

ADOBE® CONNECT™ ENTERPRISE

TECHNICAL OVERVIEW



© 2007 Adobe Systems Incorporated. All rights reserved.

Adobe® Connect™ Enterprise Technical Overview

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

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

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

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

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

Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Java is a trademark or registered trademark of Sun Microsystems, Inc. in the United States and other countries. All other trademarks are the property of their respective owners.

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

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

Notice to U.S. Government End Users. The Software and Documentation are “Commercial Items,” as that term is defined at 48 C.F.R. §2.101, consisting of “Commercial Computer Software” and “Commercial Computer Software Documentation,” as such terms are used in 48 C.F.R. §12.212 or 48 C.F.R. §227.7202, as applicable. Consistent with 48 C.F.R. §12.212 or 48 C.F.R. §§227.7202-1 through 227.7202-4, as applicable, the Commercial Computer Software and Commercial Computer Software Documentation are being licensed to U.S. Government end users (a) only as Commercial Items and (b) with only those rights as are granted to all other end users pursuant to the terms and conditions herein. Unpublished-rights reserved under the copyright laws of the United States. Adobe Systems Incorporated, 345 Park Avenue, San Jose, CA 95110-2704, USA. For U.S.

Government End Users, Adobe agrees to comply with all applicable equal opportunity laws including, if appropriate, the provisions of Executive Order 11246, as amended, Section 402 of the Vietnam Era Veterans Readjustment Assistance Act of 1974 (38 USC 4212), and Section 503 of the Rehabilitation Act of 1973, as amended, and the regulations at 41 CFR Parts 60-1 through 60-60, 60-250, and 60-741. The affirmative action clause and regulations contained in the preceding sentence shall be incorporated by reference.

Contents

Architecture	1
Enterprise Server components	2
Hosted and licensed solutions	5
Enterprise integration	7
Extensibility and custom integration	10
Connect Edge Server	11
Deploying servers in a cluster	14
Security	15
Requirements	18

Technical overview

Adobe® Connect™ Enterprise Server 6 is a rich web communication system that provides online meetings, training, and presentations that anyone can access through any web browser. Enterprise Server allows nontechnical subject matter experts to easily create communications that include voice, video, and animations, which participants view using Adobe® Flash® Player.

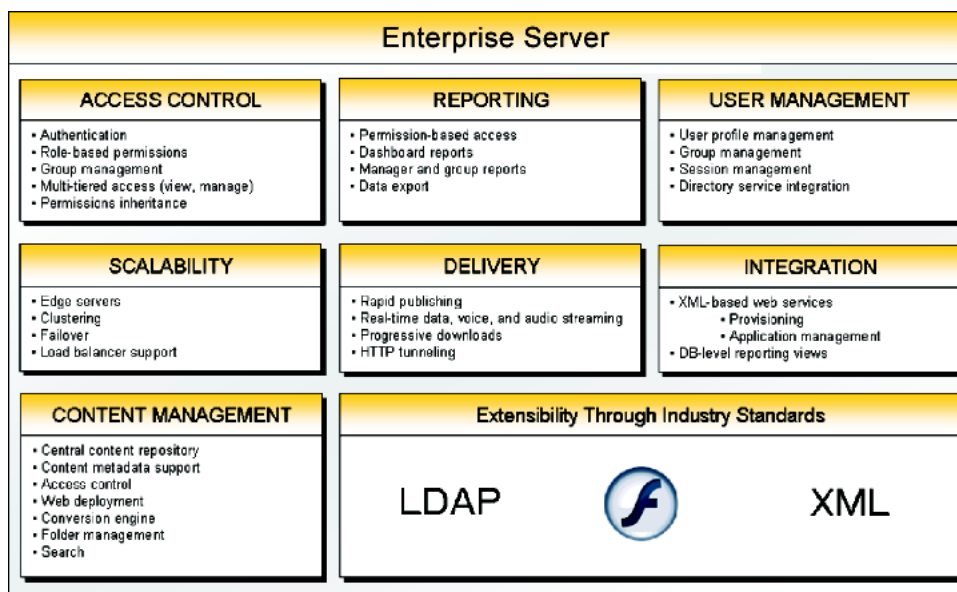
Architecture

Modular architecture

Enterprise Server uses a highly scalable, secure, and flexible architecture that enables people to collaborate in real time no matter where they are. Enterprise Server also allows people to access communications at their own convenience through on-demand presentations.

Enterprise Server offers enterprise-class scalability, with support for single-server or clustered environments, and it provides reliable redundant deployment that can support thousands of concurrent users. Furthermore, Enterprise Server is designed to be an open platform and can be extended and integrated with other systems through a comprehensive set of APIs.

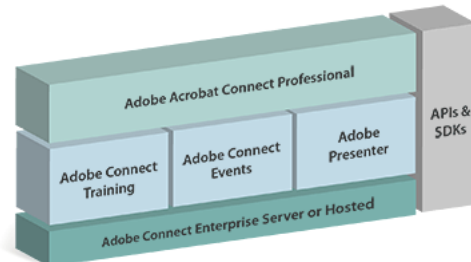
Enterprise Server uses industry-standard technologies, such as Java, C++, XML, XSLT, Flash, and ActionScript™, to deliver a solution for addressing current and future customer requirements.



Features of the Enterprise Server modular architecture

Application suite

Enterprise Server includes a suite of applications that can be combined to meet your needs. It also includes a web-based interface that lets you manage content, enroll in courses, start meetings, and so on.



Enterprise Server has four applications with features for training, events, presentations, and live meetings. You can also extend Enterprise Server and integrate it with other systems through its web services APIs and SDKs.

Adobe Acrobat Connect Professional Adobe® Acrobat® Connect™ Professional lets users conduct online meetings and seminars in which presenters can show multimedia presentations, share their screen, and broadcast live audio and video to participants in real time.

Adobe Connect Training Adobe® Connect® Training lets users create, manage, deploy, and track e-learning courses and curriculums complete with enrollment, assessments, surveys, learner management, and robust reporting.

Adobe Connect Events Adobe® Connect® Events lets users manage the full life cycle of large- or small-scale events, such as attendee qualification, registration management, reporting, and notification management.

Adobe Presenter Adobe® Presenter 6 is a plug-in application for Microsoft PowerPoint that lets users rapidly create e-learning content and high-quality multimedia on-demand presentations. Finished presentations are in the Macromedia® Flash® from Adobe (SWF file) format and are SCORM and AICC compliant.

Adobe Acrobat Connect Enterprise Manager Adobe® Acrobat® Connect™ Enterprise Manager is a web-based application that lets users and administrators manage account-related information and content. Use Enterprise Manager to create meetings, manage presentations, create curriculums and events, view and download reports, and more. For more information, see [Content access](#).

