C-Series How to configure SSL

Points of Interest

- The installer for C-Series products will set up HTTP and HTTPS access by default. If you select the option to “Turn on HTTPS only” as part of the installation, ONLY HTTPS connections will be allowed. For details how to disallow access via HTTP and force HTTPS after installation, see the section below on Forcing HTTPS only on Admin and Client web sites.
- The Installer will automatically create a self-signed SSL certificate labelled with the name of server. This certificate is valid for twelve months only.

The sections below detail:

1. Trusting the Self-Signed Certificate - Details of the self-signed certificate generated by the Installer and how to ensure it is trusted by client operating systems and browsers;
2. Forcing HTTPS only on the Admin and Client web sites - How to disable HTTP and allow HTTPS access only if this was not configured at installation-time;
3. How to generate a replacement self-signed certificate – How to generate a self-signed certificate using the java keytool.exe.

For details on how to generate a certificate request for a more formal certificate from a trusted Certificate Authority (VeriSign, Thawte, etc.) refer to resources online:

http://www.verisign.com/support/

https://search.thawte.com/support/ssl-digital-certificates/index?page=content&id=SO2644

Bottomline Technologies Europe

115 Chatham Street, Reading, Berkshire RG1 7JX UK

tel +44 118 925 8250 **fax** +44 118 956 9990 **web** www.bottomline.co.uk

Registered in England No: 1911956

1. Trusting the Self-Signed Certificate

The Installer for C-Series products will automatically create an RSA 1024-bit self-signed SSL certificate labelled with the name of server. As this is a self-signed certificate not associated with a trusted commercial Certificate Authority such as VeriSign or Thwate, the operating system will not automatically trust the certificate. Users will see warnings around untrusted connections when attempting to access web pages of the C-Series product.

Similarly, these instructions apply to any alternative self-signed certificate used, for example, as per the instructions in the section entitled How to replace the self-signed certificate.

The self-signed certificate will need to be added to the Trusted Root Certification Authorities Store in Windows. Depending on the customer's group policies around certificates, this will likely need to be done on each client PC.

The full details for the certificate as created by the Installer will be:

CN = <SERVERNAME>
OU = bottomline
O = bottomline
C = US

The keystore containing the certificate and a pre-exported certificate file are installed in to:

`<installed product path>\jboss\server\default\conf`

Replace *<installed product path>* with the path of the root directory of your installation (e.g. C:\Paybase, D:\WebSeries etc.)

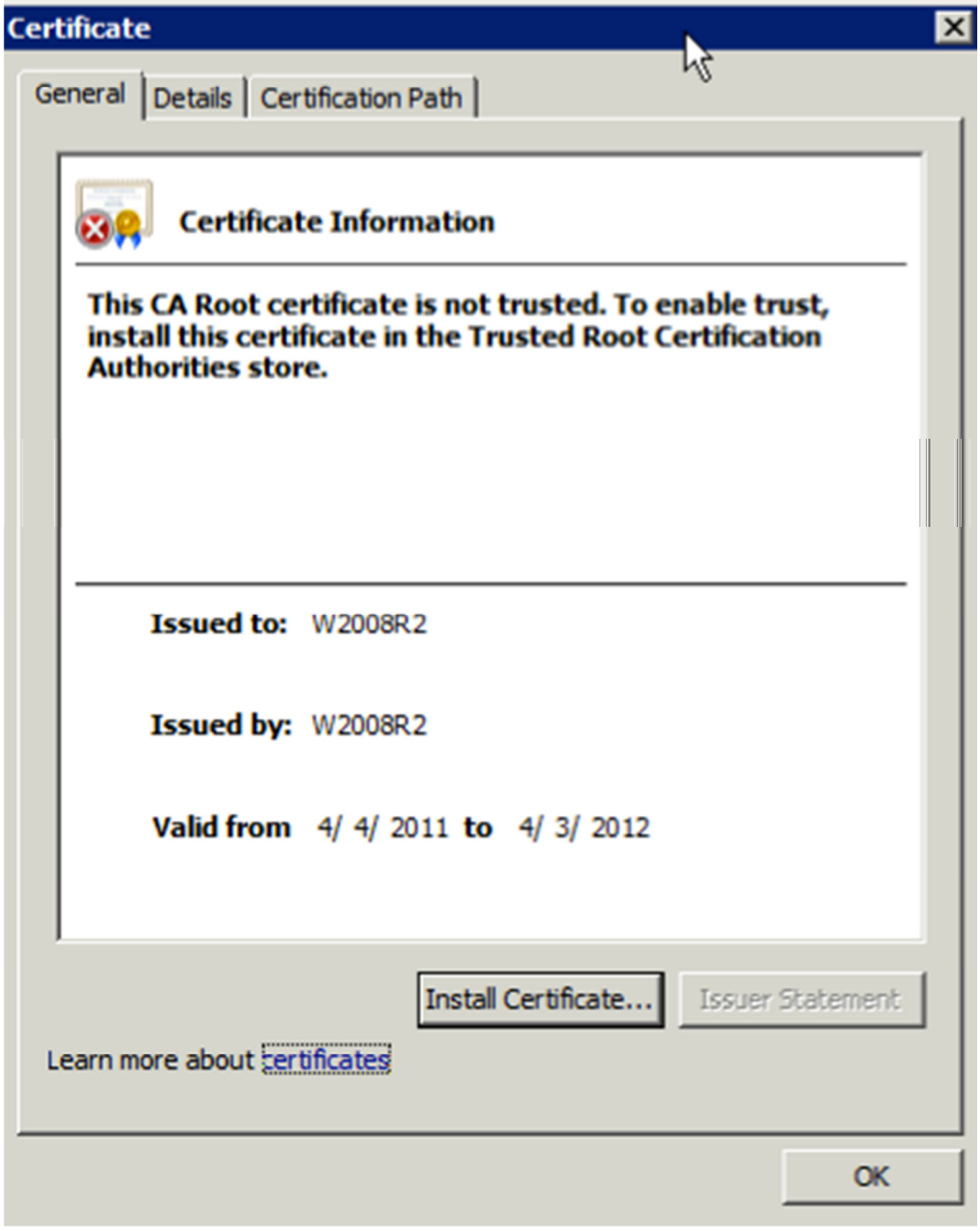
- Keystore File: server.keystore
- SSL Certificate: server.crt

