	Stat...	Startup ...	Log On As
Health Key and Certificate Management	Provides X.509 certificate and key management services for the Net...		Manual	Local System
HP Business Service Management	HP Business Service Management	Started	Automatic	Local System
HP Business Service Management Web Server	Apache/2.2.11 (Win32) mod_ssl/2.2.11 OpenSSL/0.9.8i mod_jk/1.2.28	Started	Automatic	Local System
HP OpenView Ctrl Service	HP OpenView Control Service for controlling and monitoring integrate...	Started	Automatic	Local System
HP Software Shared Trace Service	HP Software Shared Service for diagnostic tracing facility.	Started	Automatic	Local System

3. Next, open the browser and try to access BSM using the URL http://mybsmserver.domain.com/bsm. Replace "mybsmserver.domain.com" with the FQDN of the gateway server that is currently being worked on. You should see the following login page to proceed:



2. Generate a server key (server.key) and obtain or generate a server certificate (server.crt)

If you already have a server certificate (.crt) signed by a trusted CA and a server key (.key), you can proceed to the next step

The following steps describe how to generate a server certificate and server key:

1. Setup the required folders and configure openssl.cnf
    a. Create a folder named "certificates" in the C drive (c:\certificates) and another folder named "newcerts" within the certificates folder (c:\certificates\newcerts)
    b. Backup the file "<drive>:\HPBSM\WebServer\conf\openssl.cnf"
    c. Open "<drive>:\HPBSM\WebServer\conf\openssl.cnf" in notepad and change the following:

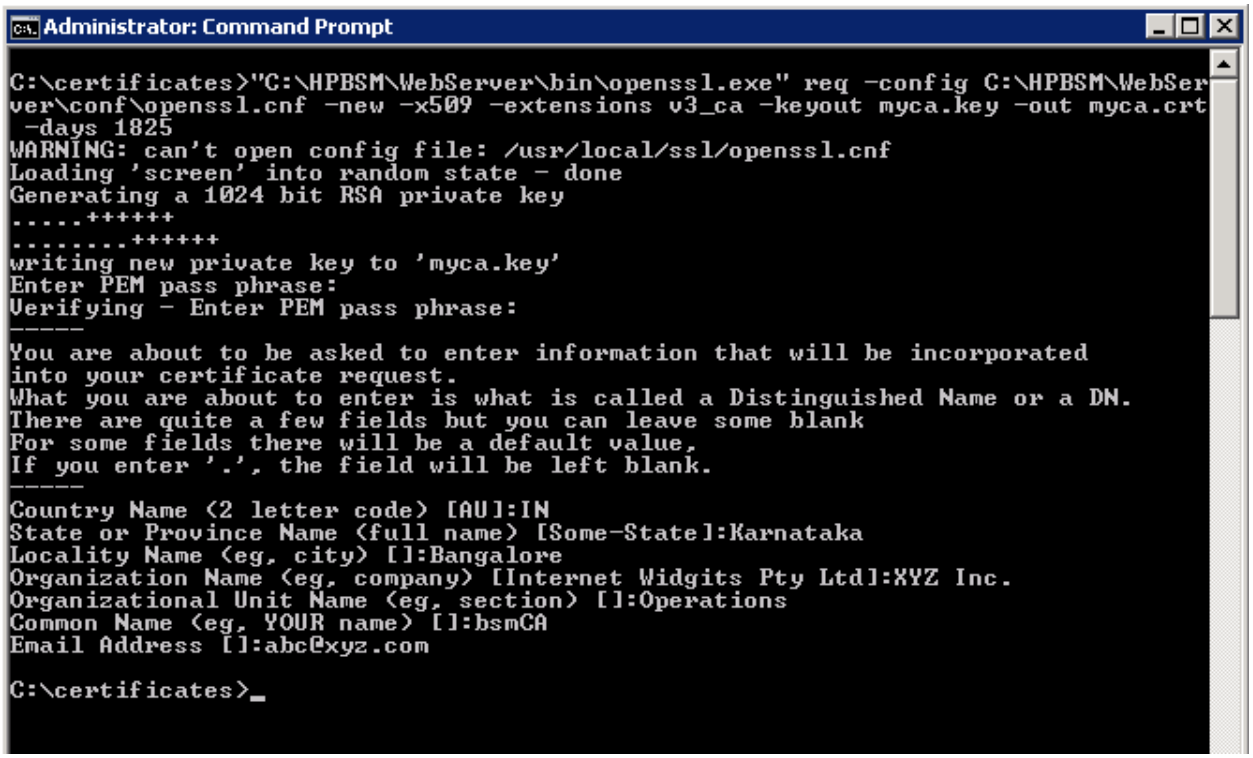
```
[ CA_default ]

dir             = c:/certificates       # Where everything is kept
certs           = $dir                  # Where the issued certs are kept
crl_dir         = $dir                  # Where the issued crl are kept
database        = $dir/index.txt        # database index file.
#unique_subject         = no            # Set to 'no' to allow creation of
                                        # several ctificates with same subject.
new_certs_dir   = $dir/newcerts         # default place for new certs.


certificate     = $dir/myca.crt         # The CA certificate
serial          = $dir/serial           # The current serial number
crlnumber       = $dir/crlnumber        # the current crl number
                                        # must be commented out to leave a V1 CRL
crl             = $dir/crl.pem          # The current CRL
private_key     = $dir/myca.key         # The private key
RANDFILE        = $dir/private/.rand    # private random number file
```

