Adobe Connect on-premise SSL Guide

This is supposed to be a complete SSL configuration guide for Connect on-premise installs of version 9.0 and higher. The first part of this guide is to configure SSL for the application and meeting server (both or just one of the two, then it is also detailed how to configure SSL for the Event services (CQ author and publish server). The examples are all set out for SSL termination in Stunnel. If you want to terminate SSL on your load balancer or SSL accelerator it should not take much effort to take the information from this guide and use it to configure your environment.

If you need assistance, please contact Enterprise Support on the usual support channels.
https://helpx.adobe.com/adobe-connect/connect-support.html

Content

Adobe Connect on-premise SSL Guide 1
- Things you need: 2
- Stunnel installation 2
- Application server SSL only: 3
  - Sample stunnel.conf for Application server SSL only: 3
- Meeting server SSL only: 5
  - Sample stunnel.conf for Meeting server SSL only: 5
- Application and Meeting server SSL: 6
  - Stunnel.conf sample for Application and Meeting server SSL: 7
- Configure SSL for Event Services (CQ author and publish server) 9
  - Stunnel.conf sample for CQauthor and CQpublish SSL 10
  - Configure the Connect server to work with Events over SSL 11
  - Edit the CQ author server config: 11
  - Edit the CQ Publish Server config: 12
  - Check the CRX configuration of the CQ author server is correctly set for SSL. 12
  - Check the CRX configuration of the CQ publish server is correctly set for SSL. 14
  - Import the CQ publish server SSL certificates to the Connect server Java keystore: 17

Things you need:

Depending on what you want to configure SSL for you need to have the following ready:

1. If you want to configure SSL for both application (http) and meeting (rtmp) **you need to have a second IP address** for your server and a have a second DNS entry resolve to the second IP.
2. If you want to configure SSL for both, application and meeting service, **you need to request two certificates for your two names**. I.e. one for "connect.mycompany.com" and one for "meeting01.mycompany.com". (note, the second name used on the meeting server stays hidden from participants). Don't use a passphrase on your SSL keys.
3. If you also want to configure SSL for the AEM based Events service, you'll need two more IPs and two more names and two more certificates.
4. Your certificates should be in a **.pem format** and SSL key and cert should be in separate files.
5. Unless you want to use another external device to terminate SSL such as a load balancer, you will need the **Stunnel installer**, so download the latest and greatest version now: https://www.stunnel.org/downloads.html

Stunnel installation

By now you should have the Stunnel installer downloaded to the server.

To install it, just run the executable. When asked, point it to an install path in your Connect home directory. i.e. C:\Connect\Stunnel\ . It's not required to use this path, but it makes life easier when troubleshooting as all is in one place and it's also more consistent with other configuration guides.

Check if the folder structure contains a folder called */certs/*. If it does not, create it now and place your certificates and key files in it.

Application server SSL only:

1. Configure Stunnel.

a) Copy the contents of the sample config below to your own stunnel.conf file (in C:\Connect\Stunnel\conf\ ) and overwrite whatever is there right now.
b) Configure your own IP address in the sections headed with "application server SSL / HTTPS ". Where it reads "accept=10.1.1.1" just insert your own IP.
c) "Cert =" and "key=" should have the path to your public certificate and private key.
d) Check Stunnel works with your cert and IP by launching it manually
    a. Double click the Stunnel.exe in the /bin/ folder, and then click on the new icon that appeared in the notification area (near the clock, bottom right).
    b. You should see the log output of Stunnel and a line indicating a successful configuration:
        i. *"2016.03.25 11:40:18 LOG5[main]: Configuration successful"*
e) Close the window and exit Stunnel by right-clicking on the icon in the notification area.
f) Now install Stunnel as a Windows service. Open a command line and change to the /bin directory of Stunnel:
    - In the command line run: stunnel.exe –install
    - You will have a new service named: Stunnel SSL wrapper
    - Start the service and check that it is set to automatic start.

Sample stunnel.conf for Application server SSL only:

```
; Protocol version (all, SSLv2, SSLv3, TLSv1)
sslVersion = all
options = NO_SSLv2
options = NO_SSLv3
options = DONT_INSERT_EMPTY_FRAGMENTS
options = CIPHER_SERVER_PREFERENCE
renegotiation=no
fips = no
;Some performance tunings
socket = l:TCP_NODELAY=1
socket = r:TCP_NODELAY=1
TIMEOUTclose=0

; application server SSL / HTTPS
```

[https-vip]
*accept = **10.1.1.1**:443*
connect = 127.0.0.1:8443
*cert = C:\Connect\stunnel\certs**public_certificate_app-server.pem***
*key = C:\Connect\stunnel\certs**private_key_app-server.key***
;configure ciphers as per your requirement and client support.
;this should work for most:
ciphers = TLSv1+HIGH:!SSLv2:!aNULL:!eNULL:!3DES

2. Find the **custom.ini** in c:\Connect\9.x\ and add the following:

ADMIN_PROTOCOL=https://
SSL_ONLY=yes

3. Open C:\Connect\9.x\appserv\conf**server.xml** and uncomment the following two sections:

```
<Connector port="8443" protocol="HTTP/1.1"
           executor="httpsThreadPool"
               enableLookups="false"
                        acceptCount="250"
                          connectionTimeout="20000"
                        SSLEnabled="false"
                        scheme="https"
                        secure="true"
                        proxyPort="443"
                        URIEncoding="utf-8"/>
```

And:

```
<Executor name="httpsThreadPool"
    namePrefix="https-8443-"
    maxThreads="350"
    minSpareThreads="25"/>
```

You're done. Stop and start all services, Adobe Connect, Adobe Media Server and Stunnel.

