Installation and Configuration Guide
CONTENTS

INTRODUCTION: Breeze Installation Overview ........................................ 5
  Guide to documentation and additional resources .......................... 6
  Troubleshooting ................................................................. 8

CHAPTER 1: Before You Begin ....................................................... 9
  Basics of Breeze Server technology ......................................... 9
  Planning for bandwidth requirements .................................. 11
  Planning for directory services integration ........................... 13
  Planning for SSL ................................................................. 14
  Planning for security ......................................................... 15
  Ports used by Breeze .......................................................... 22
  Available Breeze configurations ......................................... 23
  Planning for a Breeze Server cluster ................................... 24
  Installation requirements .................................................. 25
  Breeze user requirements .................................................. 27
  The Breeze database ......................................................... 29

CHAPTER 2: Preparing to Upgrade ............................................... 31
  Overview ................................................................................. 31
  Before you begin ..................................................................... 32
  Backing up your Breeze files ............................................... 32
  Backing up the Breeze database ......................................... 33
  Preparing for the upgrade .................................................. 34

CHAPTER 3: Installing and Upgrading Breeze ............................... 35
  Installation checklist ............................................................. 35
  Installation and configuration overview ................................ 36
  Using the Breeze installer .................................................... 37
  The Application Management Console ................................... 43
  Starting and stopping Breeze components ............................. 53
  Uninstalling Breeze ............................................................... 54
  Troubleshooting ................................................................. 54
  Breeze technical support ..................................................... 55
  Macromedia online forums .................................................. 55
CHAPTER 4: Post-installation ................................................. 57
  Deploying Breeze to your organization .................................. 57
  Implementing single sign-on ............................................... 61
  Configuring the Breeze Directory Service Integration .................. 62
  Configuring SSL support for Breeze ...................................... 77
  Configuring FCS for SSL .................................................. 78
  Configuring a Breeze Server cluster ...................................... 84
  Maintaining Breeze reliability ............................................. 87

CHAPTER 5: Verifying Your Installation ....................................... 91
  Verifying that the Breeze database and Breeze Server work together .... 92
  Verifying that you can use Breeze Manager and send e-mail notifications .... 92
  Verifying that you can use Breeze Server .................................. 94
  Verifying that you can use Breeze Training ................................ 95
  Verifying that you can use Breeze Meeting ................................ 95
  Verifying that you can use the Breeze seminar feature ................... 96
  Verifying that you can use Breeze Events .................................. 96

INDEX ................................................................. 97
INTRODUCTION
Breeze Installation Overview

Macromedia Breeze consists of Breeze Server and its applications: Macromedia Breeze Meeting, Macromedia Breeze Presenter, Macromedia Breeze Manager, Breeze Events, and Breeze Training. Depending on the configuration purchased and the terms of your license, you may be installing one, two, or all of these applications.

**Breeze Server**  Makes it possible to quickly create multimedia presentations that combine audio and video with slides and graphics.

**Breeze Events**  Lets users manage the full lifecycle of large- or small-scale events, from registrations, invitations, and reminders, to reporting.

**Breeze Manager**  Lets you create courses, enroll students, and track and monitor students and courses.

**Breeze Meeting**  Lets you conduct online real-time meetings in which you can show multimedia presentations and broadcast live audio and video to participants.
Breeze Presenter  Lets you rapidly create e-learning content and high-quality multimedia presentations. Breeze Presenter is a plug-in for Microsoft PowerPoint. Finished presentations are in Macromedia Flash (SWF file) format and are SCORM and AICC compliant.

Breeze Training   Lets you build e-learning systems, with surveys, tracking, analysis, and course management.

Guide to documentation and additional resources

Macromedia Breeze contains a variety of media to help you quickly learn how to use the Breeze applications. This section describes the variety of resources available to ensure the successful deployment of the Breeze applications within your organization.

About the electronic manuals and online help

In addition to this manual, the following electronic manuals and online help systems are available:

- *Breeze Manager User Guide* describes how to use the administration, presentation, and meeting applications of Breeze. You can access *Breeze Manager User Guide* from the Breeze Manager Home page, and from the Help link in Breeze Manager.

- *Breeze Presenter User Guide* describes how to create Breeze presentations from PowerPoint and publish them to Breeze. You can access this document from the Breeze Manager Home page, and from the Breeze menu in PowerPoint by selecting *Breeze > Help*.

- *Breeze Meeting User Guide for Hosts and Presenters* includes information about using the Breeze web application to host online real-time meetings. The documentation includes procedures that demonstrate the simplicity of adding slides, Flash SWF files, images, and live audio and video to your presentation. You can access *Breeze Meeting User Guide* from the Breeze Manager Home page, and from the Help menu within a Breeze meeting room (when you enter as a Presenter) by selecting *Meeting > Help*.

- *Breeze Meeting User Guide for Participants* includes information relevant to users participating in an online real-time meeting. Breeze Meeting offers meeting participants a variety of options to make their experience truly participatory, including the ability to send messages and questions to Presenters and to each other, and the ability to participate through live video and audio. You can access *Breeze Meeting User Guide* from the Breeze Manager Home page, and from the Help menu within a Breeze meeting room (when you enter as a Participant) by selecting *Meeting > Help*.

- *Breeze Integration Guide* includes information necessary to make application programming interface (API) calls on the Breeze server from your external system, such as a web application. It also explains how to interpret the XML results that Breeze returns. In addition, the documentation contains reference material about each API and its parameters.

**Note:** The relevance of these guides to users depends on the Breeze Server applications that you are authorized to use, the type of user (such as meeting content manager, information technology engineer, or course presenter), and the user’s Breeze account permissions.
To help you determine what documentation is relevant to your needs, see the following table:

<table>
<thead>
<tr>
<th>Breeze user type</th>
<th>Recommended reading</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information technology (IT) engineer</td>
<td>• Breeze Installation and Configuration Guide</td>
</tr>
<tr>
<td></td>
<td>• Review the system requirements in all other user guides</td>
</tr>
<tr>
<td>Content managers in charge of overall content within Breeze, and administrators who may add users and permissions</td>
<td>• Breeze Manager User Guide</td>
</tr>
<tr>
<td></td>
<td>• Breeze Meeting User Guide for Hosts and Presenters</td>
</tr>
<tr>
<td>Content authors and instructional designers who create presentations and training with Breeze Meeting</td>
<td>• Breeze Manager User Guide</td>
</tr>
<tr>
<td></td>
<td>• Breeze Presenter User Guide</td>
</tr>
<tr>
<td></td>
<td>• Breeze Meeting User Guide for Hosts and Presenters</td>
</tr>
<tr>
<td>Meeting administrators who create and manage Breeze meetings</td>
<td>• Breeze Manager User Guide</td>
</tr>
<tr>
<td></td>
<td>• Breeze Meeting User Guide for Hosts and Presenters</td>
</tr>
<tr>
<td>End users who attend Breeze meetings</td>
<td>• Breeze Meeting User Guide for Participants</td>
</tr>
</tbody>
</table>

**Information about specialized topics**

This manual primarily provides information for a basic installation of Breeze applications in which no more than one instance of each application is installed on a computer. It also covers the installation of Breeze applications on multiple networked computers, which is called a cluster. For information about specialized topics not discussed in this installation manual, visit the Macromedia Breeze Licensed Support website at www.macromedia.com/go/breeze_licensed_support.

To access the licensed support website, you will need to have available the Breeze License Certificate from Macromedia.

The following are among the topics that the website covers:

- Installing and configuring Breeze Edge Servers
- Upgrading from an release earlier than Breeze 4.0
- Port numbers used by Breeze
- Using and managing the embedded database engine
- Integrating Breeze with a learning management system (LMS)
- Troubleshooting

**Additional resources**

Additional documentation, white papers, and articles are available at the following websites:

**Breeze Resource Center**  This site, at www.macromedia.com/resources/breeze, is updated regularly with tutorials, simulations, best-practices information, and links to procedures.
**Breeze Documentation Center**  This site, at www.macromedia.com/go/breeze_documentation, contains documentation for all Breeze products, answers to frequently asked questions, articles about specialized topics, and Breeze presentations.

**Breeze Support Center**  This site, at www.macromedia.com/support/breeze, contains current support information, including technical notes, helpful Breeze presentations, and support program details.

**Troubleshooting**

If you encounter unexpected results after installing Breeze on a single server or on a cluster of servers, consult the following helpful resources:

- TechNotes on the Breeze Support Center website at www.macromedia.com/support/breeze
- Macromedia Support
  
  You will need to provide your Macromedia license number to the representative.
- Macromedia Online Forums at www.macromedia.com/support/forums.

8 Introduction: Breeze Installation Overview
For a successful installation of Macromedia Breeze, read the information provided in this chapter. It contains the following sections:

- “Basics of Breeze Server technology” on page 9
- “Planning for bandwidth requirements” on page 11
- “Planning for directory services integration” on page 13
- “Planning for SSL” on page 14
- “Planning for security” on page 15
- “Ports used by Breeze” on page 22
- “Available Breeze configurations” on page 23
- “Planning for a Breeze Server cluster” on page 24
- “Installation requirements” on page 25
- “Additional software requirements” on page 27
- “Breeze user requirements” on page 27
- “The Breeze database” on page 29

Before you start the installation, you should plan how Breeze is to be configured. When you run the Breeze installer, you will see only those Breeze applications and options purchased by your organization.

**Basics of Breeze Server technology**

Breeze Server includes a suite of applications that interact to form a total solution. End users log in, enroll in courses, view reports, and complete additional basic functions using a web-based application that runs in a browser. Breeze users can also participate in meetings using any supported browser. For a list of supported browsers, see “Breeze user requirements” on page 27.
The web browser interacts primarily with the Breeze Server applications. When a user starts a meeting, Flash Player interacts primarily with Breeze Meeting, although there is still some interaction with Breeze Presenter. The following figure illustrates how the server hosting Breeze interacts with the user's computer, sometimes called the client.

For two computers to communicate over the Internet, the client computer must have the URL of the server (computer) where Breeze is installed. Typically, the client uses a domain name such as www.mycompany.com, and a name server translates the IP address of the server. To send information to a specific application running on a server, the client must also know the port number for that application. For example, most web servers listen on port 80. Servers typically run a few applications, such as a web server, a mail server, and an FTP server, and each application owns or listens on a specific port.
Starting a meeting

Tracing the sequence in which Breeze applications execute when users start a meeting can help you understand the primary system applications. The following list explains the typical order in which Breeze calls upon applications to place users successfully in a meeting:

1. The web browser collects the login credentials and communicates the credentials to Breeze Server.
2. Breeze Server accepts the login credentials and validates the user.
3. Breeze Server creates a session and sends the home page information to the browser. (Some users might not see the home page if they received a Breeze Meeting invitation directly.)
4. In the web browser, the user sees Breeze Meeting on the home page, clicks the link and presses the Meeting button to start the meeting.
5. Flash Player initiates communication with both Breeze Server and Breeze Meeting to participate in the meeting.
6. Breeze Meeting handles most of the requests from Flash Player to display media, such as video and audio, and to conduct screen sharing.
7. Breeze Server interacts with Flash Player to provide meeting services, such as content display and views into the Content library.

Planning for bandwidth requirements

There are many network factors that can affect the Breeze Meeting experience. This section contains information and suggestions that will help you understand bandwidth requirements so the system can provide sufficient resources for a successful Breeze Meeting experience.

A Presenter can configure the room bandwidth setting in a Breeze Meeting by accessing the Meeting menu and navigating to Meeting > Optimized Room Bandwidth. The default setting is for LAN connections. When you use a LAN connection, Breeze applications send high-quality audio, video and screen-shared images. Use the LAN setting only if all the users are on a high-speed network and Presenters are using high-end systems (2Ghz and faster desktop computers).

**Note:** The LAN setting not only increases bandwidth consumption but also increases CPU usage on the host's system. If CPU usage goes beyond 80%, latency will increase, resulting in choppy audio and video.

The users’ primary method of access determines the appropriate setting.

- Change the setting for the bandwidth option to DSL for users on LAN and broadband connections.
- Change the setting to Modem if most of the users are using a modem connection.
Calculating bandwidth usage

Here are some bandwidth calculations based on a meeting with audio, video, and slides. Calculations are based on 1024x768 full screen.

• Room bandwidth: Modem setting
  ■ One Presenter can generate about 26 Kbits/sec of data.
  ■ Viewers need about 29 Kbits/sec of downstream bandwidth to have a good experience.
  ■ Having more than one Presenter on a modem room setting is not recommended.
  ■ Screen sharing is not recommended for use with the Modem bandwidth setting.
  ■ If screen sharing is added to Modem, the total bandwidth required is about 49 Kbits/sec. This is close to saturating a modem connection. Any bottleneck in the network can cause latency or an undelivered message.

• Room bandwidth: DSL setting
  ■ One Presenter generates close to 125 Kbits/sec of data.
  ■ Each viewer requires about 128 Kbits/sec to consume all the data generated.
  ■ Adding screen sharing requires 184 Kbits/sec.
  ■ To have a good Breeze Meeting experience with the DSL setting, make sure viewers have available at least 200 Kbits/sec downstream bandwidth and Presenters have a 200 Kbits/sec upstream bandwidth.

• Room bandwidth: LAN setting
  ■ One Presenter generates close to 250 Kbits/sec of data.
  ■ Each viewer requires about 255 Kbits/sec to consume all the data generated.
  ■ Adding screen sharing requires about 300 Kbits/sec.
  ■ To have a good Breeze Meeting experience with the LAN setting, make sure viewers have available at least 400 Kbits/sec downstream bandwidth and Presenters have a 400 Kbits/sec upstream bandwidth.

Note: The bandwidth requirements for screen sharing can vary according to the content being shared and the screen resolution. These numbers are a general guideline—actual capacity varies in each network environment.
Planning for directory services integration

Directory services integration lets the Breeze administrator synchronize the Breeze internal directory of users and groups with an external source such as an organization’s LDAP (Lightweight Directory Access Protocol) server. The Breeze administrator can synchronize the internal and external directories on demand or at scheduled intervals. Directory services integration allows those external users and groups that originate in a corporate database to continue to coexist with the internal users and groups created with Breeze.

A directory service is like a database, but tends to contain more descriptive, attribute-based information. The information in a directory is generally read much more often than it is written. Only complete directory service updates are allowed. No partial updates are permitted. They replicate information widely in order to increase availability and reliability, while reducing response time.

Directory services integration lets Breeze incorporate the information about an organization’s users and groups. Breeze administrators do not need to perform manually the arduous processes of recreating users and groups. Breeze uses LDAP to access the organization’s information directories. LDAP is an industry-standard access method to directory services. The LDAP protocol is supported by Microsoft Active Directory along with most other user directories.

With the LDAP protocol, Breeze acquires its user data directly from an organization’s user directory, including basic information such as email addresses, names, phone numbers, and the users’ groups and departments. After the Breeze internal directory has been synchronized through the LDAP (or SLDAP) protocol to the organization’s directory for authentication, Breeze identifies the external users and groups as Breeze users and groups.