    d. Create an empty text file called "index.txt" under the certificates folder (c:\certificates\index.txt)
    e. Create a text file named "serial" (please note, no extensions) under the certificates folder (c:\certificates\serial). Open the file with notepad and add just one line to it: "01" without the quotes.
2. Open a command prompt and navigate to c:\certificates

3. Generate CA key and certificate. If you plan to get the server certificate signed by a trusted CA (like VeriSign), you can skip this step and move to step 4.
    a. Run the following command, all in one line, to generate a CA certificate and a CA key (replace the drive for BSM as required).

    "C:\HPBSM\WebServer\bin\openssl.exe" req -config C:\HPBSM\WebServer\conf\openssl.cnf -new -x509 -extensions v3_ca -keyout myca.key -out myca.crt -days 1825

    b. Provide the details required while generating the certificate and key. Note down the PEM pass phrase entered – it will be required later. A sample of the output is shown below



    c. You should now see two files created in the c:\certificates directory. One named "myca.crt" and the other "myca.key"

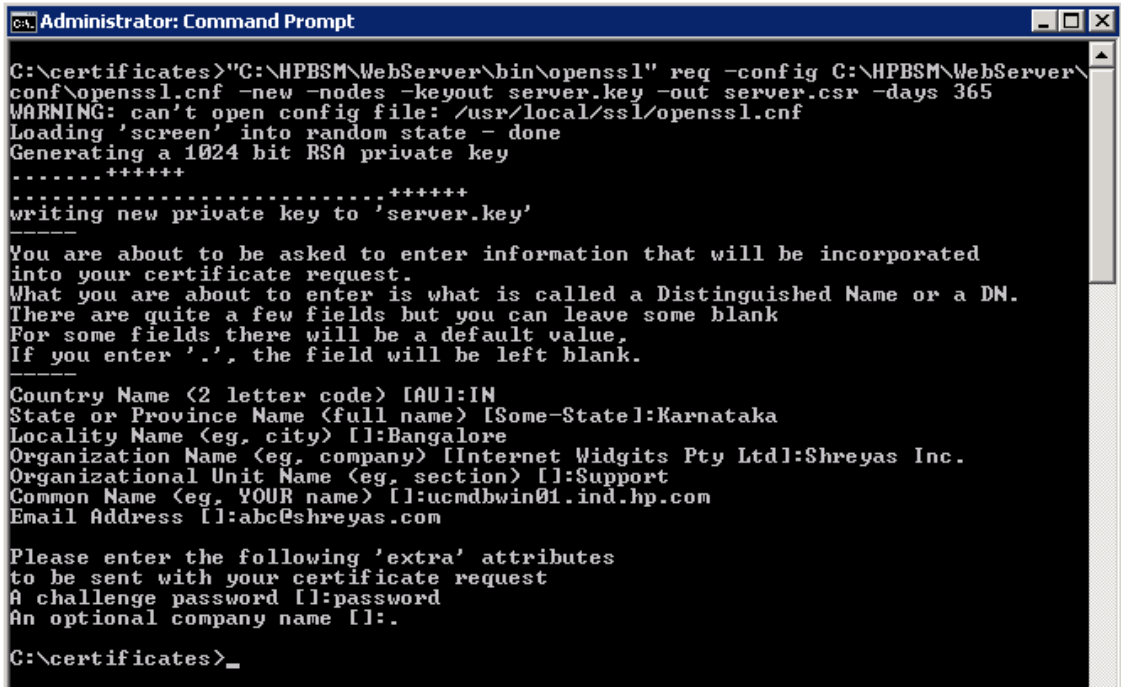
Name	Date modified	Type	Size
.rnd	4/14/2011 6:21 PM	RND File	1 KB
index.txt	4/14/2011 6:21 PM	Text Document	0 KB
myca.crt	4/14/2011 4:26 PM	Security Certificate	2 KB
myca.key	4/14/2011 4:26 PM	KEY File	1 KB
serial	4/14/2011 6:21 PM	File	1 KB

