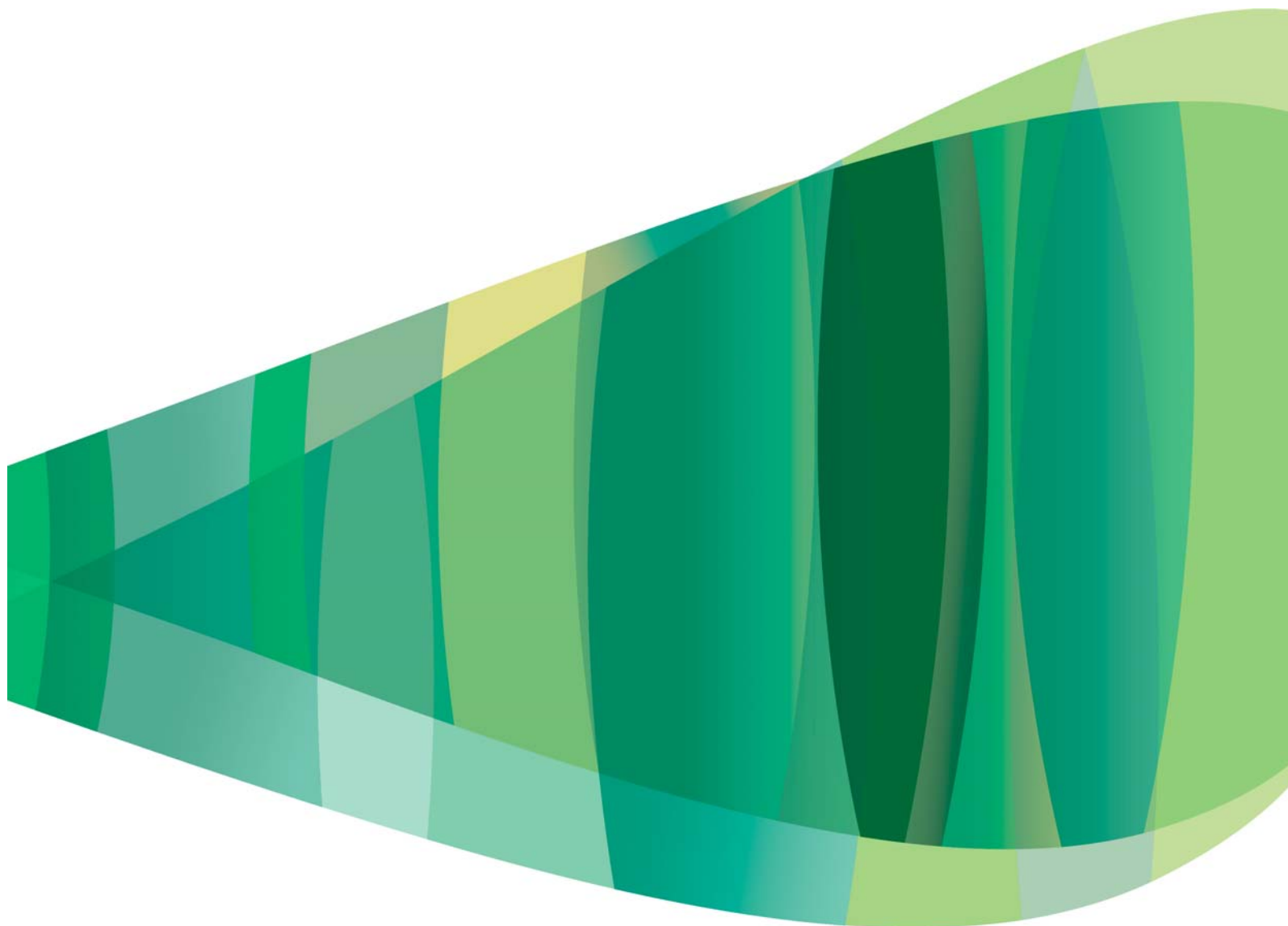


ADOBE® ACROBAT® CONNECT™ PRO 7

MIGRATING, INSTALLING, AND CONFIGURING ADOBE ACROBAT CONNECT PRO SERVER 7



© 2008 Adobe Systems Incorporated. All rights reserved.

Migrating, Installing, and Configuring Adobe® Acrobat® Connect™ Pro Server 7 for Windows®

Protected by U.S. Patents 5,929,866; 5,943,063; 6,289,364; 6,563,502; 6,639,593; 6,754,382; 7,002,597; 7,006,107; 7,039,643; 7,209,258; 7,246,356; 7,262,782; 7,272,658; 7,333,110; Patents Pending in the U.S. and other countries.

If this guide is distributed with software that includes an end user agreement, this guide, as well as the software described in it, is furnished under license and may be used or copied only in accordance with the terms of such license. Except as permitted by any such license, no part of this guide may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, recording, or otherwise, without the prior written permission of Adobe Systems Incorporated. Please note that the content in this guide is protected under copyright law even if it is not distributed with software that includes an end user license agreement.

The content of this guide is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by Adobe Systems Incorporated. Adobe Systems Incorporated assumes no responsibility or liability for any errors or inaccuracies that may appear in the informational content contained in this guide.

Please remember that existing artwork or images that you may want to include in your project may be protected under copyright law. The unauthorized incorporation of such material into your new work could be a violation of the rights of the copyright owner. Please be sure to obtain any permission required from the copyright owner.

Any references to company names in sample templates are for demonstration purposes only and are not intended to refer to any actual organization.

Adobe, the Adobe logo, Acrobat, Acrobat Connect, Adobe Connect, Adobe Press, Breeze, Flash, and JRun are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Microsoft, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. All other trademarks are the property of their respective owners.

Updated Information/Additional Third Party Code Information available at www.adobe.com/go/thirdparty/

Portions include software under the following terms:

RealDuplex™ Acoustic Echo Cancellation is Copyright © 1995-2004 SPIRIT.

This product contains either BSAFE and/or TIPEM software by RSA Security, Inc.

This product includes software developed by the Apache Software Foundation (www.apache.org/).

Flash video compression and decompression is powered by On2 TrueMotion video technology. © 1992-2005 On2 Technologies, Inc. All Rights Reserved. <http://www.on2.com>.

This product includes software developed by the OpenSymphony Group (<http://www.opensymphony.com/>).

Portions licensed from Nellymoser (www.nellymoser.com).

MPEG Layer-3 audio compression technology licensed by Fraunhofer IIS and THOMSON multimedia (<http://www.iis.fhg.de/amm/>).

Sorenson™ Spark™ video compression and decompression technology licensed from Sorenson Media, Inc.



Thomson: Licensee shall not use the MP3 compressed audio within the Software for real time broadcasting (terrestrial, satellite, cable or other media), or broadcasting via Internet or other networks, such as but not limited to intranets, etc., or in pay-audio or audio on demand applications to any non-PC device (i.e., mobile phones or set-top boxes). Licensee acknowledges that use of the Software for non-PC devices, as described herein, may require the payment of licensing royalties or other amounts to third parties who may hold intellectual property rights related to the MP3 technology and that Adobe has not paid any royalties or other amounts on account of third party intellectual property rights for such use. If Licensee requires an MP3 decoder for such non-PC use, Licensee is responsible for obtaining the necessary MP3 technology license.

Notice to U.S. Government End Users: The Software and Documentation are "Commercial Items," as that term is defined at 48 C.F.R. §2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation," as such terms are used in 48 C.F.R. §12.212 or 48 C.F.R. §227.7202, as applicable. Consistent with 48 C.F.R. §12.212 or 48 C.F.R. §§227.7202-1 through 227.7202-4, as applicable, the Commercial Computer Software and Commercial Computer Software Documentation are being licensed to U.S. Government end users (a) only as Commercial Items and (b) with only those rights as are granted to all other end users pursuant to the terms and conditions herein. Unpublished-rights reserved under the copyright laws of the United States. Adobe agrees to comply with all applicable equal opportunity laws including, if appropriate, the provisions of Executive Order 11246, as amended, Section 402 of the Vietnam Era Veterans Readjustment Assistance Act of 1974 (38 USC 4212), and Section 503 of the Rehabilitation Act of 1973, as amended, and the regulations at 41 CFR Parts 60-1 through 60-60, 60-250, and 60-741. The affirmative action clause and regulations contained in the preceding sentence shall be incorporated by reference.

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

Contents

Chapter 1: Preparing for migration, installation, and configuration

Installation requirements	1
Supported configurations	2
Preparing to migrate	3
Preparing to install	6

Chapter 2: Installing Acrobat Connect Pro Server 7 and Acrobat Connect Pro Edge Server 7

Install Acrobat Connect Pro Server 7	13
Verify your installation	16
Install Acrobat Connect Pro Edge Server 7	18
Start and stop the servers	18
Uninstall the servers	21

Chapter 3: Deploying and configuring Acrobat Connect Pro Server 7 and Acrobat Connect Pro Edge Server 7

Deploying Acrobat Connect Pro Server 7	22
Deploying Acrobat Connect Pro Edge Server 7	25
Integrating with a directory service	28
Configuring shared storage	35
Configuring account notification settings	38
Integrating with Microsoft Live Communications Server 2005 and Microsoft Office Communications Server 2007	39
Configuring single sign-on (SSO)	45
Hosting Acrobat Connect Add-in	47

Chapter 4: Security

SSL (secure sockets layer)	50
PKI (public key infrastructure)	63
Securing the infrastructure	66
Security tips and resources	69

Index	71
--------------------	----

Chapter 1: Preparing for migration, installation, and configuration

Review the installation requirements, supported configurations, and technical overview as you prepare to design and install an Adobe® Acrobat® Connect™ Pro Server 7 system. If you are upgrading to Acrobat Connect Pro Server 7, follow the instructions for backing up files.

Installation requirements

Hardware, software, and user requirements

For Adobe Acrobat Connect Pro Server 7 and Adobe Acrobat Connect Pro Edge Server 7 requirements, see www.adobe.com/go/connect_sysreqs_en.

Port requirements

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

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

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

The following table describes the ports open inside a cluster. Each Acrobat Connect Pro 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 Acrobat Connect Pro 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 Acrobat Connect Pro uses to communicate internally. These ports must not be in use on a server hosting Acrobat Connect Pro or Acrobat Connect Pro may fail to start.

Number	Bind Address	Access	Protocol
1111	127.0.0.1	Internal	RTMP
1434	127.0.0.1 This port is active only when you are using the embedded database.	Internal	TSQL
2909	127.0.0.1	Internal	RMI
8510	127.0.0.1	Internal	HTTP

Supported configurations

Supported server-database configurations

Acrobat Connect Pro uses a database to store information about users and content. The following are the supported Acrobat Connect Pro and database configurations:

Single server with embedded database engine Install Acrobat Connect Pro on a single computer and install the embedded database engine (included on the Acrobat Connect Pro 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 database Install Acrobat Connect Pro on a single computer and install Microsoft® SQL Server 2005 Standard Edition on the same computer.

Single server with external SQL Server database Install Acrobat Connect Pro on a single computer and install SQL Server 2005 Standard Edition on another computer.

Single server with multiple external SQL Server databases Install Acrobat Connect Pro on a single computer and install SQL Server 2005 Standard Edition on multiple computers (also called a cluster) external to Acrobat Connect Pro.

Multiple servers with external SQL Server database Install Acrobat Connect Pro on multiple servers (also called a cluster) and install SQL Server 2005 Standard Edition on another computer.

Multiple servers with multiple external SQL Server databases Install Acrobat Connect Pro on multiple servers (also called a cluster) and install SQL Server 2005 Standard Edition in a separate cluster.

Note: Microsoft SQL Server 2005 Standard Edition is not included with Acrobat Connect Pro Server 7 and must be purchased separately.

See also

“[Preparing to install](#)” on page 6

“[Install Acrobat Connect Pro Server 7](#)” on page 13

Supported LDAP directory servers

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

Note: Any LDAP v.3 directory server may integrate with Acrobat Connect Pro Server 7. However, only directory servers that have been tested by Adobe are supported.

See also

“[Integrating with a directory service](#)” on page 28

Supported content storage devices

You can configure your Acrobat Connect Pro 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/connect_sysreqs_en.

See also

“[Configuring shared storage](#)” on page 35

Preparing to migrate

Migration paths

Run the Adobe Acrobat Connect Pro Server 7 installer to upgrade from Adobe Connect Enterprise 6 to Acrobat Connect Pro Server 7; this is the only upgrade path. The Acrobat Connect Pro installer and Application Management Console provide graphical user interfaces that guide you through the upgrade.

For more information about upgrading, contact Adobe Support:
www.adobe.com/go/connect_licensed_programs_en.

Migrating from Connect Enterprise 6 to Acrobat Connect Pro Server 7

Follow this workflow to migrate from Connect Enterprise 6 to Acrobat Connect Pro Server 7.

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 4.

3. Stop Connect Enterprise 6 and back up files.

See “[Back up files](#)” on page 4.