Meeting server SSL only:

1. Configure Stunnel.

a) Copy the contents of the sample config below to your own stunnel.conf file (in C:\Connect\Stunnel\conf\ ) and overwrite whatever is there right now.
b) Configure your own IP address in the sections headed with "meeting server SSL / RTMPS ". Where it reads "accept=10.1.1.2" just insert your own IP.
c) "Cert = " and "key= " should have the path to your public certificate and private key.
d) Check Stunnel works with your cert and IP by launching it manually:
    - Double click the Stunnel.exe in the /bin/ folder, and then click on the new icon that appeared in the notification area (near the clock, bottom right).
    - You should see the log output of Stunnel and a line indicating a successful configuration:

      "2016.03.25 11:40:18 LOG5[main]: Configuration successful"

e) Close the window and exit Stunnel by right-clicking on the icon in the notification area
f) Install Stunnel as a Windows service. Open a command line and change to the /bin directory of Stunnel:
    - In the command line run: stunnel.exe –install
    - You will have a new service named: Stunnel SSL wrapper
    - Start the service and check that it is set to automatic start.

Sample stunnel.conf for Meeting server SSL only:

```
; Protocol version (all, SSLv2, SSLv3, TLSv1)
sslVersion = all
options = NO_SSLv2
options = NO_SSLv3
options = DONT_INSERT_EMPTY_FRAGMENTS
options = CIPHER_SERVER_PREFERENCE
renegotiation=no
fips = no
;Some performance tunings
socket = l:TCP_NODELAY=1
socket = r:TCP_NODELAY=1
TIMEOUTclose=0

; meeting SSL / RTMPS
[rtmps-vip]
accept = 10.1.1.2:443
```

connect = 127.0.0.1:1935
*cert = C:\Connect\stunnel\certs**public_certificate_meeting-server.pem***
*key = C:\Connect\stunnel\certs**private_key_meeting-server.key***

;configure ciphers as per your requirement and client support.
;this should work for most:
ciphers = TLSv1+HIGH:!SSLv2:!aNULL:!eNULL:!3DESciphers

2. Find the **custom.ini** in c:\Connect\9.x\ and add the following:

RTMP_SEQUENCE=rtmps://external-host:443/?rtmp://localhost:8506/

You're done. Stop and start all services, Adobe Connect, Adobe Media Server and Stunnel.

Application and Meeting server SSL:

1. Configure Stunnel:

a) Copy the contents of the sample below to your own stunnel.conf file (in C:\Connect\Stunnel\conf\ ) and overwrite whatever is there right now.
b) Configure your own IP addresses in the sections headed with "application server SSL / HTTPS " and "meeting SSL / RTMPS". Where it reads "accept=10.1.1.1" or "accept=10.1.1.2" just insert your own.
c) Remember, your names should resolve to those IP addresses by now.
d) "Cert =" and "key=" should have the path to your public certificate and private key.
e) Check Stunnel works with your certs and IPs by launching it manually
    - Double click the Stunnel.exe in the /bin/ folder, then click on the new icon that appeared in the notification area (near the clock, bottom right).
    - You should see the log output of Stunnel and a line indicating a successful configuration:

      "2016.03.25 11:40:18 LOG5[main]: Configuration successful"

f) Close the window and exit Stunnel by right-clicking on the icon in the notification area
g) Now install Stunnel as a Windows service. Open a command line and change to the /bin directory of Stunnel.
    - In the command line run: stunnel.exe –install
    - You will have a new service named: Stunnel SSL wrapper
    - Start the service and check that it is set to automatic start.

Stunnel.conf sample for Application and Meeting server SSL:

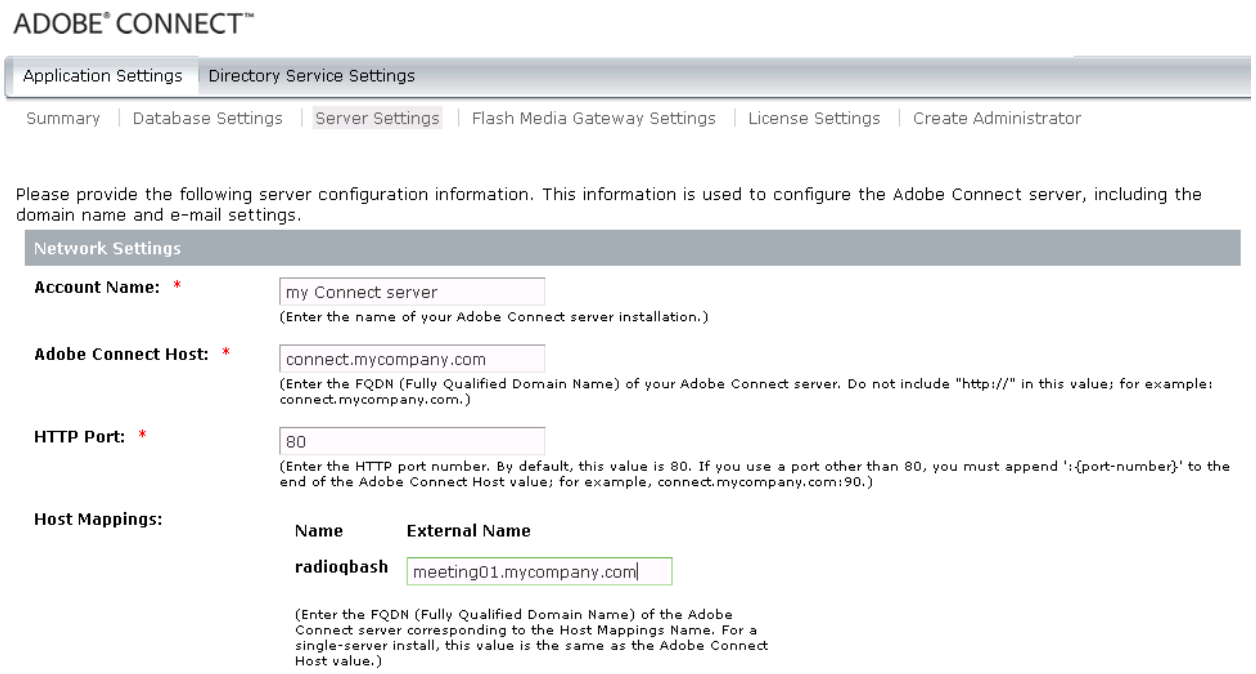
; Protocol version (all, SSLv2, SSLv3, TLSv1)
; we want TLS1, TLS1.1 and TLS1.2 active, so set =all and then say "not SSLv2, SSLv3"
sslVersion = all
options = NO_SSLv2
options = NO_SSLv3
options = DONT_INSERT_EMPTY_FRAGMENTS
options = CIPHER_SERVER_PREFERENCE
renegotiation=no
fips = no
;Some performance tunings:
socket = l:TCP_NODELAY=1
socket = r:TCP_NODELAY=1
TIMEOUTclose=0

; application server SSL / HTTPS
[https-vip]
*accept = **10.1.1.1**:443*
connect = 127.0.0.1:8443
*cert = C:\Connect\stunnel\certs**public_certificate_app-server.pem***
*key = C:\Connect\stunnel\certs**private_key_app-server.key***
;configure ciphers as per your requirement and client support.
;this should work for most:
ciphers = TLSv1+HIGH:!SSLv2:!aNULL:!eNULL:!3DES

; meeting SSL / RTMPS
[rtmps-vip]
*accept = **10.1.1.2**:443*
connect = 127.0.0.1:1935
*cert = C:\Connect\stunnel\certs**public_certificate_meeting-server.pem***
*key = C:\Connect\stunnel\certs**private_key_meeting-server.key***
;configure ciphers as per your requirement and client support.
;this should work for most:
ciphers = TLSv1+HIGH:!SSLv2:!aNULL:!eNULL:!3DES

2. Configure the Connect Server:

a) Open the Connect configuration console at http://localhost:8510/console/
b) Go to “Server Settings” and set the External Name value to the second host name you defined (meeting01.mycompany.com for example as mentioned previously)



c) Click save and close the browser.

3. Find the **custom.ini** in c:\Connect\9.x\ and add the following:

```
ADMIN_PROTOCOL=https://
SSL_ONLY=yes
RTMP_SEQUENCE=rtmps://external-host:443/?rtmp://localhost:8506/
```

4. Open C:\Connect\9.x\appserv\conf**server.xml** and uncomment the following two sections: (just search for the keywords “uncomment for SSL support”)

```
<Connector port="8443" protocol="HTTP/1.1"
           executor="httpsThreadPool"
               enableLookups="false"
                        acceptCount="250"
                          connectionTimeout="20000"
                        SSLEnabled="false"
                        scheme="https"
                        secure="true"
                        proxyPort="443"
                        URIEncoding="utf-8"/>
```

And:

```
<Executor name="httpsThreadPool"
    namePrefix="https-8443-"
    maxThreads="350"
    minSpareThreads="25"/>
```

You're done. Stop and start all services, Adobe Connect, Adobe Media Server and Stunnel.

Configure SSL for Event Services (CQ author and publish server)

(also see here: http://blogs.adobe.com/connectsupport/ssl-configuration-checklist-for-connect-with-aem-based-events/)

Continue here if you also use the Events service (aka CQ) and want to secure its two services.

It is strongly recommended to install CQ on its own machine. Running it on the same machine as Connect can cause performance issues in production. I assume you followed this recommendation and hence we get started with another Stunnel installation.

To install Stunnel on the CQ server just run the Stunnel executable. When asked, point it to an install path in your Connect home directory. i.e. C:\Connect\Stunnel\ . It's not required to use this path, but it makes life easier when troubleshooting as all is in one place and it's also more consistent with other configuration guides.

Check if the folder structure contains a folder called "*certs*". If it does not, create it now and place your certificates and key files in it.

