Migrating, Installing, and Configuring
ADOBE® CONNECT™ 9

Legal notices

Contents

Chapter 1: Preparing for migration, installation, and configuration

Chapter 2: Installing Adobe Connect

Chapter 3: Deploying and configuring Adobe Connect

Chapter 4: Security

Chapter 5: Administering Adobe Connect

Chapter 1: Preparing for migration, installation, and configuration

The techniques you use to install Adobe® Connect™ depend on the type of installation you are performing.

- If you are installing Adobe Connect for the first time, review the installation requirements, supported configurations, and technical overview throughout this chapter. Then see “Install Adobe Connect 9” on page 20.
- If you are migrating from version 7.5.2.3, or 8.0 to 8.2.x, review the information below that explains what’s new in this version. Then see “Preparing to migrate” on page 4.

Installation requirements

Hardware, software, and user requirements

For Adobe Connect and Adobe Connect Edge Server requirements, see www.adobe.com/go/learn_cnn_sysreqs_en.

Port requirements

The following table describes ports on which users must be able to establish TCP connections.

Number	Bind Address	Access	Protocol
80	*/Any Adaptor	Public	HTTP, RTMP
443	*/Any Adaptor	Public	HTTPS, RTMPS
1935	*/Any Adaptor	Public	RTMP

Note: *RTMP (Real-Time Messaging Protocol) is an Adobe protocol.*

The following table describes the ports open inside a cluster. Each Adobe Connect server in a cluster must be able to establish TCP connections to all other servers in the cluster on these ports.

Note: *These ports should not be open to the public, even if you are not using a cluster.*

Number	Source Port	Bind Address	Access	Protocol
8506	Any	*/Any Adaptor	Private	RTMP
8507	Any	*/Any Adaptor	Private	HTTP

Each Adobe Connect server in a cluster must be able to establish a TCP connection to the database server on the following port:

Number	Source Port	Access	Protocol
1433	Any	Private	TSQL

The following table describes server ports that Adobe Connect uses to communicate internally. These ports must not be in use by any other process or program on a server hosting Adobe Connect, or Adobe Connect may fail to start.

Number	Bind Address	Access	Protocol
1111	127.0.0.1	Internal	RTMP
2909	127.0.0.1	Internal	RMI
4111	*/Any Adaptor	Internal	JMX
8510	127.0.0.1	Internal	HTTP

If you are installing an integrated or custom telephony adaptor, each Adobe Connect server in a cluster must have the following port available:

Number	Bind Address	Access	Protocol
9080	*/Any Adaptor	Public if using InterCall telephony adaptor; internal otherwise	HTTP

Some integrated telephony adaptors require access to specific ports in addition to the ports listed in the tables above. These ports are listed in the information for each adaptor; see “Preparing to install integrated telephony adaptors” on page 14.

For information about Flash Media Gateway ports, see “Flash Media Gateway ports and protocols” on page 43.

Supported configurations

Supported Adobe Connect-Adobe CQ configurations

Adobe Connect uses Adobe CQ technology to create and manage event and email templates, and event catalog. Adobe CQ Author and Publish servers support authoring and publishing, respectively. In this document these servers are referred to as CQA and CQP, respectively, whereas Adobe Connect 9 is referred below as C9.

The following are the supported configurations:

C9, CQA, and CQP on a single machine The most basic setup scenario involves installing all the three servers on a single machine.

C9, CQA, and CQP on different machines All three different servers can be available on three different machines.

C9 on a machine, and CQA and CQP on another machine Adobe Connect can be deployed on two different machines with Adobe Connect deployed on a machine and Adobe CQ servers deployed on another machine.

C9, single or multiple CQA, and single or multiple CQP servers A possible deployment scenario is having a single Adobe Connect server, a single or multiple CQA servers, and a single or multiple CQP servers, all deployed on individual.

C9 and CQA server on a machine and one or more CQP servers on one or more machines Adobe Connect and CQA servers can be installed on a single machine, alongside at least a CQP machine, or an array of CQP clusters.

C9 and CQP server on a machine and one or more CQA servers on one or more machines Adobe Connect and CQP servers can be installed on a single machine, alongside at least a CQA machine, or an array of CQA clusters.

Supported server-database configurations

Adobe Connect uses a database to store information about users and content. The Adobe Connect installer includes Microsoft® SQL Server® 2005 Express Edition. Adobe Connect also supports Microsoft SQL Server 2005 Standard Edition and Microsoft SQL Server 2008. These editions of SQL Server are not included with Adobe Connect.

The following are the supported Adobe Connect and database configurations:

Single server with embedded database engine Install Adobe Connect on a single computer and install the embedded database engine (included on the Adobe Connect installer) on the same computer. The embedded database engine is Microsoft SQL Server 2005 Express Edition.

Note: *This configuration should be used only in testing environments, not in production environments.*

Single server with SQL Server Install Adobe Connect on a single computer and install MicrosoftSQL Server 2005 Standard Edition on the same computer.

Single server with an external SQL Server database Install Adobe Connect on a single computer and install SQL Server on another computer.

Single server with multiple external SQL Server databases Install Adobe Connect on a single computer and install SQL Server on multiple computers (also called a cluster) external to Adobe Connect. Adobe Connect supports mirroring and clustering of the SQL Server databases.

Multiple servers with an external SQL Server database Install Adobe Connect on multiple servers (also called a cluster) and install SQL Server on another computer.

Multiple servers with multiple external SQL Server databases Install Adobe Connect on multiple servers (also called a cluster) and install SQL Server in a separate cluster. Adobe Connect supports mirroring and clustering of the SQL Server databases.

Supported Flash Media Gateway deployments

Deploy Flash Media Gateway to enable Universal Voice. The following are supported deployments:

Single computer Install Adobe Connect, Flash Media Gateway, and SQL Server on the same computer.

Two computers Install Adobe Connect and Flash Media Gateway on the same computer and SQL Server on a separate computer.

A cluster of computers Install each Adobe Connect server and each Flash Media Gateway on its own computer.

More Help topics

"Adobe Connect audio and video conferencing options" on page 14

"Deploying Universal Voice" on page 42

Supported LDAP directory servers

You can configure user authentication against your organization's LDAP directory server and import directory information into Adobe Connect from your organization's LDAP directory server. For a list of the supported LDAP directory servers, see www.adobe.com/go/learn_cnn_sysreqs_en.

Note: *Any LDAP v.3 directory server may integrate with Adobe Connect. However, only directory servers that have been tested by Adobe are supported.*

More Help topics

"Integrating with a directory service" on page 35

Supported content storage devices

You can configure your Adobe Connect system to store content on Network Attached Storage (NAS) and Storage Area Network (SAN) devices. For a list of supported NAS and SAN devices, see www.adobe.com/go/learn_cnn_sysreqs_en.

More Help topics

"Configuring shared storage" on page 52

Preparing to migrate

Migration paths

Run the Adobe Connect 9 installer to upgrade from Adobe Connect Pro 7.5.2.3, Adobe Connect 8.0, Adobe Connect 8.1.x, or Adobe Connect 8.2.x to Adobe Connect 9. The Adobe Connect installer guides you through the upgrade.

For more information about upgrading, contact Adobe Support: www.adobe.com/support/programs/connect.

Workflow for migrating to Adobe Connect 9

Follow this workflow to migrate to Adobe Connect 9.

1. Test the migration in a non-production environment.

It's a good idea to take a snapshot of your current production environment and test the migration in a non-production environment before you migrate your production environment. Once you've successfully migrated in a test environment, proceed to step 2.

2. Inform users about the migration.

See "Informing users about the migration" on page 5.

3. (Optional) Back up content and configuration files.

See "Back up files" on page 5.

4. Back up the database.

See "Back up the database" on page 92.

5. Run the Adobe Connect 9 installer.

See "Install Adobe Connect 9" on page 20. The installer stops the Adobe Connect services and backs up existing files, including the custom.ini file.

(Optional) Gather information required to install one or more integrated telephony adaptors.

See "Preparing to install integrated telephony adaptors" on page 14.

Verify your installation.

See "Verify your installation" on page 24.

Informing users about the migration

As with any software upgrade—especially one that affects a workgroup—communication and planning are important. Before you begin migrating or adding modules to Adobe Connect, Adobe suggests that you do the following:

- Allocate enough time to ensure a successful migration. The upgrade should fit into your normal maintenance period.
- Let users know in advance that they won't be able to use Adobe Connect during the migration.
- Let users know what types of changes they can expect (such as new features or improved performance) after the migration. For information about what's new, see www.adobe.com/products/connect.

Back up files

The installer creates backup copies of the appserv and comserv directories and the custom.ini file and installs new versions. The installer does not erase or overwrite the content directory. Customizations done in `ConnectProSvc.conf` or `TelephonyService.conf` files, on a 64-bit OS, are not retained after a migration to Adobe Connect 9.

You can optionally choose to create backup copies of these directories and files.

Upgrading from SQL Server 2005 Express edition

Follow this workflow to migrate from using the embedded database to using SQL Server 2005 Standard Edition or SQL Server 2008 on a different computer.

***Note:** You may perform this migration when you migrate to Adobe Connect. You may also perform this migration at any time after installing Adobe Connect.*

1. Install SQL Server on a different computer than the computer hosting Adobe Connect.

Follow the instructions provided by Microsoft to install SQL Server.

2. Back up the embedded database (SQL Server 2005 Express Edition).

See "Back up the database" on page 92.

3. Copy the BAK file from the computer hosting Adobe Connect to the computer hosting SQL Server.

When you back up SQL Server Express Edition, a file is created called *breeze*.bak (where *breeze* is the name of the database).

4. Restore the database on the computer hosting SQL Server.

For more information about restoring SQL Server, see Microsoft TechNet.

5. Enter the SQL Server database information in the Application Management Console on the server hosting Adobe Connect.

Choose Start > Programs > Adobe Connect Server > Configure Adobe Connect Server.

Preparing to install Adobe Connect

Adobe Connect technical overview

An Adobe Connect installation consists of several components: Adobe Connect Central Application Server, Adobe® Flash® Media Server, Adobe Connect Presence Service, Flash Media Gateway (Universal Voice), a database, the Adobe Connect Telephony service, and telephony adaptors for audio conferencing.

The Adobe Connect Central Application Server is built as a J2EE web application running on the Tomcat servlet engine. Called the *application server*, it manages users, groups, on-demand content, and client sessions. Some of the application server's duties include access control, security, quotas, licensing, and auditing and management functions such as clustering, failover, and replication. It also transcodes media, including converting Microsoft® PowerPoint and audio to Adobe® Flash®. The application server handles meeting requests and content transfer requests (slides, HTTP pages, SWF files, and files in the File Share pod) over an HTTP or HTTPS connection.

Certain components of Flash Media Server (FMS), also called the *meeting server*, are installed with Adobe Connect to handle real-time audio and video streaming, data synchronization, and rich-media content delivery, including Adobe Connect meeting interactions. Some Flash Media Server tasks include meeting recording and playback, timing the synchronization of audio and video, and transcoding—converting and packaging data for real-time screen sharing and interaction. Flash Media Server also reduces server load and latency by caching frequently accessed web pages, streams, and shared data. Flash Media Server streams audio, video, and accompanying meeting data over Adobe's high-performance Real-Time Messaging Protocol (RTMP or RTMPS).

The Adobe Connect Presence Service integrates Adobe Connect with Microsoft® Live Communications Server 2005 and Microsoft® Office Communications Server 2007. You can see IM presence in Adobe Connect meeting rooms and send IM messages to users not present in the meeting room. Choose whether to install the Presence Service during installation.

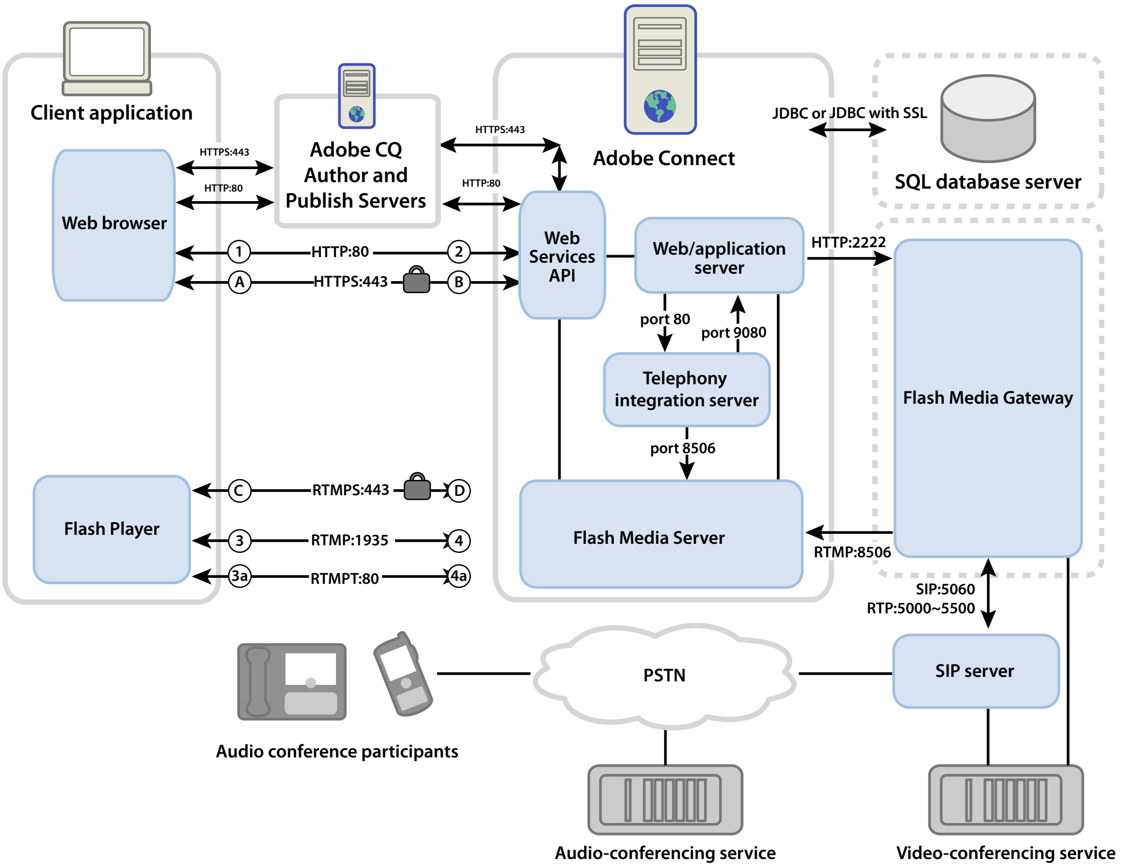
Flash Media Gateway integrates Adobe Connect with your SIP/RTP infrastructure. Flash Media Gateway receives audio from a SIP server and sends it into Adobe Connect meeting rooms. Flash Media Gateway also streams video and audio from Video Conference devices to the Video Telephony pod. This solution is called Universal Voice.

Adobe Connect requires a database for persistent storage of transactional and application metadata, including user, group, content, and reporting information. You can use the embedded database engine (SQL Server 2005 Express Edition) included in the Adobe Connect installer, or you can purchase and install Microsoft SQL Server 2005 Standard Edition.

Adobe Connect supports several telephony adaptors to enable audio conferencing. You can choose to install one or more adaptors during the installation process.

Data flow

The following diagram illustrates how data flows between a client application and Adobe Connect.



The data can flow over an unencrypted connection or an encrypted connection.

Unencrypted connection

Unencrypted connections are made over HTTP and RTMP and follow the paths described in the table. The numbers in the table correspond to the numbers in the data flow diagram.

Number	Description
1	The client web browser requests a meeting or content URL over HTTP:80.
2	The web server responds and transfers the content or provides the client with information to connect to the meeting.
3	The client Flash Player requests a connection to the meeting over RTMP:1935.
3a	The client Flash Player requests a connection to the meeting but can only connect over RTMP:80.
4	Flash Media Server responds and opens a persistent connection for Adobe Connect streaming traffic.
4a	Flash Media Server responds and opens a tunneled connection for Adobe Connect streaming traffic.

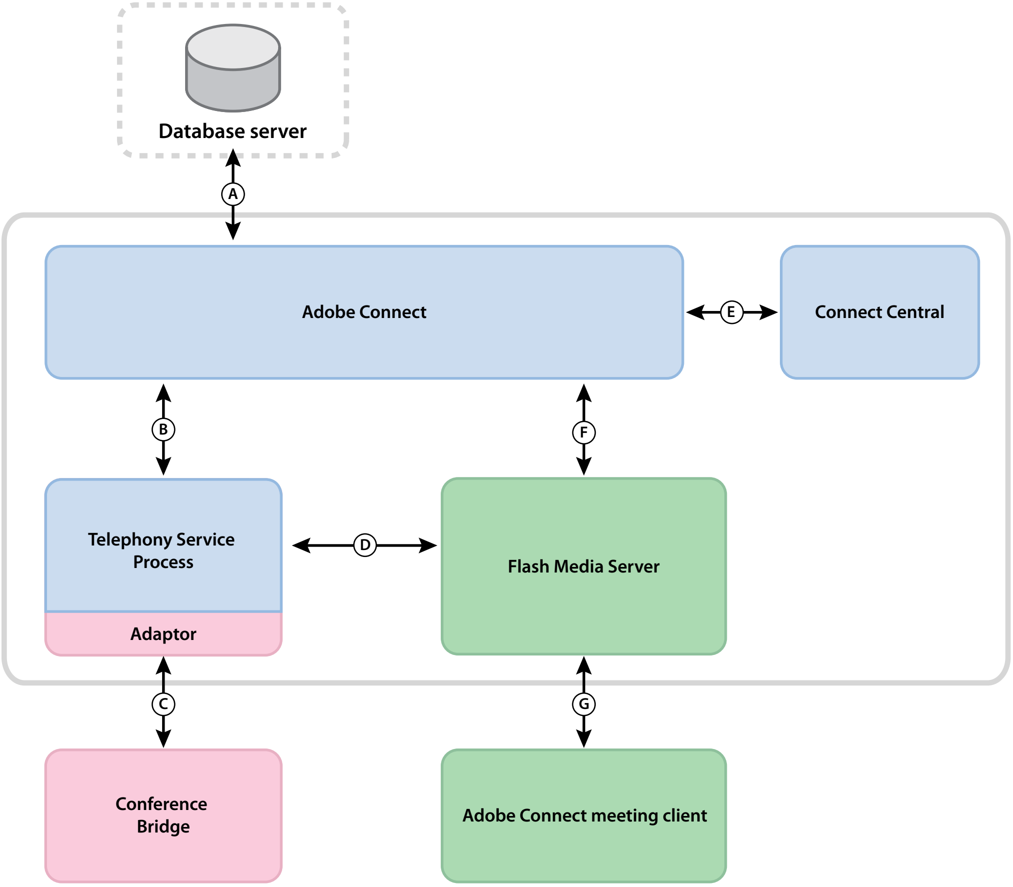
Encrypted connection

Encrypted connections are made over HTTPS and RTMPS and follow the paths described in the table. The letters in the table correspond to the letters in the data flow diagram.

Letter	Description
A	The client web browser requests a meeting or content URL over a secure connection on HTTPS:443.
B	The web server responds and transfers the content over a secure connection or provides the client with information to connect to the meeting securely.
C	The client Flash Player requests a secure connection to Flash Media Server over RTMPS:443.
D	Flash Media Server responds and opens a secure, persistent connection for Adobe Connect streaming traffic.

Telephony data flow

The following diagram illustrates how data flows between telephony services and Adobe Connect.



A. Persistence. B. Service management and failover, service connection and session brokering, and user data provisioning and access. C. Native commands and events using proprietary vendor APIs for conference control. D. Commands and events using RPC calls. E. Provisioning. F. Telephony service request. G. Telephony commands and state.

Installation workflow

The following steps help you design, install, and configure an Adobe Connect system. Some steps require you to make a decision, and other steps require you to complete a task. Each step refers you to background information about the decision or task.

1. Choose which database to use.

For more information, see “Choosing a database” on page 11.

2. If you chose SQL Server in step 1, install it.

For more information, see the SQL Server documentation.

Note: *If you are installing the embedded database, you don’t have to perform this step.*

3. (Optional) Choose and gather information needed for installing telephony adaptors.

If you are installing one or more of the integrated telephony adaptors, collect the information that the installer requires. For more information, see “Choosing to install integrated telephony adaptors” on page 12.

4. Install Adobe Connect and Adobe CQ servers on a single machine.

During the installation of Adobe Connect, you can also install Adobe CQ Author and Publish servers, embedded database engine, one or more telephony adaptors, Flash Media Gateway (Universal Voice) and the Presence Server. See “Install Adobe Connect 9” on page 20.

5. Verify that Adobe Connect and Adobe CQ servers are installed correctly.

For more information, see “Verify your installation” on page 24.

6. Deploy Adobe Connect.

For more information, see “Deploying Adobe Connect” on page 29.

7. (Optional) Integrate Adobe Connect with your infrastructure.

There are many possibilities for integrating Adobe Connect into your organization’s existing infrastructure. It’s a good idea to verify that Adobe Connect is functional after configuring each of these features.

Integrate with Adobe Omniture Adobe Connect 9 uses the Omniture technology to provide detailed event analytics reports. SiteCatalyst integration involves providing the credentials to Adobe’s Omniture website in Adobe Connect configuration. For more information, contact Omniture support at http://www.omniture.com/en/contact/support.

Integrate with a SIP provider Integrate Adobe Connect with your organization’s SIP server or a third-party SIP provider (also called a *VoIP provider*) to provide seamless audio conferencing. See “Deploying Universal Voice” on page 42.

Integrate with an LDAP Directory Integrate Adobe Connect with your organization’s LDAP directory server so you don’t need to manage multiple user directories. See “Integrating with a directory service” on page 35.

Configure a secure sockets layer Conduct all Adobe Connect communication securely. See “SSL (secure sockets layer)” on page 72.

Store content on NAS/SAN devices Use network devices to share content storage duties. See “Configuring shared storage” on page 52.

Integrate with Live Communications Server and Office Communications Server Integrate with a communication server to let Meeting Hosts see the IM presence of invitees in meeting rooms. Meeting Hosts can also send messages to IM users from the meeting room. See “Integrating with Microsoft Live Communications Server 2005 and Microsoft Office Communications Server 2007” on page 59.

Configure a public key infrastructure If you’ve integrated Adobe Connect with an LDAP directory server, add a security layer by requiring client certificates. See “PKI (public key infrastructure)” on page 72.

Host Adobe Connect Add-in Users can download the Adobe Connect Add-in easily from Adobe servers. However, if your organization's security policy doesn't allow external downloads, host the add-in on your own server and still retain a great user experience. See "Hosting Adobe Connect Add-in" on page 70.

8. (Optional) Choose whether to install Adobe Connect in a cluster.

For more information, see "Choosing to deploy Adobe Connect in a cluster" on page 10.

9. (Optional) Choose whether to install edge servers.

For more information, see "Choosing to deploy Adobe Connect Edge Server" on page 12.

Choosing to deploy Adobe Connect in a cluster

It is possible to install all Adobe Connect components, including the database, on a single server, but this system design is best used for testing, not production.

A group of connected servers, each doing an identical job, is usually called a *cluster*. In an Adobe Connect cluster, you install an identical copy of Adobe Connect on each server in the cluster.

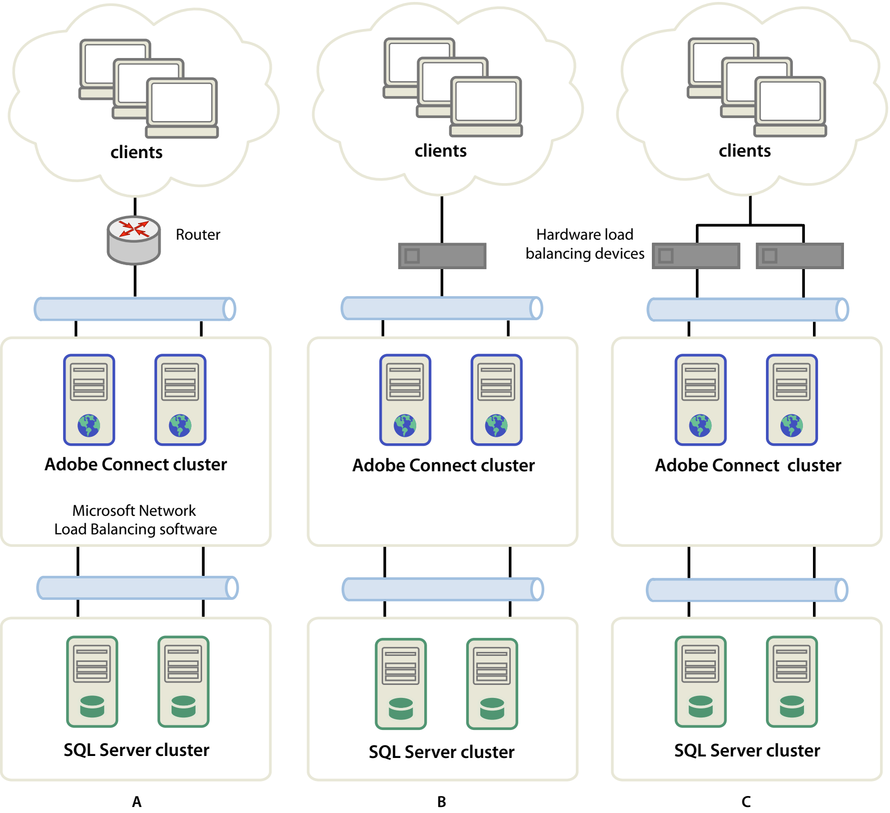
***Note:** When you install Adobe Connect in a cluster, you must use SQL Server 2005 Standard Edition and install it on a separate computer.*

If one host in the cluster fails, another host in the cluster can take over and host the same meeting. You must use third-party hardware or software to provide load balancing for the cluster. Often, load balancing hardware can also function as an SSL accelerator.

***Note:** In the Application Management Console you can configure shared storage so that content is stored on external devices and cached on the Adobe Connect server.*

Reliable networked systems are designed with redundant components; if one component fails, another identical (*redundant*) component can take over the same job. When a component fails and its counterpart takes over, *failover* has occurred.

Ideally, every component in a system should be redundant, not just Adobe Connect. For example, you could use multiple hardware load balancing devices (such as BIG-IP by F5 Networks), a cluster of servers hosting Adobe Connect, and SQL Server databases on multiple external computers. Build your system with as many redundancies as possible and add to your system over time.



Three clustering options
A. *A cluster with Network Load Balancing software and two external databases* ***B.*** *BIG-IP hardware load balancing devices, cluster, and two external databases* ***C.*** *Two BIG-IP load balancing devices, cluster, and two external databases*

More Help topics

"Deploy a cluster of Adobe Connect servers" on page 30

"Configuring shared storage" on page 52

Choosing a database

Adobe Connect uses a database to store information about users, content, courses, meetings, and reports. You can use the embedded database engine (included with the installer), or you can install Microsoft SQL Server 2005 Standard Edition (which must be purchased separately).

Note: *The embedded database engine is Microsoft SQL Server 2005 Express Edition.*

Embedded database

The embedded database engine is recommended for testing and development. It uses the same data structures as SQL Server 2005 Standard Edition, but it isn't as robust.

The embedded database engine has the following limitations:

- Because of licensing restrictions, you must install the embedded database engine on the same computer as Adobe Connect. The computer must be a single-processor computer.
- 2 GB is the maximum size of the database.
- The embedded database engine has a command-line interface, rather than a graphical user interface.

