ADOBE® CONNECT™ ENTERPRISE SERVER 6

SSL CONFIGURATION GUIDE

Adobe®

Adobe® Connect™ Enterprise Server 6 SSL Configuration Guide, for Windows®

Adobe Systems Incorporated, 345 Park Avenue, San Jose, California 95110, USA.

Contents

SSL Configuration Guide

Preparing to configure SSL 1

Configuring SSL for Connect Enterprise Server 2

SSL configuration reference 8

SSL Configuration Guide

Configure SSL to create secure client-server connections for Adobe® Connect™ Enterprise Server and Adobe Connect Edge Server.

Preparing to configure SSL

About SSL support

Connect Enterprise Server 6 is made up of two servers: Macromedia® Flash® Media Server from Adobe and the Connect Enterprise application server. Flash Media Server is also called the *meeting server*, because it handles the real-time RTMP connection between the client and Adobe® Acrobat® Connect™ Professional meetings. The Connect Enterprise application server handles the HTTP connection between the client and the Connect Enterprise application logic. By default, Connect Enterprise Server uses port 443 for encrypted traffic.

You can configure SSL for the application server, the meeting server, or both:

Hardware-based solution Use an SSL accelerator for the most robust SSL configuration.

You must purchase an SSL accelerator separately. Adobe has verified that Connect Enterprise Server works with the following SSL hardware accelerators: F5 Big-IP 1000, Cisco Catalyst 6590 Switch, and Radware T100.

Software-based solution Use the native support for SSL in Connect Enterprise Server.

Note: *SSL is not supported on Microsoft® Windows® 98.*

Connect Enterprise Server uses the HTTP `CONNECT` method to request an SSL connection. To ensure that Acrobat Connect meetings can connect to clients securely without tunneling RTMP over HTTP/HTTPS, make sure any proxy servers allow clients to use the `CONNECT` method.

For help configuring SSL, contact Adobe Support at www.adobe.com/go/connect_licensed_programs_en.

Working with certificates

An SSL certificate verifies the identity of the server to the client.

To secure the meeting server connection (RTMP) and the application server connection (HTTP), you must have two SSL certificates, one for each server. To configure SSL for a cluster of computers hosting Connect Enterprise Server, you must have an SSL certificate for each meeting server, but you can use one certificate for all the application servers.

For example, to secure the meeting server and application server connections on one server, you would need two SSL certificates. To secure the meeting server and application server connections on a cluster of three servers, you would need four SSL certificates—one for the application servers and three for the meeting servers.

Obtain certificates

❖ Contact a Certificate Authority—a trusted third party who verifies the identity of the applicant. (A self-signed certificate will not work with Connect Enterprise.)

The Certificate Authority will ask you to generate an SSL Certificate Signing Request (CSR) file. A CSR is a digital file that you send to a Certificate Authority to be signed into an SSL certificate. It contains information about your organization and the FQDN (fully qualified domain name) associated with the SSL certificate. Contact the Certificate Authority for instructions about generating a CSR.

Important: *Store the passwords for your SSL certificates in a safe, accessible location.*

Install certificates

❖ Install the SSL certificates in PEM format to the root Connect Enterprise Server folder (c:\breeze, by default).

If you receive a CRT file from a Certificate Authority, you can rename the file so that its file extension is .pem.

Note: *You must have a single public/private key file.*

Configuring SSL for Connect Enterprise Server

Configure software-based SSL

When you configure software-based SSL, you can secure the application server (HTTP), the meeting server (RTMP), or both. You must configure the DNS server, and it's always a good idea to test your configuration when it's complete.

Configure the DNS server

❖ Create DNS entries for whichever server you plan to secure.

Define an FQDN for each secured server (for example, application.example.com and meeting1.example.com) because SSL certificates are associated with names, not IP addresses.

Note: *You can use one SSL certificate for all the application servers in a cluster, but you must have a unique SSL certificate for each meeting server.*

Secure the meeting and application servers

1 Open the Adaptor.xml file located at *[root_install_dir]*\comserv\win32\conf_defaultRoot_ and save a backup copy to another location.

2 Insert the following code in the original Adaptor.xml file inside the `<Adaptor></Adaptor>` tags (replace the code in italic with your own values):

```
<SSL>
    <Edge name="meetingserver">
        <SSLServerCtx>
    <SSLCertificateFile>[root_install_dir]\sslMeetingServer.pem</SSLCertificateFile>
    <SSLCertificateKeyFile
type="PEM">[root_install_dir]\sslMeetingServer.pem</SSLCertificateKeyFile>
            <SSLPassPhrase>mypassphrase</SSLPassPhrase>
            <SSLCipherSuite>ALL:!ADH:!LOW:!EXP:!MD5:@STRENGTH</SSLCipherSuite>
            <SSLSessionTimeout>5</SSLSessionTimeout>
        </SSLServerCtx>
    </Edge>
    <Edge name="applicationserver">
        <SSLServerCtx>
        <SSLCertificateFile>[root_install_dir]\sslAppServer.pem</SSLCertificateFile>
            <SSLCertificateKeyFile
type="PEM">[root_install_dir]\sslAppServer.pem</SSLCertificateKeyFile>
            <SSLPassPhrase>mypassphrase</SSLPassPhrase>
            <SSLCipherSuite>ALL:!ADH:!LOW:!EXP:!MD5:@STRENGTH</SSLCipherSuite>
            <SSLSessionTimeout>5</SSLSessionTimeout>
        </SSLServerCtx>
    </Edge>
</SSL>
```

