ADOBE® CONNECT™ ENTERPRISE SERVER 6

INSTALLATION AND CONFIGURATION GUIDE

Adobe

Adobe® Connect™ Enterprise Server 6 Installation and Configuration Guide for Windows® and Macintosh

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

Contents

Chapter 1: Before you begin

This chapter provides information about the documentation, what's new in Adobe® Connect™ Enterprise Server 6, and where you can get additional information and support.

About the documentation

Audience

This guide is intended for IT professionals who are installing and configuring an Adobe Connect Enterprise system for their organization.

What's new

The following features are new in Adobe Connect Enterprise 6 and Adobe Connect Edge Server 6.

Shared storage Configure Connect Enterprise to share content storage across multiple Network Attached Storage (NAS) and Storage Area Network (SAN) devices. As an organization's user base and content grows, use shared content storage to scale and maintain your Connect Enterprise system.

You can choose to mirror content on Connect Enterprise Server or to store all content on the external devices and cache active content on the server. Content is purged from the server when it's no longer in use. For more information, see "Configuring shared storage" on page 35.

Public key infrastructure Adobe® Acrobat® Connect™ Add-in supports client certificates. This support allows you to implement a public key infrastructure (PKI) to heighten security for your network. For more information, see "Public key infrastructure" on page 41.

LDAP query paging Specify a page size for Lightweight Directory Access Protocol (LDAP) query results so you can import all the users in your directory. For more information, see "Integrating Connect Enterprise with an LDAP directory" on page 28.

Secure LDAP Synchronize Connect Enterprise 6 with an LDAP directory server over the secure Lightweight Directory Access Protocol (LDAPS) protocol. For more information, see "Configure LDAPS" on page 34.

Edge Server clustering Deploy Adobe Connect Edge Server in a cluster to provide increased scalability and system redundancy. Edge servers consolidate streams, cache content, and provide greater control over the flow of information. For more information, see "Choosing to deploy edge servers" on page 14.

64-bit operating system support Connect Enterprise 6 adds support for Windows Server® 2003 x64.

Native SSL support In previous releases, secure connections to Adobe® Breeze® were tunneled. Native Secure Sockets Layer (SSL) support improves network performance and decreases connection latency. For more information, see www.adobe.com/go/connect_ssl_en.

Custom Whiteboard stamps You can create your own custom stamps to include with the Whiteboard drawing tools in Adobe Acrobat Connect Professional. For more information, see "Custom whiteboard stamps" on page 45.

Host Adobe Acrobat Connect Add-in Acrobat Connect Add-in downloads seamlessly from Adobe servers when it's required by a client in a meeting. However, if your organization's security policy forbids external downloads, you can host the Acrobat Connect Add-in on your own servers. For more information, see "Hosting Acrobat Connect Add-in" on page 44.

How to use this book

This book is divided into the following six chapters:

"Before you begin" A list of what's new, web resources, and how to contact Adobe Technical Support.

"Preparing for installation and configuration" System requirements, a technical overview of Connect Enterprise, and information to help you integrate Connect Enterprise with your organization's existing resources. If you understand the components and optional features of Connect Enterprise, you may want to skip all but the system requirements in this chapter and go to the installation instructions.

"Installing and upgrading Connect Enterprise" Installation instructions for both Connect Enterprise Server and Connect Edge Server.

"Deploying and configuring Connect Enterprise" Steps for deploying Connect Enterprise Server and Connect Edge Server, for configuring optional features such as external content storage, and for integrating Connect Enterprise with a directory service.

"Configuring advanced features" Steps for hosting the Acrobat Connect Add-in on your own server, implementing a PKI, configuring single sign-on, and creating custom whiteboard stamps.

"Verifying your installation" Steps for verifying that all the components of your system are operational.

"Securing Connect Enterprise" Information for securing your network, database, and Connect Enterprise Server.

Resources

Adobe.com

These resources are available on the Adobe website (www.adobe.com):

Adobe Design Center Offers articles, tips, and tutorials in various formats, including video, Adobe PDF, and HTML. The content is authored by industry experts, designers, and Adobe publishing partners, and new content is added monthly. You'll also find Adobe® Studio® Exchange, where users download and share thousands of free actions, plug-ins, and other content. Adobe Design Center is available in English, French, German, and Japanese.

Adobe Developer Center Provides information for advanced users, including software and plug-in developers. You'll find tutorials, SDKs, scripting guides, and sample code, in addition to forums, RSS feeds, online seminars, and other technical resources.

Support Home Contains information about free and paid technical support options. Top issues are listed by product on the Adobe U.S. and Adobe Japan websites. Follow the Training link for access to Adobe Press books; online, video, and instructor-led training resources; Adobe software certification programs; and more.

Downloads Provides free updates, tryouts, and other useful software. In addition, the Plugins section of the Adobe Store provides access to thousands of plug-ins from third-party developers, helping you to automate tasks, customize workflows, create specialized professional effects, and more.

Communities Features forums, blogs, and other avenues for users to share technologies, tools, and information; ask questions; and find out how others are getting the most out of their software. User-to-user forums are available in English, French, German, and Japanese; blogs are posted in a wide range of languages.

Contacting Technical Support

If you encounter unexpected results after you install Connect Enterprise Server or Connect Edge Server either on a single server or on a cluster of servers, or for help configuring the server, contact Adobe Technical Support at www.adobe.com/go/connect_licensed_programs_en.

Chapter 2: Preparing for installation and configuration

Review the installation requirements, supported configurations, and technical overview as you prepare to design and install a Connect Enterprise system. If you are upgrading to Adobe Connect Enterprise Server 6, follow the instructions for backing up files and migrating to a more advanced system.

Installation requirements

Hardware requirements for Connect Enterprise Server

Component	Requirement
Server processor	Dual Xeon, 3 GHz processor or faster (recommended) Pentium 4, 2 GHz (minimum)
Memory	4 GB RAM (recommended)
Hard drive	100+ GB recommended Breakdown: 1 GB for installation 10 GB per 100 presentations 80 GB minimum of disk space for content storage (disk space requirements increase as more content is stored)
Network connection	100 MBit (minimum)
Drive	CD-ROM or DVD-ROM
Other	To enable SSL, you can use an SSL hardware accelerator or native (software) SSL. For more information, see www.adobe.com/go/connect_ssl_en. To load balance a cluster, you need load balancing hardware such as BIG-IP from F5 or Network Load Balancing (NLB) software from Microsoft. Connect Enterprise Server requires a dedicated server. The computer hosting Connect Enterprise Server and the computer hosting SQL Server must be synchronized to the same time source. See the Microsoft articles "How to configure an authoritative time server in Windows 2000" and "How to configure an authoritative time server in Windows Server 2003".

For updated Connect Enterprise Server system requirements and recommendations, see www.adobe.com/go/connect_sysreqs_en.

Software requirements for Connect Enterprise Server

Component	Requirement
Operating system	Microsoft Windows Server 2000, or Microsoft Windows Server 2003 SP2
Databases	SQL Server 2000 SP4 (English version), or SQL Server 2005 SP1 (English version), or MSDE embedded database engine (included with Connect Enterprise Server)
SMTP e-mail server	The SMTP server can be on the same computer or can be relayed to another computer such as a UNIX® sendmail server or a Microsoft Exchange Server. It is used to send e-mail notifications. An SMTP server is not required, but a System e-mail address and a Support e-mail address are required.
File system	New Technology File System (NTFS)
Web server	Connect Enterprise Server has its own web server; no other web servers (such as Apache) can be used with Connect. Adobe recommends that you disable the default IIS web server service because Connect uses the IIS port.
Other	Real-time virus checking cannot be installed on the server.

See also

"Choosing a database" on page 13

User requirements for Connect Enterprise Server

For Adobe Connect Enterprise Server 6 user requirements, see www.adobe.com/go/connect_sysreqs_en.