Microsoft SQL Server 2005 Standard Edition

It's a good idea to use the Microsoft SQL Server 2005 Standard Edition engine in production environments because it is a scalable database management system (DBMS) designed to support a large number of concurrent users. SQL Server 2005 Standard Edition also provides graphical user interfaces for managing and querying the database.

You can install SQL Server 2005 Standard Edition on the same computer as Adobe Connect or on a different computer. If you install them on different computers, synchronize the computers to the same time source. For more information, see the following TechNote: www.adobe.com/go/2e86ea67.

Install SQL Server in mixed login mode so that you can use SQL authentication. Set the database to case insensitive.

You must use SQL Server in the following deployment scenarios:

- You want to install the database on a computer that doesn't have Adobe Connect installed.
- Adobe Connect is deployed in a cluster.
- Adobe Connect is installed on multiprocessor computers with Hyper-Threading.

More Help topics

"Supported server-database configurations" on page 3

Choosing to install integrated telephony adaptors

During the Adobe Connect installation process, you have the option to install one or more telephony adaptors.

Each adaptor requires you to supply specific pieces of information. If you have the information, you can configure the adaptor during the initial installation of Adobe Connect. If you prefer, you can install the adaptor without configuring it. When you are ready to configure the adaptor, run the installer again. For more information, see "Preparing to install integrated telephony adaptors" on page 14.

Choosing to deploy Adobe Connect Edge Server

When you deploy Adobe Connect Edge Server on your network, clients connect to the edge server and the edge server connects to Adobe Connect (also called the *origin server*). This connection occurs transparently—to users, it appears that they are connected directly to the origin server hosting the meeting.

Edge servers provide the following benefits:

Decreased network latency Edge servers cache on-demand content (such as recorded meetings and presentations) and split live streams, resulting in less traffic to the origin. Edge servers place resources closer to clients.

Security Edge servers are an additional layer between the client Internet connection and the origin.

If your license permits it, you can install and configure a cluster of edge servers. Deploying edge servers in a cluster has the following benefits:

Failover When an edge server fails, clients are routed to another edge server.

Support for large events If you require more than 500 simultaneous connections to the same meeting, a single edge server will run out of sockets. A cluster allows more connections to the same meeting.

Load balancing If you require more than 100 simultaneous meetings, a single edge server may run out of memory. Edge servers can be clustered behind a load balancer.

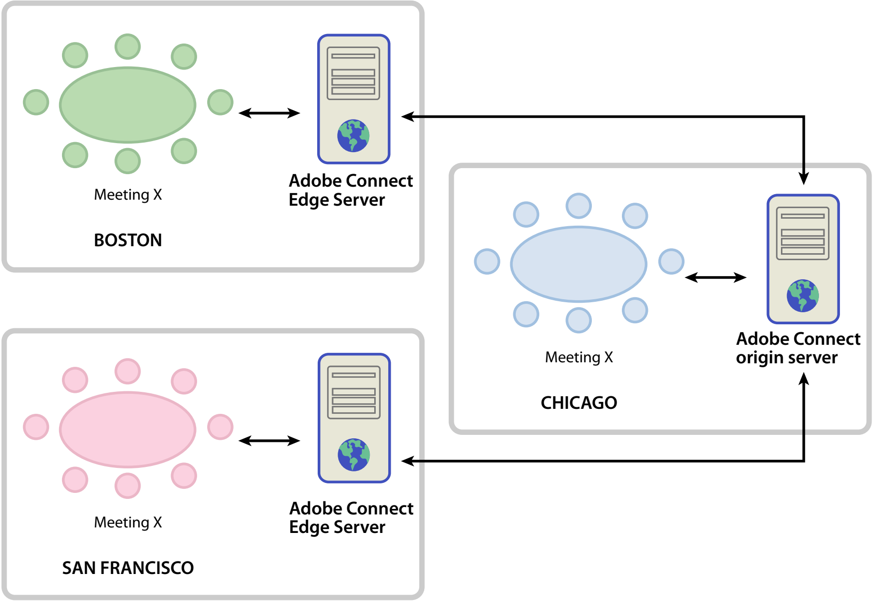
How edge servers work

Edge servers authenticate users and authorize their requests for web services such as Adobe Connect Meeting rather than forwarding every request to the origin server and consuming its resources for these tasks. If the requested data is found in the edge server's cache, it returns the data to the requesting client without calling Adobe Connect.

If the requested data is not found in the edge server's cache, the edge server forwards the client's request to the origin server, where the user is authenticated and the request for services is authorized. The origin server returns the results to the requesting edge server, and the edge server delivers the results to the requesting client. The edge server also stores this information in its cache, where other authenticated users can access it.

Sample edge server deployment

Consider the following sample edge server deployment:


Meeting X
Adobe Connect Edge Server
BOSTON
Meeting X
Adobe Connect origin server
CHICAGO
Meeting X
Adobe Connect Edge Server
SAN FRANCISCO

Clients on-site in Chicago use the origin located in a data center in Chicago. The edge servers in Boston and San Francisco aggregate local client requests and forward them to the origin. The edge servers receive the responses from the origin in Chicago and transmit them to clients in their zones.

More Help topics

"Install Adobe Connect Edge Server" on page 26

"Deploying Adobe Connect Edge Server" on page 33

Building and optimizing a VMWare environment

Installing Adobe Connect on VMWare is no different than installing it on a physical computer. For information about hardware, software, and configuration requirements, see the white paper about running Adobe Connect in a virtual environment.

Adobe Connect audio and video conferencing options

Adobe Connect supports two ways to connect to audio conferencing providers: Universal Voice and integrated telephony adaptors. Each solution has different benefits. You can configure one solution or both solutions for a single audio conferencing provider. You can configure any number of audio conferencing providers for an Adobe Connect account.

Universal Voice enables Adobe Connect to send and receive audio from any audio conferencing provider. You can record the audio along with your web conference and stream the audio to VoIP-only attendees.

Use Universal Voice to integrate video telephony devices that support SIP/H.264. Adobe Connect offically supports the Tandberg 990MXP and Edge 95 video conferencing devices, though other Tandberg H.264 devices should work as well. For more information, see the Tandberg website.

The Universal Voice solution uses a component called Flash Media Gateway that installs with Adobe Connect. Flash Media Gateway receives audio from a SIP server and sends it to Adobe Connect over RTMP. To use Universal Voice you need to host your own SIP server or have an account with a SIP provider. For information about configuring Flash Media Gateway, see “Deploying Universal Voice” on page 42.

After you have deployed Universal Voice, account administrators can use Adobe Connect Central to configure audio conference information. For more information, see Configure audio providers for universal voice.

Integrated telephony adaptors are Java extensions that provide communication between Adobe Connect and specific audio conferencing providers. Integrated telephony adaptors provide enhanced call control. You can install one or more telephony adaptors when you install Adobe Connect. For more information, see “Choosing to install integrated telephony adaptors” on page 12.

You can also use the Adobe Connect Telephony Java API to develop an integrated telephony adaptor for any audio conferencing provider.

The following table describes the features of both solutions:

	Universal Voice Audio Provider	**Integrated Telephony Adaptor**
Broadcast audio to VoIP-only attendees	Yes	No (unless adaptor is configured for Universal Voice)
Enhanced call control. For example, mute, hold, and so on.	No	Yes
Record audio with Adobe Connect meeting	Yes	Yes
Requires Flash Media Gateway (bundled in the Adobe Connect installer)	Yes	No (unless adaptor is configured for Universal Voice)

Preparing to install integrated telephony adaptors

Integrated telephony adaptors provide communication between Adobe Connect and specific audio conferencing providers. Integrated adaptors have advanced call capabilities, allowing hosts and presenters to control the audio conference from the meeting.

To install integrated telephony adaptors, run the Adobe Connect installer.

Each adaptor requires you to supply specific pieces of information during when you install it. For more information, see:

- “Avaya telephony adaptor” on page 15
- “Cisco Unified MeetingPlace telephony adaptor” on page 16

- “InterCall telephony adaptor” on page 16
- “MeetingOne telephony adaptor” on page 17
- “PGi (formerly Premiere Global) NA or EMEA telephony adaptor” on page 18
- “Arkadin telephony adapter” on page 19

Note: *You can enable multiple audio bridges for Adobe Connect Server. Meeting hosts choose which audio bridge to use when they create a meeting in Adobe Connect Central. Each meeting can have only one audio bridge.*

Avaya telephony adaptor

The Avaya Meeting Exchange™ telephony adaptor allows meeting hosts, presenters, and participants to control audio conference features from Adobe Connect meeting rooms. Complete the following workflow to enable the telephony adaptor.

Working with Avaya customer support

It’s a good idea to involve Avaya customer support early in the planning process. Make certain that you have the contact information for the Avaya account representative and Avaya customer support available. Contact Avaya support to inform them that you are installing and using the adaptor and gather information about the bridge.

Note: *A current maintenance contract with Avaya covering the audio bridge is required.*

1 Contact Avaya Customer Support.

2 Request the following information:

- The IP address of the bridge

  Communication between Adobe Connect and the telephony adaptor takes place through the Avaya bridge.

- An administration login

  Use the administration login to configure and restart the bridge, change the number of operators, add new users, and view statistics.

  Note: *Avaya uses an additional login for root access. Avaya does not usually supply that login to customers. For operations that require root access, contact Avaya Customer Support.*

- A file access login

  Use the file access login to connect to the recording files directory.

- A Bridge Talk user name and password

  Bridge Talk is an application to manage conferences and callers on the Avaya Meeting Exchange Audio Conference Bridge. Use Bridge Talk to determine if there is a problem with the bridge or the adaptor. You can also use this program to dial phone numbers; create, schedule, and manage new conferences; view running conferences; and monitor bridge activity. For more information, including a User Guide, see www.avaya.com.

3 Verify that you have FTP access to the recording files directory by entering the following from an FTP prompt:

```
ftp://bridgeIPAddress
ftp>dcbguest:abc123@machineNameOrIPAddress
ftp>cd /usr3/confrp
ftp>bye
```

Information needed when installing

Items marked with an asterisk (*) are required.

Enable Dial Out Select this option to enable system-wide dial out. If you don't select this option, any selections you make for the following four entries are ignored. If you do select this option, use the following four entries to specify how dial out is implemented.

Enable Dial Out for Host Select this option to permit the meeting host to dial out.

Enable Dial Out for Presenter Select this option to permit the presenter to dial out.

Enable Dial Out for Participant Select this option to permit participants to dial out.

Enable "Call Me" Dialog If dial out is enabled, select this option to display the "Call Me" dialog box to participants when they join a meeting.

Meeting Exchange Host Name* The hostname or address of the Avaya Meeting Exchange server.

Phone Operator ID* The ID of the operator channel used to associate with the Meeting Exchange server.

Login ID* The Login ID used to establish a connection with the Meeting Exchange Server.

Password* The password used with the Login ID to connect to the Avaya Meeting Exchange server.

FTP Directory* The FTP directory for audio files on the Avaya Bridge.

FTP Login* User name for FTP login.

FTP Password* Password for FTP login.

Meeting Exchange Dial In Number* A valid phone number dialed by Adobe Connect to reach the Meeting Exchange server.

Cisco Unified MeetingPlace telephony adaptor

The MeetingPlace telephony adaptor allows meeting hosts, presenters, and participants to control audio conference features from Adobe Connect meeting rooms.

Information needed while installing

Items marked with an asterisk (*) are required.

CISCO Unified MeetingPlace Server* URL for the MeetingPlace server

CISCO Unified MeetingPlace Administrator* The ID you use to conect to MeeetingPlace server as an administrator.

CISCO Unified MeetingPlace Password* Password for the MeetingPlace administrator account.

Confirm Password retype the password for the MeetingPlace administrator account.

InterCall telephony adaptor

The InterCall telephony adaptor allows meeting hosts, presenters, and participants to control audio conference features from Adobe Connect meeting rooms. This adaptor requires a VoIP or SIP provider and Flash Media Gateway (Universal Voice) for recording meetings. Complete the following workflow to enable the telephony adaptor.

Planning for deployment

To deploy the InterCall adaptor, certain ports must be available, as shown in the following table:

Port	Description
80	InterCall uses port 80 to communicate with Adobe Connect over HTTP. This port must be open for incoming communication, to be able to receive callbacks from InterCall to Adobe Connect.
443	InterCall uses port 443 to communicate with Adobe Connect over HTTPS (SSL). This port must be open for incoming communication, to be able to receive callbacks from InterCall to Adobe Connect.
8443	Adobe Connect uses port 8443 to communicate with InterCall over HTTPS (SSL). Adobe Connect uses this port for CCAPI and authorization services. This port must be open so that outgoing messages can be sent from Adobe Connect to InterCall.
9080	As mentioned earlier, this port is required for telephony in general. For InterCall, however, it must additionally be opened on the firewall for each node in a cluster.

Information needed when installing

Items marked with an asterisk (*) are required.

Enable Dial Out Select this option to enable system-wide dial out. If you don’t select this option, any selections you make for the following four entries are ignored. If you do select this option, use the following four entries to specify how dial out is implemented.

Enable Dial Out for Host Select this option to permit the meeting host to dial out.

Enable Dial Out for Presenter Select this option to permit the presenter to dial out.

Enable Dial Out for Participant Select this option to permit participants to dial out.

Enable “Call Me” Dialog If dial out is enabled, select this option to display the "Call Me" dialog box to participants when they join a meeting.

CCAPI Host* URL for the InterCall CCAPI service

CCAPI Auth Host* URL for the InterCall CCAPI authorization service.

Client Callback URL* Callback URL used the InterCall service to call back to Adobe Connect. This URL must be publicly accessible.

Application Token* Value used to identify your connection with the InterCall audio service.

Country Codes* List of country codes for which Adobe Connect displays available conference service numbers.

Toll Free Number Country Code The country code whose conference number is toll-free; for example, US.

MeetingOne telephony adaptor

The MeetingOne telephony adaptor allows meeting hosts, presenters, and participants to control audio conference features from Adobe Connect meeting rooms.

Information needed when installing

Items marked with an asterisk (*) are required.

Enable Dial Out Select this option to enable system-wide dial out. If you don’t select this option, any selections you make for the following four entries are ignored. If you do select this option, use the following four entries to specify how dial out is implemented.

Enable Dial Out for Host Select this option to permit the meeting host to dial out.

Enable Dial Out for Presenter Select this option to permit the presenter to dial out.

Enable Dial Out for Participant Select this option to permit participants to dial out.

Enable “Call Me” Dialog If dial out is enabled, select this option to display the "Call Me" dialog box to participants when they join a meeting.

MeetingOne API URL* URL for the MeetingOne audio conference API service.

SSH Specifies whether SSH downloading of recordings is enabled.

Telephony API Server Login* The ID you use to for the MeetingOne audio conference API service.

Telephony API Server Password* Password for the administrator account.

Confirm Password retype the password for the MeetingPlace administrator account.

PGi (formerly Premiere Global) NA or EMEA telephony adaptor

The PGi telephony adaptor allows meeting hosts, presenters, and participants to control audio conference features from Adobe Connect meeting rooms. The information in this section applies to both the PGi NA and the PGi EMEA adaptors.

Information needed when installing

Items marked with an asterisk (*) are required.

Enable Dial Out Select this option to enable system-wide dial out. If you don’t select this option, any selections you make for the following four entries are ignored. If you do select this option, use the following four entries to specify how dial out is implemented.

Enable Dial Out for Host Select this option to permit the meeting host to dial out.

Enable Dial Out for Presenter Select this option to permit the presenter to dial out.

Enable Dial Out for Participant Select this option to permit participants to dial out.

Enable “Call Me” Dialog If dial out is enabled, select this option to display the "Call Me" dialog box to participants when they join a meeting.

Note: *The next four values are supplied to you by PGi.*

PGi Hostname* The host name or IP address of the PGi audio conference service. For PGi NA, this value is usually csaxis.premconf.com. For PGi EMEA, this value is usually euaxis.premconf.com.

PGi Port Number* The port number that Adobe Connect uses to connect to the PGi audio conference service. This value is usually 443.

PGi Web ID* The ID you use when you connect to the PGi audio conference service.

PGi Password* The password you use when you connect to the PGi audio conference service.

Recording Download Login* The login used to download audio recordings from the PGi audio conference service.

Download Password* The password used with the Recording Download Login to retrieve recordings from the PGi audio conference service.

Download URL The URL that Adobe Connect uses to download recordings from the PGi audio conference service. The default value is for PGi NA is https://ww5.premconf.com/audio/. The default value for PGi EMEA is http://eurecordings.premiereglobal.ie/audio/.

Arkadin telephony adapter

The Arkadin telephony adaptor allows meeting hosts, presenters, and participants to control audio conference features from Adobe Connect meeting rooms. This adaptor requires a VoIP or SIP provider and Flash Media Gateway (Universal Voice) for recording meetings. Complete the following workflow to enable the telephony adaptor.

Planning for deployment

For Arkadin telephony adapter to work, you must get the host IP address of your Adobe Connect Server running telephony services, whitelisted on the firewall of Arkadin. Since the IP address is allowed on Arkadin's firewall, the Adobe Connect Server hosting Arkadin services, must have a public IP address.

For more information, see http://www.arkadin.com/.

Information needed when installing

Enable Dial Out Select this option to enable system-wide dial out. If you don't select this option, any selections you make for the following four entries are ignored. If you select this option, use the following four entries to specify how dial out is implemented.

Enable Dial Out for Host Select this option to permit the meeting host to dial out.

Enable Dial Out for Presenter Select this option to permit the presenter to dial out.

Enable Dial Out for Participant Select this option to permit participants to dial out.

Arkadin client application identifier* Arkadin client application identifier (provided by Arkadin, no default value).

Arkadin server URL* Arkadin server URL (provided by Arkadin, no default value).

Adobe Connect external hostname* Adobe Connect external hostname (https://[external-hostname]/servlet/bamboo/ is the default value).

Arkadin Access Number server URL* Arkadin access number server URL (provided by Arkadin, no default value).

Arkadin authentication server URL* Arkadin authentication server URL (provided by Arkadin, no default value.

Chapter 2: Installing Adobe Connect

After reviewing and gathering required information (see "Preparing for migration, installation, and configuration" on page 1), you are ready to install Adobe® Connect™.

Install Adobe Connect 9

Run the installer

1 Verify that the computer is connected to the internet.

2 Log on to the computer as an Administrator.

3 Close all applications.

4 Set JAVA_HOME environment variable.

5 Extract the files from the Adobe Connect 9 ESD file to a location on your hard disk, such as C:\Connect_9_ESD. This folder is referred to as *extract-dir* in this document.

6 Double-click the install.exe file located at *[extract_dir]*\Adobe Connect\Disk1\InstData\VM\install.exe.

7 Select a language and click OK to continue.

8 On the Introduction screen click Next to continue.

9 On the License Agreement screen read the agreement, select I Accept the terms of the License Agreement, and click Next.

10 On the Deployment Options screen, select Deploy Adobe Connect to install Adobe Connect.

11 Do one of the following to select the Adobe Connect installation location:

- Click Next to accept the default Adobe Connect installation location (C:\Connect), or click Choose to select a different location.

***Note:** When you install Adobe Connect, the files are installed at C:\Connect\9.0.0.1, and referred to as [root_install_dir] in this document. However, the content and logs folder are placed in C:\Connect. This means that subsequent installs will share content and logs location, but files will be in their own version folder C:\Connect\9.0.0.1. If you're migrating from an earlier release, all files except content and logs are backed up.*

- If you've chosen a different location and decide to use the default location instead, click Restore Default.
- If Adobe Connect is already installed on this computer, the Update Existing Install screen appears. Select the check box to confirm you've backed up your database and the Adobe Connect root directory.

12 Enter your serial number and click Next.

13 Click the link to download your license file from Adobe. Click Choose and browse to the downloaded license file. Click Next.

14 Choose products to install and click Next to continue:

***Note:** Adobe CQ related options can be selected only if your license has events enabled. Otherwise the CQ options are greyed out.*

- Adobe Connect Server
- Flash Media Gateway (Universal Voice)

Note: *Flash Media Gateway requires an upstream SIP/VoIP provider. For more information, see "Adobe Connect audio and video conferencing options" on page 14.*

- CQ Author Server

Note: *Select only this option to install only CQ Author server on a machine. If you want to install CQ Author server on a machine where Adobe Connect Server is already installed, you must remove the existing installation of Adobe Connect Server. Proceed with installing both the servers. Otherwise, the installer assumes an upgrade scenarios and proceeds accordingly.*

- CQ Publish Server

Note: *Select only this option to install only CQ Publish server on a machine. If you want to install CQ Publish server on a machine where Adobe Connect Server is already installed, you must remove the existing installation of Adobe Connect Server. Proceed with installing both the servers. Otherwise, the installer assumes an upgrade scenarios and proceeds accordingly.*

- PGi (NA) Telephony Adaptor
- PGi (EMEA) Telephony Adaptor
- Cisco Unified MeetingPlace
- Avaya Telephony Adaptor
- InterCall Telephony Adaptor

Note: *If you want to use the InterCall adaptor, you must install Flash Media Gateway.*

- Arkadin Telephony Adaptor
- MeetingOne Telephony Adaptor
- Presence Server

15 On the Embedded Database Engine screen, do one of the following:

- If you plan to install a database on a different computer, select Do not install the embedded database engine.
- To install the embedded database, select Install the embedded database engine. To install to the default location, click Next. To select a different location, click Choose.

Note: *If the installer detects that Microsoft SQL Server is already installed on this computer, the installer does not install the database. If you're migrating and are already using the embedded database, Adobe Connect uses the existing database. However, sometimes the installer detects an old version of SQL Server that doesn't work with Adobe Connect. Follow the steps in "Uninstalling Adobe Connect" on page 27 and start the installation again.*

16 If you installed the embedded database engine, enter a strong password and confirm it, and then click Next.

17 Set values for the database connection settings listed below, then click Next. Items marked with an asterisk (*) are required.

- **Host*** The host name of the computer on which the database is installed. If you installed the embedded database, the value is `localhost`.
- **Port*** The port the database uses to communicate with Adobe Connect. The default value is 1433.
- **Database Name*** The name of the database. The default value is `breeze`.
- **User*** The name of the database user. If you installed the embedded database, the default value is `sa`.
- **Password*** The password for the database user. If you installed the embedded database, you set the password in the previous step.

18 Set values for the network settings listed below, then click Next. Items marked with an asterisk (*) are required.

- **Account Name*** A name that identifies the Adobe Connect account, such as “Adobe Connect account”.
- **Adobe Connect Host*** A Fully Qualified Domain Name (FQDN) clients use to connect to Adobe Connect. For example, if the URL of the account is http://connect.example.com, the Adobe Connect Host value would be connect.example.com (without the leading http://).
- **Installation Type** Select the type of installation as Single or Cluster.

19 Set values for the mail settings listed below, then click Next. Items marked with an asterisk (*) are required.

- **SMTP Host** The host name of the computer hosting the SMTP mail server.
- **SMTP Username** The username used to authenticate against the SMTP host. If this field is left blank, Adobe Connect tries to send e-mails without authenticating with the SMTP server.
- **SMTP Password** The password for the SMTP username.
- **System E-mail*** The e-mail address to which administrative messages are addressed.
- **Support E-mail*** The e-mail address to which Adobe Connect user support requests are sent.
- **BCC E-mail** A blind-copy e-mail address to which all user notifications are also sent. This variable allows administrative tracking of e-mail messages sent through Adobe Connect without exposing an internal e-mail address.

20 Enter values for the shared storage settings listed below, then click Next.

- **Shared Storage** A volume and directory on an external server where content is stored, for example, \\volume\directory. If you want to store content on multiple volumes, separate them with semicolons (;). Before configuring this feature, see “Configuring shared storage” on page 52.
- **Content Cache Size** An integer from 1 through 100 specifying the percent of free disk space to use to store content on Adobe Connect. The cache can grow beyond the percent you specify, so it’s a good idea to keep the value from 15 through 50. If you leave the box blank or enter 0, no cache is used, and content is mirrored on Adobe Connect or any external volumes. Before configuring this feature, see “Configuring shared storage” on page 52.

21 If you choose to install CQ servers, specify the External Host Settings.

- **Is your CQ environment is SSL enabled?** Select the checkbox, if you plan to access CQ setup via https.
- **CQ Author server URL*** Provide the FQDN of the CQ Author server, along with the port. If CQ Author server is clustered, provide the load balancer URL.
- **CQ Publish server URL*** Provide the FQDN of the CQ Publish server, along with the port. If CQ Publish server is clustered, provide the load balancer URL.
- **Adobe Connect Host Cookie Prefix*** A text string that is used as a prefix for the Adobe Connect Host cookie.

22 If you choose to install the CQ Author server, specify the cluster and author settings.

- **Is CQ Author Server clustered** Select the checkbox if your CQ Author server is a cluster.
- **Node designation*** If your CQ Author server is clustered, then one node is designed as the master node and all the other nodes are designated as Slave. Choose the node designation of the machine on which you are installating CQ Author server.
- **Master Node IP*** Provide the IP of the master node if you are installing CQ Author instance on a slave node.

Note: *While installing a slave node the corresponding Master node must bedeployed over the network.*

- **Hostname (ie http://)*** Specify the hostname URL of the author.
- **Port*** Specify the port of the CQ Author server. The default value is 4502.

- **Publish Hosts*** Specify the FQDN and port of all the Publish servers.

23 If you choose to install CQ Publish server, specify its settings.

- **Hostname (ie http://)*** Specify the hostname of the CQ Publish server.
- **Port*** Specify the port of the Publish server. Default value if 4503.
- **Adobe Connect Host Cookie Prefix*** A text string that is used as a prefix for the Adobe Connect Host cookie.

Note: *Cookie prefix you specify here, must exactly match the cookie prefix specified on the External Host Settings screen.*

24 If you install CQ Author or Publish server, create a password for CQ administration.

Note: *Credentials of CQ administrators must be exactly the same for all the CQ Author and Publish servers.*

25 If you chose to install Flash Media Gateway, enter the following settings and click next. The settings do not take effect instantaneously. When you click OK to confirm the settings, Adobe Connect may restart all Flash Media Gateway servers. The settings are pushed to all Flash Media Gateway servers in a cluster.

- **Username** The username for the SIP profile that Flash Media Gateway server uses to create SIP sessions, for example sipUN1.
- **Password** The password for the SIP profile that Flash Media Gateway server uses to create SIP sessions.
- **SIP Address** The address of the SIP server for the SIP profile that Flash Media Gateway server uses to create SIP sessions, for example, 10.12.13.14.
- **Default Host** The default host for the SIP profile. This parameter is the SIP server address to use if registration with the SIP server fails. This parameter is usually set to the same value as SIP Address.
- **Port Lower Limit** The lowest port number that can be used for RTP audio data. The default value is 5000.
- **Port Upper Limit** The highest port number that can be used for RTP audio data. The default value is 6000.
- **Registration Expiration** The interval, in seconds, at which Flash Media Gateway renews its registration with the SIP server. The default value is 2400 seconds (40 minutes).
- **SIP Port** The port on which Flash Media Gateway server listens for SIP requests. The default value is 5060.
- **Registration** Choose whether a Flash Media Gateway server must register on the SIP server.

26 Fill in the requested values to create an account administrator, and then click Next.

Every Adobe Connect account needs at least one administrator to perform tasks in the Adobe Connect Central web application. Upgraded accounts already have at least one account administrator, but you can add an additional one here.

If the person installing Adobe Connect is not the Administrator who will maintain Adobe Connect, then select the option to change the password at next login.

27 Fill in requested information for any telephony adaptors you want to install. For more information on telephony adaptors, see "Choosing to install integrated telephony adaptors" on page 12.

If you don't have all the required information but want to install the adaptor anyway, select Install But Do Not Configure. When you are ready to enter the required information, run the installer again.