3 Locate the following line in the Adaptor.xml file:

```
<HostPort name="edge1">${DEFAULT_FCS_HOSTPORT}</HostPort>
```

4 Replace the code in step 3 with the following:

```
<HostPort name="meetingserver" ctl_channel=":19350">meetingServerIP:-443</HostPort>
<HostPort name="applicationserver" ctl_channel=":19351">appServerIP:-443</HostPort>
```

5 Save the Adaptor.xml file.

6 (Optional) Open the Adaptor.xml file in a web browser to validate the syntax.

If the browser reports an error, correct it and reopen the file in a web browser. Repeat this process until the file is valid.

7 Open the custom.ini file located in the root installation directory (c:\breeze, by default) and save a backup copy to another location.

8 Insert the following code in the custom.ini file without replacing or deleting any existing text:

```
ADMIN_PROTOCOL=https://
SSL_ONLY=yes
HTTPS_PORT=8443
RTMP_SEQUENCE=rtmps://external-host:443/?rtmp://localhost:8506/
```

9 Save the custom.ini file.

10 Open the VHost.xml file located at *[root_install_dir]*\comserv\win32\conf_defaultRoot__defaultVHost_ and save a backup copy to another location.

11 Locate the following line in the VHost.xml file:

```
<RouteEntry></RouteEntry>
```

12 Replace the line in step 11 with the following code:

```
<RouteEntry protocol="rtmp">*:*;*:${ORIGIN_PORT}</RouteEntry>
```

13 Save the VHost.xml file.

14 (Optional) Open the VHost.xml file in a web browser to validate the syntax.

15 Restart Adobe Connect Enterprise Server:

a Choose Start > All Programs > Adobe Connect Enterprise Server > Stop Adobe Connect Enterprise Server.

b Choose Start > All Programs > Adobe Connect Enterprise Server > Stop Adobe Connect Meeting Server.

c Choose Start > All Programs > Adobe Connect Enterprise Server > Start Adobe Connect Meeting Server.

d Choose Start > All Programs > Adobe Connect Enterprise Server > Start Adobe Connect Enterprise Server.

16 Open the Application Management Console (http://localhost:8510/console or Start > All Programs > Adobe Connect Enterprise Server > Configure Adobe Connect Enterprise Server).

17 On the Application Settings screen, select Server Settings and do the following:

a Enter the FQDN for your Connect Enterprise account in the Connect Enterprise Host box.

b Enter the FQDN for the Connect Enterprise meeting server in the Host Mappings External Name box.

Secure the application server only

1 Open the Adaptor.xml file located at *[root_install_dir]*\comserv\win32\conf_defaultRoot_ and save a backup copy to another location.

2 Insert the following code in the original Adaptor.xml file inside the `<Adaptor></Adaptor>` tags (replace the code in italic with your own values):

```
<SSL>
    <Edge name="applicationserver">
        <SSLServerCtx>
        <SSLCertificateFile>[root_install_dir]\sslAppServer.pem</SSLCertificateFile>
            <SSLCertificateKeyFile
type="PEM">[root_install_dir]\sslAppServer.pem</SSLCertificateKeyFile>
            <SSLPassPhrase>mypassphrase</SSLPassPhrase>
            <SSLCipherSuite>ALL:!ADH:!LOW:!EXP:!MD5:@STRENGTH</SSLCipherSuite>
            <SSLSessionTimeout>5</SSLSessionTimeout>
        </SSLServerCtx>
    </Edge>
</SSL>
```

3 Locate the following line in the Adaptor.xml file:

```
<HostPort name="edge1">${DEFAULT_FCS_HOSTPORT}</HostPort>
```

4 Add the following code below the line in step 3:

```
<HostPort name="applicationserver" ctl_channel=":19351">:-443</HostPort>
```

5 Save the Adaptor.xml file.

6 (Optional) Open the Adaptor.xml file in a web browser to validate the syntax.

If the browser reports an error, correct it and reopen the file in a web browser. Repeat this process until the file is valid.

7 Open the custom.ini file located in the root installation directory (c:\breeze, by default) and save a backup copy to another location.