4. Back up the database.

See “[Back up the database](#)” on page 4.

5. Run the Adobe Acrobat Connect Pro Server 7 installer.

See “[Install Acrobat Connect Pro Server 7](#)” on page 13.

6. Configure Acrobat Connect Pro Server 7.

See “[Configuring Acrobat Connect Pro with the Application Management Console wizard](#)” on page 14.

7. Verify your installation.

See “[Verify your installation](#)” on page 16.

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 Acrobat Connect Pro, 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 Acrobat Connect Pro 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/go/learn_cnn_whatsnew_en.

Back up files

1 To stop all Connect Enterprise 6 services, do the following:

- a Select Start > Programs > Adobe Connect Enterprise Server > Stop Adobe Connect Enterprise Server.
- b Select Start > Programs > Adobe Connect Enterprise Server > Stop Adobe Connect Meeting Server.

2 Make a backup copy of the content directory.

The default location is c:\breeze\content.

3 Make a backup copy of the custom.ini file.

The default location is c:\breeze\custom.ini.

Back up the database

You must back up the database before you migrate. To back up the embedded database engine, use the Command Prompt window; the embedded database engine doesn’t have a graphical user interface.

Note: If you have access to SQL Server Enterprise Manager, you can configure it to back up the embedded database engine. See the following Adobe TechNote: www.adobe.com/go/79895439.

To back up SQL Server, use SQL Server Enterprise Manager.

Important: Do not uninstall the database.

Back up the SQL Server database

If you are using a purchased version of Microsoft SQL Server, you can use SQL Server Enterprise Manager to back up your database.

Important: Do not uninstall the database.

- 1 In Windows, select Start > Programs > Microsoft SQL Server > Enterprise Manager.
- 2 In the Tree pane of the Enterprise Manager window, select the database (named “breeze,” by default).

- 3 Select Tools > Backup Database.

Note: For complete instructions for SQL Server database backup and recovery, see the Microsoft Support site.

Back up the embedded database

If you are using the embedded database, use the following procedure to create a backup of the database.

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 Connect Enterprise Server 6.

- 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:\MSSQL\Binn`.

Note: This is the default directory for Connect Enterprise Server 6. The default directory for Acrobat Connect Pro Server 7 is `c:\Program Files\Microsoft SQL Server\90\Tools\Binn`.

- 5 At the `MSSQL\Binn` 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.

For more information on backing up the embedded database engine, see the Microsoft article “How to back up a Microsoft Data Engine database by using Transact-SQL”.

Migrating from the embedded database to SQL Server

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

Note: You may perform this migration when you migrate from Connect Enterprise 6 to Acrobat Connect Pro Server 7. You may also perform this migration at any time after installing Acrobat Connect Pro Server 7.

1. Install SQL Server 2005 Standard Edition.

Follow the instructions provided by Microsoft to install SQL Server.

2. Back up the embedded database.

See “[Back up the database](#)” on page 4.

Note: The embedded database is a limited version of SQL Server.

3. Copy the .bak file from the Acrobat Connect Pro server to the server hosting SQL Server.

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

4. Restore the database on the server hosting SQL Server 2005 Standard Edition.

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 Acrobat Connect Pro.

Choose Start > Programs > Adobe Acrobat Connect Pro Server 7 > Configure Adobe Acrobat Connect Pro Server 7.

Preparing to install

Acrobat Connect Pro technical overview

A Acrobat Connect Pro installation consists of several components: Connect Pro Central Application Server, Adobe® Flash® Media Server, Connect Pro Presence Service, and a database.

Connect Pro Central Application Server is built on J2EE using components of Macromedia® JRun™ from Adobe. Also 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.

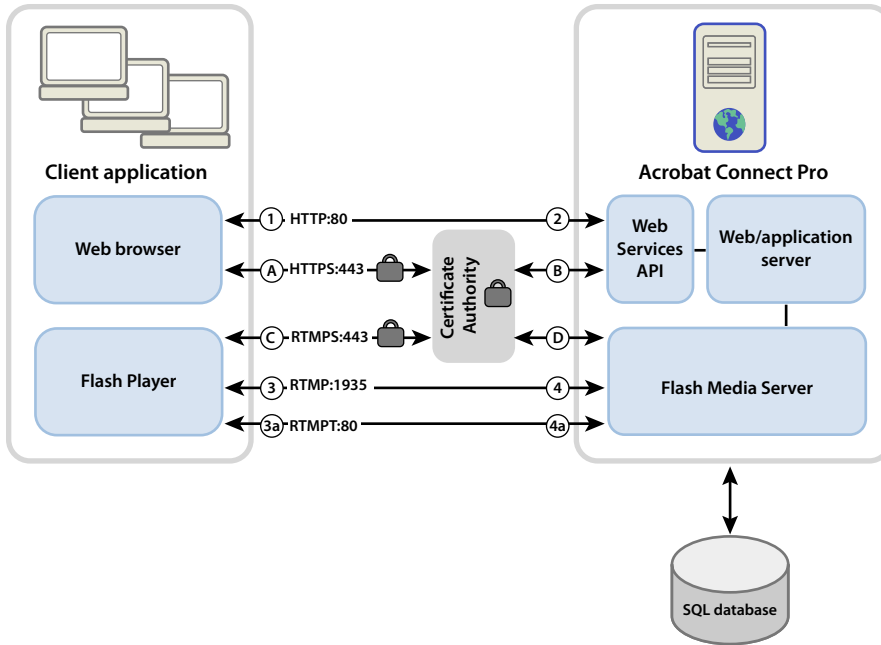
Flash Media Server, also called the *meeting server*, is installed with Acrobat Connect Pro to handle real-time audio and video streaming, data synchronization, and rich-media content delivery, including Acrobat Connect Pro meeting interactions. Some Flash Media Server tasks include meeting recording 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).

Connect Pro Presence Service integrates Acrobat Connect Pro with Microsoft® Live Communication Server 2005 and Microsoft® Office Communication Server to display their IM presence in Acrobat Connect Pro meeting rooms.

Acrobat Connect Pro 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 (MSDE) included in the Acrobat Connect Pro Server 7 installer, or you can install a full version of Microsoft SQL Server. (The embedded database engine is included in the Acrobat Connect Pro installation; Microsoft SQL Server is not.)

Data flow

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



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 Acrobat Connect streaming traffic.
4a	Flash Media Server responds and opens a tunneled connection for Acrobat 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 RTMP:443.
D	Flash Media Server responds and opens a secure, persistent connection for Acrobat Connect Pro streaming traffic.

Installation workflow

The following steps help you design, install, and configure a Acrobat Connect Pro 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 10.

2. Install Acrobat Connect Pro on a single server.

For more information, see [“Install Acrobat Connect Pro Server 7”](#) on page 13. If you chose the embedded database engine in step 1, install it too. The embedded database engine is part of the Acrobat Connect Pro installer.

3. If you chose SQL Server 2005 Standard Edition in step 1, install it.

For more information, see the SQL Server documentation.

4. Deploy Acrobat Connect Pro.

For more information, see [“Deploying Acrobat Connect Pro Server 7”](#) on page 22.

5. Verify that Acrobat Connect Pro is installed correctly.

For more information, see [“Verify your installation”](#) on page 16.

6. (Optional) Integrate Acrobat Connect Pro with your infrastructure.

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

Integrate with an LDAP Directory Integrate Acrobat Connect Pro 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 28.

Configure a secure socket layer Conduct all Acrobat Connect Pro communication securely. See [SSL \(secure sockets layer\)](#).

Store content on NAS/SAN devices Use network devices to share content storage duties. See [“Configuring shared storage”](#) on page 35.

Integrate with Live Communication Server and Office Communication 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 39.

Configure a public key infrastructure If you've integrated Acrobat Connect Pro with an LDAP directory server, add a security layer by requiring client certificates. See "[PKI \(public key infrastructure\)](#)" on page 63.

Host Acrobat Connect Add-in Users can download Acrobat 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 Acrobat Connect Add-in](#)" on page 47.

7. (Optional) Choose whether to install Acrobat Connect Pro Server 7 in a cluster.

For more information, see "[Choosing to deploy Acrobat Connect Pro in a cluster](#)" on page 9 and "[Deploy a cluster of Acrobat Connect Pro servers](#)" on page 22.

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

For more information, see "[Choosing to deploy Acrobat Connect Pro Edge Server](#)" on page 11 and "[Deploy Acrobat Connect Pro Edge Server](#)" on page 26.

Choosing to deploy Acrobat Connect Pro in a cluster

It is possible to install all Acrobat Connect Pro Server 7 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 a Acrobat Connect Pro Server 7 cluster, you install an identical copy of Acrobat Connect Pro Server 7 on each server in the cluster.

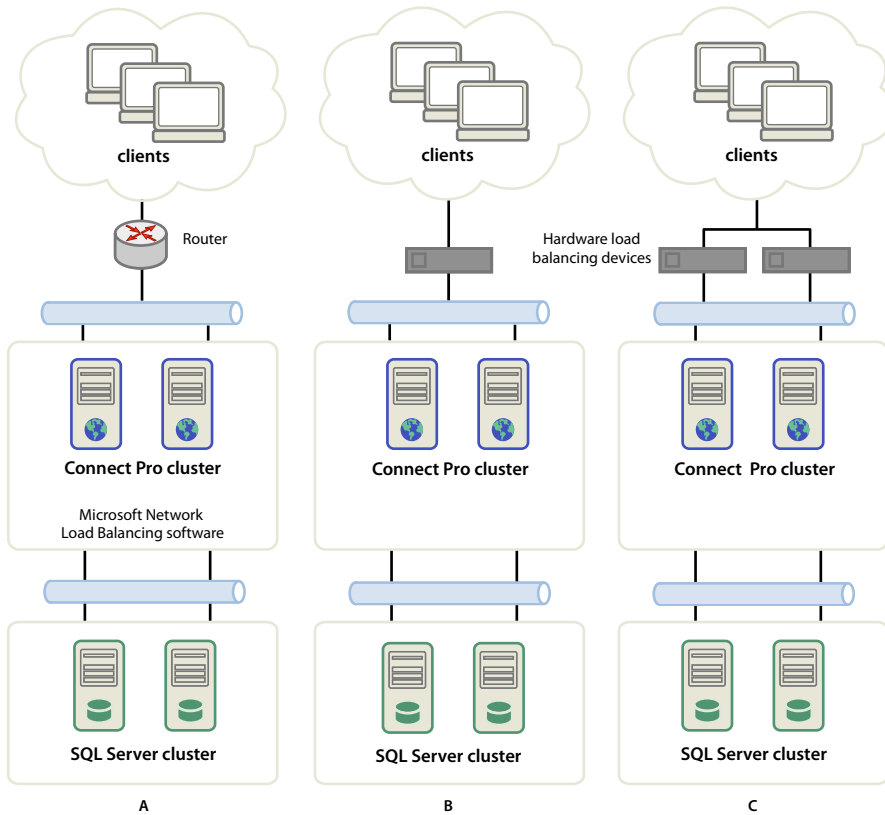
Note: When you install Acrobat Connect Pro Server 7 in a cluster, you must use SQL Server 2005 Standard Edition and install it on a separate computer.

All computers in a cluster have copies of the same contents. If one computer in the cluster fails, another computer 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 Acrobat Connect Pro Server 7.

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 Acrobat Connect Pro Server 7. For example, you could use multiple hardware load balancing devices (such as BIG-IP by F5 Networks), a cluster of servers hosting Acrobat Connect Pro Server 7, 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

See also

[“Deploy a cluster of Acrobat Connect Pro servers”](#) on page 22

[“Configuring shared storage”](#) on page 35

Choosing a database

Acrobat Connect Pro Server 7 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 Acrobat Connect Pro Server 7. 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 Acrobat Connect Pro Server 7 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 Acrobat Connect Pro Server 7 installed.
- Acrobat Connect Pro Server 7 is deployed in a cluster.
- Acrobat Connect Pro Server 7 is installed on multiprocessor computers with Hyper-Threading.

See also

[“Supported server-database configurations”](#) on page 2

[“Install Acrobat Connect Pro Server 7”](#) on page 13

Choosing to deploy Acrobat Connect Pro Edge Server

When you deploy Acrobat Connect Edge Server on your network, clients connect to the edge server and the edge server connects to Acrobat Connect Pro (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.