Port requirements for Connect Enterprise Server

This 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

This table describes the ports open inside a cluster. Each Connect Enterprise 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 Connect Enterprise 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

This table describes server ports that Connect Enterprise uses to communicate internally. These ports must not be in use on a server hosting Connect Enterprise or Connect Enterprise 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

Hardware requirements for Connect Edge Server

For Adobe Connect Edge Server 6 system requirements, see www.adobe.com/go/connect_sysreqs_en.

Supported configurations

Supported server-database configurations

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

Single server with embedded database engine Install Connect Enterprise Server on a single computer and install the embedded database engine (included on the Connect Enterprise Server installer) on the same computer.

Single server with SQL Server database Install Connect Enterprise Server on a single computer and install either SQL Server 2000 or SQL Server 2005 on the same computer.

Single server with external SQL Server database Install Connect Enterprise Server on a single computer and install either SQL Server 2000 or SQL Server 2005 on another computer.

Multiple servers with external SQL Server database Install Connect Enterprise Server on multiple servers (also called a cluster) and install either SQL Server 2000 or SQL Server 2005 on another computer.

Note: *Microsoft SQL Server is not included with Connect Enterprise Server 6 and must be purchased separately.*

See also

"Preparing to install" on page 9

"Installing Connect Enterprise Server 6" on page 16

Supported LDAP directory servers

You can import directory information into Connect Enterprise from your organization's LDAP directory server. The following LDAP directory servers are supported for integrating with Connect Enterprise:

- Active Directory Application Mode SP1 (ADAM)
- Active Directory (Windows Server 2000 and Windows Server 2003)
- IBM® 5.2
- Novell eDirectory 8.7.3 for Win32
- OpenLDAP 2.3.19
- Sun™ Directory Server 5.2 for Win32
- Netscape 6.02 for Win32

See also

"Integrating Connect Enterprise with a directory service" on page 26

Supported single sign-on solutions

You can configure your Connect Enterprise system to work with single sign-on authentication. Single sign-on lets users who are logged in to your organization's network use other resources, including Connect Enterprise, without logging in again. Connect Enterprise supports the following single sign-on solutions:

- HTTP header authentication
- Windows NT Lan Manager (NTLM) authentication

See also

"Single sign-on" on page 37

Supported content storage devices

You can configure your Connect Enterprise 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 upgrade

Upgrade paths

The Connect Enterprise Server installer and Application Management Console provide graphical user interfaces that guide you through the upgrade. The following upgrade paths are supported:

5.1 to 6.0 Run the Adobe Connect Enterprise 6.0 installer.

5.0 to 6.0 Run the Adobe Connect Enterprise 6.0 installer.

4.1 to 6.0 Run the Adobe Connect Enterprise 6.0 installer and follow the instructions for the 4.1 upgrade path.

3.0.7 to 6.0 See the Upgrade Documentation section on the Connect Enterprise Licensed Support Center (www.adobe.com/go/connect_licensed_support_en) to upgrade to 4.1, then follow the 4.1 to 6.0 upgrade path.

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

Upgrading from Breeze to Connect Enterprise

Follow this workflow to upgrade Adobe Breeze to Connect Enterprise Server 6.

1. **Test the upgrade in a non-production environment.**

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

2. **Inform users about the upgrade.**

See "Informing users about the upgrade" on page 8.

3. **Stop Connect Enterprise Server and back up files.**

See "Back up files" on page 8.

4. **Back up the database.**

See "Back up the database" on page 8.

5. **Run Adobe Connect Enterprise Server 6 installer.**

See "Installing Connect Enterprise Server 6" on page 16.

6. **Configure Connect Enterprise Server.**

See "Configuring Connect Enterprise Server with the Application Management Console wizard" on page 17.

7. **Verify the installation.**

See "Verifying your installation" on page 47.

Upgrading from the embedded database to SQL Server

Follow this workflow to upgrade from using the embedded database to using SQL Server on a different computer.

1. **Install SQL Server.**

Follow the instructions provided by Microsoft to install SQL server.

2. **Back up the embedded database.**

See "Back up the database" on page 8.

3. Copy the .bak file from the Breeze 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.

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

5. Enter the SQL Server database information in the Application Management Console.

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

Informing users about the upgrade

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

- Allocate enough time to ensure a successful upgrade. The upgrade should fit into your normal maintenance period.
- Let users know in advance that they won't be able to use Connect Enterprise during the upgrade.
- Let users know what types of changes they can expect (such as new features or improved performance) after the upgrade.

See also

"What's new" on page 1

Back up files

1 To stop all Breeze server services, select Start > All Programs > Macromedia > Macromedia Breeze > Stop Breeze 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\.

Back up the database

You must back up the database (either the embedded database engine or SQL Server 2000) that Connect Enterprise Server uses before you upgrade.

To back up the embedded database engine, use the Command Prompt window; the embedded database engine doesn't have a graphical user interface.

Note: *You can configure SQL Server Enterprise Manager to back up the embedded database engine. See the following Adobe TechNote: www.adobe.com/go/79895439.*

To back up SQL Server 2000, use SQL Server Enterprise Manager.

Important: *Do not uninstall the database.*

Back up the SQL Server database

If you are using Microsoft SQL Server 2000, you can use SQL Server Enterprise Manager to back up your database.

Important: *Do not uninstall the database.*

1 In Windows, select Start > All 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.

Important: *Do not uninstall the database.*

1 Log on to the server hosting Connect Enterprise Server.

2 Create a folder to store the database backup files.

This example uses the folder c:\Connect_Database.

3 From your Windows desktop, select Start > Run.

4 In the Run dialog box, type `cmd` in the Open box.

5 At the prompt, change to the directory where you installed the database. By default, the directory is MSSQL\binn.

6 At the MSSQL\Binn prompt, type `osql -E -Q "BACKUP DATABASE breeze TO DISK = 'c:\Connect_Database\breeze.bak'"` and press Enter.

A message indicates whether the backup was successful.

When you use the -E command, you enter SQL in "sa" mode.

To access help information for database commands, type `osql ?` at the DOS prompt and press Enter.

7 At the prompt, type `quit` and press Enter.

8 To verify that the backup was successful, confirm that the breeze.bak file exists in the c:\Connect_Database directory.

9 To restart your database, from your Windows desktop, select Start > Control Panel > Administrative Tools > Services. In the Services window, right-click 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".

Preparing to install

Connect Enterprise Server technical overview

A Connect Enterprise Server installation consists of several components: Connect Enterprise Server, Macromedia® Flash® Media Server from Adobe, and a database.

Connect Enterprise Server is a 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 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.

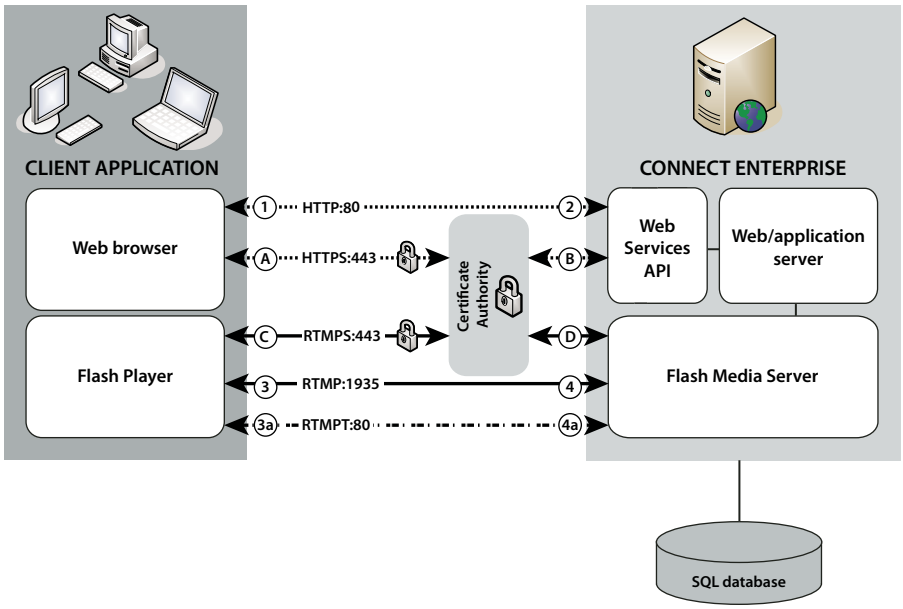
Note: *The application server includes a web server and is sometimes referred to as the "web/application server".*

Flash Media Server, also called the *meeting server*, is installed with Connect Enterprise Server to handle real-time audio and video streaming, data synchronization, and rich-media content delivery, including Acrobat Connect Professional 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 Enterprise Server 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 Connect Enterprise Server installer, or you can install the full version of Microsoft SQL Server 2000 or 2005. (The embedded database engine is included in the Connect Enterprise Server installation; Microsoft SQL Server is not.)