28 Review the Pre-Installation summary. Click Previous to change these settings. Click Install to install the software.

29 On the Initializing Adobe Connect service screen, do one of the following and click Next:

- Select Start Adobe Connect... (recommended). Choose to open Connect or the Application Management Console.
- Select Do not start Connect now.

30 If you chose to start Adobe Connect, a message reports that the service is starting.

31 Click Done to quit the Installer.

32 If you chose to open Adobe Connect, Adobe Connect Central opens. If you chose to open the Application Management Console, it opens.

33 Verify your installation.

Follow the instructions in the next section to ensure that your installation of Adobe Connect is configured and functioning as expected.

Verify your installation

Perform the following tasks to confirm that your installation was successful and that all standard components are working correctly. When you are ready to deploy Adobe Connect, see "Deploying and configuring Adobe Connect" on page 29.

To change configuration settings you entered in the installer, use the Application Management Console. Choose Start > Programs > Adobe Connect Server > Configure Connect Server.

Installation log is created in the *[extract_dir]*\Connect\9.0.0.1\Disk1\InstData\VM\ folder. Incase this location is read-only, the log file is created in the {user folder}\Local Settings\Temp\AdobeConnect.

Log in to Adobe Connect Central

Adobe Connect Central is a web application that lets you administrate Adobe Connect Server. If you can log in to Adobe Connect Central, the database and Adobe Connect Server can communicate with each other.

1 Open a browser and enter the following URL: http://*[hostname]*.

Note: *The [hostname] parameter is the value you set for Adobe Connect Host in the Network Settings screen in the installer.*

2 Enter the user name and password for the account administrator you created in the installer.

Note: *After you create additional users, you can log in to Adobe Connect Central with any user account.*

Verify that Adobe Connect services are started

Adobe Connect Server runs as the following Windows services:

- Adobe Connect Presence Server
- Adobe Connect Service
- Adobe Connect Telephony Service
- Flash Media Administration Server
- Flash Media Gateway
- Flash Media Server (FMS)
- CQ Author server
- CQ Publish server

More Help topics

"Start and stop the servers" on page 80

Verify that you can send e-mail notifications

If you didn’t enter a value in the SMTP Host field in the Installer, Adobe Connect cannot send e-mail notifications. If you entered an SMTP Host, do the following to verify that Adobe Connect can send e-mail notifications:

1 Click the Administration tab on the Adobe Connect Central home tab.

2 Click the Users and Groups tab.

3 Click New User.

4 On the New User Information page, enter the required information. A partial list of options follows:

E-mail Use the new user’s e-mail address. Make sure the E-mail the new user account information, login, and password option is selected.

New Password Create a password of 4 to 16 characters.

5 Click Next to continue.

6 Under the Edit Group Membership heading, select a group, assign the user to the group, and click Finish.

7 Allow enough time for the user to check for the e-mail notification.

If the user received the notification, Adobe Connect is functional and you can send e-mail messages using your e-mail server.

8 If the e-mail doesn’t arrive, do the following:

a Make sure the e-mail address is valid.

b Make sure the e-mail wasn’t filtered as spam.

c Make sure that you configured Adobe Connect with a valid SMTP host, and make sure the SMTP service works outside Adobe Connect.

d Contact Adobe Support at www.adobe.com/support/programs/connect.

Verify that you can use Adobe Presenter

To verify that you can use Adobe Presenter, publish a Microsoft PowerPoint presentation to Adobe Connect for compilation into a Flash presentation, and then view it.

1 If you haven’t already done so, install Adobe Presenter on a desktop client machine on which PowerPoint is already installed.

2 Launch a browser and open Adobe Connect Central using the FQDN of your Adobe Connect server (for example, connect.example.com).

3 Click Resources > Getting Started.

4 On the Getting Started page, click on Publish Presentations > Install Adobe Presenter.

5 Run the installer.

6 If you don’t have a PowerPoint presentation, create and save a presentation of one or two slides.

7 Open the Adobe Connect Publish wizard by selecting Publish from the Adobe Presenter menu in PowerPoint.

8 Select Connect and enter the information for your server.

9 Log in with your e-mail address and password, and follow the steps in the Publish wizard. Make sure that you are enrolled in the Authors group (Administration > Users and Groups in Adobe Connect Central).

When you complete the steps in the Publish wizard, Adobe Presenter uploads your PowerPoint presentation to Adobe Connect, which compiles into a Flash presentation.

10 When the compilation is complete, go to the Content tab in Adobe Connect Central and search for your presentation.

11 Open your presentation to view it.

Verify that you can use Training (if enabled)

***Note:** Adobe Connect Training is an optional feature that must be enabled in your license.*

❖ Go to the Training tab in Adobe Connect Central.

If the Training tab is visible and accessible, Training is functioning. Make sure that you are enrolled in the Training Managers group (Administration > Users and Groups).

Verify that you can use Meeting (if enabled)

***Note:** Adobe Connect Meeting is an optional feature that must be enabled in your license.*

To verify that Adobe Connect Meeting is functional, you must be enrolled in the Meeting Hosts group or the Administrators group.

1 Log in to Adobe Connect Central as a user who is enrolled in the Meeting Hosts group or the Administrators group.

2 Click the Meetings tab and select New Meeting.

3 On the Enter Meeting Information page, enter the required information. For the Meeting Access option, select the Only Registered Users and Accepted Guests May Enter the Room option. Click Finish to create the meeting.

4 Click the Enter Meeting Room button.

5 Log in to enter the meeting as a Registered User.

6 If the Adobe Connect Add-in window appears, follow the instructions to install it.

If the meeting room opens, Adobe Connect Meeting is functional.

Verify that you can use Events (if enabled)

***Note:** Adobe Connect Events is an optional feature that must be enabled in your license.*

1 Log in to Adobe Connect Central as a user who is enrolled in the Events Managers group or the Administrators group.

2 Go to the Event Management tab in Adobe Connect Central.

If this tab is visible and accessible, Adobe Connect Events is functioning.

Install Adobe Connect Edge Server

Follow the steps below if you want to install the Adobe Connect Edge Server.

Run the installer

1 Close all other applications.

2 Navigate to the location of the files you extracted when you installed Adobe Connect, such as C:\Connect_9. Then double-click the [extract-dir]\Adobe Edge Server\AdobeConnectEdgeServerx.exe file.

3 Select a language from the Select Setup Language dialog box. Click OK to continue.

4 On the Setup screen click Next to continue.

5 On the License Agreement screen, read the agreement, select I Accept The Agreement, and click Next.

6 Do one of the following:

- Click Next to accept the default installation location (C:\Connect), or click Browse to select a different location, and then click Next.
- If Adobe Connect Edge Server is already installed on this computer, the Update Existing Adobe Connect Edge Server Install screen appears. Click Next.

7 On the Select Start Menu Folder screen do one of the following:

- Click Next to accept the default location of the Start Menu shortcuts.
- Click Browse to select a different location.

8 In the Ready To Install dialog box, review the location where Adobe Connect Edge Server will be installed and where the Start Menu folder will be installed. Click Back to review or change these settings, or click Install.

9 Click Finish to exit the Adobe Connect Edge Server installation.

More Help topics

"Deploying Adobe Connect Edge Server" on page 33

Uninstalling the servers

If you want to uninstall the servers, follow the instructions in this section.

Uninstalling Adobe Connect

***Note:** Uninstalling Adobe Connect does not uninstall SQL Server and user-generated data such as, log files and content folders.*

1 Select Start > Programs > Adobe Connect Server > Uninstall Connect Server.

***Important:** The root folder (deleted in the following step) contains the custom.ini and config.ini files and the content files. If you want to keep the content, copy these files to another location.*

2 Delete the root Adobe Connect folder. By default, the location is C:\Connect. This folder contains the following folders: 8.1.0.0, logs, and content. The Adobe_Connect_Install.log file is located in the 8.1.0.0 folder.

3 (Optional) Uninstall Microsoft SQL Server. For information, see http://msdn.microsoft.com.

Uninstalling Adobe Connect Edge Server

1 Select Start > Settings > Control Panel > Add or Remove Programs > Adobe Connect Edge Server > Remove.

2 Delete the root Adobe Connect folder. By default, the location is C:\Connect.

Uninstalling Flash Media Gateway

Flash Media Gateway uninstalls when you uninstall Adobe Connect. You can also run the following program to uninstall Flash Media Gateway: Program Files\Adobe\Flash Media Gateway\Uninstall_Flash Media Gateway\Uninstall Flash Media Gateway.exe.

Chapter 3: Deploying and configuring Adobe Connect

After you install Adobe® Connect™, Flash Media Gateway, or Adobe Connect Edge Server and complete the first phase of configuration with the Application Management Console, configure any of these optional features and deploy the server.

Use the Application Management Console to configure Adobe Connect Server

Use the Application Management Console to configure Adobe Connect Server application settings and directory service settings and to see which features are enabled on your server.

When you install the server, the installer prompts you to enter the application settings. After you install the server, you can use the Application Management Console to edit these settings.

To configure directory service settings, open the Application Management Console after you install the server.

❖ To open the Application Management Console, do one of the following:

- Choose Start > Programs > Adobe Connect Server > Configure Adobe Connect Server.
- In a browser, open the following URL: http://localhost:8510/console.

***Note:** If another application is running on port 80, the Application Management Console cannot open. Stop the application running on port 80 and reopen the Application Management Console. To check whether an application is running on port 80, open the Command Prompt and enter **netstat -a -n -o | findstr LISTEN | findstr ":80 "**.*

More Help topics

"Integrating with a directory service" on page 35

"Deploying Universal Voice" on page 42

Deploying Adobe Connect

Deploy Adobe Connect server

1 On your DNS server, define a fully qualified domain name (FQDN) for Adobe Connect (such as connect.mycompany.com). Map the domain name to the static IP address of the computer hosting Adobe Connect.

2 If you want Adobe Connect to be available outside your network, configure the following ports in a firewall:

80 The default port for the Adobe Connect application server. The tertiary port for the meeting server (Flash Media Server).

1935 The default port for the meeting server (Flash Media Server).

443 The default port for SSL. The secondary port for the meeting server (Flash Media Server).

***Note:** If Adobe Connect traffic is routed through a gateway (with a different IP address), make sure any firewall is configured to accept requests from the gateway IP address.*

To restore the customizations, redo them in the new ConnectProSvc.conf.

For help deploying Adobe Connect, contact Adobe Support at www.adobe.com/support/programs/connect.

More Help topics

"Port requirements" on page 1

Deploy a cluster of Adobe Connect servers

1 Install and configure Adobe Connect on a dedicated server.

Use the same serial number and license file each time you install Adobe Connect. Do not install the embedded database engine and, if your shared storage requires a user name and password, do not start Adobe Connect from the installer.

2 If your shared storage requires a user name and password, do the following to add them to the Adobe Connect Service:

a Open the Services control panel.

b Double-click Adobe Connect Service.

c Click the Log On tab.

d Click the This account radio button and enter the shared storage user name into the box. The user name syntax is [subdomain\]username.

e Enter and confirm the shared storage password.

f Click Apply then click OK.

3 Do the following to start Adobe Connect:

a In the Services control panel, select Flash Media Server (FMS) and click Start the service.

b In the Services control panel, select Adobe Connect Service and click Start the service.

4 Choose Start > Programs > Adobe Connect Server > Configure Adobe Connect Server to open the Application Management Console. Click Next.

5 On the Database Settings screen, enter the information for the SQL Server database and click Next.

If Adobe Connect successfully connected to the database, you see a confirmation and the Database Settings. Click Next.

6 On the Server Settings screen, do the following and click Next:

a Enter an account name.

b In the Adobe Connect Host box, enter the name of the computer running the load balancer.

c Enter an HTTP port number. This number could be 80 or 8080 depending on the load balancer.

d Enter the external name of the cluster node.

e Enter the domain name of the SMTP host and system and support email addresses.

f If you're using shared storage, enter the path to the volume or volumes (separate multiple volumes with semicolons).

g Enter the percentage of the Adobe Connect server you want to use as a local cache.

***Note:** Content is written to the local cache and the shared storage volume. Content is kept in the local cache for 24 hours after it was last used. At that time, if the cache percentage has been exceeded, the content is purged.*

7 Upload the license file and click Next.

8 Create an administrator and click Finish.

9 Repeat steps 1 though 8 for each server in the cluster.

10 To configure the load balancer do the following:

a Configure the load balancer to listen on port 80.

b Add all cluster node names to the configuration file of the load balancer.

Note: *For detailed information about configuring the load balancer, see the vendor documentation.*

11 Open a web browser and enter the domain name of the load balancer, for example, http://connect.mycompany.com.

For help deploying a cluster, contact Adobe Support at www.adobe.com/support/programs/connect.

More Help topics

"Install Adobe Connect 9" on page 20

"Configuring shared storage" on page 52

Verifying operations in a cluster

If one computer in a cluster shuts down, the load balancer routes all HTTP requests to a running computer in the cluster.

When a meeting starts, the application server assigns a primary and backup host to the meeting room based on load. When the primary host shuts down, clients reconnect to the backup host.

It's also a good idea to verify that content uploaded to one server in a cluster is replicated to the other computers in the cluster.

The following procedures assume that the cluster contains two computers, Computer1 and Computer2.

Verifying load balancing and meeting failover

1 Start Adobe Connect on both computers.

a Select Start > Programs > Adobe Connect Server > Start Adobe Connect Meeting Server.

b Select Start > Programs > Adobe Connect Server > Start Adobe Connect Central Application Server

2 Log in to Adobe Connect Central from the following URL:

http://*[hostname]*

For *hostname*, use the Adobe Connect Host value you entered in the Application Management Console.

3 Select the Meetings tab and click a meeting link to enter a meeting room.

Create a new meeting if necessary.

4 Stop Adobe Connect on Computer2.

a Select Start > Programs > Adobe Connect Server > Stop Adobe Connect Central Application Server

b Select Start > Programs > Adobe Connect Server > Stop Adobe Connect Meeting Server.

If meeting failover was successful, the meeting should still have a green connection light.

5 In Adobe Connect Central, click on any tab or link.

If the load balancer is working, you should still be able to send successful requests to Adobe Connect Central and receive responses.

If the cluster contains more than two computers, apply this start-stop procedure to each computer in the cluster.

Verify content replication

1 Start Adobe Connect on Computer1.

a Select Start > Programs > Adobe Connect Server > Start Adobe Connect Meeting Server.

b Select Start > Programs > Adobe Connect Server > Start Adobe Connect Central Application Server

2 Stop Adobe Connect on Computer2.

a Select Start > Programs > Adobe Connect Server > Stop Adobe Connect Central Application Server

b Select Start > Programs > Adobe Connect Server > Stop Adobe Connect Meeting Server.

3 Log in to Adobe Connect Central from the following URL:

http://*[hostname]*

For *hostname*, enter the Adobe Connect Host value you entered in the Application Management Console.

4 Upload a JPEG image or other content to Adobe Connect on Computer1:

- Make sure that you are a member of the Authors group. (If you are an Account Administrator, you can add yourself to the Authors group in Adobe Connect Central.)
- Click the Content tab.
- Click New Content and follow the steps displayed in your browser for adding content.

After your test content is uploaded, a User Content page opens and displays a list of the content that belonged to you.

5 Click the link to the newly uploaded test content.

A Content Information page with a URL for viewing your test content opens.

6 Make a note of the URL; you will use it in step 10.

7 Click the URL.

8 Start Computer2, wait until Adobe Connect has fully started, and then stop Computer1.

If you have configured an external storage device, you don’t need to wait for Computer2 to stop; the required content is copied from the external device.

9 Close the browser window in which you were viewing the test content.

10 Open a new browser window and go to the URL to view your test content.

If your test content is displayed, replication to Computer2 was successful. A blank window or an error message means that replication failed.

Deploying Adobe Connect Edge Server

Adobe Connect Edge Server installation workflow

1. Design edge server zones.

You can set up edge servers or clusters of edge servers in different locations, or *zones*, to allocate and balance access to Adobe Connect. For example, you could set up an edge server in San Francisco for West Coast users and an edge server in Boston for East Coast users.

2. Install Adobe Connect Edge Server.

Install Adobe Connect Edge Server on each computer in each zone. For example, if you have a cluster of edge servers in a zone, install Adobe Connect Edge Server on each computer in the cluster. See “Install Adobe Connect Edge Server” on page 26.

3. Modify the DNS server for each zone.

Map the FQDN of the origin Adobe Connect server to the static IP address of Adobe Connect Edge Server in each zone. See “Deploying Adobe Connect Edge Server” on page 33.

4. Configure the edge server.

You must add configuration parameters to the custom.ini file on each Adobe Connect Edge Server. See “Deploying Adobe Connect Edge Server” on page 33.

5. Configure the origin server.

You must add configuration parameters to the custom.ini file on each Adobe Connect server. Also, you must set the External Name of the edge server in the Application Management Console on the origin server. See “Deploying Adobe Connect Edge Server” on page 33.

6. Set up a load balancer.

If you set up multiple edge servers in a zone, you must use a load balancer to balance the load between edge servers and configure it to listen on port 80. The edge servers listen on port 8080. For more information, see the documentation provided by the vendor of the load balancer.

Deploy Adobe Connect Edge Server

Before you deploy edge servers, you should have Adobe Connect and any additional features (for example, SSL, a directory service integration, single sign-on, or shared content storage) running successfully.

1 On your DNS server, map the FQDN of the origin server to the static IP address of the edge server. If you’re installing edge servers in multiple zones, repeat this step for each zone.

***Note:** Alternatively, you can use a hosts file; if you do, every client must have a hosts file that points the static IP address of the edge server to FQDN of the origin server.*

2 On the Adobe Connect Edge Server, open the file *[root_install_dir]*\edgeserver\win32\conf\HttpCache.xml and replace the computer name in the HostName tag with the FQDN of the edge server computer, for example, edge1.mycompany.com.

```
<!-- The real name of this host. -->
<HostName>edge1.yourcompany.com</HostName>
```

3 On the Adobe Connect Edge Server, create a new file *[root_install_dir]*\edgeserver\custom.ini file and enter the following parameters and values:

FCS_EDGE_HOST The FQDN of the edge server, for example, `FCS_EDGE_HOST=edge1.yourcompany.com`.

FCS_EDGE_REGISTER_HOST The FQDN of the Adobe Connect origin server, for example, `FCS_EDGE_REGISTER_HOST=connect.yourcompany.com`.

FCS_EDGE_CLUSTER_ID The name of the cluster. Each edge server cluster must have a unique ID. Each computer within the cluster must have the same ID. The recommended format is *`companyname-clustername`*, for example, `FCS_EDGE_CLUSTER_ID=yourcompany-us`.

Note: *Even if you are only deploying one Adobe Connect Edge Server, you must configure this parameter.*

FCS.HTTPCACHE_BREEZE_SERVER_NORMAL_PORT The IP address or domain name and port number of the computer where Adobe Connect is installed, for example, `FCS.HTTPCACHE_BREEZE_SERVER_NORMAL_PORT=connect.yourcompany.com:80`. The Adobe Connect Edge Server connects to the Adobe Connect origin server at this location.

FCS_EDGE_PASSWORD (Optional) A password for the edge server. If you set a value for this parameter, you must set the same value for every edge server and origin server.

FCS_EDGE_EXPIRY_TIME (Optional) The number of milliseconds in which the edge server must register itself to the origin before it expires from the cluster and the system fails over to another edge. Start with the default value, `FCS_EDGE_EXPIRY_TIME=60000`.

FCS_EDGE_REG_INTERVAL (Optional) The interval, in milliseconds, at which the edge server attempts to register with the origin server. This parameter determines how often the edge server makes itself available to the origin server. Start with the default value, `FCS_EDGE_REG_INTERVAL=30000`.

DEFAULT_FCS_HOSTPORT (Optional) To configure the edge server ports, add the following line: `DEFAULT_FCS_HOSTPORT=:1935,80,-443`.

The minus sign (-) in front of 443 designates port 443 as a secure port that receives only RTMPS connections. If you attempt an RTMPS connection request to port 1935 or 80, the connection will fail. Similarly, an unsecured RTMP connection request to port 443 will fail.

Note: *If your edge server uses an external hardware accelerator, port 443 does not have to be configured as a secure port.*

The following are sample values for the config.ini file:

```
FCS_EDGE_HOST=edge.yourcompany.com
FCS_EDGE_REGISTER_HOST=connect.yourcompany.com
FCS_EDGE_CLUSTER_ID=yourcompany-us
FCS.HTTPCACHE_BREEZE_SERVER_NORMAL_PORT=connect.yourcompany.com:80
```

4 Restart the edge server.

5 On the Adobe Connect origin server, open the *[root_install_dir]*\custom.ini file in a text editor and map the value of the `FCS_EDGE_CLUSTER_ID` parameter to a zone ID; the syntax is `edge.`*`FCS_EDGE_CLUSTER_ID=zone-id`*. Even if you are only deploying one edge server, you must map the cluster ID to a zone ID.

Each edge server cluster must have a zone ID. A zone ID can be any positive integer greater than 0. For example, you could have three clusters mapped to zones 1 to 3:

```
edge.yourcompany-us=1
edge.yourcompany-apac=2
edge.yourcompany-emea=3
```

The following is a sample custom.ini file for the origin server:

```
DB_HOST=localhost
DB_PORT=1433
DB_NAME=breeze
DB_USER=sa
DB_PASSWORD=#V1#4cUsRJ6oeFwZLnQPpS4f0w==
# DEBUG LOGGING SETTINGS
HTTP_TRACE=yes
DB_LOG_ALL_QUERIES=yes
# EDGE SERVER SETTINGS
edge.yourcompany-us=1
```

Note: *If you set an* `FCS_EDGE_PASSWORD` *parameter in the config.ini file on the edge server, set the same password in the custom.ini file on the origin server.*

6 Restart the origin server.

7 On the origin server, open the Application Management Console (Start > Programs > Adobe Connect Server > Configure Adobe Connect Server). Select the Application Settings tab, then select Server Settings and, in the Host Mappings section, enter the External Name for the edge server. The External Name should be identical to the value set for the `FCS_EDGE_HOST` parameter on the edge server.

8 On the origin server, configure the Windows firewall so the edge servers can access port 8506.

9 Repeat steps 2-4 for each edge server in each zone.

10 Repeat steps 5-7 for each origin server in each zone.

For help deploying edge servers, contact Adobe Support at www.adobe.com/support/programs/connect.

More Help topics

"Choosing to deploy Adobe Connect Edge Server" on page 12

Integrating with a directory service

Directory service integration overview

You can integrate Adobe Connect with a directory service to authenticate users against the LDAP directory and to avoid manually adding individual users and groups. User accounts are created automatically in Adobe Connect through manual or scheduled synchronizations with the directory of your organization.

To integrate with Adobe Connect, your directory server must use Lightweight Directory Access Protocol (LDAP) or secure Lightweight Directory Access Protocol (LDAPS). LDAP is an Internet client-server protocol for lookup of user contact information from an LDAP-compliant directory server.

Adobe Connect connects as an LDAP client to an LDAP directory. Adobe Connect imports users and groups, and synchronizes information about these users and groups with the LDAP directory. You can also configure Adobe Connect to authenticate users against the LDAP directory.

Any LDAP-compliant directory service may integrate with Adobe Connect. For a list of certified LDAP directories, see www.adobe.com/go/learn_cnn_sysreqs_en.

About LDAP directory structure

LDAP directories organize information according to the X.500 standard.

A user or group in an LDAP directory is called an *entry*. An entry is a collection of attributes. An attribute consists of a type and one or more values. Types use mnemonic strings, such as `ou` for organizational unit or `cn` for common name. Attribute values consist of information such as phone number, e-mail address, and photo. To determine your organization's LDAP directory structure, contact your LDAP administrator.

Each entry has a *distinguished name* (DN) that describes a path to the entry through a tree structure from the entry to the root. The DN for an entry in the LDAP directory is a concatenation of the name of the entry (called a *relative distinguished name*, RDN) and the names of its ancestor entries in the tree structure.

A tree structure may reflect geographical locations or departmental boundaries within a company. For example, if Alicia Solis is a user in the QA department of Acme, Inc. in France, the DN for this user might be as follows:

cn=Alicia Solis, ou=QA, c=France, dc=Acme, dc=com

Importing directory branches

When importing users and groups from an LDAP directory into Adobe Connect, you specify a path to a section of the LDAP tree by using the DN of the section. This specifies the scope of the search. For example, you may want to import only the users of a particular group within your organization. To do this, you need to know where the entries for that group are located in the directory tree structure.

A common technique is to use the organization's Internet domain as the root for the tree structure. For example, Acme, Inc. might use `dc=com` to specify the root element in the tree. A DN that specifies the Singapore sales office for Acme, Inc. might be `ou=Singapore`, `ou=Marketing`, `ou=Employees`, `dc=Acme`, `dc=com`. (In this example, `ou` is an abbreviation for organizational unit, and `dc` is an abbreviation for domain component.)

Note: *Not all LDAP directories have a single root. In this situation, you can import separate branches.*

Importing users and groups

There are two ways of structuring user and group entries in an LDAP directory: under the same node of a branch or under different branches.

If users and groups are under the same node in an LDAP branch, user and group settings for importing entries contain the same branch DN. This means that when you import users, you must use a filter to select only users, and when you import groups, you must use a filter to select only groups.

If users and groups are under different branches in the tree, use a branch DN that selects the user branch when you import the users and the group branch when you import the groups.

You can also import sub-branches to import users from all branches below a certain level. For example, if you want to import all the employees in the sales department, you might use the following branch DN:

```
ou=Sales, dc=Acme, dc=com
```

However, salespeople might be stored in sub-branches. In that case, on the User Profile Mapping screen, set the Subtree Search parameter to `true` to ensure that users are imported from the sub-branches below that level in the tree.

Filtering selected entries

A filter specifies a condition that an entry must satisfy to be selected. This restricts the selection of entries within a part of the tree. For example, if the filter specifies `(objectClass=organizationalPerson)`, only entries that have the attribute `organizationalPerson` are selected for import.

Note: *The attribute `objectClass` must be present in every entry in a LDAP directory.*

Internal and external users and groups

Users and groups that you create directly in Adobe Connect rather than importing them from an LDAP directory are called *internal* users and groups. Users and groups imported into the Adobe Connect database from an LDAP directory are called *external* users and groups.

To ensure that imported groups are kept synchronized with the external LDAP directory, you cannot add internal users and groups to external groups. However, you can add external users and groups to internal groups.

If the value of the login or name of an imported user or group entry matches the login for an existing internal user or group, synchronizing the directories changes the imported user or group from internal to external and places a warning in the synchronization log.

Integrate Adobe Connect with an LDAP directory

Directory service integration takes place in the Directory Service Settings tab of the Application Management Console. Use an Administrator account.

You can configure one directory server for user authentication and LDAP synchronization. The configuration can point to one or several branches of the directory service.

1. Open the Application Management Console.

Choose Start > Programs > Adobe Connect Server > Configure Adobe Connect Server.

2. Enter LDAP server connection settings.

Select the Directory Service Settings tab. Enter values on the LDAP Settings > Connection Settings screen and click Save.

When you click Save, Adobe Connect tests the LDAP connection. If the test fails, you see the following message: Your settings were successfully saved but LDAP connectivity could not be verified. Please check your LDAP URL and port.