Stunnel.conf sample for CQauthor and CQpublish SSL

```
; Protocol version (all, SSLv2, SSLv3, TLSv1)
sslVersion = all
options = NO_SSLv2
options = NO_SSLv3

options = DONT_INSERT_EMPTY_FRAGMENTS
options = CIPHER_SERVER_PREFERENCE

renegotiation=no
fips = no

;Some performance tunings
socket = l:TCP_NODELAY=1
socket = r:TCP_NODELAY=1
TIMEOUTclose=0


; CQ author / HTTPS
[cqauthor-vip]
accept = 10.1.1.3:443
connect = 127.0.0.1:4502
cert = C:\Connect\stunnel\certs\cqauthor-cert.pem
key = C:\Connect\stunnel\certs\cqauthor-key.key

;configure ciphers as per your requirement and client support.
;this should work for most:
ciphers = TLSv1+HIGH:!SSLv2:!aNULL:!eNULL:!3DES


; CQ publish / HTTPS
[cqpublish-vip]
accept = 10.1.1.4:443
connect = 127.0.0.1:4503
cert = C:\Connect\stunnel\certs\cqpublish-cert.pem
key = C:\Connect\stunnel\certs\cqpublish-key.key

;configure ciphers as per your requirement and client support.
;this should work for most:
ciphers = TLSv1+HIGH:!SSLv2:!aNULL:!eNULL:!3DES
```

Configure the Connect server to work with Events over SSL

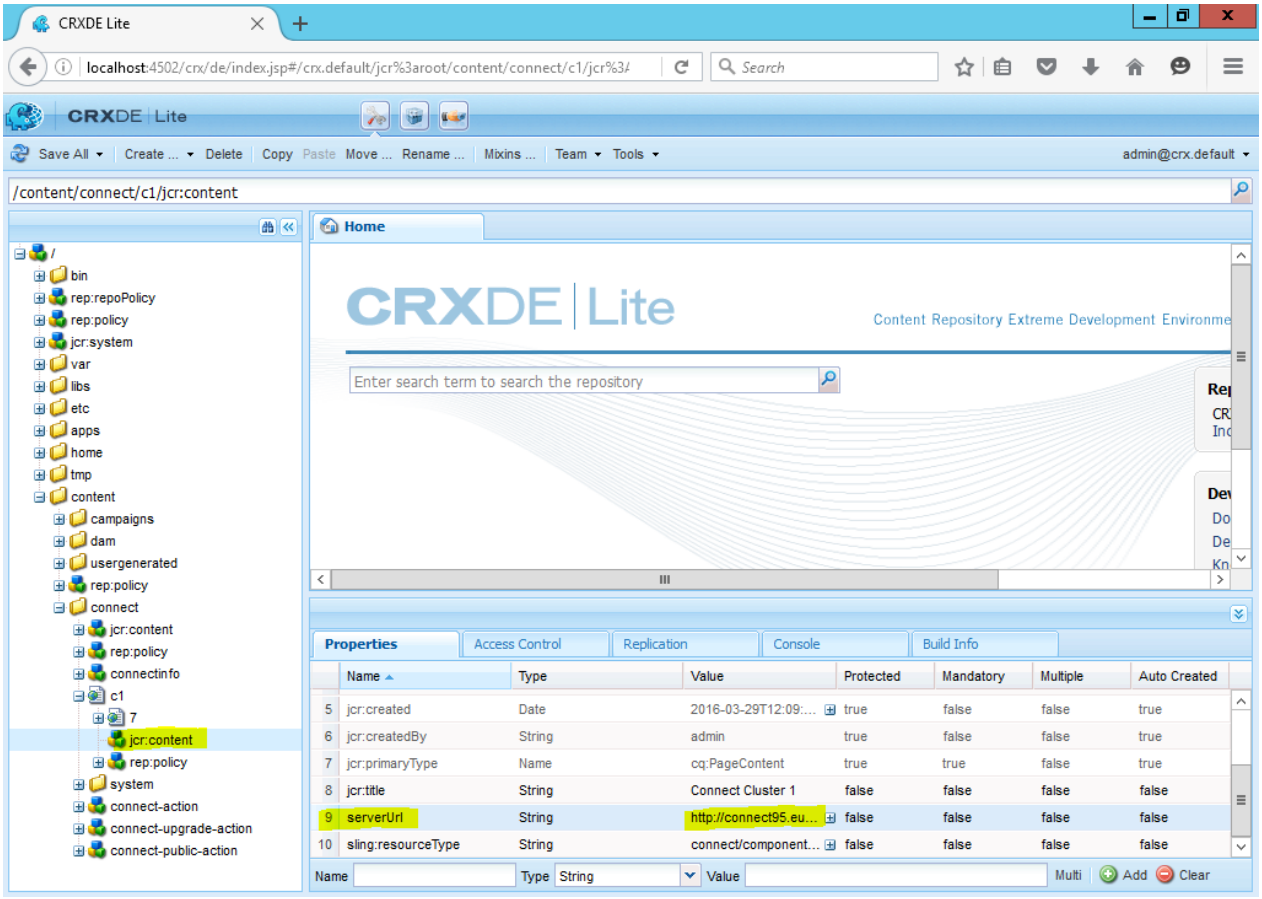
1. On the Connect server open the custom.ini in \Connect\9.x\
2. Add or modify the following lines:

DOMAIN_COOKIE=.mycompany.com
*CQ_AUTHOR_SERVER=https://**cqauthor.mycompany.com***
*CQ_PUBLISH_SERVER=https://**cqpublish.mycompany.com***

Edit the CQ author server config:

Login at http://localhost:4502/ with the CQ admin credentials you set during install.