Data flow

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



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

Installation workflow

The following steps help you design, install, and configure a Connect Enterprise 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 13.

2. Install Connect Enterprise Server on a single server.

For more information, see "Installing Connect Enterprise Server 6" on page 16. If you chose the embedded database engine in step 1, install it too. The embedded database engine is part of the Connect Enterprise Server installer.

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

For more information, see the SQL Server documentation.

4. Deploy Connect Enterprise Server.

For more information, see "Deploying Connect Enterprise Server 6" on page 23.

5. Verify that Connect Enterprise Server is installed correctly.

For more information, see "Installation verification tasks" on page 47.

6. (Optional) Integrate Connect Enterprise with your infrastructure.

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

Directory service integration Integrate Connect Enterprise with your organization's LDAP directory server so you don't need to manage multiple user directories. See "Integrating Connect Enterprise with a directory service" on page 26.

Configure a secure socket layer Conduct all Connect Enterprise communication securely. See www.adobe.com/go/connect_ssl_en.

Store content on NAS/SAN devices Use network devices to share content storage duties. See "Configuring shared storage" on page 35.

Configure single sign-on authentication If you've integrated Connect Enterprise with an LDAP directory server, allow users to access Connect Enterprise resources without logging in. See "Single sign-on" on page 37.

Configure a public key infrastructure If you've integrated Connect Enterprise with an LDAP directory server, add a security layer by requiring client certificates. See "Public key infrastructure" on page 41.

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 44.

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

For more information, see "Choosing to deploy Connect Enterprise in a cluster" on page 12 and "Deploy Connect Enterprise Server in a cluster" on page 23.

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

For more information, see "Choosing to deploy edge servers" on page 14 and "Deploy Connect Edge Server" on page 25.

Choosing to deploy Connect Enterprise in a cluster

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

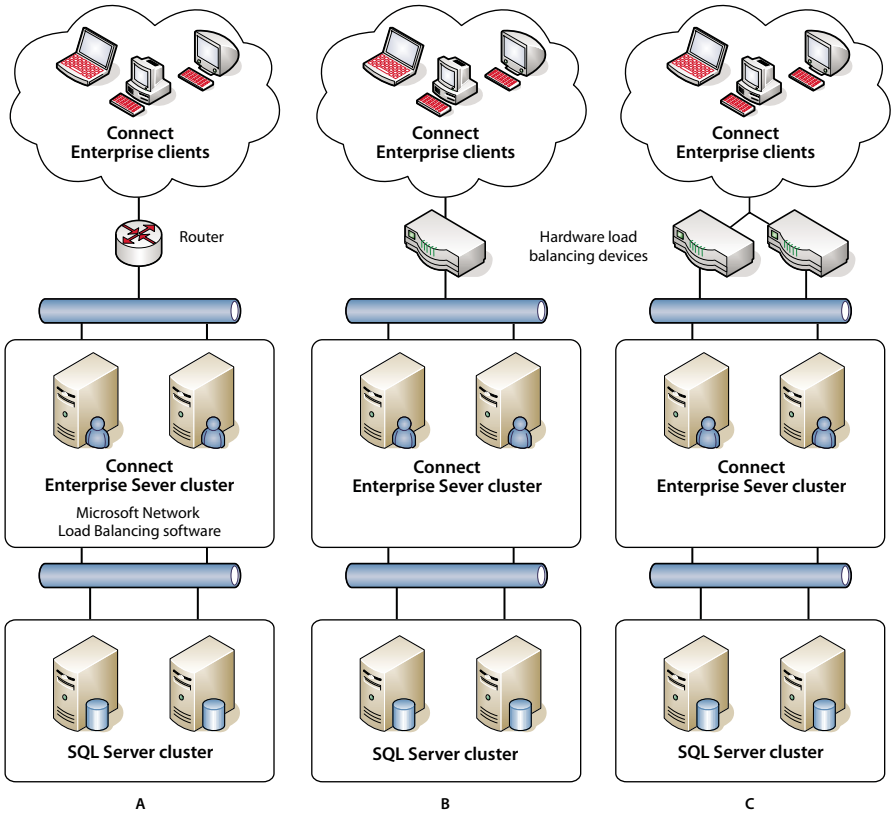
A group of connected servers, each doing an identical job, is usually called a *cluster*. In a Connect Enterprise Server cluster, you install an identical copy of Connect Enterprise Server on each server in the cluster.

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 Connect Enterprise Server.*

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

Ideally, every component in a system should be redundant, not just Connect Enterprise Server. For example, you could use multiple hardware load balancing devices (such as BIG-IP by F5 Networks), a cluster of servers hosting Connect Enterprise Server, 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 Connect Enterprise Server in a cluster" on page 23

"Configuring shared storage" on page 35

Choosing a database

Connect Enterprise Server 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 2000 or 2005 (which must be purchased separately).

Embedded database

Consider using this database engine for testing and development. It uses the same data structures as SQL Server, 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 Connect Enterprise Server. 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.

For more information about the embedded database engine (MSDE), see the Microsoft article "MSDE security and authentication."

Microsoft SQL Server

You can install SQL Server on the same computer as Connect Enterprise Server 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.

It's a good idea to use the Microsoft SQL Server 2000 or 2005 engine in production environments because SQL Server is a scalable database management system (DBMS) designed to support a large number of concurrent users. SQL Server also provides graphical user interfaces for managing and querying the database.

Install SQL Server in mixed login mode so that you can use SQL authentication. Set the database to case insensitive and, if you're using SQL Server 2000, apply Service Pack 4.

You must use SQL Server in the following deployment scenarios:

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

See also

"Supported server-database configurations" on page 5

"Installing Connect Enterprise Server 6" on page 16

Choosing to deploy edge servers

When there are edge servers on an organization's network, clients connect to Connect Edge Server and Connect Edge Server connects to Connect Enterprise Server. This connection occurs transparently—to users, it appears that they are connected directly to the server hosting the meeting.

Note: *When edge servers are used, the server on which Connect Enterprise Server is installed is called the "origin" server.*

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.

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.

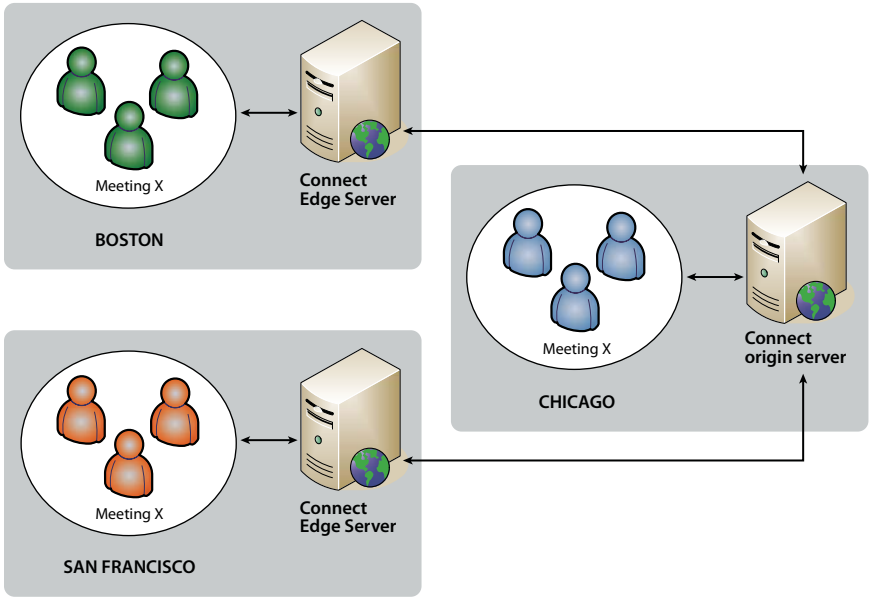
How edge servers work

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

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

"Installing Connect Edge Server 6" on page 20

"Deploying Connect Edge Server 6" on page 24

Chapter 3: Installing and upgrading Connect Enterprise

To install and configure Adobe Connect Enterprise Server and Connect Edge Server, you will interact with a series of installer and Application Manager Console screens. Have this guide open to this chapter as you proceed.