To add the certificate to the Trusted Root store on the server do the following:

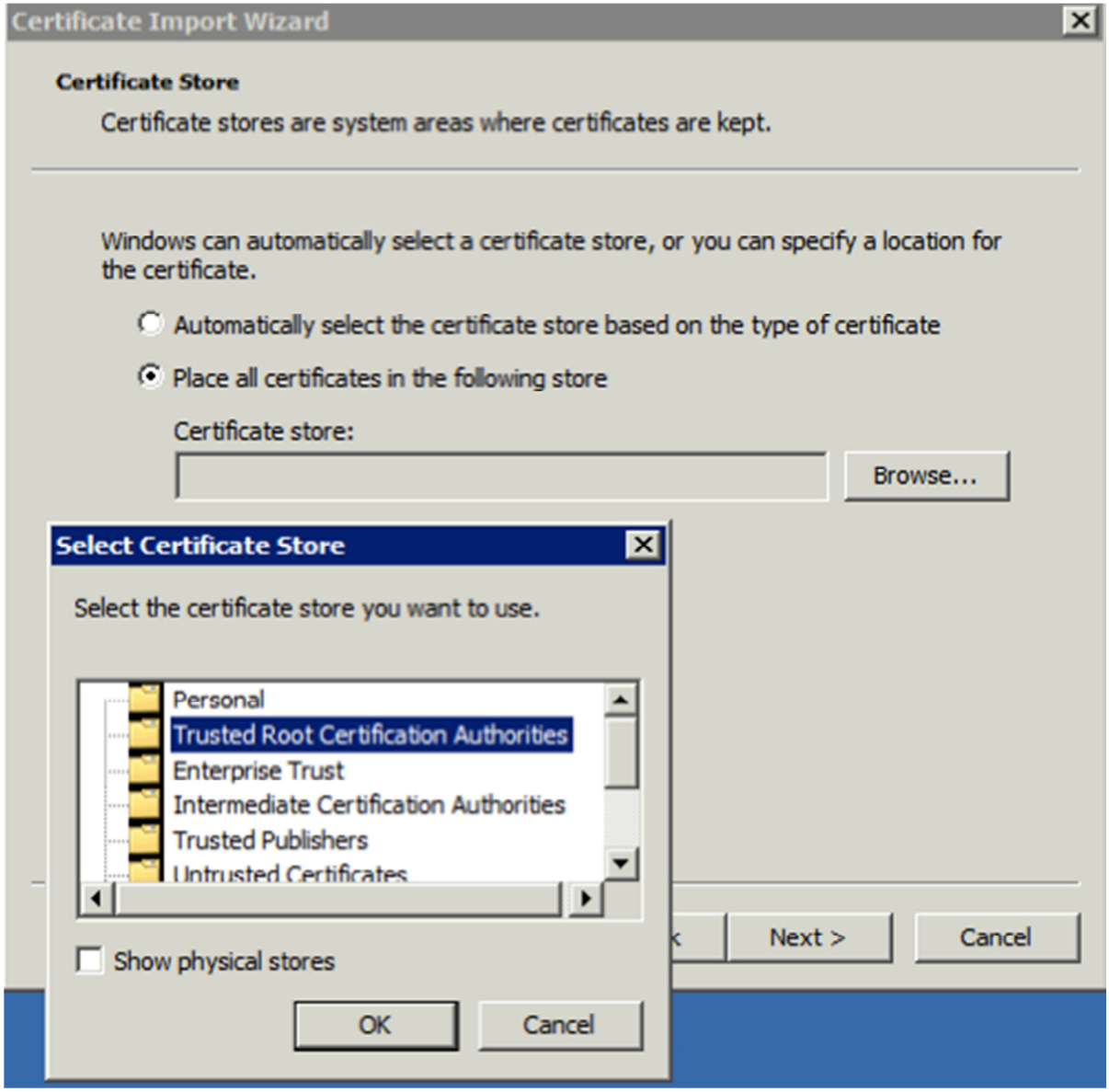
Open (double-click)