Enterprise Server components

Application server

The Connect Enterprise application server is built on J2EE, using select components from Macromedia® JRun™ by Adobe. JRun provides the foundation that the application layer and web-server functionality are built on. The server contains and executes all of the business logic necessary for delivering content to users. The Connect Enterprise application server manages users, groups, on-demand content, and client sessions, among other tasks.

Some of the application server's specific duties include access control, security, quotas, licensing, and auditing and management functions such as clustering, failover, and replication. The Connect Enterprise application server also transcodes media; this includes Microsoft PowerPoint and audio conversion to Flash, as well as to other associated media files.

The Connect Enterprise application server is stateless and follows a service-oriented architecture (SOA). Because the application server is stateless, scaling is near-linear. The transactional and application metadata that the application server manages can be stored in either single or multiple replicated SQL databases.

Meeting server

Enterprise Server includes an embedded instance of Macromedia® Flash® Media Server from Adobe. In the context of Connect Enterprise, Flash Media Server is referred to as the *meeting server*. This component handles all of the real-time streaming of audio, video, synchronization of data, and delivery of rich-media content, including Acrobat Connect Professional meeting interactions.

Flash Media Server streams audio, video, and accompanying meeting data using the Adobe Real-Time Messaging Protocol (RTMP). Flash Media Server can also act as a proxy to route internal system HTTP traffic in a single-server or software-based SSL configuration.

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 plays a vital role in reducing server load and latency by caching frequently accessed streams and shared data.

Flash Media Server and Connect Enterprise application server components work together on the same computer to deliver the Connect Enterprise solution.

Database

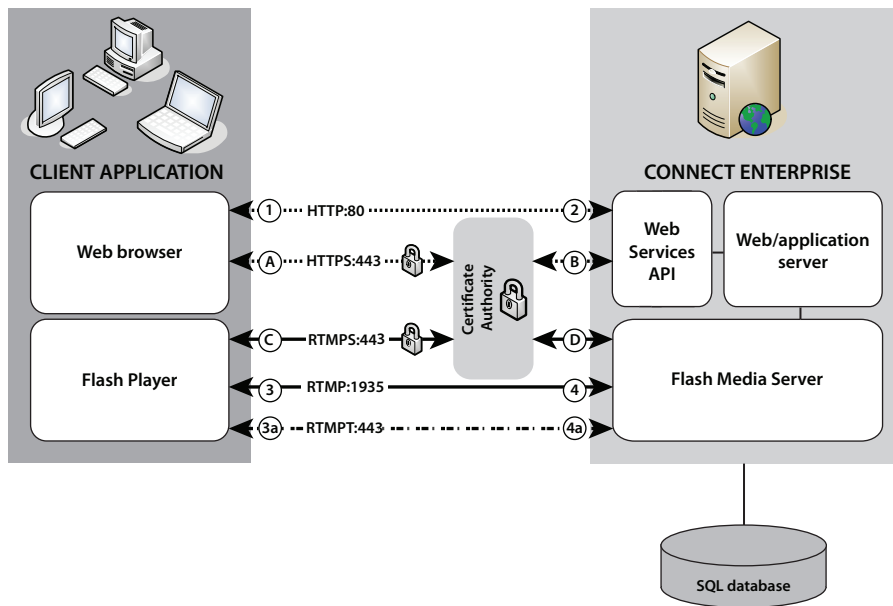
The Enterprise Server database is used for persistent storage of transactional and application metadata, including user, group, content, and reporting information.

Enterprise Server can use either the embedded database engine (MSDE) or the full version of Microsoft SQL Server 2000 or Microsoft SQL Server 2005. The embedded database engine is included with Enterprise Server and must be installed on the same computer as Enterprise Server. SQL Server can reside on the same computer as Enterprise Server, or you can deploy it on a different computer or in a cluster (a configuration with multiple computers) for scalability and redundancy.

When Enterprise Server is deployed in a cluster, or with multiprocessor computers with Hyper-Threading Technology (HTT), you must use SQL Server and it cannot be installed on the same computer as Enterprise Server.

Data flow

Enterprise Server uses the following communication protocols: HTTP, HTTPS, RTMP, and RTMPS. Adobe's Real-Time Messaging Protocol (RTMP) is optimized to deliver real-time, high-impact streams. RTMPS is the secure implementation of RTMP.



Data flow between a client and Enterprise Server

Depending on whether or not communications are encrypted, the connection paths vary.

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.
4	Flash Media Server responds and opens a persistent connection for Acrobat Connect streaming traffic.
3a	The client Flash Player requests a connection to the meeting but can only connect over RTMPT:443.
4a	Flash Media Server responds and opens a tunneled connection for Acrobat Connect streaming traffic.

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.

A client initiates the first connection to the application server. These connections, such as for login requests, file publishing, or content and event management, are made through HTTP or HTTPS. After the client engages in real-time communication, a connection to Flash Media Server is started, and Enterprise Server uses either RTMP or RTMPS to deliver streamed content.

By default, RTMP travels over port 1935 and is used for live interactions in an Acrobat Connect Professional meeting (video, voice, and screen sharing). HTTP traffic travels over port 80, and is used for client login and to transfer content (slides, documents, and so on). An RTMP connection uses port 443 if a connection through port 1935 is not successful, or if the server is configured to use SSL encryption. However, tunneling incurs additional overhead, and negatively affects streaming performance.

For licensed deployments, you can customize the Enterprise Server communication ports to resolve cases in which corporate proxy servers and firewalls block port 1935 for inbound and outbound traffic on the local area network (LAN).

Hosted and licensed solutions

Hosted solution

The Adobe® Connect™ Enterprise Hosted 6 solution is an easy way for organizations to use the Adobe feature-rich web communication system without having to install or manage the software. Clients can manage, view, and participate in on-demand or live web presentations and training from anywhere in the world. The Enterprise Server hosted model provides the following advantages:

- Immediate account access, without having to set up and configure servers on-site
- Service updates, infrastructure upgrades, and routine maintenance
- Reliable, redundant deployment with multiple, automated failover provisions
- Scalable deployment from a high-bandwidth Tier 1 hosting center that can handle thousands of simultaneous connections
- Lower initial investment

Hosted security

The Enterprise Server hosted solution provides a high degree of individual component and system-wide security. Customer data is protected through multiple layers of security across the application, transport, network, and physical layers.