Installing Connect Enterprise Server 6

Before installing Connect Enterprise Server

Before you begin the installation process, check that all the requirements listed in "Installation requirements" on page 3 are satisfied. To install Connect Enterprise Server, you need a license number. You should have received an e-mail from Adobe with a link to a web site that provides the license number.

Install Connect Enterprise Server

1 Close all applications.

2 Insert the installation CD into the CD-ROM drive. On the splash screen click the Adobe Connect Enterprise Server 6 Install button.

If the installer does not start automatically, double-click the setup.exe file in the installation CD's root folder.

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 Connect Enterprise Server is already installed on this computer, the Update Existing Connect Enterprise Server Install screen appears. Select the check box to confirm you've backed up your database and the Connect Enterprise Server 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:\MSSQL), 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 and click Next.
- If the installer detects that the embedded database engine or Microsoft SQL Server is already installed on this computer, a dialog box appears to tell you that the embedded database engine will not be 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 uninstalled 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, click Next to accept the default location of the Start Menu shortcuts (Adobe Connect Enterprise Server), or click Browse to select a different location, and then click Next.

10 In the Ready To Install dialog box, review the location where Connect Enterprise Server will be installed and where the Start Menu folder will be installed. 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 Enterprise Server service screen, do one of the following:

- Select Start Connect Enterprise Server to launch the Application Management Console wizard to continue configuring Connect Enterprise Server. Click Next.
- Select Do Not Start Connect Enterprise Server Now. Click Next.

13 If you started Connect Enterprise Server, a message reports that the application service is starting.

Connect Enterprise Server runs as three Windows services: Adobe Connect Enterprise Server, Flash Media Server, and Flash Media Administration Server.

14 On the Completing the Adobe Connect Enterprise Server Setup Wizard screen, click Finish.

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

Configuring Connect Enterprise Server with the Application Management Console wizard

After installing Connect Enterprise Server, 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 > All Programs > Adobe Connect Enterprise Server > Configure Adobe Connect Enterprise Server 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 Connect Enterprise Server. The default value is 1433. (If you're using the embedded database engine, the default value is 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 Connect Enterprise account, such as "Connect Enterprise 6 account".

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

HTTP Port The port Connect Enterprise 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 Connect Enterprise account.

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

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 Connect Enterprise 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 Connect Enterprise 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 Connect Enterprise Server. 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 Connect Enterprise Server and any external volumes. Before configuring this feature, see "Configuring shared storage" on page 35.

4. Upload your license file.

Connect Enterprise Server is not enabled until you download a license file from Adobe and install it on the computer hosting Connect Enterprise Server. 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 Connect Enterprise Server installation.

5. Create an account administrator.

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

6. Continue using Connect Enterprise Server.

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 Connect Enterprise Server), return to the Application Management Console (to change or review settings), or consult the documentation to learn more about Connect Enterprise Server.

Start and stop Connect Enterprise Server

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

Stop Enterprise Server from the Start menu

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

Start Enterprise Server from the Start menu

1. Choose Start > All Programs > Adobe Connect Enterprise Server > Start Adobe Connect Meeting Server.
2. Choose Start > All Programs > Adobe Connect Enterprise Server > Start Adobe Connect Enterprise Server.

Stop Enterprise Server from the Services window

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

Start Enterprise Server 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 Server service.

Stop Enterprise 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 Connect Enterprise Server:

```
net stop BreezeApp
```

3. Enter the following to stop Macromedia Flash Media Server from Adobe:

```
net stop FMS
```

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

```
net stop FMSAdmin
```

Start Enterprise 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 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 Connect Enterprise Server:

```
net start BreezeApp
```

Uninstall Connect Enterprise Server

1 Stop the Connect Enterprise Server services in the following order: Flash Media Server (FMS), Flash Media Server Administration Server, Adobe Connect Enterprise Server.

2 Select Start > All Programs > Adobe Connect Enterprise Server > Uninstall Adobe Connect Enterprise Server.

3 Delete the root Connect Enterprise Server folder. By default, the location is c:\breeze.

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

4 (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.

Installing Connect Edge Server 6

Before installing Connect Edge Server

Before you begin the installation process, check that all the requirements listed at www.adobe.com/go/connect_sysreqs_en are satisfied. To install Connect Edge Server 6, you need a license number. You should have received an e-mail from Adobe with a link to a web site that provides the license number.

See also

"Choosing to deploy edge servers" on page 14

Install Connect Edge Server

1 Close all other applications.

2 Insert the Connect Enterprise Server 6 installation CD into the CD-ROM drive.

If the Connect Enterprise Server 6 installer does not start automatically, double-click the edgesetup.exe file in the installation CD's root folder.

3 On the splash screen, click the Adobe Connect Edge Server 6 Install button.

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

5 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 Connect Edge Server is already installed on this computer, the Update Existing Connect Edge Server Install screen appears. Click Next.

6 Accept the default shortcut, or click Browse to select a different location, and then click Next.

7 On the Select Start Menu Folder screen, click Next to accept the default location of the Start Menu shortcuts (Adobe Connect Edge Server), or click Browse to select a different location, and then click Next.

8 In the Ready To Install dialog box, review the location where Connect Enterprise 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 Connect Edge Server installation.

See also

"Deploying Connect Edge Server 6" on page 24

Install the Connect Edge Server license file

When your order for Connect Edge Server is processed, Adobe sends you an e-mail message with the Connect Edge Server license file attached.

1 Open the e-mail message from Adobe.

2 Save the license file to the licenses folder: *[root_install_dir]*\edgeserver\win32\licenses. By default, the root installation directory is c:\breeze.

3 Stop and start Connect Edge Server to verify that the installation was successful.

Start and stop Connect Edge Server

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

Stop Edge Server from the Start menu

❖ Choose Start > All Programs > Adobe Connect Edge Server > Stop Adobe Connect Edge Server.

Start Edge Server from the Start menu

❖ Choose Start > All Programs > Adobe Connect Edge Server > Start Adobe Connect Edge Server.

Stop Edge Server from the Services window

1 Choose Start > 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 Edge Server from the Services window

1 Choose Start > 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 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 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 Connect Edge Server

1 Stop the Connect Edge Server services in the following order: Flash Media Server (FMS), Flash Media Server Administration Server.

2 Select Start > All Programs > Adobe Connect Edge Server > Uninstall Adobe Connect Edge Server.

3 Delete the root folder. By default, the location is c:\breeze.

Chapter 4: Deploying and configuring Connect Enterprise

This chapter describes the series of deployment and configuration tasks that you complete after you install Adobe Connect Enterprise Server or Adobe Connect Edge Server and complete the first phase of configuring Connect Enterprise with the Application Management Console.

Deploying Connect Enterprise Server 6

Deploy Connect Enterprise Server

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

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

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

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 Connect Enterprise Server 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 Connect Enterprise Server, contact Adobe Support at www.adobe.com/go/connect_licensed_programs_en.

Deploy Connect Enterprise Server in a cluster

Before you deploy Connect Enterprise Server in a cluster, you should perform a successful installation on a single computer. You should also 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.

This procedure assumes you are migrating from a successful single-server installation to a multi-server installation.

1 Install SQL Server on a dedicated server (or verify that it has been installed).

If you install Connect Enterprise Server in a cluster, you must use Microsoft SQL Server 2000 or 2005 as the database engine and not the embedded database engine. This is because each server hosting Connect Enterprise Server must be able to access the database, but licensing restrictions do not allow more than one server to access the embedded database engine.