4. Generate a certificate request (.csr) and a server key (server.key)
    a. Run the following command, all in one line, to generate a server certificate request and a server key (replace the drive for BSM as required).

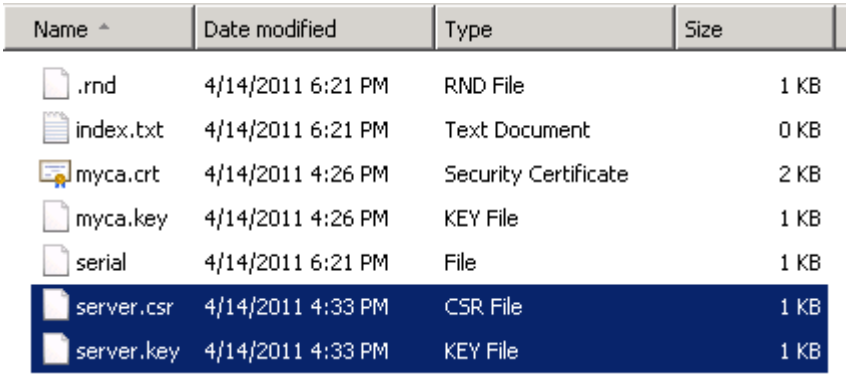
    Important point to remember while generating the certificate: the Common Name MUST be the FQDN of the GW server currently being worked on.

    "C:\HPBSM\WebServer\bin\openssl" req -config C:\HPBSM\WebServer\conf\openssl.cnf -new -nodes -keyout server.key -out server.csr -days 365

    b. Provide the details required while generating the certificate request and key. A sample of the output is shown below.



c. You should now see two more files created in the c:\certificates directory. One named "server.csr" and the other "server.key"