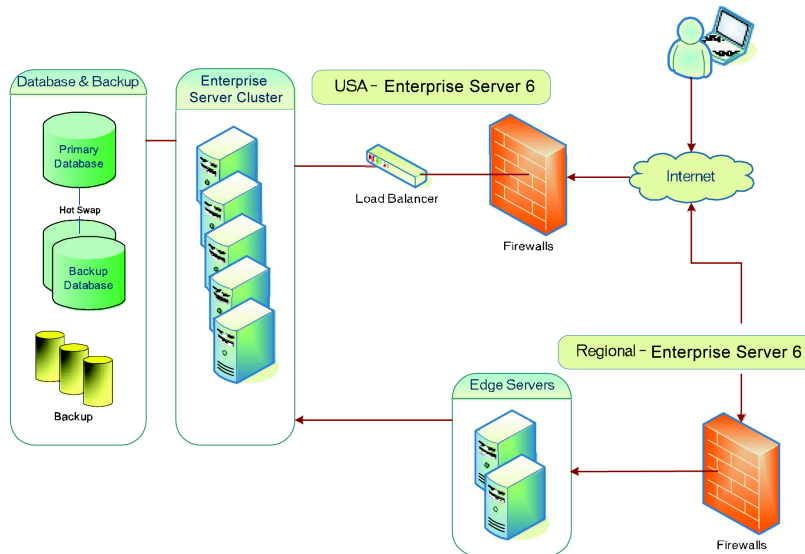
Adobe conducts regular security and vulnerability audits, executed by internal security personnel and third party firms, to validate the security of the hosted infrastructure and software. The audit results are reviewed internally, and any issues identified during this process are addressed in a timely manner to maintain the overall integrity of the service and ensure the security of customer data.

Hosted architecture

The hosted infrastructure uses a high-availability model. Multiple Enterprise Server servers are clustered behind a hardware load balancer. Connections on this deployment are fast because they are routed to the most available application server in the cluster; and in the unlikely event of system failure of any application server, the client connection fails over to a healthy system. This is true whether the client is working with on-demand content, or interacting in real time in an Acrobat Connect Professional meeting.

The Enterprise Hosted database stores account metadata such as users, groups, event and meeting details, content access, and so on. Microsoft SQL Server is used as the enterprise database solution for Enterprise Hosted, and is implemented with redundant database nodes to ensure high availability.

The following diagram depicts an overview of the Enterprise Hosted infrastructure. Redundancy, failover, security, and global performance are key considerations in the design, delivery, and regular improvements of the hosted service.



Enterprise Hosted architecture

Licensed solution

A licensed solution is available to deploy Enterprise Server in your own corporate network. The Enterprise Server licensed model provides the following advantages:

- Long-term cost savings based on software ownership
- Deployment behind a firewall
- No bandwidth or disk space restrictions
- Uses internal hardware and Information Technology (IT) personnel for delivery and management

Licensed architecture

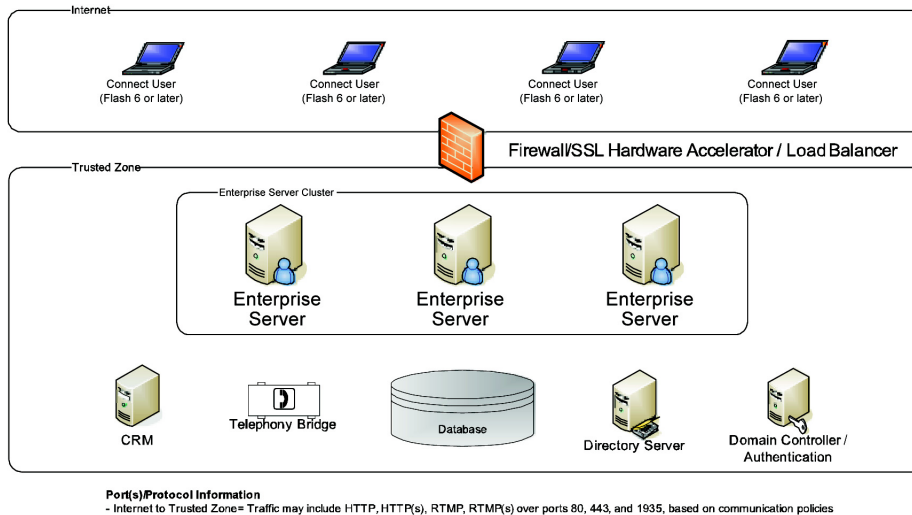
Depending on the organization's size, projected Enterprise Server use, and how crucial Enterprise Server is to your business, you can deploy Enterprise Server in either single-server or highly redundant clustered configurations. For small- to medium-sized companies with simple network configurations, a dedicated single-server Enterprise Server deployment is a viable solution. However, organizations that require high availability can deploy Enterprise Server in a cluster. This configuration is ideal for customers who have many users and are concerned about the load on a single server, or for companies that want a redundant system in the event of a single-node failure.

When you deploy Enterprise Server in a cluster, clients connect to an Enterprise Server farm behind a load balancer. Because Enterprise Server separates the network access layer from the application layer, clustering provides the following advantages:

- On-demand stream caching
- Connection aggregation
- Three-tier architecture

The Enterprise Server cluster connects to a database solution: either a single SQL database or a SQL cluster for increased transaction performance and reliability.

To use SSL, implement your preferred solution across a single or clustered Enterprise Server deployment. You can also include additional components in the overall deployment—such as integrations to your customer relationship management (CRM) system or learning management system (LMS), telephony bridge, or directory service provider to synchronize LDAP user accounts with Enterprise Server.



Licensed deployment architecture

Firewalls, proxies, and ports

The Enterprise Server licensed solution works with standard enterprise firewall (proxy) configurations, and can also be implemented in the DMZ (perimeter network). Reverse proxies, however, are not yet certified for use with Enterprise Server. Enterprise Server uses standard communication protocols, so that it works like any other application or web server, and does not cause problems with network devices. Adobe has been successful in all standard deployments of Enterprise Server at customer sites.

The client initiates all communications with Enterprise Server (this is also true for edge servers). The inbound ports (from the Internet) that the Enterprise Server system uses are ports 80, 443, and 1935, and the outbound port (to the mail server) used is port 25.

Enterprise integration

User administration

Administrators can define managers and team members in Enterprise Server, as well as customize the attributes included in user profiles. You can change any attribute of an existing user profile field, set a required field, or add a comment for a field.

A user profile field is an attribute of your organization's Enterprise Server user profile. The customization feature in Enterprise Manager lets you access user profile fields and attributes in three ways:

- By selecting one or more components from the default list that Enterprise Server provides
- By selecting additional components from a list of predefined fields
- By creating your own custom components

The fields for First Name, Last Name, and E-mail are all required for Enterprise Server—you cannot select, remove, or modify these. However, you can modify any other existing field to designate it as required and to include a descriptive comment, and do the same for any new fields that you create. You can also move a component up or down in the profile list, depending on its importance.

Enterprise Server allows administrators to define policies for password management that are consistent with industry best practices, including administrator password resets and special character requirements. These policies are enforced across the Enterprise Server applications and allow administrators to align Enterprise Server with their existing security policies. An administrator can govern the details that pertain to the organization's Enterprise Server account through the Administration tab in the web-based Enterprise Manager.

To learn more about Enterprise Server user administration, see the *Adobe Connect Enterprise User Guide* available online at www.adobe.com/go/connect_documentation_en.