Field	**Default value**	**Description**
LDAP Server URL	No default.	Usual form is `ldap://` ***`[servername:portnumber]`***. If your organization uses a secure LDAP server, use `ldaps://`. If you do not specify a port, Adobe Connect uses the standard LDAP port (389) or LDAPS port (636). LDAPS requires SSL certificates. If you configure Adobe Connect to work in a Microsoft Active Directory forest where the Global Catalog is enabled, use the Global Catalog (standard port: 3268).
LDAP Connection Authentication Method	No default.	The mechanism for authenticating the credentials (LDAP user name, LDAP password) of the LDAP service account for Adobe Connect (admin rights). **Simple** (standard authentication - recommended). **Anonymous** (no password - your LDAP server must be configured to allow anonymous login). **Digest MD5** (configure your LDAP server to allow digest authentication).
LDAP Connection Username	No default.	Administrative login on the LDAP server.

Field	**Default value**	**Description**
LDAP Connection Password	No default.	Administrative password on the LDAP server.
LDAP Query Timeout	No default.	Time that can elapse before the query is canceled, in seconds. If you leave the field empty, there is no timeout. Set this value to 120.
LDAP Entry Query Page Size Limit	No default.	The page size of the results returned from the LDAP server. If this box is blank or 0, a page size is not used. Use this field for LDAP servers that have a maximum results size configured. Set the page size to less than the maximum results size so all the results are retrieved from the server in multiple pages. For example, if you try to integrate a large LDAP directory that can only display 1000 users and there are 2000 users to import, the integration fails. If you set the Query Page Size to 100, the results would be returned in 20 pages and all users would be imported.

The following is an example of LDAP syntax for connection settings:

```
URL:ldap://ldapserver.mycompany.com:389
UserName:MYCOMPANY\jdoe
Password:password123
Query timeout:120
Authentication mechanism:Simple
Query page size:100
```

3. Map Adobe Connect and LDAP directory user profiles.

Choose the User Profile Mapping tab, enter values, and click Save.

Field	**Default value**	**Description**
Login	No default.	The directory service login attribute.
First Name	No default.	The directory service first name attribute.
Last Name	No default.	The directory service last name attribute.
E-mail	No default.	The directory service email attribute.

If you have defined custom fields, they are added to the User Profile Mapping screen. This example maps an Adobe Connect user profile to an Active Directory LDAP user profile; Network Login is a custom field.

```
Login:mail
FirstName:givenName
LastName:sn
Email:userPrincipalName
NetworkLogin:mail
```

4. (Optional) Add a user branch.

Click Add to add user information from a particular branch of your company. Enter values in the Branch and Filter fields and click Save.

If you want to import users from subbranches, select True from the Subtree Search menu; otherwise, select False.

For more information, see “About LDAP directory structure” on page 35.

Field	Default value	LDAP attribute/notes
Branch DN	No default.	DN (distinguished name) of the branch root node. A link to the selected branch is displayed.
Filter	No default.	The query filter string.
Subtree Search	True	True or False. A value of True initiates a recursive search of all subtrees in the branch.

5. Map Adobe Connect and LDAP directory group profiles.

Select the Group Profile Mapping tab, enter values, and click Save.

Note: *Adobe Connect group profiles do not support custom fields.*

Field	Default value	LDAP attribute/notes
Group Name	No default.	The directory service group name attribute.
Group Member	No default.	The directory service group member attribute.

The following is a mapping between LDAP group entry attributes and an Adobe Connect group profile:

```
Name:cn
Membership:member
```

6. (Optional) Add a group branch.

Click Add to add user information from a branch of your organization. Enter values in the Branch and Filter fields and click Save.

If you want to import groups from subbranches, select True from the Subtree Search menu; otherwise, select False.

For more information, see "About LDAP directory structure" on page 35.

Field	Default value	LDAP attribute/notes
Branch DN	No default.	DN (distinguished name) of the branch root node. Each branch in the organization has its own LDAP DN attribute. A link to the selected branch is displayed.
Filter	No default.	The query filter string.
Subtree Search	True	A Boolean value of `true` or `false`. A value of `true` initiates a recursive search of all subtrees in the branch.

The following example shows one LDAP syntax for adding a branch of the organization and defining its groups:

```
DN:cn=USERS,DC=myteam,DC=mycompany,DC=com
Filter:(objectClass=group)
Subtree search:True
```

7. Enter authentication settings.

Select the Authentication Settings tab. If you want to authenticate Adobe Connect users against the directory service of your organization, select "Enable LDAP Directory authentication". If you do not select this option, Adobe Connect uses native authentication (user credentials stored in the Adobe Connect database).

If you check "Enable Connect fall-back on unsuccessful LDAP Directory authentication", Adobe Connect uses native authentication.

***Note:** This option can be useful in the event of a temporary LDAP connectivity failure on your network. However, LDAP credentials can be different from credentials in the Adobe Connect database.*

Check “Create Connect user account upon successful LDAP Directory authentication” to provision first-time users on the Adobe Connect server if LDAP authentication is successful. If any user in your directory service is allowed to use Adobe Connect, leave this option checked and select “Internal” as user account type. For more information, see “Internal and external users and groups” on page 37.

Check “Enable group enrollment on first login only” to create a login ID in Adobe Connect and place users into specified groups when users log into Adobe Connect for the first time. Enter the groups in the Group names box.

8. Schedule synchronization.

Select the Synchronization Settings tab. On the Schedule Settings screen, select the Enable scheduled synchronization check box to schedule regular synchronizations either once daily, weekly, or monthly at a certain time. For more information, see “Recommended practices for synchronization” on page 40.

You can also perform a manual synchronization on the Synchronization Actions screen.

9. Set a password policy and a deletion policy.

Select the Policy Settings tab, choose a Password Setup Policy and a Deletion Policy, and click Save. For more information about password policy, see “Managing passwords” on page 40.

***Note:** If you select the Delete users and groups... option, during a synchronization, all external users that have been deleted from the LDAP server are also deleted from the Adobe Connect server.*

10. Preview the synchronization.

Select the Synchronize Actions tab. In the Preview Directory Synchronization section, click Preview. For more information, see “Recommended practices for synchronization” on page 40.

Managing passwords

If you do not enable LDAP authentication, you must choose how Adobe Connect authenticates users.

When Adobe Connect imports user information from an external directory, it does not import network passwords. Therefore, implement another method for managing passwords for users imported into the Adobe Connect directory.

Notifying users to set a password

On the Policy Settings screen of the Synchronization Settings tab, you can choose to send an e-mail to imported users with a link that lets them set a password.

Set the password to an LDAP attribute

You can choose to set the initial password of an imported user to the value of an attribute in directory entry of that user. For example, if the LDAP directory contains the employee ID number as a field, you could set the initial password for users to their employee ID number. After users log in using this password, they can change their passwords.

Recommended practices for synchronization

As an administrator, you can synchronize Adobe Connect with the external LDAP directory in two ways:

- You can schedule synchronization so that it takes place at regular intervals.
- You can perform a manual synchronization that immediately synchronizes the Adobe Connect directory with the organization’s LDAP directory.

Before you import users and groups in an initial synchronization, it's a good idea to use an LDAP browser to verify the connection parameters. The following browsers are available online: LDAP Browser/Editor and LDAP Administrator.

Important: *Do not reboot your LDAP server or run parallel jobs during synchronization. Doing so can cause users or groups to be deleted from Adobe Connect.*

Scheduled synchronizations

Scheduled synchronizations are recommended because they ensure that Adobe Connect has an up-to-date picture of the users and groups imported from the organization's LDAP directory.

If you are importing a large number of users and groups, the initial synchronization might consume significant resources. If this is the case, it's a good idea to schedule this initial synchronization at an off-peak time, such as late at night. (Alternatively, you can do the initial synchronization manually.)

To set up a scheduled synchronization, use the Synchronization Settings > Schedule Settings screen in the Application Management Console.

When a synchronization takes place, Adobe Connect compares LDAP directory entries to Adobe Connect directory entries and imports only those entries that contain at least one changed field.

Previewing the synchronization

Before you import users and groups in an initial synchronization, Adobe recommends that you test your mappings by previewing the synchronization. In a preview, users and groups are not actually imported, but errors are logged; you can examine these errors to diagnose problems in the synchronization.

To access the synchronization logs, use the Synchronization Logs screen. Each line of the log shows a synchronization event; the synchronization produces at least one event for each principal (user or group) processed. If any warnings or errors are generated during the preview, they are listed in a second warning log.

Log file values

The synchronization logs store values in a comma-separated format. In the following tables, *principal* refers to user and group entries. The following values are included in the log entries:

Field	Description
Date	The formatted date-time value, with time to the millisecond. The format is *yyyyMMdd'T'HHmmss.SSS*.
Principal ID	The login or group name.
Principal type	A single character: U for user, G for group.
Event	The action taken or condition encountered.
Detail	Detailed information about the event.

The following table describes the different kinds of events that can appear in the synchronization log files:

Event	**Description**	**Detail**
add	The principal was added to Adobe Connect.	An abbreviated XML packet that describes the updated fields using a series of tag pairs in the format ***<fieldname>value</fieldname>*** (for example, `<first-name>Joe</first-name>`). The parent node and non-updated fields are omitted.
update	The principal is an external user and some fields were updated.	

update-members	The principal is an external group, and principals were added to or removed from membership in the group.	An abbreviated XML packet that describes the added and removed members. The parent node is omitted:
		`<add>ID list</add>`
		`<remove>ID list</remove>`
		The ID list is a series of `<id>principal ID</id>` packets where `principal ID` is an ID that would be listed in the Principal ID column, such as a user login or group name. If there are no members of an ID list, the parent node is output as `<add/>` or `<remove/>`.

delete	The principal was deleted from Adobe Connect.	
up-to-date	The principal is an external principal in Adobe Connect and is already synchronized with the external directory. No changes were made.	A user or group created in Adobe Connect is considered an internal principal. A user or group created by the synchronization process is considered an external principal.
make-external	The principal is an internal principal in Adobe Connect and was converted to an external principal.	This event permits the synchronization to modify or delete the principal and is usually followed by another event that does one or the other. This event is logged in the warning log.
warning	A warning-level event occurred.	A warning message.
error	An error occurred.	Java exception message.

About LDAPS

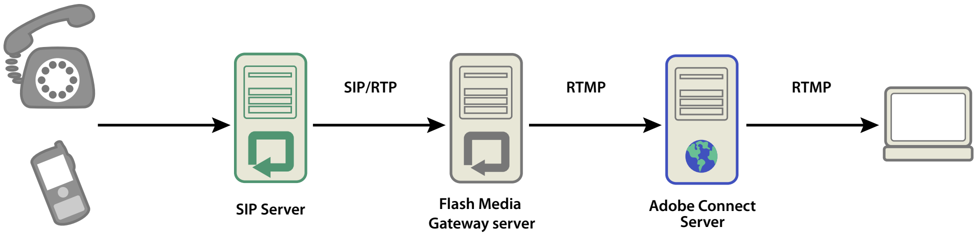
Adobe Connect supports the secure LDAP protocol, *LDAPS*, natively. The LDAP directory server must provide SSL connectivity. To connect securely to an LDAP directory server, use the LDAPS protocol in the connection URL, as follows: ldaps://*exampleDirectoryServer:portNumber*.

Deploying Universal Voice

Workflow for deploying Universal Voice

Note: *For a comparison of Universal Voice and integrated telephony adaptors, see "Adobe Connect audio and video conferencing options" on page 14.*

Adobe Connect Universal Voice uses a component called Flash Media Gateway to send and receive audio from a SIP server. Install Flash Media Gateway and configure it to communicate with a SIP server. The SIP server can be hosted by a third-party or part of your company's infrastructure. (SIP providers are also called *VoIP providers*.)



Audio flows from a phone, through an audio conference server (not pictured), through a SIP server, through Flash Media Gateway, to an Adobe Connect meeting room.

***Note:** Adobe Connect supports two-way communication and video devices.*

Follow this workflow to implement the Universal Voice solution:

1 To install and configure Universal Voice, you must have the following:

- Adobe Connect
- SIP provider credentials

2 Install Flash Media Gateway.

You can install Flash Media Gateway on the same computer as Adobe Connect Server or on a dedicated computer. You can deploy Flash Media Gateway on a single computer or in a cluster of servers. The Flash Media Gateway installer is part of the Adobe Connect Server installer. See “Run the installer” on page 20.

3 Configure Flash Media Gateway to connect to a SIP server.

4 Open ports. See “Flash Media Gateway ports and protocols” on page 43.

If a firewall uses NAT, see “Configuring Flash Media Gateway to communicate from behind a firewall that uses NAT” on page 44.

5 To install Flash Media Gateway on a cluster of computers, see “Deploy Flash Media Gateway on a cluster of servers” on page 47.

6 To create a dialing sequence and test the audio connection, see Configure audio providers for universal voice.

7 If you can’t hear audio in an Adobe Connect meeting, see “Troubleshoot Universal Voice issues” on page 48.

Flash Media Gateway ports and protocols

***Note:** To view a diagram of how data flows between a SIP provider, Flash Media Gateway, and Adobe Connect Server, see “Data flow” on page 7.*

Flash Media Gateway listens for requests from Adobe Connect Central Application Server on the following port:

Port number	Bind address	Protocol
2222	*/Any Adaptor	HTTP

Flash Media Gateway initiates a connection with Flash Media Server like a regular RTMP client. Flash Media Server listens for Flash Media Gateway on the following port:

Port number	Bind address	Protocol
8506	*/Any Adaptor	RTMP

Flash Media Gateway communicates with the audio conferencing provider over the SIP and RTP protocols on the following ports:

Direction	**Rule**
Flash Media Gateway to Internet	SRC-IP=<Server-IP>, SRC-PORT=5060, DST-IP=ANY, DST-PORT=5060
Internet to Flash Media Gateway	SRC-IP=ANY, SRC-PORT=5060, DST-IP=<Server-IP>, DST-PORT=5060
Flash Media Gateway to Internet	SRC-IP=<Server-IP>, SRC-PORT=5000_TO_6000, DST-IP=ANY, DST-PORT=ANY_HIGH_END
Internet to Flash Media Gateway	SRC-IP=ANY, SRC-PORT=ANY_HIGH_END, DST-IP=<Server-IP>, DST-PORT=5000_TO_6000

***Note:** ANY_HIGH_END means any port above 1024. The default port range is 5000-6000. You can change these values in the Application Management Console. Alternatively, you can also update these values from the sip.xml file of Flash Media Gateway, by configuring the nodes* `portUpperLimit` *and* `portLowerLimit`*.*

Configuring Flash Media Gateway to communicate from behind a firewall that uses NAT

***Note:** You may not need to complete this task if your firewall is SIP-capable or SIP-aware. Also, in some cases the ALG (application-level gateway) for SIP in a firewall can cause problems. If you can't enable successful communication through ALG, disable ALG for SIP in the firewall and use the technique described in this section.*

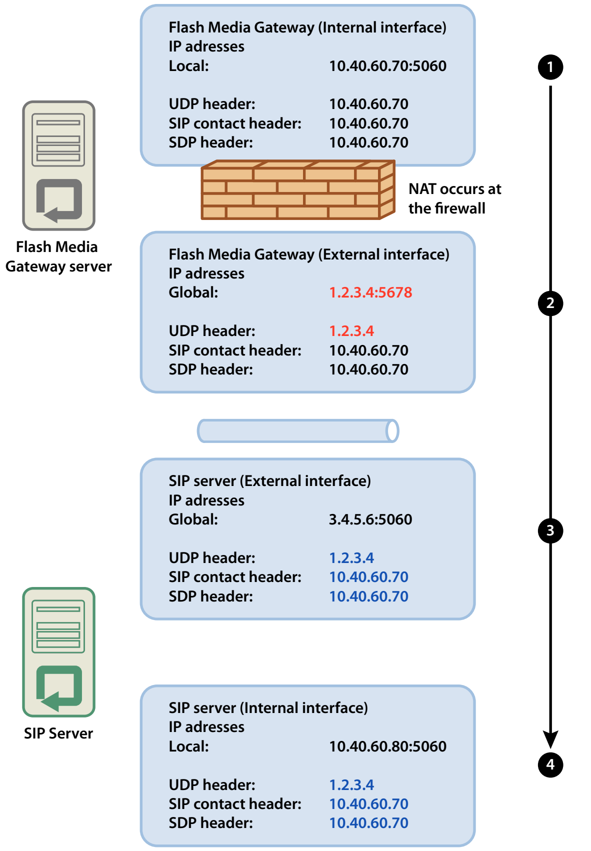
Network address translation (NAT) is a process that allows networks to use fewer external IP addresses and to obscure internal IP addresses. NAT changes the IP address and port number of packets flowing out of a network. The internal IP addresses are changed to an external IP address. NAT also tries to direct responses sent to the external IP address to the correct internal IP addresses.

When Flash Media Gateway is behind a firewall that uses NAT, it may not be able to receive packets from the SIP server. NAT changes the local IP address and the UDP header (packet source) IP address to match the external IP address.

The UDP header IP address is the same as the Flash Media Gateway external IP address. Therefore, if the SIP server uses the UDP header IP address to send a reply, the reply finds Flash Media Gateway.

The contact header IP address is the same as the Flash Media Gateway local IP address. Therefore, if the SIP server uses the SIP contact header IP address to send a reply, the reply can't find Flash Media Gateway. The local IP address is hidden behind the firewall and not visible to the SIP server.

The following image shows how NAT changes the IP addresses at the firewall:


Flash Media Gateway (Internal interface)
IP adresses
Local: 10.40.60.70:5060
UDP header: 10.40.60.70
SIP contact header: 10.40.60.70
SDP header: 10.40.60.70
NAT occurs at the firewall
Flash Media Gateway server
Flash Media Gateway (External interface)
IP adresses
Global: 1.2.3.4:5678
UDP header: 1.2.3.4
SIP contact header: 10.40.60.70
SDP header: 10.40.60.70
SIP server (External interface)
IP adresses
Global: 3.4.5.6:5060
UDP header: 1.2.3.4
SIP contact header: 10.40.60.70
SDP header: 10.40.60.70
SIP Server
SIP server (Internal interface)
IP adresses
Local: 10.40.60.80:5060
UDP header: 1.2.3.4
SIP contact header: 10.40.60.70
SDP header: 10.40.60.70
1
2
3
4

NAT changes the IP address

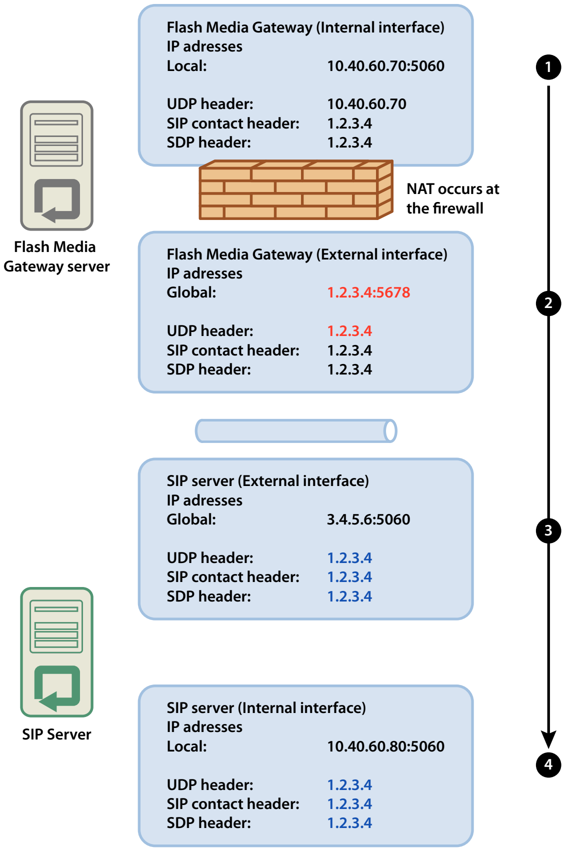
1 Flash Media Gateway (internal interface). The UDP header (packet source IP address) and the SIP contact header IP address are the same as the local IP address.

2 Flash Media Gateway (external interface). NAT changes the UDP header IP address to the global IP address.

3 SIP server (external interface). The packet reaches the global interface on the SIP server. To reach the internal interface, directly forward the port. If the port is not forwarded, the packet is lost and communication breaks.

4 SIP server (internal interface). The packet is processed when it reaches this interface. If the SIP server uses the UDP header IP address to send a reply the reply reaches Flash Media Gateway successfully. If the SIP server uses the contact header IP address, the reply cannot reach Flash Media Gateway.

The following image shows a successful configuration in which the SIP contact header IP address is same as the Flash Media Gateway external IP address. This change allows packets to be routed back to Flash Media Gateway from the SIP server.


Flash Media Gateway (Internal interface)
IP adresses
Local: 10.40.60.70:5060
UDP header: 10.40.60.70
SIP contact header: 1.2.3.4
SDP header: 1.2.3.4
Flash Media Gateway server
NAT occurs at the firewall
Flash Media Gateway (External interface)
IP adresses
Global: 1.2.3.4:5678
UDP header: 1.2.3.4
SIP contact header: 1.2.3.4
SDP header: 1.2.3.4
SIP server (External interface)
IP adresses
Global: 3.4.5.6:5060
UDP header: 1.2.3.4
SIP contact header: 1.2.3.4
SDP header: 1.2.3.4
SIP Server
SIP server (Internal interface)
IP adresses
Local: 10.40.60.80:5060
UDP header: 1.2.3.4
SIP contact header: 1.2.3.4
SDP header: 1.2.3.4
1
2
3
4

A configuration that allows successful communication

To ensure that Flash Media Gateway can receive packets successfully from a SIP server, do the following:

1 On Flash Media Gateway, open the *[root_install_dir]*/conf/sip.xml file in a text editor. (The default root installation folder is C:\Program Files\Adobe\Flash Media Gateway.)

a Create a `<globalAddress>` tag under the `<Profile>` tag. Enter the Flash Media Gateway external IP address, as in the following:

```
...
<Profiles>
    <Profile>
        <profil e I D>   s ipGateway </profileID>
        <userName>141583220 00 </ userName>
        <password></password>
        <displayName> sipGateway </displayName>
        <registrarAddress>8.15.247.100:5060</registrarAddress>
        <doRegister>0</doRegister>
        <defaulthost>8.15.247.100:5060</defaulthost>
        <hostPort> 0 </hostPort>
        <context> sipGatewayContext </context>
        <globalAddress>8.15.247.49</globalAddress>
        <supportedCodecs><codecID> G711u </codecID><codecID> speex </codecID>
    </supportedCodecs>
    </Profile>
</Profiles>
...
```

In a cluster, each Flash Media Gateway server must have a unique external IP address.

Important: *If the external IP address is dynamic, you must reconfigure Flash Media Gateway every time the external IP address changes.*

b Restart the Flash Media Gateway service. See “Start and stop Flash Media Gateway” on page 82.

2 On the firewall between the Flash Media Gateway server and the SIP server directly forward the SIP port (5060 by default) and all RTP voice ports (5000 - 6000 by default) toward the Flash Media Gateway server. The ports open at the firewall must be the same as the ports open on the Flash Media Gateway server.

Note: *The servers can communicate without port forwarding. However, without port forwarding calls may disconnect unexpectedly, especially after long durations.*

Configure the Flash Media Gateway log level

A high log level can cause audio glitches when the load on Flash Media Gateway is high. Higher log levels write more information to the log. Writing to the log uses processing power and leaves less power for transmitting audio. For best performance, Adobe recommends setting the log level for audio data to 4.

1 Open the fmsmg.xml file in a text editor (By default, the file is located at C:\Program Files\Adobe\Flash Media Gateway\conf.)

2 Set `logLevel` to 4:

```
<logLevel>4</logLevel>
```

3 Restart Flash Media Gateway.

Deploy Flash Media Gateway on a cluster of servers

Flash Media Gateway installed on a computer with two processors can make 100 calls simultaneously. To handle a higher load increase the number of processors or add more Flash Media Gateway servers to the cluster.

To deploy a cluster of servers, install Flash Media Gateway on its own computers and install Adobe Connect Server on its own computers. Do not install Adobe Connect Server and Flash Media Gateway on the same computers.

When you deploy Flash Media Gateway on a cluster of servers, Adobe Connect Server handles load balancing and failover. Adobe Connect Edge Server does not require any additional configuration.

1 Run the installer on every server in the cluster and choose to install Flash Media Gateway. See “Run the installer” on page 20.

   ***Note:** For information about deploying Adobe Connect Server in a cluster, see “Deploy a cluster of Adobe Connect servers” on page 30.*

2 On one Adobe Connect server, open the Application Management Console at http://localhost:8510/console.

3 Select Flash Media Gateway settings and click Add to add and configure additional Flash Media Gateway servers.

   ***Note:** Use the Application Management Console on one server to enter configuration parameters for all the servers in the cluster. The Application Management Console pushes the configuration settings to every server in the cluster.*

Troubleshoot Universal Voice issues

If you can’t hear audio from a Universal Voice audio conference in a meeting room, do the following:

1 Make sure that the volume is up on the computer. If you’re using headphones, make sure they’re plugged into the output jack.

2 Test the dial-in sequence. See Test a dialing sequence.

3 Verify that Flash Media Gateway is configured successfully:

   a Open the Application Management Console (http://localhost:8510/console) on Adobe Connect Server and click Flash Media Gateway Settings. The status of each Flash Media Gateway must be “Active”.

   b If the status is not active, open the *[root_install_dir]*/custom.ini file. Make sure that you see the following entries:

```
FMG_ADMIN_USER=sa
FMG_ADMIN_PASSWORD=breeze
```

   If you don’t see the entries, enter them and restart Adobe Connect Central Application Server.

4 Contact Adobe Support at www.adobe.com/support/programs/connect.

If you don’t see an option to add a Video Telephony pod in the meeting room Pods menu:

❖ Ensure that Video Telephony Pod is not disabled in Adobe Connect Central > Administration >Compliance and Control.

Deploying integrated telephony adaptors

Integrated telephony adaptors are Java extensions that let Adobe Connect connect to an audio bridge. You can install any number of integrated telephony adaptors when you install Adobe Connect. For more information, see “Preparing to install integrated telephony adaptors” on page 14.

After installing one or more adaptors, see the following topics to verify and configure the installation.

- “Avaya telephony adaptor” on page 49
- “InterCall telephony adaptor” on page 49
- “MeetingOne telephony adaptor” on page 50
- “PGi NA telephony adaptor” on page 50
- “PGi EMEA telephony adaptor” on page 51

To configure additional adaptor capabilities after installation is complete, see Configure Adobe Connect Telephony Adaptors..

Avaya telephony adaptor

Complete the following two tasks to confirm the adaptor is working as expected.

Confirm that telephony is enabled

1. Log in to Adobe Connect Central.
2. Click Administration > Audio Providers.

   If telephony is successfully enabled, you'll see Avaya in the Providers list. Select Avaya and click Edit to enable or disable the adaptor for the entire Adobe Connect account.

3. To add an Avaya audio profile, click My Profile > My Audio Profiles > New Profile. From the Provider list, select Avaya.

   For more information, see Configure audio providers for universal voice.

Test audio in a meeting

❖ Before you deploy Adobe Connect to a production environment, record at least 2 minutes of a meeting. View the meeting archive to confirm that audio recorded correctly.

Disabling the adaptor

If you want to disable the Avaya adaptor:

1. Stop Adobe Connect Telephony Service.
2. Open the *[root_install_dir]*\telephony-service\conf\telephony-settings.xml file.
3. Set the `enabled` attribute of the `<telephony-adaptor>` tag to `false`, as in the following:

```
<telephony-adaptor id="avaya-adaptor" class-
name="com.macromedia.breeze_ext.telephony.AvayaAdaptor" enabled="false">
```

4. Restart Adobe Connect Telephony Service.

InterCall telephony adaptor

Complete the following two tasks to confirm the adaptor is working as expected.