Directory services integration allows organizations to continue using their existing network user names, email lists and other attributes in Breeze while retaining the ability to create Breeze-specific users and groups. After the directory service and the Breeze directory are integrated, users may keep their existing network passwords and login to Breeze. The degree of integration is determined by the organization’s information technology (IT) policies and executed by the Breeze administrator.

Synchronization of directories

The general approach to integrating Breeze users and accounts with external directories such as an organization’s human resources databases is to synchronize the Breeze internal directory of users and groups with some or all of the directory service. Synchronization copies the information from the organization’s directory to the Breeze directory. The Breeze administrator schedules the synchronizations, and defines the level of integration with Breeze on the Application Management Console screens.
Directory services integration

In an LDAP schema, all directory entries are arranged in a hierarchical tree-like structure that reflects the organization's political, geographic, or administrative regions. For example, the IT administrator at a company with multiple worksites wants to let everybody in the organization use Breeze. In this scenario, the company's directory structure consists of multiple organizational units, and these are represented by four directory branches: San Francisco, Boston, Singapore, and Paris. Everyone in the organization has a Windows domain account listed in the Microsoft Active Directory. The IT administrator would like to offer Windows users a single sign-on, or at a minimum, the ability to use their domain login to access Breeze.

The administrator synchronizes the organization's directory with Active Directory using the four branches to perform an initial synchronization. The administrator may in the future employ a solution accelerator to integrate the Breeze login screen with Windows authentication, and configure the Windows NT LAN Manager (NTLM) authentication to allow users to skip the Breeze login screen.

The NTLM protocol is the default protocol for network authentication in many different versions of Windows. NTLM uses a challenge-response mechanism for authentication, in which clients are able to prove their identities without sending a password to the server. This procedure retrieves the user’s Windows credentials to validate the user’s access to Breeze.

The IT group schedules synchronization to begin every day at 2:00 A.M. when the demand on system resources is low and to incorporate any changes since the previous synchronization. The administrator routinely checks the synchronization logs to monitor the status of the scheduled synchronization.

Planning for SSL

SSL, or Secure Socket Layer, is a technology that allows web browsers and web servers to communicate over a secured connection. This means that the data being sent is encrypted by one side, transmitted, and then decrypted by the other side before processing. This is a two-way process, meaning that both the server and the client's browser encrypt all traffic before sending out the data.

An important aspect of the SSL protocol is authentication. During your initial attempt to communicate with a web server over a secure connection, that server will present your web browser with a set of credentials in the form of a certificate as proof the site is who and what it claims to be. In certain cases, the server may also request a certificate from your web browser, asking for proof that you are who you claim to be. This procedure is known as client authentication.

Breeze can be configured to use SSL, a secure protocol for transmitting private documents over the Internet. SSL does not provide any inherent encryption capabilities, but instead performs the appropriate URL and data mapping to allow HTTPS URLs to access Breeze and the desired content.
Implementing SSL for Breeze

There are two options available for implementing SSL-based authentication with Breeze:

- Using the native support in Flash Communication Server's (FCS) for SSL.
  
  Use this option if you want to secure only Breeze and not the web application. You will need 2 IP addresses (2 DNS entries for the IP addresses) and 1 SSL certificate. You will need to modify SSL tags in the Flash Adaptor.xml and Server.xml files configuration files.

- Adding an external hardware SSL accelerator
  
  Use this option if you want to secure both FCS and the Breeze application. You will need 2 IP addresses - 2 DNS entries for the IP addresses -- and 2 SSL certificates.

  You need to purchase the accelerator separately. When you use Breeze with an SSL hardware accelerator, all logins to Breeze are sent over the secured protocol HTTPS.

Port number for SSL

The Internet uses well-known ports for unencrypted HTTP-based web traffic and encrypted HTTPS-based web traffic. Unencrypted traffic generally goes to port 80, and encrypted traffic generally goes to port 443. SSL hardware accelerators work by intercepting traffic on port 443, decrypting the information, and sending it back to the Breeze server through port 80. There is no indication to the Breeze server that the original data was encrypted.

Without SSL, all logins are conducted over HTTP connections. After you are connected to the Breeze server, all presentations and meetings are delivered over standard unencrypted HTTP and RMTP connections.

Planning for security

Breeze is a server-based web application integrated with a database to provide a powerful solution for online training and conferencing. By hosting Breeze Server and its applications on your intranet or the Internet, you are providing users the flexibility to access information anywhere at any time.

Any application run over a network, especially the Internet, has security risks associated with it. Macromedia Breeze is no different. However, these security threats can be minimized if you give careful consideration to implementing a security plan for Macromedia Breeze.

There are three levels of security that should be considered for Macromedia Breeze:

- Application-level security
- Physical security
- Infrastructure security

Breeze provides application-level security, which provides an ACL (Access Control List)-based security model for controlling which users have access to which features in the Breeze applications. Physical security means placing the actual Breeze server in a physically-secure location. The third level, infrastructure security, which deals with securing the server and the network, is the most important, yet most overlooked aspect of securing Breeze.
The discussion on security is divided into the following sections:

- Security levels
- Solutions for a secure infrastructure
- Best practices
- Additional references

### Security levels

When planning a security strategy, it is important to consider the various layers in a deployed server environment, and devise a security plan for each layer. Typically, a comprehensive security strategy incorporates the following elements:

- Infrastructure security
- Application-level security
- Physical security

### Infrastructure security

Infrastructure security is by far the most important, but most overlooked, aspect of securing Breeze. It is up to your IT department or administrator to provide a secure infrastructure for Breeze.

There are three parts to providing a secure infrastructure for Breeze:

- Network security
- Breeze web server
- Database server security

The following sections describe a secure infrastructure. The security measures you implement depend on whether your Breeze system consists of a single server running in the DMZ (demilitarized zone) or an elaborate multiserver system running with different trusted zones.

### Network security

Breeze relies on several private TCP/IP services for its communications. These services open several ports and channels for private communication. These ports must be protected from outside users. Breeze’s design requires the environment to provide security for these communications. Sensitive ports should be placed behind a firewall that separates them from non-trusted computers.

If you intend to have users access Breeze on your intranet, you should place the Breeze servers and the Breeze database in a separate subnet, separated by a firewall. This configuration of the firewall should take into consideration all Breeze ports and whether they are configured for inbound or outbound traffic.

If you intend to have users access Breeze on the Internet, it is extremely important that you separate the Breeze servers from the Internet with a firewall. If you do not take the necessary steps to secure the Breeze servers, you are leaving your valuable information available for anyone to steal. For more information, see “Security resources and references” on page 22.
**Breeze web server**

Breeze comes with its own built-in, high-performance, secure web server. This web server is based in part on Macromedia JRun Enterprise Server and has been designed specifically to serve dynamic content for Breeze, including Breeze Meetings, Breeze Presentations, Breeze Seminars, and other rich media content. Because of Breeze's special requirements, no other web servers (such as Apache) can be used with Breeze.

**Database server security**

Whether or not you are hosting your database on the same server as Breeze, 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.

The Microsoft security website contains information that applies to both securing SQL Server 2000 and the embedded database engine: www.microsoft.com/sql/techinfo/administration/2000/security/.

The following link provides a good starting point to making sure that your database is secure: www.microsoft.com/sql/techinfo/administration/2000/security/securingssqlserver.asp.

**Note:** Macromedia Breeze supports SQL authentication only. You must install SQL Server with mixed-mode authentication. Breeze does not support Windows Authentication Mode.

If you are running the embedded database engine, the database uses *breeze* as the password by default. You should change this password after you install Breeze and verify that all its applications are functioning. To change the password, type the following at the command line:

```bash
osql -E -Q "sp_password @new = 'new_password', @loginame = 'sa''"
```

where `{new_password}` is a strong password.

**Solutions for a secure infrastructure**

Most Breeze configurations fall into one of two configurations:

- A single-server configuration
- A multiple-server configuration (a cluster)

This section discusses both configurations and provides examples on how to secure these environments.
**Single-server configuration**

The easiest solution for a dedicated, single-server Breeze system is to block all ports on the server except 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, a software-based firewall can be configured to enable additional security.

The following procedure assumes that you are setting up Breeze Server on a single computer. The database is to be installed on this computer, too. It is also assumed that you want users to be able to access Breeze on the Internet.

**To secure Breeze on a single server:**

1. Install a firewall.

   Since you are allowing users to access Breeze 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 a 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 Breeze, you do not need to open up port 1433 on the firewall.

3. Install Breeze.

   For more information, see Chapter 3, “Installing and Upgrading Breeze,” on page 35.

4. Verify that the Breeze applications are working.

   After installing Breeze, you should verify that Breeze is working properly both from the Internet and from your local network. For more information, see Chapter 5, “Verifying Your Installation,” on page 91.

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.

**Multiserver solutions**

Multiserver (cluster) solutions are inherently more complex. A Breeze cluster can be located with a data center or geographically distributed across multiple Network Operation Centers. If you choose to, you can install and configure servers hosting Breeze in multiple locations and synchronize them through database replication. Note that SQL Server is required for any multiserver solution.
It is very important that you understand how to secure a multiserver installation. The following are suggestions for securing multiserver solutions.

- **Private networks**
  The simplest solution for multiserver solutions in a single location is to create an extra subnet for the Breeze system. This solution offers a high level of security, but it can be expensive.

- **Local software firewalls**
  For the Breeze servers that are located in a cluster but share a public network with other customer servers, a software firewall may be appropriate on each individual server.

- **VPN systems**
  In multiserver installations where there are multiple Breeze servers in different physical locations, customers 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. Breeze relies on this external security if data traffic must be encrypted.

**Application-level security**

Breeze has a built-in ACL (Access Control List)-based security model that lets you assign users different permissions to access Breeze's features. For example, you can control which users have permissions to publish presentations by adding them to the Account Authors group. You can also control which folders individual users can publish to.

Breeze has seven primary groups that grant users access to specific features in the Breeze system. By adding users to these groups, you can control the kind of the role a user has in your Breeze account.

These groups are as follows:
- **Administrators**
  Members of the Administrators group have access to all functions in the Breeze account. They can create and manage users, manage content, create and manage courses and create and manage meetings.

  A member of the Administrators group also needs to be a member of the relevant groups in order to:
  - publish content
  - organize events
  - create meetings
  - present seminars
  - create courses
  - enroll users
  - send notifications
• Authors
  Members of the Account Authors group have access to publishing features. They can publish content to the Breeze system.

• Events Administrators
  This group includes anyone who organizes events. An event can be any meeting, presentation, course, curriculum, or seminar that requires registration and generates reports with participant tracking information.

• Learners
  This group includes anyone who attends any meeting, presentation, course, curriculum, or seminar.

• Meeting Hosts
  Members of the Meeting Hosts group can perform all functions associated with creating meetings, including setting up a meeting, inviting participants, sending invitations and viewing reports.

• Seminar Administrators
  This group includes those who present seminars. A seminar is a special kind of meeting with its own attributes and licensing structure.

• Training Managers
  Members of the Training Managers group manage the Meeting library, including creating courses, incorporating course content from Authors, enrolling users, sending enrollee notifications, and setting up course reminders. They can also view content and course reports.

In addition to adding users to groups to grant them rights to use features in the Breeze system, you can also grant them permissions to access specific folders, content, courses and meetings. For example, you can control whether or not a certain Author has permissions to publish to a specific folder.

For more information on using Breeze's application-level security features, refer to the Breeze Manager User Guide.

Physical security

Customers who store sensitive information on their servers should be aware of the physical security of their systems. Breeze relies on the safety of the host system against intruders. Servers should be kept secured when private and confidential data is at risk. Breeze is designed to take advantage of native environmental features like file system encryption when available and if configured by the user.
Best practices

The following is a checklist of best practices that will assist you in securing Breeze.

- Protect your servers with firewalls.
  You should place the Breeze server behind a firewall, especially if Breeze is accessed through the Internet. If you do not place Breeze behind a firewall, you are leaving the server open for attacks. Your sensitive information is unsecured and open for theft. All servers should sit behind a firewall, including the system(s) hosting Breeze and the database server.

- Run only the services you need.
  You should run only the services you need for Breeze. This means that you should not run applications like a domain controller, a web server or an FTP server on the same computer as Breeze. By reducing the number of applications and services running on the computer hosting Breeze, you can minimize the chances that another application can be used to compromise the Breeze server.

- Update operating system security.
  For Windows and other platforms, customers need to check regularly for critical updates that close platform security holes and apply the required patches. Some of these issues are eliminated by a firewall. In general customers should keep their servers patched with all current security updates approved by Microsoft and the other appropriate platform vendors.

- Update database security.
  Since your database may be another targeted application of the Breeze solution, you need to check for database server security holes and apply the required patches. Like the operating system, some issues are eliminated by a firewall, but you must continue applying the latest patches.

- Secure host systems.
  Customers who store sensitive information on their servers should be aware of the physical security of their systems. Breeze relies on the safety of the host system against intruders, so servers should be kept secured when private and confidential data is at risk. Breeze is designed to take advantage of native environmental features like file system encryption.

- Use strong passwords.
  Breeze users are protected by passwords. Users, and particularly administrators, should choose strong passwords to keep their data safe. Breeze enterprise installations often use Microsoft SQL Server, which also requires strong password protection.

- Perform regular security audits.
  Users should audit their systems periodically to ensure that all security features they installed are still operating as expected. For example, firewalls are easily tested using a port scanner for validation.
Security resources and references

The following are sources of information and software that may aid the process of securing the Breeze server(s).

- Network security
  SANS Institute (www.sans.org)  The SANS (System Administration, Networking, and Security) Institute is a cooperative research and education organization comprised of system administrators, security professionals, and network administrators. It provides great network security courses, as well as certification in network security.

- SQL Server security
  Microsoft Security Resources page (www.microsoft.com/sql/techinfo/administration/2000/security)  This page on the Microsoft website provides information and resources on securing SQL Server 2000. The information on this page also applies to the embedded database engine installed with Breeze.

- Tools
  NMap (www.insecure.org/nmap/index.html)  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).

The effectiveness of any security measure is determined by various factors, including but not limited to, the security measures provided by the server and the installed security software.

Macromedia Breeze software is not intended to provide security against any unauthorized access to, or unintended or intended disruptions or harm against, your servers or any information stored or deployed by you on any computer, including servers. For more information, see the disclaimer of warranty in the applicable license agreement provided with Macromedia Breeze.

Ports used by Breeze

The following table lists the ports used by Breeze:

*Note:* RTMP is a Macromedia-specific protocol.

<table>
<thead>
<tr>
<th>Port</th>
<th>Port Configurable</th>
<th>Bind Address</th>
<th>Bind Address Configurable</th>
<th>Access</th>
<th>Protocol</th>
<th>Password Protected</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>Yes</td>
<td>Default=any</td>
<td>Yes</td>
<td>Public</td>
<td>RTMP</td>
<td>Yes</td>
</tr>
<tr>
<td>1935</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>over HTTP</td>
<td></td>
</tr>
<tr>
<td>443</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>HTTP</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RTMP</td>
<td></td>
</tr>
<tr>
<td>1111</td>
<td>Yes</td>
<td>Default=any</td>
<td>Yes</td>
<td>Private</td>
<td>RTMP</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>HTTP</td>
<td></td>
</tr>
</tbody>
</table>
Available Breeze configurations

You can install Breeze on one server or on a group of connected servers, usually called a cluster. The terms in your Breeze license determine which configuration is allowed. The single-server configuration is easier to administer.