2 Install and configure Connect Enterprise Server on a dedicated server.

Use the same serial number and license file each time you install Connect Enterprise Server.

Note: *You must have a special cluster license file that supports the number of nodes in your cluster. For more information, contact your Adobe representative.*

3 Choose Start > All Programs > Adobe Connect Enterprise Server > Configure Adobe Connect Enterprise Server to open the Application Management Console. On the Database Settings screen, verify that Database Host points to the server hosting SQL Server.

All the database settings must match the values set for your single-server installation.

4 On the Server Settings screen of the Application Management Console, set Host Mappings External Name to the FQDN of the computer you're adding to the cluster.

5 Confirm that Connect Enterprise Server is working correctly.

6 Set up a load balancer on the network and configure it to listen on port 80. Each Connect Enterprise application server should listen on port 8080.

Set the application server ports on the Server Settings screen in the Application Management Console. Enter the value in the HTTP Port field.

To configure the load balancer, see the vendor documentation.

7 Include the server in the cluster in the load-balanced pool.

For specific instructions on how to include a server in the load-balanced pool, see the vendor documentation.

8 Repeat steps 2 though 7 for each server in the cluster.

9 If you're using shared storage, copy all content from the original server to the shared storage volume.

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

See also

"Installing Connect Enterprise Server 6" on page 16

"Configuring shared storage" on page 35

Deploying Connect Edge Server 6

Connect Edge Server installation workflow

1. Design edge server zones.

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

2. Install Adobe Connect Edge Server.

Install Connect Edge Server on each computer in each zone. For example, if you have a cluster of edge servers in a zone, install Connect Edge Server on each computer in the cluster. See "Installing Connect Edge Server 6" on page 20.

3. Modify the DNS server for each zone.

Map the FQDN of the origin Connect Enterprise Server to the static IP address of Connect Edge Server in each zone. See "Deploying Connect Edge Server 6" on page 24.

4. Configure the edge server.

You must add configuration parameters to the custom.ini file on each server hosting Connect Edge Server. See "Deploying Connect Edge Server 6" on page 24.

5. Configure the origin server.

You must add configuration parameters to the custom.ini file on each server hosting Connect Edge Server. Also, you must set the External Name of the edge server in the Application Management Console on the origin server. See "Deploying Connect Edge Server 6" on page 24.

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 Connect Edge Server

Before you deploy edge servers, you should have Connect Enterprise 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 to the static IP address of the edge server.*

2 On Connect Edge Server, open the file *[root_install_dir]*\edgeserver\win32\conf\HttpCache.xml and replace `${%COMPUTERNAME%}` in the HostName tag with the FQDN of the edge server computer, for example, edge1.example.com.

```
<!-- The real name of this host. -->
<HostName>${%COMPUTERNAME%}</HostName>
```

3 On Connect Edge Server, if there is a custom.ini file in the root directory (c:\breeze, by default), delete it.

4 In a text editor, such as Notepad, create a new text file named custom.ini. Set values for the following parameters in the file and save it:

FCS.HTTPCACHE_BREEZE_SERVER_NORMAL_PORT The IP address or domain name and port number of the computer where Connect Enterprise Server is installed, for example, `myConnectServer:80`. Connect Edge Server connects to Connect Enterprise Server at this location.

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

FCS_EDGE_REGISTER_HOST The FQDN of the Connect Enterprise Server (the origin server), for example, `FCS_EDGE_REGISTER_HOST=connectserver.example.com`.

FCS_EDGE_CLUSTER_ID The name of the cluster. Each edge server cluster, or *zone*, 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=adobe-apac`.

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

FCS_EDGE_EXPIRY_TIME 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.

FCS_EDGE_REG_INTERVAL 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.

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.

DEFAULT_FCS_HOSTPORT (Optional) To configure the edge server ports, add the following line to the custom.ini file: `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.*

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

6 In the custom.ini file on the origin server, map the value of the `FCS_EDGE_CLUSTER_ID` parameter to a zone ID and save the file. This authorizes the edge zone. The syntax is `edge.cluster-id=zone-id`.

Each edge server cluster should have a zone ID. A zone ID can be any positive integer greater than 0. For example, you could have four clusters mapped to zones 1 to 4:

```
edge.adobe-emea=1
edge.adobe-apac=2
edge.adobe-sf=3
edge.adobe-boston=4
```

Note: *Even if you are only deploying one Connect Edge Server, you must map the cluster ID name to a zone ID.*

7 If you set an `FCS_EDGE_PASSWORD` parameter on the edge server, set the same password in the custom.ini file on the origin server and save the file.

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 5-8 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 edge servers" on page 14

Integrating Connect Enterprise with a directory service

Directory service integration overview

If your company uses a directory server, you can integrate it with Connect Enterprise to avoid manually adding individual users and groups. User accounts are created automatically in Connect Enterprise through manual or scheduled synchronizations with your company's directory.

To integrate with Connect Enterprise, 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.

Connect Enterprise connects as an LDAP client to an LDAP directory, imports users and groups, and ensures that information about these users and groups in the database is kept synchronized with the external LDAP directory.

Adobe has tested directory service integration with the following LDAP servers:

- Active Directory Application Mode (ADAM) SP1
- Active Directory (Windows Server 2003 and Windows Server 2000)
- IBM Directory Server 5.2
- Novell eDirectory 8.7.3 for Win32
- OpenLDAP 2.3.19
- Sun One Directory Server 5.2 for Win32
- Netscape 6.02 for Win32

There are several important concepts to understand before configuring and performing a directory service integration. These concepts are explained in the following sections. If you have experience with LDAP directory structure and LDAP integration, you may want to go directly to "Integrating Connect Enterprise with an LDAP directory" on page 28.

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 Connect Enterprise, 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. This attribute defines the rules and required attributes for that entry.*

Working with internal and external users and groups

Users and groups that you create directly in Connect Enterprise rather than importing them from an LDAP directory are called *internal* users and groups. Users and groups imported into the Connect Enterprise 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. For example, if you want to add all the users in the Singapore office to a Presentation user group, you can assign them to this internal group even if it has other users who have not been imported through synchronization.

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.

Integrating Connect Enterprise with an LDAP directory

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

Note: *If you're integrating with a secure LDAP server (LDAPS), import a server certificate into Connect Enterprise Server before beginning. See "Configure LDAPS" on page 34.*