Confirm that telephony is enabled

1. Log in to Adobe Connect Central.
2. Click Administration > Audio Providers.

   If telephony is successfully enabled, you'll see InterCall in the Providers list. Select InterCall and click Edit to enable or disable the adaptor for the entire Adobe Connect account.

3. To add an InterCall audio profile, click My Profile > My Audio Profiles > New Profile. From the Provider list, select InterCall.

   For more information, see Configure audio providers for universal voice.

Test audio in a meeting

Before you deploy Adobe Connect to a production environment, record at least 2 minutes of a meeting. View the meeting archive to confirm that audio recorded correctly.

Disabling the telephony adaptor

If you want to disable the InterCall adaptor:

1. Stop Adobe Connect Telephony Service.
2. Open the *[root_install_dir]*\TelephonyService\conf\telephony-settings.xml file.
3. Set the `enabled` attribute of the `<telephony-adaptor>` tag to `false`, as in the following:

```
<telephony-adaptor id="intercall-adaptor" class-
name="com.macromedia.breeze_ext.telephony.Intercall.IntercallTelephonyAdaptor"
enabled="false">
```

4. Restart Adobe Connect Telephony Service.

MeetingOne telephony adaptor

Complete the following two tasks to confirm the adaptor is working as expected.

Confirm that telephony is enabled

1. Log in to Adobe Connect Central.
2. Click Administration > Audio Providers.

   If telephony is successfully enabled, you’ll see MeetingOne in the Providers list. Select MeetingOne and click Edit to enable or disable the adaptor for the entire Adobe Connect account.

3. To add an MeetingOne audio profile, click My Profile > My Audio Profiles > New Profile. From the Provider list, select MeetingOne.

   For more information, see Configure audio providers for universal voice.

Test audio in a meeting

Before you deploy Adobe Connect to a production environment, record at least 2 minutes of a meeting. View the meeting archive to confirm that audio recorded correctly.

Disabling the telephony adaptor

If you want to disable the MeetineOne adaptor:

1. Stop Adobe Connect Telephony Service.
2. Open the *[root_install_dir]*\TelephonyService\conf\telephony-settings.xml file.
3. Set the `enabled` attribute of the `<telephony-adaptor>` tag to `false`, as in the following:

```
<telephony-adaptor id="meetingone-adaptor" class-
name="com.meetingone.adobeconnect.MeetingOneAdobeConnectAdaptor" enabled="false">
```

4. Restart Adobe Connect Telephony Service.

PGi NA telephony adaptor

Complete the following three tasks to ensure the adaptor is working as expected.

Configure domain names

Adobe Connect uses HTTP over port 443 to communicate with PGi. Make sure that Adobe Connect can communicate with the domain **csaxis.premconf.com**.

Confirm that telephony is enabled

1 Log in to Adobe Connect Central.

2 Click Administration > Audio Providers.

If telephony is successfully enabled, you'll see PGi NA in the Providers list. Select PGi NA and click Edit to enable or disable the adaptor for the entire Adobe Connect account.

3 To add an PGi NA audio profile, click My Profile > My Audio Profiles > New Profile. From the Provider list, select PGi NA.

For more information, see Configure audio providers for universal voice.

Test audio in a meeting

Before you deploy Adobe Connect to a production environment, record at least 2 minutes of a meeting. View the meeting archive to confirm that audio recorded correctly.

Disabling the telephony adaptor

If you want to disable the Premiere NA adaptor:

1 Open the *[root_install_dir]*\TelephonyService\conf\telephony-settings.xml file.

2 Set the `enabled` attribute of the `<telephony-adaptor>` tag to `false`, as in the following:

```
<telephony-adaptor id="premiere-adaptor" class-
name="com.macromedia.breeze_ext.premiere.gateway.PTekGateway" enabled="false">
```

3 Restart Adobe Connect.

PGi EMEA telephony adaptor

Complete the following three tasks to ensure the adaptor is working as expected.

Configure domain names

Adobe Connect uses HTTP over port 443 to communicate with PGi. Make sure that Adobe Connect can communicate with the domain **euaxis.premconf.com**.

Confirm that telephony is enabled

1 Log in to Adobe Connect Central.

2 Click Administration > Audio Providers.

If telephony is successfully enabled, you'll see PGi EMEA in the Providers list. Select PGi EMEA and click Edit to enable or disable the adaptor for the entire Adobe Connect account.

3 To add a PGi EMEA audio profile, click My Profile > My Audio Profiles > New Profile. From the Provider list, select PGi EMEA.

For more information, see Configure audio providers for universal voice.

Test audio in a meeting

Before you deploy Adobe Connect to a production environment, record at least 2 minutes of a meeting. View the meeting archive to confirm that audio recorded correctly.

Disabling the telephony adaptor

If you want to disable the PGi EMEA adaptor:

1 Stop Adobe Connect Telephony Service.

2 Open the*[root_install_dir]*\TelephonyService\conf\telephony-settings.xml file.

3 Set the `enabled` attribute of the `<telephony-adaptor>` tag to `false`, as in the following:

```
<telephony-adaptor id="premiere-emea-adaptor" class-
name="com.macromedia.breeze_ext.premiere.gateway.EMEA.PTekGateway" enabled="false">
```

4 Restart Adobe Connect Telephony Service.

Hide the Flash Media Gateway user in the Attendee list

Note: *This section applies only to integrated telephony adaptors that have been configured for Universal Voice.*

When a meeting room connects to Flash Media Gateway, the connection appears as a user in the Attendee list. To hide the Flash Media Gateway user in the Attendee list, configure the audio conference number in the custom.ini file. Use the same number for all computers in a cluster. You can get the audio conference number from your SIP provider. Or, if your account administrator has configured an audio provider in Adobe Connect Central, you can find the number in the meeting room.

1 Open the *[root_install_dir]*\custom.ini file in a text editor.

2 Add the following parameter:

```
UV_NUMBER={audio_conference_telephone_number}

// Example:
UV_NUMBER=4155551212
```

3 Save and close the custom.ini file.

4 Do the following to restart the server:

a Choose Start > Programs > Adobe Connect Server > Stop Adobe Connect Central Application Server.

b Choose Start > Programs > Adobe Connect Server > Start Adobe Connect Central Application Server.

Configuring shared storage

About shared storage

You can use the installer or the Application Management Console to configure Adobe Connect to use NAS and SAN devices to manage content storage. Content is any file published to Adobe Connect, such as courses; SWF, PPT, or PDF files; and archived recordings.

The following are possible shared storage configurations:

- Content is copied to the primary external storage device and pulled to each Adobe Connect server's content folder as needed. Old content is purged from each server's content folder to make room for new content as needed. This configuration frees resources on the application server which is especially helpful in a large cluster. (Enter a value in the Shared Storage box and the Content Cache Size box.)
- Content is copied to all servers and the primary external storage device. This configuration is recommended for small clusters unless you have a large amount of content that is randomly accessed. (Enter a value in the Shared Storage box; leave Content Cache Size blank.)

***Note:** If you have an Adobe Connect cluster and don't configure shared storage devices, the cluster works in full mirroring mode (content published to Adobe Connect is copied to all servers) and content is never automatically removed from any servers.*

Configure shared storage

If you didn't configure shared storage during installation, you can do so by following the instructions in this section.

- If you're configuring shared storage for one Adobe Connect server, follow the instructions in the first task.
- If you're configuring shared storage for a cluster, follow the instructions in the first task for one computer in the cluster and then follow the instructions in the second task for all the other computers in the cluster.

More Help topics

"Supported content storage devices" on page 4

"Deploy a cluster of Adobe Connect servers" on page 30

Configure shared storage

Adobe Connect should be configured without shared storage and running on one server before you proceed.

1 Configure a shared volume on a external storage device.

The account under which the Adobe Connect service runs must have read and write permissions on the shared volume.

2 (Optional) If you are updating an existing Adobe Connect server to use shared storage volumes, you must copy the content from one of the existing servers to the shared volume.

a Stop the server (Start > Programs > Adobe Connect Server > Stop Adobe Connect Central Application Server and Stop Adobe Connect Meeting Server).

b Copy the folder*[root_install_dir]*\content\7 to the shared volume you created in step 1.

Some computers in a cluster may have extra content. Adobe Connect cannot use these files but if you want to copy them to the shared volume for archival purposes, you could write and run a script that compares the content of every computer with the content of the shared volume.

c Start Adobe Connect (Start > Programs > Adobe Connect Server > Start Adobe Connect Meeting Server and Start Adobe Connect Central Application Server).

3 On the Adobe Connect server, choose Start > Control Panel > Administrative Tools > Services to open the Services window, select Adobe Connect Service, and do the following:

a Right-click and select Properties.

b Select the Log On tab.

c Select This account and if the shared volume has a username and password, enter them and click Apply.

4 Restart Adobe Connect (application server only).

a Choose Start > Programs > Adobe Connect Server > Stop Adobe Connect Central Application Server.

b Choose Start > Programs > Adobe Connect Server > Start Adobe Connect Central Application Server.

5 Open the Application Management Console (Start > Programs > Adobe Connect Server > Configure Adobe Connect Server).

6 On the Application Settings tab, select the Server Settings tab, scroll down to the Shared Storage Settings section and enter a folder path in the Shared Storage box (for example, **\\volume\directory**).

If the primary storage device fills up, you can add another device to the primary position. Separate the paths by semicolons (;): **\\volume\directory;\\volume2\directory**.

***Note:** Writing (copying to the storage folder) is performed only on the first folder. Reading (copying from the storage folder) is performed in sequence starting with the first folder until the file is found.*

7 (Optional) To configure the content folder on Adobe Connect to act like a cache (assets are removed automatically when space is needed and are restored on demand), enter a value in the Content Cache Size box.

The content cache size is a percentage of the disk space to use as a cache. Adobe recommends that you set the value between 15 and 50 because the cache can grow well beyond the set size. The cache is purged only after viewed content has expired (24 hours after it was last viewed).

8 Click Save and close the Application Management Console.

9 Restart Adobe Connect (application server only).

a Choose Start > Programs > Adobe Connect Server > Stop Adobe Connect Central Application Server.

b Choose Start > Programs > Adobe Connect Server > Start Adobe Connect Central Application Server.

Configure shared storage for additional servers in a cluster

1 Install Adobe Connect but do not start it. If Adobe Connect is installed and already running, stop it.

2 On the Adobe Connect server, choose Start > Control Panel > Administrative Tools > Services to open the Services window, select Adobe Connect Service, and do the following:

a Right-click and select Properties.

b Select the Log On tab.

c Select This account and if the shared volume has a username and password, enter them and click Apply.

3 Start Adobe Connect.

a Choose Start > Programs > Adobe Connect Server > Start Adobe Connect Meeting Server.

b Choose Start > Programs > Adobe Connect Server > Start Adobe Connect Central Application Server.

4 (Optional) If you are installing Adobe Connect for the first time, follow the steps in “Deploy a cluster of Adobe Connect servers” on page 30.

5 Click Save and close the Application Management Console.

Configuring Help and Resources links

Adding Support and Status links to the Help menu

Account Administrators can add a Status Page link and a Support Page link to the Help menu in Meeting rooms. The links are to HTML pages that you design. The Status Page could provide information about the current status of the Adobe Connect system. The Support Page could provide information about getting support using Adobe Connect. If you do not define these links, they are not available in the Help menu.

1 Open the *RootInstallationFolder*\custom.ini file in a text editor.

2 To edit the Status Page link, set `STATUS_PAGE = "http://`*`connect.mycompany.com/status.html`*`"`.

3 To edit the Support Page link, set `SUPPORT_PAGE="http://`*`connect.mycompany.com/support.html`*`"`.

The URLs can be absolute or relative to the domain of the meeting server. Start absolute URLs with “http://” or “https://”. Start relative URLs with “/”.

4 Do the following to restart Adobe Connect:

a Choose Start > Programs > Adobe Connect Server > Stop Adobe Connect Central Application Server.

b Choose Start > Programs > Adobe Connect Server > Start Adobe Connect Central Application Server.

Redirect the Adobe Connect Central Resources links

The Adobe Connect Central Home page has a Resources tab that provides links to a Getting Started page, Adobe Connect Central Help, Adobe Connect Documentation, and ConnectUsers.com. You can redirect these links to different locations.

Note: *You cannot redirect ConnectUsers.com because it goes to a web site.*

1 Open the page you want to edit in an HTML editor. In each file path, substitute the placeholder *lang* with the two letter language code. For example, the code for English is “en”.

Page	Location	Notes
Getting Started	appserv/common/help/*lang*/support/startmain.htm	You can edit this file in Adobe Connect Server version 7 and later.
Adobe Connect Central Help	appserv/common/help/*lang*/connect/9.0/using/AH_HOME.html	Changing this file also changes the Help link at top of Adobe Connect Central. You can edit this file in Adobe Connect Server version 7 and later.
Adobe Connect Documentation	appserv/common/help/*lang*/go/doc.html	You can edit this file in Adobe Connect Server version 7.5 and later.

2 For each of these files, put the following as the total content of the file:

```
<!-- ===================================================================
    This is used by Adobe Connect to redirect to the desired webpage.
    If there is a particular place where you would like users to be sent,
    please customize the URL below.
     =================================================================== -->
<META HTTP-EQUIV=Refresh CONTENT="0; URL=http://desiredpage.com">
```

3 Edit the value of the URL attribute to target your content. The URL can be a relative path or an absolute path.

For example, to redirect the doc.html file to documentation on your organization's server, you might use the URL http://www.mycompany.com/support/documentation/connectpro.

Configuring account notification settings

Set the time that monthly reports are sent

Adobe Connect sends a monthly email about the capacity of your account. By default, account capacity monthly reports are sent at 3:00 UTC. If you want Adobe Connect to send the email at a different time, you can add parameters to the custom.ini file and set the desired values.

1 Open the *RootInstallationFolder*\custom.ini file and add the following parameters to the file with the desired values:

THRESHOLD_MAIL_TIME_OF_DAY_HOURS The UTC hour when the monthly reports for capacity notifications are sent. This value must be an integer from 0 through 23. This parameter can be set only in the custom.ini file; it cannot be set in Adobe Connect Central.

THRESHOLD_MAIL_TIME_OF_DAY_MINUTES The minute when the monthly reports for capacity notifications are sent. This value must be an integer from 0 through 59. This parameter can be set only in the custom.ini file; it cannot be set in Adobe Connect Central.

***Note:** If either of the preceding parameters is not specified or is specified incorrectly, the email is sent at 3:00 (UTC).*

The following are sample values added to the custom.ini file:

```
THRESHOLD_MAIL_TIME_OF_DAY = 5
THRESHOLD_MAIL_TIME_OF_MINUTES = 30
```

2 Do the following to restart Adobe Connect:

a Choose Start > Programs > Adobe Connect Server > Stop Adobe Connect Central Application Server.

b Choose Start > Programs > Adobe Connect Server > Start Adobe Connect Central Application Server.

Set capacity thresholds

Adobe Connect account administrators can set capacity thresholds in Adobe Connect Central. When the account exceeds these thresholds, a notification is sent. You can add parameters in the custom.ini file that set the default capacity thresholds in Adobe Connect Central.

For more information about configuring account notifications in Adobe Connect Central, see the "Administering Adobe Connect" chapter in *Using Adobe Connect guide at http://www.adobe.com/go/learn_cnn9_usingweb_en*.

1 Open the *RootInstallationFolder*\custom.ini file and add any of the following parameters to the file with the desired values:

THRESHOLD_NUM_OF_MEMBERS The default threshold percentage for the Authors and Meeting Hosts quota. This value must be an integer from 10 through 100 and divisible by 10. If the value is not specified or is incorrectly specified, the value is 80.

THRESHOLD_CONC_USERS_PER_MEETING The default threshold percentage for the Concurrent Users per Meeting quota. This value must be an integer from 10 through 100 and divisible by 10. If the value is not specified or is incorrectly specified, the value is 80.

THRESHOLD_CONC_MEETING_USERS_PER_ACCOUNT The default threshold percentage for the Account-wide Meeting Attendees quota. This value must be an integer from 10 through 100 and divisible by 10. If the value is not specified or is incorrectly specified, the value is 80.

THRESHOLD_CONC_TRAINING_USERS The default threshold percentage for the Concurrent Learners quota. This value must be an integer from 10 through 100 and divisible by 10. If the value is not specified or is incorrectly specified, the value is 80.

The following are sample values added to the custom.ini file:

```
THRESHOLD_NUM_OF_MEMBERS = 90
THRESHOLD_CONC_USERS_PER_MEETING = 90
THRESHOLD_CONC_MEETING_USERS_PER_ACCOUNT = 90
THRESHOLD_CONC_TRAINING_USERS = 75
```

2 Do the following to restart Adobe Connect:

a Choose Start > Programs > Adobe Connect Server > Stop Adobe Connect Central Application Server.

b Choose Start > Programs > Adobe Connect Server > Start Adobe Connect Central Application Server.

Configuring the session timeout value

Adobe Connect sessions include Adobe Connect Meeting and Adobe Connect Central. The session timeout specifies how long a session can be idle before the server disconnects it. When a session is disconnected, the user is redirected to the Adobe Connect Central login page.

The Adobe Connect session timeout value is 30 minutes. Account administrators can change this value in the Adobe Connect Central Administration tab. System administrators can also change the session timeout value in the custom.ini file. The value in Adobe Connect Central takes precedence over the value in the custom.ini file.

To configure session timeout in the custom.ini file:

1 In a text editor, open *[root_install_dir]*\custom.ini.

2 Add the following parameter and set it to the desired value, in seconds:

```
SESSION_TIMEOUT = 3600
```

***Note:** This value changes the session timeout from 30 minutes to 60 minutes.*

3 Save the custom.ini file.

4 Restart the application server and the meeting server.

***Important:** Before Adobe Connect 8, the session timeout was 16 hours. You may need to update applications that use the Adobe Connect Web Services API to catch a session timeout and re-authenticate.*

More Help topics

"Start and stop the servers" on page 80

Configuring PDF to SWF conversion

About PDF conversion

You can use the Share pod in an Adobe Connect meeting room to share PDF documents. Hosts and presenters can synchronize the navigation for all attendees and use the whiteboard overlay to collaborate. You can load PDF documents into the Share pod from the desktop or from the Adobe Connect content library. Sharing documents in the Share pod offers the following advantages over screen sharing:

- Hosts and presenters can preload and organize documents in the meeting room.
- Higher quality viewing experience for all attendees.
- Lower bandwidth requirement for participants and presenters.
- Easier for multiple presenters to work together.
- Easier to collaborate using the whiteboard.

When the PDF documents are shared in a Share pod, Adobe Connect converts them to Flash format. Adobe Connect Server offers configuration parameters to control the PDF conversion.

Configure PDF to SWF conversion

1 Open the *RootInstallationFolder*\custom.ini file in a text editor.

2 Edit any of the following configuration parameters:

Parameter	Default Value	Description
`ENABLE_PDF2SWF`	true	A Boolean value specifying whether PDF to SWF conversion is enabled or not for the server. Set this parameter to false to disable conversion due to performance concerns.
`PDF2SWF_PAGE_TIMEOUT`	5	The timeout value per page, in seconds.
`PDF2SWF_CONVERTER_PORTS_START`	4000	The lowest value of the range of ports used for PDF to SWF conversions.
`PDF2SWF_CONVERTER_PORTS_END`	4030	The highest value of the range of ports used for PDF to SWF conversions.
`PDF2SWF_CONCURRENCY_LIMIT`	3	The maximum number of concurrent PDf to SWF conversions that can take place on an application server. If an application server receives more requests, the requests are queued.
`PDF2SWF_QUEUE_LIMIT`	5	The maximum number of PDF to SWF conversions that can wait in a queue at one time. If an application server receives more requests, a user sees the message “Adobe Connect could not convert the file for viewing, please retry after some time. “ An administrator sees the following in the logs: <status code="request-retry"><exception>java.lang.Exception: Conversion Load too much on server.
`PDF2SWF_TIMEOUT_NUMBER_OF_PAGES`	3	The maximum number of pages that are allowed to timeout before the conversion is stopped.

3 Restart Adobe Connect Central Application Server. See “Start and stop Adobe Connect” on page 80.

Integrating with Microsoft Live Communications Server 2005 and Microsoft Office Communications Server 2007

Workflow for configuring presence integration

Integrate Adobe Connect with a Microsoft real-time communications server so meeting hosts can see the LCS or OCS presence of registered meeting participants in the Invitees List and initiate text-based conversations with online users.

1. Adobe Connect Server and a communications server must be installed.

Install and verify the installation of Adobe Connect Server and a communications server. Adobe Connect Server supports integration with Microsoft Live Communications Server 2005 and Microsoft Office Communications Server 2007. See "Install Adobe Connect 9" on page 20and the documentation for the communications server.

2. Configure the communications server.

Configure the communications server to exchange data with Adobe Connect. See "Configure Live Communications Server 2005" on page 59or "Configure Office Communications Server 2007" on page 60.

3. Stop Adobe Connect Presence Service.

Adobe Connect Server includes the Adobe Connect Presence Service. Stop the service before you configure Adobe Connect. See "Start and stop Adobe Connect Presence Service" on page 64.

4. Configure Adobe Connect Presence Service.

Configure Adobe Connect so that it can exchange data with the communications server. The presence server is installed to *RootInstallationFolder*\presserv. See "Configure Adobe Connect Presence Service" on page 62.

5. Start Adobe Connect Presence Service.

See "Start and stop Adobe Connect Presence Service" on page 64.

6. Enable Invitee list and Chat pod in Adobe Connect Central.

Log on to Adobe Connect Central as an administrator. Select Administration > Compliance and Control > Pod Management. Uncheck the option to disable the Invitee list and Chat pod.

Configure Live Communications Server 2005

***Note:** If you are installing Office Communications Server 2007, see "Configure Office Communications Server 2007" on page 60.*

1 Choose Start > Programs > Administrative Tools > Live Communications Server 2005 to open the Configuration Console.

2 Right-click the Forest, select Properties, and do the following:

a Select the Federation tab.

b Select the Enable federation and public IM connectivity check box.

c Enter the Adobe Connect network address.

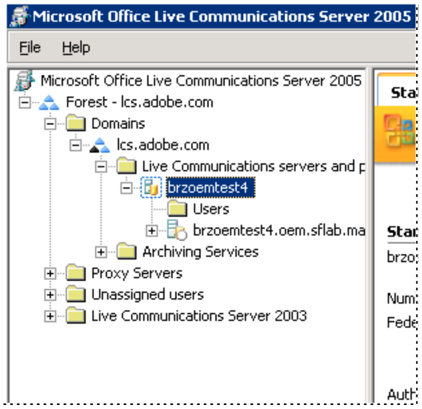
d Enter port 5072.

5072 is the default port number of the Adobe Connect Presence Service in the \presserv\conf\lcsgw.xml file.

e Click OK.

3 In the left pane of the Configuration Console, expand Domains, expand your domain, and expand Live Communications servers and pools.

4 Right-click the host name of your pool and select properties.


Microsoft Office Live Communications Server 2005
File Help
Microsoft Office Live Communications Server 2005
Forest - lcs.adobe.com
Domains
lcs.adobe.com
Live Communications servers and p
brzoemtest4
Users
brzoemtest4.oem.sflab.ma
Archiving Services
Proxy Servers
Unassigned users
Live Communications Server 2003
Sta
Star
brzo
Num
Fede
Auth

5 In the server Properties dialog, do the following:

a Select the Host Authorization tab. Add the IP address of Adobe Connect. Verify that Outbound Only is No, Throttle as Server is Yes, and Treat as Authentication is Yes.

b If a load balancer is installed in front of your Adobe Connect server, add the IP address of the load balancer.

c Click OK.

6 In the left pane of the Configuration Console, expand the FQDN of your server and select Applications.

7 Do the following:

a Click IM URL Filter Application Setting. In the Properties dialog, deselect Enable. If this setting is enabled, meeting hosts cannot send URLs in instant messages.

8 Close the Configuration Console.

Configure Office Communications Server 2007

***Note:** If you are installing Live Communications Server 2005, see “Configure Live Communications Server 2005” on page 59.*

1 Choose Start > Programs > Administrative Tools > Office Communications Server 2007 to open the Configuration Console.

2 Right-click the Forest, select Properties, and then select Global Properties.

3 Select the General tab, add or select a default domain, and then click OK.

4 Select the Federation tab, and then do the following:

a Select the Enable Federation and Public IM connectivity check box.

b Enter the FQDN of the Office Communications Server 2007.

c Enter port 5072.

5072 is the default port number of the Adobe Connect Presence Service in the \presserv\conf\lcsgw.xml file.

d Click OK.

5 In the Forest, right-click the hostname, select Properties, and then select Front End Properties.

6 Select the Authentication tab, choose NTLM as the authentication protocol, and then click OK.

7 Select the Host Authorization tab, and then do the following:

a Add the IP address of the Adobe Connect system.

b Select the Throttle As Server and Treat As Authenticated check boxes.

c Click OK.

8 Right click on the hostname and domain name (for example, brzoemtest5.oem.sflab.macromedia.com) and select Properties > Front End Properties.

9 Select the General tab, and then do the following:

a Add port 5072, Transport TCP, Address All.

b Add port 5060, Transport MTLS, Address All.

c Add port 5061, Transport MTLS, Address All.

d Enable all three ports and then click OK.

10 Select the IM Conferencing tab, and then do the following:

a Set the IP address to the address of the OCS 2007 Server.

b Set the SIP listening port to 5062.

c Click OK.

11 Select the Telephony Conferencing tab, and then do the following:

a Set the IP address to the address of the OCS 2007 Server.

b Set the SIP listening port to 5064.

c Click OK.

12 Select the Certificate tab.

You see the information about your SSL certificate.

13 In the Forest, expand the hostname and domain name (for example, brzoemtest5.oem.sflab.macromedia.com) and then do the following:

a Right-click Applications and then select Properties.

b Make sure the Intelligent IM URL Filter Application Setting is not enabled, and then click OK.

14 Close the Configuration Console.

15 If you are upgrading from Live Communications Server 2005, perform the following steps for each user to enable enhanced presence:

a Select Start > Programs > Administrative Tools > Active Directory Users and Computers.

b Right-click a user name and select Enable users for Communications Server.

Configure communications server clients

The Adobe Connect integration with Microsoft communications servers works with standard Microsoft Office Communicator 2005 (MOC 2005) clients. The clients do not require any special configuration. However, to make Adobe Connect meeting URLs clickable on MOC 2005, modify the “Allow hyperlinks in an instant message” property of the Communicator Administrative template. For more information, see http://technet.microsoft.com/en-us/library/bb963959.aspx.

1 Choose Start > Run.

2 Enter gpedit.msc in the Open box to open the Group Policy window.

3 Click to expand Computer Configuration.

4 Click to expand Administrative Templates.

5 Right-click Microsoft Office Communicator Policy Settings and choose Properties.

***Note:** If the Microsoft Office Communicator Policy Settings template is missing from the Administrative Templates folder, add it. Locate the Communicator.adm in the Microsoft Office Communicator 2005 client package and copy it to C:\WINDOWS\inf\. In the Group Policy window, right-click Administrative Templates, click Add/Remove Templates, click Add, browse to the file, and click Open.*

Configure Adobe Connect Presence Service

Complete the following four procedures to configure Adobe Connect Presence Service to exchange data with a communications server. After you complete the configuration, restart Adobe Connect Central Application Server.