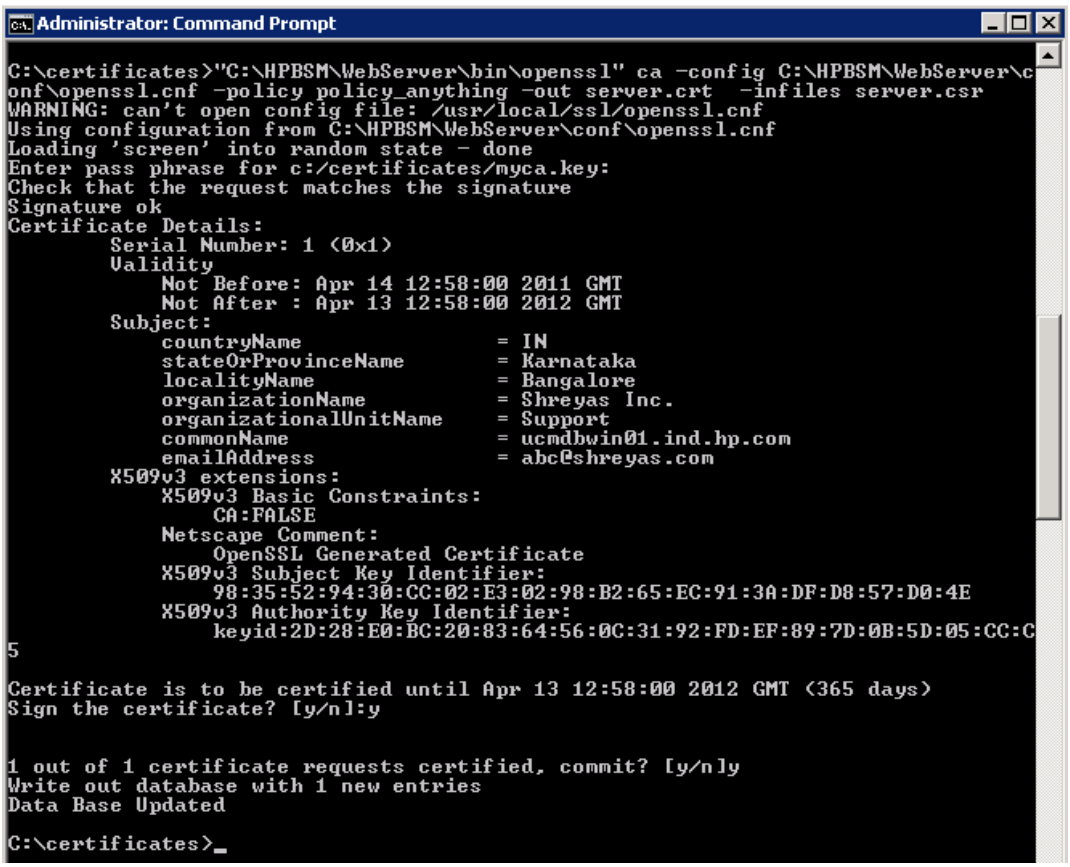


Name	Date modified	Type	Size
.rnd	4/14/2011 6:21 PM	RND File	1 KB
index.txt	4/14/2011 6:21 PM	Text Document	0 KB
myca.crt	4/14/2011 4:26 PM	Security Certificate	2 KB
myca.key	4/14/2011 4:26 PM	KEY File	1 KB
serial	4/14/2011 6:21 PM	File	1 KB
server.csr	4/14/2011 4:33 PM	CSR File	1 KB
server.key	4/14/2011 4:33 PM	KEY File	1 KB