`<installed product path>\jboss\server\default\conf\server.crt`

This should launch the Windows Certificate Properties as below.



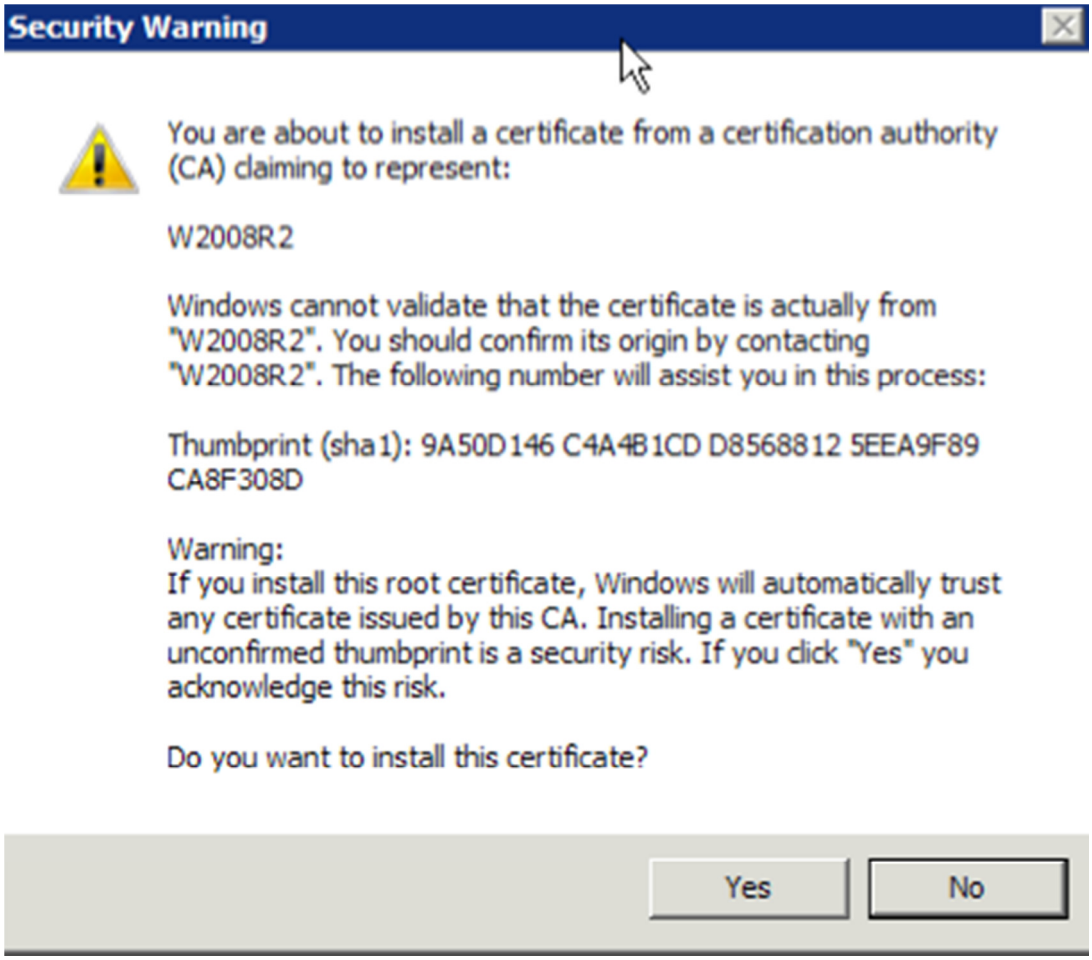
Click on Install Certificate to launch the Certificate Import Wizard, then press Next.