1. Scroll down and click on “CRXDE Lite”
2. In the folder tree on the left, go to /content/connect/c1/jcr:content/
3. edit the value of property “serverURL” to the one you set as your Connect Host name and prefix https, i.e. https://connect.mycompany.com:443



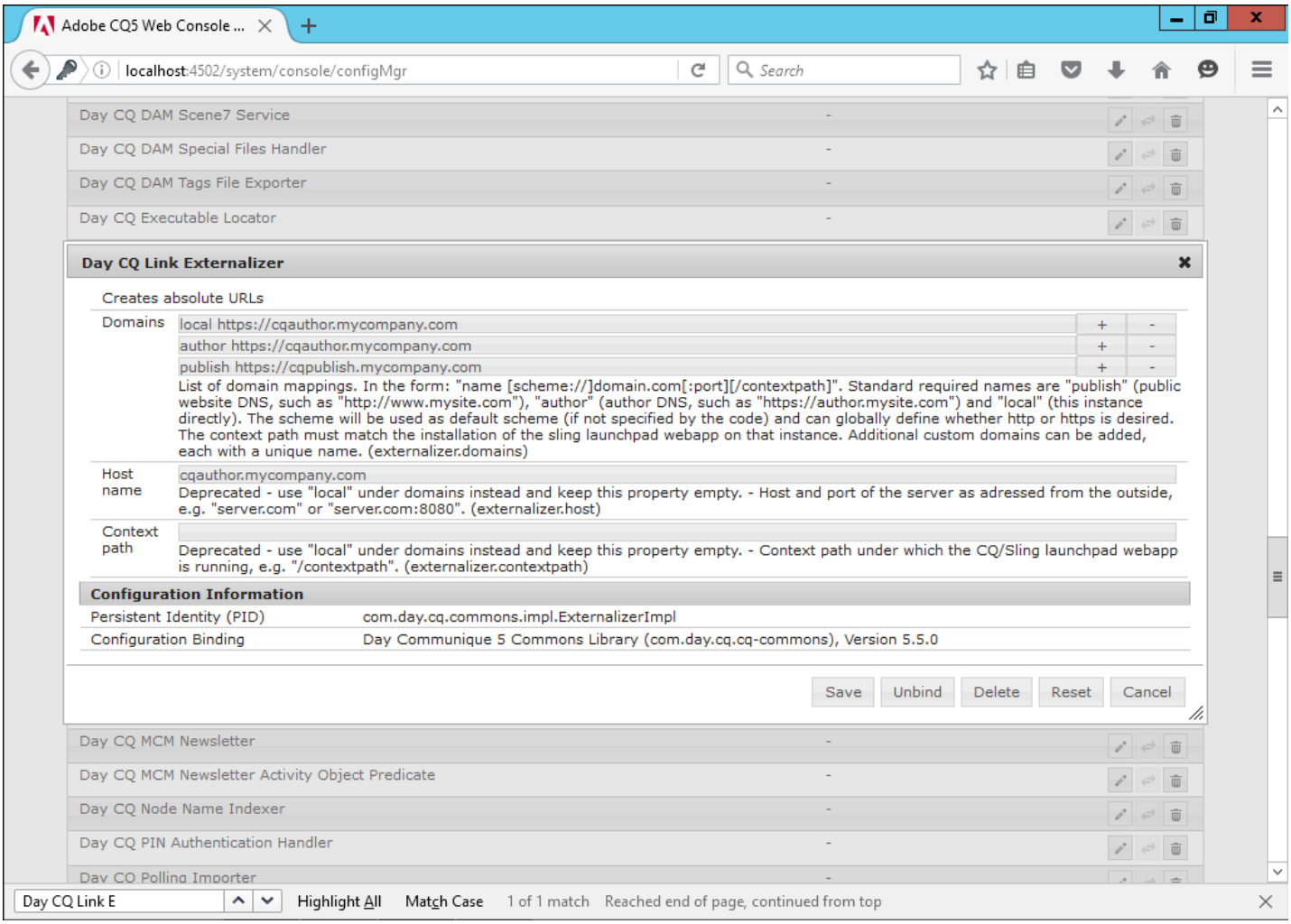
4. Click on “Save All” at the top left to save the change.
5. Log out by clicking on the drop down menu at the top right where it reads admin@crx.default.