Depending on your organization’s licensing and performance needs, you may choose to install Breeze in a multiserver configuration. You will need a special Breeze license file to run a Breeze cluster. If your Macromedia Breeze license permits, you can install Breeze Server on two or more computers and then cluster the computers with load balancing and failover.

Clustering Breeze has the following advantages:

- You can effectively use third-party hardware or software to provide load balancing and failover for HTTP requests.
- All computers in a cluster have copies of the same contents. If one computer in the cluster fails, the content on another computer in the cluster can take over and supply the same content.
• Clustering Breeze allows the computers in a cluster to share session data with each other for effective load balancing and failover.

Planning for a Breeze Server cluster

In a Breeze Server cluster, an identical copy of Breeze is installed on each server in the cluster. Each server must be able to access the Breeze database of users and groups. Because licensing restrictions do not allow more than one Breeze Server to access the embedded database engine, you must use Microsoft SQL Server 2000 as the database engine in a cluster.

Make sure the required hardware applications are operating and communicating with each other before you start the installation. For more information, see “Installation requirements” on page 25.

The following figure illustrates how to create a cluster of three servers running Breeze with a load balancer and shared access to the SQL Server 2000 database engine and the Breeze database of users and groups.
You configure Breeze on the clustered servers during the installation and post-installation by performing the following:

- Installing Breeze on each server in the cluster.
- Setting the values in the Breeze custom.ini configuration file on one server in the cluster.
- Making sure there is a copy of this configuration file on all servers in the cluster.

For more information, see Chapter 4, “Post-installation,” on page 57.

**Installation requirements**

This section lists the hardware and software requirements for those systems where Breeze Server is to be installed. For optimal performance, and to ensure the installation is not unnecessarily complicated, you should install Breeze on a dedicated computer.

This section covers the following topics:

- Breeze server requirements
  - Hardware requirements
  - Software requirements
- Additional software requirements for Breeze servers
- Breeze user requirements
  - Content Viewers, Course Learners, and Breeze Meeting Participants
  - Breeze Meeting Presenters
  - Content Authors and Course Developers

**Breeze server requirements**

The recommended and minimum hardware requirements are provided in this section. If you are going to use a cluster of Breeze servers, each computer in the cluster must meet the same hardware requirements. Deploying identical servers in a cluster is also recommended.

**Hardware requirements for the Breeze server**

The configuration of the Breeze server depends upon the terms in your Breeze license. Here are the recommended, minimum, and SSL-enabled hardware requirements.

- Recommended requirements:
  - Dual Pentium IV, 2-GHz or Xeon processor
  - 2GB of RAM
  - 100+ GB hard disk
  - CD-ROM drive
  - 10 MB Network Connection
• Minimum requirements:
  ■ Pentium 4, 2-GHz processor
  ■ 1 GB of RAM
  ■ 80 GB hard disk
  ■ CD-ROM drive
  ■ 1.5MB Network Connection (T1)
• For Breeze deployment with encrypted SSL enabled:
  ■ SSL Hardware Accelerator (optional)
• Communication ports
  ■ Port1935 for RTMP
  ■ Port 80 or other for HTTP
  ■ Port 443 secured if SSL is enabled
For a complete list of ports used by Breeze, see “Ports used by Breeze” on page 22.

Software requirements for the Breeze server
• NTFS (NT file system)
• Supported operating systems
  ■ Windows 2000 Server
  ■ Windows 2003 Server
For other supported languages, review the system requirements for French, German, Japanese, and Korean.
• Supported database
  ■ SQL Server 2000 (English version)
    This is the preferred database engine for production environments. Make sure to install it in mixed-mode. This will give you the option to use SQL or Windows authentication. Breeze supports SQL authentication only.
    SQL Server is required for configurations of multiple Breeze servers (a cluster) or multi-processor computers with HyperThreading enabled.
  ■ The embedded database engine installed with Breeze is suitable for testing and development environments, and for workgroups.
    The embedded database engine is shipped with Macromedia Breeze. This engine is built and based on core SQL Server technology. The common technology base shared between SQL Server and the embedded database engine enables developers to build applications that can scale seamlessly from portable computers to a cluster of computers.
    The embedded database engine does not have its own user interface (UI) or tools. Users interact with the embedded database engine through the Breeze application in which it is embedded.
    For information about choosing the embedded database engine or Microsoft SQL Server 2000, see “The Breeze database” on page 29.
Additional software requirements

The computers hosting Breeze Server also require the following software:

- An SMTP e-mail server
  Breeze Server requires an SMTP e-mail server for sending e-mail notifications.
  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.
- The NTFS file system

To verify that the server is using NTFS, do the following:
1. Double-click the My Computer icon on the Windows desktop.
2. In the My Computer window, right-click the drive where Breeze is to be installed and select Properties from the Context menu.
   In the General tab of the Local Disk Properties dialog box, the File System area should specify NTFS.

For updated Breeze system requirements and recommendations, see www.macromedia.com/go/breeze_sysreqs.

Breeze user requirements

Every user's computer must meet the following software and hardware requirements, which vary according to the user's role.

Learners and participants

The following software must be installed on these users' computers:

- Windows 98SE, ME, XP, NT 4.0, 2000, 2002, or 2003
- Supported browsers in Windows
  - Internet Explorer 5.0, 5.5, 6.0
  - Netscape Navigator 6.2, 7.1
  - AOL 8, 9
  - Compuserve 7 (2000, 2003 and XP only)
  - Firefox 1.0

or:
- Macintosh OS X 10.1 or later
- Supported browsers on Macintosh
  - Safari 1.1, 1.2, 1.3
  - Netscape 6.2, 7.1
  - Microsoft Internet Explorer 5.2
  - CompuServe 7 (OS 10.1 or later)
  - Firefox 1.0
Additional requirements:
- Macromedia Flash Player 6.0.79 or later
- Minimum bandwidth requirements: 56 kb/sec

**Breeze Meeting presenters**

The following software must be installed on these users’ computers:
- Windows 98SE, ME, XP, NT 4.0, 2000, 2002, or 2003
- Supported browsers in Windows
  - Internet Explorer 5.0, 5.5, 6.0
  - Netscape Navigator 6.2, 7.1
  - AOL 8, 9
  - Firefox 1.0

or:
- Macintosh 9.2, OS X 10.1 or later
- Supported browsers on Macintosh
  - Safari 1.1, 1.2
  - Netscape 6.2, 7.1
  - Microsoft Internet Explorer 5.2
  - CompuServe 7 (OS 10.1 or later)
  - Firefox 1.0

Additional requirements:
- Macromedia Flash Player 6.0.65 or later
- Web camera and microphone (optional)

For additional information, please visit the Breeze Resource Center at www.macromedia.com/resources/breeze/

**Authors and training managers**

The following software and hardware must be installed on these users’ computers.
- Windows XP, Windows 2000, 2002 or 2003
- Microsoft PowerPoint 2000, PowerPoint XP (2002), or PowerPoint 2003
- 600 Mhz Pentium III processor or equivalent
- 256 MB or more of RAM (128 MB minimum)
- Resolution 1024 x 768 or higher (800 x 600 minimum resolution)
The Breeze database

Breeze Server requires a database created with either the embedded database engine or Microsoft SQL Server 2000. The Breeze database stores information about users, content, courses, meetings, and reports.

- The embedded database engine comes with Macromedia Breeze. You install it at the same time that you install Breeze Server.
- Breeze Server deployed in a configuration with multiple computers (a cluster, for example) or with multiprocessor computers with HyperThreading requires SQL Server 2000.
- If you use Microsoft SQL Server 2000 as the database engine, make sure to install it in mixed-mode. This gives you the option to use SQL or Windows authentication. Breeze supports SQL authentication only.
- The database must be set to case insensitive. For more information on configuring the database, see Chapter 4, “Post-installation,” on page 57.

Limitations of the embedded database engine

The embedded database engine that comes with Macromedia Breeze has the following limitations:

- The licensing agreement restricts installation and use of the embedded database engine to the computer hosting Breeze Server.
- Because of licensing restrictions, you can install the embedded database engine only on a single-processor computer.
- 2 GB is the maximum size of the Breeze database using the embedded database engine.
- The embedded database engine has a command-line interface for managing and querying the database, in contrast to Microsoft SQL Server 2000, which has tools with graphical user interfaces for executing these tasks.

Database engine recommendations

The following recommendations should guide your choice of database engine:

- Consider using the embedded database engine installed with Breeze for testing and development. It uses the same data structures as SQL Server.
- In production environments, give preference to the Microsoft SQL Server 2000 engine. SQL Server is a scalable DBMS designed to support a significantly larger number of concurrent users.
CHAPTER 2
Preparing to Upgrade

This chapter provides instructions about the preparatory tasks you need to complete before you start the upgrade process from Macromedia Breeze version 4.1 to version 5. This chapter provides detailed information about the following phases of the upgrade process:

- “Overview” on page 31
- “Before you begin” on page 32
- “Backing up your Breeze files” on page 32
- “Backing up the Breeze database” on page 33
- “Preparing for the upgrade” on page 34

Overview

Breeze 5 incorporates the upgrade process into the Installer and the Application Management Console. These tools, with their graphical user interfaces, guide you through the upgrade from Breeze 4.1 to Breeze 5. This is the only direct upgrade path that this version supports.

If you are upgrading from a version of Breeze earlier than version 4.1, you must upgrade to each successive version; for example:

- To upgrade from Breeze 4, you must follow this two-phase upgrade procedure:
  a. Upgrade from Breeze 4 to Breeze 4.1.
  b. Install Breeze 5 to upgrade to Breeze 5.
- Macromedia does not support a direct upgrade from Breeze 4 to Breeze 5.
- To upgrade from a version of Breeze earlier than 4, administrators should contact Breeze Support before proceeding.

When you contact Support, you need to have available the Breeze License Certificate from Macromedia that came with the product. This certificate contains a unique serial number that identifies you as a Macromedia customer and authorizes your installation and use of Breeze 5.
Before you begin

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

• Allocate enough time to ensure a successful upgrade. Macromedia recommends that you schedule one day of downtime for a Breeze upgrade.
• Let your users know in advance that they won’t be able to use Breeze during the upgrade. Also, let them know what types of changes they can expect (such as new features or improved performance) after the upgrade.
• Back up all Breeze content, the database, and the custom.ini and config.ini configuration files using the following procedures.

Backing up your Breeze files

To back up your Breeze files:

1. Stop all Breeze services. From your Windows desktop, select Start > Programs > Macromedia > Macromedia Breeze > Stop Breeze Server.
2. Make a copy of the content directory within the Breeze installation path. The default location is C:\breeze\content.
3. Make a copy of the config.ini file within the installation path. The default location is C:\breeze\appserv\conf\config.ini.
4. Make a copy of the custom.ini file within the installation path. The default location is C:\breeze\.
5. Stop the database service:
   • From your Windows desktop, select Start > Settings > Control Panel > Administrative Tools > Services. Right-click MSSQLSERVER in the Services window and select Stop from the context menu.
6. Back up your database files:
   • If you’re accessing the embedded database engine, make backup copies of the database files breeze.mdf and breeze_log.ldf. The default location is C:\mssql\data\.
   • If you’re using Microsoft SQL Server, you can use the Enterprise Manager to back up your database. On your Windows desktop, select Start > Programs > Microsoft SQL Server > Enterprise Manager. In the Tree pane of the Enterprise Manager window, select the Breeze database (named breeze, by default), and then select Tools > Backup Database.
Backing up the Breeze database

The Breeze database includes the collected records of Breeze users and groups.

To back up the Breeze database:

1. Restart your database:
   ■ From your Windows desktop, select Start > Settings > Control Panel > Administrative Tools > Services. In the Services window, right-click MSSQLSERVER and select Start from the context menu.

2. From your Windows desktop, select Start > Run.

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

4. In the DOS prompt window that appears, type `cd \` and press Enter.

5. At the prompt, change to the directory where you installed the database. Type `cd mssql\binn` and press Enter.
   The default root directory is C:.

6. At the `root\MSSQL\Binn` prompt, type `osql -U sa -P breeze -d breeze` and press Enter.
   The OSQL utility allows you to execute commands against a database, where:
   - `U` specifies the database user
   - `P` specifies the password
   - `breeze` is the default password
   - `d` specifies the database name
   If you changed the password for the system administrator or database account, use your password in place of `breeze`.
   To access help information for database commands, type `osql ?` at the DOS prompt and press Enter.

7. At the `1>` prompt, type `BACKUP DATABASE breeze TO DISK = '<root>:\breeze.bak'` and press Enter.

8. At the `2>` prompt, type `go` and press Enter.
   A message appears, indicating whether the backup was successful.

   For more information on backing up your database, consult your database documentation.
   Also, see the Microsoft Knowledge Base article on how to back up your database: `http://support.microsoft.com:80/support/kb/articles/Q241/3/97.ASP`.

9. At the `3>` prompt, type `quit` and press Enter.

10. Verify that the backup was successful: confirm that the breeze.bak file exists at the root (C:\ by default).
Preparing for the upgrade

To prepare your system for the Breeze upgrade:

1. Stop the Macromedia Breeze Application Service, which stops Breeze Presenter and Breeze Training:
   b. In the Services window, right-click Macromedia Breeze Application Service and select Stop from the context menu.

2. If you have Breeze Meeting, stop the Flash Communication Admin Service and Flash Communication Server.
   ■ Use the same Services window and follow the procedure outlined in step 1.

3. Verify that you backed up the following directories and files:
   ■ The entire Breeze server content directory
   ■ The custom.ini file
   ■ The config.ini file
   ■ The breeze.mdf and breeze_log.LDF database files

   **Warning:** Do not uninstall your database.

When you complete these backup tasks, you are ready to install the new software and upgrade to Breeze 5. The Installer and the Application Management Console can recognize Breeze 4.1 software and will initiate the upgrade.
This chapter presents information on the following topics:

- “Installation checklist” on page 35
- “Installation and configuration overview” on page 36
- “Using the Breeze installer” on page 37
- “The Application Management Console” on page 43
- “Starting and stopping Breeze components” on page 53
- “Uninstalling Breeze” on page 54
- “Troubleshooting” on page 54
- “Breeze technical support” on page 55
- “Macromedia online forums” on page 55

**Installation checklist**

Before you begin the installation process, check that all the requirements listed in “Before You Begin” on page 9 are satisfied. In addition, verify that your system meets the following requirements, which are critical for a successful Macromedia Breeze installation:

- A fully qualified Domain Name Service (DNS) for the Breeze server.
  
  For example, example.breeze.com

  For more complete information about DNS, see “DNS configuration guidelines” on page 59.

- The NT file system (NTFS) is employed.
  