Adding users and groups

You can use three methods to add users and groups to your Enterprise Server implementation. These methods make user management much easier than manual account definition:

- LDAP synchronization, which is described in detail in [Lightweight Directory Access Protocol \(LDAP\) synchronization](#).
- Administrators can import users and groups using CSV files. If an organization's directory has a utility for exporting users and groups to CSV format, an administrator can use the web-based Import feature to import the file into Enterprise Server.
- Adobe® Connect™ Enterprise Web Services APIs allow you to write custom scripts for user creation or other Enterprise Server administration tasks.

Lightweight Directory Access Protocol (LDAP) synchronization

You can import users and groups into Enterprise Server from existing directories with compliant LDAP structures. You can use the LDAP or secure LDAPS protocols.

Enterprise Server connects as an LDAP client to an LDAP directory, imports users and groups, and synchronizes information about these imported users and groups in the Enterprise Server database with the external LDAP directory. Integrating Enterprise Server with a directory server allows administrators to avoid manually adding users individually to Enterprise Server. User and group accounts are created automatically in Enterprise Server through manual or scheduled synchronizations with an organization's directory service.

To ensure that user logins are synchronized across the organization, combine directory service integration with a system for authenticating users. Using directory service integration and an HTTP-header or Windows NT LAN Manager (NTLM)-based authentication method provides users with an automatic, single sign-on (SSO) experience for Enterprise Server. A user who is logged on to their desktop using their network user name and password can then access Enterprise Server services directly, bypassing the Enterprise Server login screen.

For additional information on Enterprise Server directory service integration and LDAP, see the *Adobe Connect Enterprise Server 6 Installation and Configuration Guide* available online at www.adobe.com/go/connect_documentation_en.

Login administration

When Enterprise Server imports user information using directory service integration, it does not receive access to the user's network password. Administrators need a different method to manage user login imported into the Enterprise Server directory from external LDAP servers.

One option is to automatically send an e-mail using Enterprise Server with a link to set a password after an account is added to Enterprise Server. Or, if users were imported with directory service integration, administrators can initially set user passwords to a default, such as a field contained in the LDAP directory (employee ID for example). After users log in using this initial password, they can change their passwords.

The recommended method for managing Enterprise Server user passwords and authentication with directory service integration is to use it with automatic SSO. SSO is a mechanism whereby a single action of user authentication allows a user to access all computers and applications where they have access permission—without having to enter multiple passwords. SSO reduces human error, which is a major component of system failures. You can configure Enterprise Server to manage users and authenticate their access to multiple applications in several ways.

Windows NT LAN Manager (NTLM) Microsoft uses Windows NTLM to pass information about authenticated users. After users log in, they can access intranet sites or applications that require valid access without being prompted each time for their login and password. Only Internet Explorer on Microsoft Windows can silently negotiate NTLM authentication without prompting the user for credentials. Enterprise Server checks the browser type of a request and only requests NTLM authentication for browsers that support NTLM.

HTTP header-based authentication HTTP header-based authentication uses extra fields in the header of an HTTP request for user authentication. In this configuration, all Enterprise Server requests must first be routed to an authentication proxy (reverse proxy) positioned between the client and the Enterprise Server. The proxy server authenticates the request and adds an extra HTTP header field. Enterprise Server uses the header information to identify the user. If the user passes the authentication test, Enterprise Server creates a valid session and allows the user to begin using the system.

Learning management system (LMS)

The Enterprise Server solution allows you to deploy an enterprise training solution using Enterprise Server tools and your existing LMS. You can develop content in either Adobe Presenter or your existing industry-standard instructional design tool, and host that content either on your LMS or on Enterprise Server. Finally, web services APIs allow you to integrate the Enterprise Server system with your LMS for coordinated course and training management.

Adobe Presenter is the content authoring tool that allows non-technical subject matter experts to rapidly create e-learning content from Microsoft PowerPoint. Adobe Presenter can produce content that conforms to AICC and SCORM standards.

When Adobe Presenter content is deployed in conjunction with an LMS, e-learning can be launched and tracked from the LMS. Content created using Adobe Presenter conforms to two output formats: AICC and ADL SCORM. Adobe Presenter content can be output in each of the AICC or SCORM protocols. An author can select the appropriate LMS standard when publishing content from Adobe Presenter.

In addition, Adobe Presenter offers several advanced settings for how presentations integrate with LMS systems. The settings let you specify what data is sent to the LMS and how the data is formatted. Typically, advanced LMS users use these settings, or LMS administrators request them. For more details, see the *Adobe Presenter 6 User Guide* (available online at www.adobe.com/go/connect_documentation_en) or the [Connect Enterprise Resource Center](#), which has instructions for how to integrate Adobe Presenter content with commonly used LMSs.

Enterprises can integrate Enterprise Server content in their LMS systems. Enterprise Server supports Aviation Industry CBT Committee (AICC) with HTTP AICC Communication Protocol (HACP), versions 2.0 through 3.5, a standard LMS communication protocol.

Although Adobe Presenter can generate AICC and SCORM content, the Enterprise Server internal LMS only supports and tracks third-party or custom content that conforms to AICC specifications. In addition, Enterprise Server can host content created by using other tools, such as Adobe Captivate and Adobe® Authorware®. In Adobe Captivate and Adobe Presenter, selecting the reporting option provides more detailed reporting information. Enterprise Server can also accept any content that adheres to the AICC interaction standard. If assessments or surveys are deployed, Enterprise Server can track completion and score data. Enterprise Server can track individual question reporting with some additional content development work.

Shared storage

Enterprise Server can be configured to use a local or external storage system. For more information, see [Shared storage](#).

Extensibility and custom integration

About extensibility and custom integration

Connect Enterprise Server 6 is highly customizable and extensible, with support for custom branding, directory services integration, system extensibility, bidirectional data integration, and meeting extensibility. Enterprise Server enables system extensibility with application interfaces that integrate web communication capabilities with the application network, including integration with enterprise portals, reporting applications, CRM systems, learning and content management systems, and other corporate systems. Enterprise Server also provides support for custom applications and components. Through published APIs, organizations can incorporate external data and functionality directly with Enterprise Server.

Web services APIs

The Enterprise Server platform provides the infrastructure that the Adobe Presenter, Training, Events, and Meetings applications use. With the web services APIs, you can extend and integrate these applications by using a complete web services framework. You can incorporate Enterprise Server functionality and reporting information directly into third-party systems such as portals and CRM and ERP systems. You can use web services to manage the full breadth of the solution, including everything from user management to in-depth reporting on application use.