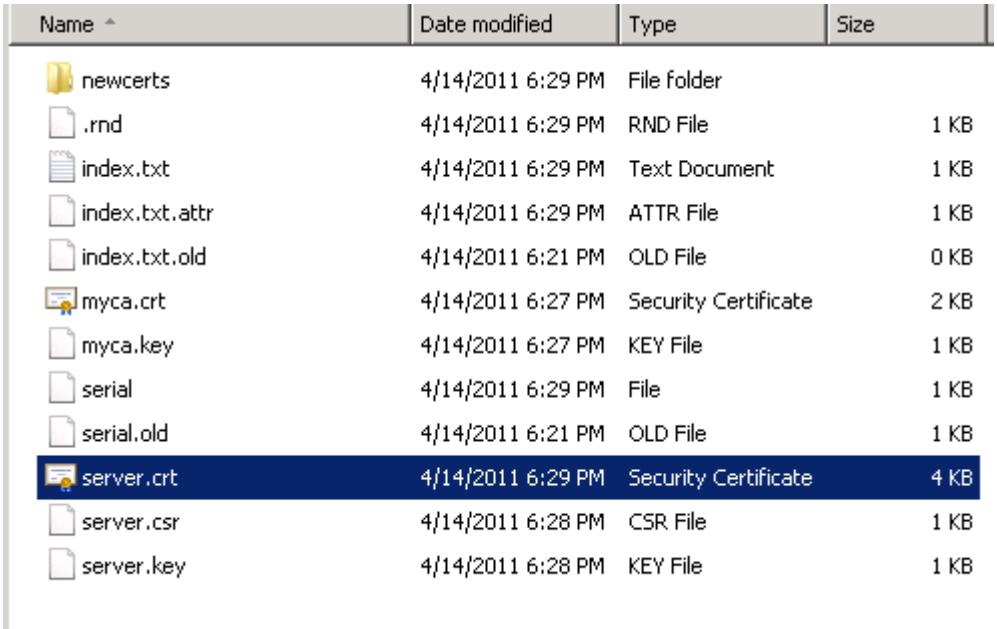
5. Generate a CA signed server certificate from the .csr file. You have two ways to perform this step:
   a. Send the Certificate Request File (.csr) to a trusted Certification Authority (like VeriSign) for signing. If you opt to use this alternative and you have a CA signed server certificate in the .crt format, you could skip to the next step
   b. Sign the Certificate Request File yourself and opt to distribute the CA certificate to the users of the application.
      i. Run the following command, all in one line, to generate a signed server certificate (replace the drive for BSM as required).

      "C:\HPBSM\WebServer\bin\openssl" ca -config C:\HPBSM\WebServer\conf\openssl.cnf -policy policy_anything -out server.crt -infiles server.csr

      ii. Provide the details required while generating the signed certificate. A sample of the output is shown below. Use the Pass Phrase mentioned in step 3b.

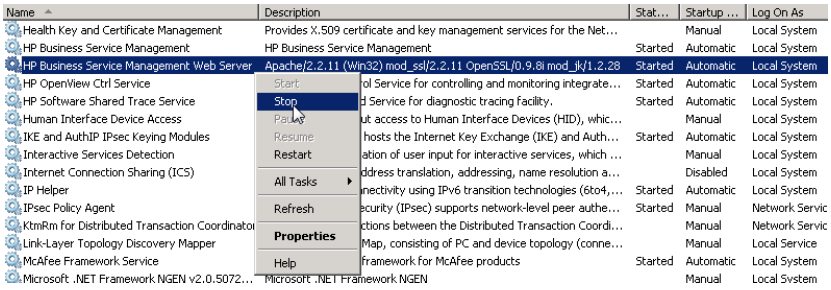


iii. You should now see one more file named "server.crt" created in the c:\certificates directory.