  Breeze does not support the FAT 32 file system.
To verify that the system employs NTFS:
1. On your Microsoft Windows desktop, double-click My Computer.
2. In the My Computer window, right-click the drive where Breeze is installed and select Properties from the context menu.
   In the General tab of the local Disk Properties window, the file system should specify NTFS.
- Adequate disk space is available on the drive or server where you want to install Breeze Server:
  - 1,224.4 MB free disk space for Breeze installation
  - 1 GB for the Breeze server
  - 10 GB per 100 presentations
  - 80 GB for the initial storage of Breeze Meeting files
    Disk requirements increase as more Breeze Meetings are stored.
- You are using Flash Player 7.

To confirm the Flash Player version you are using:
1. Right-click any Flash player content, including that found on www.macromedia.com. The Context menu should read About Flash Player 7, or specify a later version.
2. If the Context menu specifies an earlier version, click About Flash Player in this menu to download the latest Flash Player 7 version. You can also download Flash Player from www.macromedia.com/go/getflashplayer.

You also need the Breeze License Certificate from Macromedia. The certificate shipped with the installation CD and contains a unique serial number for your installation. Enter this serial number when prompted.

For updated Breeze system requirements and recommendations, see www.macromedia.com/go/breeze_sysreqs.

Installation and configuration overview

To assist you with installing and configuring Breeze, you will interact with a series of Breeze Installer and Application Manager Console screens. Have this guide open to this chapter as you proceed.

To install and configure Macromedia Breeze:
1. Make sure that you meet all hardware and software requirements described in “Installation checklist” on page 35.
2. Run the Breeze installer to install Breeze components.
3. Run the Application Management Console to configure your installation.
   The Application Management Console automatically starts after the Breeze installer completes its work.
4. Complete any configuration tasks not performed through the Application Management Console.
Using the Breeze installer

Use the procedures described in this section to install Breeze. Macromedia recommends that you close all other applications before you start to install Breeze.

To install and configure Breeze:
1. Insert the Breeze installation CD into the CD-ROM drive.
   If the Breeze installer does not start automatically, double-click the setup.exe file in the installation CD’s root folder.
   The installer Welcome screen appears.

2. Click Next.
   The License Agreement screen appears.
3. Read the agreement, click Accept, and click Next to continue. The Select Destination Location screen appears.

4. Click Next to accept the default installation (c:\breeze) location, or click Browse to select a different location, and then click Next.

If the default location already exists, the Folder Exists dialog box appears.
5. Click Yes to continue.
   The Company Information screen appears and asks you to enter your serial number.
   The License Certificate that comes with the installation CD contains the serial number.

6. Enter the serial number and click Next to continue.
   If the installer determines that a SQL database server is present on your system, the following notice appears. You do not need to uninstall the SQL server.
7. Click Next to continue.

   The Select Start Menu Folder screen appears.

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

   The Ready to Install screen alerts you that the Breeze installation is about to begin.

9. Review the choices for the destination folder where Breeze will be installed and for adding
   Macromedia Breeze to the Start Menu folder.
10. Click Back to review or change these settings or click Install to continue.

The Installing screen appears. The installer is extracting Breeze Server files on the installation CD and installing them. This process takes approximately two minutes.

11. Click Cancel at any time to terminate or cancel the installation.

You may also see the following message.
12. Click OK to continue.

You can reboot the server after the Breeze installation and configuration is complete.

The Initializing Macromedia Breeze service screen appears.

13. Select the option to start Breeze and press Next to continue.

A message appears that the Macromedia Breeze Application Service service is starting.

Breeze runs as a Windows service. Breeze is defined as the Macromedia Breeze Application service and the Flash Communication Server service in the Services screen. The Breeze Application Service is one of the services that Breeze uses.

The Completing the Macromedia Breeze Setup Wizard screen appears to alert you that the Setup is continuing the process of initializing Breeze.
Click Finish to complete the installation process. The Application Management Console opens to guide you through the tasks to configure Breeze Server.

**The Application Management Console**

After installing the software, the Breeze installer automatically starts the Application Management wizard to guide you through the next series of tasks. The Application Management Console provides a graphical user interface to the custom.ini configuration file, which is located in the folder where Breeze is installed.

In previous releases of Breeze, a customer had to configure the Breeze Server by manually editing the custom.ini configuration file. No user interface was available to validate entries or report errors to the administrator. If an error condition was encountered, the administrator had to sift through the log files to determine what went wrong.

The Console guides the Breeze administrator through a series of tasks, including the following:

- Configuring Breeze directory services
- Configuring the Breeze database settings
- Enabling recently purchased features of Breeze
- Identifying the primary Breeze administrator
- Naming the SMTP host, which is the email server that Breeze will use.
- Upgrading Breeze from a previous release
- Uploading the Breeze license file

You can also access the Console Manager through Start > Programs > Macromedia Breeze.

**Welcome**

The Welcome screen is the first screen of the Application Management Console.

Press Next to continue.
Configure the database settings

The Breeze administrator uses the Database Settings screen to configure the following variables for the Breeze database:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Default value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DB_HOST</td>
<td>localhost</td>
<td>Name of the Microsoft SQL Server 2000 host computer.</td>
</tr>
<tr>
<td>DB_NAME</td>
<td>breeze</td>
<td>Name of the Breeze database.</td>
</tr>
<tr>
<td>DB_USER</td>
<td>sa</td>
<td>User name for Breeze Server employed when creating and accessing the Breeze database.</td>
</tr>
<tr>
<td>DB_PASSWORD</td>
<td>breeze</td>
<td>Password for Breeze Server to use when creating and accessing the Breeze database. To change the default password, see “Changing the Breeze password” on page 88.</td>
</tr>
</tbody>
</table>

Click Next to continue.

The Console detects the release number of any Breeze software installed on your system. The Console automatically detects whether this is a fresh installation of Breeze 5 or an upgrade from Breeze 4.1.

- If you are installing Breeze for the first time, the Database Creation Confirmation screen appears.
- If you are upgrading from Breeze 4.1, the Upgrade Confirmation screen appears.
- If you are trying to upgrade from Breeze 4, the following screen appears.
Database creation

If the Breeze database whose name appears on the Database Settings screen (the DB_NAME variable in the custom.ini file) was not created, the administrator sees a confirmation screen. The administrator is asked to confirm whether to create the database or not.

Upgrade confirmation

The Upgrade Confirmation screen asks the administrator to confirm that they want to upgrade Breeze 4.1 to Breeze 5, and if the following backup procedures are completed:

- The content directory is backed up.
- The existing Breeze database is backed up.
- Breeze users were notified that Breeze will not be available during the upgrade.
The administrator must confirm that these procedures are complete before the Console can proceed with the upgrade to Breeze 5.

The Console creates a new Breeze 5 database. The data from the existing Breeze database is copied and migrated to a Breeze 5 database. You must specify a new name for the new database. Do not use the name of an existing database.

Step 3 of the Console asks you to verify that you completed the requirements in Steps 1 and 2. Click Upgrade Breeze to proceed.

Unsupported Version screen

If you are trying to upgrade from a version of Breeze older than 4.1, the Console displays a screen that states that upgrading to Breeze 5 from this version of Breeze is not supported.

- To upgrade from Breeze 4, you must first upgrade to Breeze 4.1 and then upgrade to Breeze 5.
  
To upgrade to Breeze 5, you must first migrate to Breeze 4.1. For information on migrating to 4.1, visit the Breeze licensed support site.

- To upgrade from a version of Breeze older than 4, contact Breeze Technical Support before you proceed.
Before you contact Breeze Technical Support, have the Breeze License Certificate from Macromedia available. The certificate contains the unique serial number required for your installation.

**Upgrade in progress screen**

The Console displays an upgrade in progress screen informing the administrator of the status of the upgrade. The system refreshes the screen every five seconds as the upgrade progresses.
Breeze Server settings

The Breeze administrator defines the settings for the Breeze Server on the Breeze Server Settings screen.

Click Next to continue.
The following table describes the fields on the Breeze Server Settings screen:

<table>
<thead>
<tr>
<th>Field</th>
<th>Default value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Name</td>
<td>[none]</td>
<td>Enter a name that readily identifies the Breeze account, such as “Enterprise Account” or “My Breeze 5 Account.”</td>
</tr>
<tr>
<td>BCC_EMAIL</td>
<td>[none]</td>
<td>Blind-copy e-mail address to which all notifications that users receive are also sent. This variable allows administrative tracking of e-mail messages sent through Breeze without exposing an internal e-mail address. The following example shows how to set this variable: BCC_EMAIL=<a href="mailto:sjones@mycompany.com">sjones@mycompany.com</a></td>
</tr>
<tr>
<td>Breeze Host</td>
<td>[none]</td>
<td>Enter the URL for accessing Breeze as a fully qualified domain name. Users wanting to connect to Breeze enter this URL in their browsers.</td>
</tr>
<tr>
<td></td>
<td>[BREEZE URL]</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>For example, for the URL <a href="http://aserver.mybreeze.com">http://aserver.mybreeze.com</a>, you set ADMIN_HOST as shown in the following example:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>aserver.mybreeze.com</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If your Breeze Server will use a port other than port 80 for receiving HTTP messages, you must add the port number to the host name, as shown in the following example:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>aserver.mybreeze.com:8080</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The Console displays this URL as the External Name for Breeze in the Host Mapping entry on this panel.</td>
</tr>
<tr>
<td>Host Mapping</td>
<td>[none]</td>
<td>Host name and external name (the fully qualified domain name) of the Macromedia Breeze site. Breeze supplies the values for these fields.</td>
</tr>
<tr>
<td>[ADMIN_HOST]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HTTP Port</td>
<td>80</td>
<td>The default port for HTTP is port 80. If your Breeze Server uses a port other than port 80 for receiving HTTP messages, you must add the port number to the host name in the URL for accessing Breeze.</td>
</tr>
<tr>
<td>SMTP_HOST</td>
<td>mail</td>
<td>The name of the outgoing SMTP mail server for Breeze to use to send e-mail notifications.</td>
</tr>
<tr>
<td>SUPPORT_EMAIL</td>
<td>[none]</td>
<td>The e-mail address or URL within your organization where you want to direct users when they need technical support or help with using Breeze. The address or URL you enter is used in Breeze e-mail notifications.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The following examples show how you can set this variable:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SUPPORT_EMAIL=<a href="http://www.mydomain.com/breeze/support/index.html">http://www.mydomain.com/breeze/support/index.html</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td>SUPPORT_EMAIL=<a href="mailto:breezesupport@mydomain.com">breezesupport@mydomain.com</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td>If you do not change the default value, users see this default text instead of a support location.</td>
</tr>
<tr>
<td>SYSTEM_EMAIL</td>
<td>[none]</td>
<td>The e-mail address that users see as the source of notifications sent by Breeze and to which they can send responses.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You can define the user name in the e-mail address as an alias so that more than one person receives user responses. The following example shows how you can set this variable: SYSTEM_EMAIL=<a href="mailto:breeze@mycompany.com">breeze@mycompany.com</a></td>
</tr>
</tbody>
</table>
Upload the Breeze license file

The Upload License File window appears. An Internet connection is required at this point. The Breeze license file identifies those Macromedia Breeze applications that you are authorized to use. Have the Breeze License Certificate from Macromedia available. The license contains a unique serial number for your installation.

To upload the Breeze license file:

1. Verify that the serial number you entered on the Company Information screen of the installation wizard appears in the link to the Macromedia Breeze license site.

2. Click Next to continue.

   The File Download window appears. The license file is a text file that enables Breeze Server.

3. Click Save.
The File Download window appears.

4. Check the Close This Dialog Box When Download Completes check box.

The Create Administrator window appears. This step is mandatory. You must create an administrator for Breeze now. Administrative privileges are required for configuring and maintaining Breeze.

Enter the name, email address, and password of the Breeze administrator. These are required fields.
5. Click Finish.
The Configuration Complete screen appears.

At this point you can do the following:

- Log in to Breeze
- Return to the Console to change the Breeze configuration.
- View the online *Getting Started Guide.*

**Application Settings Summary**

The Application Settings summary screen displays the settings you configured with the Console, and the Breeze features that the license file enables.

To return to the Console, select Start > Programs > Macromedia Breeze.
Completing a terminated installation

If the installer terminates during the installation of any Breeze component that includes the embedded database engine, use the following procedure to complete the installation.

Note: If you were installing Breeze and the embedded database engine when the installation terminated, uninstall the embedded database engine before you complete the following steps. For more information, see the Breeze TechNote “Installer detects existing installation of SQL Server” at www.macromedia.com/go/tn_18927.

To complete a terminated installation:
1. Restart the server.
2. In Windows, open the Control Panel and double-click Add/Remove Programs.
3. In the Add or Remove Programs dialog box, select Macromedia Breeze Server, and then select Change or Remove Programs on the left of the dialog box. Click Change/Remove.
4. In the installation wizard, deselect the option to install the embedded database engine and follow the steps in the wizard to finish installing Breeze Server.
5. When the installation is complete, restart the server.

Starting and stopping Breeze components

Before you start the Breeze components, do the following:

• Make sure that the Breeze components are properly configured.
  For more information, see Chapter 5, “Verifying Your Installation,” on page 91.
• Make sure that either the embedded database engine or Microsoft SQL Server is running.

To start Breeze Server:
1. Select Start > Programs > Macromedia Breeze > Start Breeze Server.
2. Make sure that you start the Breeze services in the following order:
   a Flash Communication Administration
   b Flash Communication Server
   c Macromedia Breeze Application Service (the Breeze server)
   d Follow this procedure only if Breeze Server is configured to start Breeze.

To stop Breeze Server:
1. Select Start > Programs > Macromedia Breeze > Stop Breeze Server.
2. Make sure that you stop the Breeze services in the following order:
   a Breeze Application Service (the Breeze server)
   b Flash Communication Server
   c Flash Communication Admin Service
To start Breeze Meeting:
1. Select Start > Programs > Macromedia Breeze > Start Breeze Meeting Server.
2. To verify that the following services are running, select Start > Settings > Control Panel > Administrative Tools > Services.
   Confirm that the following services associated with Breeze Meeting are running:
   ■ Flash Communication Admin Service
   ■ Flash Communication Server

To stop Breeze Meeting:
1. Select Start > Programs > Macromedia Breeze > Stop Breeze Meeting Server.
2. Verify that the following services associated with Breeze Meeting are not running:
   ■ Flash Communication Admin Service
   ■ Flash Communication Server

Uninstalling Breeze

You can uninstall Breeze through the Windows Control panel.

To uninstall Breeze by using the Windows Control Panel:
1. Stop the Breeze services in the order described in “Starting and stopping Breeze components” on page 53: Flash Communication Server, Flash Communication Admin Service, and Macromedia Breeze Application Service (the Breeze server).
2. Select Start > Programs > Macromedia Breeze > Uninstall Breeze.

When you uninstall Macromedia Breeze, the following elements are not uninstalled:

• Embedded database engine
• Log files
• The Breeze custom.ini and config.ini configuration files
• Breeze content files

To uninstall these elements, delete the folder that you installed Breeze in. By default, it is c:\breeze.