***Note:** If you use Enterprise Hosted, you can also take advantage of Enterprise Server extensibility by using XML web services. However, you must abide by the terms of service, which restricts certain activities, such as bulk user imports. Instead, you must add each user into the system individually or by importing a CSV file.*

Consider the following scenario to understand the possibilities of custom integration. You have an existing user management system of record, such as LDAP, Microsoft Active Directory, or another third-party system. This central user management system was deployed in your corporate infrastructure, and is an integral part of existing business processes. You want to use your existing investments across all solutions you deploy, including Enterprise Server. The Enterprise Server XML web services allow for complete user management by an external system, such as a directory service. You can write an application that synchronizes users between these two systems. For example, you could write an application based on J2EE (or another technology of your choice) that pulls a list of users from

the directory namespace, compares this list against a list of Enterprise Server users, and then performs requested updates in the Enterprise Server user repository, such as adding or deleting users and groups in Enterprise Server. This is just one example of how you might build an integration, or extend the Enterprise Server feature set by using the XML web services provided with Enterprise Server. Check the [Acrobat Connect Developer Center](#) for more XML web services examples.

To use web services, you need to be able to communicate with Enterprise Server over HTTP or HTTPS, depending on whether you have enabled SSL. You call Enterprise Server web services and pass in one or more parameters—either as name-value pairs or as an XML package—and the web service returns a complete XML document, which can then be parsed and leveraged as necessary in your external applications.

You can use web services for the following:

Access control Organizations are using Enterprise Server to develop and deliver a variety of on-demand and real-time content. In many cases, this content requires strict access control to ensure that information is secure and reaches only its intended audience. Enterprise Server provides a comprehensive access control framework that you can access over web services. Enterprise Server allows external systems to authenticate, manage users, set permissions, and so on—all through the web services framework.

User management You can take advantage of existing directory services to manage Enterprise Server users. Enterprise Server provides a complete set of web services that allow you to develop synchronization processes between your directory service and Enterprise Server. Additionally, these web services let you integrate user profiles, Enterprise Server content, and reporting data into external systems such as an enterprise portal, CRM, and ERP applications.

Reporting You can use the detailed reporting capabilities of Enterprise Server in external systems such as employee performance management solutions or LMS systems. With Enterprise Server web services you can integrate the Enterprise Server reporting data repository with these external systems to derive real-time reporting from a single reporting infrastructure. Similarly, you can create custom reports beyond the standard reports using Enterprise Server web services.

Content, meeting, training and event management You can upload content from a custom application into Enterprise Server. You can also create new meeting or collaboration sessions from a custom application. All of these uses are possible through the web services interface. With Enterprise Server you can create and manage Enterprise Server assets and meetings from any application that uses web services.

Database views

Database views let customers create custom reports through common third-party reporting tools such as Business Objects Crystal Reports. Database-level views are read-only; to alter or manipulate Enterprise Server information, use Enterprise Server XML web services APIs.

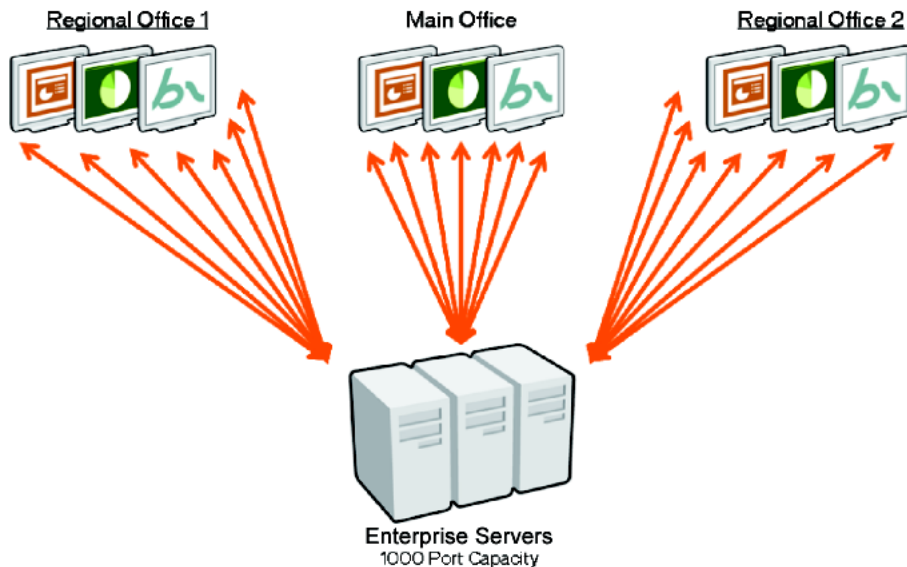
Connect Edge Server

About Connect Edge Server

Connect Edge Server provides stream consolidation, content caching, network-edge deployments, and more control over the flow of information. Benefits include reduced network traffic, increased scale across the organization, increased security through encrypted traffic, and reduced origin-server load. Although the use of Connect Edge Server is completely transparent to the end user, the benefits are clear to an organization's IT department.

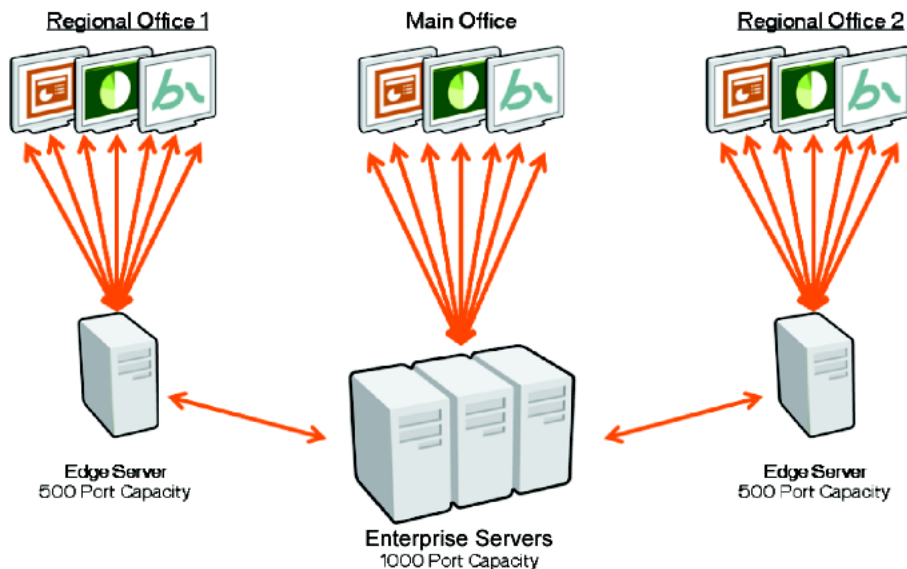
Architecture

Traditionally, users connect directly to the primary Enterprise Server or cluster, which handles authentication, access control, on-demand and real-time video, audio, and data delivery. The communication, as demonstrated in the following example, results in one thousand individual connections between clients and the server. If you take this deployment further, and consider regional office connections, these additional clients initiate direct connections to Enterprise Server as well. This additional traffic results in high bandwidth requirements between the regional offices and the primary server, and potentially increases latency during the meeting experience.