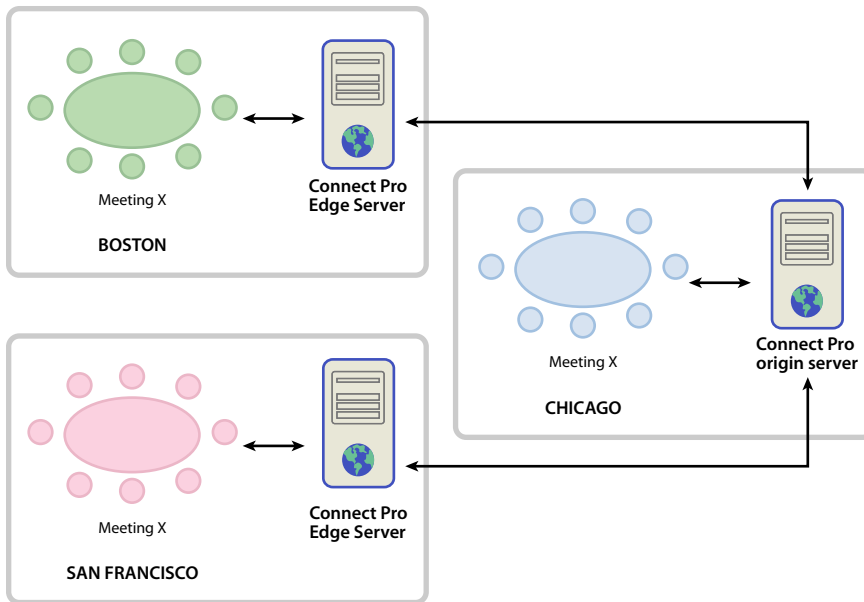
How edge servers work

Edge servers authenticate users and authorize their requests for web services such as Acrobat Connect Pro 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 Acrobat Connect Pro.

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:



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.

See also

- “[Install Acrobat Connect Pro Edge Server 7](#)” on page 18
- “[Deploying Acrobat Connect Pro Edge Server 7](#)” on page 25

Chapter 2: Installing Acrobat Connect Pro Server 7 and Acrobat Connect Pro Edge Server 7

To install Acrobat Connect Pro Server 7 and Acrobat Connect Pro Edge Server 7, run the installer and step through the Application Management Console wizard.

Install Acrobat Connect Pro Server 7

Run the installer

- 1 Close all applications.
- 2 Insert the installation DVD into the DVD-ROM drive. On the startup screen, click the Adobe Acrobat Connect Pro Server 7 Install button.

If the installer does not start automatically, double-click the setup.exe file in the installation root folder of the DVD.

- 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 to select the installation location:
 - Click Next to accept the default installation location (c:\breeze), or click Browse to select a different location, and then click Next.
 - If Acrobat Connect Pro is already installed on this computer, the Update Existing Connect Pro Install screen appears. Select the check box to confirm you've backed up your database and the Connect Pro root directory. Click Next.
- 7 On the Company Information screen enter your serial number and click Next.
- 8 Do one of the following:
 - If the embedded database engine screen appears, choose whether you want to install it. If you want to install it in the default location (c:\Program Files\Microsoft SQL Server), click Next. If you don't want to install it to the default location, click Browse to select a different location, and then click Next. If you don't want to install the embedded database engine (because you're planning to use Microsoft SQL Server), select Do not install the embedded database engine and click Next.
 - If the installer detects that the embedded database engine or Microsoft SQL Server is already installed on this computer, the embedded database engine is not installed. If the embedded database engine is already installed, the location cannot be changed. Click Next.

Note: Sometimes an old version of the embedded database is not removed properly and the installer detects it. Follow the instructions in TechNote 18927 (www.adobe.com/go/tn_18927) and start the installation again.

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

- Click Next to accept the default name and location of the Start Menu shortcuts (Adobe Acrobat Connect Pro Server 7).
- Click Browse to select a different location, and then click Next.

10 In the Ready To Install dialog box, review the installation location and the name and location of the Start Menu. Click Back to review or change these settings, or click Install.

The Installing screen appears as the program installs.

11 If you chose to install the embedded database engine, the Installing the embedded database engine screen appears. Enter a password for the database user “sa” and click Next to install.

12 On the Initializing Connect Pro service screen, do one of the following and click Next:

- Select Do not start Connect Pro now...
- Select Start Connect Pro and open a browser and launch the Application Management Console Wizard to continue the configuration—recommended.

13 If you started Acrobat Connect Pro, a message reports that the service is starting.

Acrobat Connect Pro Server 7 runs as four Windows services: Adobe Connect Enterprise Service, Flash Media Server (FMS), Flash Media Administration Server, and Acrobat Connect Pro Presence Server. See “[Start and stop the servers](#)” on page 18.

14 Click Finish in the Installer.

If you chose Start Connect Pro, the Application Management Console wizard opens in a browser to guide you through configuration tasks.

Configuring Acrobat Connect Pro with the Application Management Console wizard

After installing Acrobat Connect Pro, the installer automatically starts the Application Management Console wizard to guide you as you configure the database settings and server settings, upload your license file, and create an administrator.

Note: If another application is running on port 80, the Application Management Console will not open. Stop the application running on port 80 and reopen the Application Management Console.

You can access the Application Management Console by choosing Start > Programs > Adobe Acrobat Connect Pro Server 7 > Configure Connect Pro Server 7 or by using the following URL: <http://localhost:8510/console>.

1. Read the Welcome screen.

The Welcome screen provides an overview of the wizard.

2. Enter database settings.

Set values for the parameters listed below. Click Next to connect to the database and review your settings.

Database Host The host name of the computer on which the database is installed. If you installed the embedded database, the value is localhost.

Database Name The name of the database. The default value is breeze.

Database Port The port the database uses to communicate with Acrobat Connect Pro. The default value is 1433. (If you're using the embedded database engine, change the value to 1434.)

Database User The name of the database user. If you installed the embedded database, the default value is sa.

Database User's Password The password for the database user. If you installed the embedded database, this is the value you set in the installer.

3. Enter server settings.

Account Name A name that identifies the Acrobat Connect Pro account, such as "Acrobat Connect Pro 7 account".

Connect Pro Host A fully qualified domain name (FQDN) clients use to connect to Acrobat Connect Pro. For example, if the URL of the account is <http://connect.example.com>, the Connect Pro Host value would be connect.example.com.

HTTP Port The port Acrobat Connect Pro uses to communicate with HTTP. The default value is 80. If you enter a value other than 80, clients must add the port number to the host name in the URL when they access the Acrobat Connect Pro account.

Host Mappings Name is the host name of the computer hosting Acrobat Connect Pro. External Name is the FQDN clients use to connect to Acrobat Connect Pro.

Note: Do not append a port to the FQDN in the External Name box.

SMTP Host The host name of the computer hosting the SMTP mail server.

System E-mail The e-mail address from which administrative messages are addressed.

Support E-mail The support e-mail address for Acrobat Connect Pro users.

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 Acrobat Connect Pro without exposing an internal e-mail address.

Shared Storage A volume and directory on an external server where content will be stored, for example, `\\volume\directory`. If you want to store content on multiple volumes, separate them with semi-colons (;). Before configuring this feature, see "[Configuring shared storage](#)" on page 35.

Content Cache Size An integer between 1 and 100 specifying the percent of free disk space to use to store content on Acrobat Connect Pro. The cache can grow beyond the percent you specify, so it's a good idea to keep the value between 15 and 50. If you leave the box blank or enter 0, no cache is used and content is mirrored on Acrobat Connect Pro and any external volumes. Before configuring this feature, see "[Configuring shared storage](#)" on page 35.

4. Upload your license file.

Acrobat Connect Pro is not enabled until you download a license file from Adobe and install it on the computer hosting Acrobat Connect Pro. This screen of the wizard provides a download link and a form that lets you select the downloaded license file to copy it to your Acrobat Connect Pro installation.

5. Create an account administrator.

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

6. Continue using Acrobat Connect Pro.

This is the final screen of the Application Management Console wizard. From here, you can log in to Enterprise Manager (the web application that lets you manage your account, create meetings, events, and so on, and manage content on the computer hosting Acrobat Connect Pro), return to the Application Management Console (to change or review settings), or consult the documentation to learn more about Acrobat Connect Pro.

Verify your installation

Verify database connectivity

If you can log in to Connect Pro Central (a web application within Acrobat Connect Pro), the database and Acrobat Connect Pro can function together.

- 1 Go to the following URL: `http://[hostname]`.

Note: In this URL, `[hostname]` is the value you set for Connect Pro Host in the Application Management Console.

- 2 Enter the login ID and password that you set in the Application Management Console.

If you can log in successfully, the Connect Pro Central home tab appears.

Verify that you can send e-mail notifications

If you did not choose to enter a value in the SMTP Host field on the Application Settings > Server Settings screen in the Application Management Console, Acrobat Connect Pro will not send out e-mail notifications and you can skip this section.

- 1 Click the Administration tab on the Connect Pro 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 his e-mail notification.

If the user received the notification, Acrobat Connect Pro 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 you configured Acrobat Connect Pro with a valid SMTP host, and make sure the SMTP service works outside Acrobat Connect Pro.
 - d Contact Adobe Support at www.adobe.com/go/connect_licensed_programs_en.

Verify that you can use Adobe Presenter

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

Before you can send a PowerPoint presentation to Acrobat Connect Pro, you must install Adobe Presenter on a computer on which PowerPoint is already installed.

- 1 Insert the Adobe Acrobat Connect Pro Server 7 CD.
- 2 Click Install Adobe Presenter 7 and follow the prompts.
- 3 If you do not have a PowerPoint presentation that you can send to Acrobat Connect Pro for compilation into a Flash presentation, create and save a presentation of one or two slides.
- 4 Open the Connect Pro Publish wizard by selecting Publish from the Adobe Presenter menu in PowerPoint.
- 5 Select Connect Pro and enter the information for your server.
- 6 Log in with your e-mail address and password, and follow the steps in the Publish wizard. Make sure you are enrolled in the Authors group (Administration > Users and Groups in Connect Pro Central).

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

- 7 When the compilation is complete, go to the Content tab in Connect Pro Central and search for your presentation.
- 8 Open your presentation to view it.

Verify that you can use Training

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

- ❖ Go to the Training tab in Connect Pro 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

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

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

- 1 Log in to Connect Pro 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 Acrobat Connect Add-in window appears, follow the instructions to install it.

If the meeting room opens, Acrobat Connect Pro Meeting is functional.

Verify that you can use Events

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

- 1 Log in to Connect Pro Central as a user who is enrolled in the Events Managers group or the Administrators group.
- 2 Go to the Event Management tab in Connect Pro Central.

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

Install Acrobat Connect Pro Edge Server 7

Run the installer

- 1 Close all other applications.
- 2 Insert the installation DVD into the DVD-ROM drive. On the startup screen, click the Adobe Acrobat Connect Pro Edge Server 7 Install button.

If the installer does not start automatically, double-click the edgesetup.exe file in the installation root folder of the DVD.

- 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:\breeze), or click Browse to select a different location, and then click Next.
 - If Adobe Acrobat Connect Pro Edge Server is already installed on this computer, the Update Existing Adobe Acrobat Connect Pro Edge Server Install screen appears. Click Next.
- 7 On the Select Start Menu Folder screen, click Next to accept the default location of the Start Menu shortcuts, or click Browse to select a different location, and then click Next.
- 8 In the Ready To Install dialog box, review the location where Adobe Acrobat Connect Pro 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 Acrobat Connect Pro Edge Server 7 installation.

See also

[“Deploying Acrobat Connect Pro Edge Server 7”](#) on page 25

Start and stop the servers

Start and stop Acrobat Connect Pro Server 7

You can start or stop Acrobat Connect Pro from the Start menu, the Services window, or the command line.

Stop Acrobat Connect Pro from the Start menu

- 1 Choose Start > Programs > Adobe Acrobat Connect Pro Server 7 > Stop Connect Pro Central Application Server.
- 2 Choose Start > Programs > Adobe Acrobat Connect Pro Server 7 > Stop Connect Pro Meeting Server.

Start Acrobat Connect Pro from the Start menu

- 1 Choose Start > Programs > Adobe Acrobat Connect Pro Server 7 > Start Connect Pro Meeting Server.
- 2 Choose Start > Programs > Adobe Acrobat Connect Pro Server 7 > Start Connect Pro Central Application Server.

Stop Acrobat Connect Pro from the Services window

- 1 Choose Start > Control Panel > Administrative Tools > Services to open the Services window.
- 2 Stop the Adobe Connect Enterprise Service service.
- 3 Stop the Flash Media Server (FMS) service.
- 4 Stop the Flash Media Administration Server service.

Start Acrobat Connect Pro 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 Enterprise Service service.

Stop Acrobat Connect Pro 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 Acrobat Connect Pro:

```
net stop BreezeApp
```

- 3 Enter the following to stop Flash Media Server:

```
net stop FMS
```

- 4 Enter the following to stop Flash Media Server Administration Server:

```
net stop FMSAdmin
```

Start Acrobat Connect Pro 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 Server:

```
net start FMS
```

- 3 Enter the following to start Flash Media Server Administrator Server:

```
net start FMSAdmin
```

- 4 Enter the following to start Acrobat Connect Pro:

```
net start BreezeApp
```

Start and stop Connect Pro Presence Service

You can start and stop Connect Pro Presence Service from the Start menu or the Services window. Start Connect Pro Presence Service only if your Acrobat Connect Pro system is integrated with Microsoft Live Communications Server or Office Communications Server.