3. Modify httpd.conf and httpd-ssl.conf to support SSL

1. Stop the Apache server from Windows Services pane

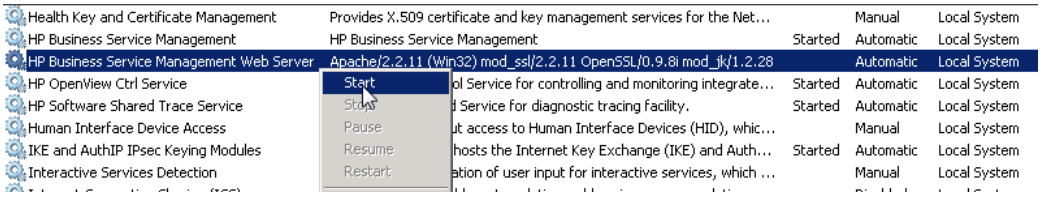


2. Backup the original "C:\HPBSM\WebServer\conf\httpd.conf" file. Adjust the drive as needed in the path mentioned.
3. Copy the server.crt and server.key files generated earlier to "C:\HPBSM/WebServer/conf/"
4. Open "C:\HPBSM\WebServer\conf\httpd.conf" in notepad and modify the following:
   a. Uncomment the following lines (i.e. remove the preceding "#"):
      i. LoadModule ssl_module modules/mod_ssl.so
      ii. Include conf/extra/httpd-ssl.conf
5. Copy the default/httpd-ssl.conf file to extra/http-ssl.conf (backup first):
   a. Make sure the following lines point to the right server certificate and key files:
      i. SSLCertificateFile "C:\HPBSM/WebServer/conf/server.crt"
      ii. SSLCertificateKeyFile "C:\HPBSM/WebServer/conf/server.key"
   b. Make sure the port referenced is correct (alter the port here if you plan to use any other port for SSL in Apache) in the following line:
      i. Listen 443
   c. Make sure SSL engine is switched on in the following line:
      i. SSLEngine on
   d. Also confirm the following lines are in order:

```
##
## SSL Virtual Host Context
##

<VirtualHost ucmdbwin01.ind.hp.com:443>

JkMountCopy On
#  General setup for the virtual host
DocumentRoot "C:\HPBSM/WebServer/htdocs"
ServerName ucmdbwin01.ind.hp.com:443
```

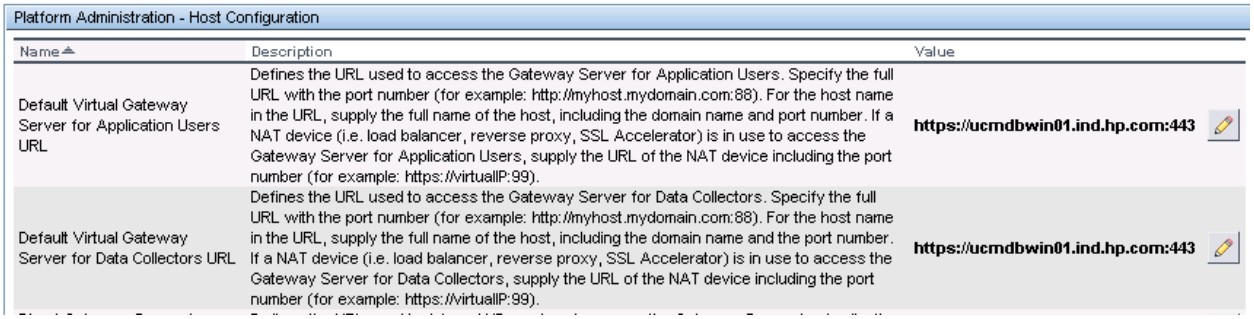
ServerAdmin abc@shreyas.com
ErrorLog "C:\HPBSM/WebServer/logs/error.log"
TransferLog "C:\HPBSM/WebServer/logs/access.log"

6. Start the Apache server from Windows Services pane



4. Modify BSM Infrastructure settings to notify BSM of the changes

1. Login to BSM using the URL http://mybsmserver.domain.com/bsm. Replace "mybsmserver.domain.com" with the FQDN of the gateway server that is currently being worked on.
2. Navigate to Admin → Platform → Infrastructure Settings. Select the "Foundations" radio button and select the "Platform Administration" option in the drop down menu.
3. Look for the section "Platform Administration - Host Configuration". Change the value for parameters "Default Virtual Gateway Server for Application Users URL" and "Default Virtual Gateway Server for Data Collectors URL" to https://mybsmserver.domain.com:443. Replace "mybsmserver.domain.com" with the FQDN of the gateway server that is currently being worked on. If the gateway server is only to be utilized for one of the above two operations (i.e. only for application user access or only for data collectors), then make sure only the relevant parameter is modified.