The increased demand in connections when Enterprise Server serves multiple regional offices and many users

Edge servers address this deployment concern by consolidating regional office streams before they connect to the primary server. Organizations can also cluster edge servers to provide system redundancy and increased capacity at the edge. Instead of five hundred unique connections between the remote office and the server, the edge server consolidates requests for meetings, real-time streams (such as VoIP or video) and content, reducing the number of streams from five hundred to one in the case of all users connecting to the same large Acrobat Connect Professional meeting (see the following example). Requests for HTTP-based content (such as on-demand content or courses) are not combined but the results are cached so multiple requests for that content do not result in multiple requests to the server. This caching not only dramatically reduces network traffic, but also reduces load on the origin Enterprise Server or cluster.



Lowered demand on the origin Enterprise Server cluster when edge servers are deployed. Connection aggregation occurs on a per meeting basis; in this figure, all users at the edge are attending the same meeting.

Data flow

Connect Edge Server is designed to allocate and balance access to an Enterprise Server by using the existing bandwidth resources more efficiently. After the edge servers are deployed, users access Enterprise Server through their configured edge server. Edge servers forward authentication requests to Enterprise Server, but after they are authorized and if the data requested is found in the edge server's cache, the edge server returns the cached meeting or training content data to the requesting client (the user's computer) without calling on Enterprise Server. This detour to Enterprise Server is transparent to users. In this scenario, aside from authentication, no additional demands are placed on the origin Enterprise Server servers.

If the requested data is not found in the edge server's cache, the edge server forwards the client's request to the origin servers, where the user is authenticated and the request for services is authorized. The origin servers return the results to the requesting edge server, which in turn delivers the results to the requesting client. The edge server also stores this information in its cache, where other authenticated users can access it. In this scenario, fewer requests for services are forwarded to the origin servers.

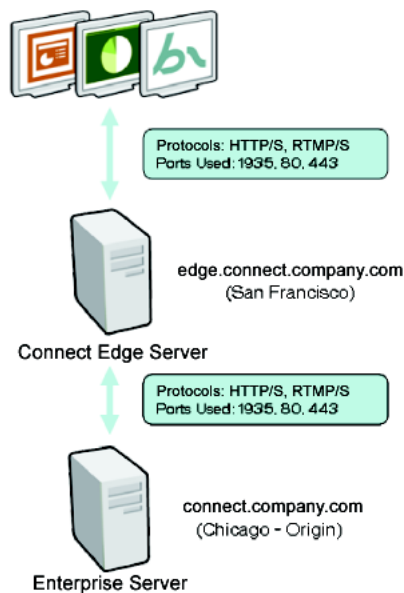
An edge server is configured to intercept the requests for Enterprise Server services from a particular zone. The Connect Edge Server then collects or aggregates these requests, and transmits them to the origin Enterprise Server servers (see the following example for data flow with edge servers). The origin server returns the results to the edge server, which forwards the data to the user's client computer.

Sample scenario

A networked Enterprise Server deployment might have multiple edge servers installed. For example, one edge server might aggregate and forward requests from San Francisco and another might aggregate and forward requests from Chicago. Each edge server then performs the following steps:

- Gathers the requests from its clients for each meeting and forwards them to the origin servers located in the data center in Chicago.
- Receives the responses from the origin.

- Transmits and distributes responses to the clients in each zone.



The flow of data from the edge network to the origin Enterprise Server cluster

Deploying servers in a cluster

About clusters

Enterprise Server offers true enterprise-class scalability with support for single-server or clustered environments. Organizations that require high availability can choose to deploy Enterprise Server in a cluster. Clusters provide reliable, redundant deployment that can support thousands of concurrent users.

An Enterprise Server cluster is made up of identical components for which each server provides identical functionality. If one server fails, the request is transparently routed to the next. This routing is easily accomplished because Enterprise Server on-demand and real-time data is replicated across multiple servers for redundancy.

Enterprise Server is designed so that no single point of control or single point of failure exists. Because of this design, you can add or remove servers from your cluster, and scale your Enterprise Server deployment to meet your organization's needs.

In an Enterprise Server cluster configuration, typically a load balancer (or SSL hardware accelerator) is placed in front of each server farm, where each HTTP connection request is selected by round robin. HTTP requests are stateless, ensuring that a server failure does not affect the uptime of the system. RTMP connections, such as Acrobat Connect Professional meetings, do not go through the load balancer. Instead, the Enterprise Server application server uses a reservation algorithm to select the appropriate servers for the primary meeting instance and the backup instance. A meeting uses health checks to manage the failover process between the servers.

To provide redundancy and instant failover, when each meeting is instantiated, a primary server is chosen to host the meeting and a secondary server is chosen as the backup. If the primary server hosting the meeting fails, all meeting attendees are reconnected to the backup server and the meeting continues with the same meeting content and environment.

Shared storage

Enterprise Server can store content on NAS and SAN devices. Content is any file published to Enterprise Server, such as courses; SWF, PPT, or PDF files; and archived recordings.

When you use shared storage, you can configure Enterprise Server to use the server's disk as a content cache so that all content is copied to the 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 (the content is always kept on the NAS/SAN device). This configuration frees resources on the application server, which is especially helpful in a large cluster.

If you don't configure a content cache, content is mirrored on all servers and the external storage device.

When an external storage device fills up, you can add more space to the device, or add another device to the front of the chain. Content only writes to the first device in the chain.

Database server clusters

If you choose to deploy Enterprise Server in a cluster, you must have a separate database layer. The database must reside on a different computer than Enterprise Server—separate from the application server layer. The database can be either a single SQL server or a SQL cluster.

To cluster the Enterprise Server database, Enterprise Server requires Microsoft SQL Server 2000 or Microsoft SQL Server 2005 and relies on the SQL server's clustering functionality. Furthermore, all Enterprise Server servers in the cluster must have access to the database. A cluster configuration reduces the load on a single computer, and enables failovers and backups without disrupting service.

Edge server clusters

Enterprise Server enables organizations to support edge networks through Connect Edge Server. Edge routing reduces the bandwidth requirements and latency, and edge servers support stateless failover. As such, you can cluster edge servers when high availability and global reach are critical to the organization. For more information about Connect Edge Server, see [Connect Edge Server](#).

Security

Planning a security strategy

The easiest solution to secure a dedicated, single-server Enterprise Server system is to block all ports on the server except for 80, 1935, and 443 (for SSL-enabled traffic). An external-hardware firewall appliance provides a layer of protection against gaps in the operating system. Some organizations 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, you can configure a software-based firewall to enable additional security.