See also

[“Integrating with Microsoft Live Communications Server 2005 and Microsoft Office Communications Server 2007”](#) on page 39

Stop the presence service from the Start menu

- ❖ Choose Start > Programs > Adobe Acrobat Connect Pro Server 7 > Stop Connect Pro Presence Service.

Start the presence service from the Start menu

- ❖ Choose Start > Programs > Adobe Acrobat Connect Pro Server 7 > Start Connect Pro 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 Acrobat Connect Pro Presence Service.
- 3 Choose Start, Stop, or Restart the service.

Start and stop Acrobat Connect Pro Edge Server 7

You can start or stop Acrobat Connect Pro Edge Server 7 from the Start menu, the Services window, and from the command line.

Stop Acrobat Connect Pro Edge Server 7 from the Start menu

- ❖ Choose Start > Programs > Adobe Acrobat Connect Pro Edge Server 7 > Stop Connect Pro Edge Server.

Start Acrobat Connect Pro Edge Server 7 from the Start menu

- ❖ Choose Start > Programs > Adobe Acrobat Connect Edge Server 7 > Start Connect Pro Edge Server.

Stop Acrobat Connect Pro Edge Server 7 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 Acrobat Connect Pro 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 Acrobat Connect Pro 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 Acrobat Connect Pro 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
```

Uninstall the servers

Uninstall Acrobat Connect Pro Server 7

- 1 Select Start > Programs > Adobe Acrobat Connect Pro Server 7 > Uninstall Connect Pro Server 7.
- 2 Delete the root Acrobat Connect Pro folder. By default, the location is c:\breeze.

When you uninstall Acrobat Connect Pro, the custom.ini and config.ini files and the content files are not deleted. Deleting the root folder deletes these files.

- 3 (Optional) If the embedded database engine was installed, you must delete its registry entry. Choose Start > Run and enter **regedit** in the Open box.

In the Registry Editor, delete the key HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft SQL Server. If there is an HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSSQLServer key, delete it as well.

Uninstall Acrobat Connect Pro Edge Server 7

- 1 Select Start > Settings > Control Panel > Add or Remove Programs > Adobe Acrobat Connect Pro Edge Server 7 > Remove.
- 2 Delete the root Acrobat Connect Pro folder. By default, the location is c:\breeze.

Chapter 3: Deploying and configuring Acrobat Connect Pro Server 7 and Acrobat Connect Pro Edge Server 7

After you install Adobe Acrobat Connect Pro Server 7 or Adobe Acrobat Connect Pro Edge Server 7 and complete the first phase of configuration with the Application Management Console, configure any of these optional features and deploy the server.

Deploying Acrobat Connect Pro Server 7

Deploy a single Acrobat Connect Pro server

- 1 On your DNS server, define a fully qualified domain name (FQDN) for Acrobat Connect Pro (such as `connect.mycompany.com`). Map the domain name to the static IP address of the computer hosting Acrobat Connect Pro.
- 2 If you want Acrobat Connect Pro to be available outside your network, configure the following ports in a firewall:
 - 80** The default port for the Acrobat Connect Pro 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 Acrobat Connect Pro 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.

For help deploying Acrobat Connect Pro, contact Adobe Support at www.adobe.com/go/connect_licensed_programs_en.

Deploy a cluster of Acrobat Connect Pro servers

Before you deploy a cluster, you need the following:

- A license that supports the number of nodes in your cluster. For more information, contact your Adobe representative.
- Each computer in the cluster must have a static IP address and a DNS entry.
- An email server.
- A SQL server installation on a dedicated computer with a static IP address. If you install Acrobat Connect Pro in a cluster, you cannot use the embedded database engine. Each server hosting Acrobat Connect Pro connects to the database, but licensing restrictions do not allow more than one server to connect to the embedded database engine.
- A hardware or software load balancing solution. Load balancing hardware requires a separate computer with a static IP address and DNS entry. Software can be installed on one of the cluster nodes.

- One or more shared storage volumes. This configuration is not required, but it is recommended.

Before you deploy Acrobat Connect Pro in a cluster, perform a successful installation on a single computer. Configure any additional features (for example, SSL, a directory service integration, single sign-on, shared content storage, and so on) and verify that they work as expected on a single server.

1 Install and configure Acrobat Connect Pro on a dedicated server.

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

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

- a Open the Services control panel.
- b Double-click Adobe Connect Enterprise 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 Acrobat Connect Pro:

- 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 Enterprise Service and click Start the service.
- 4** Choose Start > Programs > Adobe Acrobat Connect Pro Server 7 > Configure Connect Pro Server 7 to open the Application Management Console wizard. Click Next.
- 5** On the Database Settings screen, enter the information for the SQL Server database and click Next.

If Acrobat Connect Pro 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 Connect Pro 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 Acrobat Connect Pro 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 through 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.example.com>.

For help deploying a cluster, contact Adobe Support at www.adobe.com/go/connect_licensed_programs_en.

See also

“[Install Acrobat Connect Pro Server 7](#)” on page 13

“[Configuring shared storage](#)” on page 35

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 Acrobat Connect Pro on both computers.

- a Select Start > Programs > Adobe Acrobat Connect Pro Server 7 > Start Connect Pro Meeting Server.
- b Select Start > Programs > Adobe Acrobat Connect Pro Server 7 > Start Connect Pro Central Application Server

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

[http://\[hostname\]](http://[hostname])

For *hostname*, use the Connect Pro 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 Acrobat Connect Pro on Computer2.

- a Select Start > Programs > Adobe Acrobat Connect Pro Server 7 > Stop Connect Pro Central Application Server
- b Select Start > Programs > Adobe Acrobat Connect Pro Server 7 > Stop Connect Pro Meeting Server.

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

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

If the load balancer is working, you should still be able to send successful requests to Connect Pro 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 Acrobat Connect Pro on Computer1.
 - a Select Start > Programs > Adobe Acrobat Connect Pro Server 7 > Start Connect Pro Meeting Server.
 - b Select Start > Programs > Adobe Acrobat Connect Pro Server 7 > Start Connect Pro Central Application Server
- 2 Stop Acrobat Connect Pro on Computer2.
 - a Select Start > Programs > Adobe Acrobat Connect Pro Server 7 > Stop Connect Pro Central Application Server
 - b Select Start > Programs > Adobe Acrobat Connect Pro Server 7 > Stop Connect Pro Meeting Server.
- 3 Log in to Connect Pro Central from the following URL:

`http://[hostname]`

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

- 4 Upload a JPEG image or other content to Acrobat Connect Pro 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 Connect Pro 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 Acrobat Connect Pro 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 Acrobat Connect Pro Edge Server 7

Acrobat Connect Pro 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 Acrobat Connect Pro. 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 Acrobat Connect Pro Edge Server.

Install Acrobat Connect Pro Edge Server on each computer in each zone. For example, if you have a cluster of edge servers in a zone, install Acrobat Connect Pro Edge Server on each computer in the cluster. See “[Install Acrobat Connect Pro Edge Server 7](#)” on page 18.

3. Modify the DNS server for each zone.

Map the FQDN of the origin Acrobat Connect Pro server to the static IP address of Acrobat Connect Pro Edge Server in each zone. See “[Deploying Acrobat Connect Pro Edge Server 7](#)” on page 25.

4. Configure the edge server.

You must add configuration parameters to the custom.ini file on each Acrobat Connect Pro Edge Server. See “[Deploying Acrobat Connect Pro Edge Server 7](#)” on page 25.

5. Configure the origin server.

You must add configuration parameters to the custom.ini file on each Acrobat Connect Pro server. Also, you must set the External Name of the edge server in the Application Management Console on the origin server. See “[Deploying Acrobat Connect Pro Edge Server 7](#)” on page 25.

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 Acrobat Connect Pro Edge Server

Before you deploy edge servers, you should have Acrobat Connect Pro 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 Acrobat Connect Pro 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.example.com`.

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

3 On Acrobat Connect Pro Edge Server, open the `[root_install_dir]\edgeserver\conf\config.ini` file in a text editor 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 Acrobat Connect Pro 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 Acrobat Connect Pro 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 Acrobat Connect Pro is installed, for example,

`FCS.HTTPCACHE_BREEZE_SERVER_NORMAL_PORT=connect.yourcompany.com:80`. Acrobat Connect Pro Edge Server connects to the Acrobat Connect Pro 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 Acrobat Connect Pro 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 Acrobat Connect Pro Server 7 > Configure Connect Pro Server 7). 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/go/connect_licensed_programs_en.

See also

“Choosing to deploy Acrobat Connect Pro Edge Server” on page 11

Integrating with a directory service

Directory service integration overview

You can integrate Acrobat Connect Pro 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 Acrobat Connect Pro through manual or scheduled synchronizations with the directory of your organization.

To integrate with Acrobat Connect Pro, 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.

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

Any LDAP-compliant directory service may integrate with Acrobat Connect Pro. For a list of certified LDAP directories, see www.adobe.com/go/connect_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 Acrobat Connect Pro, 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 Acrobat Connect Pro rather than importing them from an LDAP directory are called *internal* users and groups. Users and groups imported into the Acrobat Connect Pro 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 Acrobat Connect Pro 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 Acrobat Connect Pro Server 7 > Configure Connect Pro Server 7.

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, Acrobat Connect Pro 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 <code>ldap://[servername:portnumber]</code> . If your organization uses a secure LDAP server, use <code>ldaps://</code> . If you do not specify a port, Acrobat Connect Pro uses the standard LDAP port (389) or LDAPS port (636). LDAPS requires SSL certificates. If you configure Acrobat Connect Pro 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 Acrobat Connect Pro (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://ldapservers.mycompany.com
UserName:MYCOMPANY\jdoe
Password:password123
Query timeout:120
Authentication mechanism:Simple
Query page size:100
```

3. Map Acrobat Connect Pro 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 a Acrobat Connect Pro 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 28.

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 Acrobat Connect Pro and LDAP directory group profiles.

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

Note: Acrobat Connect Pro 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 a Acrobat Connect Pro 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 28.

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 Acrobat Connect Pro users against the directory service of your organization, select “Enable LDAP Directory authentication”. If you do not select this option, Acrobat Connect Pro uses native authentication (user credentials stored in the Acrobat Connect Pro database).

If you check “Enable Connect Pro fall-back on unsuccessful LDAP Directory authentication”, Acrobat Connect Pro 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 Acrobat Connect Pro database.

Check “Create Connect Pro user account upon successful LDAP Directory authentication” to provision first-time users on the Acrobat Connect Pro server if LDAP authentication is successful. If any user in your directory service is allowed to use Acrobat Connect Pro, leave this option checked and select “Internal” as user account type. For more information, see “[Internal and external users and groups](#)” on page 29.

Check “Enable group enrollment on first login only” to create a login ID in Acrobat Connect Pro and place users into specified groups when users log into Acrobat Connect Pro 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 34.

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 33.

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 Acrobat Connect Pro 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 34.

Managing passwords

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

When Acrobat Connect Pro 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 Acrobat Connect Pro 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 Acrobat Connect Pro 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 Acrobat Connect Pro 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 Acrobat Connect Pro.

Scheduled synchronizations

Scheduled synchronizations are recommended because they ensure that Acrobat Connect Pro 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, Acrobat Connect Pro compares LDAP directory entries to Acrobat Connect Pro 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 <i>yyyyMMdd'T'HHmmss.SSS</i> .
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 Acrobat Connect Pro.	An abbreviated XML packet that describes the updated fields using a series of tag pairs in the format <code><fieldname>value</fieldname></code> (for example, <code><first-name>Joe</first-name></code>). 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: <code><add>ID list</add></code> <code><remove>ID list</remove></code> The ID list is a series of <code><id>principal ID</id></code> packets where <code>principal ID</code> 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 <code><add/></code> or <code><remove/></code> .
delete	The principal was deleted from Acrobat Connect Pro.	
up-to-date	The principal is an external principal in Acrobat Connect Pro and is already synchronized with the external directory. No changes were made.	A user or group created in Acrobat Connect Pro 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 Acrobat Connect Pro 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

Acrobat Connect Pro 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`.

Configuring shared storage

About shared storage

You can use the Application Management Console to configure Acrobat Connect Pro to use NAS and SAN devices to manage content storage. Content is any file published to Acrobat Connect Pro, 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 Acrobat Connect Pro 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 a Acrobat Connect Pro cluster and don't configure shared storage devices, the cluster works in full mirroring mode (content published to Acrobat Connect Pro is copied to all servers) and content is never automatically removed from any servers.*

Configure shared storage

If you're configuring shared storage for one Acrobat Connect Pro 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.

See also

["Supported content storage devices"](#) on page 3

["Deploy a cluster of Acrobat Connect Pro servers"](#) on page 22

Configure shared storage

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


1 Configure a shared volume on a external storage device.

If a shared volume has a username and password, all shared volumes must use the same username and password.