Troubleshooting

If you encounter unexpected results after you install Macromedia Breeze either on a single server or on a cluster of servers, the following helpful resources are available to you:

• TechNotes on the Breeze Support Center website at www.macromedia.com/support/breeze.
• Macromedia Support online
• If you call Support, you need to provide your Macromedia license number to the representative.
• Macromedia Online Forums at www.macromedia.com/support/forums
**Breeze technical support**

For security and privacy reasons, Breeze product support cannot assist Breeze Meeting customers in gaining access to private meetings, events, or seminars. Only the Meeting Manager or Breeze Administrator can register users or grant access to meetings, events or seminars.

If your company has a software license for Breeze (meaning it is running internally on your company network), please contact your help desk or Breeze administrator. All administration of licensed servers is handled by each individual company.

Standard e-mail support is included with every Breeze hosted account and all Breeze hosted customers are entitled to this support. Phone support is only available for customers with Silver and Gold support plans and licensed customers with a Standard Maintenance plan.

Breeze product support cannot provide administrative support for companies that host their own server. Only administrative assistance can be provided to companies that use the Macromedia hosted ASP system.

**Macromedia online forums**

Macromedia online forums are the Macromedia community's peer-to-peer discussions of Macromedia products. The forums are a useful source of information, user tips, and best practices.

*Note:* These forums are not an official customer-support channel for Macromedia.
CHAPTER 4
Post-installation

This chapter describes the series of configuration and deployment tasks that you need to complete after you install the Macromedia Breeze applications and complete the first phase of configuring Breeze with the Application Management Console.

• “Deploying Breeze to your organization” on page 57
• “DNS configuration guidelines” on page 59
• “Integrating Breeze with learning management systems” on page 61
• “Implementing single sign-on” on page 61
• “Configuring the Breeze Directory Service Integration” on page 62
• “Configuring SSL support for Breeze” on page 77
• “Configuring a Breeze Server cluster” on page 84
• “Maintaining Breeze reliability” on page 87

Deploying Breeze to your organization

Before you deploy Breeze, answer the following questions:

• How should you configure the networks and DNS Server to allow Breeze users to interact with the Breeze servers?

  Make a plan that includes the IP addresses and domains that you need to support. Review the installation documentation to confirm that you know how to change these settings in Breeze.

• How many servers are required if you are using a firewall or proxy server? Is a cluster of servers needed?

  Review the planning requirements in Chapter 1, “Before You Begin,” on page 9 to determine if you require additional servers, and to learn how to create a multiserver configuration.
• Will some users interact with the servers by communicating through a firewall or proxy?
  Verify that your firewall or proxy server configuration allows end users to interact with the
  servers. You must also use the proper configuration of servers.
• Are you adding a Secure Sockets Layer (SSL) and encryption?
  Verify that you correctly set up and configured your SSL solution following the tips in this
  document.
  For details, see “Configuring SSL support for Breeze” on page 77.

**Breeze server configurations**

For small- to medium-sized organizations with simple network configurations, installing all
Breeze applications on a single server is a viable solution.
If you are installing Breeze in large organizations where there may be more demands on system resources, you might consider the following strategies:

- **Clustering Breeze Servers**
  Creating a cluster of servers lets you distribute end-user traffic across multiple servers. Use this configuration if you have many users and are concerned about the load on a single server, or when you want to have more than one server as a redundant system, in case a single server experiences hardware failure.
  In addition to distributing the workload, clustering Breeze Servers also creates failover that prevents loss of service and data if any server in the cluster fails.

- **Separating the Breeze database from Breeze Server**
  In a Breeze cluster, Microsoft SQL Server 2000 must be identified as the database engine and installed on a separate server that all computers in the cluster hosting Breeze can access.
  Microsoft SQL Server 2000 for the Breeze database must be installed in mixed mode. This configurations allows you to use either SQL or Windows authentication. Breeze supports SQL authentication.
  For Breeze single-server installations, you can install SQL Server and place the Breeze database on a separate computer from Breeze Server. Doing so lets you create more stringent and secure backup and redundancy procedures for the database.

### DNS configuration guidelines

The following guidelines can help you set up your network and Domain Name Service (DNS) for Breeze:

- **Static IP addresses**
  You cannot access Breeze content or Meetings by using an IP address in the URL line. The Breeze server must have a fully qualified domain name (FQDN) and that name must appear in the URL. Unlike many websites and systems that let you access their content by entering either a URL, such as www.search.com, or an IP address, such as 66.252.27.254, you must set up a FQDN for your Breeze server and map that name to the proper IP address by using either a DNS server or a hosts file.
• Firewalls and proxy servers

Firewalls and proxy servers can cause problems for a single-server Breeze configuration. Breeze Server uses port 80 by default, which most firewalls and proxy servers allow. Breeze Meeting uses port 1935 by default, and reverts to port 443 if port 1935 is not successful. Ports 443 and 1935 are not as common to firewalls and proxy servers; if necessary, Breeze Meeting attempts to use port 80 to interact with the Breeze user's computer if ports 1935 and 443 aren't available.
Integrating Breeze with learning management systems

All LMS integration occurs through Breeze Presenter. For more information, see Breeze Presenter User Guide.

Implementing single sign-on

Single sign-on (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 the need to enter multiple passwords. Single sign-on reduces human error, a major component of systems failure.

You can manage users and authenticate their access to multiple applications in several ways. Breeze 5 supports the following:

- NTLM authentication
  Microsoft uses Windows NTLM to pass information that authenticates users. After a user is logged 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. Breeze checks the browser type of a request and only requests NTLM authentication for browsers that support NTLM.

  NTLM authentication uses the jCIFS library. A servlet or filter servlet interacts with the client and implements the appropriate handshake with the server that hosts Breeze.

  Note: jCIFS supports only NTLM authentication. This implementation will not work for customers who use NTLM2 or Kerberos.

- HTTP-header based authentication
  HTTP-header based authentication inspects the HTTP header to extract the user ID for the authenticated user.

  If Breeze Server is not installed behind an authentication proxy, the standard login page appears to Breeze users.

  Netegrity Siteminder uses HTTP-header based authentication. Siteminder provides a software developer’s kit (SDK) that implements a servlet or filter servlet that acts as the authentication proxy.

Configuring SSO

You need to configure the following variables in the custom.ini configuration file to implement the SSO feature:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTLM_DOMAIN</td>
<td>NT Domain Name</td>
<td>The NT domain users authenticate against</td>
</tr>
<tr>
<td>NTLM_SERVER</td>
<td>IP address</td>
<td>The IP address of one or more WINS servers on the network, separated by a comma (&quot;,&quot;)</td>
</tr>
</tbody>
</table>
Reconciling login policies

Breeze and the Microsoft NTLM have different login policies for authenticating users. These policies must be reconciled before the user can employ a single login to access Breeze and other applications. The organization’s login and password policy determines what the external login looks like. By default, Breeze employs the user’s email address (jdoe@mycompany.com) and password as the primary login to authenticate the user. Breeze can be configured to use an external login as authentication.

For example, NTLM employs a login policy of username and password. The username can be a variant of the user’s real name (jdoe), employee ID number (1234), or an encrypted name. Once again, the organization’s login and password policy determines what the username looks like.

The Breeze login and password policy is configured in Breeze Manager (select Administration > Edit Login and Password Policies). In the Login Policy section, you can specify whether or not to use the user’s email login as the default login to Breeze. Select No to have Breeze accept a username as the authentication mechanism. This configuration matches the Breeze password policy with the NTLM password policy.

Configuring the Breeze Directory Service Integration

The administrator uses the Directory Service tab of the Application Management Console to control the integration of the enterprise’s directory services with the Breeze directory of users and groups. To perform a directory integration task, you must be defined as an administrator in your Breeze profile. An administrator is defined on the Create Administrator screen of the Application Management Console.

Breeze has its own directory of security principals (users and groups). Directory synchronization integrates Breeze with an organization’s Directory Service. This is a one-way synchronization that copies the information about principals from the external directory to the Breeze directory.

Integration of the directories of the organization and of Breeze is performed on the Console. You use the Console to perform the following tasks:

- Directory Service settings
  - “Configure the connection settings”
  - “Map the Breeze user profile to the Directory Service” on page 65
  - “Map the Breeze group profile to the Directory Service” on page 68
- Synchronization settings
  - “Schedule the synchronization” on page 70
  - “Define the password policies” on page 75
  - “Define the deletion policies” on page 76
  - “Define the synchronization action” on page 70
- Log files
  - “View the synchronization log files” on page 72
  - “Log file format” on page 73
Configure the connection settings

On this screen the administrator provides the location of the organization's Directory Service and the authorization to access it. Breeze uses this information to connect to the Directory Service.

<table>
<thead>
<tr>
<th>Field</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP Connection</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>Authentication Method</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>Username</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>Query Timeout (seconds)</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>Service URL</td>
<td>none</td>
<td></td>
</tr>
</tbody>
</table>

The following table provides the field names and descriptions for the Connection Settings screen:

<table>
<thead>
<tr>
<th>Field</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
</table>
| LDAP Connection Authentication Method | none          | The administrator defines the mechanism to transmit the LDAP username and password over the network:  
  • None: Anonymous (no password)  
  • Simple: Transmit password as clear text  
  • Digest MD5: More secure mechanism to transmit password |
| LDAP Connection Password   | none          | Administrative password is hidden. |
| LDAP Connection Username   | none          | Administrative login to conduct queries against the LDAP server. |
| LDAP Query Timeout         | none          | Timeout permitted before canceling the query. Leaving the field blank means no timeout is defined. |
| LDAP Service URL           | none          | Usual form is "ldap://servername:portnumber". |
The following example shows connections settings in one LDAP syntax:

URL: ldap://mycompany.com:636
Username: MYCOMPANY\jdoe
Password: password123
Query timeout: (empty)
Authentication mechanism: Simple

*Note:* This is an example. Consult your local LDAP admin for the appropriate settings and syntax.
Map the Breeze user profile to the Directory Service

The administrator uses the User Profile Mapping screens to provide the information that Breeze uses to map the fields in its user profiles to their equivalent LDAP attributes when the organization’s Directory Service and the Breeze directory of users are synchronized.

<table>
<thead>
<tr>
<th>Macromedia Breeze User Field Name</th>
<th>Directory Service Field Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login**</td>
<td>mail</td>
</tr>
<tr>
<td>First Name**</td>
<td>givenName</td>
</tr>
<tr>
<td>Last Name**</td>
<td>sn</td>
</tr>
<tr>
<td>E-mail**</td>
<td>mail</td>
</tr>
<tr>
<td>Custom Field 1</td>
<td>customField1</td>
</tr>
</tbody>
</table>

* - indicates required fields

Search for users in these branches:

<table>
<thead>
<tr>
<th>Branch DN</th>
<th>Filter</th>
<th>Subtree Search</th>
</tr>
</thead>
<tbody>
<tr>
<td>ou=branch1,dc=example,dc=com</td>
<td>(objectClass=organizationalPerson)</td>
<td>true</td>
</tr>
</tbody>
</table>

Save    Cancel
The following table describes the field names in the User Profile Mapping screen:

<table>
<thead>
<tr>
<th>Field</th>
<th>Default Value</th>
<th>LDAP attribute/Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Name</td>
<td>Required field.</td>
<td>givenName</td>
</tr>
<tr>
<td></td>
<td>No default.</td>
<td></td>
</tr>
<tr>
<td>Last Name</td>
<td>Required field.</td>
<td>sn</td>
</tr>
<tr>
<td></td>
<td>No default.</td>
<td></td>
</tr>
<tr>
<td>Email</td>
<td>Required field.</td>
<td>UserPrincipalName</td>
</tr>
<tr>
<td></td>
<td>No default.</td>
<td></td>
</tr>
<tr>
<td>Custom Field 1</td>
<td>Optional field.</td>
<td>Many options are available for defining custom fields under Admin &gt; Users and Groups &gt; Customize User Profile.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Login</td>
<td>Required field.</td>
<td>sAMAccountName</td>
</tr>
<tr>
<td></td>
<td>No default.</td>
<td></td>
</tr>
</tbody>
</table>

The required fields are: Login, First Name, Last Name, and Email. If you have defined any custom fields (Breeze Administration > Users and Groups > Customize User Profile), these fields are added to this screen.

Click Save to retain the user mapping information.

The following example shows one LDAP syntax of how to map a Breeze user profile:

First Name: givenName  
Last Name: sn  
Email: userPrincipalName  
Login: sAMAccountName  
External Login: sAMAccountName

Note: This is an example. Consult your local LDAP admin for the appropriate settings and syntax.
Adding user branches

Each branch in the organization is defined by its own DN (distinguished name) attribute. When you click Add in the User Profile Mapping screen to add the user information for other branches of the organization when the directories are synchronized, the following screen is displayed.

The following table describes the fields in the User Profile Mapping screen.

<table>
<thead>
<tr>
<th>Field</th>
<th>Default Value</th>
<th>LDAP attribute/Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Branch DN</td>
<td>No default</td>
<td>DN (distinguished name) of the branch root node. A link to the selected branch is displayed.</td>
</tr>
<tr>
<td>Filter</td>
<td>none</td>
<td>Defines the query filter.</td>
</tr>
<tr>
<td>Subtree Search</td>
<td>none</td>
<td>The Boolean value is true or false. A value of true initiates a recursive search of all subtrees in the branch.</td>
</tr>
</tbody>
</table>

Click Save to add a user branch, or click Delete to delete a user branch.

The following example shows one LDAP syntax of how to add a branch of the organization and define its users:

Add branch:
DN: cn=USERS,DC=myteam,DC=mycompany,DC=com
Filter: ((objectClass=group))
Subtree search: True
Note: This is an example. Consult your local LDAP admin for the appropriate settings and syntax. The same information is used for mapping group branches.

Map the Breeze group profile to the Directory Service

On the Group Profile Mapping screen, the administrator provides the information that Breeze uses to map the fields in its group profiles to their equivalent LDAP group entries when the organization's Directory Service and the Breeze directory of groups are synchronized.

The following table describes the field names in the Group Profile Mapping screen.

<table>
<thead>
<tr>
<th>Field</th>
<th>Default Value</th>
<th>LDAP attribute/Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Name</td>
<td>Required field. No default.</td>
<td>sAMAccountName</td>
</tr>
<tr>
<td>Group Member</td>
<td>Required field. No default.</td>
<td>member</td>
</tr>
</tbody>
</table>

Click Save to retain the group mapping information.
The following example shows one LDAP syntax of how to map a group profile:

Name: sAMAccountName
Membership attribute: member

**Note:** This is an example. Consult your local LDAP admin for the appropriate settings and syntax.

To map additional groups, click Add to display the Group Branch screen.

**Adding group branches**

Each group in the organization is defined by its own DN attribute on the following screen. The information on the following screen is used to define groups in other branches of the organization when the directories are synchronized.

The following table describes the fields in the Group Profile Mapping screen.

<table>
<thead>
<tr>
<th>Field</th>
<th>Default Value</th>
<th>LDAP attribute/Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Branch DN</td>
<td>No default</td>
<td>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.</td>
</tr>
<tr>
<td>Filter</td>
<td>none</td>
<td>The string for the query filter is defined here. In this example, the LDAP syntax indicates that the attribute equals the attribute group.</td>
</tr>
<tr>
<td>Subtree Search</td>
<td>none</td>
<td>The Boolean value is <strong>true</strong> or <strong>false</strong>. A value of <strong>true</strong> initiates a recursive search of all subtrees in the branch.</td>
</tr>
</tbody>
</table>

Click Save to retain the group profile mapping information.
The following example shows one LDAP syntax for how to add a branch of the organization and define its groups:

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

**Note:** This is an example. Consult your local LDAP admin for the appropriate settings and syntax. The same information is used for mapping user branches.