Multiserver (cluster) solutions are inherently more complex. You can configure and extend the Enterprise Server service with geographically dispersed edge servers. However, you must understand how to secure the communications between the origin cluster and edge clusters. The following are suggestions for securing multiserver solutions:

- Create an extra subnet for the Enterprise Server system. For multiserver solutions in a single location, a private network is simple and offers a high level of security.

- Use a local software firewall. For a clustered Enterprise Server system that shares a public network with other customer servers, you may find that a software firewall is appropriate on each individual server.
- Configure SSL. You can use an SSL to secure communications between the Enterprise Server edge servers and the origin Enterprise Server.

Web server security

Enterprise Server relies on Macromedia JRun from Adobe for its web server functionality. The server is hardened in the Adobe implementation. Enterprise Server uses a simplified version of the JRun server: this means that only the component of the server that accepts and responds to HTTP requests is present and in use; Adobe removed or disabled the rest of the functionality. For example, Adobe eliminated the following components: the JRun content server, auto-deploy, JSP support, sample applications, clustering, session management, and web services.

Secure Sockets Layer (SSL)

You can deploy a licensed version of Enterprise Server with an SSL layer in one of two ways: A software-based solution that uses the native support for SSL in Flash Media Server; or a hardware-based solution that routes all communication through an external SSL accelerator, which you must purchase separately through your preferred vendor.

Without SSL, all logins are conducted over HTTP connections, and all subsequent content and meetings are delivered over standard unencrypted HTTP and RTMP connections. You can configure SSL to encrypt the HTTP connection, the RTMP connection, or the HTTP and RTMP connections.

SSL hardware accelerators intercept traffic on port 443, decrypt the information, and send it back to Enterprise Server over a port and IP address that is presumably not exposed outside your corporate security measures. The server has no indication that the original data was encrypted. Adobe has tested and verified Enterprise Server with the following SSL hardware accelerator providers:

- F5 Big-IP 1000
- Cisco Catalyst 6590 Switch
- Radware T100

Your network configuration and environment has a direct effect on Enterprise Server performance and these variables ultimately determine how Enterprise Server should be deployed with your SSL hardware. Enterprise Server may support other solutions in the industry, but the providers listed are the only ones that are confirmed at this time.

You may decide to use a software-based SSL, but Adobe recommends hardware accelerators for better performance. For details on setting up a software-based SSL solution with Enterprise Server, see the *Adobe Connect Enterprise Server 6 Administration Guide* available online at www.adobe.com/go/connect_documentation_en.

In the Enterprise Hosted solution, SSL is enabled for login and content management. SSL for real-time communications is an available option on a per-account basis.

Public key infrastructure (PKI)

You can set up a public key infrastructure (PKI) to manage identification credentials as part of your Enterprise Server 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 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 Enterprise Server.

Note: Use HTTP header-based authentication to implement PKI. For more information, see [HTTP header-based authentication](#).

Database security

Whether or not you are hosting your database on the same server as Enterprise Server, you must be certain that your database is secure. Computers hosting a database must be in a physically secure location. Additional precautions include installing the database in the secure zone of your organization's intranet, never connecting the database directly to the Internet, and backing up all data regularly and storing copies in a secure off-site location.

To further secure your Microsoft SQL database, see the Microsoft security website (www.microsoft.com/sql/technologies/security/). It contains information that applies to SQL Server 2000, SQL Server 2005, and the embedded database engine (MSDE).

Note: Enterprise Server supports SQL authentication only; you must select SQL Server with mixed-mode authentication. Enterprise Server does not support Windows Authentication mode.

The Enterprise Server application server is designed to prevent unauthorized remote access to the database. Enterprise Server uses only prepared statements to communicate with the database, thereby preventing the most common remote SQL exploits. Enterprise Server further checks the validity of arguments to the database, and finally performs a security check on each access to every key in the database. The Enterprise Server security system's default behavior is to deny access where permission is not explicitly granted to a given row.

Enterprise Server also encrypts columns in the database that contain sensitive data. Even someone with full access to the database server is not able to access user passwords or other sensitive information.

Content access

Adobe Acrobat Connect Enterprise Manager is a web application that acts as an access and control point for all Enterprise Server applications. Enterprise Manager not only allows you to set up and manage meetings, seminars, and training courses and curriculums, but also enables you to manage and control content that you can share through meetings, presentations, training courses, and events.

To secure content, you can use the user management component of Enterprise Manager to set access permissions for the users of the content and the administration of the content itself through a simple, intuitive user interface. All Enterprise Server content is contained and organized in a directory of folders called the Content library, which you access through Enterprise Manager.

Furthermore, not everyone can use all the Enterprise Manager features. These access-controlled features depend on the Enterprise Server configuration and each user's permissions. For example, if a user is not a member of the Administrators group, they cannot access the Administration tab in Enterprise Manager. For more information on securing content and working with the Content library, see the *Adobe Connect Enterprise User Guide* available online at www.adobe.com/go/connect_documentation_en.

Hosting 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.

Requirements

System and user requirements

For the latest system requirements, visit the Adobe Connect website at www.adobe.com/go/connect_sysreqs_en.

Bandwidth requirements

The Enterprise Server client is Flash Player, which is installed on approximately 98% of web browsers. Because participants don't need to download software, obtaining the meeting client does not affect the network. Enterprise Server offers an Acrobat Connect Add-In—an enhanced version of Flash Player that adds features to the meeting experience, but is not required to host or attend a meeting.

Enterprise Server optimizes communications and reduces bandwidth through the following mechanisms:

TCP-based streaming All rich content including audio, video, screen sharing, and software simulations is streamed.

Optimal data stream delivery Using adaptive technology, Enterprise Server detects the bandwidth of the client and delivers the optimal data stream.

Compressed content Regardless of the bandwidth available, Flash content is highly compressed to reduce the effect on the network.

Vector graphics Flash graphics, text, animations, and images are automatically resized in the viewing window, thereby maintaining image quality.

Incremental image differentials When screen sharing and running live video, Enterprise Server sends only incremental image differentials.

Audio control Enterprise Server offers audio options for controlling your existing infrastructure: high-performance PC to PC (VoIP) or integrated conference calling.

Edge Servers Deploy Connect Edge Server to dramatically increase the efficiency of global network traffic and improve the quality of service (latency is only to the edge, but lowers network bandwidth use).

In the following figures, the Enterprise Server bandwidth and quality characteristics are detailed under three common meeting scenarios: 1-to-1 collaborative meeting, 10-person interactive collaborative meeting, and 1-to-many web seminar.