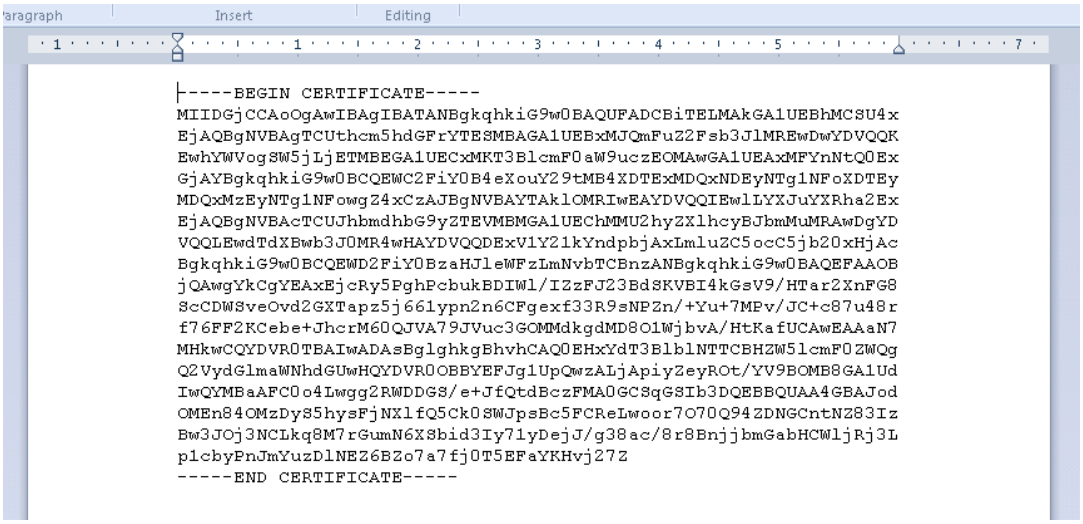

Platform Administration - Host Configuration

Name	Description	Value
Default Virtual Gateway Server for Application Users URL	Defines the URL used to access the Gateway Server for Application Users. Specify the full URL with the port number (for example: http://myhost.mydomain.com:88). For the host name in the URL, supply the full name of the host, including the domain name and port number. If a NAT device (i.e. load balancer, reverse proxy, SSL Accelerator) is in use to access the Gateway Server for Application Users, supply the URL of the NAT device including the port number (for example: https://virtualIP:99).	**https://ucmdbwin01.ind.hp.com:443**
Default Virtual Gateway Server for Data Collectors URL	Defines the URL used to access the Gateway Server for Data Collectors. Specify the full URL with the port number (for example: http://myhost.mydomain.com:88). For the host name in the URL, supply the full name of the host, including the domain name and the port number. If a NAT device (i.e. load balancer, reverse proxy, SSL Accelerator) is in use to access the Gateway Server for Data Collectors, supply the URL of the NAT device including the port number (for example: https://virtualIP:99).	**https://ucmdbwin01.ind.hp.com:443**

4. Restart the BSM service on all servers via Enable and Disable.

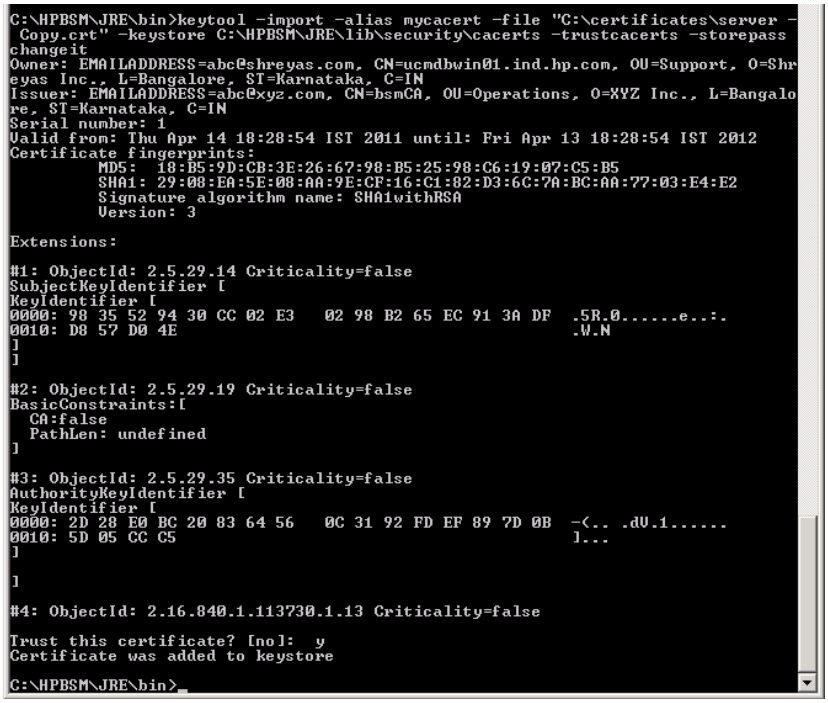
5. Import the certificate into cacerts

1. Make a copy of the server.crt file we generated earlier.
2. Open the copy, in wordpad and delete all lines before "-----BEGIN CERTIFICATE-----". Save the changes. The file contents should now look similar to the following:



3. Run the following command, all in one line, to import the certificate into cacerts (replace "server - Copy.crt" with the name provided to the altered copy of server.crt).