1. Open the Application Management Console.

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

2. Enter LDAP server connection settings.

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

Field	Default value	Description
LDAP Server URL	No default.	Usual form is `ldap://[servername:portnumber]`. If your organization uses a secure LDAP server, use `ldaps://`.
LDAP Connection Authentication Method	No default.	The mechanism for transmitting the LDAP user name and password over the network: Anonymous: No password Simple: Transmit password as clear text Digest MD5: More secure mechanism for transmitting password
LDAP Connection Username	No default.	Administrative login.
LDAP Connection Password	No default.	Administrative password is hidden.
LDAP Query Timeout	No default.	Time that can elapse before the query is canceled, in seconds. If you leave the field blank, there is no timeout.
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 will be retrieved from the server in multiple pages. For example, if you were integrating a large LDAP directory that could only display 1000 users and there were 2000 users to import, the integration would fail. 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://mycompany.com:636
UserName:MYCOMPANY\jdoe
Password:password123
Query timeout:(empty)
Authentication mechanism:Simple
Query page size:1000
```

3. Map Connect Enterprise 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 integrates Active Directory with Connect Enterprise Server. An LDAP user entry is mapped to a Connect Enterprise user profile and Network Login is a custom field.

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

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 sub-branches of the branch you specified in step 2, select True from the Subtree Search menu; otherwise, select False.

For more information, see "About LDAP directory structure" on page 27.

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 Connect Enterprise and LDAP directory group profiles.

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

Note: *Connect Enterprise 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 Connect Enterprise 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 sub-branches of the branch you specified in step 2, select True from the Subtree Search menu; otherwise, select False.

For more information, see "About LDAP directory structure" on page 27.

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. 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 32.

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

8. 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 31.

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

9. 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 32.

Managing passwords

When Connect Enterprise imports user information from an external directory, it does not import the user's network password. Therefore, you need to implement another method for managing passwords for users imported into the Connect Enterprise directory.

Single sign-on

The recommended method for managing passwords and authentication for imported users is to use single sign-on. Single sign-on allows a user who is logged in to an organization's network to gain access to Connect Enterprise (and other resources for which the user has permission) without having to log in again.

If you plan to use single sign-on authentication, set the authentication policy for directory service integration to Do Nothing in the Directory Service Integration Policy Settings screen.

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 that user's directory entry. 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.

See also

"Single sign-on" on page 37

Recommended practices for synchronization

As an administrator, you can synchronize Connect Enterprise 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 Connect Enterprise 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 Connect Enterprise Server.*

Scheduled synchronizations

Scheduled synchronizations are recommended because they ensure that Connect Enterprise 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, your initial synchronization of the Connect Enterprise directory with the external LDAP directory 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, Connect Enterprise compares LDAP directory entries to Connect Enterprise directory entries and imports only those entries that contain at least one changed field.

Previewing the synchronization

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

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

Log file values

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

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

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

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

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

delete	The principal was deleted from Connect Enterprise.	
up-to-date	The principal is an external principal in Connect Enterprise and is already synchronized with the external directory. No changes were made.	A user or group created in Connect Enterprise 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 Connect Enterprise 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.

Configure LDAPS

You can configure Connect Enterprise Server to encrypt communication to and from a secure LDAP server. Connect Enterprise Server does not encrypt such communication by default.

Use the Java keytool utility to import the LDAP server's certificate into the trust store of the Connect Enterprise Server Java virtual machine (JVM). If the server certificate is in PEM (Privacy Enhanced Mail) format, the certificate needs to be converted into DER-encoded or Base64-encoded format. (DER stands for Distinguished Encoding Rules.)

See also

"Start and stop Connect Enterprise Server" on page 19

Convert the certificate from PEM format to DER format

1 Install OpenSSL (if it is not installed yet).

Note: *OpenSSL is a third-party toolkit you can download online.*

2 Run the following command:

```
openssl x509 -in [original certificate filename and path].pem -out [target filename and path].der
```

Import an LDAP server certificate

1 To copy (export) the LDAP server's certificate file to the computer hosting Connect Enterprise Server, locate the trust store used for the server instance. For a default installation, the trust store is located here: *[root_install_dir]*/appserv/win32/jre/lib/security/cacerts.

Note: *[root_install_dir] refers to the root directory of your Connect Enterprise Server installation which is c:\breeze, by default.*

2 To import the LDAP server's certificate into the trust store, open a command prompt to the trust store directory. For a default installation, this is the *[root_install_dir]*/appserv/win32/jre/lib/security directory.

3 Enter the following command, which supplies the path (relative or fully qualified) to your LDAPS server's certificate file and the trust store file location: ***[root_install_dir]/appserv/win32/jre/bin/keytool -import -alias [nickname for cert] -file [cert filename and path] -keystore [trustStore filename and path] -storepass [trustStore password]***

The following is an example of a valid command:

```
keytool -import -alias ldapServerCert -file C:\Certs\ldapservercert.der -keystore cacerts -storepass
changeit
```

Note: *The default trust store password is* `changeit`*. You should change this password to increase file security.*

4 If the LDAPS server's certificate was created by an unknown certificate authority (for example, a self-signed certificate), you are prompted to verify the certificate's information and confirm the import.

5 Restart Connect Enterprise Server.

Configuring shared storage

About shared storage

You can use the Application Management Console to configure Connect Enterprise Server to use NAS and SAN devices to manage content storage. Content is any file published to Connect Enterprise, 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 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 Connect Enterprise Server cluster and don't configure shared storage devices, the cluster works in full mirroring mode (content published to Connect Enterprise Server 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 Connect Enterprise 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 6

"Deploy Connect Enterprise Server in a cluster" on page 23

Configure shared storage

Connect Enterprise Server 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 Connect Enterprise Server to use shared storage volumes, you must copy the content from one of the existing servers to the shared volume.

a Stop Connect Enterprise Server (Start > All Programs > Adobe Connect Enterprise Server > Stop Adobe Connect Enterprise Server and Stop Adobe Connect Meeting Server).

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

Some computers in a cluster may have extra content. Connect Enterprise 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 Connect Enterprise Server (Start > All Programs > Adobe Connect Enterprise Server > Start Adobe Connect Meeting Server and Start Adobe Connect Enterprise Server).

3 On Connect Enterprise Server, choose Start > Control Panel > Administrative Tools > Services to open the Services window, select Adobe Connect Enterprise Server, 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 Connect Enterprise Server (application server only).

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

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

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

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

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

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

Configure shared storage for additional servers in a cluster

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

2 On Connect Enterprise Server, choose Start > Control Panel > Administrative Tools > Services to open the Services window, select Adobe Connect Enterprise Server, 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 Connect Enterprise Server.

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

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

4 (Optional) If you are installing Connect Enterprise Server for the first time, follow the steps in "Deploy Connect Enterprise Server in a cluster" on page 23.

5 Click Save and close the Application Management Console.

Chapter 5: Configuring advanced features

Adobe Connect Enterprise Server 6 supports technology that lets you integrate Connect Enterprise with your existing infrastructure and adhere to your organization's security policies.

Single sign-on

Choosing a single sign-on mechanism

Single sign-on (SSO) 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 Adobe Connect Enterprise. If you've integrated Connect Enterprise with an LDAP directory, single sign-on is useful for managing passwords and authenticating imported users.

You must choose one of the following two single sign-on mechanisms:

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

Microsoft NT LAN Manager (NTLM) authentication Configure NTLM to pass authentication credentials to Connect Enterprise. Only Microsoft Internet Explorer on Microsoft Windows can negotiate NTLM authentication without prompting the user for credentials.

Note: *NTLM2 and Kerberos are not supported.*

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, Connect Enterprise login requests are routed to an agent positioned between the client and Connect Enterprise Server. 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 Connect Enterprise Server. On Connect Enterprise Server, 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 Connect Enterprise Server" on page 19

Configure HTTP header authentication on Connect Enterprise Server

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

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 Connect Enterprise:

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

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

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 Connect Enterprise. The name of the header must be *`header_field_name`*.

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

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

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

1 Set the value of the *`header_field_name`* header field to a Connect Enterprise user login.

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

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

The Java filter on Connect Enterprise Server 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 Connect Enterprise Server response for the string `"OK"` to indicate a successful authentication.

4 Parse the Connect Enterprise Server response for the `BREEZESESSION` cookie.

5 Redirect the user to the requested URL on Connect Enterprise Server, 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 Connect Enterprise Server 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 Connect Enterprise Server.

2 Choose Start > All 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 Connect Enterprise:

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

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

4 On the computer hosting Connect Enterprise Server, 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 Connect Enterprise:

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

b Choose Start > All Programs > Adobe Connect Enterprise Server > Start Adobe Connect Enterprise 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>
-->
```

Configure NTLM authentication

NTLM is a challenge/response protocol that enables a client to prove its identity without providing a password. The web browser queries an NTML authentication server for the user's credentials. The NTLM routine is hidden from the user.

In order for users to use single sign-on with NTLM authentication, they must use Internet Explorer on Windows.

See also

"Start and stop Connect Enterprise Server" on page 19

Add configuration parameters

1 Stop Connect Enterprise:

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

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

2 Add the following parameter to the custom.ini file in the root installation directory:

```
NTLM_DOMAIN=[domain]NTLM_SERVER=[NTLM_server_IP_address]
```

In the above code, *[domain]* is the name of the NT domain, such as acme.com, that users authenticate against. The value *[NTLM_server_IP_address]* is the IP address of the NTLM authentication server. The numeric IP address must be used with NTLM_SERVER; the host name does not work.