**Schedule the synchronization**

The Breeze administrator uses the Console to schedule the synchronization of the external directory service to the Breeze directory of users and groups.

![Schedule settings screenshot](image)

The administrator should schedule the synchronization at off-peak hours when there is less competition for system resources. Scheduling the synchronization is optional. The administrator might decide to use manual ad-hoc synchronizations only.

As the synchronization progresses, a log file records what happens and identifies any warnings or errors. For more information, see “View the synchronization log files” on page 72.

**Define the synchronization action**

The administrator chooses one of the following strategies for synchronizing the organization's directory service with the Breeze directory of users and groups. The administrator selects the synchronization scheme on the Synchronization Action screen of the Console.
- Manual synchronization immediately synchronizes the Breeze directory and the organization's directory service.

- Preview synchronization is similar to a manual synchronization, but no changes are made to the Breeze directory. The log file assists the administrator in diagnosing any problems that might occur during the synchronization.

- Scheduled synchronization occurs at defined intervals. The existing Breeze scheduler mechanism is used. Supported intervals are daily, weekly, and monthly, starting at a certain date and time.

<table>
<thead>
<tr>
<th>Macromedia Breeze</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Settings</td>
</tr>
<tr>
<td>LDAP Settings</td>
</tr>
</tbody>
</table>

The following features allow you to preview and execute synchronization based on your configuration settings.

**Note:** The Preview and Synchronize operations may take a long time to execute on a large directory.
- While they are running the browser will appear to be waiting for the next page to load.
- When they are complete, the result page will load.

**Preview Directory Synchronization**

Provides a preview of user synchronization based on your current settings.

**Perform Directory Synchronization**

Executes a user synchronization based on your current settings (recommended at off-peak hours).

**Make Synchronized Data Editable**

By default synchronized data is not editable within the Breeze application. This action removes this restriction on the synchronized data currently in Breeze, allowing admins to edit synchronized user fields and group memberships.
View the synchronization log files

Each synchronization generates a log file that describes each principal processed and the result. In the case of a preview synchronization, the log describes the action that would be taken if this were a manual synchronization.

Logs consist of events with one line per event. The synchronization produces at least one event for every individual principal processed. In some cases more than one event might be produced.

If any warnings or errors are encountered during a manual or preview synchronization, a second warning log listing the warnings and errors is generated. The warning log highlights the items requiring the administrator's attention. These entries are also found in the main log. The administrator can use both log files to identify errors and diagnose any warnings.

The synchronization logs page lists, in chronological order, all of the synchronization logs in the system: whether they are manual, preview or scheduled log files.
Log file format

The log is in comma-separated value format and demarcates the following values:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date</td>
<td>Formatted date-time value to the millisecond. The format is yyyyMMdd'T'HHmmss.SSS.</td>
</tr>
<tr>
<td>Principal ID</td>
<td>Breeze login or group name.</td>
</tr>
</tbody>
</table>
| Principal Type | A single character:  
|               | U for user, G for group.                                                   |
| Event        | The action taken or condition encountered.                                 |
| Detail       | Detailed information about the event.                                      |
### Synchronization events and details

The following table describes the events found in the synchronization log files:

<table>
<thead>
<tr>
<th>Event</th>
<th>Description</th>
<th>Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>add</td>
<td>Principal added to Breeze</td>
<td>Abbreviated XML packet that describes the updated fields. A series of <code>&lt;fieldname&gt;value&lt;/fieldname&gt;</code>. The parent node and non-updated fields are omitted. For example: <code>&lt;first-name&gt;Joe&lt;/first-name&gt;</code> <code>&lt;last-name&gt;Schmoe&lt;/last-name&gt;</code></td>
</tr>
<tr>
<td>update</td>
<td>The principal exists as an external user in Breeze and some fields were updated.</td>
<td></td>
</tr>
<tr>
<td>update-members</td>
<td>The principal exists as an external group in Breeze and principals were added or removed to its membership.</td>
<td>Abbreviated XML packet that describes the added and removed members. The parent node is omitted. <code>&lt;add&gt;ID list&lt;/add&gt;</code> <code>&lt;remove&gt;ID list&lt;/remove&gt;</code> The ID list is a series of <code>&lt;id&gt;principal ID&lt;/id&gt;</code> 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 <code>&lt;add/&gt;</code> or <code>&lt;remove/&gt;</code>. For example: <code>&lt;add&gt;&lt;id&gt;jschmoe&lt;/add&gt;&lt;id&gt;jpublic&lt;/id&gt;</code> <code>&lt;remove/&gt;</code></td>
</tr>
<tr>
<td>delete</td>
<td>The principal was deleted from Breeze.</td>
<td>A user or group created in Breeze is considered an internal principal. A user or group created by the synchronization is considered an external principal.</td>
</tr>
<tr>
<td>up-to-date</td>
<td>The principal exists as an external principal in Breeze and is already synchronized with the external directory. No changes were made.</td>
<td></td>
</tr>
<tr>
<td>make-external</td>
<td>The principal exists as an internal principal in Breeze 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 to that effect. This event is logged in the warning log.</td>
<td></td>
</tr>
<tr>
<td>warning</td>
<td>Some other warning-level event occurred.</td>
<td>Warning message</td>
</tr>
<tr>
<td>error</td>
<td>An error occurred.</td>
<td>Java exception message</td>
</tr>
</tbody>
</table>
Define the password policies

The Breeze administrator uses the Policy Setting screen to define the password setup policy for the synchronization. Passwords are pieces of user data that are dealt with separately from the other data in an external directory. Passwords are rarely available in clear text form, if they are available at all. A synchronization cannot copy a password into Breeze from another source. There are two approaches to handling user authentication in Breeze:

- Integrate Breeze with an external authentication system.
  For more information, see “User authentication” on page 77.
- Create new passwords for users to log in to Breeze with. These passwords are stored in the Breeze database and are specific to the Breeze application.

The password setup policy determines how the synchronization creates passwords for new users. These actions are triggered only when a user is first added to Breeze.
The administrator chooses one of the following options for how the synchronization should set the passwords for new users. The administrator determines the password policy on the Password Setup Policy screen of the Console.

- **Do nothing.**
  If you have integrated Breeze with an external authentication system, there is no need for the synchronization to create new passwords just for Breeze. Users will log in to Breeze according to the mechanism of the external authentication system.

- **Send a link to set the password.**
  This policy option instructs Breeze to send an e-mail to each user that contains a URL they may access to set their own password for accessing Breeze.
  See the “Map the Breeze user profile to the Directory Service” on page 65 and “Map the Breeze group profile to the Directory Service” on page 68.

- **Set the password to the value on an LDAP attribute by entering the LDAP attribute in the text box provided.**
  This policy option sets the user’s initial password to the value of an attribute (also known as a field) in the corresponding LDAP entry. For example, if the LDAP directory contains users’ employee IDs and you specified the employee ID LDAP attribute as the password, users can log in to Breeze using their employee ID as their password. After users have logged in to Breeze, they can change their passwords.
  If validation rules are specified in the password policy, the rules are ignored when setting the initial password, but are enforced for all subsequent password changes.

  **Note:** The usual password validation policies are not applied to this initial value.

  Click Save to set the password policy.

**Define the deletion policies**

When a principal is deleted from an external directory, the organization’s deletion policy controls whether or not to keep the records of the principal in the Breeze database. Breeze may hold additional, unsynchronized field data for the principal that the admin may wish to use in another application. Keeping the records avoids erroneously deleting a user if the synchronization settings did not reflect a change in the directory server configuration.

The administrator determines what happens when a principal is deleted from the external directory: either no action is taken or the synchronization deletes the Breeze users and groups that were deleted from the directory service.

Click Save to continue.
User authentication

Organizations need to authenticate users of applications such as email. The following strategies use the Breeze authentication mechanism to validate users:

- No external authentication integration
  Breeze users keep separate passwords. Application users keep their passwords to log in with their organization’s network username. Not integrating the internal and external logins means that users keep their existing network logins and Breeze passwords. IT administrators have to retain separate Breeze passwords for all users. Macromedia does not recommend this option because it is laborious for a directory service of any appreciable size.

- Breeze login screen integration
  Users log in to the Breeze login screen with their network username and password. The IT administrator uses a solution accelerator to authenticate Breeze users against the organization’s directory service.

- Automatic single sign-on integration
  Users who are already logged in to their desktop under their network login bypass the Breeze login screen and automatically log in to Breeze. This strategy allows the organization to employ an authentication method that allows users to use the same login and password to access all applications on its internal network, including Breeze.

  For more information, see “Implementing single sign-on” on page 61.

Configuring the FCS ports

FCS needs to be configured to listen on ports 80 and 443 in addition to the default port of 1935. To accomplish this, you must modify the value of the DEFAULT_FCS_HOSTPORT variable in the custom.ini file. Once again, if this is not in the custom.ini file you must add and define it as follows:

```
DEFAULT_FCS_HOSTPORT=:1935,80,-443
```

This tag now specifies that FCS will listen on ports 1935, 80, and 443. Port 443 is designated as a secure port that will only receive RTMPS connections. Attempting an RTMPS connection request to ports 1935 or 80 will result in a failure to connect. Similarly, an unsecured RTMP connection request to port 443 will fail to connect.

Configuring SSL support for Breeze

Breeze Server generates specific URLs to allow users to go directly to meetings and courses. If the Breeze server is running with an SSL hardware accelerator, these URLs must begin with https instead of http (the “s” in HTTPS indicates encrypted Internet traffic). Breeze uses the port number of incoming traffic to determine whether the URL should begin with HTTP or HTTPS. When you set up your SSL solution with Breeze, you must send the decrypted traffic to Breeze on port 443, even though the traffic is already decrypted and could, in theory, go to an unencrypted port.
You can deploy Breeze with an SSL layer in one of the following ways:

- A software-based solution by configuring the native support for SSL in Flash Communication Server (FCS).

  Use this option if you want to secure only Breeze and not the web application. You will need 2 IP addresses (2 DNS entries for the IP addresses) and 1 SSL certificate. You will need to modify SSL tags in the Flash Adaptor.xml and Server.xml files configuration files. The default location of the FCS configuration files is: c:\breeze\serv.

- A hardware-based solution that routes all communication through an external SSL accelerator.

  Use this option if you want to secure both FCS and the Breeze application. You will need 2 IP addresses - 2 DNS entries for the IP addresses -- and 2 SSL certificates.

  You need to purchase the accelerator separately. Consult the vendor's documentation for instructions about how to configure the accelerator.

  When you use Breeze with an SSL hardware accelerator, all logins to Breeze are sent over the secured protocol HTTPS.

  With SSL, all presentations and meetings are conducted over fully encrypted HTTPS or RTMPS connections. The Breeze server uses port 443 for encrypted traffic.

### Configuring FCS for SSL

To use the native SSL support in FCS for secure communications you must modify the FCS Adaptor.xml and Server.xml configuration files by defining the SSL tags in these files. The default location of the FCS files is c:\breeze\serv. The configuration files for FCS are found in c:\breeze\serv\win32\conf.

### Adding the required SSL tags in the Adaptor.xml file

The SSL tags are included in the Server.xml file. Not all of the required SSL tags in Adaptor.xml are present by default, however. You will need to insert the following SSL-specific tags in the Adaptor.xml file.

```
<SSL>
  <SSLServerCtx>
    <SSL CertificateFile></SSL CertificateFile>
    <SSL CertificateKeyFile type="PEM"></SSL CertificateKeyFile>
    <SSLPassPhrase></SSLPassPhrase>
    <SSL CipherSuite></SSL CipherSuite>
    <SSL SessionTimeout>5</SSL SessionTimeout>
  </SSLServerCtx>
</SSL>
```

Place this section right after the end tag </HTTPTunneling> for the HTTPTunneling section but before the root end tag </Adaptor>.

*Note:* HTTP Tunneling is enabled by default.
Locating the required SSL tags in the Server.xml file

The SSL-enabling tags in the Server.xml file occur in the following sequence:

- SSLEngine
- SSLRandomSeed
- SSLSessionCacheGC
- SSLVerifyCertificate
- SSLCACertificatePath
- SSLCACertificateFile
- SSLVerifyDepth
- SSLCipherSuite

Defining the SSL tags in FCS

The following table lists the tags in the Adaptor.xml and Server.xml files that configure FCS for SSL.

<table>
<thead>
<tr>
<th>FCS File</th>
<th>XML Tag</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adaptor.xml</td>
<td>Redirect</td>
<td>[none]</td>
<td>Specifies whether unknown requests are redirected to an external server such as Breeze. When FCS receives an unknown request, the request is redirected to the specified redirect host. For redirection to work, HTTP tunneling must be enabled. You can control which port on the redirect host will listen for redirected traffic: Request redirection to a specific host can be <code>&lt;Redirect enable=false&gt;</code> <code>&lt;Host port=&quot;80&quot;&gt;:8080&lt;/Host&gt;</code> <code>&lt;Host port=&quot;443&quot;&gt;:8443&lt;/Host&gt;</code> &lt;/Redirect&gt;`</td>
</tr>
<tr>
<td>Adaptor.xml</td>
<td>SSLCertificateFile</td>
<td>[none]</td>
<td>Specifies the location of the certificate file to send to the client. If an absolute path is not specified, the certificate is assumed to be located relative to the Adaptor directory.</td>
</tr>
<tr>
<td>Adaptor.xml</td>
<td>SSLCertificateKeyFile</td>
<td>PEM</td>
<td>Specifies the location of the private key file for the certificate. If an absolute path is not specified, the key file is assumed to be located relative to the Adaptor directory. If the key file is encrypted, the pass phrase must be specified in the SSLPassPhrase tag. The type attribute specifies the type of encoding used for the certificate key file. This can be either PEM or ASN1.</td>
</tr>
</tbody>
</table>
Specifies the ciphers to use. This is a list of colon-delimited components. A component can be a key exchange algorithm, authentication method, encryption method, digest type, or one of a selected number of aliases for common groupings. For a list of components, see the FCS documentation.

The default setting for this tag is:
ALL:!ADH:!LOW:!EXP:!MD5:@STRENGTH

Contact Breeze Technical Support before changing the default settings.

Specifies the passphrase to use for decrypting the private key file. If the private key file is not encrypted, leave this tag empty.

This tag specifies the directory containing CA certificates. Note that each file in the directory can contain only a single CA certificate, and the files must be named by the subject name’s hash, and an extension of .0.

Specifies the cryptic graphic accelerator to use, if any. The following cryptographic engines are allowed: cswift, chil, atalla, nuron, ubsec, aep, surewave, or 4758cca. Each item identifies a type of cryptographic hardware accelerator.