Edit the CQ Publish Server config:

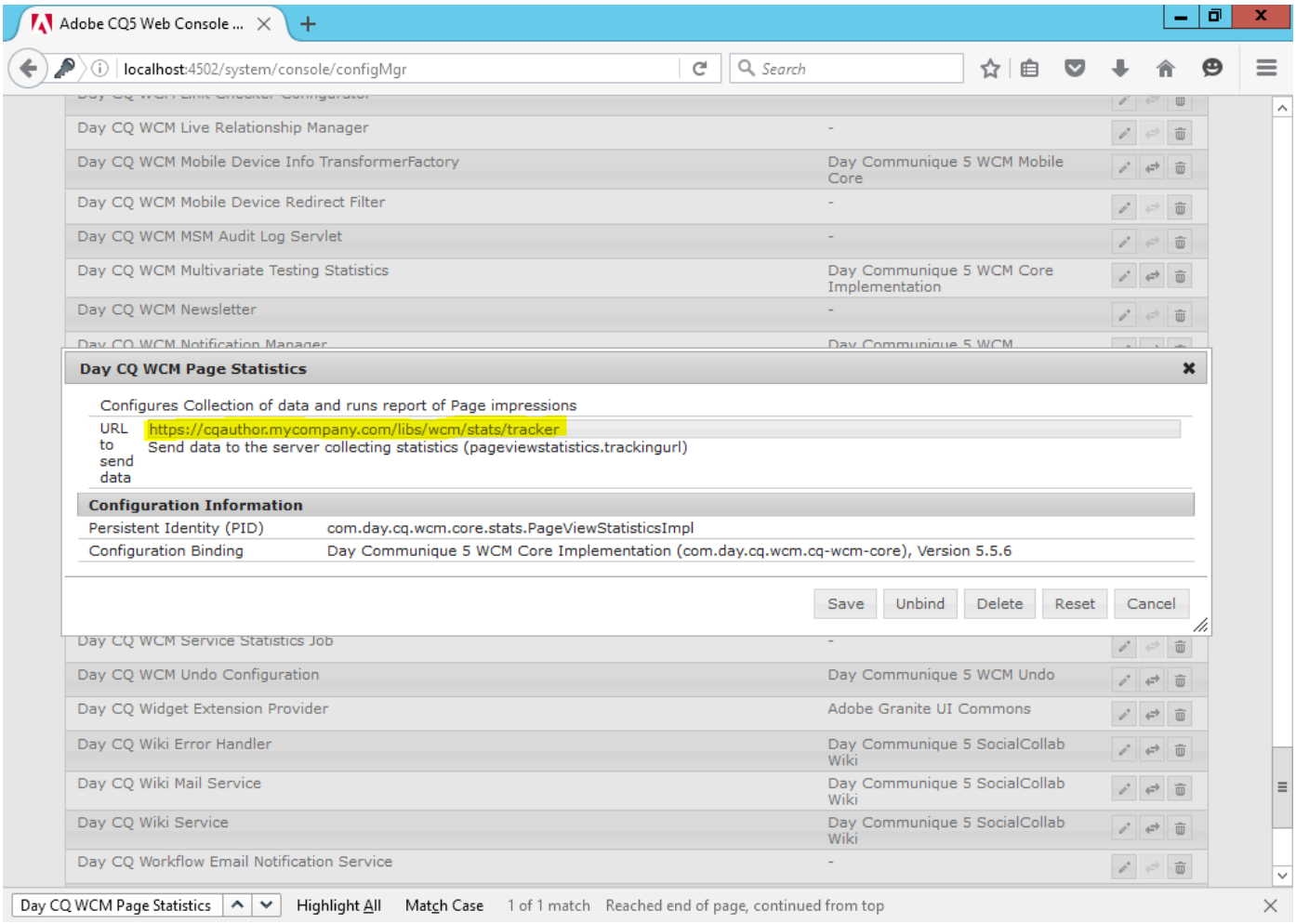
1. Browse to http://localhost:4503/crx/de/index.jsp
2. At the top right, click on anonymous@crx.default to bring up the login prompt, login in with your CQ admin credentials.
3. Again, in the folder tree on the left, go to /content/connect/c1/jcr:content/
4. Edit the value of property “serverURL” and set your Connect Host name and prefix https://, i.e. https://connect.mycompany.com:443
5. Click “Save All” at the top left to save your changes.
6. Logout.

Check the CRX configuration of the CQ author server is correctly set for SSL.

1. Browse to http://localhost:4502/system/console/configMgr
2. Login with your CQ admin credentials
3. Scroll down to find the “Day CQ Link Externalizer”.
4. On the right, click on the “edit” button.
5. Make sure the entries under “Domain” are prefixed with https
6. Under “Hostname” set your CQ Author host name without a prefix.