Define the gateway connection between the Adobe Connect Presence Service and the communications server

1 Open the *RootInstallationFolder*\presserv\conf\lcsgw.xml file in an XML editor.

2 Edit the file to read as follows, substituting your values for the values in bold:

```
<?xml version="1.0" encoding="UTF-8"?>
<config>
<block xmlns="accept:config:sip-lcsgw">
<service trace="off" name="lcsgw" id="internal.server">
<stack name="lcs">
<via/>
</stack>
<state type="enabled"/>
<host type="external">lcs.adobe.com</host>
<domain-validation state="false"/>
<binding name="connector-0" transport="tcp">
<port>5072</port>
<bind>10.59.72.86</bind> <!-- LCS server IP -->
<area>lcs.adobe.com</area> <!-- LCS domain -->
</binding>
</service>
</block>
</config>
```

Parameter	Description
`<host>`	SIP realm of LCS or OCS users
`<bind>`	IP address of LCS or OCS server (or load balancer
`<area>`	SIP realm of LCS or OCS users

Configure the custom.ini file

1 Open *RootInstallationFolder*\custom.ini in a text editor.

2 Enter the following parameters and values:

Parameter	Value
OPN_ADAPTOR	com.macromedia.breeze.opn.OPNGateway This value is case-sensitive.
OPN_HOST	The network address of the Adobe Connect Presence Service (for example, localhost).
OPN_PORT	The internal port used between Adobe Connect and Adobe Connect Presence Service. The default value (10020) must match the value in the *RootInstallationFolder*\presserv\conf\router.xml file. Do not modify this value.
OPN_PASSWORD	The internal token used between Adobe Connect and Adobe Connect Presence Service. The default value (secret) must match the value in the *RootInstallationFolder*\presserv\conf\router.xml file. Do not modify this value.
OPN_DOMAIN	The domain name of the Adobe Connect server (application server). Adobe Connect Presence Service uses this name to identify the application server. In a cluster, each application server must have its own domain name.
MEETING_PRESENCE_POLL_INTERVAL	Host clients poll the presence server periodically to retrieve the status of invitees. This parameter sets the number of seconds between polling requests. The default value is 30. Do not modify this value.

The following are sample settings:

```
OPN_ADAPTOR=com.macromedia.breeze.opn.OPNGateway
OPN_HOST=localhost
OPN_PORT=10020
OPN_PASSWORD=secret
OPN_DOMAIN=breeze01.com
```

Define the SIP gateway to Adobe Connect Presence Service

1 Open the *RootInstallationFolder*\presserv\conf\router.xml file in an XML editor.

2 Edit the file to read as follows, substituting your values for the values in bold:

```
<block xmlns="accept:config:xmpp-gateway">
...
<block xmlns="accept:config:sip-stack-manager">
<service trace="off">
<bind>10.133.192.75</bind> <!-- presence server machine IP -->
<state type="enabled"/></service></block>
```

In the `<bind>` tag, enter the IP address of the computer hosting Adobe Connect. If multiple IP addresses are returned, select the internal or external IP address that the remote LCS or OCS server can resolve to connect to Adobe Connect.

3 Restart Adobe Connect Central Application Server.

Configure Adobe Connect Presence Service in a cluster

If you are running Adobe Connect in a cluster, run Adobe Connect Presence Service on only one computer in the cluster. However, configure Adobe Connect Presence Service on all computers in the cluster so the computers can exchange presence traffic.

1 Open the *[root_install_dir]*\custom.ini file in a text editor.

2 Enter the following parameters and values:

Parameter	**Value**
OPN_ADAPTOR	com.macromedia.breeze.opn.OPNGateway This value is case-sensitive.
OPN_HOST	The FQDN of the computer running Adobe Connect Presence Service. The value of the OPN_HOST parameter is the same on every computer in a cluster.
OPN_PORT	The internal port used between Adobe Connect and Adobe Connect Presence Service. The default value (10020) must match the value in the *RootInstallationFolder*\presserv\conf\router.xml file. Do not modify this value.
OPN_PASSWORD	The internal token used between Adobe Connect and Adobe Connect Presence Service. The default value (secret) must match the value in the *RootInstallationFolder*\presserv\conf\router.xml file. Do not modify this value.
OPN_DOMAIN	The domain Adobe Connect Presence Service uses to identify an Adobe Connect server in a cluster. Each computer in a cluster must have a unique value. The OPN_DOMAIN parameter can have any value (for example, presence.connect1, presence.connect2, connect3) as long as the value is unique within the cluster.
MEETING_PRESENCE_POLL_INTERVAL	Host clients poll the presence server periodically to retrieve the status of invitees. This parameter sets the number of seconds between polling requests. The default value is 30. Do not modify this value.

The following are sample settings:

```
OPN_ADAPTOR=com.macromedia.breeze.opn.OPNGateway
OPN_HOST=localhost
OPN_PORT=10020
OPN_PASSWORD=secret
OPN_DOMAIN=presence.connect1
```

3 Restart Adobe Connect Central Application Server.

Start and stop Adobe Connect Presence Service

You can start and stop Adobe Connect Presence Service from the Start menu or from the Services window.

Start and stop Adobe Connect Presence Service from the Start menu

❖ Do one of the following:

- Choose Start > Programs > Adobe Adobe Connect Server > Start Adobe Connect Presence Service.
- Choose Start > Programs > Adobe Connect Server > Stop Adobe Connect Presence Service.

Start and stop Adobe Connect Presence Service from the Services window

1 Choose Start > Control Panel > Administrative Tools > Services to open the Services window.

2 Select Adobe Connect Presence Service and click Start the service, Stop the service, or Restart the service.

Configuring single sign-on (SSO)

About single sign-on

Single sign-on is a mechanism that allows a user to authenticate once and gain access to multiple applications. Single sign-on uses a proxy server to authenticate users so they don’t need to log in to Adobe Connect.

Adobe Connect supports the following single sign-on mechanisms:

HTTP header authentication Configure an authentication proxy to intercept the HTTP request, parse the user credentials from the header, and pass the credentials to Adobe Connect.

Microsoft NT LAN Manager (NTLM) authentication Configure Adobe Connect to attempt to automatically authenticate connecting clients against a Windows domain controller using the NTLMv1 protocol. Microsoft Internet Explorer on Microsoft Windows can negotiate NTLM authentication without prompting the user for credentials.

***Note:** NTLM authentication doesn't work on edge servers. Use LDAP authentication instead.*

***Note:** Mozilla Firefox clients may be able to negotiate NTLM authentication without prompting. For information about configuration, see this Firefox document.*

You can write your own authentication filter as well. For more information, contact Adobe Support.

Configure HTTP header authentication

When HTTP header authentication is configured, Adobe Connect login requests are routed to an agent positioned between the client and Adobe Connect. The agent can be an authentication proxy or a software application that authenticates the user, adds another header to the HTTP request, and sends the request to Adobe Connect. On Adobe Connect, you must uncomment a Java filter and configure a parameter in the custom.ini file that specifies the name of the additional HTTP header.

More Help topics

“Start and stop Adobe Connect” on page 80

Configure HTTP header authentication on Adobe Connect

To enable HTTP header authentication, configure a Java filter mapping and a header parameter on the computer hosting Adobe Connect.

1 Open the file *[root_install_dir]*\appserv\web\WEB-INF\web.xml and do the following:

a Remove the comment tags around the filter and filter-mapping elements for `HeaderAuthenticationFilter`.

b Add comment tags around the NtlmAuthenticationFilter filter and filter-mapping elements.

2 Stop Adobe Connect:

a Choose Start > Programs > Adobe Connect Server > Stop Adobe Connect Central Application Server.

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

3 Add following line to the custom.ini file:

```
HTTP_AUTH_HEADER=header_field_name
```

Your authentication agent must add a header to the HTTP request that is sent to Adobe Connect. The name of the header must be *`header_field_name`*.

4 Save the custom.ini file and restart Adobe Connect:

a Choose Start > Programs > Adobe Connect Server > Start Adobe Connect Meeting Server.

b Choose Start > Programs > Adobe Connect Server > Start Adobe Connect Central Application Server.

Write the authentication code

The authentication code must authenticate the user, add a field to the HTTP header that contains the user login, and send a request to Adobe Connect.

1 Set the value of the *`header_field_name`* header field to an Adobe Connect user login.

2 Send an HTTP request to Adobe Connect at the following URL:

```
http://connectURL/system/login
```

The Java filter on Adobe Connect catches the request, looks for the *`header_field_name`* header, then looks for a user with the ID passed in the header. If the user is located, the user is authenticated and a response is sent.

3 Parse the HTTP content of the Adobe Connect response for the string `"OK"` to indicate a successful authentication.

4 Parse the Adobe Connect response for the `BREEZESESSION` cookie.

5 Redirect the user to the requested URL on Adobe Connect, and pass the `BREEZESESSION` cookie as the value of the `session` parameter, as follows:

```
http://connectURL?session=BREEZESESSION
```

***Note:** You must pass the `BREEZESESSION` cookie in any subsequent requests to Adobe Connect during this client session.*

Configure HTTP header authentication with Apache

The following procedure describes a sample HTTP header authentication implementation that uses Apache as the authentication agent.

1 Install Apache as a reverse proxy on a different computer than the one hosting Adobe Connect.

2 Choose Start > Programs > Apache HTTP Server > Configure Apache Server > Edit the Apache httpd.conf Configuration file and do the following:

a Uncomment the following line:

```
LoadModule headers_module modules/mod_headers.so
```

b Uncomment the following three lines:

```
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_connect_module modules/mod_proxy_connect.so
LoadModule proxy_http_module modules/mod_proxy_http.so
```

c Add the following lines to the end of the file:

```
RequestHeader append custom-auth "ext-login"
ProxyRequests Off
<Proxy *>
Order deny,allow
Allow from all
</Proxy>
ProxyPass / http://hostname:[port]/
ProxyPassReverse / http://hostname:[port]/
ProxyPreserveHost On
```

3 Stop Adobe Connect:

a Choose Start > Programs > Adobe Connect Server > Stop Adobe Connect Central Application Server.

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

4 On the computer hosting Adobe Connect, add the following lines of code to the custom.ini file (located in the root installation directory, C:\Connect, by default):

```
HTTP_AUTH_HEADER=custom-auth
```

The `HTTP_AUTH_HEADER` parameter should match the name configured in the proxy. (In this example, it was configured in line 1 of step 2c.) The parameter is the additional HTTP header.

5 Save the custom.ini file and restart Adobe Connect:

a Choose Start > Programs > Adobe Connect Server > Start Adobe Connect Meeting Server.

b Choose Start > Programs > Adobe Connect Server > Start Adobe Connect Central Application Server.

6 Open the file *[root_install_dir]*\appserv\web\WEB-INF\web.xml and do the following:

a Uncomment the complete HeaderAuthenticationFilter filter.

b Comment out the complete NtlmAuthenticationFilter filter.

Configure NTLM authentication

NTLMv1 is an authentication protocol used with the SMB network protocol in Microsoft Windows networks. You can use NTLM to allow a user to prove their identity to a Windows domain once and thereafter be authorized to access another network resource, such as Adobe Connect. To establish the user's credentials, the user's web browser automatically performs a challenge and response authentication with the domain controller through Adobe Connect. If this mechanism fails, the user can log into Adobe Connect directly. Only Internet Explorer on Windows supports single sign-on with NTLMv1 authentication.

***Note:** By default, Windows Server 2003 domain controllers require a security feature called SMB signatures. SMB signatures are not supported by the default configuration of the NTLM authentication filter. You can configure the filter to work within this requirement. For more information on this and other advanced configuration options, see the JCIFS NTLM HTTP authentication documentation.*

Add configuration parameters

Do the following for each host in an Adobe Connect cluster:

1 Open the *[root_install_dir]*\custom.ini file in a text editor and add the following parameters:

```
NTLM_DOMAIN=[domain]
NTLM_SERVER=[WINS_server_IP_address]
```

The value `[domain]` is the name of the Windows domain that users are members of and authenticate against, for example, CORPNET. You may need to set this value to the pre-Windows 2000 compatible version of the domain name. For more information, see TechNote 27e73404. This value is mapped to the filter property `jcifs.smb.client.domain`. Setting the value directly in the web.xml file overrides the value in the custom.ini file.

The value `[WINS_server_IP_address]` is the IP address or a comma-separated list of IP addresses of WINS servers. Use the IP address, the host name does not work. The WINS servers are queried in the order specified to resolve the IP address of a domain controller for the domain specified in the `NTLM_DOMAIN` parameter. (The domain controller authenticates users.) You can also specify the IP address of the domain controller itself, for example, 10.169.10.77, 10.169.10.66. This value is mapped to the filter property `jcifs.netbios.wins`. Setting the value in the web.xml file overrides the value in the custom.ini file.

2 Save the custom.ini file.

3 Open the file *[root_install_dir]*\appserv\web\WEB-INF\web.xml in a text editor and do the following:

a Remove comments tags around the entire NtlmAuthenticationFilter and filter-mapping elements.

b Add comment tags to the HeaderAuthenticationFilter filter and filter-mapping elements.

4 Save the web.xml file.

5 Restart Adobe Connect.

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

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

Reconcile login policies

Adobe Connect and NTLM have different login policies for authenticating users. Reconcile these policies before users can employ a single login.

The NTLM protocol uses a login identifier that can be a user name (jdoe), an employee ID number (1234), or an encrypted name, depending on the policy or the organization. By default, Adobe Connect uses an e-mail address (jdoe@mycompany.com) as a login identifier. Change the Adobe Connect login policy so that Adobe Connect shares a unique identifier with NTLM.

1 Open Adobe Connect Central.

To open Adobe Connect Central, open a browser window and enter the FQDN of the Adobe Connect Host (for example, http://connect.mycompany.com). You entered the Adobe Connect Host value on the Server Settings screen of the Application Management Console.

2 Select the Administration tab. Click Users and Groups. Click Edit Login and Password Policies.

3 In the Login Policy section, select No for Use e-mail address as the login.

Configuring a reverse proxy in front of Adobe Connect

Using a reverse proxy

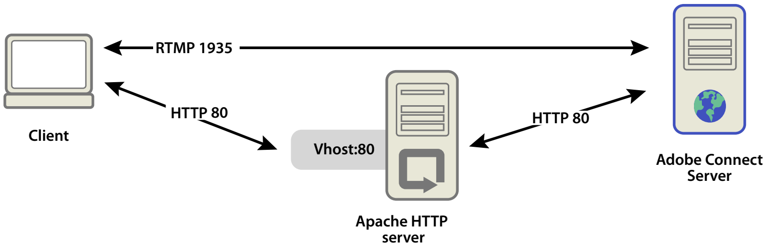
You can configure a reverse proxy in front of Adobe Connect. Traffic flows through the reverse proxy before it reaches Adobe Connect. Use this configuration to do the following:

- Keep Adobe Connect out of the DMZ.

  Put the reverse proxy in the DMZ and put Adobe Connect behind your organization’s firewall.

- Authenticate users before they reach Adobe Connect.

  The reverse proxy authenticates users with another system and authorizes them to connect to Adobe Connect.



HTTP traffic flows through Apache HTTP Server to reach Adobe Connect.

Configure a reverse proxy

This example uses the Windows (32 bit) installation of Apache HTTP Server. The configuration is identical on any operating system Apache supports. This example does not use SSL; traffic to the Adobe Connect application server is not encrypted.

***Note:** Flush the reverse proxy cache when you upgrade Adobe Connect to ensure the new file versions are served.*

Do the following to force all HTTP traffic to pass through Apache HTTP Server before it reaches Adobe Connect:

***Note:** RTMP traffic does not pass through Apache HTTP Server in this configuration.*

1 Install Apache HTTP Server.

By default, the Apache configuration files are located in the folder c:\Program Files\Apache Software Foundation\Apache2.2\conf\.

2 Configure Apache to listen for all traffic on port 80.

Open the c:\Program Files\Apache Software Foundation\Apache2.2\conf\httpd.conf file in a text editor and add the following:

```
#
# Listen: Allows you to bind Apache to specific IP addresses and
# ports, instead of the default. See also the <VirtualHost>
# directive.
#
# Change this to Listen on specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
#
#Listen 12.34.56.78:80
Listen 80
#
#
```

3 Load the modules required for operation as a reverse proxy.

In the same file (httpd.conf), uncomment the following lines:

```
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_http_module modules/mod_proxy_http.so
LoadModule proxy_connect_module modules/mod_proxy_connect.so
```

4 Link the httpd.conf file to the configuration file that directs connections to Adobe Connect.

Add the following line as the last line of the httpd.conf file:

```
Include conf/extra/httpd-connect.conf
```

5 Create a text file called httpd-connect.conf and save it to c:\Program Files\Apache Software Foundation\Apache2.2\conf\extra.

6 Add the following lines to the httpd-connect.conf file (insert your IP addresses and ports where requested):

```
#vhost for application server
<VirtualHost *:80>
ProxyRequests Off
ProxyPreserveHost On
ProxyPass / http://<IP-of-Adobe-Connect-Application-Server>:80/
ProxyPassReverse / http://<IP-of-Adobe-Connect-Application-Server>:80/
ServerName <FQDN of Apache host>
</VirtualHost>
```

7 Save the file and restart the Apache service.

8 Open the Adobe Connect Application Management Console in a browser: http://localhost:8510/console/

9 On the Server settings screen, do the following:

- Set the Adobe Connect Host to the FQDN of the Apache HTTP Server.
- Set the External Name to the FQDN of the computer hosting Connect Meeting Server.

10 Restart Adobe Connect Service (the application server) and Flash Media Server (FMS) service (the meeting server). See “Start and stop the servers” on page 80.

RTMP is routed to Adobe Connect and HTTP is routed through Apache.

Hosting Adobe Connect Add-in

About Adobe Connect Add-in

The Adobe Connect Add-in is a version of Flash Player that includes enhanced features for Adobe Connect meetings.

When Adobe Connect Add-in is required, it’s downloaded from an Adobe server in a seamless process that is hidden to the user. However, if your organization doesn’t allow employees to download software from external servers, you can host Adobe Connect Add-in on your own server.

Meeting guests, registered users, and presenters are asked to download Adobe Connect Add-in if they have an old version installed and are promoted to host or presenter or given enhanced rights to the Share pod.

Meeting hosts and presenters are required to download Adobe Connect Add-in if it isn’t installed or if an old version is installed.

Customize Adobe Connect Add-in download location

You can host Adobe Connect Add-in on your server and send users directly to the executable files. You may want to send users to a page with download instructions that contains links to the executable files. You can create your own download instruction page or use one provided by Adobe. The Adobe page is localized for all supported languages.

Send users directly to the executable files:

1 Locate the Adobe Connect language XML files on the server hosting Adobe Connect. The XML files are in the following two directories: *[root_install_dir]*\appserv\common\intro\lang and*[root_install_dir]*\appserv\common\meeting\lang.

2 In each language file, enter a path to the executable files for each platform:

```
<m id="addInLocation" platform="Mac OSX">/common/addin/ConnectAddin.z</m>
<m id="addInLocation" platform="Windows">/common/addin/setup.exe</m>
<m id="addInLocation" platform="Linux">/common/addin/ConnectAddin.deb</m>
```

***Note:** These are the default locations of the add-in executable files. You can change the locations on your server and change the paths in the `addInLocation` section accordingly.*

Send users to download instruction pages provided by Adobe

1 Locate the Adobe Connect language XML files on the server hosting Adobe Connect. The XML files are in the following two directories:*[root_install_dir]*\appserv\common\intro\lang and *[root_install_dir]*\appserv\common\meeting\lang.

2 In each language file, enter the path to the download instruction page:

```
<m id="addInLocation" platform="Mac OSX">/common/help/#lang#/support/addindownload.htm</m>
<m id="addInLocation" platform="Windows">/common/help/#lang#/support/addindownload.htm</m>
<m id="addInLocation" platform="Linux">/common/help/#lang#/support/addindownload.htm</m>
```

***Note:** The path includes a `#lang#` string that Adobe Connect translates to the language of the meeting at runtime.*

3 The addindownload.htm files include links to the add-in executable files at their default locations on Adobe Connect (/common/addin/setup.exe, /common/addin/AdobeConnectAddin.z, and /common/addin/ConnectAddin.deb). If you change the location of the executable files, update the links in the addindownload.htm page for each language.

Send users to download instruction pages you create

1 Locate the Adobe Connect language XML files on the server hosting Connect. The XML files are in the following two directories: *[root_install_dir]*\appserv\common\intro\lang and *[root_install_dir]*\appserv\common\meeting\lang.

2 In each language file, add the following paths to the instruction page you created:

```
<m id="addInLocation" platform="Mac
OSX">common/help/#lang#/support/addin_install_instructions.html</m>
<m id="addInLocation"
platform="Windows">common/help/#lang#/support/addin_install_instructions.html</m>
<m id="addInLocation"
platform="Linux">common/help/#lang#/support/addin_install_instructions.html</m>
```

***Note:** You can choose to create separate instruction pages for each platform.*

3 Create an instruction page in each language you want to support. Include links on the instruction page to the add-in executable files for each platform.

Chapter 4: Security

Securing Adobe® Connect™ protects your organization against loss of property and malicious acts. It is important to secure the infrastructure of your organization, Adobe Connect Server, and the database server used by Adobe Connect.

SSL (secure sockets layer)

About SSL support

Adobe Connect Server is made up of two servers: Adobe® Flash® Media Server and the Adobe Connect application server. Flash Media Server is called the *meeting server* because it serves meetings over a real-time RTMP connection to the client. The Adobe Connect application server handles the HTTP connection between the client and the Adobe Connect application logic. Adobe Connect Server also connects to a SQL Server database.

***Note:** In the Start menu, the meeting server is called "Adobe Connect Meeting Server" and the application server is called "Adobe Connect Central Application Server". In the Services window, the meeting server is called "Flash Media Server" and the application server is called "Adobe Connect Service".*

You can configure SSL for the application server, the meeting server, and the database.

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

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

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

Adobe Connect uses the HTTP `CONNECT` method to request an SSL connection. Proxy servers must allow clients to use the `CONNECT` method. If clients cannot use the `CONNECT` method, RTMP connections tunnel over HTTP/HTTPS.

For information about configuring SSL, see Configure SSL for Adobe Connect Server 8.

For help configuring SSL, contact Adobe Support at www.adobe.com/support/programs/connect.

PKI (public key infrastructure)

About PKI (public key infrastructure)

You can set up a public key infrastructure (PKI) to manage identification credentials as part of your Adobe Connect security architecture for clients. In the more familiar SSL protocol, the server must verify its identity to the client; in PKI, the client must verify its identity to the server.

A trusted third party, called a Certification Authority, verifies the identity of a client and binds a certificate to the client. The certificate (also called a *public key*) is in X.509 format. When a client connects to Adobe Connect, a proxy negotiates the connection for PKI. If the client has a cookie from a previous session or has a valid certificate, the client is connected to Adobe Connect.

For more information about PKI, see the Microsoft PKI Technology Center.

PKI user requirements

Users must run Windows XP or Windows 2003 and have a valid client-certificate installed on their local computer before joining a meeting that requires PKI authentication. When a user joins a meeting, they are presented with a dialog to choose a valid client-certificate from the certificates installed on their computer.

Adobe recommends that clients use the Adobe Connect Add-in to attend meetings that require PKI authentications. Clients must use the add-in stand-alone installer to install the add-in before joining a meeting.

Clients can also use the latest version of Adobe Flash Player in the browser to attend meetings, but Flash Player PKI support is not as extensive as add-in PKI support. One exception is that to view meeting archives, clients must have the latest version of Flash Player installed.

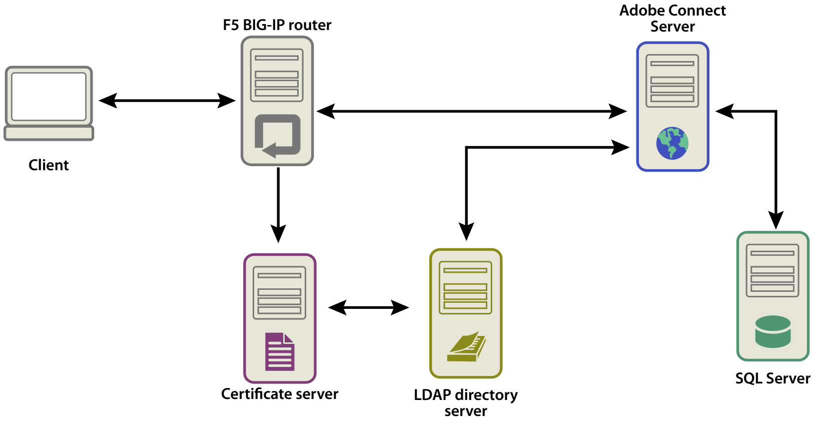
You can design a PKI system to require authentication for only HTTP connections or for both HTTP and RTMP connections. If you require client-side certificates on both HTTP and RTMP connections, users are prompted each time a new server connection is established. For example, there would be two prompts to log in to a meeting, once for HTTP and once for RTMP. An RTMP connection cannot be established without HTTP authentication, so you may choose to require client-side authentication only on the HTTP connection.

Implementing PKI

The following steps guide you through a reference implementation of PKI configured with an F5 BIG-IP LTM 9.1.2 (Build 40.2) router as the proxy. Use the critical sections to build your own solution, either with an F5 router or with another device.

This reference implementation adheres to strict security standards, for example, it requires a client-side certificate for both HTTP (application server) and RTMP (meeting server) connections.

Note: *Adobe strongly recommends that you create a security policy before implementing PKI. There are many different technologies used in PKI, and upholding security is critical when these systems interact.*



Data flow in a public key infrastructure

This example assumes the following:

- Adobe Connect is installed.
- Adobe Connect is integrated with an LDAP directory service.
- A user imported from the LDAP directory service can enter a meeting served by Adobe Connect.
- An F5 router is installed.

1. Configure the LDAP directory server.

An LDAP `email` attribute must be specified for each user. This attribute is added to the subject field of the client certificate.

The F5 iRule parses the X.509::subject for the e-mail address and inserts the value into the HTTP header. Adobe Connect uses the HTTP header to authenticate the user.

***Note:** This example uses the `email` attribute. You can use any unique identifier that the X.509 format exposes, has a length of 254 characters or less, and that the LDAP directory service and Adobe Connect share.*

2. Set Adobe Connect login policy.

Adobe Connect must use an e-mail address for user login. In Adobe Connect Central, select the Administration tab, then click Users and Groups, the click Edit Login and Password Policies.

3. Configure a CA server.

The CA (Certification Authority) server handles requests for certificates, verifies client identities, issues certificates, and manages a CRL (client revocation list).

In this implementation, the CA points to the LDAP directory server to obtain a client certificate. The CA queries the LDAP server for the client information and, if it exists and hasn't been revoked, formats it into a certificate.

Verify that the client certificate is installed and usable by looking at the subject field. It looks like the following:

```
E = adavis@asp.sflab.macromedia.com
CN = Andrew Davis
CN = Users
DC = asp
DC = sflab
DC = macromedia
DC = com
```

4. Configure Adobe Connect to use HTTP-header authentication.

In the file *[root_install_dir]*\appserv\web\WEB-INF\web.xml, uncomment the following code:

```
<filter-mapping>
    <filter-name>HeaderAuthenticationFilter</filter-name>
    <url-pattern>/*</url-pattern>
</filter-mapping>
```

Stop the meeting server and the application server. In the custom.ini file in the root installation directory, add the following line:

```
HTTP_AUTH_HEADER=hah_login
```

Save the custom.ini file and restart Connect.

5. Configure the F5 application logic.

The application logic in F5 parses the subject field of the client certificate for the e-mail address. The logic passes the e-mail address to Adobe Connect in an additional HTTP header.

A client that doesn't have a certificate is rejected. If a client has a certificate, the certificate must be authenticated. Example authentication mechanisms are OCSP (Online Certification Status Protocol) and LDAP lookup.