3 Save the custom.ini file and restart Connect Enterprise:

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

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

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

a Uncomment the NtlmAuthenticationFilter mapping.

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

b Comment out the HeaderAuthenticationFilter filter mapping.

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

Reconcile login policies

Connect Enterprise and NTLM have different login policies for authenticating users. These policies must be reconciled before users can employ a single login.

The NTLM protocol uses a login identifier that can be a user name (jdoe), an employee ID number (1234), or an encrypted name, depending on the organization's policy. By default, Connect Enterprise uses an e-mail address (jdoe@mycompany.com) as a login identifier. You can configure Connect Enterprise so that a unique identifier is shared between NTLM and Connect Enterprise.

1 Open Connect Enterprise Manager.

To open the Connect Enterprise Manager, open a browser window and enter the FQDN of the Connect Enterprise Host (for example, http://connect.examplecompany.com). You entered the Connect Enterprise Host value on the Server Settings screen of the Application Management Console.

2 Select the Administration tab, then click Users and Groups, then click Edit Login and Password Policies.

3 In the Login Policy section, select No for Use e-mail address as the login.

Public key infrastructure

About public key infrastructure (PKI)

You can set up a public key infrastructure (PKI) to manage identification credentials as part of your Connect Enterprise 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 in X.509 format (also called a *public key*) to that client. When a client connects to Connect Enterprise Server, 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 Connect Enterprise Server.

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 should use the add-in stand-alone installer to install the add-in before joining a meeting.

Clients may 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.

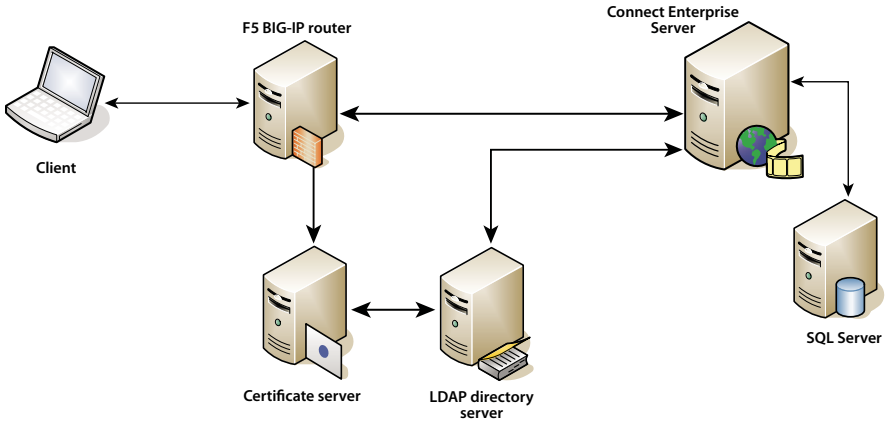
You can design a PKI system to require authentication for only HTTP connections or for both HTTP and RTMP connections. If you require client-side certificates on both HTTP and RTMP connections, users are prompted each time a new server connection is established. For example, there will be two prompts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

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:

- Connect Enterprise Server is installed.
- Connect Enterprise Server is integrated with an LDAP directory service.
- A user imported from the LDAP directory service can enter a meeting served by Connect Enterprise.
- 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 that Connect Enterprise uses to authenticate the user.

Note: *This example uses the* `email` *attribute, but you could use any unique identifier that is exposed by the X.509 format, has a length of 254 characters or less, and is shared by the LDAP directory service and Connect Enterprise.*

2. Set the Connect Enterprise login policy.

Connect Enterprise should use an e-mail address for user login. In Enterprise Manager, select the Administration tab, then click Users and Groups, the click Edit Login and Password Policies.

3. Configure a CA server.

The CA (Certification Authority) server handles requests for certificates, verifies client identities, issues certificates, and manages a CRL (client revocation list).

In this implementation, the CA points to the LDAP directory server to obtain a client certificate. The CA queries the LDAP server for the client information and, if it exists and hasn't been revoked, formats it into a certificate.

Verify that the client certificate is installed and usable by looking at the subject field. It should look something like this:

```
E = adavis@asp.sflab.macromedia.com
CN = Andrew Davis
CN = Users
DC = asp
DC = sflab
DC = macromedia
DC = com
```

4. Configure Connect Enterprise Server 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>
```

Choose Start > All Programs > Adobe Connect Enterprise Server > Stop Adobe Connect Enterprise Server and Stop Adobe Connect Enterprise Meeting Server to stop the server. In the custom.ini file in the root installation directory, add the following line:

```
HTTP_AUTH_HEADER=hah_login
```

Save the custom.ini file and restart Connect Enterprise.

5. Configure the F5 application logic.

The application logic in F5 parses the subject field of the client certificate for the e-mail address and passes it to Connect Enterprise in an additional HTTP header.

A client that doesn't have a certificate is rejected. If a client has a certificate, the certificate must be authenticated. Example authentication mechanisms are OCSP (Online Certification Status Protocol) and LDAP lookup.

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

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

If the request doesn't include the `session` string or `BREEZESESSION` cookie, the user needs to "log in" to Connect Enterprise. 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 Connect Enterprise login page.

The following code is an F5 iRule placed on the HTTPS profile that handles requests:

```
set id [SSL::sessionid]
set the_cert [session lookup ssl $id]
set uname [X509::subject $the_cert]
set emailAddr [getfield $uname "emailAddress=" 2]
if { [HTTP::cookie exists BREEZESESSION] } {
    set cookie_payload [HTTP::cookie value BREEZESESSION]
}
elseif { [HTTP::uri] contains "/system/login" }
{
    # Connection has been redirected to the "login page"
    # The email address has been parsed from the certificate
    #
    HTTP::header insert hah_login $emailAddr
}
elseif { [HTTP::uri] contains "session" }
{
    #do nothing, Connect Enterprise verifies the token found in session=$token
}
else
{
    # URI encode the current request, and pass it to
    # the Connect Enterprise 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 Connect Enterprise Server" on page 19

"Configure HTTP header authentication" on page 37

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 Professional.

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 Connect Enterprise language XML files on the server hosting Connect Enterprise: *[root_install_dir]*\appserv\web\common\intro\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 Connect Enterprise language XML files on the server hosting Connect Enterprise: *[root_install_dir]*\appserv\web\common\intro\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 Connect Enterprise 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 Connect Enterprise Server (/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 Connect Enterprise language XML files on the server hosting Connect Enterprise: *[root_install_dir]*\appserv\web\common\intro\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.

Custom whiteboard stamps

About whiteboards

You can use a whiteboard in Acrobat Connect Professional to create text, lines, circles, squares, and other free-hand drawings in real time during a meeting.

The whiteboard includes stamps that let you leave a check mark, arrow, star, or cross on the screen. A check mark is the default stamp. You can change the stamp image by clicking the check mark, arrow, and star buttons. You can customize image color and shape size by using the color picker and size pop-up menu. You can also create your own custom stamps.

Creating custom stamps

To create custom stamps for the whiteboard tool, you create a library of movie clip symbols in Macromedia Flash by Adobe. Create an ActionScript (.as) file and write code to link the label of each stamp to its movie clip symbol. Publish the custom stamp library as a SWF file and copy the SWF file and the AS file to Connect Enterprise Server.

For more information, see the article "Creating Custom Whiteboard Stamps for Connect Enterprise" on the Adobe Connect Enterprise Developer Center (www.adobe.com/go/devnet_connect_stamps).

Chapter 6: Verifying your installation

This chapter contains tasks that help you verify that Adobe Connect Enterprise Server was installed successfully. Some tasks are only applicable if you have a license for a particular Connect Enterprise module.

Installation verification tasks

Verify database connectivity

If you can log in to Adobe Connect Enterprise Manager (a web application within Connect Enterprise Server), the database and Connect Enterprise Server can function together.

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

Note: *In this URL, [hostname] is the value you set for Connect Enterprise 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 Enterprise Manager 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, Connect Enterprise Server will not send out e-mail notifications and you can skip this section.