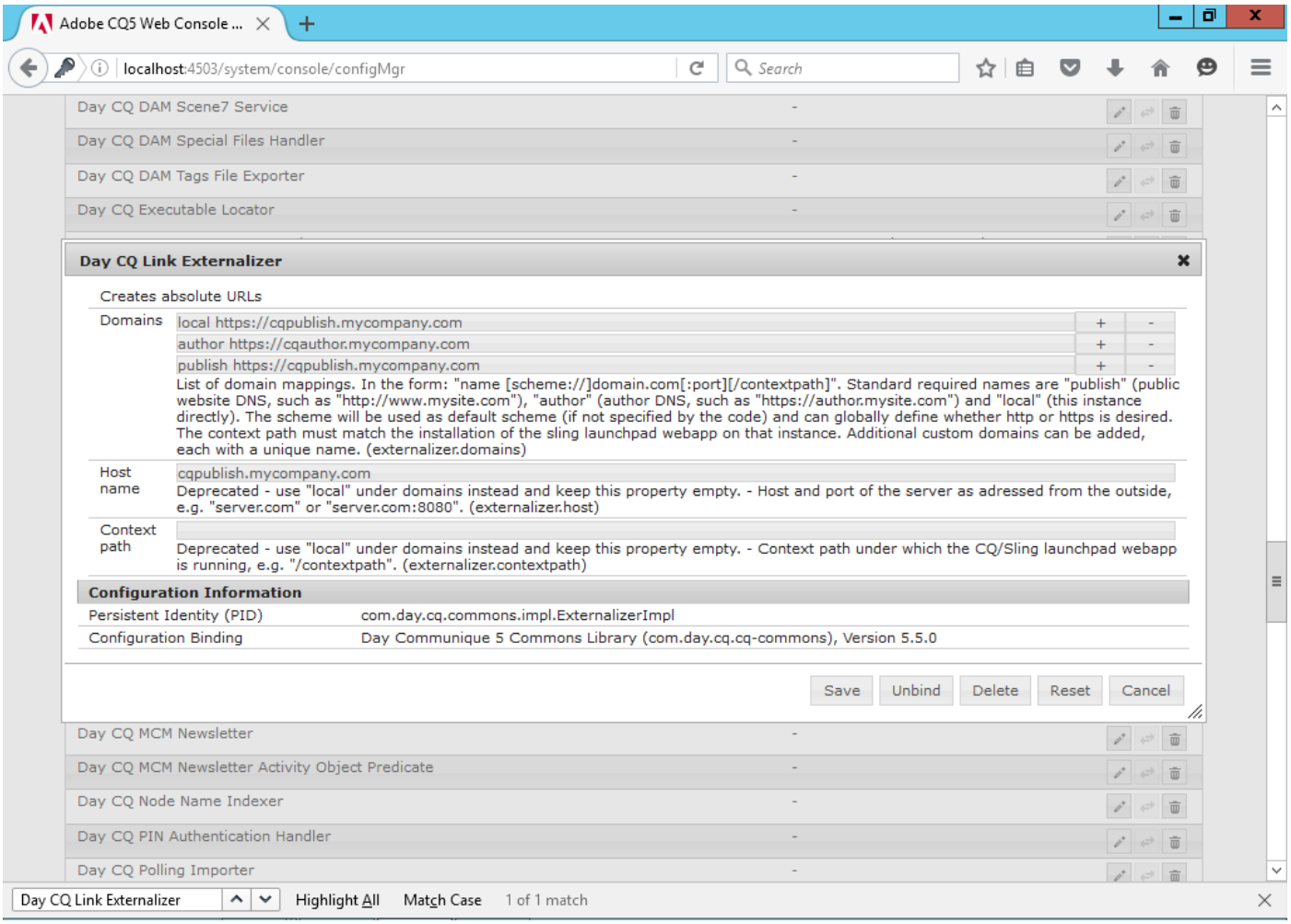
7. Click “Save”
8. Back in the list view find “Day CQ WCM Page Statistics” and click on the edit button.
9. Check the URL contains your CQ author domain name instead of “localhost” and has the https:// prefix.
10. Click “Save”.



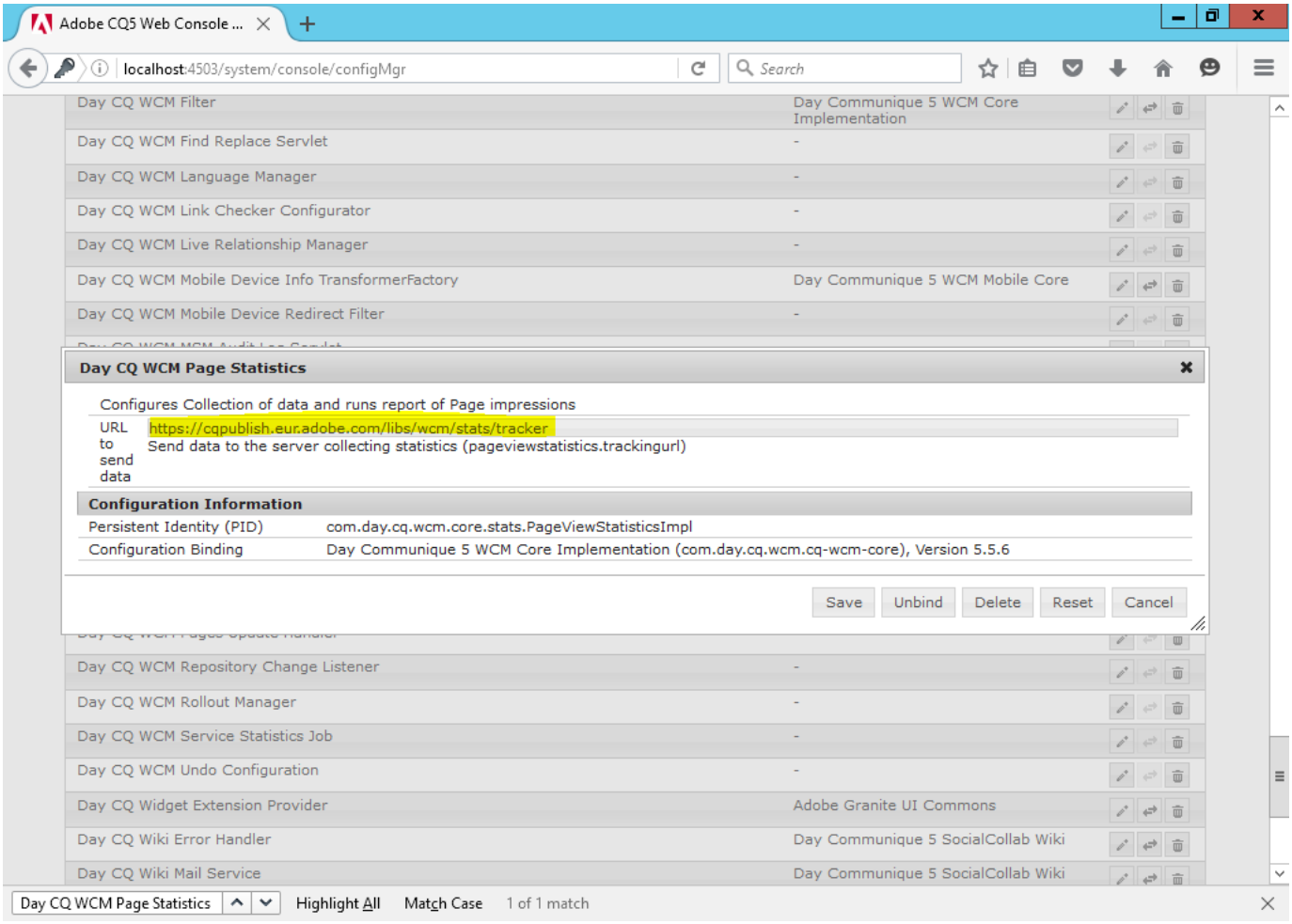
Check the CRX configuration of the CQ publish server is correctly set for SSL.