Select the option to “Place all certificates in the following store” then click Browse.

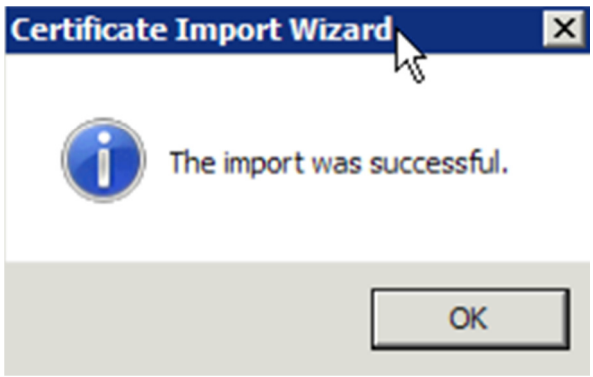
Select Trusted Root Certification Authorities, press OK, then press Next >

Click Finish on the next screen. Next, you will likely see a security warning like the below.



To continue, you **must** select Yes.

You should be notified that the import was successful. If not, please liaise with the IT team around possible Group Policy or other Rights restrictions relating to the import of Root certificates.



2. Forcing HTTPS only on the Admin and Client web sites

To force the use of SSL/HTTPS connections follow the below instructions:

After applying these changes, a user attempting to connect to the admin and client websites using http will be redirected automatically to connect via https. As some content is cached in the browser, the end-user may need to refresh the page for this to become apparent.

Replace *<installed product path>* with the path of the root directory of your installation (e.g. C:\Paybase, D:\WebSeries etc.)

Edit the web.xml file under WEB-INF directory for the admin and client web sites

Admin Web Site:

<installed product path>\jboss\server\default\deploy\webseries-admin.war\WEB-INF\web.xml

Client Web Site:

<installed product path>\jboss\server\default\deploy\webseries-client.war\WEB-INF\web.xml

Take a backup copy of web.xml in both locations then edit the web.xml files and insert the following text between the <web-app> tags (before the closing<\web-app)>.

```
<!-- Force SSL for entire site -->
<security-constraint>

        <web-resource-collection>
                <web-resource-name>Entire Application</web-resource-name>
                <url-pattern>/*</url-pattern>
        </web-resource-collection>

        <user-data-constraint>
                <transport-guarantee>CONFIDENTIAL</transport-guarantee>
        </user-data-constraint>

</security-constraint>
```

As you are “touching” files in the WEB-INF directories, changes should take effect straight away and you do not need to restart any services.

3. How to generate a replacement self-signed certificate

Follow the below instructions to replace the SSL certificate produced by the installer or to generate your own self-signed certificate.

The Installer for C-Series products will automatically create an RSA 1024-bit self-signed SSL certificate labelled with the name of server.

Before proceeding any further ensure that you have taken a backup copy of the server.keystore and server.crt file that which are already in place under:

```
<installed product path>\jboss\server\default\conf
```

We will be using the keytool.exe that ships as part of the Java JRE.
This should be installed under:

```
<installed product path>\java\bin
```

It may be convenient to add this to the PATH. From a cmd prompt, you could issue the following command to add this to your PATH for that session only