Bandwidth and Quality Tables for 1-to-1 Collaborative Meeting Scenario (Values are per user or edge server connection, unless otherwise indicated)

Action	Connection Speed or Bandwidth Setting (kbps)			Frame Rate (FPS)			Sample Rate (kHz)			Compression ¹ /Color Depth ²		
	LAN	DSL	Modem	LAN	DSL	Modem	LAN	DSL	Modem	LAN	DSL	Modem
View Slides	HTTP delivery; size dependent on content											
Lead Slides	HTTP delivery; size dependent on content											
Screen Sharing	400 ³	400 ³		6/2 ⁴	6/2 ⁴	6/1 ⁴				6/15	8/9	9/9
VoiP Audio	22	22	10				11	11	5			
Webcam Video												
Slow Images	40	40	40	1	1	1				50	50	50
Fast Images	250	125		15	12					100	60	100
High Quality	250	125		7.5	6					100	100	100
High Bandwidth	400			15						100	100	100
Playing FLV	RTMP streaming; dependent on bit rate of content ⁵											
Playing SWF	HTTP delivery; size dependent on content											
Chat	Negligible ⁶	Negligible ⁶	Negligible ⁶									
Whiteboard	Negligible ⁷	Negligible ⁷	Negligible ⁷									
File Share	Negligible ⁸	Negligible ⁸	Negligible ⁸									
Room Cap Up	400	250	28									
Room Cap Down	800	600	40									
My Connection Cap Up	Unlimited	250	28									
My Connection Cap Down	Unlimited	600	40									

1 - Compression-Higher value indicates higher quality and lower compression'

2 - Color Depth-Screen Share also includes a 24-bit color setting that can be applied using the Screen Share Pod settings.

3 - Average typically ranges from 50 to 400kbps dependent on content, but a peak of 1mpbs is possible.

4 - Screen Sharing FPS-(A/B): where the value A is FPS when remote control of screen share is enabled and the value B is when a person is screen sharing without remote control.

5 - Dependent on bit rate of FLV been streamed. If downstream speed is less than what is required for viewing the authored FLV, users will experience stalls.

6 - Data transmitted for chat is equivalent to amount of chat text written and causes no significant traffic.

7 - Data transmitted for whiteboard is only information about the object type and position to display, and causes no significant traffic.

8 - Displaying a list of content in the File Share Pod has no impact on bandwidth; if the user downloads the file the transfer is HTTP and the impact depends on document size.

Bandwidth and Quality Tables for 5-to-5 Collaborative Meeting Scenario (Values are per user or edge server connection, unless otherwise indicated)

Action	Connection Speed or Bandwidth Setting (kbps)			Frame Rate (FPS)			Sample Rate (kHz)			Compression ¹ /Color Depth ²		
	LAN	DSL	Modem	LAN	DSL	Modem	LAN	DSL	Modem	LAN	DSL	Modem
View Slides	HTTP delivery; size dependent on content											
Lead Slides	HTTP delivery; size dependent on content											
Screen Sharing	400 ³	400 ³		6/2 ⁴	6/2 ⁴	6/1 ⁴				6/15	8/9	9/9
VoiP Audio	22	22	10				11	11	5			
Webcam Video												
Slow Images	40	20	3	1	1	0.3				50	50	50
Fast Images	40	20		5	2.4					100	60	100
High Quality	40	20		2.5	1.2					100	100	100
High Bandwidth	300			5						100	100	100
Playing FLV	RTMP streaming; dependent on bit rate of content ⁵											
Playing SWF	HTTP delivery; size dependent on content											
Chat	Negligible ⁶	Negligible ⁶	Negligible ⁶									
Whiteboard	Negligible ⁷	Negligible ⁷	Negligible ⁷									
File Share	Negligible ⁸	Negligible ⁸	Negligible ⁸									
Room Cap Up	400	250	28									
Room Cap Down	800	400	40									
My Connection Cap Up	Unlimited	250	28									
My Connection Cap Down	Unlimited	600	40									

1 - Compression-Higher value indicates higher quality and lower compression¹

2 - Color Depth-Screen Share also includes a 24-bit color setting that can be applied using the Screen Share Pod settings.

3 - Average typically ranges from 50 to 400kbps dependent on content, but a peak of 1mpbs is possible.

4 - Screen Sharing FPS-(A/B): where the value A is FPS when remote control of screen share is enabled and the value B is when a person is screen sharing without remote control.

5 - Dependent on bit rate of FLV been streamed. If downstream speed is less than what is required for viewing the authored FLV, users will experience stalls.

6 - Data transmitted for chat is equivalent to amount of chat text written and causes no significant traffic.

7 - Data transmitted for whiteboard is only information about the object type and position to display, and causes no significant traffic.

8 - Displaying a list of content in the File Share Pod has no impact on bandwidth; if the user downloads the file the transfer is HTTP and the impact depends on document size.

Bandwidth and Quality Tables for 1-to-N Collaborative Meeting Scenario (Values are per user or edge server connection, unless otherwise indicated)

Action	Connection Speed or Bandwidth Setting (kbps)			Frame Rate (FPS)			Sample Rate (kHz)			Compression ¹ /Color Depth ²		
	LAN	DSL	Modem	LAN	DSL	Modem	LAN	DSL	Modem	LAN	DSL	Modem
View Slides	HTTP delivery; size dependent on content											
Lead Slides	HTTP delivery; size dependent on content											
Screen Sharing	400 ³	400 ³		6/2 ⁴	6/2 ⁴	6/1 ⁴				6/15	8/9	9/9
VoIP Audio	44	22	10				22	11	5			
Webcam Video												
Slow Images	40	40	40	2	2	2				50	50	50
Fast Images	250	125		15	15					100	60	100
High Quality	250	125		12	12					100	100	100
High Bandwidth	400			15						100	100	100
Playing FLV	RTMP streaming; dependent on bit rate of content ⁵											
Playing SWF	HTTP delivery; size dependent on content											
Chat	Negligible ⁶	Negligible ⁶	Negligible ⁶									
Whiteboard	Negligible ⁷	Negligible ⁷	Negligible ⁷									
File Share	Negligible ⁸	Negligible ⁸	Negligible ⁸									
Room Cap Up	400	250	28									
Room Cap Down	800	400	40									
My Connection Cap Up	Unlimited	250	28									
My Connection Cap Down	Unlimited	600	40									

1 - Compression-Higher value indicates higher quality and lower compression'

2 - Color Depth-Screen Share also includes a 24-bit color setting that can be applied using the Screen Share Pod settings.

3 - Average typically ranges from 50 to 400kbps dependent on content, but a peak of 1mpbs is possible.

4 - Screen Sharing FPS-(A/B): where the value A is FPS when remote control of screen share is enabled and the value B is when a person is screen sharing without remote control.

5 - Dependent on bit rate of FLV been streamed. If downstream speed is less than what is required for viewing the authored FLV, users will experience stalls.

6 - Data transmitted for chat is equivalent to amount of chat text written and causes no significant traffic.

7 - Data transmitted for whiteboard is only information about the object type and position to display, and causes no significant traffic.

8 - Displaying a list of content in the File Share Pod has no impact on bandwidth; if the user downloads the file the transfer is HTTP and the impact depends on document size.