This is a repeat of the above steps, only for the author server, browse to http://localhost:4503/system/console/configMgr and login as admin.

1. Login with your CQ admin credentials
2. Scroll down to find the “Day CQ Link Externalizer”.
3. On the right, click on the “edit” button.
4. Make sure the entries under “Domains” are prefixed with https
5. Under “Hostname” set your CQ Publish host name without a prefix.



6. Click “Save”
7. Back in the list view find “Day CQ WCM Page Statistics” and click on the edit button.
8. Check the URL contains your CQ publish domain name instead of “localhost” and has the https:// prefix.
9. Click “Save”.


Adobe CQ5 Web Console ...
localhost:4503/system/console/configMgr
Search
Day CQ WCM Filter
Day Communique 5 WCM Core Implementation
Day CQ WCM Find Replace Servlet
Day CQ WCM Language Manager
Day CQ WCM Link Checker Configurator
Day CQ WCM Live Relationship Manager
Day CQ WCM Mobile Device Info TransformerFactory
Day Communique 5 WCM Mobile Core
Day CQ WCM Mobile Device Redirect Filter
Day CQ WCM Page Statistics
Configures Collection of data and runs report of Page impressions
URL to send data
https://cqpublish.eur.adobe.com/libs/wcm/stats/tracker
Send data to the server collecting statistics (pageviewstatistics.trackingurl)
Configuration Information
Persistent Identity (PID)
com.day.cq.wcm.core.stats.PageViewStatisticsImpl
Configuration Binding
Day Communique 5 WCM Core Implementation (com.day.cq.wcm.cq-wcm-core), Version 5.5.6
Save
Unbind
Delete
Reset
Cancel
Day CQ WCM Repository Change Listener
Day CQ WCM Rollout Manager
Day CQ WCM Service Statistics Job
Day CQ WCM Undo Configuration
Day CQ Widget Extension Provider
Adobe Granite UI Commons
Day CQ Wiki Error Handler
Day Communique 5 SocialCollab Wiki
Day CQ Wiki Mail Service
Day Communique 5 SocialCollab Wiki
Day CQ WCM Page Statistics
Highlight All
Match Case
1 of 1 match

Almost done.

Import the CQ publish server SSL certificates to the Connect server Java keystore:

This last step is also outlined here: http://blogs.adobe.com/connectsupport/connect-on-premise-event-emails-may-fail-to-be-sent/

When you create a new Event there are a number of different email notifications available, including confirmation of new registrations, event reminders, thank you notes etc.

These emails are created from email templates that the Connect application server needs to download from the CQ publish server before they're sent out.If you have the CQ service configured with SSL the Connect server needs to trust the certificates you configured on the remote CQ publish host, otherwise it will fail on the email template download. To enable the template download import the SSL certificate of your CQ publish server to the Connect server keystore.

On the Connect server, open a command line and change to this directory:

<drive>:\Connect\9.x\jre\bin\

The command to import the certificate is as follows (of course replace c:\pathToCertFile\cert.crt with your own path and filename). Also, make sure the path to the keystore is correct for your environment and version of Connect.

keytool -importcert -trustcacerts -alias connectcerts -file **c:\pathToCertFile\cert.crt** *-keystore c:\Connect***9.x***jre\lib\security\cacerts*

Cycle all services. Start with the Flash Media Server (called Adobe Media Server in Connect 9.5 and higher).

You're done!