8 Insert the following code in the custom.ini file without replacing or deleting any existing text:

```
ADMIN_PROTOCOL=https://
SSL_ONLY=yes
HTTPS_PORT=8443
```

9 Save the custom.ini file.

10 Restart Adobe Connect Enterprise Server:

a Choose Start > All Programs > Adobe Connect Enterprise Server > Stop Adobe Connect Enterprise Server.

b Choose Start > All Programs > Adobe Connect Enterprise Server > Stop Adobe Connect Meeting Server.

c Choose Start > All Programs > Adobe Connect Enterprise Server > Start Adobe Connect Meeting Server.

d Choose Start > All Programs > Adobe Connect Enterprise Server > Start Adobe Connect Enterprise Server.

Secure the meeting server only

1 Open the Adaptor.xml file located at *[root_install_dir]*\comserv\win32\conf_defaultRoot_ and save a backup copy to another location.

2 Insert the following code in the original Adaptor.xml file inside the `<Adaptor></Adaptor>` tags (replace the code in italic with your own values):

```
<SSL>
    <Edge name="meetingserver">
        <SSLServerCtx>
    <SSLCertificateFile>[root_install_dir]\sslMeetingServer.pem</SSLCertificateFile>
    <SSLCertificateKeyFile
type="PEM">[root_install_dir]\sslMeetingServer.pem</SSLCertificateKeyFile>
            <SSLPassPhrase>mypassphrase</SSLPassPhrase>
            <SSLCipherSuite>ALL:!ADH:!LOW:!EXP:!MD5:@STRENGTH</SSLCipherSuite>
            <SSLSessionTimeout>5</SSLSessionTimeout>
        </SSLServerCtx>
    </Edge>
</SSL>
```

3 Locate the following line in the Adaptor.xml file:

```
<HostPort name="edge1">${DEFAULT_FCS_HOSTPORT}</HostPort>
```

4 Replace the code in step 3 with the following:

```
<HostPort name="meetingserver" ctl_channel=":19350">:-443</HostPort>
```

5 Save the Adaptor.xml file.

6 (Optional) Open the Adaptor.xml file in a web browser to validate the syntax.

If the browser reports an error, correct it and reopen the file in a web browser. Repeat this process until the file is valid.

7 Open the VHost.xml file located at *[root_install_dir]*\comserv\win32\conf_defaultRoot__defaultVHost_ and save a backup copy to another location.

8 Locate the following line in the VHost.xml file:

```
<RouteEntry></RouteEntry>
```

9 Replace the line in step 8 with the following code:

```
<RouteEntry protocol="rtmp">*:*;*:${ORIGIN_PORT}</RouteEntry>
```

10 Save the VHost.xml file.

11 (Optional) Open the VHost.xml file in a web browser to validate the syntax.

12 Open the custom.ini file located in the root installation directory (c:\breeze, by default) and save a backup copy to another location.

13 Insert the following code in the custom.ini file without replacing or deleting any existing text:

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

14 Save the custom.ini file.

15 Restart Adobe Connect Enterprise Server:

a Choose Start > All Programs > Adobe Connect Enterprise Server > Stop Adobe Connect Enterprise Server.

b Choose Start > All Programs > Adobe Connect Enterprise Server > Stop Adobe Connect Meeting Server.

c Choose Start > All Programs > Adobe Connect Enterprise Server > Start Adobe Connect Meeting Server.

d Choose Start > All Programs > Adobe Connect Enterprise Server > Start Adobe Connect Enterprise Server.

Test the configuration

1 If you secured the application server, log in to Enterprise Manager. You should see a lock in your browser.

2 If you secured the meeting server, enter an Acrobat Connect Professional meeting room. You should see a lock in the connection light.

Configure hardware-based SSL

When you configure hardware-based SSL, you can secure the application server (HTTP), the meeting server (RTMP), or both. You must configure the DNS server, and it's always a good idea to test your configuration when it's complete.

For additional instructions about how to configure the hardware accelerator, see the vendor's documentation.

Configure the DNS server

❖ Create DNS entries for whichever server you plan to secure.

You need to define an FQDN for each secured server (for example, application.example.com and meeting1.example.com), because SSL certificates are associated with names, not IP addresses.

Note: *You can use one SSL certificate for all the application servers in a cluster, but you must have a unique SSL certificate for each meeting server.*

Configure SSL for the meeting and application servers

1 Configure the hardware device to do the following:

a Listen externally on port 443 for application.example.com.

b Forward unencrypted data to the application server on port 8443.

c Listen externally on port 443 for meeting1.example.com.

d Forward unencrypted data to the meeting server on port 1935.

e (Optional) Listen externally on port 80 for application.example.com and forward unencrypted data to the application server on port 80. The application server will redirect users to port 443.