2 (Optional) If you are updating an existing Acrobat Connect Pro 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 Acrobat Connect Pro Server 7 > Stop Connect Pro Central Application Server and Stop Connect Pro 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. Acrobat Connect Pro 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 Acrobat Connect Pro (Start > Programs > Adobe Acrobat Connect Pro Server 7 > Start Connect Pro Meeting Server and Start Connect Pro Central Application Server).

3 On Acrobat Connect Pro, choose Start > Control Panel > Administrative Tools > Services to open the Services window, select Adobe Connect Enterprise 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 Acrobat Connect Pro (application server only).
 - a Choose Start > Programs > Adobe Acrobat Connect Pro Server 7 > Stop Connect Pro Central Application Server.
 - b Choose Start > Programs > Adobe Acrobat Connect Pro Server 7 > Start Connect Pro Central Application Server.
- 5 Open the Application Management Console (Start > Programs > Adobe Acrobat Connect Pro Server 7 > Configure Connect Pro Server 7).
- 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, \\storage).

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

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 Acrobat Connect Pro 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 Acrobat Connect Pro (application server only).
 - a Choose Start > Programs > Adobe Acrobat Connect Pro Server 7 > Stop Connect Pro Central Application Server.
 - b Choose Start > Programs > Adobe Acrobat Connect Pro Server 7 > Start Connect Pro Central Application Server.

Configure shared storage for additional servers in a cluster

- 1 Install Acrobat Connect Pro but do not start it. If Acrobat Connect Pro is installed and already running, stop it.
- 2 On Acrobat Connect Pro, choose Start > Control Panel > Administrative Tools > Services to open the Services window, select Adobe Connect Enterprise 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 Acrobat Connect Pro.
 - a Choose Start > Programs > Adobe Acrobat Connect Pro Server 7 > Start Adobe Connect Meeting Server.
 - b Choose Start > Programs > Adobe Acrobat Connect Pro Server 7 > Start Connect Pro Central Application Server.
- 4 (Optional) If you are installing Acrobat Connect Pro for the first time, follow the steps in “[Deploy a cluster of Acrobat Connect Pro servers](#)” on page 22.
- 5 Click Save and close the Application Management Console.

Configuring account notification settings

Set the time that monthly reports are sent

Acrobat Connect Pro 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 Acrobat Connect Pro to send the email at a different time, you can add parameters to the custom.ini file and set the desired values.

For more information about configuring account notifications in Connect Pro Central, see the “Administering Acrobat Connect Pro” chapter in *Using Adobe Acrobat Connect Pro 7* available online at www.adobe.com/go/connect_documentation_en.

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 Connect Pro 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 Connect Pro 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 Acrobat Connect Pro:

- a Choose Start > Programs > Adobe Acrobat Connect Pro Server 7 > Stop Connect Pro Central Application Server.
- b Choose Start > Programs > Adobe Acrobat Connect Pro Server 7 > Start Connect Pro Central Application Server.

Set capacity thresholds

Acrobat Connect Pro account administrators can set capacity thresholds in Connect Pro 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 Connect Pro Central.

For more information about configuring account notifications in Connect Pro Central, see the “Administering Acrobat Connect Pro” chapter in *Using Adobe Acrobat Connect Pro 7* available online at www.adobe.com/go/connect_documentation_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 Acrobat Connect Pro:

- a Choose Start > Programs > Adobe Acrobat Connect Pro Server 7 > Stop Connect Pro Central Application Server.
- b Choose Start > Programs > Adobe Acrobat Connect Pro Server 7 > Start Connect Pro Central Application Server.

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

Workflow for configuring presence integration

Integrate Acrobat Connect Pro 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.

For information about the Invitees List, see *Using Adobe Acrobat Connect Pro 7* available online at www.adobe.com/go/connect_documentation_en.

1. Acrobat Connect Pro Server 7 and a communications server must be installed.

Install and verify the installation of Acrobat Connect Pro Server 7 and a communications server. Acrobat Connect Pro Server 7 supports integration with Microsoft Live Communications Server 2005 and Microsoft Office Communications Server 2007. See “[Install Acrobat Connect Pro Server 7](#)” on page 13 and the documentation for the communications server.

2. Configure the communications server.

Configure the communications server to exchange data with Acrobat Connect Pro Server 7. See “[Configure Live Communications Server 2005 or Office Communications Server 2007](#)” on page 40.

3. Stop Connect Pro Presence Service.

Acrobat Connect Pro Server 7 includes the Connect Pro Presence Service. Stop the service before you configure Acrobat Connect Pro. See “[Start and stop Connect Pro Presence Service](#)” on page 44.

4. Configure Connect Pro Presence Service.

Configure Acrobat Connect Pro so that it can exchange data with the communications server. The presence server is installed by default to C:\breeze\presserv. See “[Configure Connect Pro Presence Service](#)” on page 42.

5. Start Connect Pro Presence Service.

See “[Start and stop Connect Pro Presence Service](#)” on page 44.

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

Log on to Connect Pro 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 or Office Communications Server 2007

1 Choose Start > Programs > Administrative Tools > Live Communications Server 2005 or Office Communications Server 2007 to open the Configuration Console.

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

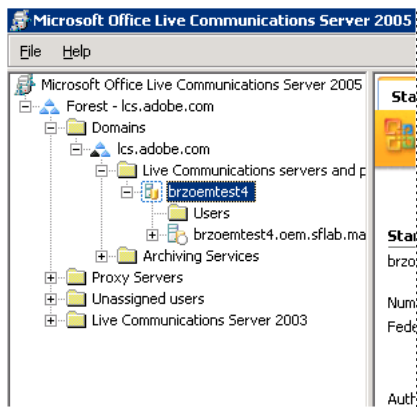
- a Select the Federation tab.
- b Select the Enable federation and public IM connectivity check box.
- c Enter the Acrobat Connect Pro network address.
- d Enter port 5072.

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

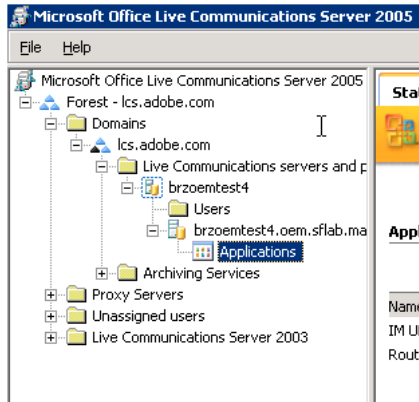
e Click OK.

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.



- 5 In the server Properties dialog, do the following:
 - a Select the Host Authorization tab. Add the IP address of Acrobat Connect Pro. 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 Acrobat Connect Pro 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 communications server clients

The Acrobat Connect Pro 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 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 Connect Pro Presence Service

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

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

- 1 Open the `\breeze\presserv\conf\lcs gw.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
<code><host></code>	SIP realm of LCS or OCS users
<code><bind></code>	IP address of LCS or OCS server (or load balancer)
<code><area></code>	SIP realm of LCS or OCS users

Configure the custom.ini file

- 1 Open `\breeze\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 Connect Pro Presence Service (for example, localhost).
OPN_PORT	The internal port used between Acrobat Connect Pro and Connect Pro Presence Service. The default value (10020) must match the value in the <code>\breeze\presserv\conf.router.xml</code> file. Do not modify this value.

Parameter	Value
OPN_PASSWORD	The internal token used between Acrobat Connect Pro and Connect Pro Presence Service. The default value (secret) must match the value in the \breeze\presserv\conf.router.xml file. Do not modify this value.
OPN_DOMAIN	The domain name of the Acrobat Connect Pro server (application server). Connect Pro 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 Connect Pro Presence Service

- 1 Open the \breeze\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 Acrobat Connect Pro. 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 Acrobat Connect Pro.

- 3 Restart Connect Pro Central Application Server.

Configure Connect Pro Presence Service in a cluster

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

- 1 Open *root_install\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 FQDN of the computer running Connect Pro 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 Acrobat Connect Pro and Connect Pro Presence Service. The default value (10020) must match the value in the \breeze\presserv\conf.router.xml file. Do not modify this value.
OPN_PASSWORD	The internal token used between Acrobat Connect Pro and Connect Pro Presence Service. The default value (secret) must match the value in the \breeze\presserv\conf.router.xml file. Do not modify this value.
OPN_DOMAIN	The domain Connect Pro Presence Service uses to identify a Connect Pro 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 Connect Pro Central Application Server.

Start and stop Connect Pro Presence Service

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

Start and stop Connect Pro Presence Service from the Start menu

❖ Do one of the following:

- Choose Start > Programs > Adobe Acrobat Connect Pro Server 7 > Start Connect Pro Presence Service.
- Choose Start > Programs > Adobe Acrobat Connect Pro Server 7 > Stop Connect Pro Presence Service.

Start and stop Connect Pro Presence Service from the Services window

- 1 Choose Start > Control Panel > Administrative Tools > Services to open the Services window.
- 2 Select Acrobat Connect Pro 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 authenticates users for all applications to which they have access permission on a network. Single sign-on uses a proxy server to authenticate users so they don't need to log in to Acrobat Connect Pro.

Acrobat Connect Pro supports the following single sign-on mechanism:

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

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, Acrobat Connect Pro login requests are routed to an agent positioned between the client and Acrobat Connect Pro. 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 Acrobat Connect Pro. On Acrobat Connect Pro, you must uncomment a Java filter and configure a parameter in the custom.ini file that specifies the name of the additional HTTP header.

See also

[“Start and stop Acrobat Connect Pro Server 7”](#) on page 18

Configure HTTP header authentication on Acrobat Connect Pro

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

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

a Uncomment the `HeaderAuthenticationFilter` Java filter mapping.

```
<filter-mapping>
  <filter-name>HeaderAuthenticationFilter</filter-name>
  <url-pattern>/*</url-pattern>
</filter-mapping>
```

b Comment out the `NtlmAuthenticationFilter` Java filter mapping.

```
<!--
<filter-mapping>
  <filter-name>NtlmAuthenticationFilter</filter-name>
  <url-pattern>/*</url-pattern>
</filter-mapping>
-->
```

2 Stop Acrobat Connect Pro:

a Choose Start > Programs > Adobe Acrobat Connect Pro Server 7 > Stop Connect Pro Central Application Server.

b Choose Start > Programs > Adobe Acrobat Connect Pro Server 7 > 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 Acrobat Connect Pro. The name of the header must be `header_field_name`.

- 4 Save the custom.ini file and restart Acrobat Connect Pro:
 - a Choose Start > Programs > Adobe Acrobat Connect Pro Server 7 > Start Adobe Connect Meeting Server.
 - b Choose Start > Programs > Adobe Acrobat Connect Pro Server 7 > Start Connect Pro 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 Acrobat Connect Pro.

- 1 Set the value of the `header_field_name` header field to a Acrobat Connect Pro user login.
- 2 Send an HTTP request to Acrobat Connect Pro at the following URL:

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

The Java filter on Acrobat Connect Pro 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 Acrobat Connect Pro response for the string "OK" to indicate a successful authentication.
- 4 Parse the Acrobat Connect Pro response for the `BREEZESESSION` cookie.
- 5 Redirect the user to the requested URL on Acrobat Connect Pro, 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 Acrobat Connect Pro 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 Acrobat Connect Pro.
- 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 Acrobat Connect Pro:

- a Choose Start > Programs > Adobe Acrobat Connect Pro Server 7 > Stop Connect Pro Central Application Server.
- b Choose Start > Programs > Adobe Acrobat Connect Pro Server 7 > Stop Adobe Connect Meeting Server.
- 4 On the computer hosting Acrobat Connect Pro, add the following lines of code to the custom.ini file (located in the root installation directory, c:\breeze, 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 Acrobat Connect Pro:

- a Choose Start > Programs > Adobe Acrobat Connect Pro Server 7 > Start Adobe Connect Meeting Server.
- b Choose Start > Programs > Adobe Acrobat Connect Pro Server 7 > Start Connect Pro Central Application Server.
- 6 Open the file *[root_install_dir]\appserv\conf\WEB-INF\web.xml* and do the following:

- a Uncomment the HeaderAuthenticationFilter Java filter mapping.

```
<filter-mapping>  
  <filter-name>HeaderAuthenticationFilter</filter-name>  
  <url-pattern>/*</url-pattern>  
</filter-mapping>
```

- b Comment out the NtlmAuthenticationFilter Java filter mapping.

```
<!--  
<filter-mapping>  
  <filter-name>NtlmAuthenticationFilter</filter-name>  
  <url-pattern>/*</url-pattern>  
</filter-mapping>  
-->
```

Hosting Acrobat Connect Add-in

About Acrobat Connect Add-in

Adobe Acrobat Connect Add-in is a version of Flash Player that includes enhanced features for Acrobat Connect Pro meetings.

When Acrobat 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 Acrobat Connect Add-in on your own server.