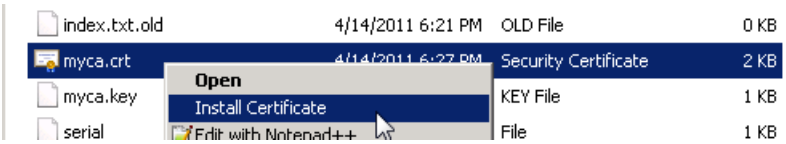
   C:\HPBSM\JRE\bin\keytool -import -alias mycacert -file "C:\certificates\server - Copy.crt" -keystore C:\HPBSM\JRE\lib\security\cacerts -trustcacerts -storepass changeit



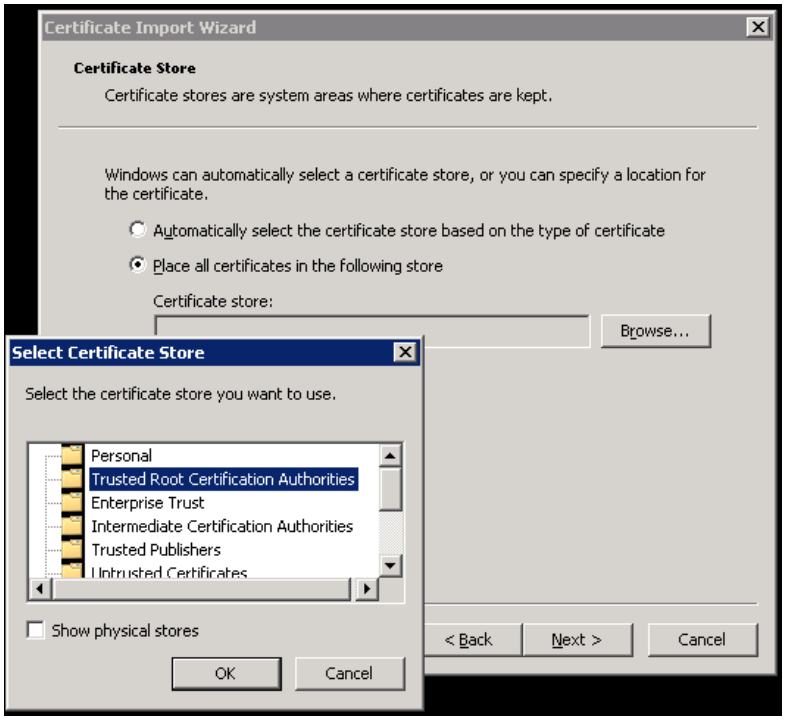
4. Restart the BSM service on all servers via Enable and Disable.

6. Test the SSL connection

1. Import the CA certificate into IE. If you've signed the server.crt using an external trusted CA (i.e. you haven't used the myca.crt created earlier), you can skip to the next step.
   a. Right click the myca.crt file and select "Install Certificate"



   b. Under the "Certificate Store" screen, select "Place all certificates in the following store". Click "Browse" and choose "Trusted Root Certification Authorities" and click OK



   c. Click Finish and choose "Yes" to the Security Warning that is shown.

2. Next, login to BSM using the URL https://mybsmserver.domain.com/bsm. Replace "mybsmserver.domain.com" with the FQDN of the gateway server that is currently being worked on.
3. Confirm that you do not receive any certificate warnings within IE. Also confirm that you are now able to navigate through the various tabs within BSM using HTTPS.