Once the certificate is authenticated, parse it for a unique identifier that Adobe Connect knows. In this example, a valid certificate is parsed for an e-mail address.

A request that includes the string `session` or has a `BREEZESESSION` cookie is allowed to pass without authentication because the client has already authenticated. (Adobe Connect verifies these arguments with a database query.)

If the request doesn't include the `session` string or `BREEZESESSION` cookie, the user must log in to Adobe Connect. To log in a user, place the unique identifier (in this case, the e-mail address) into the `HTTP_AUTH_HEADER` field and redirect the request to the Adobe Connect login page.

The following code is an F5 iRule placed on the HTTPS profile that handles requests:

```
set id [SSL::sessionid]
set the_cert [session lookup ssl $id]
set uname [X509::subject $the_cert]
set emailAddr [getfield $uname "emailAddress=" 2]
if { [HTTP::cookie exists BREEZESESSION] } {
    set cookie_payload [HTTP::cookie value BREEZESESSION]
}
elseif { [HTTP::uri] contains "/system/login" }
{
    # Connection has been redirected to the "login page"
    # The email address has been parsed from the certificate
    #
    HTTP::header insert hah_login $emailAddr
}
elseif { [HTTP::uri] contains "session" }
{
    #do nothing, Adobe Connect verifies the token found in session=$token
}
else
{
    # URI encode the current request, and pass it to
    # the Adobe Connect system login page because the client
    # does not have a session yet.
    HTTP::redirect https://[HTTP::host]/system/login/ok?next=[URI::encode
https://[HTTP::host][HTTP::uri]]
}
```

More Help topics

"Start and stop Adobe Connect" on page 80

Securing the infrastructure

Network security

Adobe Connect relies on several private TCP/IP services for its communications. These services open several ports and channels that must be protected from outside users. Adobe Connect requires that you place sensitive ports behind a firewall. The firewall should support stateful packet inspection (not only packet-filtering). The firewall should have an option to "deny all services by default except those explicitly permitted". The firewall should be at least a dual-home (two or more network interfaces) firewall. This architecture helps prevent unauthorized users from bypassing the security of the firewall.

The easiest solution for securing Adobe Connect is to block all ports on the server except 80, 1935, and 443. An external hardware firewall appliance provides a layer of protection against gaps in the operating system. You can configure layers of hardware-based firewalls to form DMZs. If the server is carefully updated by your IT department with the latest Microsoft security patches, a software-based firewall can be configured to enable additional security.

Intranet access

If you intend to have users access Adobe Connect on your Intranet, place the Adobe Connect servers and the Adobe Connect database in a separate subnet, separated by a firewall. The internal network segment where Adobe Connect is installed should use private IP addresses (10.0.0.0/8, 172.16.0.0/12, or 192.168.0.0/16) to make it more difficult for an attacker to route traffic to a public IP and from the network address translated internal IP. For more information, see RFC 1918. This configuration of the firewall should consider all Adobe Connect ports and whether they are configured for inbound or outbound traffic.

Database server security

Whether you are hosting your database on the same server as Adobe Connect, make sure that your database is secure. Computers hosting a database should be in a physically secure location. Additional precautions include the following:

- Install the database in the secure zone of your intranet.
- Never connect the database directly to the Internet.
- Back up all data regularly and store copies in a secure off-site location.
- Install the latest patches for your database server.
- Use SQL trusted connections.

For information on securing SQL Server, see the Microsoft SQL security website.

Create service accounts

Creating a service account for Adobe Connect lets you run Adobe Connect more securely. Adobe recommends creating a service account and a SQL Server 2005 Express Edition service account for Adobe Connect. For more information, see the Microsoft articles “How to change the SQL Server or SQL Server Agent service account without using SQL Enterprise Manager in SQL Server 2000 or SQL Server Configuration Manager in SQL Server 2005” and “The Services and Service Accounts Security and Planning Guide”.

Create a service account

1 Create a local account called ConnectService that doesn’t include any default groups.

2 Set the Adobe Connect Service service, the Flash Media Administration Server service, and the Flash Media Server (FMS) service to this new account.

3 Set “Full Control” for the following registry key:

```
HKLM\SYSTEM\ControlSet001\Control\MediaProperties\PrivateProperties\Joystick\Winmm
```

4 Set “Full Control” on the NTFS folders in the root Adobe Connect folder path (C:\Connect, by default).

Subfolders and files must have the same permissions. For clusters, modify the corresponding paths on each computer node.

5 Set the following logon rights for the ConnectService account:

Log on as a service—SeServiceLogonRight

Create an SQL Server 2005 Express Edition service account

1 Create a local account called ConnectSqlService that doesn't include any default groups.

2 Change the SQL Server 2005 Express Edition Service Account from LocalSystem to ConnectSqlService.

3 Set "Full Control" for ConnectSqlService for the following registry keys:

```
HKEY_LOCAL_MACHINE\Software\Clients\Mail
HKEY_LOCAL_MACHINE\Software\Microsoft\Microsoft SQL Server\80
HKEY_LOCAL_MACHINE\Software\Microsoft\Microsoft SQL Server\ [databaseInstanceName]
```

For clusters, follow this step on every node in the cluster. Full Control permission applies to all the child keys of a named database instance

4 Set "Full Control" for ConnectSqlService on the database folders. Subfolders and files must also have the same permissions. For clusters, modify the corresponding paths on each computer node.

5 Set the following user rights for the ConnectSqlService service:

Act as part of the operating system—SeTcbPrivilege Bypass traverse checking—SeChangeNotify Lock pages in memory—SeLockMemory Log on as a batch job—SeBatchLogonRight Log on as a service—SeServiceLogonRight Replace a process level token—SeAssignPrimaryTokenPrivilege

Securing single server installations

The following workflow summarizes the process of setting up and securing Adobe Connect on a single computer. It assumes that the database is installed on the same computer, and that users access Adobe Connect on the Internet.

1. Install a firewall.

Since you are allowing users to connect to Adobe Connect through the Internet, the server is open to an attack by hackers. By using a firewall, you can block access to the server and control the communications that occur between the Internet and the server.

2. Configure the firewall.

After installing your firewall, configure it as follows:

- Inbound ports (from the Internet): 80, 443, 1935.
- Outbound ports (to the mail server): 25.
- Use the TCP/IP protocol only.

  Since the database is located on the same server as Adobe Connect, you do not have to open port 1434 on the firewall.

3. Install Adobe Connect.

4. Verify that the Adobe Connect applications are working.

After installing Adobe Connect, verify that it is working properly both from the Internet and from your local network.

5. Test the firewall.

After you have installed and configured the firewall, verify that your firewall is working correctly. Test the firewall by attempting to use the blocked ports.

Securing clusters

Clusters (multi-server) systems are inherently more complex than single-server configurations. An Adobe Connect cluster can be located at a data center or geographically distributed across multiple network operation centers. You can install and configure servers hosting Adobe Connect in multiple locations and synchronize them through database replication.

***Note:** Clusters must use Microsoft SQL Server 2005 Standard Edition, not the embedded database engine.*

The following are important suggestions for securing clusters:

Private networks The simplest solution for clusters in a single location is to create an extra subnet for the Adobe Connect system. This approach offers a high level of security.

Local software firewalls For Adobe Connect servers that are located in a cluster but share a public network with other servers, a software firewall may be appropriate on each individual server.

VPN systems In multiserver installations hosting Adobe Connect in different physical locations, you may want to consider using an encrypted channel to communicate with the remote servers. Many software and hardware vendors offer VPN technology to secure the communications to remote servers. Adobe Connect relies on this external security if data traffic must be encrypted.

Security tips and resources

Security best practices

The following checklist describes best practices to you secure your Adobe Connect system:

Use SSL to protect network traffic You can secure the connection to the meeting server, the application server, or both.

Run only the services you need Do not run applications such as a domain controller, a web server, or an FTP server on the same computer as Adobe Connect. To minimize the chances that another application can be used to compromise the server, reduce the number of applications and services running on the computer that hosts Adobe Connect.

Update operating system security Check regularly for critical updates that close security holes and apply the required patches. A firewall eliminates some of these security problems. In general, keep your servers patched with all current security updates approved by Microsoft and the other relevant platform vendors.

Secure host systems If you store sensitive information on your servers, be aware of the physical security of your systems. Adobe Connect relies on the safety of the host system against intruders, so keep servers secure when private and confidential data is at risk. Adobe Connect is designed to take advantage of native environmental features such as file system encryption.

Use strong passwords Strong passwords protect data. Adobe Connect administrators can set login and password policies in the Adobe Connect Central. Adobe Connect installations often use Microsoft SQL Server 2005 Standard Edition, which also requires strong password protection.

Use LDAP for authentication It is a best practice to use LDAP for Adobe Connect authentication.

Perform regular security audits Audit your systems periodically to ensure that all security features are still operating as expected. For example, you can use a port scanner to test a firewall.

Security resources and references

The following resources help you secure your servers:

Network security The SANS (System Administration, Networking, and Security) Institute is a cooperative research and education organization including system administrators, security professionals, and network administrators. It provides network security courses, as well as certification in network security.

SQL Server security The Microsoft SQL security resources page on the Microsoft website provides information on securing SQL Server.

Tools Nmap is a powerful port-scanning program that tells you what ports a system is listening on. It is available at no cost under the GNU Public License (GPL).

Note: *The effectiveness of any security measure is determined by various factors, such as security measures provided by the server and the installed security software. Adobe Connect software is not intended to provide security for your server or the information on it. For more information, see the disclaimer of warranty in the applicable license agreement provided with Adobe Connect.*

Chapter 5: Administering Adobe Connect

Administering Adobe Connect involves the following:

- Managing and monitoring log files to maintain system uptime
- Maintaining disk space
- Backing up data
- Building and generating usage reports

Start and stop the servers

Start and stop Adobe Connect

You can start or stop Connect from the Start menu, the Services window, orthe command line. Verify that the database is running before you start Adobe Connect.

Stop Connect from the Start menu

1 Choose Start > Programs > Adobe Connect Server > Stop Adobe Connect Central Application Server.

2 Choose Start > Programs > Adobe Connect Server > Stop Adobe Connect Meeting Server.

Start Adobe Connect from the Start menu

1 Choose Start > Programs > Adobe Connect Server > Start Adobe Connect Meeting Server.

2 Choose Start > Programs > Adobe Connect Server > Start Adobe Connect Central Application Server.

Stop Adobe Connect from the Services window

1 Choose Start > Control Panel > Administrative Tools > Services to open the Services window.

2 Stop the Adobe Connect Service service.

3 Stop the Flash Media Server (FMS) service.

4 Stop the Flash Media Administration Server service.

Start Adobe Connect from the Services window

1 Choose Start > Control Panel > Administrative Tools > Services to open the Services window.

2 Start the Flash Media Server (FMS) service.

3 Start the Flash Media Server Administration Server service.

4 Start the Adobe Connect Service service.

Stop Adobe Connect from the command line

1 Choose Start > Run to open the Run window. Enter **cmd** to open a Command prompt.

2 Go to the *[root_install_dir]*\appserv\win32 directory.

3 Enter the following command to stop Adobe Connect:

```
net stop ConnectPro
```

4 Enter the following to stop Flash Media Server:

```
net stop FMS
```

5 Enter the following to stop Flash Media Server Administration Server:

```
net stop FMSAdmin
```

Start Adobe Connect from the command line

1 Choose Start > Run to open the Run window. Enter **cmd** to open a Command prompt.

2 Go to the *[root_install_dir]*\appserv\win32 directory.

3 Enter the following to start Flash Media Server:

```
net start FMS
```

4 Enter the following to start Flash Media Server Administrator Server:

```
net start FMSAdmin
```

5 Enter the following to start Adobe Connect:

```
net start ConnectPro
```

Start and stop Adobe Connect Presence Service

You can start and stop Adobe Connect Presence Service from the Start menu or the Services window. Start Adobe Connect Presence Service only if your Adobe Connect system is integrated with Microsoft Live Communications Server or Office Communications Server.

More Help topics

"Integrating with Microsoft Live Communications Server 2005 and Microsoft Office Communications Server 2007" on page 59

Stop the presence service from the Start menu

❖ Choose Start > Programs > Adobe Connect Server > Stop Adobe Connect Presence Service.

Start the presence service from the Start menu

❖ Choose Start > Programs > Adobe Connect Server > Start Adobe Connect Presence Service.

Stop, start, or restart the presence service from the Services window

1 Choose Start > Control Panel > Administrative Tools > Services to open the Services window.

2 Select the Adobe Connect Presence Service.

3 Choose Start, Stop, or Restart the service.

Start and stop Adobe Connect Telephony Service

You can start and stop the Adobe Connect Telephony Service from the Services window.

1 Choose Start > Control Panel > Administrative Tools > Services to open the Services window.

2 Select the Adobe Connect Telephony Service.

3 Choose Start, Stop, or Restart the service.

Start and stop Flash Media Gateway

You can start and stop Flash Media Gateway from the Services window or from the command line. Verify that Adobe Connect Server is running before you start Flash Media Gateway.

Start and stop Flash Media Gateway from the Services window

1 Choose Start > Control Panel > Administrative Tools > Services to open the Services window.

2 Select Flash Media Gateway Service.

3 Choose Start, Stop, or Restart the service

Start and stop Flash Media Gateway from the command line

1 Choose Start > Run to open the Run window. Enter **cmd** to open a Command prompt.

2 Enter the following to start Flash Media Gateway:

```
net start fmg
```

3 Enter the following to stop Flash Media Gateway:

```
net stop fmg
```

Start and stop Adobe Connect Edge Server

You can start Adobe Connect or stop Adobe Connect Edge Server from the Start menu, the Services window, and from the command line.

Stop Adobe Connect Edge Server from the Start menu

❖ Choose Start > Programs > Adobe Connect Edge Server > Stop Adobe Connect Edge Server.

Start Adobe Connect Edge Server from the Start menu

❖ Choose Start > Programs > Adobe Connect Edge Server > Start Adobe Connect Edge Server.

Stop Adobe Connect Edge Server from the Services window

1 Choose Start > Settings > Control Panel > Administrative Tools > Services to open the Services window.

2 Stop the Flash Media Server (FMS) service.

3 Stop the Flash Media Server Administration Server service.

Start Adobe Connect Edge Server from the Services window

1 Choose Start > Settings > Control Panel > Administrative Tools > Services to open the Services window.

2 Start the Flash Media Server Administration Server service.

3 Start the Flash Media Server (FMS) service.

Stop Adobe Connect Edge Server from the command line

1 Choose Start > Run to open the Run window. Enter **cmd** to open a Command prompt.

2 Enter the following to stop Flash Media Server:

```
net stop FMS
```

3 Enter the following to stop the Flash Media Server Administrator Server:

```
net stop FMSAdmin
```

Start Adobe Connect Edge Server from the command line

1 Choose Start > Run to open the Run window. Enter **cmd** to open a Command prompt.

2 Enter the following to start the Flash Media Server Administrator Server:

```
net start FMSAdmin
```

3 Enter the following to start Flash Media Server:

```
net start FMS
```

Managing and monitoring logs

About log files

Use Adobe Connect log files to view information about events that occur during operation. You can use the information in the log files to create monitoring mechanisms and reports, and to troubleshoot problems. Log files provide information about user activities and server performance. For example, log files can indicate the reason a user was denied access when attempting to log in, or the reason that a telephony connection failed.

Adobe Connect log files are in the *RootInstallationFolder*\logs folder.

The Apache Tomcat log files are in the *RootInstallation*\logs\tomcat folder.

Configuring log files

Adobe Connect uses the Apache log4j tool. Use the file *RootInstallationFolder*\appserv\conf\log4j.xml to configure logging. For more information, see Log4j XML Configuration Primer.

To configure log appender use the details provided at the DailyRollingFileAppender page.

Sample log file entry

The following sample entry from the access.log file includes a heading, a list of the fields used in the log entry, and the specific data for this log entry:

```
#Version: 1.0
#Start-Date: 2010-10-30 17:09:24 PDT
#Software: Adobe Connect Server
#Date: 2010-04-30
#Fields: date time x-comment x-module x-status x-severity x-category x-user x-access-request
time-taken db-logical-io db-transaction-update-count
2006-10-30 18:12:50 Not logged in. PRINCIPAL NO_ACCESS_NO_LOGIN W A PUBLIC
{cookie=breezxnb5pqusyshfgttt, ip=138.1.21.100} GET http://joeuser.adobe.com&mode=xml 0 20/5 0
```

The following table explains the sample entry:

Field	Data	Description
date	2010-10-30	The date on which the logged event occurred.
time	18:12:50	The time when the logged event occurred.
x-comment	Not logged in.	Indicates that a user was unable to log in to the application server.
x-module	PRINCIPAL	The event occurred in the Principal module in the application server.

Field	Data	Description
x-status	NO_ACCESS_NO_LOGIN	Indicates that the user was unable to log in.
x-severity	W	Identifies the event severity as a warning (W).
x-category	A	Indicates the event is an access (A) issue (appearing in the access.log file).
x-user	PUBLIC	The current user; in this case, an unidentified guest, or public user.
x-access-request	http://joeuser.adobe.com&mode=xml	Source of the request.
time-taken	0	No time was required to process this request.
db-logical-io	20/5	20 database reads were required and 5 rows of data were returned.
db-transaction-update-count	0	No database rows were updated in processing this request.

Log file format

The log files use the W3C Extended Log File Format and you can use any text editor to read them.

Log fields in the access.log and error.log files

Each log entry contains 11 log fields, which provide information about what type of event occurred, where it occurred, its severity, and other relevant data:

Field	Format	Description
date	YYYY/MM/DD	Date on which transaction completed.
time	HH:MM:SS	Local computer time at which transaction completed.
x-comment	String	Contains human-readable information about the log entry. This field is always output as the left most field.
x-module	String	Indicates where the error occurred.
x-status	String	Indicates what event occurred.
x-severity	Text (one character)	Indicates whether the logged event is critical (C), error (E), warning (W), or information (I).
x-category	Text (one character)	Indicates whether the log entry represents an access (A) or system (S) event.
x-user	String	Text that represents current user. Applicable only if x-category is access (A); otherwise field is set to a single hyphen (-) to denote an unused field.
x-access-request	String	Text that represents the access request. This text can be a URL or an API name with passed parameters. Applicable only if x-category is access (A); otherwise this field is set to a single hyphen (-) to denote an unused field.
time-taken	Number	Time required to process the request (in seconds). Applicable only if x-category is access (A); otherwise this field is set to a single hyphen (-) to denote an unused field.
db-logical-io	String	Number of database reads required to process the request and the number of rows returned in <reads>/<rows> format.
db-transaction-update-count	String	Number of rows updated in transactions while processing the requests. If the request uses more than one transaction, this value is the sum of all updates.

Module field entries

A module is a component of the server that manages some related set of operations. Each module belongs to either the application server or the meeting server. The x-module field indicates where the log event occurred:

Log Entry for x-module Field	Description	Server
ACCESS_KEY	Manages access keys.	Application server
ACCOUNT	Manages account operations.	Application server
ACL	Manages ACL-related operations.	Application server
AICC	Manages all AICC communication between server and content.	Application server
BUILDER	Performs SCO builds.	Application server
Client	Client methods.	Meeting server
CLUSTER	Manages all cluster-related operations.	Application server
CONSOLE	Manages all console-related operations.	Application server
Content	Share pod.	Meeting server
DB	Represents the database.	Application server
EVENT	Manages all event-related operations.	Application server
HOSTED_MANAGER	Manages system accounts (create, update, delete, settings, and so on).	Application server
MEETING	Manages all meeting-related operations.	Application server
Misc	Miscellaneous module.	Meeting server
NOTIFICATION	Manages all e-mail operations.	Application server
PERMISSION	Manages all permission-related operations.	Application server
Poll	Poll pod.	Meeting server
PLATFORM_FRAMEWORK	Represents the platform framework.	Application server
PRINCIPAL	Manages all principal-related operations.	Application server
REPORT	Represents reports.	Application server
Room	Manages meeting room startup and shutdown.	Meeting server
RTMP	Represents RTMPHandler.	Application server
SCO	Manages all SCO-related operations.	Application server
SEARCH	Manages all search-related operations.	Application server
START_UP	Represents the startup component.	Application server
TELEPHONY	Manages all telephony-related operations.	Application server
TRACKING	Manages all transcript-related operations.	Application server
TRAINING	Manages all training-related operations.	Application server

Comment and status field entries

The x-comment field and the x-status field indicate what type of event occurred. The x-status field provides a code for each logged event. The x-comment field provides a human-readable description of each logged event.

The following table lists the status codes, the comment associated with each status code, and an explanation of each logged event:

Log Entry for x-status Field	**Log Entry for x-comment Field**	**Description**
ACCESS_DENIED	Client trying to access protected method. Access is denied. {1}	Logged when client attempts to access protected method.
BECAME_MASTER	Server {1} has been designated the master.	Logged when the scheduler quits and this server becomes the scheduler.
CLUSTER_CON_BROKEN	Server {1} unable to reach {2} on port {3} to perform cluster operations.	Logged when Adobe Connect is unable to reach another server in the cluster.
CLUSTER_FILE_TRANSFER_ERROR	Unable to transfer {1} from server {2}.	Logged when an error is thrown while transferring a file.
CONNECT	New client connecting: {1}	Logged when new client connects.
CONNECT_WHILE_GC	Connecting while the application is shutting down - forcing shutdown.	Logged when client attempts to connect while application is shutting down.
DB_CONNECTION_ERROR	Unable to connect to database {1}.	Logged when Adobe Connect cannot reach the database.
DB_CONNECTION_TIME_OUT	Timed out waiting for database connection.	Logged when database connection takes too long.
DB_VERSION_ERROR	Database {1} is incompatible with the current version of Adobe Connect.	Logged when the database is out of date.
DISCONNECT	A client is leaving. Details: {1}	Logged when client disconnects.
EXT_ERROR	External error thrown by a third party.	Logged when external code threw an error.
FMS_CON_BROKEN	Health check failed due to broken FMS service connection.	Logged when service connection is severed.
FMS_NOT_FOUND	Unable to connect to FMS at startup.	Logged when Adobe Connect is unable to establish the service connection at startup.
INTERNAL_ERROR	Internal error occurred.	Logged when internal error is thrown.
INVALID	-	Logged when invalid operation is attempted.
INVALID_DUPLICATE	Value {1} is a duplicate in the system.	Logged when value entered duplicates a value in the system.
INVALID_FORMAT	Field {1} of type {2} is invalid.	Value specified is invalid for this field.
INVALID_ILLEGAL_OPERATION	Illegal operation performed.	Requested operation is not legal.
INVALID_ILLEGAL_PARENT	-	Logged when an ACL has an invalid parent. For example, if folder A is inside folder B, folder B cannot be in folder A.
INVALID_MISSING	Field {1} of type {2} is missing.	Missing required value for this field.
INVALID_NO_SUCH_ITEM	Value {1} is an unknown in the system.	Requested item does not exist.
INVALID_RANGE	The specified value must be between {1} and {2}.	Logged when value entered is out of range.

Log Entry for x-status Field	**Log Entry for x-comment Field**	**Description**
INVALID_TELEPHONY_FIELD	Telephony authentication values were not validated by the service provider.	Service provider unable to validate telephony account.
INVALID_VALUE_GTE	The specified value must be greater than or equal to {1}.	Logged when value entered is out of range.
INVALID_VALUE_LTE	The specified value must be less than or equal to {1}.	Logged when value entered is out of range.
KILLING_LONG_CONNECTION	Client has been in the room for 12 hours, disconnecting.	Logged when client connection is terminated after time limit is reached.
LICENSE_EXPIRED	Your license has expired and your account will be disabled on {1}. Please upload a new license file through the console manager to continue using Adobe Connect.	Logged when customer is using Adobe Connect during grace period and access is about to be cut off.
LICENSE_EXPIRY_WARNING	Your license will expire on {1}. Please upload a new license file through the console manager to continue using Adobe Connect.	Logged when license is 15 days or fewer from expiring.
MASTER_THREAD_TIMED_OUT	Master thread has not reported progress in {1} milliseconds.	Scheduler thread not running.
MEETING_BACKUP_END	Server {1} is no longer the backup for room {2}.	Meeting backup has ended.
MEETING_BACKUP_START	Server {1} is now the backup for room {2}.	Meeting backup has started.
MEETING_FAILOVER	Meeting {1} failed over to {2}.	Logged when a meeting fails over to this server.
MEETING_TMP_READ	Meeting template {1} read for room {2}.	Template read from meeting.
MEETING_TMP_WRITTEN	Meeting template {1} written to room {2}.	Template written to meeting.
NO_ACCESS_ACCOUNT_EXPIRED	Your account has expired.	Accessed account has expired.
NO_ACCESS_DENIED	Permission check failed.	Permission check error.
NO_ACCESS_LEARNER	No permission to take courses.	Must be a member of the learner group to take a course.
NO_ACCESS_LEARNING_PATH_BLOCKED	You have not fulfilled a prerequisite or preassessment.	Prerequisite or pre assessment error.
NO_ACCESS_NO_EXTERNAL_USER_MODIFICATION	External users cannot be modified.	User is not allowed to modify LDAP users.
NO_ACCESS_NO_LICENSE_FILE	Your license file has not been uploaded.	License file not found.
NO_ACCESS_NO_LOGIN	Not logged in.	Error thrown when user not logged in.
NO_ACCESS_NO_QUOTA	A {1} quota error occurred for account {2} with limit {3}.	Out of quota.
NO_ACCESS_NO_RETRY	You have reached the max limit and can not take the course again.	User has exceeded course retry limit.
NO_ACCESS_NO_SERVER	Server not available	Requested server is not available.
NO_ACCESS_NOT_AVAILABLE	The requested resource is unavailable.	Logged when the requested resource is not available.
NO_ACCESS_NOT_SECURE	SSL request made on a non-SSL server.	Secure request made on non-secure server.
NO_ACCESS_PASSWORD_EXPIRED	Your password has expired.	Logged when a user password has expired.

Log Entry for x-status Field	**Log Entry for x-comment Field**	**Description**
NO_ACCESS_PENDING_ACTIVATION	Your account has not been activated yet.	Account is not activated yet.
NO_ACCESS_PENDING_LICENSE	Your account activation is pending a license agreement.	Account not usable until license agreement is read.
NO_ACCESS_SCO_EXPIRED	The course you tried to access is no longer available.	Course end date is passed.
NO_ACCESS_SCO_NOT_STARTED	Course is not open yet.	Course start date is not reached.
NO_ACCESS_WRONG_ZONE	Content accessed from wrong zone.	Thrown when content or user accesses a server in the wrong zone.
NO_DATA	Permission check failed.	Query did not return any data.
NO_DISKSPACE	Health check failed due to lack of disk space.	Logged when the account runs out of disk space.
NOT_AVAILABLE	Requested resource is not available.	Error thrown when resource is not available.
OK	-	Request successfully processed.
OPERATION_SIZE_ERROR	Operation too large to complete.	Logged when operation can’t be completed because of size.
REQUEST_RETRY	Unable to process request. Please try again.	The request failed.
RESPONSE_ABORTED	Client that made request is not available to receive response.	Logged when user closes browser before server can send response back.
RTMP_SVC_BLOCKED	Adobe Connect service request blocked from {1} because the server has not fully started up yet.	Service connection requested from SCO but the server is still starting.
RTMP_SVC_CLOSED	Adobe Connect service connection closed for {1}.	Service connection closed for SCO.
RTMP_SVC_REQUEST	Adobe Connect service request received from {1}.	Service connection requested from SCO.
RTMP_SVC_START	Adobe Connect service connection established with {1}.	Service connection established with SCO.
SCRIPT_ERROR	Run-Time Script Error. Details: {1}	Logged when script error is detected.
SERVER_EXPIRED	Health check failed due to server expiry (expiry date={1}, current time={2}).	Logged when server does not pass health check before timing out.
SOME_ERRORS_TERMINATED	Some actions terminated with an error.	Logged when an error causes some actions to terminate.
START_UP_ERROR	Start up error: {1}.	Logged when an exception is thrown during startup.
START_UP_ERROR_UNKNOWN	Unable to start up server. Adobe Connect might already be running.	Logged when an unknown error is thrown during startup. JRUN prints the error.
TEL_CONNECTION_BROKEN	Telephony connection {1} was unexpectedly broken.	Logged when the telephony connection breaks.
TEL_CONNECTION_RECOVERY	Telephony connection {1} was reattached to conference {2}.	Logged when Adobe Connect recovers a connection to the conference again.