Meeting guests, registered users, and presenters are asked to download Acrobat 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 are required to download Acrobat Connect Add-in if it isn't installed or if an old version is installed.

Customize Connect Add-in download location

You can host Acrobat 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 Acrobat Connect Pro language XML files on the server hosting Acrobat Connect Pro. The XML files are in the following two directories: `[root_install_dir]\appserv\web\common\intro\lang` and `[root_install_dir]\appserv\web\common\meeting\lang\`.

2 Enter a path to the executable files for each platform in the `addInLocation` section of each platform in each language file:

```
<m id="addInLocation" platform="Mac OS 10">/common/addin/AcrobatConnectAddin.z</m>  
<m id="addInLocation" platform="Windows">/common/addin/setup.exe</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 Acrobat Connect Pro language XML files on the server hosting Acrobat Connect Pro. The XML files are in the following two directories: `[root_install_dir]\appserv\web\common\intro\lang` and `[root_install_dir]\appserv\web\common\meeting\lang\`.

2 Enter the path to the download instruction page in the `addInLocation` section of each platform in each language file:

```
<m id="addInLocation" platform="Mac OS  
10">/common/help/#lang#/support/addindownload.htm</m>  
<m id="addInLocation" platform="Windows">/common/help/#lang#/support/addindownload.htm</m>
```

Note: The path includes a `#lang#` string that Acrobat Connect Pro 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 Acrobat Connect Pro (`/common/addin/setup.exe` and `/common/addin/AcrobatConnectAddin.z`). 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 Acrobat Connect Pro language XML files on the server hosting Acrobat Connect Pro. The XML files are in the following two directories: `[root_install_dir]\appserv\web\common\intro\lang` and `[root_install_dir]\appserv\web\common\meeting\lang\`.

2 In the `addInLocation` section of each platform in each language file, enter the path to the instruction page you created:

```
<m id="addInLocation" platform="Mac OS  
10">common/help/#lang#/support/addin_install_instructions.html</m>  
<m id="addInLocation"  
platform="Windows">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 Acrobat Connect Pro Server 7 protects your organization against loss of property and malicious acts. It is important to secure the infrastructure of your organization, Acrobat Connect Pro, and the database server used by Acrobat Connect Pro.

SSL (secure sockets layer)

About SSL support

Acrobat Connect Pro is made up of two servers: Adobe® Flash® Media Server and the Acrobat Connect Pro application server. Flash Media Server is called the *meeting server* because it serves meetings over a real-time RTMP connection to the client. The Acrobat Connect Pro application server handles the HTTP connection between the client and the Acrobat Connect Pro application logic.

Note: In the Start menu, the meeting server is called “Connect Pro Meeting Server” and the application server is called “Connect Pro Central Application Server”. In the Services window, the meeting server is called “Flash Media Server (FMS)” and the application server is called “Adobe Connect Enterprise Service”.

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

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

Purchase an SSL accelerator separately. Adobe has verified that Acrobat Connect Pro works with the following SSL hardware accelerators: F5 Big-IP 1000, Cisco Catalyst 6590 Switch, and Radware T100.

Software-based solution Use the native support for SSL in Acrobat Connect Pro.

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

Acrobat Connect Pro 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 help configuring SSL, contact Adobe Support at www.adobe.com/go/connect_licensed_programs_en.

Working with certificates

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

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

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

Obtain certificates

- ❖ Contact a Certificate Authority—a trusted third party who verifies the identity of the applicant. (Self-signed certificates do not work with Acrobat Connect Pro.)

The Certificate Authority asks you to generate an SSL Certificate Signing Request (CSR) file. Send the CSR to the Certificate Authority and they convert it into an SSL certificate. It contains information about your organization and the FQDN (fully qualified domain name) associated with the SSL certificate. Contact the Certificate Authority for instructions about generating a CSR.

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

Install certificates

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

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

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

Configure software-based SSL

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

Configure the DNS server

- ❖ Create DNS entries that define an FQDN for each secured connection.

The FQDN for the application server is the URL end users use to connect to Acrobat Connect Pro. Enter this FQDN for the Connect Pro Host value on the Server Settings page in the Application Management Console. For example, a good value is *connect.yourcompany.com*

End users do not see the FQDN for the meeting server. However, you must have a FQDN for the meeting server if you want to conduct meetings over a secure connection. Enter this FQDN in the External Name box on the Server Settings page in the Application Management Console. For example, a good value is *fms.yourcompany.com*.

Note: You can use one SSL certificate for all the application servers in a cluster, but you must have a unique SSL certificate for each meeting server. If you want to secure both the HTTP and RTMP connections on one server, you need two FQDNs and two certificates.

Secure the meeting and application servers

- 1 Open the Adaptor.xml file located at *[root_install_dir]\comserv\win32\conf_defaultRoot_* and save a backup copy to another location.
- 2 Insert the following code in the original Adaptor.xml file inside the `<Adaptor></Adaptor>` tags (replace the code in italic with your own values):

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

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

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

4 Replace the code in step 3 with the following:

```
<HostPort name="meetingserver" ct1_channel=":19350">meetingServerIP:-443</HostPort>
<HostPort name="applicationserver" ct1_channel=":19351">appServerIP:-443</HostPort>
```

5 Save the Adaptor.xml file.

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

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

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

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

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

Note: The custom.ini file is case sensitive—use capital letters for parameter names and lowercase letters for values.

9 Save the custom.ini file.

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

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

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

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

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

13 Save the VHost.xml file.

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

15 Restart Adobe Connect Pro Server 7:

- a Choose Start > Programs > Adobe Acrobat Connect Pro Server 7 > Stop Connect Pro Central Application Server.
- b Choose Start > Programs > Adobe Acrobat Connect Pro Server 7 > Stop Connect Pro Meeting Server.
- c Choose Start > Programs > Adobe Acrobat Connect Pro Server 7 > Start Connect Pro Meeting Server.
- d Choose Start > Programs > Adobe Acrobat Connect Pro Server 7 > Start Connect Pro Central Application Server.

16 Open the Application Management Console (<http://localhost:8510/console> or Start > Programs > Adobe Acrobat Connect Pro Server 7 > Configure Connect Pro Server 7).

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

- a Enter the FQDN for your Acrobat Connect Pro account in the Connect Pro Host box. This FQDN is the URL end users use to connect to Acrobat Connect Pro.
- b Enter the FQDN for the Acrobat Connect Pro meeting server in the Host Mappings External Name box. The server uses this value internally.

Secure the application server only

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

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

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

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

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

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

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

5 Save the Adaptor.xml file.

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

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

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

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

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

Note: The custom.ini file is case sensitive—use capital letters for parameter names and lowercase letters for values.

9 Save the custom.ini file.

10 Restart Acrobat Connect Pro Server 7:

- a Choose Start > Programs > Adobe Acrobat Connect Pro Server 7 > Stop Connect Pro Central Application Server.
- b Choose Start > Programs > Adobe Acrobat Connect Pro Server 7 > Stop Connect Pro Meeting Server.
- c Choose Start > Programs > Adobe Acrobat Connect Pro Server 7 > Start Connect Pro Meeting Server.
- d Choose Start > Programs > Adobe Acrobat Connect Pro Server 7 > Start Connect Pro Central Application Server.

Secure the meeting server only

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

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

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

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

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

4 Replace the code in step 3 with the following:

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

5 Save the Adaptor.xml file.

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

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

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

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

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

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

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

10 Save the VHost.xml file.

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

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

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

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

14 Save the custom.ini file.

15 Restart Acrobat Connect Pro Server 7:

- a Choose Start > Programs > Adobe Acrobat Connect Pro Server 7 > Stop Connect Pro Central Application Server.
- b Choose Start > Programs > Adobe Acrobat Connect Pro Server 7 > Stop Connect Pro Meeting Server.
- c Choose Start > Programs > Adobe Acrobat Connect Pro Server 7 > Start Connect Pro Meeting Server.
- d Choose Start > Programs > Adobe Acrobat Connect Pro Server 7 > Start Connect Pro Central Application Server.

Test the configuration

- 1 If you secured the application server, log in to Connect Pro Central. You see a lock in your browser.
- 2 If you secured the meeting server, enter an Acrobat Connect Pro meeting room. You see a lock in the connection light.

Configure hardware-based SSL

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

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

Configure the DNS server

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

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

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

Configure SSL for the meeting and application servers

- 1 Configure the hardware device to do the following:
 - a Listen externally on port 443 for application.example.com.

- b Forward unencrypted data to the application server on port 8443.
 - c Listen externally on port 443 for meeting1.example.com.
 - d Forward unencrypted data to the meeting server on port 1935.
 - e (Optional) Listen externally on port 80 for application.example.com and forward unencrypted data to the application server on port 80. The application server redirects users to port 443.
- 2 Configure the firewall to do the following:
 - a Allow traffic to the application server on port 443 (and on port 80 if you completed step 1e).
 - b Allow traffic to the meeting server on port 443.
 - 3 Choose Start > Programs > Adobe Acrobat Connect Pro Server 7 > Configure Connect Pro Server 7 to open the Application Management Console. On the Applications Settings screen, select Server Settings and do the following:
 - a Enter the FQDN of the application server (for example, connect.example.com) in the Connect Pro Host box. This FQDN is the URL end users use to connect to Acrobat Connect Pro.
 - b Enter the FQDN of the meeting server (for example, fms.example.com) in the Host Mappings External Name box. The server uses this value internally.
 - 4 Open the custom.ini file located in the root installation directory (c:\breeze, by default) and save a backup copy to another location.
 - 5 Insert the following code in the custom.ini file without replacing or deleting any existing text:

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

Note: The custom.ini file is case sensitive—use capital letters for parameter names and lowercase letters for values.

- 6 Save the custom.ini file.
- 7 Restart Acrobat Connect Pro Server 7:
 - a Choose Start > Programs > Adobe Acrobat Connect Pro Server 7 > Stop Connect Pro Central Application Server.
 - b Choose Start > Programs > Adobe Acrobat Connect Pro Server 7 > Start Connect Pro Central Application Server.

Configure SSL for the meeting server only

- 1 Configure the hardware device to do the following:
 - a Listen externally on port 443 for meeting1.example.com.
 - b Forward unencrypted data to the meeting server on port 1935.
 - 2 Configure the firewall to allow traffic to the meeting server on port 443.
 - 3 Open the custom.ini file located in the root installation directory (c:\breeze, by default) and save a backup copy to another location.
 - 4 Insert the following code in the custom.ini file without replacing or deleting any existing text:
- ```
RTMP_SEQUENCE=rtmps://external-host:443/?rtmp://localhost:8506/
```
- 5 Save the custom.ini file.

### Configure SSL for the application server only

- 1 Configure the hardware device to do the following:
  - a Listen externally on port 443 for application.example.com.
  - b Forward unencrypted data to the application server on port 8443.
  - c (Optional) Listen externally on port 80 for application.example.com and forward unencrypted data to the application server on port 80. The application server redirects users to port 443.
- 2 Configure the firewall to allow traffic to the application server on port 443 (and on port 80 if you completed step 1c).
- 3 On Acrobat Connect Pro, add the following to the custom.ini file in the root installation folder (c:\breeze, by default):

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

*Note: The custom.ini file is case sensitive—use capital letters for parameter names and lowercase letters for values.*

- 4 Restart Acrobat Connect Pro Server 7:
  - a Choose Start > Programs > Adobe Acrobat Connect Pro Server 7 > Stop Connect Pro Central Application Server.
  - b Choose Start > Programs > Adobe Acrobat Connect Pro Server 7 > Start Connect Pro Central Application Server.

### Test the configuration

- 1 If you secured the application server, log in to Connect Pro Central. You see a lock in your browser.
- 2 If you secured the meeting server, enter an Acrobat Connect Pro meeting room. You see a lock in the connection light.

### Configure software-based SSL for an edge server

If you have software SSL configured on the origin server, configure software-based SSL for any edge server you want to secure.

Just like an origin server, an edge server is made of two services: a meeting service and an application service. To configure SSL for both the meeting service and the application service, you must have two FQDNs and two IP addresses. You can share the application service FQDN with the origin server, but the meeting service must have its own FQDN. The FQDN of the application service is the URL users use to connect to their Acrobat Connect Pro accounts.

For example, if you have one edge server and one origin server, you must have three FQDNs and three SSL certificates: one for each meeting service and one for the application services to share. You must have four IP addresses, one for each meeting service and one for each application service.

In this example set-up, the origin server has the following IP addresses and FQDNs:

```
10.192.37.11 = connect.yourcompany.com
10.192.37.10 = meeting1.yourcompany.com
```

The edge server has the following IP addresses and FQDNs:

```
10.192.37.100 = connect.yourcompany.com
10.192.37.101 = edge1.yourcompany.com
```

**Note:** If you are installing both the edge and origin servers for the first time, set up both servers without SSL and verify that they can communicate with each other. Once you have determined that the edge and origin can communicate, you can configure SSL for both servers.