2 Configure the firewall to do the following:

a Allow traffic to the application server on port 443 (and on port 80 if you completed step 1e).

b Allow traffic to the meeting server on port 443.

3 Choose Start > All Programs > Adobe Connect Enterprise Server > Configure Adobe Connect Enterprise Server to open the Application Management Console. On the Applications Settings screen, select Server Settings and do the following:

a Enter the FQDN of the application server (for example, application.example.com) in the Connect Enterprise Host box.

b Enter the FQDN of the meeting server (for example, meeting1.example.com) in the Host Mappings External Name box.

4 Open the custom.ini file located in the root installation directory (c:\breeze, by default) and save a backup copy to another location.

5 Insert the following code in the custom.ini file without replacing or deleting any existing text:

```
ADMIN_PROTOCOL=https://
SSL_ONLY=yes
HTTPS_PORT=8443
RTMP_SEQUENCE=rtmps://external-host:443/?rtmp://localhost:8506/
```

6 Save the custom.ini file.

7 Restart Adobe Connect Enterprise Server:

a Choose Start > All Programs > Adobe Connect Enterprise Server > Stop Adobe Connect Enterprise Server.

b Choose Start > All Programs > Adobe Connect Enterprise Server > Start Adobe Connect Enterprise Server.

Configure SSL for the meeting server only

1 Configure the hardware device to do the following:

a Listen externally on port 443 for meeting1.example.com.

b Forward unencrypted data to the meeting server on port 1935.

2 Configure the firewall to allow traffic to the meeting server on port 443.

3 Open the custom.ini file located in the root installation directory (c:\breeze, by default) and save a backup copy to another location.

4 Insert the following code in the custom.ini file without replacing or deleting any existing text:

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

5 Save the custom.ini file.

Configure SSL for the application server only

1 Configure the hardware device to do the following:

a Listen externally on port 443 for application.example.com.

b Forward unencrypted data to the application server on port 8443.

c (Optional) Listen externally on port 80 for application.example.com and forward unencrypted data to the application server on port 80. The application server will redirect users to port 443.

2 Configure the firewall to allow traffic to the application server on port 443 (and on port 80 if you completed step 1c).

3 On Connect Enterprise Server, add the following to the custom.ini file in the root installation folder (c:\breeze, by default):

```
ADMIN_PROTOCOL=https://
SSL_ONLY=yes
HTTPS_PORT=8443
```

4 Restart Adobe Connect Enterprise Server:

a Choose Start > All Programs > Adobe Connect Enterprise Server > Stop Adobe Connect Enterprise Server.

b Choose Start > All Programs > Adobe Connect Enterprise Server > Start Adobe Connect Enterprise Server.

Test the configuration

1 If you secured the application server, log in to Enterprise Manager. You should see a lock in your browser.

2 If you secured the meeting server, enter an Acrobat Connect Professional meeting room. You should see a lock in the connection light.

SSL configuration reference

XML tags

Tag	Default value	Description
`SSLCertificateFile`	No default.	The location of the certificate file to send to the client. If an absolute path is not specified, the certificate is assumed to be relative to the Adaptor directory.
`SSLCertificateKeyFile`	No default.	The location of the private key file for the certificate. If an absolute path is not specified, the key file is assumed to be relative to the Adaptor directory. If the key file is encrypted, the pass phrase must be specified in the `SSLPassPhrase` tag. The `type` attribute specifies the type of encoding used for the certificate key file. This can be either `PEM` or `ASN1`.
`SSLCipherSuite`	See description.	The algorithm, which consists of colon-delimited elements that can be key exchange algorithms, authentication methods, encryption methods, digest types, or one of a selected number of aliases for common groupings. For a list of components, see the Flash Media Server documentation. This tag has the following default setting: `ALL:!ADH:!LOW:!EXP:!MD5:@STRENGTH` Contact Adobe Technical Support before changing the default settings.
`SSLPassPhrase`	No default.	The pass phrase to use for decrypting the private key file. If the private key file is not encrypted, leave this tag empty.
`SSLSessionTimeout`	5	The amount of time an SSL-enabled session remains valid, in minutes.

Configuration parameters

Parameter	Default value	Description
`ADMIN_PROTOCOL`	`http://`	The protocol used by the application server. Set to `https://` to configure SSL.
`DEFAULT_FCS_HOST PORT`	`:1935`	The port used by Flash Media Server to communicate using the RTMP protocol. Set to:-443,1935 to configure SSL.
`HTTPS_PORT`	No default.	The port on which the application server listens for HTTPS requests. This parameter is usually set to `443` or `8443` to configure SSL.
`SSL_ONLY`	`no`	Set to `yes` if the server supports only secure connections. This setting forces all Connect Enterprise URLs to use HTTPS.
`RTMP_SEQUENCE`	No default.	The origins, edges, and ports used to connect to Flash Media Server (the meeting server).