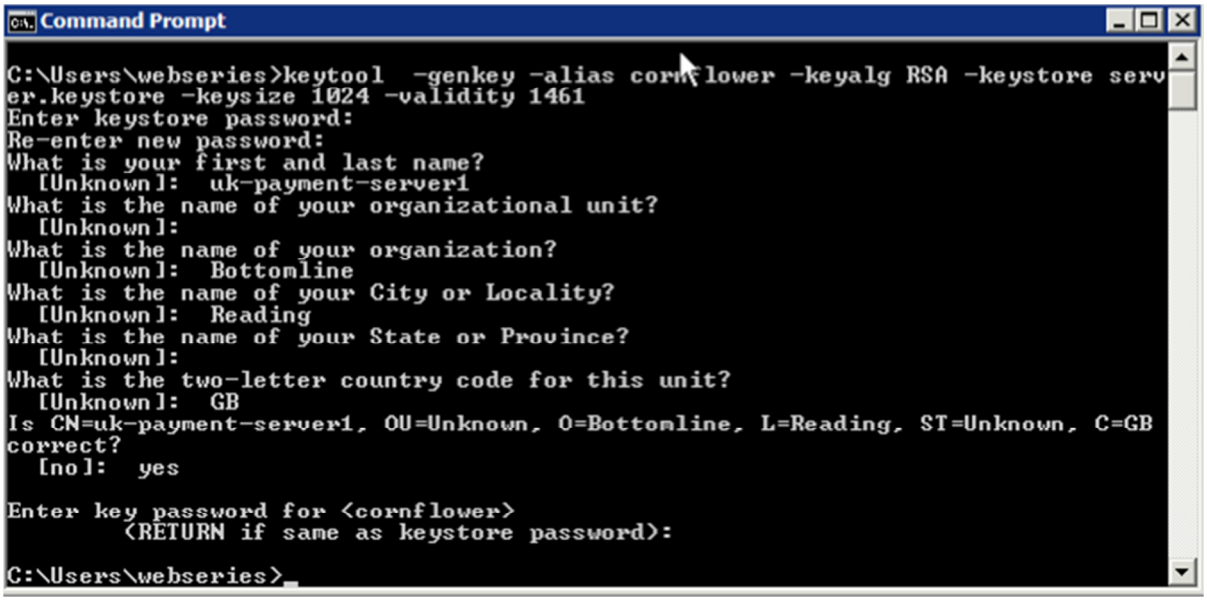
```
Set PATH=%PATH%;<installed product path>\java\bin
```

Open a cmd prompt and issue the following commands:

```
<installed product path>\bin\keytool -genkey -alias cseries -keyalg RSA -
keystore server.keystore -keysize 1024 -validity 1461
```

Adjust the number after the validity switch depending on how long you wish the keys/certificate to be valid. This example uses four years (1461 days including one leap year)

You will be prompted for various details as follows:



For the keystore password, either use the default “changeit” or a password agreed with the customer. Remember the password as it will be needed later on.

Under First and Last Name enter the server name ***in the format that it will be used by users in their browsers.***

For instance if the user-base will use the server name only in their browsers, e.g: **https://uk-payment-server1/PayBase/ux** enter **uk-payment-server1** when asked “What is your first and last name?”

If the fully qualified domain name is to be used, e.g:
https://uk-payment-server1.example.com/PayBase/ux
enter **uk-payment-server1.example.com** when asked “What is your first and last name?”

You will now have a file named server.keystore

Export the certificate from the keystore

In the same cmd prompt (and in the same directory as new server.keystore file) issue the following command:

```
<installed product path>\bin\keytool -export -alias cseries -file
server.crt -keystore server.keystore
```

Enter the keystore password (“changeit” or whatever was chosen) when prompted. The certificate will be stored in a new file named server.crt

Deploying the new key store and certificate

Stop the Bottomline JBOSS Application Server service using the Windows Services control panel.

Copy your server.keystore and server.crt files in to

<installed product path>\jboss\server\default\conf replacing the existing files.

Open the following file in a text editor to ensure that JBOSS uses the new keystore:

<installed product path>\jboss\server\default\deploy\jbossweb.sar\server.xml

Find the section headed <!-- SSL/TLS Connector configuration using the admin devl guide keystore -->

Change the port to port=”443”
and - if appropriate - the keystorePass

From:

```
<!-- SSL/TLS Connector configuration using the admin devl guide keystore -->
  <Connector protocol="HTTP/1.1" SSLEnabled="true"
     port="8443" address="${jboss.bind.address}"
     scheme="https" secure="true" clientAuth="false"
     keystoreFile="c:\WebSeries\jboss\server\default\conf\server.keystore"
     keystorePass="changeit" sslProtocol = "TLS" />
```

To this:

```
<!-- SSL/TLS Connector configuration using the admin devl guide keystore -->
<Connector protocol="HTTP/1.1" SSLEnabled="true"
   port="443" address="${jboss.bind.address}"
   scheme="https" secure="true" clientAuth="false"
   keystoreFile="c:\WebSeries\jboss\server\default\conf\server.keystore"
   keystorePass="changeit" sslProtocol = "TLS" />
```

Save the File.
Start the Bottomline JBOSS Application Server service using the Windows Services control panel.

As this is a self-signed certificate you will need to follow the instructions in Section 1 *Trusting the Self-Signed Certificate*