## See also

“Deploying Acrobat Connect Pro Edge Server 7” on page 25

“About SSL support” on page 50

## Configure the edge server

1 On the origin server, open the c:\breeze\comserv\win32\conf\\_defaultRoot\_\Adaptor.xml file and copy the entire <SSL></SSL> section, as follows:

```
<SSL>
 <Edge name="applicationserver">
 <SSLServerCtx>
 <SSLCertificateFile>C:\breeze\connect.yourcompany.com.pem</SSLCertificateFile>
 <SSLCertificateKeyFile type="PEM">C:\breeze\connect.yourcompany.com.pem
 </SSLCertificateKeyFile>
 <SSLCipherSuite>ALL:!ADH:!LOW:!EXP:!MD5:@STRENGTH</SSLCipherSuite>
 <SSLSessionTimeout>5</SSLSessionTimeout>
 </SSLServerCtx>
 </Edge>
 <Edge name="meetingserver">
 <SSLServerCtx>
 <SSLCertificateFile>C:\breeze\meeting1.yourcompany.com.pem
 </SSLCertificateFile>
 <SSLCertificateKeyFile type="PEM">C:\breeze\meeting1.yourcompany.com.pem
 </SSLCertificateKeyFile>
 <SSLPassPhrase></SSLPassPhrase>
 <SSLCipherSuite>ALL:!ADH:!LOW:!EXP:!MD5:@STRENGTH</SSLCipherSuite>
 <SSLSessionTimeout>5</SSLSessionTimeout>
 </SSLServerCtx>
 </Edge>
</SSL>
```

**Note:** Your code might contain different values, but it must contain the same XML elements.

2 On the edge server, open the c:\breeze\edgeserver\win32\conf\\_defaultRoot\_\Adaptor.xml file and paste the <SSL></SSL> codeblock from the origin server after the <Adaptor> tag.

3 Do the following to configure the application service and the meeting service on the edge server:

- a The application service is the <Edge name="applicationserver"> tag within the <SSL> block. The application service uses the same FQDN as the application service on the origin server. Copy the certificate and key .pem files from the origin server to the same location on the edge server. In this example, the FQDN is connect.yourcompany.com.

```
<Edge name="applicationserver">
 <SSLServerCtx>
 <SSLCertificateFile>C:\breeze\connect.yourcompany.com.pem</SSLCertificateFile>
 <SSLCertificateKeyFile type="PEM">C:\breeze\connect.yourcompany.com.pem
 </SSLCertificateKeyFile>
 <SSLCipherSuite>ALL:!ADH:!LOW:!EXP:!MD5:@STRENGTH</SSLCipherSuite>
 <SSLSessionTimeout>5</SSLSessionTimeout>
 </SSLServerCtx>
</Edge>
```

- b** The meeting service is the `<Edge name="meetingserver">` tag within the `<SSL>` block. Edit the XML so the meeting service points to a unique certificate and key for its unique FQDN. In this example, the FQDN is `edge1.yourcompany.com`:

```
<Edge name="meetingserver">
 <SSLServerCtx>
 <SSLCertificateFile>C:\breeze\edge1.yourcompany.com.pem
 </SSLCertificateFile>
 <SSLCertificateKeyFile type="PEM">C:\breeze\edge1.yourcompany.com.pem
 </SSLCertificateKeyFile>
 <SSLPassPhrase></SSLPassPhrase>
 <SSLCipherSuite>ALL:!ADH:!LOW:!EXP:!MD5:@STRENGTH</SSLCipherSuite>
 <SSLSessionTimeout>5</SSLSessionTimeout>
 </SSLServerCtx>
</Edge>
```

- 4** In the `Adaptor.xml` file on the edge server, locate the `<HostPort name="edge1">${FCS.HOST_PORT}</HostPort>` line. Add the following two lines after it:

```
<HostPort name="meetingserver" ctl_channel=":19354">206.192.37.100:-443</HostPort>
<HostPort name="applicationserver" ctl_channel=":19355">206.192.37.101:-443</HostPort>
```

This code binds the internal IP addresses of the edge server to secure port 443. This example uses the internal IP addresses 206.192.37.100 and 206.192.37.101. In your code, substitute the internal IP addresses of your edge server.

- 5** Save the `Adaptor.xml` file.

- 6** Open the `Adaptor.xml` file in a web browser to verify that the XML is valid.

If there are syntax errors, the web browser displays an error message. Correct the XML errors and recheck the file.

- 7** On the edge server, open the `c:\breeze\edgeserver\win32\conf\_defaultRoot\_defaultVHost\_Vhost.xml` file. Locate the `<RouteEntry></RouteEntry>` tag and replace it with the following:

```
<RouteEntry protocol="rtmp">*:*;10.192.37.11:8506</RouteEntry>
```

This code causes the edge server to route RTMP connections from any IP address and any port to the origin server over port 8506. This example uses the IP address 10.192.37.11. In your code, substitute the IP address of the application service on the origin server.

- 8** Save the `Vhost.xml` file.

- 9** Open the `Vhost.xml` file in a web browser to verify that the XML is valid.

If there are syntax errors, the web browser displays an error message. Correct the XML errors and recheck the file.

- 10** On the edge server, open the `c:\breeze\edgeserver\custom.ini` file.

- 11** Enter the `FCS.HTTPCACHE_BREEZE_SERVER_SECURE_PORT` parameter and set it to either the IP address or the FQDN of the origin server, as in the following:

```
FCS.HTTPCACHE_BREEZE_SERVER_SECURE_PORT=connect.yourcompany.com:443
FCS.HTTPCACHE_BREEZE_SERVER_NORMAL_PORT=connect.yourcompany.com:80
FCS_EDGE_HOST=edge1.yourcompany.com
FCS_EDGE_REGISTER_HOST=connect.yourcompany.com
FCS_EDGE_CLUSTER_ID=sanfran
FCS_EDGE_EXPIRY_TIME=60000
FCS_EDGE_REG_INTERVAL=30000
```

If you want to configure your system to connect only over SSL, comment out the `FCS.HTTPCACHE_BREEZE_SERVER_NORMAL_PORT` parameter, as follows:

```
FCS.HTTPCACHE_BREEZE_SERVER_NORMAL_PORT=connect.yourcompany.com:80
```

**Note:** If the edge server has trouble resolving the FQDN of the origin server, use the IP address.

**12** On the edge server, open the `C:\breeze\edgeserver\win32\conf\HttpCache.xml` and update the `<HostName>` tag as follows:

```
<HostName>${FCS_EDGE_HOST}</HostName>
```

**13** Save the `HttpCache.xml` file.

**14** Open the `HttpCache.xml` file in a web browser to verify that the XML is valid.

If there are syntax errors, the web browser displays an error message. Correct the XML errors and recheck.

### Configure the origin server

**1** Configure the origin server for SSL. For more information, see “[SSL \(secure sockets layer\)](#)” on page 50.

**2** On the origin server, open the `c:\breeze\custom.ini` file and enter the following to bind the edge server to the origin server:

```
edge.FCS_EDGE_CLUSTER_ID=1
```

Use the value for the `FCS_EDGE_CLUSTER_ID` parameter set in the `custom.ini` file on the edge server. In this example, the value is `sanfran`, so the code is `edge.sanfran=1`.

**Note:** The value 0 is reserved and cannot be used.

**3** Restart Connect Pro Central Application Server and Connect Pro Meeting Server.

**4** Choose `Start > Programs > Adobe Acrobat Connect Pro Server 7 > Configure Connect Pro Server 7` to open the Application Management Console. Do the following:

- a Click Server Settings.
  - b In the External Names box, you see the FQDN of the edge server with an empty box to the right of it. If you do not see the FQDN, wait a few minutes and refresh the browser.
  - c Enter the FQDN of the edge server in the empty box and click Save. This registers the edge server with the origin server.
- 5** Set up the local DNS server to direct users to the edge server when they request an Acrobat Connect Pro URL.

### Configure hardware-based SSL for an edge server

If you have hardware SSL configured on the origin server, configure hardware-based SSL for any edge servers you want to secure.

Just like an origin server, an edge server is made of two services: a meeting service and an application service. To configure SSL for both the meeting service and the application service, you must have two FQDNs and two IP addresses. You can share the application service FQDN with the origin server, but the meeting service must have its own FQDN. The FQDN of the application service is the URL users use to connect to their Acrobat Connect Pro accounts.

For example, if you have one edge server and one origin server, you must have three FQDNs and three SSL certificates: one for each meeting service and one for the application services to share. You must have four IP addresses, one for each meeting service and one for each application service.

In this example set-up, the origin server has the following IP addresses and FQDNs:

```
10.192.37.11 = connect.yourcompany.com
10.192.37.10 = meeting1.yourcompany.com
```

The edge server has the following IP addresses and FQDNs:

```
10.192.37.100 = connect.yourcompany.com
10.192.37.101 = edge1.yourcompany.com
```

**Note:** If you are installing both the edge and origin servers for the first time, set up both servers without SSL and verify that they can communicate with each other. Once you have determined that the edge and origin can communicate, you can configure SSL for both servers.

## See also

[“Deploying Acrobat Connect Pro Edge Server 7”](#) on page 25

[“About SSL support”](#) on page 50

## Configure the edge server

- 1 On the edge server, open the `c:\breeze\edgeserver\custom.ini` file.
- 2 Enter the `FCS.HTTPCACHE_BREEZE_SERVER_SECURE_PORT` parameter and set it to either the IP address or the FQDN of the origin server, as in the following:

```
FCS.HTTPCACHE_BREEZE_SERVER_SECURE_PORT=connect.yourcompany.com:443
FCS.HTTPCACHE_BREEZE_SERVER_NORMAL_PORT=connect.yourcompany.com:80
FCS_EDGE_HOST=edge1.yourcompany.com
FCS_EDGE_REGISTER_HOST=connect.yourcompany.com
FCS_EDGE_CLUSTER_ID=sanfran
FCS_EDGE_EXPIRY_TIME=60000
FCS_EDGE_REG_INTERVAL=30000
```

If you want to configure your system to connect only over SSL, comment out the `FCS.HTTPCACHE_BREEZE_SERVER_NORMAL_PORT` parameter, as follows:

```
FCS.HTTPCACHE_BREEZE_SERVER_NORMAL_PORT=connect.yourcompany.com:80
```

**Note:** If the edge server has trouble resolving the FQDN of the origin server, use the IP address.

- 3 On the edge server, open the `C:\breeze\edgeserver\win32\conf\HttpCache.xml` and update the `<HostName>` tag as follows:

```
<HostName>${FCS_EDGE_HOST}</HostName>
```

- 4 Save the `HttpCache.xml` file.
- 5 Open the `HttpCache.xml` file in a web browser to verify that the XML is valid.



If there are syntax errors, the web browser displays an error message. Correct the XML errors and recheck.

**Configure the origin server**

- 1 Configure the origin server for SSL. For more information, see “[SSL \(secure sockets layer\)](#)” on page 50.
- 2 On the origin server, open the c:\breeze\custom.ini file and enter the following to bind the edge server to the origin server:

```
edge.FCS_EDGE_CLUSTER_ID=1
```

Use the value for the `FCS_EDGE_CLUSTER_ID` parameter set in the custom.ini file on the edge server. In this example, the value is `sanfran`, so the code is `edge.sanfran=1`.

*Note: The value 0 is reserved and cannot be used.*

- 3 Restart Connect Pro Central Application Server and Connect Pro Meeting Server.
- 4 Choose Start > Programs > Adobe Acrobat Connect Pro Server 7 > Configure Connect Pro Server 7 to open the Application Management Console. Do the following:
  - a Click Server Settings.
  - b In the External Names box, you see the FQDN of the edge server with an empty box to the right of it. If you do not see the FQDN, wait a few minutes and refresh the browser.
  - c Enter the FQDN of the edge server in the empty box and click Save. This registers the edge server with the origin server.
- 5 Set up the local DNS server to direct users to the edge server when they request an Acrobat Connect Pro URL.

**SSL XML tags**

Tag	Default value	Description
SSLCertificateFile	No default.	The location of the certificate file to send to the client. If an absolute path is not specified, the certificate is assumed to be relative to the Adaptor directory.
SSLCertificateKey-File	No default.	The location of the private key file for the certificate. If an absolute path is not specified, the key file is assumed to be relative to the Adaptor directory. If the key file is encrypted, the pass phrase must be specified in the SSLPassPhrase tag.  The type attribute specifies the type of encoding used for the certificate key file. The type can be either PEM or ASN1.