A cryptic graphic accelerator is a piece of hardware that offloads the CPU-intensive cryptographic operations, thereby reducing the demand on resources and making the server more scalable.
To configure FCS manually:

1. Stop all Breeze services.
2. Open the Adaptor.xml file by using a text editor such as Notepad.
3. Make a backup of the current Adaptor.xml configuration file by saving it as Adaptor.bak.
4. Search for the `<SSL>` tag where the SSL schema is located.
5. Search for the variable(s) you want to set.
6. Enter the new value(s).
7. Save the modified file as Adaptor.xml.
8. Use the procedure outlined in steps 2 through 7 to reconfigure the Server.xml file for SSL.
9. Restart all Breeze services.

<table>
<thead>
<tr>
<th>FCS File</th>
<th>XML Tag</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server.xml</td>
<td>SSLCACertificatePath</td>
<td>[none]</td>
<td>Specifies the name of a directory containing CA certificates. Each file in the directory must contain only a single CA certificate, and the files must be named by the subject name's hash, and an extension of &quot;.0&quot;. Win32 Only: If this tag is empty, FCS will attempt to find CA certificates in the certs directory located at the same level as the conf directory. The Windows cert store can be imported into this directory by running FCSMaster -console -initialize from the command line.</td>
</tr>
<tr>
<td>Server.xml</td>
<td>SSLRandomSeed</td>
<td>16</td>
<td>Specifies the number of bytes of entropy to use for seeding the pseudo-random number generator (PRNG). Entropy is a measure of randomness. The more entropy, the more random numbers from the PRNG will be. The default number is 16. You cannot specify less than 8 bytes,</td>
</tr>
<tr>
<td>Server.xml</td>
<td>SSLSessionCacheGC</td>
<td>5</td>
<td>Specifies in minutes how often to flush expired sessions from the server-side session cache.</td>
</tr>
<tr>
<td>Server.xml</td>
<td>SSLVerifyCertificate</td>
<td>true</td>
<td>Configures the server to act as an SSL client (out-going SSL connections). The tag specifies whether or not to verify the certificate that is returned by the server being connected to. Certificate verification is enabled by default. To disable certificate verification, specify false. <strong>Warning:</strong> Disabling the certificate verification can result in a security risk.</td>
</tr>
<tr>
<td>Server.xml</td>
<td>SSLVerifyDepth</td>
<td>9</td>
<td>Configures the server to act as an SSL client (out-going SSL connections). The tag specifies the maximum depth in the certificate chain we are willing to accept. If a self-signed root certificate cannot be found within this depth, the certificate verification will fail.</td>
</tr>
</tbody>
</table>
Implementing SSL-enabled Breeze with an Accelerator

To implement Breeze with an SSL-enabled accelerator, the following resources are required:

- Two external IP addresses and one internal IP address.
- One NIC card.
- Breeze Server is configured to listen on port 443 externally and forwards unencrypted to the Breeze server on port 443.
- Breeze Server is also configured to forward any port 80 traffic coming from Breeze Server, and loop this traffic back to Breeze Server on port 80.
- The FCS IP address is configured to listen on port 443 externally and forward unencrypted to the Breeze server on port 1935.
- The FCS IP address is also configured to forward any port 1935 traffic coming from the Breeze server back to the Breeze server on port 1935.

Modifying the custom.ini file for SSL

You configure Breeze for an SSL accelerator by modifying the installed Breeze Server configuration. The following example creates an SSL-only configuration for Breeze. Only port 443 is opened for Breeze Server or FCS traffic. No FCS traffic is tunneled over port 80, and no external HTTP traffic goes over port 80.

To modify the custom.ini file for SSL:

1. Edit the following variables in the custom.ini configuration file. Substitute your local server names for the variables ADMIN_HOST, ADMIN_PROTOCOL, SSLONLY, and USE_HOST_MAPPINGS to enable SSL.

   ```
   # breeze external DNS, which is the SSL Certificate A.
   Certificate-ns.macromedia.com
   # SSL Configuration Begins
   ADMIN_PROTOCOL=https://
   SSLONLY=yes
   DEFAULT_FCS_HOSTPORT=:1935
   # ps-breezewin1 is the Breeze server name; ps-breezewin4.macromedia.com is Meeting’s External DNS AND the SSL Certificate B.
   USE_HOST_MAPPINGS=yes
   shost.ps-breezewin1=ps-breezewin4.macromedia.com
   host.ps-breezewin1=ps-breezewin4.macromedia.com
   
   2. Bind one IP address to Breeze Server.
   a. Open the c:\breeze\appserv\conf\SERVER-INF\jrun.xml file.
   b. Change the value of bindAddress from the asterisk (*) to the IP address of Breeze Server.
   ```
<table>
<thead>
<tr>
<th>Variable</th>
<th>Default value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADMIN_HOST</td>
<td>[none]</td>
<td>Host name to use in a URL for accessing Breeze. This is the host name that users enter directly in their browsers. For example, for the URL <a href="http://aserver.mybreeze.com">http://aserver.mybreeze.com</a>, you set ADMIN_HOST as shown in the following example: ADMIN_HOST=aserver.mybreeze.com. If your web server uses a port other than port 80 for receiving HTTP messages, the port number must be added to the host name, as shown in the following example: ADMIN_HOST=aserver.mybreeze.com:8080.</td>
</tr>
<tr>
<td>ADMIN_PROTOCOL</td>
<td>http</td>
<td>Set to https when SSL is used.</td>
</tr>
<tr>
<td>SSL_ONLY</td>
<td>false</td>
<td>Set this variable to true to configure a trusted or secured environment.</td>
</tr>
<tr>
<td>USE_HOST_MAPPING</td>
<td>yes</td>
<td>Specifies the fully qualified host name. host.machinename=hostname.company.com</td>
</tr>
</tbody>
</table>
Setting up the SSL hardware accelerator

You perform the following tasks on the SSL hardware accelerator:

• Configure SSL Certificate A and B to send the unencrypted data to the Breeze IP address (Breeze Server) listening on port 443.

In the preceding example, these are yourserver-ns.macromedia.com (Certificate A) and ps-breezewin4.macromedia.com (Certificate B).

• Create SSL certificates for both Breeze Server and the Breeze Meeting servers.

If you do not create these certificates, each client must install a trusted certificate when trying to load a presentation or a Live Meeting. If either of the SSL certificates is not installed or if the client doesn’t install the client certificates when prompted on an untrusted site, the SSL solution will not work.

• All requests on port 80 on IP associated with the SSL Certificate A server must be accepted and forwarded to Breeze Server (the IP address for the server where Breeze is installed).

*:80 forward to -> 10.1.204.40:80 (Breeze Server IP)
*:443 forward to -> 10.1.204.40:443

• All requests on the server associated with SSL Certificate B from the IP Breeze IP address and port 1935 must be accepted and then forwarded back to the server where Breeze is installed using port 1935.

*:443 forward to -> 10.1.204.36:1935 (Meeting IP)
10.1.204.36:1935 forward to -> 10.1.204.36:1935 (loop back the request)

All requests coming in to SSL Certificate B are looped back to the Breeze server on port 1935. If you omit any of these four steps, Breeze with SSL support through a hardware accelerator does not work.

Configuring a Breeze Server cluster

Each Breeze Server in a cluster must be able to access the Breeze database. Because licensing restrictions do not allow more than one Breeze Server to access the embedded database engine, you must use Microsoft SQL Server 2000 as the database engine.

To set up a cluster of Breeze Servers:

1. Locate or install SQL Server on a dedicated server.
2. Install and configure the first Breeze Server.

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

   Note: A special cluster license file is required. For more information, contact your Macromedia reps.
3. Confirm that Breeze Server is working correctly.

   For more information on how to test that all the applications in Breeze Server are functioning correctly see, Chapter 5, “Verifying Your Installation,” on page 91.
4. Make sure Breeze Server points to the database server where SQL Server resides.
5. Set up a fully-qualified client-visible Domain Name Service (DNS) name (the direct name) that routes traffic directly to Breeze Server.
   ■ The direct name for each Breeze Server in the cluster should route traffic to ports 80, 443, and 1935 to the corresponding Breeze Server.
   For more information, see “DNS configuration guidelines” on page 59.
6. Set up a load balancer on the network and configure it to listen on port 80.
   ■ Consult the vendor documentation for instructions on how to configure the load balancer.
7. Include each Breeze Server in the cluster in the load balanced pool.
   ■ Make sure that port 80 on the load balancer connects to port 80 on each Breeze server.
   ■ If you are using SSL, configure port 443 on the load balancer to connect to port 8443 on each Breeze Server.
   ■ Consult the vendor documentation for specific instructions on how to include each Breeze Server in the load balancer pool.
8. Install and configure the second Breeze Server in the cluster.
9. Make sure that this Breeze Server also points to the SQL Server.
10. Configure the second Breeze Server with an external DNS name.
    ■ For 'Breeze Web Address', enter the fully-qualified client-visible DNS name that points to the load balancer.
    ■ For each Breeze Server, enter its fully-qualified client-visible DNS name (the direct name.)
11. Repeat steps 8 though 10 for each server in the cluster.

Your Breeze Servers are now clustered. To expand the cluster’s capacity, add new Breeze Servers to the cluster and configure them by following these instructions.

Verifying cluster failover

Failover means that all computers in a cluster have copies of the same contents. If one computer in the cluster fails, the content on another computer in the cluster can take over and supply the same contents. This section describes how to verify that your Breeze Server cluster provides content failover in the event that one of the computers in the cluster fails.

The test is to demonstrate failover when you are using the Breeze Manager, a web application within Breeze Server. If the computer you are accessing for the Breeze Manager fails and you can continue to use Breeze Manager without logging in again and without interruption, failover is successful.

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

To demonstrate failover:
1. Make sure Microsoft SQL Server 2000 is running.
2. Start Breeze Server on Computer1.
   Select Start > Programs > Macromedia > Macromedia Breeze 5 > Start Breeze Server.
   Select Start > Programs > Macromedia > Macromedia Breeze 5 > Stop Breeze Server.
4. Log in to the Breeze Manager.
   You can log in to the Breeze Manager from the following URL:
   \text{http://admin\_host/servlet/admin}
   where \text{admin\_host} is the host name you entered as the value of the \text{ADMIN\_HOST} variable in the Breeze Server custom.ini configuration file.
   When you log in, the Breeze Manager home page opens.
5. Start Breeze Server on Computer2.
7. Click the Reports tab.
   If failover is successful, the Breeze Manager Reports page opens. If the login page opens or any other page is displayed, failover was not successful.
   If the cluster contains more than two computers, apply this start-stop procedure to each computer in the cluster.

Verifying content replication

This section explains how you can verify that content uploaded to one Breeze Server in a cluster is replicated to the other Breeze Server applications in the cluster and is therefore available whenever failover is necessary. As in the preceding section, the following procedure assumes a cluster with two Breeze Presentation platforms.

To verify replication of content across a cluster with two Breeze Presentation platforms:
1. Make sure Microsoft SQL Server 2000 is running.
2. Make sure that Breeze Server on Computer1 is started and that Breeze Server on Computer2 is stopped.
   To start Breeze Server:
   - Select Start > Programs > Macromedia Breeze > Start Breeze Server.
   To stop Breeze Server:
   - Select Start > Programs > Macromedia > Macromedia Breeze 5 > Stop Breeze Server.
3. Log in to the Breeze Manager.
   You can log in to the Breeze Manager from the following URL:
   \text{http://admin\_host/servlet/admin}
   where \text{admin\_host} is the host name you entered as the value of the \text{ADMIN\_HOST} variable in Breeze Server custom.ini configuration file.
   When you log in, the Breeze Manager home page opens.
4. Upload a JPEG image or other content to Breeze Server on Computer1:
   a. Make sure that you are a member of the Account Authors user group.

   To upload content, even if you are an account administrator, you must also be a member of the Account Authors user group. As an account administrator, you can add yourself to the Account Authors group. For information on how to do this, select Breeze Manager Help > Contents > Managing Users and Groups > Managing Groups > Adding members to a group.

   b. Click the Content tab in Breeze Manager.

   The Content page opens.

   c. 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.

   Your test content is displayed.

8. Start Computer2, wait 10 seconds or so, and then stop Computer1.

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.

---

**Maintaining Breeze reliability**

The reliable and secure operation of Breeze demands that your organization create, schedule, and publish certain safekeeping practices, including the following tasks:

- Change the Breeze database password periodically.
- Back up the Breeze database.
- Back up Breeze files.
- Periodically back up the entire Breeze root directory.
- Occasionally delete log files, located in [Boot drive]\breeze\logs, to conserve disk space.
Changing the Breeze password

The password for Breeze Server allows access to the Breeze database. For the integrity of your system security, change the default password if you’re using the Breeze database.

Note: Microsoft SQL Server 2000 users usually already have a password that the database administrator has set.

To change the database password:
1. Open the command prompt window on the computer that is hosting the database.
2. Log in to the Breeze database,
   osql -U sa -P breeze -d breeze
3. Enter the command for the new password, as shown in the following example:
   sp_password @old=breeze, @new='NewPassword', @loginame = 'sa' go

For additional information about changing the password, see the Microsoft article, “How to Verify and Change the MSDE System Administrator Password” at: http://support.microsoft.com/default.aspx?scid=kb;EN-US;322336#3.

Backing up the Breeze database

A database backup creates a duplicate of the data that is in the database. This is a single operation, usually scheduled at regular intervals. To safeguard your Breeze operations, routinely back up the Breeze database. With regularly scheduled backups of the Breeze database, you can recover from many failures, including media failures, user errors, and permanent loss of a server.

The scheduled routine of backing up and restoring databases is useful for other purposes, such as copying a database from one server to another. By backing up a database from one computer and restoring the database to another, a copy of a database can be made quickly and easily.

You can re-create the entire database from a database backup in one step by restoring the database. The restore process overwrites the existing database or creates the database if it does not exist. The restored database matches the state of the database at the time the backup was performed, minus any uncommitted transactions. Uncommitted transactions are rolled back when the database is recovered.

You create backups on backup devices, such as disk or tape media. With SQL Server, you can decide how you want to create your backups on backup devices. For example, you can overwrite outdated backups, or you can append new backups to the backup media.

Best practices for backups

When working with database backups, Macromedia recommends the following best practices:

• Schedule a nightly backup of the Breeze database.
• Maintain backups in a secure place, preferably at a site different from the site where the data resides.
• Keep older backups for a designated amount of time in case the most recent backup is damaged, destroyed, or lost.
• Establish a system for overwriting backups, reusing the oldest backups first.
• Use expiration dates on backups to prevent premature overwriting.
• Label backup media to prevent overwriting critical backups. This allows for easy identification of the data stored on the backup media or the specific backup set.

Backing up the Breeze database with SQL Server utilities

The following utilities are available for creating a backup of a SQL Server database:

• Transact-SQL
• Enterprise Manager
• SQL-DMO
• Create Database Backup Wizard

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

• In Windows, select Start > Programs > Microsoft SQL Server > Enterprise Manager.
• In the Tree pane of the Enterprise Manager window, select the Breeze database (named “breeze,” by default).
• Select Tools > Backup Database.

Macromedia recommends a nightly backup of the Breeze database. Complete instructions for SQL Server database backup and recovery are available at the Microsoft Support site.