1 Click the Administration tab on the Connect Enterprise Manager 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, Connect Enterprise Server 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 Connect Enterprise with a valid SMTP host, and make sure the SMTP service works outside Connect Enterprise.

d Contact Adobe Support at www.adobe.com/go/connect_licensed_programs_en.

Verify that you can use Presenter

To verify that you can use Connect Enterprise Server, send a Microsoft PowerPoint presentation to Connect Enterprise Server for compilation into a Flash presentation, and then view it.

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

1 Insert the Adobe Connect Enterprise CD.

2 Click Install Adobe Presenter 6 and follow the prompts.

3 If you do not have a PowerPoint presentation that you can send to Connect Enterprise Server for compilation into a Flash presentation, create and save a presentation of one or two slides.

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

5 Select Connect Enterprise Server 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 the Connect Enterprise Manager).

When you complete the steps in the Publish wizard, your PowerPoint presentation is uploaded to the Connect Enterprise Server and compiled into a Flash presentation.

7 When the compilation is complete, go to the Content tab in Connect Enterprise Manager and search for your presentation.

8 Open your presentation to view it.

Verify that you can use Training

Note: *Adobe Connect Training 6 is an optional feature that must be enabled in your license.*

❖ Go to the Training tab in Connect Enterprise Manager.

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 Acrobat Connect Professional

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

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

1 Log in to Connect Enterprise Manager 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 Professional is functional.

Verify that you can use Seminars

Note: *Acrobat Connect Professional Seminars is an optional feature that must be enabled in your license.*

1 Log in to Connect Enterprise Manager as a user who is enrolled in the Seminar Hosts group or the Administrators group.

2 In Connect Enterprise Manager, click the Seminar Rooms tab.

3 Create or browse to a folder in the Seminar library and click New Seminar.

4 On the Enter Meeting Information page, enter the required information. For the Seminar Access option, select Only Registered Users And Accepted Guests May Enter The Room, and then click Finish.

5 Click the Seminar URL.

6 Log in to enter the seminar as a registered user.

If the seminar room opens, the seminar feature is functional.

Verify that you can use Events

Note: *Adobe Connect Events 6 is an optional feature that must be enabled in your license.*

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

2 Go to the Event Management tab in Connect Enterprise Manager.

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

Verify cluster load balancing and meeting failover

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.

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

The following procedure assumes that the cluster contains two computers, Computer1 and Computer2.

1 Start Connect Enterprise Server on both computers.

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

b Select Start > Programs > Adobe Connect Enterprise Server > Start Adobe Connect Enterprise Server

2 Log in to Connect Enterprise Manager from the following URL:

http://*[hostname]*

For *hostname*, use the Connect Enterprise 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 Connect Enterprise Server on Computer2.

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.

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

5 In Connect Enterprise Manager, click on any tab or link.

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

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

See also

"Choosing to deploy Connect Enterprise in a cluster" on page 12

Verify content replication

It's a good idea to verify that content uploaded to one Connect Enterprise Server in a cluster is replicated to the other computers in the cluster. The following procedure assumes that the cluster contains two computers on which Adobe Presenter is installed, Computer1 and Computer2.

1 Start Connect Enterprise Server on Computer1.

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

b Select Start > Programs > Adobe Connect Enterprise Server > Start Adobe Connect Enterprise Server

2 Stop Connect Enterprise Server on Computer2.

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.

3 Log in to Connect Enterprise Manager from the following URL:

http://*[hostname]*

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

4 Upload a JPEG image or other content to Connect Enterprise Server 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 Enterprise Manager.)
- 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 Connect Enterprise 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.

See also

"Choosing to deploy Connect Enterprise in a cluster" on page 12

Chapter 7: Securing Connect Enterprise

Securing Adobe Connect Enterprise protects your organization against loss of property and malicious acts. It is important to secure your organization's infrastructure, Adobe Connect Enterprise Server, and the database server used by Connect Enterprise Server. You may also choose to configure SSL so that all connections to Connect Enterprise Server are secure; for more information, see www.adobe.com/go/connect_ssl_en. Connect Enterprise also supports PKI; for more information, see "Public key infrastructure" on page 41.

Securing the infrastructure

Network security

Connect Enterprise Server relies on several private TCP/IP services for its communications. These services open several ports and channels that must be protected from outside users. Connect Enterprise Server requires that you place sensitive ports behind a firewall. The firewall should support stateful packet inspection (not just 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 Connect Enterprise 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 Connect Enterprise Server on your intranet, you should place the Connect Enterprise servers and the Connect Enterprise Server database in a separate subnet, separated by a firewall. The internal network segment where Connect Enterprise Server 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 take into consideration all Connect Enterprise Server ports and whether they are configured for inbound or outbound traffic.

Internet access

If you intend to have users access Connect Enterprise Server on the Internet, it is extremely important that you separate the Connect Enterprise servers from the Internet with a firewall. If you do not take the necessary steps to secure the Connect Enterprise servers, you are leaving your valuable information available for anyone to steal.

Database server security

Whether or not you are hosting your database on the same server as Connect Enterprise Server, you must 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 organization's 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 2000 and 2005 and the embedded database engine, see the Microsoft SQL security website.

For a list of steps to help you secure your database, see the Microsoft article "10 Steps to Help Secure SQL Serve 2000".

Securing Connect Enterprise Server

Create service accounts

Creating a service account for Connect Enterprise lets you run Connect Enterprise more securely. Adobe recommends creating a Connect Enterprise Server service account and an MSDE service account. 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 Connect Enterprise service account

1 Create a local account called ConnectService that doesn't include any default groups.

2 Set the Adobe Connect Enterprise Server 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 Connect Enterprise folder path (c:\breeze, by default).

Subfolders and files must have the same permissions. For clusters, you must 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, you must 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 Connect Enterprise Server on a single computer. It assumes that the database is to be installed on the same computer, and that users will access Connect on the Internet.

1. Install a firewall.

Since you are allowing users to access Connect Enterprise Server 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 Connect Enterprise, you do not need to open port 1434 on the firewall.

3. Install Connect Enterprise Server.

4. Verify that the Connect Enterprise Server applications are working.

After installing Connect Enterprise Server, you should verify that Connect Enterprise Server is working properly both from the Internet and from your local network.

5. Test the firewall.

After you have installed and configured the firewall, you should verify that your firewall is working correctly. Test the firewall by attempting to use the blocked ports.

See also

"Verifying your installation" on page 47

Securing clusters

Clusters (multi-server) systems are inherently more complex than single-server configurations. A Connect Enterprise Server cluster can be located at a data center or geographically distributed across multiple network operation centers. You can install and configure servers hosting Connect Enterprise Server 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 Connect Enterprise system. This approach offers a high level of security.

Local software firewalls For the Connect Enterprise 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 where there are multiple computers hosting Connect Enterprise Server 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. Connect Enterprise relies on this external security if data traffic must be encrypted.

Security tips and resources

Security best practices

The following checklist describes best practices that will help you secure your Connect Enterprise Server system.

Use SSL to protect network traffic For more information, see www.adobe.com/go/connect_ssl_en.

Run only the services you need You should not run applications such as a domain controller, a web server, or an FTP server on the same computer as Connect Enterprise Server. By reducing the number of applications and services running on the computer that hosts Connect Enterprise Server, you can minimize the chances that another application can be used to compromise the server.

Update operating system security Check regularly for critical updates that close security holes and apply the required patches. Some of these security problems are eliminated by a firewall. In general, you should 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. Connect Enterprise Server relies on the safety of the host system against intruders, so servers should be kept secured when private and confidential data is at risk. Connect Enterprise Server is designed to take advantage of native environmental features such as file system encryption.

Use strong passwords Connect Enterprise users are protected by passwords. Users, and particularly administrators, should choose strong passwords to keep their data safe. Connect Enterprise Administrators can set login and password policies in the Connect Enterprise Manager. Connect Enterprise Server 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 may help you secure your servers.

Network security The SANS (System Administration, Networking, and Security) Institute is a cooperative research and education organization comprising 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 2000. 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. Connect Enterprise Server 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 Connect Enterprise Server.*

Index