Tag	Default value	Description
SSLCipherSuite	See description.	The encryption algorithm. The algorithm consists of colon-delimited elements. These elements can be key exchange algorithms, authentication methods, encryption methods, digest types, or one of a selected number of aliases for common groupings. For a list of components, see the Flash Media Server documentation.  This tag has the following default setting:  ALL: !ADH: !LOW: !EXP: !MD5: @STRENGTH  Contact Adobe Technical Support before changing the default settings.
SSLPassPhrase	No default.	The pass phrase to use for decrypting the private key file. If the private key file is not encrypted, leave this tag empty.
SSLSessionTimeout	5	The amount of time an SSL-enabled session remains valid, in minutes.

### SSL configuration parameters

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

## 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 Acrobat Connect Pro 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 Acrobat Connect Pro, 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 Acrobat Connect Pro.

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 Acrobat 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.

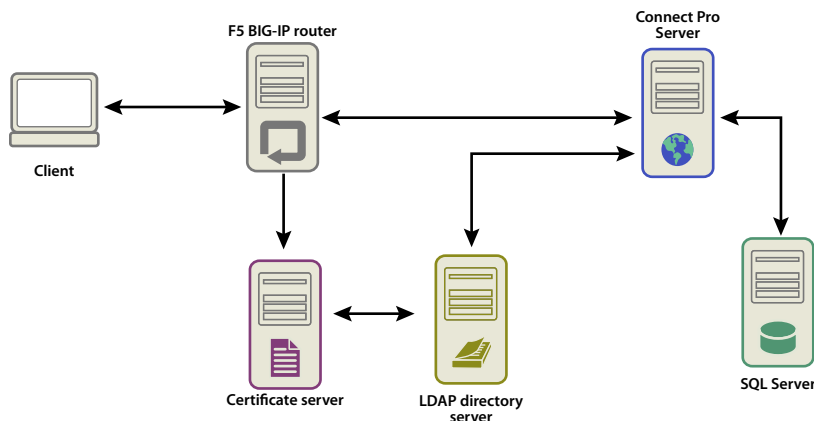
You can design a PKI system to require authentication for only HTTP connections or for both HTTP and RTMP connections. If you require client-side certificates on both HTTP and RTMP connections, users are prompted each time a new server connection is established. For example, there would be two prompts 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:

- Acrobat Connect Pro is installed.
- Acrobat Connect Pro is integrated with an LDAP directory service.
- A user imported from the LDAP directory service can enter a meeting served by Acrobat Connect Pro.
- 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. Acrobat Connect Pro 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 Acrobat Connect Pro share.*

### 2. Set the Acrobat Connect Pro login policy.

Acrobat Connect Pro must use an e-mail address for user login. In Connect Pro Central, select the Administration tab, then click Users and Groups, then 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 Acrobat Connect Pro to use HTTP-header authentication.

In the file `[root_install_dir]\appserv\conf\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 Acrobat Connect Pro.

### 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 Acrobat Connect Pro 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 OSCP (Online Certification Status Protocol) and LDAP lookup.

Once the certificate is authenticated, parse it for a unique identifier that Acrobat Connect Pro knows. In this example, a valid certificate is parsed for an e-mail address.

A request that includes the string `session` or has a `BREEZESSESSION` cookie is allowed to pass without authentication because the client has already authenticated. (Acrobat Connect Pro verifies these arguments with a database query.)

If the request doesn't include the `session` string or `BREEZESSESSION` cookie, the user must log in to Acrobat Connect Pro. 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 Acrobat Connect Pro 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 BREEZESSESSION] } {
 set cookie_payload [HTTP::cookie value BREEZESSESSION]
}
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 $emailAddr
}
elseif { [HTTP::uri] contains "session" }
{
 #do nothing, Acrobat Connect Pro verifies the token found in session=$token
}
else
{
 # URI encode the current request, and pass it to
 # the Acrobat Connect Pro 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]]
}
```

### See also

[“Start and stop Acrobat Connect Pro Server 7”](#) on page 18

## Securing the infrastructure

### Network security

Acrobat Connect Pro relies on several private TCP/IP services for its communications. These services open several ports and channels that must be protected from outside users. Acrobat Connect Pro 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 Acrobat Connect Pro 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 Acrobat Connect Pro on your Intranet, place the Acrobat Connect Pro servers and the Acrobat Connect Pro database in a separate subnet, separated by a firewall. The internal network segment where Acrobat Connect Pro 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 Acrobat Connect Pro 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 Acrobat Connect Pro, 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.

For information on securing SQL Server, see the Microsoft SQL security website.

### **Create service accounts**

Creating a service account for Acrobat Connect Pro lets you run Acrobat Connect Pro more securely. Adobe recommends creating a service account and an MSDE service account for Acrobat Connect Pro. 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 Enterprise 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 Acrobat Connect Pro folder path (c:\breeze, 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 MSDE service account**

- 1 Create a local account called ConnectSqlService that doesn't include any default groups.
- 2 Change the MSDE 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 Acrobat Connect Pro on a single computer. It assumes that the database is installed on the same computer, and that users access Acrobat Connect Pro on the Internet.

**1. Install a firewall.**

Since you are allowing users to connect to Acrobat Connect Pro 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 Acrobat Connect Pro, you do not have to open port 1434 on the firewall.

**3. Install Acrobat Connect Pro.**

**4. Verify that the Acrobat Connect Pro applications are working.**

After installing Acrobat Connect Pro, 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 Acrobat Connect Pro cluster can be located at a data center or geographically distributed across multiple network operation centers. You can install and configure servers hosting Connect Pro in multiple locations and synchronize them through database replication.

*Note: Clusters must use Microsoft SQL Server, 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 Acrobat Connect Pro system. This approach offers a high level of security.

**Local software firewalls** For Acrobat Connect Pro 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 Acrobat Connect Pro 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. Acrobat Connect Pro 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 Acrobat Connect Pro 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 Acrobat Connect Pro. 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 Acrobat Connect Pro.

**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. Acrobat Connect Pro relies on the safety of the host system against intruders, so keep servers secure when private and confidential data is at risk. Acrobat Connect Pro is designed to take advantage of native environmental features such as file system encryption.

**Use strong passwords** Strong passwords protect data. Acrobat Connect Pro administrators can set login and password policies in the Connect Pro Central. Acrobat Connect Pro installations often use Microsoft SQL Server, which also requires strong password protection.

**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. This information also applies to the embedded database engine installed with Connect.

**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. Acrobat Connect Pro 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 Acrobat Connect Pro.*

# Index

## A

- account administrator, creating 15
- account capacity 38
- account notification reports, monthly 38
- accounts, service 67
- administrator, creating 15
- Adobe Acrobat Connect Add-in hosting 47
- Adobe Acrobat Connect Enterprise Manager verifying connectivity 16
- Adobe Acrobat Connect Professional, verifying installation 17
- Adobe Connect Edge Server
  - about 11
  - deploying 11
  - starting and stopping 20
- Adobe Connect Enterprise Server
  - account administrator 15
  - configuring with Application Management Console 14
  - database connectivity, verifying 16
  - license file 15
  - service 18
  - starting and stopping 18
- Adobe Connect Events, verifying installation 18
- Adobe Connect Training, verifying installation 17
- Adobe Presenter, verifying installation 17
- Apache 46
- Application Management Console
  - about 14
  - Authentication Settings 32
  - Create Administrator tab 15
  - Database Settings tab 14
  - Directory Service Settings tab 30
  - LDAP Settings 30
  - License Settings tab 15
  - Server Settings tab 15, 23
  - Shared Storage Settings 35
- application server 6

## authentication

- about 45
- HTTP header 45
- PKI 64, 65
- Authentication Settings 32

## B

- BREEZESSESSION cookie 46, 66

## C

- CA (certificate authority) 63, 65
- cache, configuring 15
- certificate authority 63, 65
- certificates
  - client 63
- client-certificate 63
- clustering 9
- clusters 23, 24
  - deploying 9
  - ports 1
  - securing 69
- command line, starting and stopping services from 19
- Connect Enterprise Manager. *See* Adobe Acrobat Connect Enterprise Manager
- Connect Enterprise Server, migrating from 3
- Connect Events, verifying installation 18
- Connect Pro Edge Server. *See* edge servers
- Connect Pro Presence Service 39
  - starting and stopping 20
- Connect Professional, verifying installation 17
- Connect Training, verifying installation 17
- content
  - cache, configuring 15
  - shared storage 15, 35
  - supported storage devices 3
- Create Administrator tab 15

## custom.ini file

- HTTP\_AUTH\_HEADER parameter 45
- parameters for configuring edge server 26

## D

- data flow 7
- database
  - about 6
  - backup 4, 67
  - choosing 10
  - cluster 22
  - configuring 14
  - ports 1
  - security 67
  - SQL Server 22
  - supported server configurations 2
  - upgrading 5
  - verifying connectivity 16
- DEFAULT\_FCS\_HOSTPORT parameter 26
- deploying 22
- directory servers, supported 2
- directory service integration 28
- directory service integration. *See* LDAP
- Directory Service Settings tab 30
- distinguished name 28
- DMZ (demilitarized zone) 67

## E

- edge servers 26
  - deploying 26
  - host mappings 28
  - load balancing 26
- e-mail notifications, verifying 16
- Enterprise Manager. *See* Adobe Acrobat Connect Enterprise Manager
- Events, verifying installation 18

## F

- F5
  - iRule 66
- failover, verifying 24

FCS\_EDGE\_CLUSTER\_ID  
parameter 26

FCS\_EDGE\_EXPIRY\_TIME  
parameter 26

FCS\_EDGE\_HOST parameter 26

FCS\_EDGE\_PASSWORD  
parameter 26

FCS\_EDGE\_REG\_INTERVAL  
parameter 26

FCS\_EDGE\_REGISTER\_HOST  
parameter 26

FCS.HTTPCACHE\_BREEZE\_SERV  
ER\_NORMAL\_PORT  
parameter 26

files

- custom.ini. *See* custom.ini file
- license 15

filters

- Java 45
- LDAP 29

firewalls, configuring 66, 68

Flash Media Server 6

Flash Media Server (FMS) service 18

Flash Media Server Administration  
Server service 18

Flash Player 47

FMS service 18

FQDN (fully qualified domain  
name) 15, 23, 26

**G**

groups, LDAP 29, 32

**H**

host mappings 15, 23, 28

HTTP

- port 15

HTTP header authentication

- about 45
- PKI 64, 65
- single sign-on 45

HTTP\_AUTH\_HEADER  
parameter 45

hypertext transfer protocol. *See*  
HTTP

**I**

IM integration 39

iRule 66

**J**

Java

- application server 6
- filter 45

**L**

LDAP

- attribute 28
- deletion policy 33
- directory servers supported 2
- directory service integration 28
- directory structure 28
- filtering 29
- groups 32
- importing branches 29
- importing users and groups 29
- password management 33
- password policy 33
- PKI integration 64
- synchronization 33, 34
- user profile mapping 31

LDAP integration 29

LDAP Settings 30

license file

- Connect Enterprise Server 15

License Settings tab 15

load balancing

- edge servers 26
- verifying 24

login policies 65

logs, synchronization 34

**M**

Management Console. *See*  
Application Management  
Console

mappings, host 15, 23, 28

meeting server 6

meeting. *See* Adobe Acrobat Connect  
Professional

memory management. *See* content  
Microsoft database engine (MSDE).  
*See* database

Microsoft Live Communications  
Server 2005 39

Microsoft Office Communications  
Server 2007 39

Microsoft SQL Server 22

migration 3

MSDE. *See* database

**N**

NAS device 35

network security 66

NMap tool 70

notifications 38

notifications, e-mail 16

**O**

operating systems

- security 69

**P**

passwords

- management (LDAP) 33
- policy (LDAP) 33
- strong 69

PKI

- about 63
- user requirements 64

ports

- database 14
- HTTP 15
- list of 1
- protecting 66
- scanning tool 70

presence 39

Presenter, verifying installation 17

profiles, LDAP users and groups 31

protocols

- HTTP 6, 15
- HTTPS 6
- LDAP 2, 28
- RTMP 6
- RTMPS 6
- SMTP 15

public key infrastructure. *See* PKI

**R**

real-time messaging protocol. *See*  
RTMP

requirements

- PKI 64

resources, security 69, 70

router, F5 64

RTMP (real-time messaging  
protocol) 1, 6

**S**

SAN device 35

security

- checklist 69
- clusters 69
- network 66
- PKI 63
- service accounts 67
- single server installation 68

Server Settings tab 15

service accounts 67

Services window 18, 20

session parameter 46

shared storage

- about 35
- configuring 36
- server setting 15

simple mail transfer protocol. *See* SMTP

single sign-on

- about 45
- authentication 45

SMTP

- settings 15

SQL Server 22

Start menu 18

starting and stopping Connect Edge Server 18

starting and stopping Connect Enterprise Server 18

storage management. *See* content synchronization 34

**T**

technical overview 6

Training, verifying installation 17

**U**

upgrade paths 3

upgrading

- backing up database 4
- backing up files 4
- database 5
- informing users about 4
- paths 3

user profile mapping 31

users and groups, LDAP 29

**W**

web servers 46

**X**

X.509 standard 63