Backing up the Breeze database with the embedded database engine

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

To create a Breeze database backup:

1. Log in to the embedded database engine:
   ```
   osql -U sa -P password -d databasename
   ```

2. Run the MSSQL BACKUP DATABASE utility to back up the database.
   For example:
   ```
   BACKUP DATABASE databasename TO DISK = 'c:\msde\backup\databasename.bak'
   ```
   This command writes the database named databasename.bak to the hard disk located in c:\msde\backup.

3. Enter the following command to back up the database to tape:
   ```
   go
   ```
Backing up your Breeze files

You should create backups of the Breeze configuration files and the Breeze content folder:

- Back up the custom.ini found in the breeze directory
- Back up the two config.ini files found in:
  - \c:\breeze\appserv\conf
  - \c:\breeze\comserv\conf
- Back up the content folder in the following location: [Boot drive]\Breeze\content.

To back up your Breeze files:

1. Stop all Breeze services.
   - In Windows, select Start > Programs > Macromedia Breeze > Stop Breeze Server.
2. Make a copy of the content directory within the Breeze installation path.
   - The default location is c:\breeze\content.
3. Make a copy of the config.ini file within the installation path.
   - The default location is c:\breeze\appserv\conf\config.ini.
4. Make a copy of the custom.ini file within the installation path.
   - The default location is c:\breeze\.
After you install and configure Macromedia Breeze, verify that the installation was successful and that all features are functional.

To verify a successful Breeze installation:

1. Verify that the Breeze database and Breeze Server work together (see “Verifying that the Breeze database and Breeze Server work together” on page 92).

2. Verify that you can use Macromedia Breeze Manager, a web application within Breeze Server, and that it can send e-mail messages using your e-mail server (see “Verifying that you can use Breeze Manager and send e-mail notifications” on page 92).

3. Verify that you can use basic features of Breeze Server: publish a presentation to Breeze, save it in the Breeze Server Content library, and then view it (see “Verifying that you can use Breeze Server” on page 94).

4. If you purchased Macromedia Breeze Training, verify that you can use it (see “Verifying that you can use Breeze Training” on page 95).

5. If you purchased Macromedia Breeze Meeting, verify that you can use it (see “Verifying that you can use Breeze Meeting” on page 95).

6. If you purchased the Breeze seminar feature, verify that you can use it (see “Verifying that you can use the Breeze seminar feature” on page 96).

7. If you purchased Macromedia Breeze Events, verify that you can use it (see “Verifying that you can use Breeze Events” on page 96).

If you receive error messages or cannot perform any of the steps, visit the following website for troubleshooting information: www.macromedia.com/go/breezeLicensedSupport.
Verifying that the Breeze database and Breeze Server work together

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

To verify that the Breeze database and Breeze Server work together:

   
   Note: In this URL, hostname is the value you set for the ADMIN_HOST variable in the custom.ini configuration file. This is the Fully Qualified Domain Name (FQDN) of the Breeze Server host computer.

   The Getting Started page for Macromedia Breeze appears. Under the Publish Presentations heading, there is a link for installing Macromedia Breeze Presenter and a link for logging in to Breeze Manager. You will download Breeze Presenter in a later step (see “Verifying that you can use Breeze Server” on page 94).

2. Click the login link.
   
   The Breeze Login window appears.

3. As your login name, enter the value you set for the ADMIN_EMAIL variable in the Application Management Console.

4. As your password, enter the value you set for the ADMIN_PASSWORD variable in the Application Management Console.

   If you can log in successfully, the Breeze Manager home tab appears:
   
   ■ If you do not have Breeze Training, the Training tab is not visible.
   ■ If you do not have Breeze Meeting, the Meetings tab is not visible.
   ■ If you do not have the Breeze seminar feature, the Seminar Rooms tab is not visible.
   ■ If you do not have Breeze Events, the Event Management tab is not visible.

Verifying that you can use Breeze Manager and send e-mail notifications

To verify that you can use Breeze Server and that it can send e-mail messages using your e-mail server, you need to create a new Breeze user, send an e-mail notification to the user, and then confirm that the e-mail was received.

To create a new user and send an e-mail notification:

1. Click the Administration tab on the Breeze Manager home tab.

2. Click the Users and Groups link.
3. Click New User.
   The New User Information page appears and requires the following information:
   - First Name
   - Last Name
   - E-mail
   - Login (the new user's e-mail address is usually his login name)
   - Password (must be between 4 and 16 characters)
4. Enter the required information using the new user's e-mail address in the E-mail text box, and make sure that the E-mail the New User Account Information, Login and Password option is selected.
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, Breeze Server is functional and can send e-mail messages using your e-mail server.
   Here is a sample new user e-mail message.

   Hello John Smythe,

   Welcome! A user account has been created for you on Macromedia Breeze by Ingrid Jones (ijones).

   Macromedia Breeze is an integrated web communication solution for real-time meetings, eLearning, and online presentations that audiences can see and hear anytime, anywhere, through any standard web browser. Depending on which Breeze applications your organization has selected, you'll be able to use Breeze to deliver rich, engaging content through live meetings, online training courses, on-demand presentations, or all three.

   Your account information is as follows:

   Macromedia Breeze Account:

   Account Name: Enterprise Account
   Administrator Contact Information: ijonestycompany.com>

   Please use the following login and password when accessing Macromedia Breeze:

   Your Login ID: jsmythe@mycompany.com
   Your Password: breeze

   To begin using Macromedia Breeze, please browse to the following "Getting Started Guide" at:

In addition to the “Getting Started” guide, we recommend you visit the following resources to learn more about using Macromedia Breeze:

Macromedia Breeze Resource Center (tutorials, best practices, and other resources):
http://www.macromedia.com/resources/breeze/

Macromedia Breeze Support Center (self-service and assisted support options):
http://www.macromedia.com/go/breeze_contact_support_en

Macromedia Breeze Developer Center (technical resources):
http://www.macromedia.com/devnet/breeze/

Thank you,
"Breeze Administrator"<ijones@mycompany.com>

To start using your Macromedia Breeze account, use the following link:
Here, ADMIN_HOST is the value you set for the ADMIN_HOST variable in the Application Management Console.

The URL takes you to the Breeze Getting Started page, from which you can download Breeze Presenter, which is required in the next section.

**Verifying that you can use Breeze Server**

To verify that you can use Breeze Server, send a Microsoft PowerPoint presentation to the Breeze server for compilation into a Macromedia Flash presentation and then view it.

Before you can send a PowerPoint presentation to the Breeze server, you must install Breeze Presenter on a computer on which PowerPoint is already installed.

To create a Breeze Presentation and view it:

1. Go to the URL that you received in the new-user notification (http://ADMIN_HOST/common/help/en/support/startmain.htm). For more information, see “Verifying that you can use Breeze Manager and send e-mail notifications” on page 92.
   A Getting Started page appears, with a link for downloading Breeze Presenter.
2. Click the download link and follow the instructions to install Breeze Presenter.
3. If you do not have a PowerPoint presentation that you can send to the Breeze server for compilation into a Flash presentation, create a presentation of one or two slides and save the presentation.
4. Open the Breeze Publish wizard by selecting Publish from the Breeze menu in PowerPoint.
   The Publish window appears.
5. Select Breeze 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 that you are enrolled in the Authors group.
   When you complete the steps in the Publish wizard, your PowerPoint presentation is uploaded to the Breeze server and compiled into a Flash presentation.
7. When the compilation is complete, go to the Content tab in Breeze Manager and search for your presentation.

8. Open your presentation to view it.

Verifying that you can use Breeze Training

To verify that Breeze Training is functional, go to the Training tab in Breeze Manager. If the Training tab is visible and accessible, Breeze Training is functioning. Make sure that you are enrolled in the Training Managers group.

Verifying that you can use Breeze Meeting

To verify that Breeze Meeting is functional, you create a Breeze meeting and then enter (log in to) the meeting room. Make sure that you are enrolled in the Meeting Hosts group.

To verify that Breeze Meeting is installed and functioning successfully:

1. In Breeze Manager, click the Meetings tab and select New Meeting.

   The Enter Meeting Information page appears and requires the following information:
   - Meeting Name
   - Start Time
   - Duration
   - Select Meeting Template
   - Meeting Access

2. Enter the required information. For the Meeting Access option, select the Only Registered Users and Accepted Guests May Enter the Room option, and then click Next.

   The Select Participants page appears.

3. Select the user you created earlier (see “Verifying that you can use Breeze Manager and send e-mail notifications” on page 92) and click Add, and then click Next.

   The Send Invitations page appears.

4. Click Finish to send the invitations and create the meeting.

   The Meeting Information page for the meeting you created appears. This invitation contains a link to the meeting room in which the meeting is held.

5. When the meeting invitation arrives, click the meeting link.

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

   Use the e-mail address and password for the user you created earlier (see “Verifying that you can use Breeze Manager and send e-mail notifications” on page 92).

7. If the Breeze Meeting Add-in window appears, click Yes.

   If your browser successfully displays the online meeting room for your meeting, Breeze Meeting is functional.
Verifying that you can use the Breeze seminar feature

To verify that the Breeze seminar feature is functional, you create a Breeze seminar in Breeze Manager and then enter (log in to) the seminar room. Make sure that you are enrolled in the Seminar Hosts group.

**To verify that the Breeze seminar feature is installed and functioning successfully:**

1. In Breeze Manager, click the Seminar Rooms tab and select New Seminars.

   The Enter Seminar Information page appears and requires the following information:
   - Seminar Name
   - Start Time
   - Duration
   - Select Seminar Template
   - Seminar Access

2. Enter the required information. For the Seminar Access option, select Only Registered Users and Accepted Guests May Enter the Room, and then click Next.

   The Select Participants page appears.

3. Select the user you created earlier (see “Verifying that you can use Breeze Manager and send e-mail notifications” on page 92) and click Add, and then click Next.

   The Send Invitations page appears.

4. Click Finish to send the invitations and create the seminar.

   The Seminar Information page for the seminar you created appears. This invitation contains a link to the seminar room in which the seminar is held.

5. When the seminar invitation arrives, click the Seminar link.

   A login window for your seminar appears.

6. Log in to enter the seminar as a Registered User.

   Use the e-mail address and password for the user you created earlier (see “Verifying that you can use Breeze Manager and send e-mail notifications” on page 92).

   If your browser successfully displays the online seminar room for your seminar, the Breeze seminar feature is functional.

Verifying that you can use Breeze Events

To verify that Breeze Events is functional, go to the Event Management tab in Breeze Manager. If this tab is visible and accessible, Breeze Events is functioning. Make sure that you are enrolled in the Event Managers group.
A
accelerator
  hardware setup for SSL  84
Adaptor.xml file  78
Application Management Console  43–52
  configuring database settings  44
  database creation confirmation  45
  unsupported upgrades  46
  upgrade confirmation  45
  upgrade in progress  47
B
backing up the Breeze database  88
bandwidth
  calculating usage  12
  requirements  11
best practices
  backing up Breeze files  90
  backing up the Breeze database  88
  changing password  88
  security  21
  single-server configuration  58
  verifying failover  85, 86
  verifying installation  95
Breeze hardware and software requirements
  See Requirements
Breeze Manager  92
Breeze Meeting  95
  bandwidth requirements  11
  starting  11
Breeze Presenter  94
Breeze Server
  cluster  24, 84
  configuring database settings  44
  hardware requirements  25
  integrating learning management systems  61
  load balancer for cluster  24
  multi-server configuration  18
  ports used  22
  security  17
  single-server configuration  18, 58
  software requirements  26
  technical support  55
  technology basics  9
  verifying connection to the Breeze database  92
Breeze T raining  95, 96
C
cluster  84
  adding capacity  85
  Breeze Server  24
  load balancer port  85
  load balancer required  24
  verifying failover  85
  verifying replication of content  86
configuration
  custom.ini file  82
  Directory Service Integration  62
  DNS  59
  multi-server Breeze  18
  single sign-on  61
  single-server Breeze  18
  SSL  77
  custom.ini file  82
D
database backups, best practices  88
database engine
  backing up  88, 89
  Breeze Server requirements  29
  DBMS required  27
  limits of embedded engine  29
  SQL Server recommendations  29
database server, security  17
Directory Service Integration 62–77
configuring 62–71
connection settings 63
define the deletion policies 76
define the password policies 75
defining synchronization actions 70
events in synchronization log file 74
log file format 73
mapping Breeze group profile 68
mapping Breeze user profile 65
planning 13
schedule synchronization 70
user authentication 77
viewing synchronization log files 72
DNS
configuration 59
configuration in cluster 85
Documentation for Breeze 6
Domain Name Service
See DNS

F
failover 85, 86
Flash Communication Server
configuration for SSL 78

H
hardware requirements, Breeze Server 25

I
installation
checklist 35
free disk space requirements 35
overview 35
installing and configuring Breeze 37–42

L
learning management systems
See LMS
license file 50

M
Macromedia online forums 55

N
network security 16, 22
NTFS file system required 35

O
overview
installation 35
post-installation 57
preinstallation 9

P
password
changing the default 88
default for embedded database engine 17
planning
backing up Breeze files 90
backing up the Breeze database 88
bandwidth requirements 11
Breeze Server cluster 24
changing password 88
database backups 88
Directory Service Integration 13
security 15
SSL 14
ports
Breeze Server 22
configuring the FCS ports 77
scanning tool 22
post-installation, overview 57
preinstallation, overview 9

R
requirements
authors and training managers 28
bandwidth 11
Breeze Server 25
free disk space needed for installation 35
load balancer for cluster 24
NTFS file system 35
software for learners and participants 27
software for presenters 28
resources
Breeze Documentation Center 7
Breeze Resource Center 7
Breeze Support 7
documentation 6
security 22

S
Secure Socket Layer
See SSL
security
application-level 19
backing up Breeze files 90
backing up the Breeze database 88
backups 88
best practices 21
Breeze Server 17
changing password 88
database server 17
infrastructure 16
network 16
planning 15
resources and references 22
single-server Breeze 18
system 20
security considerations 15
Server.xml file 78
Single sign on
implementing 61
login policy 62
single sign-on
configuration 61
single-server configuration 18
software requirements
Breeze Server 26
database management system 27
SQL Server
install in mixed-mode 59
security 22
SSL 77–84
Adaptor.xml file 78
configuration options 77
custom.ini file 82
enterprise environments 14
hardware accelerator setup 84
hosted environments 14
implementation with accelerator 82
implementation with FCS 78
planning for 14
required resources for accelerator 82
secured port number 443 15
Server.xml 78
support, Macromedia online forums 55
support, online Breeze 8
system security 20

T
technical support 55
tools, port-scanning 22
troubleshooting resources 8, 54

U
unsupported versions of Breeze 46
upgrading
backing up Breeze files before 32
backing up the database before 33
Breeze version 47
Breeze versions 46
confirmation 45
the system, preparing for 34
uploading the license file 50

V
verifying failover
Breeze Server cluster 85
calcontent in cluster 86
verifying installation 91–96
Breeze Manager 95
Breeze Manager sends e-mail 92
Breeze Presenter 94
Breeze Server connects to database 92
Breeze Training 95, 96