Log Entry for x-status Field	Log Entry for x-comment Field	Description
TEL_DOWNLOAD_FAILED	Unable to download {1} for archive {2}.	Logged when time out occurs while downloading telephony audio files.
TOO_MUCH_DATA	Multiple rows unexpectedly returned.	Logged when an operation returns more data than expected.
UNKNOWN_TYPE	{1}	Logged when variable type is unknown.

***Note:** In the preceding table, {1} and {2} are variables that are replaced with a value in the log entry.*

Severity field entries

The x-severity field indicates how serious a condition is, which helps you determine the appropriate response level.

Log Entry for x-severity	Meaning	Suggested Action	Example
C	Critical	Configure third- party monitoring tools to alert pagers when a log entry with this severity level occurs.	Can’t reach the database. Can't start or end a process. A failure is affecting the system.
E	Error	Configure third- party monitoring tools to send an e-mail when a log entry with this severity level occurs.	Can't reach Adobe® Premiere®. Conversion failed. A failure is affecting a user or account, but not the whole system.
W	Warning	Generate and review periodic reports to identify possible operational and product improvements.	Disk or memory use has exceeded the specified threshold.
I	Info	Review log entries for auditing or RCA purposes.	Server started, stopped, or restarted.

Category field entries

The x-category field indicates whether the event relates to access issues (A) or general system issues (S). All entries of category A appear in the access.log file, and all entries of category S appear in the error.log file.

Log Entry for x-category field	Meaning	Description
A	access	Status code is related to access issues. Logged in access.log file.
S	system	Status code is related to general system issues. Logged in error.log file.

Maintaining disk space

About maintaining disk space

The Adobe Connect system must have a minimum of 1 GB of free space. Adobe Connect does not have any built-in tools that monitor disk space—the administrator must monitor disk space with operating system utilities or third-party tools.

Content can be stored on the server hosting Adobe Connect, on external shared storage volumes, or both.

More Help topics

"Configuring shared storage" on page 52

Maintain disk space on Adobe Connect servers

❖ Do any of the following:

- Use Adobe Connect Central to delete unused content. See Delete a file or folder.
- Replace your server disk with a bigger disk.

Note: *If the free disk space on the server falls below 1 GB, the server stops.*

Maintain disk space on shared storage devices

❖ Monitor the primary shared storage device for free space and available file system nodes. If either drops below 10%, add more storage to the device or add another shared storage device.

Note: *10% is a recommended value. Also, if you're using shared storage, set a maximum cache-size value in Application Management Console or the cache can fill up the disk.*

Clear the edge server cache

Adobe recommends that you create a weekly scheduled task to clear the edge server cache. It's a good idea to run the task during off-peak hours, such as early Sunday morning.

1 Create a cache.bat file to delete the cache directory. The entry in this file must use the following syntax:

```
del /Q /S [cache directory]\*.*
```

The default cache directory is C:\Connect\edgeserver\win32\cache\http. To delete the cache, use the following command:

```
del /Q /S c:\Connect\edgeserver\win32\cache\http\*.*
```

2 Select Start > Programs > Adobe Connect Edge Server > Stop Adobe Connect Edge Server.

3 Run the cache.bat file and verify that it deletes files in the cache directory.

Note: *The directory structure remains, and any files that the edge server locks are not deleted.*

4 Select Start > Programs > Adobe Connect Edge Server > Start Adobe Connect Edge Server.

5 Select Start > Control Panel > Scheduled Tasks > Add Scheduled Task.

6 Select cache.bat as the new file to run.

7 Repeat this procedure for each edge server.

Backing up data

About backing up data

There are three types of data you must back up at regular intervals: content (any files stored in the libraries), configuration settings, and database data.

If you aren't using shared storage devices, all the content in the libraries is stored in the *[root_install_dir]*\content folder (C:\Connect\content, by default). The configuration settings are stored in the custom.ini file in the root installation folder (C:\Connect, by default).

A database backup creates a duplicate of the data in the database. Regularly scheduled database backups can let you recover from many failures, including media failures, user errors, and permanent loss of a server. Back up the database daily.

You can also use backups to copy a database from one server to another. You can re-create the entire database from a backup in one step by restoring the database. The restoration process overwrites the existing database or creates the database if it does not exist. The restored database matches the state of the database at the time the backup was performed, minus any uncommitted transactions.

You create backups on backup devices, such as disk or tape media. You can use a SQL Server utility to configure your backups. For example, you can overwrite outdated backups, or you can append new backups to the backup media.

Follow best practices when backing up the database:

- Schedule a nightly backup.
- Maintain backups in a secure place, preferably at a site different from the site where the data resides.
- Keep older backups for a designated period in case the most recent backup is damaged, destroyed, or lost.
- Establish a system for overwriting backups, reusing the oldest backups first. Use expiration dates on backups to prevent premature overwriting.
- Label backup media to identify the data and prevent overwriting critical backups.

  Use SQL Server utilities to back up the database:

- Transact-SQL
- SQL Distributed Management Objects
- Create Database Backup wizard
- SQL Server Management Studio

Back up server files

Back up and protect system data, just as you protect all the valuable assets of your organization.

It's a good idea to perform this procedure nightly.

1 Do the following to stop Adobe Connect:

a Select Start > Programs > Adobe Connect Server > Stop Adobe Connect Central Service.

b Select Start > Programs > Adobe Connect Server > Stop Adobe Connect Meeting Service.

2 Make a backup copy of the content directory.

The default location is C:\Connect.

3 Make a backup copy of the custom.ini file.

The default location is C:\Connect\.

4 Do the following to start Adobe Connect:

a Select Start > Programs > Adobe Connect Server > Start Adobe Connect Meeting Service.

b Select Start > Programs > Adobe Connect Server > Start Adobe Connect Central Service.

Back up the database

To back up any edition of Microsoft SQL Server, you can use Microsoft SQL Server Management Studio or the Command Prompt window.

The edition of SQL Server that installs with Adobe Connect Server does not include SQL Server Management Studio. However, you can download Microsoft SQL Server Management Studio Express from Microsoft.

Use SQL Server Management Studio to back up SQL Server

***Important:** Do not uninstall the database.*

1 In Windows, select Start > Programs > Microsoft SQL Server 2005 > SQL Server Management Studio.

2 In the Tree pane of the Object Explorer window, right-click on the database (named “breeze,” by default) and choose Tasks > Back Up...

***Note:** For complete instructions for SQL Server database backup and recovery, see the Microsoft Support site.*

Use the Command Prompt window to back up SQL Server

To access help information for database commands, type `osql ?` at the DOS prompt and press Enter.

***Important:** Do not uninstall the database.*

1 Log on to the server hosting Adobe Connect Server.

2 Create a folder to store the database backup files.

This example uses the folder C:\Connect_Database.

3 Select Start > Run, enter **cmd** in the Open box and click OK.

4 At the prompt, change to the directory where you installed the database. By default, the directory is C:\Program Files\Microsoft SQL Server\90\Tools\Binn.

5 At the prompt, enter **osql -E** to log in to the database engine and press Enter.

6 Enter **BACKUP DATABASE database-name TO DISK = 'C:\Connect_Database\database-name.bak'** to run a Microsoft SQL utility that backs up the Connect database and press Enter.

The default database name is *breeze*.

7 At the prompt, enter **go** and press Enter.

The command window displays messages regarding the back up.

8 At the prompt, enter **quit** and press Enter.

9 To verify that the backup was successful, confirm that the breeze.bak file exists in the C:\Connect_Database directory.

10 To restart your database, from your Windows desktop, select Start > Control Panel > Administrative Tools > Services. In the Services window, right-click SQL Server (MSSQLSERVER) and select Start from the context menu.

Building custom reports

Building custom reports using star schema views

Adobe Connect uses a database to store information about users, content, courses, and meetings. User activity populates the database. You can use tools such as Adobe® ColdFusion® Studio and Business Objects Crystal Reports to query star schema views and view the data. You can also use SQL-based tools such as SQL Query Analyzer.

The following Adobe Connect applications can output data to reports:

Adobe Connect Meeting Meeting attendance, meeting duration, and meeting content.

Adobe Presenter Content views, slide views, and presentation views.

Adobe Connect Training Course management information such as course attendee statistics, content viewing statistics, and quiz results.

Note: *In addition, you can run reports from the Adobe Connect Central web application and either view or download them in CSV format. For more information, see Generating reports in Adobe Connect Central.*

SCO fact

Column	Description
dim_sco_details_sco_id	SCO id
dim_sco_details_sco_version	SCO version
max_retries	Maximum number of retries
owner_user_id	User id of the SCO owner
disk_usage_kb	Disk usage in kilobytes
passing_score	Passing score
max_possible_score	Maximum possible score
views	Number of views
unique_viewers	Number of unique users who have viewed the SCO
slides	Number of slides
questions	Number of questions
max_score	Maximum score
min_score	Minimum score
average_score	Average score
average_passing_score	Average passing score
total_registered	Average failing score
total_participants	Total registered users
account_id	Total participants

SCO details dimension

Column	Description
sco_id	SCO id
sco_version	SCO version
sco_name	Name
sco_description	Description
sco_type	SCO type
sco_int_type	Integer type
is_content	Is SCO a content SCO?
url	URL
parent_name	Name of parent SCO
parent_sco_id	SCO id of parent SCO
parent_type	Type of parent SCO
date_sco_created	Date created
date_sco_modified	Date modified
sco_start_date	Start date
sco_end_date	End date
version_start_date	Version start date
version_end_date	Version end date
sco_tag_id	Tag id
passing_score	Passing score
max_possible_score	Maximum possible score
linked_sco_id	Id of a linked SCO
linked_type	Type of a linked SCO
owner_user_id	Owner user id
storage_bytes_kb	Storage bytes in kilobytes
account_id	Account id

Activity fact

Column	Description
dim_activity_details_activity_id	Activity id
score	Score
passed	Passed
completed	Completed
peak_session_users	Peak session users

Column	Description
number_correct	Number correct
number_incorrect	Number incorrect
number_of_questions	Number of questions
number_of_responses	Number of responses
account_id	Account id

Activity details dimension

Column	Description
activity_id	Activity id
dim_sco_details_sco_id	SCO id
dim_sco_details_sco_version	SCO version
dim_users_user_id	User id
dim_sco_details_parent_sco_id	Parent SCO id
score	Score
passed	Passed
completed	Completed
activity_type	Activity type
role	Role
date_activity_started	Date started
date_activity_finished	Date finished
dim_cost_center_id	Cost center id
cost_center_audit_id	Audit id
session_start_date	Session start date
session_end_date	Session end date
attendance_activity	Is attendance activity?
session_id	Session id
account_id	Account id

Curriculum test outs dimension

Column	Description
dim_sco_details_curriculum_sco_id	Curriculum id
dim_sco_details_curriculum_sco_version	Curriculum version
test_out_subject_sco_id	Subject SCO id
test_out_target_sco_id	Target SCO id
test_out_type	Test out type

Column	Description
account_id	Account id

Curriculum prerequisites dimension

Column	Description
dim_sco_details_curriculum_sco_id	Curriculum id
dim_sco_details_curriculum_sco_version	Curriculum version
pre_requisite_subject_sco_id	Subject SCO id
pre_requisite_target_sco_id	Target SCO id
pre_requisite_type	Prerequisite type
account_id	Account id

Curriculum completion requirements dimension

Column	Description
dim_sco_details_curriculum_sco_id	Curriculum id
dim_sco_details_curriculum_sco_version	Curriculum version
completion_subject_sco_id	Subject SCO id
completion_target_sco_id	Target SCO id
completion_requirement_type	Completion requirement type
account_id	Account id

Slide views fact

Column	Description
dim_slide_view_details_slide_view_id	Slide view id
dim_activity_details_activity_id	Activity id
slide_view_display_sequence	Display sequence
account_id	Account id

Slide views details dimension

Column	Description
slide_view_id	Slide view id
date_slide_viewed	Date slide viewed
slide_name	Slide name
slide_description	Slide description
account_id	Account id

Answers fact

Column	**Description**
dim_answer_details_answer_id	Answer id
dim_activity_details_activity_id	Activity id
dim_question_details_question_id	Question id
answer_display_sequence	Display sequence
answer_score	Score?
answer_correct	Is correct?
account_id	Account id

Answer details dimension

Column	**Description**
answer_id	Answer id
date_answered	Date answered
response	Response
account_id	Account id

Question fact

Column	**Description**
dim_sco_details_sco_id	SCO id
dim_sco_details_sco_version	SCO version
dim_question_details_question_id	Question id
number_correct	Number of correct answers
number_incorrect	Number of incorrect answers
total_responses	Total responses
high_score	High score
low_score	Low score
average_score	Average score
account_id	Account id

Question details dimension

Column	**Description**
question_id	Question id
question_display_sequence	Display sequence
question_description	Description
question_type	Question type

Column	Description
account_id	Account id

Question responses dimension

Column	Description
dim_question_details_question_id	Question id
response_display_sequence	Response display sequence
response_value	Value
response_description	Description
account_id	Account id

Groups dimension

Column	Description
group_id	Group id
group_name	Group name
group_description	Group description
group_type	Group type
account_id	Account id

User groups dimension

Column	Description
user_id	User id
group_id	Group id
group_name	Group name
account_id	Account id

User dimension

Column	Description
user_id	User id
login	Login
first_name	First name
last_name	Last name
email	E-mail address
user_descrription	User description
user_type	User type
most_recent_session	Most recent session date

Column	Description
session_status	Session status
manager_name	Manager name
disabled	Disabled
account_id	Account id
custom_field_1	Custom field 1 value
custom_field_2	Custom field 2 value
custom_field_3	Custom field 3 value
custom_field_4	Custom field 4 value
custom_field_5	Custom field 5 value
custom_field_6	Custom field 6 value
custom_field_7	Custom field 7 value
custom_field_8	Custom field 8 value
custom_field_9	Custom field 9 value
custom_field_10	Custom field 10 value

Custom field names dimension

Column	Description
dim_column_name	Custom field column name
custom_field_name	Custom field name
account_id	Account id

Cost centers dimension

Column	Description
cost_center_id	Cost center id
cost_center_name	Cost center name
cost_center_description	Cost center description

Building custom reports from legacy database views

***Note:** Adobe Connect version 7 introduced star schema views that you can query to build custom reports. The legacy database views are still supported, but the star schema views are more standardized and robust.*

Adobe Connect uses a database to store information about users, content, courses, and meetings. User activity populates the database. You can use tools such as Business Objects Crystal Reports to query the database and view the data. You can also use SQL-based tools such as SQL Query Analyzer.

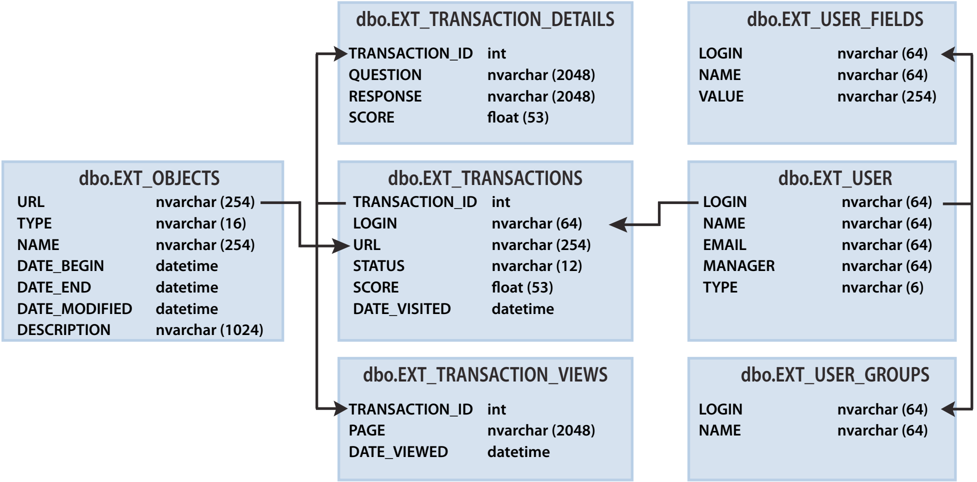
The following Adobe Connect applications can output data to reports:

Adobe Connect Meeting Meeting attendance, meeting duration, and meeting content.

Adobe Presenter Content views, slide views, and presentation views.

Adobe Connect Training Course management information such as course attendee statistics, content viewing statistics, and quiz results.

View relationships between database views



dbo.EXT_TRANSACTION_DETAILS

TRANSACTION_ID	int
QUESTION	nvarchar (2048)
RESPONSE	nvarchar (2048)
SCORE	float (53)

dbo.EXT_USER_FIELDS

LOGIN	nvarchar (64)
NAME	nvarchar (64)
VALUE	nvarchar (254)

dbo.EXT_OBJECTS

URL	nvarchar (254)
TYPE	nvarchar (16)
NAME	nvarchar (254)
DATE_BEGIN	datetime
DATE_END	datetime
DATE_MODIFIED	datetime
DESCRIPTION	nvarchar (1024)

dbo.EXT_TRANSACTIONS

TRANSACTION_ID	int
LOGIN	nvarchar (64)
URL	nvarchar (254)
STATUS	nvarchar (12)
SCORE	float (53)
DATE_VISITED	datetime

dbo.EXT_USER

LOGIN	nvarchar (64)
NAME	nvarchar (64)
EMAIL	nvarchar (64)
MANAGER	nvarchar (64)
TYPE	nvarchar (6)

dbo.EXT_TRANSACTION_VIEWS

TRANSACTION_ID	int
PAGE	nvarchar (2048)
DATE_VIEWED	datetime

dbo.EXT_USER_GROUPS

LOGIN	nvarchar (64)
NAME	nvarchar (64)

Arrows depict the entity relationships among the seven reporting views.

***Note:** The following are not supported: views that are not identified in this document, altering the views that are identified in this document, or direct access to the underlying database schema.*

❖ Use a diagramming tool that connects to your database to see the relationships between the database views.

EXT_TRANSACTIONS

A unique transaction ID is generated each time a user interacts with an object. The EXT_TRANSACTIONS view returns the data listed in the following table:

Column	Data type	Description
TRANSACTION_ID	INT	Unique ID for this transaction.
LOGIN	NVARCHAR	Name of user who carried out this transaction.
URL	NVARCHAR	Object that the user interacted with.
STATUS	NVARCHAR	Can be passed, failed, complete, or in-progress.
SCORE	FLOAT	How the user scored.
DATE_VISITED	DATETIME	Date this transaction was taken or viewed.

Sample query and data The following query returns the data in the following table:

```
select * from ext_transactions where url = '/p63725398/' order by login, date_visited asc;
```

TRANSACTION_ID	LOGIN	URL	STATUS	SCORE	DATE_VISITED
10687	test1-lnagaraj@test.enang.com	/p63725398/	in-progress	0.0	2006-12-15 00:56:16.500
10688	test1-lnagaraj@test.enang.com	/p63725398/	in-progress	0.0	2006-12-15 00:56:16.500
10693	test1-lnagaraj@test.enang.com	/p63725398/	in-progress	0.0	2006-12-15 00:58:23.920

TRANSACTION_ID	LOGIN	URL	STATUS	SCORE	DATE_VISITED
10714	test1-lnagaraj@test.enang.com	/p63725398/	in-progress	10.0	2006-12-15 01:09:20.810
10698	test2-lnagaraj@test.enang.com	/p63725398/	in-progress	10.0	2006-12-15 01:00:49.483
10723	test3-lnagaraj@test.enang.com	/p63725398/	in-progress	10.0	2006-12-15 01:11:32.153
10729	test3-lnagaraj@test.enang.com	/p63725398/	completed	20.0	2006-12-15 01:12:09.700

Query notes The EXT_TRANSACTIONS view returns all existing transactions for a given user and training session. To view the latest transaction, check the maximum DATE_VISITED value.

You can filter on the STATUS and URL fields to get a list of passing users for a specific training session, for example:

```
select * from ext_transactions where url = '/p31102136/' and status = 'user-passed' order by
login, date_visited asc;
```

Generating data User actions that generate data in this view:

- Attending a meeting
- Viewing a piece of content
- Taking a training session (a course or curriculum)

Excluded data •Certificate number, which does not exist in the database

- Maximum score, which is often unavailable

EXT_TRANSACTIONS_VIEWS

The EXT_TRANSACTIONS_VIEWS view retrieves data about the slides or pages that users view.

Column	Data type	Description
TRANSACTION_ID	INT	Unique ID for this transaction (can be merged with TRANSACTION_DETAILS to summarize by URL).
PAGE	NVARCHAR	Slide or page number that was viewed.
DATE_VIEWED	DATETIME	Date this view occurred.

Sample query and data The following query returns the data in the following table:

```
select * from ext_transaction_views where transaction_id = 10702 order by page asc;
```

TRANSACTION_ID	PAGE	DATE_VISITED
10702	0	2006-12-15 01:01:13.153
10702	1	2006-12-15 01:01:18.233
10702	2	2006-12-15 01:01:59.840
10702	3	2006-12-15 01:02:20.717

Generating data Data is generated in this view whenever a user views content or a training session.

EXT_USERS

The EXT_USERS view lists users and associated profile attributes:

Column	Data type	Description
LOGIN	NVARCHAR	Unique user identifier.
NAME	NVARCHAR	Unique user name.
EMAIL	NVARCHAR	Unique e-mail address.
MANAGER	NVARCHAR	The login of the manager. Manager is always set to NULL.
TYPE	NVARCHAR	User or guest. Type is always set to user.

Sample query and data The following query returns the data in the following table:

```
select * from ext_users;
```

LOGIN	NAME	EMAIL	MANAGER	TYPE
test4-lnagaraj@test.enang.com	test4 laxmi	test4-lnagaraj@test.enang.com	NULL	user
test7-lnagaraj@test.enang.com	TEST7 laxmi	test7-lnagaraj@test.enang.com	NULL	user

Generating data Data is updated in this view whenever a guest or user is created, updated, or deleted.

Excluded data •Password, which is not stored in plain text.

- Time zone and language, which are not available in human readable form. For example, PST is 323.
- Last login, which is too resource intensive to calculate. Instead, use a `max(date_visited)` query from the EXT_TRANSACTIONS view to retrieve this data.
- Active session, which is data from the EXT_TRANSACTION view. Instead, use a `STATUS='IN-PROGRESS'` query to retrieve this data.
- Deleted users do not appear in the EXT_USERS view. Deleted users continue to appear in the EXT_TRANSACTION view.
- Data on groups is not included in this view.
- Data on new and pre-defined user custom fields. This information is available for each user in the EXT_USER_FIELDS view.

EXT_USER_FIELDS

The EXT_USER_FIELDS view lists new and predefined custom fields for a specific user. It also lists custom fields for users who are converted to guests.

Column	Data type	Description
LOGIN	NVARCHAR	Unique user identifier.
NAME	NVARCHAR	Field name such as telephone number.
VALUE	NVARCHAR	Field value such as 415.555.1212.

Sample query and data The following query returns the data in the following table:

```
select * from ext_user_fields where login = 'test4-lnagaraj@test.enang.com';
```

LOGIN	NAME	VALUE
test4-lnagaraj@test.enang.com	{email}	test4-lnagaraj@test.enang.com
test4-lnagaraj@test.enang.com	{first-name}	test4
test4-lnagaraj@test.enang.com	{last-name}	laxmi
test4-lnagaraj@test.enang.com	{x-job-title}	sw engr 4
test4-lnagaraj@test.enang.com	{x-direct-phone}	NULL
test4-lnagaraj@test.enang.com	{x-direct-phone-key}	NULL
test4-lnagaraj@test.enang.com	SSN	777

Generating data Actions that generate data in this view: adding, creating, or updating new or predefined custom fields for one or more users.

EXT_USER_GROUPS

The EXT_USER_GROUPS view lists data about groups and associated group members. The EXT_USER_GROUPS view uses the data listed in the following table:

Column	Data type	Description
LOGIN	NVARCHAR	Name of user.
NAME	NVARCHAR	Name of group.

Sample query and data The following query returns the data in the following table:

```
select * from ext_user_groups where login = 'lnagaraj@adobe.com';
```

LOGIN	NAME
lnagaraj@adobe.com	{admins}
lnagaraj@adobe.com	{authors}
lnagaraj@adobe.com	{everyone}
lnagaraj@adobe.com	Laxmi Nagarajan

Query notes Nesting of multiple groups is supported in version 5.1 and later. For example, if group A contains group B, and you are in group B, you are listed as a member of A.

Built-in groups, like the Administrators group, use code names in the schema, as in the following SQL query: `SELECT * FROM EXT_USER_GROUPS where group='{admins}`. The code name distinguishes built-in groups from user-defined groups.

Generating data User actions that generate data in this view:

- Creating, updating, or deleting a group
- Changing group membership

EXT_OBJECTS

The EXT_OBJECTS view lists all system objects (such as meetings, content, courses, and so on) and their attributes.

Column	Data type	Description
URL	NVARCHAR	Unique identifier for the object.
TYPE	NVARCHAR	Either a presentation, course, FLV file, SWF file, image, archive, meeting, curriculum, folder, or event.
NAME	NVARCHAR	Object name as it appears in the content listing.
DATE_BEGIN	DATETIME	The date on which the object is scheduled to begin.
DATE_END	DATETIME	The date on which the object is scheduled to end.
DATE_MODIFIED	DATETIME	The date this object was modified.
DESCRIPTION	NVARCHAR	Object summary information entered when creating a meeting, content, course, or other object type.

Sample query and data The following SQL query returns the data in the following table:

```
select * from ext_objects order by type asc;
```

URL	TYPE	NAME	DATE_BEGIN	DATE_END	DATE_MODIFIED	DESCRIPTION
/p79616987/	course	test api	2006-12-08 23:30:00.000	NULL	2006-12-08 23:36:55.483	NULL
/p47273753/	curriculum	test review curric	2006-12-14 21:00:00.000	NULL	2006-12-14 21:00:30.060	NULL
/tz1/	meeting	{default-template}	2006-12-12 19:15:00.000	2006-12-12 20:15:00.000	2006-12-12 19:25:07.750	release presentation
/p59795005/	presentation	In-QUIZ-TEST1	NULL	NULL	2006-12-15 00:43:19.797	managers meeting

Query notes You can get all objects of a specific type by filtering on the TYPE field. For example, the following SQL query filters for courses and curriculums:

```
select * from ext_objects where type in ('course', 'curriculum');
```

Use the following SQL query to return a list of available system types:

```
select DISTINCT (type) from ext_objects;
```

Generating data User actions that generate data in this view:

- Creating or updating a meeting, course, or curriculum
- Uploading or updating content

Excluded data •Duration, which you can use `date_end- date_begin` to calculate.

- Size on disk, which exposes business rules regarding copies versus originals
- Folder ID
- Deleted objects do not appear in the EXT_OBJECTS view. Deleted objects do exist in the EXT_TRANSACTION view.